目　录

引论：预备知识

为了方便读者，我们从第1节到第6节扼要叙述了一些基本内容。我们假定读者非常熟悉这些内容（可能的例外是：第2节中集合与本性类之间的区别，用泛映射性质刻划Cartesian积(定理5.2)和递归定理6.2)。以后将常常用到势的定义（第8节第一部分)。选择公理和它的一些等价公理(第7节)以及势的算术(第8节后一部分)可以推迟到实际使用这些知识的时候再读。最后，假定读者熟悉有理数域$\boldsymbol{Q}$，实数域$\boldsymbol{R}$和复数域$\boldsymbol{C}$的基本性质。

1. 逻　辑

我们采用通常的逻辑习惯用语，并且只考虑具有真值“真”或者“假”（但不能同时又真又假)的命题。假设P和Q是两个命题。如果P和Q均是真的，则命题“P并且Q”是真的，否则它便是假的。如果P和Q均是假的，则命题“P或者Q”是假的，否则它便是真的。所谓蕴涵是形如“P推出Q”或者“如果P，则Q”这样的命题（表示成$P\to Q$)。如果P真并且Q假，则这个蕴涵是假的，否则它便是真的。特别地，如果一个蕴涵式的前提假，则此

蕴涵命题永远是真的。所谓等价是形如“P 推出Q并且Q推出P”的命题。通常将它简记为“P当且仅当Q”（表示成 $P\Longleftrightarrow Q$）。如果P和 Q同时真或者同时假，则等价“$P\Longleftrightarrow Q$”是真的，否则它便是假的。命题 P 的否命题为“不是P”。这个否命题真当且仅当命题P假。

2. 集合与类

我们处理集合论的方式是相当随便的。尽管如此，为了定义势（第 8 节）和范畴（第1.7节），我们还是需要介绍集合论中形式公理化的一些基本知识。事实上，假如你愿意的话，整个讨论可以做得非常严密和精确，见 Eisenberg[8] 或者 Suppes[10]。集合论的公理化方法还有另一个好处，就是可避免某些悖论，这些悖论在纯直觉地处理对象时容易引起一些困难。如果一个命题和它的否命题均可以从公理推演出来，则在这个公理系统中就出现悖论。反过来（作为初等逻辑的一个习题），这个悖论又使得该公理系统中的每个命题都是正确的，而这种情况显然是我们所不希望的。

我们将采用公理集合论中的Gödel-Bernays 形式。在这种形式中，原始的（即无定义的）术语是类、成员和相等。直观上，我们把类考虑成是一些对象（元素）组成的集合体 A，使得对于每个给定的对象x，均可以决定x是否为A 的成员（即元素）。我们以$x\in A$表示“x是A的元素”，而以$x\notin A$表示“x不是A的元素”。所有的公理均用这些原始术语和一阶谓词演算来叙述（所谓一阶

谓词演算即是一种语言，它的句子是用连词并且、或者、不、蕴含以及量词存在和所有构造成的)。例如相等便有如下的性质：对于所有的类A，B，C：$A=A$；$A=B\Rightarrow B=A$；$A=B$并且$B=C\Rightarrow A=C$；$A=B$并且$x\in A\Rightarrow x\in B$。而外延性公理是说：具有相同的元素的两个类是相等的(形式上写成：$[x\in A\Leftrightarrow x\in B]\Rightarrow A=B$)。

类A叫作一个集合，当且仅当存在另一个类B，使得$A\in B$。因此集合是一种特殊的类。不是集合的类叫作本性类。集合与本性类的区别在直观上不是很清楚的。粗糙地说，集合是一个"小"类，而本性类则异乎寻常地"大"。类形式公理是说，对于包含变量y的任意一个一阶谓词演算命题$P(y)$，均存在一个类A，使$x\in A\Leftrightarrow$命题$P(x)$真。我们将这个类A表示成$\{x|P(x)\}$，并且说成是"使$p(x)$成立的全部x所组成的类"。有时也把一个类简单地表示成用括号把它的所有元素括起来，例如$\{a, b, c\}$。

例[1] 考虑类$M=\{X|X$是集合，并且$X\notin X\}$。命题$X\notin X$不是不合理的，因为有许多集合满足它(例如全部书组成的集合不是一本书)。M是本性类，因为若M是集合，则或者$M\in M$，或者$M\notin M$但是由M的定义，$M\in M$导致$M\notin M$，而$M\notin M$又导致$M\in M$。所以不论哪一种情形，由假设M为集合均导致一个不能容许的悖论：$M\in M$同时又$M\notin M$。

现在我们复习一些大家所熟悉的内容(并，交，函数，关系，Cartesian 积等等)。这里的表述方式不是很严格的，而且只叙述少量的公理，很多公理我们都略去不提。但是应当知道，存在着充分多的公理，以保证当这些运算在集合上进行时，其结果也是一个集合(例如集合的并是一个集合，集合的子类也是一个集合)。

1. 这个例子首先由Bertrand Russell (以稍微不同的形式) 于1902年给出。当时作为一个悖论，以表明集合论形式公理化的必要性。

证明一个给定的类是集合，通常的办法是证明可以从一些集合通过一系列这些允许的运算而得到它。

类A叫作类B的子类(记为$A\subset B$)，指的是

$$\text{对所有}x\in A,\ x\in A\Rightarrow x\in B \tag{1}$$

根据外延性公理和相等性质，可知：

$$A=B\Longleftrightarrow A\subset B\text{并且}B\subset A$$

如果类B的子类A本身是一个集合，我们也把A称作是B的子集合。有公理保证：一个集合的子类必然是子集合。

没有元素的集合叫作空集合或者零集合，表示成$\varnothing$(即对于任何x均有$x\notin\varnothing$)。由于命题"$x\in\varnothing$"永远假，因此当$A=\varnothing$时，蕴涵式(1)永远真，即对于每个类B均有$\varnothing\subset B$。如果$A\subset B$，$A\neq\varnothing$并且$A\neq B$，我们称A是B的真子类。

幂公理是说：对于每个集合A，由A的所有子集合所构成的类$P(A)$本身也是集合。我们把$P(A)$叫作A的幂集合，它也表示成2^A。

以I(非空类)作下标的集族是对每个$i\in I$取一个集合A_i而构成的集合体。给了这样一个集族，它的并和交分别定义为类

$$\bigcup_{i\in I}A_i=\{x\mid x\in A_i,\ \text{对于某个}\ i\in I\}$$

$$\bigcap_{i\in I}A_i=\{x\mid x\in A_i,\ \text{对于所有}\ i\in I\}$$

如果I是一个集合，则有适当的公理保证$\bigcup_{i\in I}A_i$和$\bigcap_{i\in I}A_i$事实上均是集合。如果$I=\{1,2,\cdots,n\}$。人们常常将$\bigcup_{i\in I}A_i$记为$A_1\cup A_2\cup\cdots\cup A_n$，类似地将$\bigcap_{i\in I}A_i$记为$A_1\cap A_2\cap\cdots\cap A_n$。如果$A\cap B=\varnothing$，便称$A$和$B$是非交的。

如果A和B是类，A在B中的相对补是B的如下子类：

$$B-A=\{x\mid x\in B\text{并且}x\notin A\}.$$

如果全部所讨论的类均是某个固定集合U的子集合（称U为该讨论过程中的万有集合），则将$U-A$记为A'，并且简称作A的补。读者能够验证下列一些命题：

$$A\cap(\bigcup_{i\in I}B_i)=\bigcup_{i\in I}(A\cap B_i) \tag{2}$$

$$A\cup(\bigcap_{i\in I}B_i)=\bigcap_{i\in I}(A\cup B_i)$$

$$(\bigcup_{i\in I}A_i)'=\bigcap_{i\in I}A_i',$$

$$(\bigcap_{i\in I}A_i)'=\bigcup_{i\in I}A_i' \quad \text{(De Morgan 法则)} \tag{3}$$

$$A\cup B=B\Longleftrightarrow A\subset B\Longleftrightarrow A\cap B=A \tag{4}$$

3. 函　数

给了类A和B，从A到B的函数（或者叫作映射）f是指对于每个$a\in A$恰好安排一个元素$b\in B$（记为$f:A\to B$）。b叫作此函数在a的值，或者叫作a的象，通常将它记为$f(a)$。A是此函数的定义域（有时写作Dom f），而B叫作此函数的值域。有时为方便起见，用$a\mapsto f(a)$表达出函数f在A的元素上如何作用。两个函数叫作相等的，是指它们有同样的定义域和值域，并且它们对于公共定义域上的每个元素均有同样的值。

如果$f:A\to B$是一个函数，并且$S\subset A$，则由

$$a\mapsto f(a)\quad(\text{对于}a\in S)$$

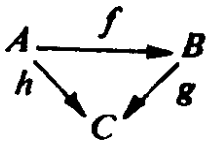
给出的从S到B的函数叫作f在S上的限制，并且表示成$f|S: S\to B$。如果A是任一类，则A上的恒等函数是指由$a\mapsto a$所给出的函数（表示成$1_A: A\to A$）。如果$S\subset A$，则函数$1_A|S: S\to A$叫作是S到A的包含映射。

假设$f: A\to B$和$g: B\to C$均为函数，则f和g的合成是指由下式给出的函数$A\to C$：

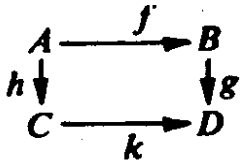
$$a\mapsto g(f(a)),\quad a\in A.$$

这个合成函数记为$g\circ f$，或者简记为gf。如果$h: C\to D$是第三个函数，易知$h(gf)=(hg)f$。如果$f: A\to B$，则$f\circ 1_A=f=1_B\circ f: A\to B$。

函数图表



叫作交换的，是指$gf=h$。类似地，图表



叫作交换的，是指$kh=gf$。我们常常处理由一系列这种三角形和矩形图表组成的更复杂的图表。这样一个图表叫作交换的，是指每个三角形和矩形图表均是交换的。

设$f: A\to B$是一个函数。如果$S\subset A$，则S在f之下的象（表示成$f(S)$）是指类

$$\{b\in B\mid b=f(a),\ \text{对某个}\ a\in S\}$$

类$f(A)$叫作f的象，有时将它表示成$\mathrm{Im}f$。如果$T\subset B$，则T在f作用下的原象（表示成$f^{-1}(T)$）是指类

$$\{a\in A\mid f(a)\in T\}$$

如果T只包含一个元素，$T=\{b\}$，我们也用$f^{-1}(b)$代替$f^{-1}(T)$。容易证明下面一些事实：

$$\text{对于}S\subset A,\ f^{-1}(f(S))\supset S \tag{5}$$

$$\text{对于}T\subset B,\ f(f^{-1}(T))\subset T \tag{6}$$

对于B的任意一个子集族$\{T_i\mid i\in I\}$，

$$f^{-1}\left(\bigcup_{i\in I}T_i\right)=\bigcup_{i\in I}f^{-1}(T_i) \tag{7}$$

$$f^{-1}\left(\bigcap_{i\in I}T_i\right)=\bigcap_{i\in I}f^{-1}(T_i) \tag{8}$$

函数$f: A\to B$叫作单射（或者叫作一对一的），是指

对于所有的$a,a'\in A$，$a\neq a'\Rightarrow f(a)\neq f(a')$。换句话说，$f$是单射当且仅当

对于所有的$a,a'\in A$，$f(a)=f(a')\Rightarrow a=a'$。函数$f$叫作满射（或者叫作映上），是指$f(A)=B$。换句话说，即是指

对每个$b\in B$，均有$a\in A$，使得$b=f(a)$。函数f叫作一一对应，是指它同时是单射和满射。从这些定义立刻得知，对于任意一个类A，恒等映射$1_A: A\to A$是一一对应。读者可以证明，对于映射$f: A\to B$和$g: B\to C$我们有：

$$f\text{和}g\text{均为单射}\Rightarrow gf\text{为单射} \tag{9}$$

$$f\text{和}g\text{均为满射}\Rightarrow gf\text{为满射} \tag{10}$$

$$gf\text{为单射}\Rightarrow f\text{为单射} \tag{11}$$

$$gf\text{为满射}\Rightarrow g\text{为满射} \tag{12}$$

定理3.1 假设$f: A\to B$是一个函数，并且A是非空的，则

(i) f为单射$\Longleftrightarrow$存在映射$g: B\to A$，使得$gf=1_A$。

(ii) 如果A是一个集合，则f为满射$\Longleftrightarrow$存在映射$h: B\to A$，

使得$fh=1_B$。

证明 因为每个恒等映射都是一一对应，从而由(11)和(12)式即可推出(i)和(ii) 中的(⇐)部分。反之，如果f是单射，那末对于每个$b\in f(A)$，均存在唯一的$a\in A$，使得 $f(a)=b$。取一个固定的$a_0\in A$，定义

$$g:\ B\to A,\quad g(b)=\begin{cases}a, & \text{如果}b\in f(A),\ \text{并且}f(a)=b.\\ a_0, & \text{如果}b\notin f(A).\end{cases}$$

容易验证$gf=1_A$.对于(ii)的(⇒)部分，假设f是满射,那末对于每个$b\in B$，$f^{-1}(b)\subset A$均是非空集合.对于每个$b\in B$,取$a_b\in f^{-1}(b)$（注意：这需要选择公理，见第7节)。定义映射 h：$B\to A$，$h(b)=a_b$，容易验证$fh=1_B$。∎

定理3.1中的映射g叫作f的左逆，而h叫作f的右逆.如果映射f：$A\to B$同时有左逆g和右逆h，则

$$g=g1_B=g(fh)=(gf)h=1_Ah=h.$$

我们把映射$g=h$叫作f的双侧逆。上面的推理也表明,一个映射如果有双侧逆的话，那末它的双侧逆是唯一的。根据定理3.1,如果A是一个集合，而f：$A\to B$是一个函数，则

f为一一对应$\Longleftrightarrow f$有双侧逆[2]。 (13)

一一对应f的唯一的双侧逆表示成f^{-1}。显然f为f^{-1}的双侧逆，因此f^{-1}也是一一对应。

4. 关系与分拆

成对公理是说，对于任意两个集合[元素]a和b，均存在一个

2.事实上，当A为本性类时，(13) 也是成立的.见Eisenberg[8；第146页]。

集合$P=\{a, b\}$，使得$x\in P\Longleftrightarrow x=a$或者$x=b$。如果$a=b$，则$P$为一元集合$\{a\}$。一个有序对$(a, b)$定义为集合$\{\{a\},\{a, b\}\}$。$a$和$b$分别称为它的第一分量和第二分量。不难看出，$(a,b)=(a', b')\Longleftrightarrow a=a'$并且$b=b'$。类$A$和$B$的Cartesian积是类

$$A\times B=\{(a,b)\mid a\in A, b\in B\}。$$

注意$A\times\varnothing=\varnothing=\varnothing\times B$。

$A\times B$的一个子类R叫作$A\times B$上的一个关系。例如若$f: A\to B$是一个函数，则f的图象是关系$R=\{(a,f(a))\mid a\in A\}$。由于$f$是函数，从而$R$有如下特殊性质：

A中每个元素恰好是R中一个序对的第一分量　　(14)

反过来，$A\times B$上任一关系R如果满足(14)，它便决定唯一的函数$f: A\to B$，使f的图象是R(这只要定义$f(a)=b$即可，其中(a,b)是R中第一分量为a的(唯一的)序对)。基于此，在集合论的形式公理化表达方式中，习惯上将函数等同于它的图象，即将函数定义成满足(14)的一个关系。比如，为了从公理系统证明一个集合在一个函数作用下的象仍旧是集合，就需要这样做。

这种方法的另一个好处是使我们可以定义其定义域为空集合的函数。由于$\varnothing\times B=\varnothing$是$\varnothing\times B$的唯一的子集合，并且它自然满足(14)，从而有唯一的函数$\varnothing\to B$。从(14)也可知道，一个函数若值域为空集合，则定义域也必为空集合。今后只要方便，我们就把函数看作是满足(14)的一个关系。

$A\times A$上的关系R叫作A上的等价关系，是指R满足下述三个条件：

自反性：对于每个$a\in A$，$(a,a)\in R$　　(15)

对称性：$(a,b)\in R\Rightarrow(b,a)\in R$　　(16)

传递性：$(a,b)\in R$，$(b,c)\in R\Rightarrow(a,c)\in R$　　(17)

如果R是A的等价关系，并且$(a, b)\in R$. 我们便称在R之下a与b等价，记为$a\sim b$或者aRb. 用这样的符号，则(15)—(17)变成

$$a\sim a \tag{15'}$$

$$a\sim b\Rightarrow b\sim a \tag{16'}$$

$$a\sim b,\ b\sim c\Rightarrow a\sim c \tag{17'}$$

设$R(\sim)$是A上的等价关系. 如果$a\in A$，则a的等价类是指A中等价于a的所有元素构成的类，表示成$\bar{a}$. 即$\bar{a}=\{b\in A\mid b\sim a\}$. A中所有等价类构成的类表示成A/R，叫作A对于关系R的商类. 由于R的自反性，可知对于每个$a\in A$，$a\in\bar{a}$. 于是

$$\text{如果}A\text{为集合，则对每个}a\in A,\ \bar{a}\neq\varnothing \tag{18}$$

$$\bigcup_{a\in A}\bar{a}=A=\bigcup_{\bar{a}\in A/R}\bar{a} \tag{19}$$

此外还有

$$\bar{a}=\bar{b}\iff a\sim b. \tag{20}$$

因为若$\bar{a}=\bar{b}$，则$a\in\bar{a}\Rightarrow a\in\bar{b}\Rightarrow a\sim b$. 反之若$a\sim b$，而$c\in\bar{a}$，则$c\sim a$并且$a\sim b\Rightarrow c\sim b\Rightarrow c\in\bar{b}$. 因此$\bar{a}\subset\bar{b}$. 根据对称性又可知$\bar{b}\subset\bar{a}$. 因此$\bar{a}=\bar{b}$. 进而我们证明

$$\text{对于}a,\ b\in A,\ \text{或者}\bar{a}\cap\bar{b}=\varnothing,\text{或者}\ \bar{a}=\bar{b} \tag{21}$$

这是因为，如果$\bar{a}\cap\bar{b}\neq\varnothing$，则有元素$c\in\bar{a}\cap\bar{b}$. 于是$c\sim a$并且$c\sim b$. 利用对称性、传递性和(20)，我们有$a\sim c$并且$c\sim b\Rightarrow a\sim b\Rightarrow\bar{a}=\bar{b}$.

假设A是一个非空类，而$\{A_i\mid i\in I\}$是A的一个子集族，满足

$$A_i\neq\varnothing\ (\text{对每个}i)$$

$$\bigcup_{i\in I}A_i=A$$

$$\text{当}i\neq j\in I\text{时，}\ A_i\cap A_j=\varnothing.$$

这时，我们称$\{A_i\mid i\in I\}$为A的一个分拆

定理4.1 如果A是非空集合，则$R\longmapsto A/R$定义了从A上全部等价关系构成的集合$E(A)$到A的所有分拆构成的集合$Q(A)$之上的一一对应。

证明概要 如果R是A上的等价关系，由(18)，(19)和(21)可知等价类集合A/R是A的一个分拆从而$R\longmapsto A/R$定义出一个函数$f:E(A)\to Q(A)$。现在如下定义一个函数$g:Q(A)\to E(A)$：如果$S=\{A_i\mid i\in I\}$是A的一个分拆，以$g(S)$表示如下给出的A上一个等价关系：

$a\sim b\Longleftrightarrow$有(唯一)$i\in I$，使$a\in A_i$并且$b\in A_i$。证明$g(S)$事实上是一个等价关系，并且对$a\in A_i$有$\bar{a}=A_i$。然后证明$fg=1_{Q(A)}$，$gf=1_{E(A)}$。根据(13)便知$f$是一一对应。∎

5. 积

注：本节中我们只处理集合，不涉及本性类。

考虑两个集合的Cartesian积$A_1\times A_2$。$A_1\times A_2$中的元素为(a_1, a_2)，其中$a_i\in A_i$，$i=1,2$。从而(a_1,a_2)决定出一个函数$f:\{1,2\}\to A_1\cup A_2$，$f(1)=a_1, f(2)=a_2$。反之，每个函数$f:\{1,2\}\to A_1\cup A_2$如果具有性质"$f(1)\in A_1$，$f(2)\in A_2$"，则f也决定出$A_1\times A_2$中一个元素$(a_1,a_2)=(f(1), f(2))$。从而不难看出，这种函数构成的集合和集合$A_1\times A_2$之间存在着一一对应。这一事实使我们把Cartesian积以下面的形式加以推广。

定义5.1 假设$\{A_i\mid i\in I\}$是一个集族，它的(非空)下标集合

为I，则诸集合A_i的Cartesian积是指集合

$$\{\text{函数}f: I\to\bigcup_{i\in I}A_i \mid \text{对每个}i\in I,\ f(i)\in A_i\}.$$

我们将它表示成$\prod_{i\in I}A_i$。

与$I=\{1,2\}$的情形一样，每个$f\in\prod_{i\in I}A_i$由它的象$\{f(i)\mid i\in I\}$所完全决定，即由形如$\{a_i\mid \text{对每个}i\in I,\ a_i\in A_i\}$的一个集合所完全决定。为方便起见，往往将函数$f$与这样一个集合等同(即对于每个$i$令$a_i=f(i)$)。并且(在不会发生混淆时)将这个集合表示成$\{a_i\}_{i\in I}$或者简记为$\{a_i\}$。同样地，如果$I=\{1,2,\cdots,n\}$，则积$\prod_{i\in I}A_i$常常表示成$A_1\times A_2\times\cdots\times A_n$，并且将它等同于所有$n$-序组$(a_1,a_2,\cdots,a_n)(a_i\in A_i,\ i=1,2,\cdots,n)$所构成的集合。

如果某个$A_j=\varnothing$，则$\prod_{i\in I}A_i=\varnothing$。因为没有函数$f: I\to\cup A_i$使得$f(j)\in A_j$。

如果$\{A_i\mid i\in I\}$和$\{B_i\mid i\in I\}$均是集族，并且对于每个$i\in I$，$B_i\subset A_i$，则每个函数$I\to\bigcup_{i\in I}B_i$均可考虑成函数$I\to\bigcup_{i\in I}A_i$。从而我们可以将$\prod_{i\in I}B_i$看成是$\prod_{i\in I}A_i$的子集合。

假设$\prod_{i\in I}A_i$是Cartesian积。对于每个$k\in I$，定义映射π_k：$\prod_{i\in I}A_i\to A_k$，$f\longmapsto f(k)$，或者采用另一种记号：$\{a_i\}\longmapsto a_k$。我们将π_k叫作此Cartesian积在它第k分量(或第k因子)上的(正则)射影。如果每个A_i均非空，则每个π_k均是满射(见习题7.6)。

Cartesian积$\prod_{i\in I}A_i$和它的射影正是我们证明下一定理所需要的。

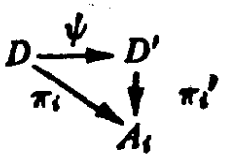
定理5.2 假设$\{A_i \mid i\in I\}$是下标集合为I的集族，则存在一个集合D和映射族$\{\pi_i: D\to A_i \mid i\in I\}$满足以下性质：对于每个集合$C$和映射族$\{\varphi_i: C\to A_i \mid i\in I\}$，均存在唯一的映射$\varphi: C\to D$，使得对每个$i\in I$均有$\pi_i\varphi=\varphi_i$，进而，$D$唯一决定到相差一个一一对应。

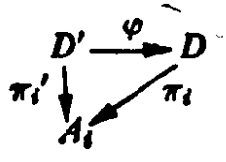
后一句话的意思是：如果集合D'和映射族$\{\pi_i': D'\to A_i \mid i\in I\}$有与$D$和$\{\pi_i\}$同样性质，则存在一一对应$D\to D'$。

证明（存在性） 令$D=\prod_{i\in I} A_i$，而映射π_i是到第i分量上的射影。给了C和诸映射φ_i，定义$\varphi: C\to\prod_{i\in I} A_i$，$c\longmapsto f_c$，其中$f_c(i)=\varphi_i(c)\in A_i$。易知对每个$i\in I$均有$\pi_i\varphi=\varphi_i$。为证$\varphi$的唯一性，我们假定$\varphi': C\longrightarrow\prod_{i\in I} A_i$是另一个映射，使对每个$i\in I$均有$\pi_i\varphi'=\varphi_i$。要证$\varphi=\varphi'$。为此我们必需对于每个$c\in C$，证明$\varphi(c)$和$\varphi'(c)$是$\prod_{i\in I} A_i$中同一元素。即要证$\varphi(c)$和$\varphi'(c)$作为$I$上的函数是一致的。即要证对于每个$i\in I$均有$(\varphi(c))(i)=(\varphi'(c))(i)$。但是由假设和$\pi_i$的定义，可知对于每个$i\in I$均有：

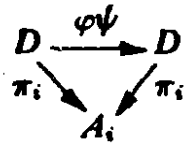
$$(\varphi'(c))(i)=\pi_i\varphi'(c)=\varphi_i(c)=f_c(i)=(\varphi(c))(i).$$

（唯一性） 设D'（和诸映射$\pi_i': D'\to A_i$）与$D=\prod_{i\in I} A_i$有同样性质。如果我们将（对于D的）那个性质用于映射族$\{\pi_i': D'\to A_i\}$，而将（对于D'的）同样性质用于映射族$\{\pi_i: D\to A_i\}$，便得到（唯一的）映射$\varphi: D'\to D$和$\psi: D\to D'$，使得对于每个$i\in I$，下面的图表都是交换的：





将二者合在一起，可以对每个 $i\in I$，使下面的图表均是交换的。



从而$\varphi\psi$：$D\to D$是一个映射，使得对每个$i\in I$均有$\pi_i(\varphi\psi)=\pi_i$。但是根据上述证明，只有唯一的映射具有此性质。由于1_D：$D\to D$也满足$\pi_i 1_D=\pi_i(\forall i\in I)$，从唯一性我们必需有$\varphi\psi=1_D$。类似的推理可证$\psi\varphi=1_{D'}$。从(13)便知$\varphi$是一一对应，而$D=\prod_{i\in I}A_i$唯一决定的到相差一个一一对应。∎

注意：定理5.2的叙述中没有提到元素，而只涉及到集合与映射。它实际上意味着，Cartesian积$\prod_{i\in I}A_i$可以用某个泛映射性质来刻划。今后在处理范畴和函子的时候，我们还会更精确地讨论这一概念。

6. 整　数

我们不打算用公理方法介绍整数，而是假定读者完全熟悉整数集合$\mathbb{Z}$，我们有

$$(a+b)+c=a+(b+c),\quad (ab)c=a(bc)\quad \text{(结合律)} \tag{23}$$

$$a+b=b+a,\quad ab=ba\quad \text{(交换律)} \tag{24}$$

$$a(b+c)=ab+ac,\quad (a+b)c=ac+bc\quad \text{(分配律)} \tag{25}$$

$$a+0=a,\quad a1=a \tag{26}$$

对于每个$a\in\boldsymbol{Z}$，均有$-a\in\boldsymbol{Z}$，使得$a+(-a)=0$(加法逆)

(27)

我们用$a-b$表示$a+(-b)$.

$$ab=0\Longleftrightarrow a=0 \text{ 或者 } b=0 \tag{28}$$

$$a<b\Rightarrow a+c<b+c \text{ (对于每个}c\in\boldsymbol{Z}\text{)} \tag{29}$$

$$a<b\Rightarrow ad<bd \text{ (对于每个}d\in\boldsymbol{N}^{*}\text{)} \tag{30}$$

我们认为$a<b$和$b>a$是一回事，而以$a\leqslant b$表示$a<b$或者$a=b$.$a\in\boldsymbol{Z}$的绝对值定义为 $|a|=a$(如果$a\geqslant 0$)，或$-a$(如果$a<0$).最后，作为基本公理我们假定

良序公理 $\boldsymbol{N}$ 的每个非空子集S均包含极小元素(即元素$b\in S$,使得对每个$c\in S$，$b\leqslant c$).

特别地，0为$\boldsymbol{N}$的极小元素.

除了上述之外，我们还需要初等数论中的一些事实，在这里我们简要地复习其中某些事实.

定理6.1 (数学归纳法) 如果S是自然数集合$\boldsymbol{N}$的一个子集合，$0\in S$，并且下面两个条件中有一条成立：

(i) $n\in S\Rightarrow n+1\in S$(对所有的$n\in\boldsymbol{N}$).

(ii) $m\in S(m=0,\ 1,\ \cdots,\ n-1)\Rightarrow n\in S$(对所有$n\in\boldsymbol{N}$)，则$S=\boldsymbol{N}$.

证明 如果$\boldsymbol{N}-S\neq\varnothing$,以$n\neq 0$表示它的极小元素，那末对每个$m<n$，$m\notin\boldsymbol{N}-S$，从而$m\in S$.由此从(i)或者(ii)均推出 $n\in S$，这就导致矛盾.从而$\boldsymbol{N}-S=\varnothing$，即$\boldsymbol{N}=S$. ∎

注：对于任一$c\in\boldsymbol{N}$，将0，$\boldsymbol{N}$分别改成c和 $M_c=\{x\in\boldsymbol{Z}\mid x\geqslant c\}$之后，定理6.1仍旧成立.

为了保证今后(例如后面的定理8.8和III.3.7)的正确性，我们需要一个技术性结果：

定理6.2 （逆归定理） 假设S是一个集合，$a\in S$，并且对于每个$n\in \boldsymbol{N}$，$f_n: S\to S$ 均是函数，则存在唯一的函数$\varphi: \boldsymbol{N}\to S$，使得$\varphi(0)=a$并且$\varphi(n+1)=f_n(\varphi(n))(\forall n\in \boldsymbol{N})$。

证明概要 我们将构作 $\boldsymbol{N}\times S$ 上的一个关系 R，使得它是满足上述性质的函数$\varphi: \boldsymbol{N}\to S$的图象，令

$\mathcal{J}=\{Y\subset \boldsymbol{N}\times S\mid (0,\ a)\in Y$,并且$(n,x)\in Y\Rightarrow(n+1,\ f_n(x))\in Y(\forall n\in \boldsymbol{N})\}$由于$\boldsymbol{N}\times S\in\mathcal{J}$,从而$\mathcal{J}\neq\varnothing$。令$R=\bigcap_{Y\in\mathcal{J}} Y$，则 $R\in\mathcal{J}$。又设M为子集合

$\{n\in \boldsymbol{N}\mid$存在唯一的$x_n\in S$，使得$(n,x_n)\in R\}$，我们归纳证明$M=\boldsymbol{N}$。如果$0\notin M$,则有$(0,b)\in R$,其中$b\neq a$，并且集合$R-\{(0,b)\}\subset \boldsymbol{N}\times S$属于$\mathcal{J}$。从而$R=\bigcap_{Y\in\mathcal{J}} Y\subset R-\{(0,\ b)\}$，这就导致矛盾。因此$0\in M$。现在假定$n\in M$(即有唯一的$x_n\in S$,使得$(n,x_n)\in R$),则$(n+1,\ f_n(x_n))\in R$。如果又有$(n+1,c)\in R$,而$c\neq f_n(x_n)$，则 $R-\{(n+1,\ c)\}\in\mathcal{J}$(验证！)，由此又可象上面那样导致矛盾。因此$x_{n+1}=f_n(x_n)$是$S$中唯一的元素，使得$(n+1,\ x_{n+1})\in R$。于是由归纳法(定理6.1)可知$\boldsymbol{N}=M$，即$n\longmapsto x_n$定义了一个函数$\varphi: \boldsymbol{N}\to S$，它的图象为$R$。由于$(0,\ a)\in R$，从而$\varphi(0)=a$。对于每个$n\in \boldsymbol{N}$，$(n,\ x_n)=(n,\ \varphi(n))\in R$。由于$R\in\mathcal{J}$，从而$(n+1,\ f_n(\varphi(n)))\in R$。但是 $(n+1,\ x_{n+1})\in R$。由 x_{n+1} 的唯一性推出$\varphi(n+1)=x_{n+1}=f_n(\varphi(n))$。∎

如果A是非空集合,A中的序列是一个函数$\boldsymbol{N}\to A$。一个序列通常表示成$\{a_0,a_1,\cdots\}$，$\{a_i\}_{i\in N}$或者$\{a_i\}$，其中$a_i\in A$是$i\in \boldsymbol{N}$的

象。类似地，函数$\boldsymbol{N}^*\to A$也称作序列，并且表示成$\{a_1,a_2,\cdots\}$，$\{a_i\}i\in\boldsymbol{N}^*$或者$\{a_i\}$，这些符号在课文中不会引起混乱。

定理6.3 （除法算式） 如果a，$b\in\boldsymbol{Z}$，$a\neq0$，则存在唯一的一对整数q和r，使得$b=aq+r$并且$0\leqslant r<|a|$。

证明概要 先证$S=\{b-ax|x\in\boldsymbol{Z},\ b-ax\geqslant0\}$是$\boldsymbol{N}$的非空子集合，从而包含一个极小元素$r=b-aq$(对于某个$q\in\boldsymbol{Z}$)。因此$b=aq+r$。然后根据$r$为$S$中极小元这一事实来证明$0\leqslant r<|a|$和$q$，$r$的唯一性。∎

我们称整数$a\neq0$整除整数b(写成$a\mid b$)，是指存在整数k，使得$ak=b$。如果a不能整除b，则记为$a\nmid b$。

定义6.4 正整数c叫作整数a_1，a_2，…，a_n的最大公因数，是指

(1) $c|a_i$ $(1\leqslant i\leqslant n)$，

(2) $d\in\boldsymbol{Z}$并且$d|a_i(1\leqslant i\leqslant n)\Rightarrow d|c$。

我们将c表示成$(a_1,a_2,\cdots,a_n)$。

定理6.5 如果a_1，a_2，…，a_n是整数并且不全为0，则$(a_1,a_2,\cdots,a_n)$存在，并且存在整数k_1，k_2，…，k_n，使得

$$(a_1,a_2,\cdots,a_n)=k_1a_1+k_2a_2+\cdots+k_na_n。$$

证明概要 利用除法算式证明非空集合$S=\{x_1a_1+x_2a_2+\cdots+x_na_n|x_i\in\boldsymbol{Z},\ \sum_i x_ia_i>0\}$的极小正元素即是$a_1$，$a_2$，…，$a_n$的最大公因数。详见shockley[51，第10页]。∎

整数a_1，a_2，…，a_n称为互素的，是指$(a_1,a_2,\cdots,a_n)=1$。

正整数$p>1$称为素数，是指它只有因子± 1和$\pm p$。因此，如果p为素数而$a\in\mathbb{Z}$，则或者$(a, p)=p$(当$p|a$时)，或者$(a,p)=1$(当$p\nmid a$时)。

定理6.6 如果a和b是互素的整数，并且$a|bc$，则$a|c$。如果p为素数并且$p|a_1a_2\cdots a_n$，则有某个i使得$p|a_i$。

证明概要 从定理6.5有$1=ra+sb$，因此$c=rac+sbc$，于是$a|c$。对n归纳即可证第二论断。∎

定理6.7 (算术基本定理) 每个正整数$n>1$均可唯一地写成如下形式

$$n=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$$

其中$p_1<p_2<\cdots<p_k$均为素数，而$t_i>0$(对于每个i)。

证明可用归纳法。见shockley[51，第17页]。∎

假设$m>0$为一固定的整数。如果a，$b\in\mathbb{Z}$并且$m|(a-b)$，便称a与b模m同余，并且表示成$a\equiv b(\mathrm{mod}m)$。

定理6.8 假设$m>0$为整数而a，b，c，$d\in\mathbb{Z}$。

(i) 模m同余是整数集合$\mathbb{Z}$上的等价关系，并且恰好有m个等价类。

(ii) 如果$a\equiv b(\mathrm{mod}m)$，$c\equiv d(\mathrm{mod}m)$，则$a+c\equiv b+d(\mathrm{mod}m)$，$ac\equiv bd(\mathrm{mod}m)$。

(iii) 如果$ab\equiv ac(\mathrm{mod}m)$并且$a$和$m$互素，则$b\equiv c(\mathrm{mod}m)$。

证明 (i) 从定义容易推出模m是等价关系。将整数a的等价类记为$\bar{a}$。注意性质(20)在这里可以叙述成

$$\bar{a}=\bar{b}\Longleftrightarrow a\equiv b(\mathrm{mod}m) \qquad (20')$$

给了任一$a\in\mathbb{Z}$，存在整数q和r，$0\leqslant r<m$，使得$a\equiv mq+r$．于是$a-r=mq$，即$a\equiv r(\mathrm{mod}m)$．由(20′)可知$\bar{a}=\bar{r}$．由于a是任意整数而$0\leqslant r<m$，从而每个等价类必为$\bar{0}$，$\bar{1}$，$\bar{2}$，$\bar{3}$，…，$\overline{(m-1)}$中之一个．但是这m个等价类是两两不同的：因为如果$0\leqslant i<j<m$，则$0<(j-i)<m$．从而$m\nmid(j-i)$．因此$i\not\equiv j(\mathrm{mod}m)$．由(20′)即知$\bar{i}\neq\bar{j}$．这就表明恰有$m$个等价类．

(ii) 由条件可知$m|a-b$和$m|c-d$．从而$m|(a-b)+(c-d)=(a+c)-(b+d)$，因此$a+c=b+d(\mathrm{mod}m)$．同样地，$m|(a-b)c+(c-d)b=ac-bc+bc-bd=ac-bd$，从而$ac\equiv bd(\mathrm{mod}m)$．

(iii) 由于$ab\equiv ac(\mathrm{mod}m)$，$m|a(b-c)$．但是$(m,a)=1$．由定理6.6可知$m|(b-c)$，即$b\equiv c(\mathrm{mod}m)$．∎

7. 选择公理，序和Zorn引理

注：本节只处理集合，而不涉及本性类，

如果$I\neq\varnothing$而$\{A_i|i\in I\}$是一个集族，使对每个$i\in I$，$A_i\neq\varnothing$，我们希望知道是否$\prod_{i\in I}A_i\neq\varnothing$．有人证明了，这个看来似乎是很自然的结论是不能由集合论通常一些公理推导出来的（虽然它与这些通常公理也不是不相容的．参见P.J.Cohen[59]）．所以我们假定

选择公理 由一些非空集合所构成的集族，如果其下标集合是非空的，则它们的积集合也是非空的．

选择公理的另一形式见习题 4．还有两个命题等价于选择公理，它们在证明许多重要定理时起着关键性的作用。为了叙述这两个等价的命题，我们还需要引进另一些概念。

所谓半序集合是一个非空集合A与$A\times A$上一个关系R（这个关系称作是A上的半序），并且R满足自反性，传递性(见第4节中的(15)和(17))以及

反对称性：$(a,b)\in R$并且$(b,a)\in R\Rightarrow a=b$　　(31)

如果R是A上的半序，我们通常将$(a,b)\in R$记成$a\leqslant b$。用这种符号，则条件(15)，(17)和(31)变成为(对所有a，b，$c\in A$)：

$a\leqslant a$；

$a\leqslant b$，$b\leqslant c\Rightarrow a\leqslant c$；

$a\leqslant b$，$b\leqslant a\Rightarrow a=b$。

如果$a\leqslant b$并且$a\neq b$，我们记为$a<b$。

元素a和$b\in A$叫作是可比较的，如果$a\leqslant b$或者$b\leqslant a$。但是，在半序集合中两个给定的元素不一定是可比较的。对于集合A的一个半序，如果任意两个元素均可比较，我们便称它是线性序（或者叫作全序或简单序）。

例　设A是{1，2，3，4，5}的幂集合(即它的全部子集所构成的集合)。定义$C\leqslant D$为$C\subset D$，则A是半序，但不是线性序（例如{1，2}和{3，4}便不可比较)。

假设$(A,\leqslant)$是一个半序集。元素$a\in A$叫作A中的极大元，是指对于每个$c\in A$，若c与a可比较，则必然$c\leqslant a$。换句话说，即对于每个$c\in A$，$a\leqslant c\Rightarrow a=c$。注意如果$a$为极大元，它不需要对每个$c\in A$均有$c\leqslant a$(即可能存在$c\in A$与$a$不可比较)。此外，一个给定的半序集合可能有许多极大元（习题5)，也可能没有极大元(如$\mathbb{Z}$对于通常的序)。A的非空子集合B的上界是指元素$d\in A$，

使得对每个 $b\in B$，$b\leqslant d$．A的一个非空子集B若对于$\leqslant$为线性序集合，则称B是A中的一个链．

Zorn引理 假设A是非空半序集．如果A中每个链均有上界，则A必包含有极大元．

如果集合论的所有其他的通常公理均保持，可以证明，Zorn引理等价于选择公理．参见E.Hewitt 和 K.Stromberg[57，第14页]．Zorn引理是非常有用的工具，我们今后经常使用它．

假设B是半序集合$(A，\leqslant)$的非空子集合．元素$c\in B$叫作B的最小元，如果对于每个$b\in B$，均有$c\leqslant b$．如果A的每个非空子集均有最小元，便称A为良序集合．每个良序集合都是线性序集合(但反之则不然)，因为对于任意的a，$b\in A$，子集合$\{a，b\}$必有最小元，即或者$a\leqslant b$或者$b\leqslant a$．可以证明，下面命题与选择公理也是等价的(见E.Hewitt和K.Stromberg[57，第14页])．

良序原则 如果A是非空集合，则存在着A的一个线性序$\leqslant$，使$(A，\leqslant)$为良序集合．

例 我们已经看到(第6节) 自然数集合$\boldsymbol{N}$是良序集合．整数集合对于通常的序是线性序集合，但不是良序集合（例如，负整数子集合不存在最小元)．但是下面几个都是$\boldsymbol{Z}$的良序（其中$a<b\Longleftrightarrow a$在b之左)：

(i) 0，1，-1，2，-2，3，-3，…，n，$-n$，…；

(ii) 0，1，3，5，7，…，2，4，6，8，…，-1，-2，-3，-4，…；

(iii) 0，3，4，5，6，…，-1，-2，-3，-4，…，1，2．

这些序彼此是很不相同的．序(i)中每个非零元素a都有直接先导

(即元素c，使得a是子集合$\{x|c<x\}$的最小元)。但是序(ii)中的-1和2与序(iii)中的-1和1均没有直接先导。另一方面，序(i)和(ii)中没有极大元，而序(iii)中2为极大元。在所有三种序中，0均为整个序集的最小元。

良序原则的主要益处是可以将对于正整数的数学归纳法（定理6.1)推广到任意良序集合上：

定理7.1 （超限归纳法） 如果B是良序集合$(A, \leqslant)$的子集合，并且对于每个$a\in A$均有

$$\{c\in A\,|\,c<a\}\subset B \Rightarrow a\in B,$$

则$B=A$。

证明 如果$A-B\neq\varnothing$，则存在最小元$a\in A-B$。由最小元和$A-B$的定义，可知$\{c\in A\,|\,c<a\}\subset B$。再由假设推出$a\in B$，从而$a\in B\cap(A-B)=\varnothing$，这就导致矛盾。因此$A-B=\varnothing$，即$A=B$。∎

习　题

1. 假设$(A,\leqslant)$为半序集合，而B为非空子集合.B的下界是元素$d\in A$，使得对于每个$b\in B$，$d\leqslant b$.B的下端是B的一个下界d_0，使得对于B的任何一个下界d，$d\leqslant d_0$. B的上端是B的一个上界t_0，使得对于B的任何一个上界t均有$t_0\leqslant t$.称$(A,\leqslant)$是格，是指对任意$a,b\in A$，集合$\{a, b\}$均有上端和下端。

   (a) 如果$S\neq\varnothing$，则幂集合$P(S)$对于集合论的包含序是格，并且有唯一的极大元。

   (b) 给出不是格的半序集合的例子。

   (c) 给出没有极大元的格和具有两个极大元的半序集的例子。

2. 格$(A,\leqslant)$叫作是完备的，如果A的每个非空子集均有下端和上端.半序集合之间的映射f：$A\to B$叫作是保序的，如果$a\leqslant a'$（在A中）$\Rightarrow f(a)\leqslant f(a')$（在$B$中）.求证：完备格$A$到自身的保序映射$f$必有固定元素（即必有$a\in A$，使得$f(a)=a$）.

3. 给出有理数集合$\mathbf{Q}$的一个良序.

4. 假设S是一个集合.S的一个选择函数是从S的所有非空子集构成的集合到S的一个函数，使得$f(A)\in A$（对于每个$A\neq\varnothing, A\subset S$）.求证选择公理等价于：每个集合$S$均有选择函数.

5. 假设$S=$｛平面上的点$(x,y)\mid y\leqslant 0$｝.定义序为$(x_1,y_1)\leqslant(x_2,y_2)\Longleftrightarrow x_1=x_2$并且$y_1\leqslant y_2$.求证这是$S$的半序，并且$S$有无限多个极大元.

6. 求证：如果集族｛$A_i\mid i\in I\neq\varnothing$｝中每个集合均非空，则每个射影$\pi_{i_1}:\prod_{i\in I}A_i\to A_{i_1}$都是满射.

7. 假设$(A,\leqslant)$是线性序集合.$a\in A$的直接后继（如果存在的话）是集合｛$x\in A\mid a<x$｝中的最小元.求证：如果$\leqslant$是A上的良序，则A中至多有一个元素没有直接后继.给出线性序集合的例子.使它恰好有两个元素没有直接后继.

8. 势

我们今后经常需要势的定义和它的基本性质.但是本节中的其他内容（从定理8.5开始）则只是偶尔用到（定理II.1.2和IV.2.6，引理V.3.5，定理V.3.6和VI.1.9）.因此暂时可以跳过这些内容.

两个集合A和B叫作是等势的，如果存在着一一对应映射A

$\to B$。这时我们记成$A \sim B$。

定理8.1 在全体集合所构成的类$\mathscr{S}$上，等势是一个等价关系。

证明 作为练习。注意$\varnothing \sim \varnothing$，由于$\varnothing \subset \varnothing \times \varnothing$是一个关系，它(无条件地)为一一对应函数[3]。∎

假设$I_0 = \varnothing$，并且对于每个$n \in \boldsymbol{N}^*$，令$I_n = \{1,2,3,\cdots,n\}$。不难证明，I_m和I_n等势$\Longleftrightarrow m = n$(习题1)。我们说一个集合$A$恰好有$n$个元素，这意味着$A$和$I_n$等势。这样的集合(即对某个(唯一的)$n \geqslant 0$，$A \sim I_n$)叫作有限集合，否则便叫作无限集合。于是，对于有限集合A，A的等势等价类给出下面问题的答案：A中包含多少元素？基于这些考虑我们给出

定义8.2 集合A的势是A对于等势关系的等价类，表示成$|A|$。$|A|$称作无限或有限势，视A为无限集合或者有限集合而定。

势也用α,β,γ等小写希腊字母表示。基于上面一段所指出的原因，我们把整数$n \geqslant 0$等同于势$|I_n|$，并且写成$|I_n| = n$，从而有限集合的势恰好是该集合中的元素个数。

通常定义势的方法与我们上面所作的稍有不同。通常的定义可表明势实际上是一个集合（不象定义 8.2 中那样只是一个本性类)。但是我们选择了定义8.2，不但为了节省时间，而且也是因为它更好地反映了“集合中元素个数”这一直观概念。不论我们采用势的哪一个定义，它均具有下列一些性质(在我们这里，前两个性

3. 参见第9页。

质是定理8.1和定义8.2的直接推论)。

(i) 每个集合都有唯一的势;

(ii) 两个集合有同样的势，当且仅当它们是等势的(即:$|A|=|B| \Longleftrightarrow A \sim B$);

(iii) 有限集合的势是该集合中的元素个数。

于是,关于势的命题只不过是关于集合等势性的命题。

例 自然数集合$\boldsymbol{N}$的势习惯上表为 $\aleph_0$(读成"阿列夫零")。势为$\aleph_0$的集合A(即与$\boldsymbol{N}$等势的集合)叫作是可数集合.集合$\boldsymbol{N}^*$，整数集合$\boldsymbol{Z}$和有理数集合$\boldsymbol{Q}$均是可数集合(习题3),但是实数集合$\boldsymbol{R}$不是可数的(习题9)。

定义8.3 假设α和β为势,A和B是非交集合，并且$|A|=\alpha$，$|B|=\beta$。则和$\alpha+\beta$定义为势$|A \cup B|$，而积$\alpha\beta$定义为势$|A \times B|$。

在定义积$\alpha\beta$的时候，实际上不必假定A和B是非交的(习题4)。从势α的定义可知，永远存在集合A，使得$|A|=\alpha$。不难证明，定义$\alpha+\beta$时所需要的非交集合是永远存在的，并且和$\alpha+\beta$从及积$\alpha\beta$均与集合A和B的选取方式无关(习题4)。势的加法和乘法满足结合律和交换律，并且分配律也成立(习题5)。此外，有限势的加法和乘法与它们所等同的非负整数之间的加法和乘法是一致的。这是因为，如果A和B分别有m和n个元素，并且$A \cap B=\phi$，则$A \cup B$有$m+n$个元素，而$A \times B$有mn个元素(更确切内容可见习题6)。

定义8.4 假设α和β为势，A和B为集合，并且$|A|=\alpha,|B|=\beta$。如果A与B的一个子集合等势(即存在一个单射$A \to B$)，我们便称α小于或等于β(表示成$\alpha \leqslant \beta$或者$\beta \geqslant \alpha$)。如果$\alpha \leqslant \beta$并且

$\alpha \neq \beta$，则称α严格小于β（表示成$\alpha < \beta$ 或者$\beta > \alpha$）。

不难验证，$\leqslant$的定义与A和B的选取方式无关（习题7）。在定理8.7中要证明，所有势所构成的类中，$\leqslant$为线性序。对于有限势，$\leqslant$与非负整数的通常序关系是一致的（习题1）。从下面定理立即知道，最大势是不存在的。

定理8.5 如果A是集合而 $P(A)$ 是它的幂集合，则 $|A| < |P(A)|$。

证明概要 $a \longmapsto \{a\}$，$A \to P(A)$ 是一个单射，从而 $|A| \leqslant |P(A)|$。如果存在一一对应f：$A \to P(A)$，那末对于集合$B = \{a \in A \mid a \notin f(a)\} \subset A$，存在着某个 $a_0 \in A$，使得 $f(a_0) = B$。但这就导致矛盾：$a_0 \in B$同时 又$a_0 \notin B$。因此 $|A| \neq |P(A)|$，即 $|A| < |P(A)|$。∎

注：根据定理8.5，$\aleph_0 = |\boldsymbol{N}| < |P(\boldsymbol{N})|$。可以证明$|P(\boldsymbol{N})| = |\boldsymbol{R}|$，其中$\boldsymbol{R}$为实数集合。猜想没有势$\beta$，使得$\aleph_0 < \beta < |P(\boldsymbol{N})| = |\boldsymbol{R}|$，这个猜想叫作连续统假设 已经证明了它与选择公理和集合论其他基本公理是独立的，见P.J.Cohen[59]。

本节其余部分所讲的事实，今后只在少数地方需要（见本节第一段所述）。

定理8.6 (Schroeder-Bernstein) 假设 A和B 是集合。如果$|A| \leqslant |B|$并且$|B| \leqslant |A|$，则$|A| = |B|$。

证明概要 根据假设可知存在单射f：$A \to B$和g：$B \to A$。我们要用f和g构作一个一一对应 h：$A \to B$，由此推出 $A \sim B$，从而 $|A| = |B|$。如果$a \in A$，由于g为单射，从而集合 $g^{-1}(a)$ 或者为空集合（这时我们称a是无前辈的），或者恰由一个元素$b \in B$组成

(这时我们写成$g^{-1}(a)=b$，并且称b为a的前辈)。类似地，对于每个$b\in B$，或者$f^{-1}(b)=\varnothing$ (b是无前辈的)，或者 $f^{-1}(b)=a'\in A$ (a'为b 的前辈)。如果我们继续采用这种方法追寻元素 $a\in A$ 的"家谱"，便会产生三种情况；或者我们寻到A中一个无前辈的元素处而停止 (此元素叫作是$a\in A$的祖宗)，或者我们在B中一个无前辈元素处停止 (它也叫作是a的祖宗)最后，也可能无休止地追寻下去(无限长的家谱！)。现在定义A(和 B)的三个子集合：

$$A_1=\{a\in A\mid a\text{在}A\text{中有祖宗}\}$$

$$A_2=\{a\in A\mid a\text{在}B\text{中有祖宗}\}$$

$$A_3=\{a\in A\mid a\text{有无限长的家谱}\}$$

$$B_1=\{b\in B\mid b\text{在}A\text{中有祖宗}\}$$

$$B_2=\{b\in B\mid b\text{在}B\text{中有祖宗}\}$$

$$B_3=\{b\in B\mid b\text{有无限长的家谱}\}$$

证明诸A_i (或者诸B_i) 是两两非交的，并且它们的并是集合A(或者集合B)。此外，对于$i=1$，3，$f\mid A_i$：$A_i\to B_i$ 是一一对应。而$g\mid B_2$：$B_2\to A_2$是一一对应。因此如果我们定义

$$h:\quad A\to B,\quad h(a)=\begin{cases}f(a), & \text{如果}a\in A_1\cup A_3,\\ g^{-1}(a), & a\in A_2.\end{cases}$$

则h是一一对应。∎

定理8.7 在所有势构成的类中，$\leqslant$为线性序。如果α和β为势，则下面三条恰有一个是正确的：

$$\alpha<\beta;\qquad \alpha=\beta;\qquad \beta<\alpha \qquad\qquad (\text{三分律})$$

证明概要 不难看出$\leqslant$是半序。假设α和β是势，A和B是集合，并且$|A|=\alpha$，$|B|=\beta$。为了证明$\leqslant$是线性序 (即或者 $\alpha\leqslant\beta$ 或者$\beta\leqslant\alpha$)。我们对于集合$\mathscr{F}=\{(f,X)\mid X\subset A,\text{而且}f:X\to B\text{是单}$

射}利用Zorn引理.先证明$\mathscr{F}\neq\varnothing$.然后在$\mathscr{F}$中引进序：$(f_1, X_1)\leqslant(f_2, X_2)\Longleftrightarrow X_1\subset X_2$并且$f_2|X_1=f_1$.这是$\mathscr{F}$的半序.如果$\{(f_i, X_i)|i\in I\}$是$\mathscr{F}$中的一个链，令$X=\bigcup_{i\in I}X_i$，并且定义$f$：$X\to B$为$f(x)=f_i(x)$（对于$x\in X_i$）。证明$f$是可定义的单射，并且$(f, X)$是该链在$\mathscr{F}$中的上界。从而根据Zorn引理，$\mathscr{F}$存在极大元$(g, X)$。我们断言：或者$X=A$，或者$\mathrm{Im}g=B$。因为如果这两条均不成立，我们可以求得$a\in A-X$和$b\in B-\mathrm{Im}g$，并且使映射

$$h:\ X\cup\{a\}\to B,\ h(x)=\begin{cases}g(x), & \text{如果}x\in X\\ b, & x=a\end{cases}$$

是单射。于是$(h, X\cup\{a\}\in\mathscr{F}$，并且$(g, X)<(h, X\cup\{a\})$，这就与$(g, X)$的极大性相矛盾.因此或者$X=A$从而$|A|\leqslant|B|$，或者$\mathrm{Im}g=B$从而$B\xrightarrow{g^{-1}}X\subset A$为单射，即$|B|\leqslant|A|$。利用这些事实，Schroeder-Bernstein定理8.6和定义8.4便可证明三分律.■

注：象定理8.7的证明中那样将函数族赋以半序的方法称作是扩充序。本定理的证明是使用Zorn引理的典型例子。今后作类似推理的时候，我们往往略去细节。

定理8.8 每个无限集合均有可数子集合。特别地，对于每个无限势a，均有$\aleph_0\leqslant a$。

证明概要 如果B是无限集合A的有限子集合，则$A-B$非空。对于A的每个有限子集合B，取一个元素$x_B\in A-B$（选择公理）。以F表示A的全部有限子集合所构成的集合，定义映射

$$f:\ F\to F,\ f(B)=B\cup\{x_B\}.$$

取$a\in A$。由递归定理6.2（对于每个n均取$f_n=f$），可知存在函数φ：$\mathbf{N}\to F$，使得，

$\varphi(0)=\{a\}$ 并且$\varphi(n+1)=f(\varphi(n))=\varphi(n)\cup\{x_{\varphi(n)}\}$

$(n\geqslant 0)$

设函数g：$\boldsymbol{N}\to A$定义为

$$g(0)=a,\ g(1)=x_{\varphi(0)}=x_{\{a\}},\ \cdots,\ g(n+1)=x_{\varphi(n)},\ \cdots$$

利用$\boldsymbol{N}$的序性质及以下诸事实可以证明g为单射

(i) $g(n)\in\varphi(n)$ $(\forall n\geqslant 0)$;

(ii) $g(n)\notin\varphi(n-1)$ $(\forall n\geqslant 1)$;

(iii) $g(n)\notin\varphi(m)$ $(\forall m<n)$。

从而Img 是A的子集合，并且 $|\mathrm{Im}g|=|\boldsymbol{N}|=\aleph_0$。∎

引理8.9 如果 A 是无限集合，F 是有限集合，则 $|A\cup F|=|A|$。特别地，对于每个无限势α和每个自然数（有限势）n，$\alpha+n=\alpha$。

证明概要 必要时用$F-A$代替F,不妨假定$A\cap F=\varnothing$。如果$F=\{b_1,\ b_2,\ \cdots,\ b_n\}$而$D=\{X_i|\ i\in\boldsymbol{N}^*\}$是$A$的一个可数子集(定理8.8)，证明 f：$A\to A\cup F$ 是一一对应，其中f定义为

$$f(x)\begin{cases}b_i, & \text{如果}x=x_i \quad (1\leqslant i\leqslant n);\\ x_{i-n}, & \text{如果}x=x_i \quad (i>n);\\ x, & \text{如果}x\in A-D。\end{cases}$$

∎

定理8.10 如果α和β为势,$\beta\leqslant\alpha$并且α为无限势，则$\alpha+\beta=\alpha$。

证明概要 只需证 $\alpha+\alpha=\alpha$（因为容易验证 $\alpha\leqslant\alpha+\beta\leqslant\alpha+\alpha=\alpha$，然后用 Schroeder-Bernstein 定理即给出结论 $\alpha+\beta=\alpha$)。假设A为集合，$|A|=\alpha$，而$\mathscr{F}$为集合。

$\{(f,X)|\ X\subset A$并且f：$X\times\{0,1\}\to X$是一一对应$\}$。$\mathscr{F}$中赋以扩充序(象定理8.7的证明中所作的那样)，证明它满足Zorn 引理

中的假定条件。唯一困难之处是证明 $\mathscr{F}\neq\varnothing$。为此注意映射。

$$\boldsymbol{N}\times\{0,\ 1\}\longrightarrow\boldsymbol{N},\ (n,\ 0)\longmapsto 2n,\ (n,\ 1)\longmapsto 2n+1$$

是一一对应。由此可构作一一对应 f：$D\times\{0,\ 1\}\to D$，其中 D 是 A 的一个可数子集合（即 $|D|=|\boldsymbol{N}|$，见定理8.8）。因此，由Zorn引理可知存在极大元 $(g,\ C)\in\mathscr{F}$。

显然 $C_0=\{(c,\ 0)\mid c\in C\}$ 和 $C_1=\{(c,\ 1)\mid c\in C\}$ 是非交集合，并且 $|C_0|=|C|=|C_1|$，$C\times\{0,\ 1\}=C_0\times C_1$。映射 g：$C\times\{0,\ 1\}\to C$ 是一一对应。于是由定义8.3便知

$$|C|=|C\times\{0,\ 1\}|=|C_0\cup C_1|=|C_0|+|C_1|=|C|+|C|.$$

为了完成证明，我们只需再证 $|C|=\alpha$ 即可。如果 $A-C$ 是无限集合，根据定理8.8，它包含一个可数子集合 B，并且象上面那样有一一对应 ζ：$B\times\{0,\ 1\}\longrightarrow B$。将 ζ 和 g 组合在一起，我们可以构作一一对应 h：$(C\cup B)\times\{0,\ 1\}\longrightarrow C\cup B$，因此 $(g,\ C)<(h,\ C\cup B)\in\mathscr{F}$，这就与 $(g,\ C)$ 的极大性相矛盾。因此 $A-C$ 是有限集合。由于 A 是无限的，并且 $A=C\cup(A-C)$，从而 C 也是无限的。于是由引理8.9便有 $|C|=|C\cup(A-C)|=|A|=\alpha$。∎

定理8.11 如果 α 和 β 为势，$0\neq\beta\leqslant\alpha$ 并且 α 是无限的，则 $\alpha\beta=\alpha$。特别地，$\alpha\aleph_0=\alpha$。又若 β 是有限的，则 $\aleph_0\beta=\aleph_0$。

证明概要 由于 $\alpha\leqslant\alpha\beta\leqslant\alpha\alpha$，从而（象定理8.10的证明那样）只需证明 $\alpha\alpha=\alpha$。假设 A 是无限集合，$|A|=\alpha$，而令 $\mathscr{F}=\{$一一对应 f：$X\times X\to X$ $|X$ 为 A 的无限子集合$\}$。由于 A 有可数子集合 D（从而 $|D|=|\boldsymbol{N}|=|\boldsymbol{N}^*|$），并且映射 $\boldsymbol{N}^*\times\boldsymbol{N}^*\to\boldsymbol{N}^*$，$(m,\ n)\longmapsto 2^{m-1}(2n-1)$ 是一一对应，可知 $\mathscr{F}\neq\varnothing$。将 $\mathscr{F}$ 赋以扩充序，利用Zorn 引理得到极大元 g：$B\times B\to B$。从 g 的定义可知 $|B\times B|=|B|$。从而为了完成证明，只需证 $|B|=|A|=\alpha$。

假如 $|A-B|>|B|$，由定义8.4给出$A-B$的子集C，使得 $|C|=|B|$。证明 $|C|=|B|=|B\times B|=|B\times C|=|C\times B|=|C\times C|$，并且这些集合是彼此非交的。于是由定义8.3和定理 8.10可知 $|(B\cup C)\times(B\cup C)|=|(B\times B)\cup(B\times C)\cup(C\times B)\cup(C\times C)|=|B\times B|+|B\times C|+|C\times B|+|C\times C|=(|B|+|B|)+(|C|+|C|)=|B|+|C|=|B\cup C|$，从而有一一对应 $(B\cup C)\times(B\cup C)\to(B\cup C)$，这便与$\mathscr{F}$中$g$的极大性相矛盾。因此由定理8.7和8.10可知 $|A-B|\leqslant B$并且 $|B|=|A-B|+|B|=|(A-B)\cup B|=|A|=a$。∎

定理8.12 假设A为集合，并且对于每个整数$n\geqslant 1$，令$A^n=A\times A\times\cdots\times A$（$n$个因子）。

(i) 如果A是有限的，则 $|A^n|=|A|^n$。如果A是无限的，则 $|A^n|=|A|$。

(ii) $\left|\bigcup_{n\in N^*}A^n\right|=\aleph_0|A|$。

证明概要 (i) 如果 $|A|$ 有限，则命题显然。如果 $|A|$ 无限，可以对n归纳证明（对于$n=2$的情形即是定理8.11）。

(ii) 集合$A^n(n\geqslant 1)$是彼此非交的。如果A是无限的，由(i)可知对每个n均有一一对应f_n：$A^n\to A$。映射 $\bigcup_{n\in N^*}A^n\to \boldsymbol{N}^*\times A$，$u(\in A^n)\longmapsto(n,\ f_n(u))$是一一对应。因此 $\left|\bigcup_{n\in N^*}A^n\right|=|\boldsymbol{N}^*\times A|=|\boldsymbol{N}^*||A|=\aleph_0|A|$。如果$A=\varnothing$，则(ii)显然成立。于是下设$A$为有限非空集合。这时每个$A^n$都是非空的，并且不难证明$\aleph_0=|\boldsymbol{N}^*|\leqslant\left|\bigcup_{n\in N^*}A^n\right|$。进而，每个$A^n$均是有限的，从而对每个$n$均有单射$g_n$：$A^n\to\boldsymbol{N}^*$。映射 $\bigcup_{n\in N^*}A^n\to\boldsymbol{N}^*\times\boldsymbol{N}^*$，$u(\in A^n)\longmapsto$

$(n, g_n(u))$是单射，从而由定理 8.11有 $\left|\bigcup_{n\in N^*} A^n\right| \leqslant |\boldsymbol{N}^* \times \boldsymbol{N}^*|$ $= |\boldsymbol{N}^*| = \aleph_0$。于是由Schroeder-Bernstein 定理可知 $\left|\bigcup_{n\in N^*} A^n\right|$ $= \aleph_0$。但是由于A为有限集合，从而 $\aleph_0 = \aleph_0 |A|$ (定理8.11).∎

系8.13 如果A为无限集合而$F(A)$为A的所有有限子集构成的集合，则 $|F(A)| = |A|$。

证明 映射$A \longrightarrow F(A)$，$a \longmapsto \{a\}$ 是单射，所以 $|A| \leqslant |F(A)|$。另一方面，对于A 的每个n元子集合 S，取 $(a_1, \cdots, a_n) \in A^n$，使得$S = \{a_1, \cdots, a_n\}$。这定义出一个单射$F(A) \to \bigcup_{n\in N^*} A^n$，从而由定理8.11和8.12可知 $|F(A)| \leqslant \left|\bigcup_{n\in N^*} A^n\right| = \aleph_0 |A| = |A|$。于是由 Schroeder-Bernstein 定理有 $|A| = |F(A)|$。∎

习　题

1. 假设$I_0 = \varnothing$，并且对于每个$n \in \mathbf{N}^*$ 令$I_n = \{1, 2, 3, \cdots, n\}$。
   (a) I_n与它的任何一个真子集合均不等势（提示：用归纳法）。
   (b) I_m和I_n等势$\Longleftrightarrow m = n$。
   (c) I_m与I_n 的一个子集合等势，但是I_n与I_m的任一子集合均不等势$\Longleftrightarrow m < n$。
2. (a) 每个无限集合均与它的某个真子集合等势。
   (b) 一个集合是有限的充要条件是它与它的每个真子集合均不等势〔见习题 1〕。
3. (a) $\mathbf{Z}$ 是可数集合。
   (b) 有理数集合$\mathbf{Q}$是可数的〔提示：证明$|\mathbf{Z}| \leqslant |\mathbf{Q}| \leqslant |\mathbf{Z}\times\mathbf{Z}| = |\mathbf{Z}|$〕。

4. 如果A，A'，B，B'是集合并且$|A|=|A'|$，$|B|=|B'|$，则$|A\times B|=|A'\times B'|$.此外如果又有 $A\cap B=\varnothing=A'\cap B'$ 则 $|A\cup B|=|A'\cup B'|$.从而可以定义势的加法和乘法.

5. 对于任意势α，β，γ：

(a) $\alpha+\beta=\beta+\alpha$，$\alpha\beta=\beta\alpha$（交换律）

(b) $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$，$(\alpha\beta)\gamma=\alpha(\beta\gamma)$（结合律）

(c) $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$，$(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma$（分配律）

(d) $\alpha+0=\alpha$，$\alpha\mathbf{1}=\alpha$.

(e) 如果$\alpha\neq 0$，则不存在β使$\alpha+\beta=0$.如果$\alpha\neq 1$,则不存在β使$\alpha\beta=1$.因此我们不能定义势的减法和除法.

6. 假设I_n如习题1所示.如果$A\sim I_m$，$B\sim I_n$并且$A\cap B=\varnothing$,则$(A\cup B)\sim I_{m+n}$，$A\times B\sim I_{mn}$.因此，如果将$|A|$和$|B|$分别等同于m和n，则$|A|+|B|=m+n$，$|A|\ |B|=mn$.

7. 如果$A\sim A'$,$B\sim B'$,f：$A\to B$为单射，则存在着单射$A'\to B'$，从而在势集合上可以定义关系$\leqslant$.

8. 可数集合的无限子集合仍是可数集合.

9. 实数集合$\mathbf{R}$是不可数的(即$\aleph_0<|\mathbf{R}|$).〔提示：由习题8可知只需证明开区间（0，1)是不可数的.你可以认为每个实数均可写成无限十进小数.如果（0，1）是可数集合,则存在一一对应f：$\mathbf{N}^*\to(0,1)$.构作在(0，1）中一个无限十进小数（实数）$0.a_1a_2\cdots$，使得a_n不等于$f(n)$的小数点后第n位数字.这个数便不在I_mf中〕.

10. 如果α和β是势，A和B为集合，$|A|=\alpha$，$|B|=\beta$.定义α^β为所有函数$B\to A$所构成的集合的势.

(a) α^β与A和B的选取无关.

(b) $\alpha^{\beta+\gamma}=(\alpha^\beta)(\alpha^\gamma)$ $(\alpha\beta)^\gamma=(\alpha^\gamma)(\beta^\gamma)$，$\alpha^{\beta\gamma}=(\alpha^\beta)^\gamma$.

(c) $\alpha\leqslant\beta\Longrightarrow\alpha^\gamma\leqslant\beta^\gamma$.

(d) 如果α和β有限而γ无限，并且$\alpha>1$，$\beta>1$，则$\alpha^\gamma=\beta^\gamma$.

(e) 对于每个有限势n，$\alpha^n=\alpha\alpha\cdots\alpha$（$n$个因子）.从而若$\alpha$无限,则$\alpha^n=\alpha$.

(f) 如果$P(A)$是集合A的幂集，则 $|P(A)| = 2^{|A|}$。

11. 如果 I 是无限集合，并且对于每个 $i \in I$，A_i均是有限集合，则

$$\left| \bigcup_{i \in I} A_i \right| \leqslant |I| .$$

12. 设 α 是一个固定的势，并且对于每个 $i \in I$，集合A_i均有 $|A_i| = \alpha$，则

$$\left| \bigcup_{i \in I} A_i \right| \leqslant |I| \alpha .$$

第I章　群

群的概念在代数研究中是最基本的。从代数结构观点看来，本质上相同的群称作同构的。在研究群的时候，我们的理想目标是对所有的群作同构分类。这在事实上则意味着寻求两个群同构的充要条件。到目前为止，将任意群加以分类的希望甚小。但是对于加以某些限制的各类群，可以得到完满的结构定理。例如，对循环群（第3节），有限生成Abel 群（第II. 2节），满足链条件的群（第II.3节）和小阶数的有限群，我们都可以这样做。但是即使为了证明这些很有限的结构定理，也需要发展比较一般的群的许多结构性质（第I章第1，2，4，5,8节和第II章第4，5节）。此外，我们还将研究某些种类的群，这些群的结构大部分已经知道，并且它们被有效地应用到其他数学领域中。这些群包括对称群（第6节），自由〔Abel〕群（第9节和第II.1节），幂零群与可解群（第II,7和II,8节）

下面一个基本原则不仅应用于群上，也用到许多其他代数对象（例如环、模、向量空间和域）上：为了有效地研究具有一给定结构的对象，我们必须同时研究保持这一代数结构的函数（这样的函数叫作是同态）。为了提供一种方便的语言和有益的框架，以便考查这些公共的概念，我们在第7节介绍了范畴术语，并且以后则常常使用这种术语。当然，不提到范畴，我们也完全可以

研究群、环等。可是，读者只需花费很小的努力即可理解这些术语，以后能得到很大益处，即对于我们所涉及的各种代数结构，能够更深入地理解它们之间的基本关系。

本章中每一节都依赖它前面的各节，只有第7节例外。

1. 半群，幺半群和群

如果G是一个非空集合，每个函数$G\times G\to G$叫作G上的一个二元运算。对(a, b)在一个二元运算之下的象有许多常用的记号：ab（乘法记号），$a+b$（加法记号），$a\cdot b, a\times b$等等。为方便起见，我们在本章中一般采用乘法记号，并且把ab叫作a和b的积。一个集合上可以有许多个不同的二元运算（例如在$\mathbb{Z}$上由$(a,b)\longmapsto a+b$和$(a, b)\longmapsto ab$分别给出通常的加法和乘法运算）。

定义1.1 一个半群是指一个非空集合G和G上满足

(i) 结合律：$a(bc)=(ab)c$（对所有$a, b, c\in G$）的一个二元运算。如果一个半群G包含有一个

(ii)（双侧）幺元素$e\in G$，使得$ae=ea=a$（对所有$a\in G$），便称G是一个幺半群。如果幺半群G满足：

(iii) 对于每个$a\in G$均存在（双侧）逆元素$a^{-1}\in G$，使得$a^{-1}a=aa^{-1}=e$，

便称G是一个群。半群G的二元运算如果满足

(iv) 交换律：$ab=ba$（对所有$a, b\in G$），

便称G为交换半群或者 Abel 半群。

我们的主要兴趣是群。但是有时为了尽可能一般地叙述某些定理，采用半群和幺半群是方便的，见下面所给的一些例子。势 $|G|$ 叫作群G的阶。如果 $|G|$ 是有限的或者是无限的，则群G也分别叫做有限的或者无限的。

定理1.2 如果 G 是幺半群，则幺元素e是唯一的。如果G是群，则

(i) $c\in G$并且$cc=c\Rightarrow c=e$;

(ii) 对于所有的a, b, $c\in G$, $ab=ac\Rightarrow b=c$，同样地$ba=ca\Rightarrow b=c$（左消去律和右消去律）;

(iii) 对于每个$a\in G$, 逆元素a^{-1}是唯一的;

(iv) 对于每个$a\in G$, $(a^{-1})^{-1}=a$;

(v) 对于a, $b\in G$, $(ab)^{-1}=b^{-1}a^{-1}$;

(vi) 对于a, $b\in G$, 方程$ax=b$和$ya=b$均在G中有唯一解：$x=a^{-1}b$, $y=ba^{-1}$。

证明概要 如果e'也是双侧幺元素，则$e=ee'=e'$。

(i)$cc=c\Rightarrow c^{-1}(cc)=c^{-1}c\Rightarrow(c^{-1}c)c=c^{-1}c\Rightarrow ec=e\Rightarrow c=e$。

类似地证明(ii)、(iii)和(Vi)。

(v) $(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=(ae)a^{-1}=aa^{-1}=e\Rightarrow$ $(ab)^{-1}=b^{-1}a^{-1}$(根据(iii))。

类似地证明(iv)。∎

如果G是幺半群而其上的二元运算写成乘法，则 G 的幺元素永远写成e。如果二元运算写成加法，则$a+b(a,b\in G)$叫做a 与b的和，并且幺元素写成0。这时又如果 G 是群，则$a\in G$的逆元素表示成$-a$。我们以$a-b$表示$a+(-b)$。Abel 群常常写成加法形式。

定义1.1中用来定义群的那些公理事实上可以大大地减弱：

命题1.3 假设G是半群，则G是群的充要条件是下面两条件成立：

(i) 存在一个元素$e\in G$,使得对所有$a\in G$均有$ea=a$(左幺元素)；

(ii) 对于每个$a\in G$，均存在一个元素$a^{-1}\in G$，使得$a^{-1}a=e$(左逆)。

注：如果改成“右幺元素”和“右逆”,则类似的结果也成立。

证明概要 ($\Rightarrow$)显然。

($\Leftarrow$)：注意在这些假定之下，定理1.2(i)是对的。由于$e\in G$,从而$G\neq\varnothing$。如果$a\in G$，由(ii)可知$(aa^{-1})(aa^{-1})=a(a^{-1}a)a^{-1}=a(ea^{-1})=aa^{-1}$，从而由定理1.2(i)可知$aa^{-1}=e$。因此$a^{-1}$是$a$的双侧逆。由于对每个$a\in G$均有$ae=(aa^{-1}a)=(aa^{-1})a=ea=a$，从而$e$为双侧幺元素。因此由定义1.1可知$G$是群。∎

命题1.4 假设G是半群。则G是群的充要条件是对于所有a，$b\in G$，方程$ax=b$和$ya=b$在G中均可解。

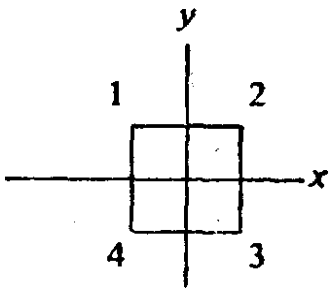
证明作为练习。利用命题1.3。∎

例 整数集合$\boldsymbol{Z}$，有理数集合$\boldsymbol{Q}$和实数集合$\boldsymbol{R}$对于通常加法都是无限Abel 群。对于通常的乘法都是幺半群但不是群（0没有逆)。但是$\boldsymbol{Q}$和$\boldsymbol{R}$的非零元素集合对于乘法分别形成无限 Abel群。偶整数集合对于乘法形成半群但不是幺半群。

例 考虑中心在x-y平面的原点而边平行于坐标轴的正方形，其顶点依次标记为1,2,3,4。

以D_4^*表示正方形如下的“变换”集合：$D_4^*=\{R,R^2,R^3,I,$

T_x, T_y, $T_{1,3}$, $T_{2,4}$}，其中R是绕中心反时针旋转 90°，R^2是反时针旋转 180°，R^3是反时针旋转270°，而I是旋转 360°（=0°）；T_x是对x轴的反射，$T_{1,3}$是对通过顶点1和3的对角线的反射。T_y和$T_{2,4}$有类似的意义。注意每个$U\in D_4^*$均是此正方形到自身上的一一对应。在D_4^*中定义二元运算为函数的合成：对于U，$V\in D_4^*$，$U\circ V$是变换V再接着作变换U。D_4^*是一个8阶的非Abel群，称作此正方形的对称群。注意每个对称（即D_4^*中的元素）由它在四个顶点上的作用所完全决定。



例 设S是非空集合而$A(S)$是全部一一对应$S\to S$所构成的集合。在函数合成运算$f\circ g$之下，$A(S)$是群，因为合成满足结合律，而一一对应的合成仍旧是一一对应，1_s是一一对应，并且每个一一对应都有逆（见引论第3节的(13)）。$A(S)$中的元素叫作置换，而$A(S)$叫作集合S上的置换群。如果$S=\{1,2,\cdots,n\}$，则$A(S)$叫作n个字母的对称群，表示成S_n。验证$|S_n|=n!$（习题5）。群S_n在有限群理论中起着重要作用。

由于S_n中的元素σ是有限集合$S=\{1,2,\cdots,n\}$上的函数，它可以写成：将S中的元素排成一条线，然后将每个元素在σ之下的象写在该元素的下方：$\begin{pmatrix}1&2&3&\cdots&n\\ i_1&i_2&i_3&\cdots&i_n\end{pmatrix}$。$S_n$中两个元素的乘积$\sigma\tau$是函数$\tau$之后再作用函数$\sigma$，即$S$上的合成函数 $k\longmapsto\sigma(\tau(k))$[1]。例如令$\sigma=\begin{pmatrix}1&2&3&4\\ 3&1&2&4\end{pmatrix}$ 和$\tau=\begin{pmatrix}1&2&3&4\\ 4&1&2&3\end{pmatrix}$ 是S_4中的元素。则在$\sigma\tau$的作用下，$1\longmapsto\sigma(\tau(1))=\sigma(4)=4$，如此等等，从而$\sigma\tau=\begin{pmatrix}1&2&3&4\\ 3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\ 4&1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\ 4&3&1&2\end{pmatrix}$。类似地，$\tau\sigma=\begin{pmatrix}1&2&3&4\\ 4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\ 3&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\ 2&4&1&3\end{pmatrix}$。这个例子也表明$S_n$未必是

1．但是在许多书中，乘积$\sigma\tau$定义为“先σ后τ”。

Abel群.

利用下面一个从已知群构造新群的方法，可以得到另外一些例子. 假设G和H是群，其单位元素分别为e_G和e_H. 定义G和H的直积是如下的群：它的凭借(underlying)集合为$G\times H$，而二元运算为

$(a, b)(a', b')=(aa', bb')$，其中$a, a'\in G$；$b, b'\in H$. 注意在上面式子中，包含了G，$H$和$G\times H$中三种不同的运算. 容易验证，$G\times H$事实上是群. 如果G和$H$均是Abel群，则$G\times H$也是Abel群. (e_G, e_H)是它的幺元素，(a,b)的逆元素为(a^{-1}, b^{-1}). 显然$|G\times H|=|G||H|$ (引论，定义8.3). 如果G和H中运算均写成加法，则我们用$G\oplus H$代替$G\times H$.

定理1.5 假设$R(\sim)$是幺半群G上的一个等价关系，并且对所有$a_i, b_i\in G$，由$a_1\sim a_2$，$b_1\sim b_2$可以导出$a_1b_1\sim a_2b_2$. 则G的所有R等价类组成的集合G/R对于二元运算$(\bar{a})(\bar{b})=\overline{ab}$是幺半群. 其中$\bar{x}$表示$x\in G$的等价类. 如果$G$为〔Abel〕群，则$G/R$亦然.

幺半群G上满足此定理中条件的等价关系称作G上的一个同余关系.

证明 如果$\bar{a}_1=\bar{a}_2$并且$\bar{b}_1=\bar{b}_2(a_i, b_i\in G)$，由引论中第4节的(20)式有$a_1\sim a_2$和$b_1\sim b_2$. 由假设有$a_1b_1\sim a_2b_2$，从而再由(20)式$\overline{a_1b_1}=\overline{a_2b_2}$. 因此可以定义$G/R$中的二元运算（即与等价类代表元的选取无关). 这个二元运算是满足结合律的，因为$\bar{a}(\bar{b}\bar{c})=\bar{a}(\overline{bc})=\overline{a(bc)}=\overline{(ab)c}=\overline{(ab)}\bar{c}=(\bar{a}\bar{b})\bar{c}$. 又由于$(\bar{a})(\bar{e})=\overline{ae}=\bar{a}=\overline{ea}=(\bar{e})(\bar{a})$，从而$\bar{e}$是幺元素，于是$G/R$为幺半群. 如果$G$为群，则$\bar{a}\in G/R$显然有逆元素$\overline{a^{-1}}$，因此$G/R$也是

群。类似地，G的交换性导致G/R的交换性。∎

例 假设m是固定的整数。根据引论的定理6.8可知模m同余是加法群$\boldsymbol{Z}$上的同余关系。以Z_m表示$\boldsymbol{Z}$在模 m 同余之下的等价类集合。由定理1.5（采用加法记号）知 Z_m 是 Abel 群，其加法由$\bar{a}+\bar{b}=\overline{a+b}$给出 $(a, b\in\boldsymbol{Z})$。引论中定理6.8的证明表明 $Z_m=\{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$，从而$Z_m$对于加法是$m$ 阶有限群，叫作是模m整数(加法)群。类似地，由于$\boldsymbol{Z}$ 对于乘法是交换幺半群，而模m同余对于乘法也是同余关系（引论的定理6.8），从而 Z_m对于由$(\bar{a})(\bar{b})=\overline{ab}(a, b\in\boldsymbol{Z})$给出的乘法是交换幺半群。验证对于所有$\bar{a}$，$\bar{b}$，$\bar{c}\in Z_m$：

$\bar{a}(\bar{b}+\bar{c})=\bar{a}\bar{b}+\bar{a}\bar{c}$，$(\bar{a}+\bar{b})\bar{c}=\bar{a}\bar{c}+\bar{b}\bar{c}$（分配律）。

进而，如果p为素数，则 $\boldsymbol{Z}_p$ 的非零元素形成 $p-1$ 阶乘法群（习题7）。习惯上我们仍把$\boldsymbol{Z}_m$中元素表示成0，1，$\cdots$，$m-1$，而不写成 $\bar{0}$，$\bar{1}$，$\cdots$，$\overline{m-1}$。这种有些混淆的记号在课文中不会引起困难，所以在方便的时候我们就使用它。

例 有理数加法群$\boldsymbol{Q}$上的下列关系是同余关系（习题8）：

$$a\sim b\Longleftrightarrow a-b\in\boldsymbol{Z}.$$

由定理1.5，等价类集合（表示成$\boldsymbol{Q}/\boldsymbol{Z}$）对于由$\bar{a}+\bar{b}=\overline{a+b}$给出的加法是(无限)Abel群。$\boldsymbol{Q}/\boldsymbol{Z}$叫作模 1 有理数群。

给了$a_1, \cdots, a_n\in G(n\geqslant 3)$，直观上，在表达式$a_1a_2\cdots a_n$中有许多方法插入括号，从而得到G 中这$n$个元素以这种排列次序的许多“有意义的”乘积。进而，重复使用结合律，可以证明任意两个这样的乘积都是相等的，这些事实似乎是不言而喻的。但是在对群和环作进一步的研究之前，我们需要确切地叙述和证明这些猜想和其他有关事实。

给了半群G的任意一个元素序列$\{a_1, a_2, \cdots\}$ 我们如下归纳

地定义$a_1,\cdots,a_n$（以这种排列次序）的一个有意义乘积：如果$n=1$，则唯一的有意义乘积为a_1。如果$n>1$，则有意义乘积定义为形如$(a_1\cdots a_m)(a_{m+1}\cdots a_n)$的任何一个乘积，其中$m<n$，并且$(a_1\cdots a_m)$和$(a_{m+1}\cdots a_n)$分别是$m$元和$n-m$元的有意义乘积[2]。注意当$n\geqslant 3$时，可能存在$a_1,\cdots,a_n$的许多个有意义乘积。对于每个$n\in \boldsymbol{N}^*$，我们挑选出一个特别的有意义乘积，办法是如下归纳定义$a_1,\cdots,a_n$的标准n元乘积$\prod_{i=1}^{n}a_i$：

$$\prod_{i=1}^{1}a_i=a_1,\ \text{而当}n>1\text{时},\ \prod_{i=1}^{n}a_i=\left(\prod_{i=1}^{n-1}a_i\right)a_n.$$

由引论中的归纳定理6.2可以推出（习题16）对每个$n\in \boldsymbol{N}^*$，这个定义给出G中的唯一元素（它显然是一个有意义乘积）。

定理1.6（广义结合律） 如果G是半群而$a_1,\cdots,a_n\in G$，则$a_1,\cdots,a_n$以此排列次序的任意两个有意义乘积均彼此相等。

证明 我们归纳证明：对于每个n，任意一个有意义乘积$a_1\cdots a_n$均等于标准n元乘积$\prod_{i=1}^{n}a_i$。对于$n=1,2$这显然是对的。如果$n>2$，由定义$(a_1\cdots a_n)=(a_1\cdots a_m)(a_{m+1}\cdots a_n)$，其中$m<n$。从而根据归纳假设和结合性便有：

$$\begin{aligned}(a_1\cdots a_n)&=(a_1\cdots a_m)(a_{m+1}\cdots a_n)\\&=\left(\prod_{i=1}^{m}a_i\right)\left(\prod_{i=1}^{n-m}a_{m+i}\right)\\&=\left(\prod_{i=1}^{m}a_i\right)\left(\left(\prod_{i=1}^{n-m-1}a_{m+i}\right)a_n\right)\end{aligned}$$

---

2. 为了证明这个定义的可定义性，我们需要引论中归纳定理6.2的更强的形式，见C.W.Burrill[56，第57页]。

$$=\left(\left(\prod_{i=1}^{m}a_i\right)\left(\prod_{i=1}^{n-m-1}a_{m+i}\right)\right)a_n$$

$$=\left(\prod_{i=1}^{n-1}a_i\right)a_n=\prod_{i=1}^{n}a_i \quad \blacksquare$$

根据定理1.6，我们可以将$a_1,\cdots,a_n\in G$(G为半群) 的任何有意义乘积写成 $a_1a_2\cdots a_n$，即不加任何括号也不会有任何混淆。

系1.7 （广义交换律） 如果G为交换半群而$a_1,\cdots,a_n\in G$，则对于$1,2,\cdots,n$的任意一个置换$i_1,\cdots i_n$，均有

$$a_1a_2\cdots a_n=a_{i_1}a_{i_2}\cdots a_{i_n}$$

证明作为练习。 ■

定义1.8 假设G为半群，$a\in G$，$n\in \boldsymbol{N}^*$。元素$a^n\in G$定义为标准 n 元乘积$\prod_{i=1}^{n}a_i$，其中$a_i=a(1\leqslant i\leqslant n)$。如果 G是幺半群，则a^0定义为幺元素e。如果G是群，则对于每个$n\in \boldsymbol{N}^*$，a^{-n} 定义为$(a^{-1})^n\in G$。

定理1.6前面的注记和练习16表明方幂的可定义性。根据定义，$a^1=a$，$a^2=aa$，$a^3=(aa)a=aaa,\cdots,a^n=a^{n-1}a=aa\cdots a$（$n$个因子)。注意当$m\neq n$时可能会有$a^m=a^n$(例如在$\boldsymbol{C}$中，$-1=i^2=i^6$)。

加法记号 如果G中的二元运算写成加法，我们便用na 代替a^n。因此$0a=0$，$1a=a$，$na=(n-1)a+a$，如此等等。

定理1.9 如果 G是群〔半群，幺半群〕，而 $a\in G$，则对所有$m,n\in \boldsymbol{Z}$〔$\boldsymbol{N}^*$，$\boldsymbol{N}$〕，均有

(i) $a^m a^n = a^{m+n}$(加法记号：$ma + na = (m+n)a$)；

(ii) $(a^m)^n = a^{mn}$ (加法记号：$n(ma) = nma$)。

证明概要 证明对每个$n \in \mathbf{N}$均有$(a^n)^{-1} = (a^{-1})^n$，并且对每个$n \in \mathbf{Z}$均有$a^{-n} = (a^{-1})^n$。

(i) 对于$m > 0$和$n > 0$ 是对的，因为标准n元乘积和标准m元乘积相乘是一个有意义乘积，根据定理1.6它等于标准 $(m+n)$元乘积。将a，m，n改为a^{-1}，$-m$，$-n$ 并且利用上述推理就可得到$m < 0$和$n < 0$的情形。情形$m = 0$或者$n = 0$是平凡的。而情形$m \geqslant 0$，$n < 0$和$m < 0$，$n \geqslant 0$可以分别对m和n作归纳法。

(ii) 对于$m = 0$是显然的。当$m > 0$，$n \in \mathbf{Z}$时，可以对m归纳证得。然后用此结果证明$m < 0$和$n \in \mathbf{Z}$的情形。∎

习　题

1. 给出课文以外的例子，以表明半群和幺半群可以不是群。
2. 假设G是群（记成加法），S为非空集合，而$M(S, G)$是所有函数$f: S \to G$所成的集合。在$M(S, G)$中如下定义加法：$(f+g): S \to G$定义为$S \mapsto f(s) + g(s) \in G$。证明$M(S, G)$是群。如果$G$是Abel群，求证$M(S, G)$也是Abel群。
3. 具有左幺元素并且每个元素都有右逆（见命题1.3）的半群是否一定是群？
4. 写出群D_4^*的乘法表。
5. 证明n个字母的对称群S_n的阶是$n!$。
6. 写出$\mathbf{Z}_2 \oplus \mathbf{Z}_2$的加法表。$\mathbf{Z}_2 \oplus \mathbf{Z}_2$叫作Klein 四元群。
7. 如果p为素数，则$\mathbf{Z}_p$的非零元素对于乘法形成$p-1$阶群。〔提示：$\overline{a} \neq \overline{0} \Rightarrow (a, p) = 1$，利用引论中的定理6.5〕证明当$p$不为素数时这个命题不再成立。

8. (a) 由$a\sim b\Longleftrightarrow a-b\in\mathbf{Z}$给出的关系是加法群$\mathbf{Q}$上的同余关系〔见定理1.5〕.

(b) 等价类集合$\mathbf{Q}/\mathbf{Z}$是无限Abel群.

9. 假设p是固定的素数.R_p为分母与p互素的全部有理数所构成的集合.R_i为分母是p的方幂($p^i, i\geqslant 0$)的全部有理数所构成的集合.求证R_p和R^p对于通常的有理数加法均是Abel群.

10. 假设p为素数，$Z(p^\infty)$是群$\mathbf{Q}/\mathbf{Z}$(见第41页)的如下子集合：

$$\mathbf{Z}(p^\infty)=\{\overline{a/b}\in\mathbf{Q}/\mathbf{Z}\mid a,b\in\mathbf{Z}\text{并且}b=p^i,\ i\geqslant 0\}\ .$$

证明$\mathbf{Z}(p^\infty)$对于$\mathbf{Q}/\mathbf{Z}$的加法运算是无限群.

11. 关于群G的下列一些条件是彼此等价的：

(i) G为Abel群；

(ii) 对于所有$a,b\in G,(ab)^2=a^2b^2$；

(iii) 对于所有$a,b\in G,(ab)^{-1}=a^{-1}b^{-1}$；

(iv) 对于所有$n\in\mathbf{Z}$和$a,b\in G,(ab)^n=a^nb^n$；

(v) 对于三个相邻整数n和所有$a,b\in G$，$(ab)^n=a^nb^n$.

求证：如果“三”个相邻整数改成“两”个，则由(v)不能推出(i).

12. 如果G为群，$a,b\in G$，并且对于某个$r\in\mathbf{N}$，使得$bab^{-1}=a^r$，则对于每个$j\in\mathbf{N}$，$b^jab^{-j}=a^{r^j}$.

13. 如果对于群G的所有元素$a,a^2=e$，则G是Abel群.

14. 如果G是偶阶有限群，则G含有元素$a\neq e$，使得$a^2=e$.

15. 设G为非空有限集合，其上有一个满足结合律的二元运算，并且对所有$a,b,c\in G$，$ab=ac\Rightarrow b=c$以及$ba=ca\Rightarrow b=c$.则G是群.求证如果G是无限的，则这个结论可能不对.

16. 假设a_1，a_2，…是半群G中的元素序列.则存在唯一的函数ψ：$\mathbf{N}^*\to G$，使得$\psi(1)=a_1$，$\psi(2)=a_1a_2$，$\psi(3)=(a_1a_2)a_3$并且对于$n\geqslant 1,\psi(n+1)=(\psi(n))a_{n+1}$.注意$\psi(n)$恰好是标准$n$元乘积$\prod_{i=1}^{n}a_i$.〔提示：利用引论中的递归定理6.2,其中取$a=a_1,S=G$，并且$f_n$：$G\to G$是由$x\longmapsto xa_{n+2}$

给出的函数．由此产生出一个函数φ：$N\to G$．令$\psi=\varphi\theta$，其中θ：$N^*\to N$由$k\longmapsto k-1$给出．〕

2．同态和子群

在研究某一类代数对象的时候，最本质的事情是使给定的代数结构保持不变的那些函数。

定义2.1 假设G和H是半群。函数f：$G\to H$叫作同态，是指对于所有的$a,b\in G$，

$$f(ab)=f(a)f(b)。$$

假如f作为集合的映射是单射，称f为单同态，如果f是满射，f叫作满同态。如果f是一一对应，f便叫作同构。在后一种情形下，我们称G和H是同构的（写成$G\cong H$）。同态f：$G\to G$叫作G的自同态，而同构f：$G\to G$叫作G的自同构。

如果$f:G\to H$和$g:H\to K$均是半群的同态，不难看出，gf：$G\to K$也是同态。同样地，单同态的合成是单同态，而对于满同态、同构和自同构则有类似的论断。如果G和H是群，它们的幺元素分别为e_G和e_H，而f：$G\to H$是一个同态，则$f(e_G)=e_H$。但是这对于幺半群是不正确的（习题1）。此外，对于所有$a\in G$，$f(a^{-1})=f(a)^{-1}$（习题1）。

例 映射f：$\boldsymbol{Z}\to Z_m$，$x\longmapsto\bar{x}$（即每个整数均映成它在Z_m中的等价类）是加法群的满同态，f叫作Z到Z_m上的正则满同态，类似地，映射g：$\boldsymbol{Q}\to\boldsymbol{Q}/\boldsymbol{Z}$，$r\longmapsto\bar{r}$也是加法群的满同态。

例 如果A是Abel群，则映射$a\longmapsto a^{-1}$是A的自同构，而映

射$a\longmapsto a^2$是A的自同态。

例 设$1<m$，$k\in\mathbb{N}^*$。则映射g：$Z_m\to Z_{mk}$，$\bar{x}\longmapsto\overline{kx}$是单同态。

例 给了群G和H，存在着如下四个同态：$G\underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}}G\times H\underset{\pi_2}{\overset{\iota_2}{\rightleftarrows}}H$，其中$\iota_1(g)=(g,e)$，$\iota_2(h)=(e,h)$，$\pi_1(g,h)=g$，$\pi_2(g,h)=h$。并且$\iota_i$是单同态而$\pi_j$是满同态$(i,j=1,2)$。

定义2.2 假设$f:G\to H$是群同态。集合$\{a\in G\mid f(a)=e\in H\}$叫作$f$的核（表示成Kerf）。如果$A$是$G$的子集合，则$f(A)=\{b\in H\mid b=f(a)$，对某个$a\in A\}$叫作$A$的象。而$f(G)$叫作$f$的象，表示成Im$f$。如果$B$是$H$的子集合，$f^{-1}(B)=\{a\in G\mid f(a)\in B\}$是$B$的原象。

定理2.3 设f：$G\to H$是群同态。则

(i) f为单同态$\Longleftrightarrow$ker$f=\{e\}$；

(ii) f为同构$\Longleftrightarrow$存在同态f^{-1}：$H\to G$，使得$ff^{-1}=1_H$，并且$f^{-1}f=1_G$。

证明 (i) 如果f是单同态并且$a\in$Ker$f$，则$f(a)=e_H=f(e)$，从而$a=e$，即Ker$f=\{e\}$，如果Ker$f=\{e\}$，并且$f(a)=f(b)$，则$e_H=f(a)f(b)^{-1}=f(a)f(b^{-1})=f(ab^{-1})$，从而$ab^{-1}\in$Ker$f$。因此$ab^{-1}=e$(即$a=b$)，所以$f$为单同态。

(iii) 如果f为同构，由引论第3节中的(13)式可知存在着集合的映射f^{-1}：$H\to G$，使得$f^{-1}f=1_G$并且$ff^{-1}=1_H$。易知f^{-1}是同态。反命题则是引论第3节中的(13)式以及定义2.1的直接推论。∎

假设G是半群而H是G的非空子集合。如果对于每个$a, b\in H$均有$ab\in H$，我们称H对G中的乘积运算是封闭的。这相当于说，G上的二元运算限制在H上，为H的二元运算。

定义2.4 假设G是群，H是它的非空子集合并且对于G中的乘积运算是封闭的。如果H本身对于G中这个乘积运算是群，则称H为G的子群，并且表示成$H<G$。

群G自身与仅由幺元素组成的平凡子群(e)是G的子群的两个例子。子群H如果满足$H\neq G, H\neq(e)$，便叫作G的一个真子群。

例 某个固定整数n的所有倍数所构成的集合是$\mathbb{Z}$的子群，它同构于$\mathbb{Z}$(习题7)。

例 在$\{1, 2, \cdots, n\}$的置换群S_n中，所有保持n不变的全体置换所构成的集合形成一个子群并且同构于S_{n-1}(习题8)。

例 在$Z_6=\{0,1,2,3,4,5\}$中，$\{0,3\}$和$\{0, 2, 4\}$对于加法均是子群。如果p是素数，则$(Z_p, +)$没有真子群。

例 如果$f: G\to H$是群同态，则$\mathrm{Ker}f$是G的子群。如果A是G的子群，则$f(A)$是H的子群。特别地，$\mathrm{Im}f$是H的子群。如果B是H的子群，则$f^{-1}(B)$是G的子群(习题9)。

例 如果G是群，则G的全体自同构所构成的集合$\mathrm{Aut}G$是群，其二元运算取为函数的合成(习题15)。

由定理1.2可知，任何子群H的幺元素必为G的幺元素，而$a\in H$的逆元素即是a在G中的逆元素a^{-1}。

定理2.5 假设H是群G的非空子集，则H是G的子群$\Longleftrightarrow$对所有$a, b\in H$，$ab^{-1}\in H$。

证明 ($\Leftarrow$)：由于存在元素$a\in H$，从而$e=aa^{-1}\in H$。因此

对于任何$b\in H$，$b^{-1}=eb^{-1}\in H$。如果a，$b\in H$，则$b^{-1}\in H$，因此$ab=a(b^{-1})^{-1}\in H$。由于G是群，从而H中的乘积运算是满足结合律的，因此H是(子)群。(⇒)显然是对的。∎

系2.6 如果G是群而$\{H_i|i\in I\}$是非空的子群族，则$\bigcap_{i\in I}H_i$是G的子群。

证明作为练习。∎

定义2.7 假设G是群而X是G的子集合。令$\{H_i|i\in I\}$是G中包含X的全体子群所构成的子群族。我们将$\bigcap_{i\in I}H_i$叫作由集合X生成的G的子群，表示成$\langle X\rangle$。

X中的元素叫作子群$\langle X\rangle$的生成元，$\langle X\rangle$也可以由别的子集合生成（即可能有$\langle X\rangle=\langle Y\rangle$但是$X\neq Y$）。如果$X=\{a_1,\cdots,a_n\}$，我们也把$\langle X\rangle$记成$\langle a_1,\cdots,a_n\rangle$。如果$G=\langle a_1,\cdots,a_n\rangle(a_i\in G)$，称$G$为有限生成的。如果$a\in G$，则子群$\langle a\rangle$叫作由$a$生成的循环（子）群。

定理2.8 如果G是群而X为G的非空子集，则由X生成的子群$\langle X\rangle$即是全体有限乘积$a_1^{n_1}a_2^{n_2}\cdots a_l^{n_l}(a_i\in X,\ n_i\in\mathbb{Z})$所构成的集合。特别对于每个$a\in G$，$\langle a\rangle=\{a^n|n\in\mathbb{Z}\}$。

证明概要 证明由全体这样的乘积所构成的集合H是G的包含X的子群。并且每个包含X的子群必也包含H。因此$H<\langle X\rangle<H$。∎

例 加法群$\mathbb{Z}$是由1生成的无限循环群，因为根据定义1.8（采用加法记号），对于所有$m\in\mathbb{Z}$，$m1=m$。在$\mathbb{Z}$中，生成元素的

不同“幂次”（这里用加法记号则是不同个数的1之和）是两两相异的。对于别的群当然不必如此。在任意群 G 中，平凡子群 $\langle e\rangle$ 总是循环群。$\mathbf{C}$ 中的乘法子群 $\langle i\rangle$ 是4阶循环群。对于每个m，加法群 Z_m 是以 $1\in Z_m$ 为生成元的 m阶循环群。在第3节中我们将证明，每个循环群均同构于$\mathbf{Z}$或者某个Z_m。还见习题12。

如果$\{H_i\mid i\in I\}$ 是群G的子群族，$\bigcup_{i\in I}H_i$一般不是G的子群。由集合$\bigcup_{i\in I}H_i$生成的子群$\langle\bigcup_{i\in I}H_i\rangle$叫作由诸群 $\{H_i\mid i\in I\}$ 所生成的子群。如果H和K是子群，则由H和K生成的子群 $\langle H\cup K\rangle$ 叫作H和K的并，表示成$H\vee K$(加法记号则为$H+K$)。

习　题

1. 如果f：$G\to H$是群同态，则$f(e_G)=e_H$，并且对于所有 $a\in G$，$f(a^{-1})=f(a)^{-1}$。以例子表明，如果G和H是幺半群但不是群，则 $f(e_G)=e_H$ 可能不成立。
2. 群G是Abel群$\Longleftrightarrow$映射$G\to G$，$x\longmapsto x^{-1}$是自同构。
3. 假设Q_8是由复矩阵 $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$和 $B=\begin{pmatrix}0&i\\i&0\end{pmatrix}$（其中 $i^2=-1$）生成的群（对于通常的矩阵乘法），求证 Q_8 是8阶非 Abel 群。它称作四元数群。〔提示：注意$BA=A^3B$，从而Q_8中每个元素均可写成形式 A^iB^j。又有 $A^4=B^4=I$，　其中 $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ 是Q_8的幺元素。〕
4. 假设H是由$C=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$和 $D=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 生成的实矩阵群（对于矩阵乘法）。求证H是8阶非A bel 群，它不同构于习题3中的四元数群，但是同构于群D_4*。
5. 假设S是群G的非空子集合，在G上定义关系：$a\sim b\longleftrightarrow ab^{-1}\in S$。求证$\sim$是等价关系的充要条件是$S$为$G$的子群。
6. 某群G的一个非空有限子集合是子群的充要条件是该子集合对于G中的

乘积运算是封闭的。

7. 如果n是一固定整数，则 $\{kn \mid k \in \mathbf{Z}\} \subset \mathbf{Z}$是$\mathbf{Z}$的加法子群，并且它同构于$\mathbf{Z}$。

8. 集合 $\{\sigma \in S_n \mid \sigma(n) = n\}$ 是S_n的子群，并且它同构于S_{n-1}。

9. 假设$f: G \to H$是群同态，A是G的子群，B是H的子群。

   (a) $\ker f$和$f^{-1}(B)$均是G的子群。

   (b) $f(A)$是H的子群。

10. 列出$\mathbf{Z}_2 \oplus \mathbf{Z}_2$的全部子群。$\mathbf{Z}_2 \oplus \mathbf{Z}_2$是否同构于$\mathbf{Z}_4$？

11. 如果G是群，则$C = \{a \in G \mid ax = xa$对所有$x \in G\}$是$G$的Abel子群。$C$叫作$G$的中心。

12. 群D_4*不是循环群，但是它可以由两个元素生成。S_n也可由两个元素生成（证明并不容易）。加法群$\mathbf{Z} \oplus \mathbf{Z}$最少应由几个元素生成？

13. 如果$G = \langle a \rangle$是循环群而H是任意一个群，则每个同态$f: G \to H$均可由元素$f(a) \in H$所完全决定。

14. 下面一些循环子群是彼此同构的：C中的乘法群$\langle i \rangle$；加法群$\mathbf{Z}_4$，和S_4中的子群$\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle$。

15. 假设G是群而Aut G是G的全体自同构所构成的集合。

   (a) Aut$G$以函数合成为二元运算，则形成群。〔提示：$I_G \in \mathrm{Aut}\,G$是幺元素；根据定理2.3可知逆元素的存在性。〕

   (b) $\mathrm{Aut}\mathbf{Z} \cong \mathbf{Z}_2$，$\mathrm{Aut}\mathbf{Z}_6 \cong \mathbf{Z}_2$，$\mathrm{Aut}\mathbf{Z}_8 \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$，$\mathrm{Aut}\mathbf{Z}_p \cong \mathbf{Z}_{p-1}$（$p$为素数）。

   (c) 对于任意$n \in \mathbf{N}^*$，什么是Aut$\mathbf{Z}_n$？

16. 对于每个素数p，$\mathbf{Q}/\mathbf{Z}$的加法子群$\mathbf{Z}(p^\infty)$是由集合$\{\overline{1/p^n} \mid n \in \mathbf{N}^*\}$ 生成的。

17. 假设G是Abel群，而H、K是G的子群，求证并$H \vee K$等于集合$\{ab \mid a \in H, b \in K\}$。将此结果推广到$G$的任意有限多个子群上。

18. (a) 假设G为群而$\{H_i \mid i \in I\}$是它的子群族。叙述并证明一个条件，使得由它可推出$\bigcup_{i \in I} H_i$是子群，即$\bigcup_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i \right\rangle$。

(*b*) 给出群G和子群族$\{H_i|i\in I\}$的例子，使得$\bigcup_{i\in I}H_i\neq\left\langle\bigcup_{i\in I}H_i\right\rangle$.

19. (*a*) 群G的全部子群所构成的集合，赋以集合论的包含序（这是半序）则形成完备格（引论中的习题7.1和7.2），其中 $\{H_i|i\in I\}$ 的下端是$\bigcap_{i\in I}H_i$而上端是$\left\langle\bigcup_{i\in I}H_i\right\rangle$.

(*b*) 描述群S_3，D_4^*，Z_6，Z_{27}和Z_{36}的子群格。

3. 循 环 群

循环群的结构是相当简单的。我们将完全刻划出全部循环群（的同构类）。

定理3.1 加法群$\mathbb{Z}$的每个子群 H 都是循环群，$H=\langle 0\rangle$或者$H=\langle m\rangle$，其中m是H中的最小正整数。如果$H\neq\langle 0\rangle$，则H是无限群。

证明 H 或者为 $\langle 0\rangle$，或者包含一个最小的正整数 m。显然$\langle m\rangle=\{km|k\in\mathbb{Z}\}\subset H$。反之，如果$k\in H$，则$h=qm+r$，其中$q$，$r\in\mathbb{Z}$并且$0\leqslant r<m$(除法算式)。因为$r=h-qm\in H$，由 m 的最小性推出 $r=0$，从而 $h=qm$。因此 $H\subset\langle m\rangle$。如果 $H\neq\langle 0\rangle$，显然$H=\langle m\rangle$是无限的。∎

定理3.2 每个无限循环群均同构于加法群$\mathbb{Z}$。每个m阶有限循环群均同构于加法群Z_m。

证明 如果$G=\langle a\rangle$是循环群，则根据定理1.9和2.8，由$k\mapsto$

a^k给出的映射α：$\mathbf{Z}\to G$是满同态。如果$\ker\alpha=0$，由定理2.3(i)便知$\mathbf{Z}\cong G$。否则$\ker\alpha$便是$\mathbf{Z}$的非平凡子群(习题2.9)，从而$\ker\alpha=\langle m\rangle$，其中$m$是使$a^m=e$成立的最小正整数（定理3.1），对于所有$r,\ s\in\mathbf{Z}$，$a^r=a^s\Longleftrightarrow a^{r-s}=e\Longleftrightarrow r-s\in\ker\alpha=\langle m\rangle\Longleftrightarrow m\mid(r-s)$ $\Longleftrightarrow\bar{r}=\bar{s}$（在$Z_m$中）。（其中$\bar{k}$表示$k\in\mathbf{Z}$的同余类）。因此映射$\beta$：$Z_m\to G$，$\bar{k}\longmapsto a^k$是可定义的满同态。由于

$\beta(\bar{k})=e\Longleftrightarrow a^k=e=a^0\Longleftrightarrow\bar{k}=\bar{0}$（在$Z_m$中），从而$\beta$是单同态(定理2.3(i))，于是有同构$Z_m\cong G$。∎

定义3.3 假设G是群而$a\in G$。循环子群$\langle a\rangle$的阶也称作a的阶，并且表示成$|a|$。

定理3.4 假设G是群而$a\in G$。如果a有无限阶，则

(i) $a^k=e\Longleftrightarrow k=0$；

(ii) 元素$a^k(k\in\mathbf{Z})$是两两不同的。

如果a有有限阶 $m>0$，则

(iii) m是满足$a^m=e$的最小正整数；

(iv) $a^k=e\Longleftrightarrow m\mid k$；

(v) $a^r=a^s\Longleftrightarrow r\equiv s(\mathrm{mod}\,m)$；

(vi) $\langle a\rangle$由m个不同元素$a,\ a^2,\ \cdots,\ a^{m-1},\ a^m=e$所构成；

(vii) 对于每个$k\mid m$，$|a^k|=\dfrac{m}{k}$。

证明概要 (i)－(vi)：从定理3.2的证明可以直接推出。(vii)：$(a^k)^{m/k}=a^m=e$并且对所有$0<r<m/k$，$(a^k)^r\neq e$。因为不然的话，如果$a^{kr}=e$，其中$kr<k(m/k)=m$，便与(iii)相矛盾。因此由(iii)便知$|a^k|=m/k$。∎

定理3.5 循环群的每个同态象和每个子群都是循环群，特别地，如果H是$G=\langle a\rangle$的非平凡子群而m是满足 $a^m\in H$ 的最小正整数，则 $H=\langle a^m\rangle$。

证明概要 如果f：$G\to K$是群同态，则 $\mathrm{Im}f=\langle f(a)\rangle$。将定理3.1的证明简单地转成乘法记号（即将每个$t\in\mathbf{Z}$改成$a^t$），即可证明第二论断。即使当$G$是有限群时，这个证明也是有效的。∎

让我们回忆：群中两个不同的元素可能会生成同一个循环子群。

定理3.6 假设$G=\langle a\rangle$是循环群。如果G是无限的。则只有a和a^{-1}为G的生成元。如果G是m阶有限群，则a^k为G的生成元的充要条件是$(k,\ m)=1$。

证明概要 只需假定 $G=\mathbf{Z}$（这时容易证明定理结论）或者$G=Z_m$。对于后一情形，如果 $(k,\ m)=1$，则存在c，$d\in\mathbf{Z}$，使得 $ck+dm=1$。用此事实证明 $\bar{k}$ 生成Z_m。如果 $(k,\ m)=r>1$，证明对于$n=m/r<m$有 $n\bar{k}=\overline{nk}=\bar{0}$，从而 $\bar{k}$ 不能生成Z_m。∎

或许会有人天真地希望上面所采用的方法可以推广到具有两个生成元的群或者甚至于所有的有限生成群上去，从而能提供出一种刻划这些群结构的方法。不幸的是，即使是只有两个生成元的群都可能具有非常复杂的结构（比如它们不必是Abel群，见习题2.3和2.4）。事实上，我们能够刻划所有有限生成 Abel 群，但即使这件事也需要发展更多的理论。

习　题

1. 假定a，b是群 G 的元素，求证$|a|=|a^{-1}|$，$|ab|=|ba|$，并且对所有

$c \in G$, $|a| = |cac^{-1}|$.

2. 假设G是Abel群，其中元素a和b的阶分别为m和n. 求证G必包含一个元素，它的阶等于m和n的最小公倍数.〔提示：先对$(m, n) = 1$的情形证明〕

3. 假设G是pq阶Abel群，其中$(p, q) = 1$.如果存在$a, b \in G$使得$|a| = p$，$|b| = q$，求证G是循环群.

4. 如果$f: G \to H$是群同态，$a \in G$，并且$f(a)$在H中有有限阶，则或者$|a|$为无限，或者$|f(a)|$除尽$|a|$.

5. 令G为全体2×2的非异有理矩阵所组成的乘法群.证明$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$的阶为4，$b = \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}$的阶是3，但是$ab$有无限阶.另一方面，证明加法群$Z_2 \oplus \mathbf{Z}$中存在两个无限阶的非零元素$a$和$b$，使得$a + b$的阶数有限.

6. 如果G为n阶循环群而$k \mid n$，则G恰有一个k阶子群.

7. 设p为素数而H为$Z(p^\infty)$的子群(习题1.10).

   (a) $Z(p^\infty)$的每个元素均有有限阶p^n(对于某个$n \geqslant 0$).

   (b) 如果H至少有一个p^k阶元素但是没有阶数大于p^k的元素，则H是由$\overline{1/p^k}$生成的循环子群，从而$H \cong Z_{p^k}$.

   (c) 如果H中元素的阶没有上界，则$H = Z(p^\infty)$〔见习题2.16〕.

   (d) $Z(p^\infty)$的全部真子群为有限循环群 $C_n = \langle \overline{1/p^n} \rangle$ $(n = 0, 1, 2, \cdots)$. 并且$\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \cdots$.

   (e) 假设x_1，x_2，…是Abel群G中的元素，并且$|x_1| = p$，$px_2 = x_1$，$px_3 = x_2$，…，$px_{n+1} = x_n$，…. 则由$x_i (i \geqslant 1)$所生成的子群同构于$Z(p^\infty)$.〔提示：验证由$x_i \longmapsto \overline{1/p^i}$所诱导出的映射是可以定义的同构.〕

8. 只有有限多个子群的群必然是有限群.

9. 如果G是Abel群，则G中全体有限阶元素所组成的集合T是G的子群.〔比较习题5.〕

10. 一个非平凡的群为无限循环群的充要条件是它同构于它的每个真子群.

4. 陪集与计数

我们在本节中得到第一个重要的定理，它谈到有限群G的结构与其阶数$|G|$的数论特性之间的关系。开始我们先把群$\mathbb{Z}$中模m同余概念加以推广。根据定义，$a=b(\mathrm{mod}m)\Longleftrightarrow m|(a-b)\Longleftrightarrow a-b$是子群$\langle m\rangle=\{mk|k\in\mathbb{Z}\}$中的元素。更一般地（并且改成乘法记号）我们有

定义4.1 假设H是群G的子群，$a,b\in G$，如果$ab^{-1}\in H$，我们称a模H右同余于b，并且表示成$a\equiv_r b(\mathrm{mod}H)$。如果$a^{-1}b\in H$，则称$a$模$H$左同余于$b$，表示成$a\equiv_l b(\mathrm{mod}H)$。

假如G是Abel群，则模H的右同余和左同余是一致的（因为$ab^{-1}\in H\Longleftrightarrow(ab^{-1})^{-1}\in H$，而$(ab^{-1})^{-1}=ba^{-1}=(a^{-1}b)$。虽然存在着非Abel群$G$和它的子群$H$，使得右同余和左同余是一致的（第5节），但是在一般情形下这是不对的。

定理4.2 假设H是群G的子群，则

(i) 模H右〔左〕同余是G上的等价关系。

(ii) $a\in G$对于模H右〔左〕同余的等价类是集合$Ha=\{ha|h\in H\}$〔$aH=\{ah|h\in H\}$〕。

(iii)对于所有$a\in G$，$|Ha|=|H|=|aH|$。

集合Ha叫作是H在G中的一个右陪集，而aH叫作是H在G中的一个左陪集。一般说来，右陪集不一定也是左陪集(习题2)。

定理4.2的证明 我们将$a\equiv_r b(\mathrm{mod}H)$简记成$a\equiv b$，并且只对右同余和右陪集证明此定理，对于左同余可以采用类似的推理。

(i) 令a，b，$c\in G$。由于$aa^{-1}=e\in H$，从而$a\equiv a$，因此关系$\equiv$是自反的。又$\equiv$显然是对称的 $(a\equiv b\Rightarrow ab^{-1}\in H\Rightarrow(ab^{-1})^{-1}\in H\Rightarrow ba^{-1}\in H\Rightarrow b\equiv a)$。最后，$a\equiv b$和$b\equiv c$导致$ab^{-1}\in H$并且$bc^{-1}\in H$。因此$ac^{-1}=(ab^{-1})(bc^{-1})\in H$。从而$a\equiv c$，因此$\equiv$是传递的。所以模$H$右同余是等价关系。

(ii) $a\in G$在右同余之下的等价类是$\{x\in G|x\equiv a\}=\{x\in G|xa^{-1}\in H\}=\{x\in G|xa^{-1}=h\in H\}=\{x\in G|x=ha,\ h\in H\}=\{ha|h\in H\}=Ha$。

(iii) 易知映射$Ha\longrightarrow H$，$ha\longmapsto h$是一一对应 ∎

系4.3 假设H是群G的子群。则

(i) G是H在G中的全体右〔左〕陪集之并。

(ii) H在G中的两个右〔左〕陪集或者非交或者相等。

(iii)对于所有a，$b\in G$，$Ha=Hb\Longleftrightarrow ab^{-1}\in H$；$aH=bH\Longleftrightarrow a^{-1}b\in H$。

(iv) 如果令$\mathscr{R}$是H在G中不同的右陪集所组成的集合，而$\mathscr{L}$是H在G中不同的左陪集所组成的集合，则$|\mathscr{R}|=|\mathscr{L}|$。

证明 (i)—(iii)是上一定理和引论第4节中命题(19)—(21)的直接推论。(iv)：映射$\mathscr{R}\to\mathscr{L}$，$Ha\longmapsto a^{-1}H$是一一对应，这是因为 $Ha=Hb\Longleftrightarrow ab^{-1}\in H\Longleftrightarrow(a^{-1})^{-1}b^{-1}\in H\Longleftrightarrow a^{-1}H=b^{-1}H$。∎

加法记号 如果H是加法群G的子群，则模H右同余定义为$a\equiv_r b(\mathrm{mod}H)\Longleftrightarrow a-b\in H$。$a\in G$的等价类是右陪集$H+a=\{k+a|k\in H\}$。对于左同余和左陪集有类似结论。

定义4.4 假设H是群G的子群。则 H在G中的指数（表示成$[G:H]$）是指H在G中不同右〔或者左〕陪集集合的势。

从系4.3(iv)可知 $[G:H]$ 与定义中使用的是右陪集还是左陪集无关。我们的主要兴趣为$[G:H]$有限的情形。甚至G和 H 均是无限群时，也可能有有限的指数$[G:H]$(例如从引论中的定理6.8(i)可知$[\mathbb{Z}:\langle m\rangle]=m$。注意如果 $H=\langle e\rangle$，则对每个 $a\in G$ 均有 $Ha=\{a\}$，从而$[G:H]=|G|$。

子群H在群 G 中的右陪集完全代表集合是指集合 $\{a_i\}$，使得H在G中的每个右陪集均恰好有一个元素在 $\{a_i\}$ 之中。显然集合$\{a_i\}$的势等于$[G:H]$。由于$H=He$自己是一个右陪集，从而 $\{a_i\}$中恰包含H中一个元素。对于左陪集则有类似一些论断。

定理4.5 如果K，H，G是群，并且$K<H<G$，则 $[G:K]=[G:H][H:K]$。如果这三个指数当中任意两个是有限的，则第三个指数也有限。

证明 根据系4.3 $G=\bigcup_{i\in I}Ha_i$，其中$a_i\in G$，$|I|=[G:H]$并且诸陪集 Ha_i 是彼此非交的（即 $Ha_i=Ha_j\Longleftrightarrow i=j$）。类似地，$H=\bigcup_{j\in J}Kb_j$，其中$b_j\in H$，$|J|=[H:K]$ 并且诸陪集 Kb_j 是两两非交的。因此 $G=\bigcup_{i\in I}Ha_i=\bigcup_{i\in I}\left(\bigcup_{j\in J}Kb_j\right)a_i=\bigcup_{(i,j)\in I\times J}Kb_ja_i$ 只需再证明诸陪集 Kb_ja_i 是两两非交的，因为这时由系 4.3 便知 $[G:K]=|I\times J|$，从而$[G:K]=|I\times J|=|I||J|=[G:H][H:K]$。如果$Kb_ja_i=Kb_ra_t$，则$b_ja_i=kb_ra_t(k\in K)$。由于$b_j$，$b_r$，$k\in H$，我们有$Ha_i=Hb_ja_i=Hkb_ra_t=Ha_t$。于是$i=t$，从而 $b_j=kb_r$。因

此$Kb_j = Kkb_r = Kb_r$从而$j = r$。因此诸陪集$Kb_j a_i$是两两非交的。定理的最后论断是显然的。∎

系4.6 (Lagrange) 如果H是群G的子群，则$|G| = [G:H]|H|$。特别如果G是有限群，则$a \in G$的阶$|a|$除尽$|G|$。

证明 对于第一论断，将定理用于$K = \langle e \rangle$即可。而第二论断是第一论断取$H = \langle a \rangle$时的特殊情形。∎

(有限)群论中许多证明依赖于各种“计数”技巧，现在我们来介绍其中的一些。如果G是群而H和K是G的子集合，我们用HK表示集合$\{ab | a \in H, b \in K\}$。子群的右陪集和左陪集是其特殊情形。如果$H$和$K$是子群，$HK$可能不是子群(习题7)。

定理4.7 假设H和K是群G的有限子群，则$|HK| = |H||K|/|H \cap K|$。

证明概要 $C = H \cap K$是K的子群，指数为$n = |K|/|H \cap K|$，而K为右陪集之非交并：$Ck_1 \cup Ck_2 \cup \cdots \cup Ck_n$(对某些$k_i \in K$)。由于$HC = H$，从而$HK$是非交并$Hk_1 \cup Hk_2 \cup \cdots \cup Hk_n$。因此$|HK| = |H| \cdot n = |H||K|/|H \cap K|$。∎

命题4.8 如果H和K是群G的子群，则$[H:H \cap K] \leqslant [G:K]$。如果$[G:K]$有限，则$[H:H \cap K] = [G:K] \Longleftrightarrow G = KH$。

证明概要 令A为$H \cap K$在H中所有右陪集组成的集合，而B是K在G中所有右陪集组成的集合。则映射$\varphi: A \to B$，$(H \cap K)h \mapsto Kh (h \in H)$是可以定义的，因为$(H \cap K)h' = (H \cap K)h \Rightarrow h'h^{-1} \in H \cap K \subset K \Rightarrow Kh' = Kh$，证明$\varphi$是单射，从而$[H:H \cap K] = |A| \leqslant |B| = [G:K]$。如果$[G:K]$是有限的，再证明$[H:H \cap K] = [G:K]$

$\Leftrightarrow\varphi$是满射。而φ是满射$\Leftrightarrow G=KH$。注意对于$h\in H$，$k\in K$，则$Kkh=Kh$，这是因为$(kh)h^{-1}=k\in K$。■

命题4.9 假设H和K均是群G的指数有限的子群，则$[G:H\cap K]$有限并且$[G:H\cap K]\leqslant[G:H][G:K]$。进而，$[G:H\cap K]=[G:H][G:K]\Leftrightarrow G=HK$。

证明作为练习。利用定理4.5和命题4.8。■

习　题

1. 假设G是群而$\{H_i|i\in I\}$是一个子群族，则对每个$a\in G$，$(\bigcap_i H_i)a=\bigcap_i H_ia$。

2. (a)假设H是S_8的由$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$生成的(2阶)子群。则(除了$H$自身之外)$H$的每个左陪集均不是右陪集。此外，还存在$a\in S_8$，使得$aH\cap Ha=\{a\}$。

   (b) 如果K是S_8的由$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$生成的(3阶)子群，则$K$的每个左陪集均是$K$的右陪集。

3. 下列关于有限群G上的一些条件是彼此等价的：

   (i) $|G|$为素数。

   (ii) $G\neq\langle e\rangle$并且G没有真子群。

   (iii) $G\cong Z_p$，其中p为某个素数。

4. (Euler-Fermat) 假设a为整数，p为素数并且$p\nmid a$。则$a^{p-1}\equiv1\ (\mathrm{mod}\ p)$。〔提示：考虑$\overline{a}\in Z_p$和$Z_p$的非零元素的乘法群。见习题1.7.〕由此得出$a^p=a(\mathrm{mod}\ p)$(对任何整数$a$)。

5. 求证(不计同构)只有两个4阶群，即Z_4和$Z_2\oplus Z_2$。〔提示：根据Lagrange定理4.6，一个4阶群如果不是循环群，必然由幺元素和三个2

阶元素所组成.〕

6. H和K是群G的子群.则HK为G的子群$\Longleftrightarrow HK=KH$.

7. 假设G为p^km阶群，其中p为素数而$(p, m)=1$.令H是p^k阶子群而K为p^d阶子群，其中$0<d\leqslant k$，并且$K\not\subset H$.证明HK不是G的子群.

8. 如果H和K是群G的指数有限的子群，并且$〔G:H〕$和$〔G:K〕$互素，则$G=HK$.

9. 如果H，K，N均为群G的子群，并且$H<N$，则$HK\cap N=H(K\cap N)$.

10. 假设H，K，N是群G的子群，并且$H<K$，$H\cap N=K\cap N$，$HN=KN$，求证$H=K$.

11. 假设G是$2n$阶群，则G包含有2阶元素.如果n是奇数并且G是Abel群，则G只有一个2阶元素.

12. 如果H和K是群G的子群，则$〔H\vee K:H〕\geqslant〔K:H\cap K〕$.

13. 如果$p>q$并且p，q均是素数，则每个pq阶群至多有一个p阶子群.〔提示：假设H，K是不同的p阶子群.求证$H\cap K=\langle e\rangle$.利用习题12导出矛盾.〕

14. 假设G是群，a，$b\in G$使得 (i) $|a|=4=|b|$;(ii) $a^2=b^2$; (iii) $ba=a^3b=a^{-1}b$; (iv) $a\neq b$; (v) $G=\langle a, b\rangle$.求证$|G|=8$并且$G\cong Q_8$(见习题2.3.注意Q_8的生成元A和B也满足(i)—(v).)

5. 正规性，商群和同态

我们将研究群G具有如下性质的子群N：模N的左同余和右同余一致.在决定群G的结构和以G为定义域的同态的特性时，这样的子群起着重要的作用.

定理5.1 如果N是群G的子群，则以下一些条件是彼此等价的。

(i) 模N的左右同余一致（即在G上定义出同样的等价关系）；

(ii) N在G中的每个左陪集均是N在G中的右陪集；

(iii) 对于每个$a\in G$，$aN=Na$。

(iv) 对于每个$a\in G$，$aNa^{-1}\subset N$，其中，

$$aNa^{-1}=\{ana^{-1}\mid n\in N\};$$

(v) 对于每个$a\in G$，$aNa^{-1}=N$。

证明 (i)$\Longleftrightarrow$(iii)：两个等价关系R和S是同样的，当且仅当每个元素对于R的等价类等于它对于S的等价类。在我们这里，两种等价类分别是N的左陪集和右陪集。(ii)$\Longleftrightarrow$(iii)：如果$aN=Nb$，$b\in G$，则$a\in Nb\cap Na$，这导致$Nb=Na$，因为两个右陪集或者非交或者相等。(iii)$\Rightarrow$(iv)是显然的。(iv)$\Rightarrow$(v)：我们有$aNa^{-1}\subset N$。由于(iv)对于$a^{-1}\in G$也成立，从而$a^{-1}Na\subset N$。因此对于每个$n\in N$，$n=a(a^{-1}na)a^{-1}\in aNa^{-1}$，从而$N\subset aNa^{-1}$。(v)$\Rightarrow$(ii)是很容易的。 ∎

定义5.2 群G中满足定理5.1中等价条件的子群N叫作在G中正规的（或者叫作G的正规子群）。如果N在G中正规，我们写成$N\lhd G$。

由定理5.1可知，在表达模一个正规子群的同余时，我们可去略去下标“r”和“l”。

例 Abel群的每个子群显然都是正规子群。S_3中由$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$生成的子群$H$是正规的（习题4.2）。更一般地，群$G$中每个指数是2的子群都是正规的（习题1）。任意一个正规子群族的交也是正规子群（习题2）。

如果群G有两个子群N和M，使得$N \lhd M$，$M \lhd G$，我们不能由此推出$N \lhd G$（习题10）．但是不难看出，如果N在G中正规，则N在G的每个包含N的子群中也正规．

让我们回忆：两个子群的并$H \vee K$是由H和K生成的子群$\langle H \cup K \rangle$．

定理5.3 假设K和N是群G的子群，并且N在G中正规．则

(i) $N \cap K$是K的正规子群；

(ii) N是$N \vee K$的正规子群；

(iii) $NK = N \vee K = KN$；

(iv) 如果K在G中正规并且$K \cap N = \langle e \rangle$，则对所有$k \in K$和$n \in N$，$nk = kn$．

证明 (i) 如果$n \in N \cap K$并且$a \in K$，则$ana^{-1} \in N$（因为$N \lhd G$）和$ana^{-1} \in K$（因为$K < G$）．因此$a(N \cap K)a^{-1} \subset N \cap K$，即$N \cap K \lhd K$．

(ii) 是显然的，因为$N < N \vee K$．

(iii) 显然$NK \subset N \vee K$．元素$x \in N \vee K$具有形式$n_1 k_1 n_2 k_2 \cdots n_r k_r$，其中$n_i \in N$，$k_i \in K$（定理2.8）．由于$N \lhd G$，$n_i k_j = k_j n_i'$，$n_i' \in N$．从而$x$可以写成$n(k_1 \cdots k_r)$，$n \in N$．因此$N \vee K \subset NK$．类似地有$KN = N \vee K$．

(iv) 设$k \in K$，$n \in N$．则$nkn^{-1} \in K$（因为$K \lhd G$）并且$kn^{-1}k^{-1} \in N$（因为$N \lhd G$）．于是$(nkn^{-1})k^{-1} = n(kn^{-1}k^{-1}) \in N \cap K = \langle e \rangle$，这导致$kn = nk$．∎

定理5.4 如果N是群G的正规子群，而G/N是N在G中的全体（左）陪集所构成的集合，则对于由$(aN)(bN) = abN$所给出

的二元运算，G/N是$[G:N]$阶群。

证明 由于陪集$aN[bN, abN]$只不过是模N同余这一等价关系之下$a\in G[b\in G, ab\in G]$的等价类，根据定理1.5，只需证明模N同余是同余关系即可，即要证明由$a_1\equiv a(\mathrm{mod}N)$和$b_1\equiv b(\mathrm{mod}N)$导致$a_1b_1\equiv ab(\mathrm{mod}N)$。根据假设$a_1a^{-1}=n_1\in N$, $b_1b^{-1}=n_2\in N$。从而$(a_1b_1)(ab)^{-1}=a_1b_1b^{-1}a^{-1}=(a_1n_2)a^{-1}$。但是$N$是正规的，从而$a_1N=Na_1$，这导致$a_1n_2=n_3a_1$，其中$n_3\in N$。从而$(a_1b_1)(ab)^{-1}=(a_1n_2)a^{-1}=n_3a_1a^{-1}=n_3n_1\in N$，于是$a_1b_1\equiv ab(\mathrm{mod}N)$。

如果N是群G的正规子群，则定理5.4中的群G/N叫作G对于N的商群。如果G记成加法，则G/N中的群运算为$(a+N)+(b+N)=(a+b)+N$。

注记：如果$m>1$是(固定的)整数而$k\in\mathbf{Z}$，则定义4.1前面的注记表明，k对模m同余的等价类恰好是$\mathbf{Z}$中$\langle m\rangle$之包含k的陪集，从而作为集合我们有$Z_m=\mathbf{Z}/\langle m\rangle$。定理1.5和5.4表明二者的群运算是一致的，因此作为群也有$Z_m=\mathbf{Z}/\langle m\rangle$。

现在我们展示正规子群，商群和同态之间的关系。

定理5.5 如果$f:G\to H$是群同态，则f的核是G的正规子群。反之，如果N是G的正规子群，则映射$\pi:G\to G/N$, $\pi(a)=aN$是满同态，并且它的核为N。

证明 如果$x\in\mathrm{Ker}f$, $a\in G$，则

$$f(axa^{-1})=f(a)f(x)f(a^{-1})=f(a)ef(a)^{-1}=e$$

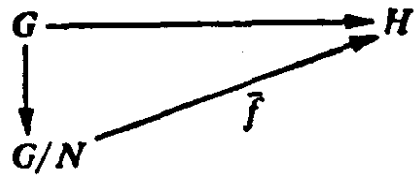
从而$axa^{-1}\in\mathrm{Ker}f$。因此$a(\mathrm{Ker}f)a^{-1}\subset\mathrm{Ker}f$，即$\mathrm{Ker}f\lhd G$。映射$\pi:G\to G/N$显然是满射。又由于$\pi(ab)=abN=aNbN=\pi(a)\pi(b)$，从而$\pi$是满同态。$\mathrm{Ker}\pi=\{a\in G\mid\pi(a)=eN=N\}=\{a\in G\mid aN=N\}$

$=\{a\in G\mid a\in N\}=N$. ∎

映射π：$G\to G/N$叫作正则满同态或者正则射影。今后若不加另外说明，$G\to G/N(N\lhd G)$永远表示这个正则满同态。

定理5.6 如果$f:G\to H$是群同态，N是G的正规子群并且$N\subset \mathrm{Ker}f$，则存在唯一的同态$\bar{f}:G/N\to H$使得对所有$a\in G$，$\bar{f}(aN)=f(a)$。此外，$\mathrm{Im}f=\mathrm{Im}\bar{f}$，$\mathrm{Ker}\bar{f}=\mathrm{Ker}f/N$。最后，$\bar{f}$是同构$\Longleftrightarrow f$为满同态并且$N=\mathrm{Ker}f$。

结论的本质部分可以重新叙述成：存在着唯一的同态$\bar{f}:G/N\to H$，使得左边图表是交换的。



下面的系5.8也可以叙述成交换图表的形式。

定理5.6的证明 如果$b\in aN$，则$b=an$，$n\in N$，并且$f(b)=f(an)=f(a)f(n)=f(a)e=f(a)$（因为$N<\mathrm{Ker}f$）。因此$f$在陪集$aN$的每个元素上取相同的值，从而可以定义函数$\bar{f}:G/N\to H$，$\bar{f}(aN)=f(a)$。由于$\bar{f}(aNbN)=\bar{f}(abN)=f(ab)=f(a)f(b)=\bar{f}(aN)\bar{f}(bN)$，从而$\bar{f}$是同态。显然$\mathrm{Im}\bar{f}=\mathrm{Im}f$，并且

$$aN\in\mathrm{Ker}\bar{f}\iff f(a)=e\iff a\in\mathrm{Ker}f.$$

从而$\mathrm{Ker}\bar{f}=\{aN\mid a\in\mathrm{Ker}f\}=(\mathrm{Ker}f)/N$。$\bar{f}$是唯一的，因为它由$f$所完全决定。最后，显然$\bar{f}$为满同态$\Longleftrightarrow f$是满同态。而由定理2.3可知$\bar{f}$为单同态$\Longleftrightarrow\mathrm{Ker}\bar{f}=(\mathrm{Ker}f)/N$是$G/N$的平凡子群$\Longleftrightarrow\mathrm{Ker}f=N$。 ∎

系5.7 （第一同构定理）如果$f:G\to H$是群同态，则f诱导出同构$G/\mathrm{Ker}f\cong\mathrm{Im}f$。

证明 $f:G\to\mathrm{Im}f$是满同态。将定理5.6用于$N=\mathrm{Ker}f$。∎

系5.8 如果$f:G\to H$是群同态，$N\lhd G, M\lhd$ 并且 $f(N)<M$。则f诱导出同态 $\bar{f}:G/N\to H/M$，$aN\longmapsto f(a)M$。 $\bar{f}$ 为同构$\Longleftrightarrow$ $\mathrm{Im}f\vee M=H$并且$f^{-1}(M)\subset N$。特别地，如果f是满同态并且$f(N)=M$，$\mathrm{Ker}f\subset N$，则$\bar{f}$ 是同构。

证明概要 考虑合成映射$G\xrightarrow{f}H\xrightarrow{\pi}H/M$，验证 $N\subset f^{-1}(M)=\mathrm{Ker}\pi f$。根据定理5.6（用于$\pi f$），映射$G/N\to H/M$，$aN\longmapsto(\pi f)(a)=f(a)M$ 是同态，并且它是同构$\Longleftrightarrow$ πf 为满同态并且 $N=\mathrm{Ker}\pi f$。但是后面条件又等价于$\mathrm{Im}f\vee M=H$和$f^{-1}(M)\subset N$。如果f是满同态，则$H=\mathrm{Im}f=\mathrm{Im}f\vee M$。如果$f(N)=M$并且$\mathrm{Ker}f\subset N$，则$g^{-1}(M)\subset N$，从而$\bar{f}$ 是同构。∎

系5.9 （第二同构定理） 如果K和N是群G的子群，$N\lhd G$，则$K/(N\cap K)\cong NK/N$。

证明 根据定理5.3，$N\lhd NK=N\vee K$。合成映射$K\xrightarrow{\subset}NK\xrightarrow{\pi}NK/N$是一个同态$f$，其核为$K\cap N$，于是由系5.7，$\bar{f}:K/K\cap N\cong\mathrm{Im}f$。$NK/N$中每个元素均有形式$nkN(n\in N,\ k\in K)$。而$N$的正规性导致$nk=kn_1(n_1\in N)$，从而$nkN=kn_1N=kN=f(k)$。因此$f$是满同态，于是$\mathrm{Im}f=NK/N$。∎

系5.10 （第三同构定理） 如果H和K均是群G的正规子群，并且$K<H$，则H/K是G/K的正规子群，并且$(G/K)/(H/K)\cong G/H$。

证明 恒等映射$1_G:G\to G$有性质$1_G(K)<H$，由此得到一个满同态I：$G/K\to G/H$，其中$I(aK)=aH$。由于$H=I(aK)\Longleftrightarrow a\in H$，从而$\mathrm{Ker}I=\{aK\mid a\in H\}=H/K$。于是由定理5.5便有$H/K\lhd$

G/K，而由系5.7便有$G/H=\mathrm{Im}I\cong(G/K)/\mathrm{Ker}I=(G/K)/(H/K)$.∎

定理5.11 如果$f:G\to H$是群的满同态，则$K\mapsto f(K)$给出G之全体包含$\mathrm{Ker}f$的子群K所组成的集合$S_f(G)$与H的全体子群所组成的集合$S(H)$之间的一一对应。并且在这个对应之下，正规子群对应于正规子群。

证明概要 根据习题2.9，$K\mapsto f(K)$定义出一个函数φ：$S_f(G)\to S(H)$，并且对于H的每个子群J，$f^{-1}(J)$是G的子群。由于$J<H$导致$\mathrm{Ker}f<f^{-1}(J)$并且$f(f^{-1}(J))=J$，从而φ是满射。习题18表明$f^{-1}(f(K))=K\Leftrightarrow\mathrm{Ker}f<K$。从而$\varphi$是单射。为证最后一个论断，只需验证$K\lhd G$导致$f(K)\lhd H$，而$J\lhd H$导致$f^{-1}(J)\lhd G$。∎

系5.12 如果N是群G的正规子群，则G/N的每个子群均有形式K/N，其中K是G的包含N的子群。进而，$K/N\lhd G/N\Leftrightarrow K\lhd G$。

证明 将定理5.11用于正则满同态$\pi:G\to G/N$。如果$N<K<G$，则$\pi(K)=K/N$。∎

习　题

1. 如果N是群G中指数为2的子群，则N在G中正规。
2. 如果$\{N_i|i\in I\}$是群G的正规子群族，则$\bigcap_{i\in I}N_i$是G的正规子群。
3. 假设N是群G的子群。则N⊲G⟺模N(右)同余是G上的同余关系。
4. 假设～是群G上的等价关系，令$N=\{a\in G|a\sim e\}$。则～是G上的同余关系⟺$N\lhd G$并且～是模N同余。
5. 以N表示满足$\sigma(4)=4$的所有置换$\sigma\in S_4$组成的子群。N是否在S_4中正规？

6. 假设$H<G$，则对于每个$a\in G$，集合aHa^{-1}是子群，并且$H\cong aHa^{-1}$。

7. 假设G为有限群而H是G的n阶子群，如果H是G之唯一的n阶子群，则H在G中正规。

8. 四元数群的每个子群都是正规的（见习题2.3和4.14）。

9. (*a*) 如果G是群，则G的中心是G的正规子群（见习题2.11）；
(*b*) 对于每个$n>2$，S_n的中心为$\langle e\rangle$。

10. 求D^*_4的子群H和K，使得$H\lhd K$，$K\lhd D^*_4$，但是H在D^*_4中不正规。

11. 如果H是群G的循环子群，并且H在G中正规，则H的每个子群在G中均正规〔比较习题10.〕

12. 如果H是群G的正规子群，使得H和G/H均是有限生成的，则G也是有限生成的。

13. (*a*) 假设$H\lhd G$，$K\lhd G$.求证$H\vee K$在G中正规。
(*b*) 求证G的全体正规子群组成的集合对于包含序形成完备格（引论的习题7.2）。

14. 如果$N_1\lhd G_1$，$N_2\lhd G_2$，则$(N_1\times N_2)\lhd(G_1\times G_2)$并且$(G_1\times G_2)/(N^1\times N_2)\cong(G_1/N_1)\times(G_2/N_2)$。

15. 假设$N\lhd G$，$K\lhd G$.如果$N\cap K=\langle e\rangle$并且$N\vee K=G$，则$G/N\cong K$。

16. 如果$f:G\to H$是同态，H是Abel群而N是G的包含Ker$f$的子群，则N在G中正规。

17. (*a*) 考虑**Z**的子群$\langle 6\rangle$和$\langle 30\rangle$，求证$\langle 6\rangle/\langle 30\rangle\cong Z_5$。
(*b*) 对于任何k，$m>0$，$\langle k\rangle/\langle km\rangle\cong Z_m$.特别地，$Z/\langle m\rangle=\langle 1\rangle/\langle m\rangle\cong Z_m$。

18. 如果$f:G\to H$是群同态，核为N，并且$K<G$，求证$f^{-1}(f(K))=KN$.从而$f^{-1}(f(K))=K\Longleftrightarrow N<K$。

19. 如果$N\lhd G$，〔$G:N$〕有限，$H<G$，$|H|$有限，并且〔$G:N$〕和$|H|$互素，则$H<N$。

20. 如果$N\lhd G$，$|N|$有限，$H<G$，〔$G:H$〕有限，并且〔$G:H$〕和$|N|$互素，则$N<H$。

21. 如果H是$Z(p^\infty)$的子群并且$H \neq Z(p^\infty)$，则$Z(p^\infty)/H \cong Z(p^\infty)$.〔提示：如果 $H = \langle \overline{1/p^n} \rangle$，令$x_i = \overline{1/p^{n+i}} + H$然后利用习题3.7〈e〉.〕

6. 对称群，交错群和正多边形群

在本节中我们将较为详细地研究对称群S_n和它的某些子群。按照定义，S_n是全体一一对应$I_n \to I_n$所构成的群，其中$I_n = \{1, 2, \cdots, n\}$。$S_n$中的元素叫作置换。对于$S_n$中的置换，除了第39页所给的记号之外，还有另一种标准的记号：

定义6.1 假设$i_1, i_2, \cdots, i_r (r \leqslant n)$是$I_n = \{1, 2, \cdots, n\}$中的不同元素。我们以 $(i_1 i_2 i_3 \cdots i_r)$ 表示如下的置换：$i_1 \mapsto i_2$，$i_2 \mapsto i_3$，$i_3 \mapsto i_4$，$\cdots$，$i_{r-1} \mapsto i_r$，$i_r \mapsto i_1$，同时将I_n中每个其他元素均映到自身。$(i_1 i_2 \cdots i_r)$ 叫作长为r的轮换或者叫作一个 r-轮换。而每个2-轮换叫作对换。

轮换的表达方式不是唯一的（见下面）。严格说来，轮换记号实际上有些含混，因为 $(i_1 \cdots i_r)$ 可以是任何$S_n (n \geqslant r)$ 中的元素。但是结合上下文不会造成混乱。1-轮换 (k) 即是恒等置换。r-轮换显然是S_n中的r阶元素。还要注意，如果τ是轮换而 $\tau(x) \neq x$（对于某个$x \in I_n$），则 $\tau = (x \tau(x) \tau^2(x) \cdots \tau^d(x))$（对于某个 $d \geqslant 1$）。轮换 $(i_1 i_2 \cdots i_r)$ 的逆是轮换 $(i_r i_{r-1} i_{r-2} \cdots i_2 i_1) = (i_1 i_r i_{r-1} i_{r-2} \cdots i_2)$（验证！）。

例 置换$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ 是4-轮换：$\tau = (1432) = (4321) = (3214) = (2143)$。如果$\sigma$是3-轮换 (125)，则$\sigma\tau = (125)(1432) = (1435)$

(记住：置换是函数并且$\sigma\tau$是先τ后σ)．类似地，$\tau\sigma=(1432)(125)=(2543)$，从而$\sigma\tau\neq\tau\sigma$。但是有一种情形下两个置换肯定是可以交换的。

定义6.2 S_n中的置换σ_1，σ_2，…，σ_r叫作非交的，是指对于某个i，$1\leqslant i\leqslant r$和$k\in I_n$，如果$\sigma_i(k)\neq k$，则对所有$j\neq i$，$\sigma_j(k)=k$。

换句话说，σ_1，σ_2，…，σ_r是非交的，当且仅当I_n中没有元素被σ_1，…，σ_r中多于一个置换所移动。不难看出，如果σ和τ是非交的，则$\tau\sigma=\sigma\tau$。

定理6.3 S_n中每个恒等置换（不计其因子的次序）唯一地表示成非交轮换之积，使得每个轮换的长度均$\geqslant 2$。

证明概要 令$\sigma\in S_n$，$\sigma\neq(1)$。验证下面是I_n上的等价关系：对于x，$y\in I_n$，$x\sim y\Longleftrightarrow$存在某个$m\in\mathbf{Z}$，使得$y=\sigma^m(x)$。这个等价关系的等价类叫作$\sigma$的轨道（orbit），全体轨道$\{B_i\mid 1\leqslant i\leqslant S\}$形成$I_n$的一个分拆（引论的定理4.1）。注意如果$x\in B_i$，则$B_i=\{u\mid x\sim u\}=\{\sigma^m(x)\mid m\in\mathbf{Z}\}$。以$B_1$，$B_2$，…，$B_r(1\leqslant r\leqslant S)$表示其中包含多于一个元素的那些轨道（由于$\sigma\neq(1)$，从而$r\geqslant 1$）。对于每个$i\leqslant r$，定义$\sigma_i\in S_n$为

$$\sigma_i(x)=\begin{cases}\sigma(x), & \text{如果}x\in B_i\\ x, & \text{如果}x\notin B_i.\end{cases}$$

每个σ_i都定义出I_n的一个非恒等置换，这是因为$\sigma\mid B_i$是一一对应$B_i\to B_i$。又由于集合B_1，…，B_r是两两非交的，从而σ_1，σ_2，…，σ_r是彼此非交的置换。最后验证$\sigma=\sigma_1\sigma_2\cdots\sigma_r$。[注意$x\in B_i$导致$\sigma(x)=\sigma_i(x)$（如果$i\leqslant r$）和$\sigma(x)=x$(如果$i>r$)。再利用非交性质]我们还需证明每个$\sigma_i$均是轮换。

如果$x\in B_i(i\leqslant r)$，由于B_i是有限集，从而有最小的正整数d，使得对某个$j(0\leqslant j<d)$，$\sigma^d(x)=\sigma^j(x)$。由于$\sigma^{d-j}(x)=x$而$0<d-j\leqslant d$，从而必然$j=0$以及$\sigma^d(x)=x$。于是$(x\sigma(x)\sigma^2(x)\cdots\sigma^{d-1}(x))$是长度$\geqslant 2$的轮换。如果$\sigma^m(x)\in B_i$，则有$a$，$b\in\mathbf{Z}$，$0\leqslant b<d$使得$m=ad+b$。于是$\sigma^m(x)=\sigma^{b+ad}(x)=\sigma^b\sigma^{ad}(x)=\sigma^b(x)\in\{x,\sigma(x),\sigma^2(x),\cdots,\sigma^{d-1}(x)\}$。因此$B_i=\{x,\sigma(x),\sigma^2(x),\cdots,\sigma^{d-1}(x)\}$由此可知$\sigma_i$是轮换

$$(x\sigma(x)\sigma^2(x)\cdots\sigma^{d-1}(x))。$$

假设τ_1，…，τ_t是非交轮换，并且$\sigma=\tau_1\tau_2\cdots\tau_t$。令$x\in I_n$使得$\sigma(x)\neq x$。由非交性质可知存在唯一的$j(1\leqslant j\leqslant t)$，使得$\sigma(x)=\tau_j(x)$。由于$\sigma\tau_j=\tau_j\sigma$，从而对每个$k\in\mathbf{Z}$，$\sigma^k(x)=\tau_j^k(x)$。因此$x$在$\tau_j$之下的轨道恰好为$x$在$\sigma$之下的轨道，设此轨道为$B_i$。这时，对每个$y\in B_i$，$\tau_j(y)=\sigma(y)$（因为对于某个$n\in\mathbf{Z}$，$y=\sigma^n(x)=\tau_j^n(x)$）。由于$\tau_j$是轮换，它只有一个非平凡的轨道（验证!）。由于$x\neq\sigma(x)=\tau_j(x)$，从而这个轨道必为$B_i$。因此对每个$y\notin B_i$，$\tau_j(y)=y$，于是$\tau_j=\sigma_j$。然后适当运用数学归纳法即可证明$r=t$并且（在重新标记之后）$\sigma_i=\tau_i$（对每个$i=1,2,\cdots,r$）。∎

系6.4 置换$\sigma\in S_n$的阶是它的诸非交轮换之阶的最小公倍数。

证明 设$\sigma=\sigma_1\cdots\sigma_r$，其中$\{\sigma_i\}$是非交的轮换。由于非交的轮换是可交换的，从而对每个$m\in\mathbf{Z}$，$\sigma^m=\sigma_1^m\cdots\sigma_r^m$。并且$\sigma^m=(1)\Longleftrightarrow$对每个$i$，$\sigma_i^m=(1)$。因此$\sigma^m=(1)\Longleftrightarrow$对每个$i$，$|\sigma_i|$均除尽$m$（定理3.4）。由于$|\sigma|$是满足这种性质的最小$m$，由此即得结论。∎

系6.5 S_n中每个置换均可写成（不必非交的）对换之积。

证明 根据定理6.3,只需证明每个轮换是对换之积. 这是很容易的: $(x_1)=(x_1x_2)(x_1x_2)$, 而对于$r>1$, $(x_1x_2x_3\cdots x_r)=(x_1x_r)(x_1x_{r-1})\cdots(x_1x_3)(x_1x_2)$. ∎

定义6.6 置换$\tau\in S_n$叫作偶置换[奇置换],是指τ可以写成偶数个[奇数个]对换之积.

如果τ是偶置换或奇置换,我们称置换τ的符号(表示成$\mathrm{sgn}\tau$)分别为1或-1. $\mathrm{sgn}\tau$的可定义性是下面定理的直接推论.

定理6.7 $S_n(n\geqslant 2)$中的置换不能同时是偶置换和奇置换.

证明 假设$i_1, i_2, \cdots i_n$是整数1, 2, …, n的某个排列, 定义

$$\Delta(i_1, \cdots, i_n)=\prod_{1\leqslant j<k\leqslant n}(i_j-i_k).$$

注意$\Delta(i_1, \cdots, i_n)\neq 0$. 我们首先对于对换$\sigma=(i_ci_d)\in S_n$, $(c<d)$计算$\Delta(\sigma(i_1), \cdots, \sigma(i_n))$. 结果是

$$\Delta(i_1, \cdots, i_n)=(i_c-i_d)ABCDEFG,$$

其中

$$A=\prod_{\substack{j<k\\ j,\,k\neq c,\,d}}(i_j-i_k),\quad B=\prod_{j<c}(i_j-i_c),\quad C=\prod_{j<c}(i_j-i_d),$$

$$D=\prod_{c<j<d}(i_j-i_d),\quad E=\prod_{c<k<d}(i_c-i_k),\quad F=\prod_{d<k}(i_c-i_k),$$

$$G=\prod_{d<k}(i_d-i_k).$$

以$\sigma(A)$表示 $\prod_{\substack{j<k\\ j,\,k\neq c,\,d}}(\sigma(i_j)-\sigma(i_k))$, 类似地有$\sigma(B)$, $\sigma(C)$等等. 证明$\sigma(A)=A$, $\sigma(B)=C$, $\sigma(C)=B$, $\sigma(D)=(-1)^{d-c-1}E$,

$\sigma(E)=(-)^{d-c-1}D$, $\sigma(F)=G$, $\sigma(G)=F$。最后，$\sigma(i_c-i_d)=\sigma(i_c)-\sigma(i_d)=i_d-i_c=-(i_c-i_d)$。从而

$$\begin{aligned}\Delta(\sigma(i_1),\ \cdots,\ \sigma(i_n))&=\sigma(i_c-i_d)\sigma(A)\sigma(B)\cdots\sigma(G)\\&=(-1)^{1+2(d-c-1)}(i_c-i_d)ABCDEFG\\&=-\Delta(i_1,\ \cdots,\ i_n)。\end{aligned}$$

现在对于$\tau\in S_n$，假设$\tau=\tau_1\cdots\tau_r=\sigma_1\cdots\sigma_s$，其中$\tau_i$，$\sigma_j$均为对换，$r$为偶数而$s$为奇数。那末对于$(i_1,\ \cdots,\ i_n)=(1,\ 2,\ \cdots,n)$，由上一段便知$\Delta(\tau(1),\ \cdots,\ \tau(n))=\Delta(\tau_1\cdots\tau_r(1),\ \cdots,\ \tau_1\cdots\tau_r(n))=-\Delta(\tau_2\cdots\tau_r(1),\ \cdots,\ \tau_2\cdots\tau_r(n))=\cdots=(-1)^r\Delta(1,\ 2,\ \cdots,\ n)=\Delta(1,\ 2,\ \cdots,\ n)$。类似地，$\Delta(s(1),\ \cdots,\ s(n))=(-1)^s\Delta(1,\ 2,\ \cdots,\ n)=-\Delta(1,\ 2,\ \cdots,\ n)$，从而$\Delta(1,\ 2,\ \cdots,\ n)=-\Delta(1,\ 2,\ \cdots,\ n)$。由于$\Delta(1,\ 2,\ \cdots,\ n)\neq0$，这就导致矛盾。∎

定理6.8 对于每个$n\geqslant2$，以A_n表示S_n中全体偶置换所构成的集合。则A_n是S_n的指数为2的正规子群，并且A_n的阶为$|S_n|/2=n!/2$。进而，A_n是S_n的唯一的指数为2的子群。

群A_n叫作n个字母的交错群或者n次交错群。

证明概要 以C表示整数的乘法子群$\{1,\ -1\}$。定义映射f：$S_n\to C$，$\sigma\longmapsto\mathrm{sgn}\sigma$。验证$f$是群的满同态。因为$f$的核显然是$A_n$，从而$A_n$在$S_n$中正规。根据第一同构定理$S_n/A_n\cong C$，从而$[S_n:A_n]=2$，而$|A_n|=|S_n|/2$。由习题6可知$A_n$是$S_n$唯一的指数为2的子群。∎

定义6.9 如果群G没有真正规子群，便称G为单群。

Abel单群只有Z_p，其中p为素数（习题4.3）。另一方面，存在着许多非Abel单群。例如

定理6.10 交错群A_n是单群$\Leftrightarrow n\neq 4$。

我们要给出的证明是非常初等的.这首先需要两个引理.注意如果τ是2－轮换,则$\tau^2=(1)$,从而$\tau=\tau^{-1}$(证明见引理6.12后面)。

引理6.11 假设r, s是$\{1, 2, \cdots, n\}$中不同的元素, 则A_n $(n\geqslant 3)$由3－轮换集合$\{(rsk)\mid 1\leqslant k\leqslant n, k\neq r, s\}$生成。

证明 假设$n>3$ ($n=3$的情形显然成立)。 A_n的每个元素均是形如$(ab)(cd)$或 $(ab)(ac)$ 的一些项之积。其中a, b, c, d是$\{1, 2, \cdots, n\}$中不同的元素。 由于$(ab)(cd)=(acb)(acd)$, $(ab)(ac)=(acb)$, 因此A_n是由全体3－轮换所生成的。 每个3－轮换均有形式 (rsa),(ras),(sab) 或者(abc),其中 a,b,c 是不同的元素,并且$a,b,c\neq r,s$。由于 $(ras)=(rsa)^2$, $(rab)=(rsb)(rsa)^2$, $(sab)=(rsb)^2(rsa)$, 和 $(abc)=(rsa)^2(rsc)(rsb)^2(rsa)$, 从而$A_n$是由

$$\{(rsk)\mid 1\leqslant k\leqslant n, k\neq r, s\}$$

生成的。 ∎

引理6.12 如果N是$A_n(n\geqslant 3)$的正规子群, 并且N包含一个3－轮换, 则$N=A_n$。

证明 如果$(rsc)\in N$, 则对每个$k\neq r$, s, c, $(rsk)=(rs)\cdot(ck)(rsc)^2(ck)(rs)=[(rs)(ck)](rsc)^2[(rs)(ck)]^{-1}\in N$。 从而由引理6.11可知$N=A_n$。 ∎

定理6.10的证明 $A_2=(1)$, A_3是3阶循环子群。 此外, 易知$\{(1), (12)(34), (13)(24), (14)(23)\}$是$A_4$的正规子群 (习

题7)。如果$n\geqslant 5$，而N是A_n的非平凡的正规子群，我们将证明$N=A_n$。为此要考虑所有可能的情形。

情形1：N包含有3－轮换，由引理6.12知$N=A_n$。

情形2：N包含一个元素σ，σ是非交轮换之积，并且至少有一个轮换的长度$r\geqslant 4$。这时$\sigma=(a_1a_2\cdots a_r)\tau$(非交)。令$\delta=(a_1a_2a_3)\in A_n$，则由正规性有$\sigma^{-1}(\delta\sigma\delta^{-1})\in N$。但是

$$\sigma^{-1}(\delta\sigma\delta^{-1})=\tau^{-1}(a_1a_ra_{r-1}\cdots a_2)(a_1a_2a_3)(a_1a_2\cdots a_r)\tau(a_1a_3a_2)$$
$$=(a_1a_3a_r)\in N。$$

从而由引理6.12可知$N=A_n$。

情形3：N包含一个元素σ，σ是非交轮换之积，并且至少有两个轮换的长度是3，从而$\sigma=(a_1a_2a_3)(a_4a_5a_6)\tau$(非交)。令$\delta=(a_1a_2a_4)\in A_n$。象上面一样，$N$包含$\sigma^{-1}(\delta\sigma\delta^{-1})=\tau^{-1}(a_4a_6a_5)(a_1a_3a_2)(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)\tau(a_1a_4a_2)=(a_1a_4a_2a_6a_3)$。由情形2可知$N=A_n$。

情形4：N包含元素σ，σ是一个3－轮换与一些2-轮换之积，即$\sigma=(a_1a_2a_3)\tau$(非交)，其中τ是非交的2-轮换之积。则$\sigma^2\in N$，而$\sigma^2=(a_1a_2a_3)\tau(a_1a_2a_3)\tau=(a_1a_2a_3)^2\tau^2=(a_1a_2a_3)^2=(a_1a_3a_2)$，于是由引理6.12有$N=A_n$。

情形5：N中每个元素都是（偶数个）非交2-轮换之积。令$\sigma\in N$，$\sigma=(a_1a_2)(a_3a_4)\tau$(非交)。由于$\delta=(a_1a_2a_3)\in A_n$，象上面一样，$\sigma^{-1}(\delta\sigma\delta^{-1})\in N$。现在$\sigma^{-1}(\delta\sigma\delta^{-1})=\tau^{-1}(a_3a_4)(a_1a_2)(a_1a_2a_3)(a_1a_2)(a_3a_4)\tau(a_1a_3a_2)=(a_1a_3)(a_2a_4)$。由于$n\geqslant 5$，有元素$b\in\{1,2,\cdots,n\}$不同于$a_1$，$a_2$，$a_3$，$a_4$。因为$\xi=(a_1a_3b)\in A_n$，$\zeta=(a_1a_3)(a_2a_4)\in N$，从而$\zeta(\xi\zeta\xi^{-1})\in N$。但是$\zeta(\xi\zeta\xi^{-1})=(a_1a_3)(a_2a_4)(a_1a_3b)(a_1a_3)(a_2a_4)(a_1ba_3)=(a_1a_3b)\in N$。由引理6.12即知$N=A_n$。

因为上面诸情形穷尽了全部可能性，因此A_n没有真正规子群，即A_n是单群. ∎

$S_n(n\geqslant 3)$的另一个重要的子群是由$a=(123\cdots n)$和$b=\begin{pmatrix}1&2&\cdots&n\\1&n&\cdots&2\end{pmatrix}$

$\begin{pmatrix}1&\cdots&i&\cdots&n\\1&\cdots&n+2-i&\cdots&n\end{pmatrix}=\prod_{2\leqslant i<n+2-i}(i\ n+2-i)$生成的子群$D_n$. 它叫作正$n$边形群. 因为它同构于（从而等同于）正$n$边形的全体对称所构成的群(习题13). 特别地，$D_4$是（同构于）正方形对称群. (见第39页).

定理6.13 对于每个$n\geqslant 3$，正多边形群D_n是$2n$阶群，并且生成元a和b满足：

(i) $a^n=(1)$，$b^2=(1)$，$a^k\neq(1)$ $(0<k<n)$.

(ii) $ba=a^{-1}b$.

反之，任意群G如果由满足(i)和(ii)（对于某个$n\geqslant 3$）的元素a，$b\in G$所生成（其中用$e\in G$代替(1)），则G必同构于D_n.

证明概要 验证上面定义的a，$b\in D_n$满足(i)和(ii). 从而$D_n=\langle a,\ b\rangle=\{a^ib^j\mid 0\leqslant i<n,\ j=0,\ 1\}$（见定理2.8）. 然后验证$2n$个元素$a^ib^j$ $(0\leqslant i<n,\ j=0,\ 1)$是两两不同的（这只要检查它们在1和2上的作用即可），从而$|D_n|=2n$.

假设G是由a，$b\in G$生成的群并且a和b满足(i)和(ii)(对于某个$n\geqslant 3$). 根据定理2.8，G中每个元素都可以表示成有限乘积$a^{m_1}b^{m_1}a^{m_2}b^{m_2}\cdots b^{m_k}$($m_i\in\mathbb{Z}$). 重复使用(i)和(ii)，可知任何一个这样的乘积均可以写成形式a^ib^j，其中$0\leqslant i<n$，$j=0$，1（特别注意$b^2=e$和(ii)式导致$b=b^{-1}$和$ab=ba^{-1}$）. 为了避免混淆起见，我们以a_1，b_1表示D_n的生成元. 验证映射$f:D_n\to G$，$a_1^ib_1^j\longmapsto a^ib^j$是群的满同态. 为完成证明，只需再证$f$是单同态即可. 假设

$f(a_1^i b_1^j) = a^i b^j = e \in G$，其中$0 \leqslant i < n$，$j = 0$，1。如果$j = 1$，则$a^i = b$。而由(ii)式，$a^{i+1} = a^i a = ba = a^{-1}b = a^{-1}a^i = a^{i-1}$，这导致$a^2 = e$。由于$n \geqslant 3$，这与(i)式相矛盾。因此$j = 0$，从而$e = a^i b^0 = a^i$，$0 \leqslant i < n$，从(i)式得出$i = 0$。因此$f(a_1^i b_1^j) = e$导致$a_1^i b_1^j = a_1^0 b_1^0 = (1)$。从而由定理2.3便知$f$是单同态。∎

这个定理是用“生成元与关系”来刻划群的一个例子。这种思想将在第9节中加以详细的讨论。

习　题

1. 找出S_4中4个同构于S_3的不同的子群和9个同构于S_2的不同的子群。
2. (a) 证明S_n是由$n-1$个对换(12)，(13)，(14)，…，(1n)生成的[提示：$(1i)(1j)(1i) = (ij)$]。

   (b) S_n是由$n-1$个对换(12)，(23)，(34)，…，$(n-1\ \ n)$生成的。[提示：$(1j) = (1j-1)(j-1j)(1j-1)$，然后利用(a)。]
3. 如果$\sigma = (i_1 i_2 \cdots i_r) \in S_n$而$\tau \in S_n$，则$\tau\sigma\tau^{-1}$是$r$-轮换$(\tau(i_1)\tau(i_2)\cdots\tau(i_r))$。
4. (a) S_n是由$\sigma_1 = (12)$和$\tau = (123\cdots n)$生成的[提示：将习题3用于σ_1，$\sigma_2 = \tau\sigma_1\tau^{-1}$，$\sigma_3 = \tau\sigma_2\tau^{-1}$，…，$\sigma_{n-1} = \tau\sigma_{n-2}\tau^{-1}$，然后利用习题2(b)。]。(b) S_n是由(12)和$(23\cdots n)$生成的。
5. 如果σ，$\tau \in S_n$，而σ为偶置换（或者奇置换），那末$\tau\sigma\tau^{-1}$也同样为偶置换（或者奇置换）。
6. A_n是S_n中唯一的指数为2的子群。[提示：证明指数为2的子群必然包含S_n中全部3-轮换，然后利用引理6.11.]。
7. 证明$N = \{(1), (12)(34), (13)(24), (14)(23)\}$是$S_4$的正规子群，$N \subset A_4$，并且$S_4/N \cong S_3$，$A_4/N \cong Z_3$。
8. 群A_4没有6阶子群。
9. 对于$n \geqslant 3$，令G_n为由$x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$和$y = \begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{2\pi i/n} \end{pmatrix}$生成的复矩阵

乘法群，其中$i^2=-1$.证明$G_n\cong D_n$[提示：注意$e^{2\pi i}=1$，并且当实数k不为整数时，$e^{k2\pi i}\neq 1$].

10. 令a是D_n的n阶生成元.证明$\langle a\rangle \lhd D_n$，并且$D_n/\langle a\rangle \cong Z_2$.

11. 找出D_n的全部正规子群.

12 当n为奇数时，群D_n的中心（习题2.11）是$\langle e\rangle$.而当n为偶数时，群D_n的中心同构于Z_2.

13. 对于每个$n\geqslant 3$，以P_n表示正n边形（对于$n=3$，P_n即是正三角形，对于$n=4$则为正方形).P_n的对称是指一个一一对应$P_n\to P_n$，它使矩离不变，并且将相邻顶点映成相邻顶点.

(a) P_n之全体对称所构成的集合D_n^*以函数合成为二元运算形成群.

(b) 每个$f\in D_n^*$由它在P_n之诸顶点上的作用所完全决定. 将顶点依次标记为1，2，…，n，则每个$f\in D_n^*$决定出唯一的$\{1, 2, \cdots, n\}$上置换σ_f. 映射$f\longmapsto\sigma_f$决定出一个群的单同态$\varphi: D_n^*\to S_n$.

(c) D_n^*由f和g生成，其中f是P_n绕中心旋转$2\pi/n$弧度，而g是对于过中心和顶点1的“直径”所作的反射.

(d) $\sigma_f=(123\cdots n)$，$\sigma_g=\begin{pmatrix}1 & 2 & 3 & \cdots & n-1 & n\\ 1 & n & n-1 & \cdots & 3 & 2\end{pmatrix}$，于是$Im\varphi=D_n$，从而$D_n^*\cong D_n$.

7. 范畴：积，余积和自由对象

现在我们手头已经有了一些例子，所以是介绍范畴概念的时候了. 范畴是一种有益的语言，它处理许多不同的数学对象，提供了一种一般性的叙述方式. 我们在第X章中还要对它作更详细的研究.

范畴定义所倚靠的直觉思想是：我们已经介绍过的(如集合，

群与幺半群）和即将介绍的（如环和模）许多数学对象，连同这些对象之间的适当的映射（如集合之间的函数，群的同态等等），有一系列形式化的性质是公共的。例如，在每种情形下，映射的合成（如果这些合成可以定义的话）满足结合律，每个对象A均有某种恒等映射1_A：$A\to A$。这些概念可以形式化成：

定义7.1 一个范畴是由一些对象（表示成A，B，C，…）形成的类$\mathscr{C}$加上

(i) 一个由一些非交集合构成的类

$$\{\hom(A,\ B)|\ A,\ B\in\mathscr{C}\}$$

（$\hom(A,\ B)$中的元素f叫作从A到B的态射(morphism)，表示成$f:A\to B$）；

(ii) 对于$\mathscr{C}$中每个3-对象组$(A,\ B,\ C)$，均存在一个函数

$$\hom(B,\ C)\times\hom(A,\ B)\to\hom(A,\ C).$$

（对于态射$f:A\to B$，$g:B\to C$，这个函数写为$(g,\ f)\longmapsto g\circ f$，把$g\circ f:A\to C$叫作$f$和$g$的合成），并且满足以下两条公理：

(I) 结合律：如果$f:A\to B$，$g:B\to C$，$h:C\to D$是$\mathscr{C}$中的态射，则$h\circ(g\circ f)=(h\circ g)\circ f$。

(II) 恒等性：对于$\mathscr{C}$中每个对象B，均存在态射$1_B:B\to B$，使得对于每个$f:A\to B$和$g:B\to C$，

$$1_B\circ f=f,\ \ g\circ 1_B=g.$$

在范畴$\mathscr{C}$中，态射$f:A\to B$叫作一个等价，是指在$\mathscr{C}$中存在一个态射$g:B\to A$，使得$g\circ f=1_A$同时$f\circ g=1_B$。两个等价的合成（如果这个合成可以定义的话）也是一个等价。如果$f:A\to B$是等价，我们也称A和B是等价的。

例 设$\mathscr{S}$为全部集合所构成的类。对于A，$B\in\mathscr{S}$，hom

(A, B)是所有函数$f: A \to B$构成的集合。不难看出$\mathscr{S}$是一个范畴。由引论第3节中的(13)式可知，$\mathscr{S}$的态射f是等价的充要条件为它是一一对应。

例 设$\mathscr{S}$是以所有群为对象的范畴，而$\hom(A, B)$是所有群同态$f: A \to B$构成的集合。从定理2.3可知，态射是等价$\Longleftrightarrow$它是同构。类似可定义Abel群范畴$\mathscr{A}$。

例 一个（乘法）群G可以看成是只有一个对象的范畴。令$\hom(G, G)$为G中元素构成的集合，而态射a和b的合成简单地定义为群G中的乘法。这时，每个态射f都是等价（因为G中每个元素均有逆），而1_G是G中幺元素e。

例 对象集合由所有半序集合$(S, \leqslant)$构成。态射$(S, \leqslant) \to (T, \leqslant)$是函数$f: S \to T$，使得对$x, y \in S$，$x \leqslant y \Longrightarrow f(x) \leqslant f(y)$。

例 假设$\mathscr{C}$为任一范畴，如下定义范畴$\mathscr{D}$。它的对象集合由$\mathscr{C}$的全部态射所构成。如果$f: A \to B$和$g: C \to D$是$\mathscr{C}$的态射，则$\hom(f, g)$是

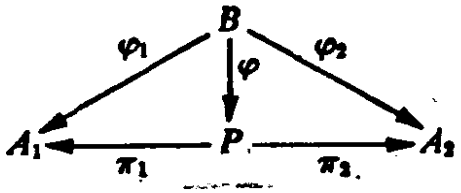
$\{(\alpha, \beta) \mid \alpha: A \to C, \beta: B \to D$为态射，并且使下面的图表交换$\}$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ C & \xrightarrow{g} & D \end{array}$$

定义7.2 假设$\mathscr{C}$是一个范畴，$\{A_i \mid i \in I\}$是$\mathscr{C}$的对象族。族$\{A_i \mid i \in I\}$的积是$\mathscr{C}$中一个对象P加上一族态射$\{\pi_i: P \to A_i \mid i \in I\}$，使得对每个对象$B$和每个态射族$\{\varphi: B \to A_i \mid i \in I\}$，均存在唯一的态射$\varphi: B \to P$，使得$\pi_i \circ \varphi = \varphi_i (\forall i \in I)$。

$\{A_i \mid i \in I\}$的积P通常表示成$\prod\limits_{i \in I} A_i$。有时，特别是$I = \{1, 2\}$的时候，用交换图表来刻划一个积是有好处的。$\{A_1, A_2\}$的积

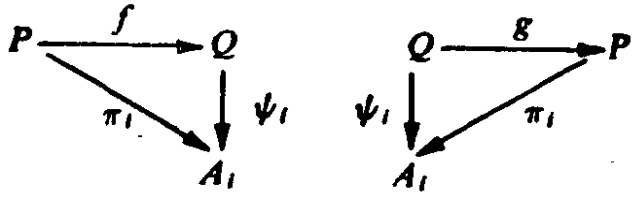
是一个（由对象和态射组成的）图表$A_1 \xleftarrow{\pi_1} P \xrightarrow{\pi_2} A_2$，使得对于形如$A_1 \xleftarrow{\varphi_1} B \xrightarrow{\varphi_2} A_2$的每个图表，均存在唯一的态射$\varphi: B \to P$，使得下面的图表是交换的：



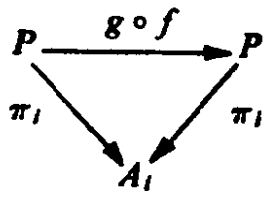
一个范畴中的一个对象族不一定有积。但是在我们比较熟悉的一些范畴中，积是存在的。例如在集合范畴中，利用引论中的定理5.2不难证明，Cartesian积$\prod_{i \in I} A_i$即是族$\{A_i \mid i \in I\}$的积。下一节我们要证明，在群范畴中积是存在的。

定理7.3 如果$(P, \{\pi_i\})$和$(Q, \{\psi_i\})$均是范畴$\mathscr{C}$中对象族$\{A_i \mid i \in I\}$的积，则P和Q等价。

证明 因为P和Q均是积，从而存在态射$f: P \to Q$和$g: Q \to P$，使得对每个$i \in I$，下面两个图表都是交换的



将两者合在一起，便对每个$i \in I$都给出交换图表：



因此$g \circ f: P \to P$是一个态射，使得对每个$i \in I$，均有$\pi_i \circ (g \circ f) = \pi_i$。但是根据积的定义，可知只有唯一的态射有此性质。由于映射

$1_P: P \to P$也具有此性质，从而由唯一性必然有$g \circ f = 1_P$。类似地，利用Q为积这一事实，可以证明$f \circ g = 1_Q$。于是$f: P \to Q$是等价。∎

由于抽象的范畴只涉及对象和态射（不涉及元素），从而对于它们的每个命题，将所有箭头（态射）反向，就得到一个对偶命题。例如定义7.2的对偶就是：

定义7.4 范畴$\mathscr{C}$中对象族$\{A_i \mid i \in I\}$的余积（或者叫作和）是$\mathscr{C}$中一个对象S和一个态射族$\{\iota_i: A_i \to S \mid i \in I\}$，使得对于每个对象$B$和每个态射族$\{\psi_i: A_i \to B \mid i \in I\}$，均存在唯一的态射$\psi: S \to B$，使得$\psi \circ \iota_i = \psi_i$（对于所有$i \in I$）。

对于余积没有统一的符号，虽然有时也使用$\coprod_{i \in I} A_i$。下面两节我们将讨论群范畴$\mathscr{G}$和Abel群范畴$\mathscr{A}$中的余积。将定理7.3的证明经过“对偶”，就可证明下一定理（你可以作这件事）。

定理7.5 如果$(S, \{\iota_i\})$和$(S', \{\lambda_i\})$是范畴$\mathscr{C}$中对象族$\{A_i \mid i \in I\}$的两个余积，则S和S'等价。∎

在上面提到的某些范畴（如群范畴）中，每个对象事实上都是集合（通常还有某些附加的结构），而每个态射$f: A \to B$都是其“凭借（underlying）集合”上的函数（通常还同时具有某些其他性质）。我们将这种思想形式化为：

定义7.6 一个具体范畴是指一个范畴$\mathscr{C}$加上一个函数σ，σ将$\mathscr{C}$的每个对象A映成一个集合$\sigma(A)$（叫作A的凭借集合），并且

(i) $\mathscr{C}$的每个态射$A \to B$都是其凭借集合上的函数$\sigma(A) \to \sigma(B)$；

(ii) $\mathscr{C}$中每个对象A的恒等态射都是其凭借集合 $\sigma(A)$ 上的恒等函数；

(iii) $\mathscr{C}$ 中态射的合成与其凭借集合上函数的合成是一致的。

例 群范畴是具体范畴，其中函数σ是将每个群映到它的通常意义下的凭借集合。类似地，Abel群范畴和半序集合范畴对于其显然的凭借集合均是具体范畴。另一方面，对于定义7.1后面的第三个例子，如果函数σ是将群G映成通常的凭借集合G，则这个范畴不是具体范畴（因为态射不是集合G上的函数）。

具体范畴是很有用的，因为我们不仅可以利用它的范畴性质，还可以利用集合，子集合等性质。在实际上，我们感兴趣的所有具体范畴中，函数 σ 均是将对象映到它通常意义下的凭借集合（如上面诸例所示），所以我们将采用同样的符号表示对象和它的凭借集合，即将函数 σ 略去不写。在少数情形下这会造成混淆，因为在具体范畴中，我们要将$\mathscr{C}$ 的态射（根据定义，它也是凭借集合上的函数）和映射（它是凭借集合上的函数，但不必为 $\mathscr{C}$ 的态射）仔细地区分开来。

定义7.7 假设F是范畴$\mathscr{C}$中的一个对象，X 为非空集合，$i: X \to F$是（集合之间的）映射。我们将F叫作在集合X上是自由的，是指对于$\mathscr{C}$ 的每个对象A和（集合之间的）映射 $f: X \to A$，均存在$\mathscr{C}$ 中唯一的态射 $\bar{f}: F \to A$，使得 $\bar{f} i = f$（作为集合之间的映射 $X \to A$）。

一个自由对象 F 的最本质事情是：为了定义以F为定义域的一个态射只需指明子集合$i(X)$ 的象即可。如下例所示。

例 假设G为群，$g \in G$。不难看出，由 $\bar{f}(n) = g^n$ 定义的映射 $\bar{f}: \mathbb{Z} \to G$，是满足 $1 \longmapsto g$ 的唯一的群同态 $\mathbb{Z} \to G$。因此若$X =$

{1}而$i:X\to\mathbb{Z}$是包含映射，则在群范畴中，$\mathbb{Z}$在X上是自由的(给定$f:X\to G$，令$g=f(1)$，然后如上法定义$\bar{f}$)。换句话说，为了决定从$\mathbb{Z}$到G的唯一的同态，我们只需指明$1\in\mathbb{Z}$的象（即$i(X)$的象）即可。有理数（加法）群$\mathbb{Q}$不具有这个性质。因为不难证明，非平凡的同态$\mathbb{Q}\to S_3$是不存在的。因此对于任意集合X，函数$i:X\to\mathbb{Q}$和函数$f:X\to S_3$如果$f(x_1)\neq(1)$(对某个$x_1\in X$)，则不存在同态$\bar{f}:\mathbb{Q}\to S_3$，使得$\bar{f}i=f$。

定理7.8 如果$\mathscr{C}$是具体范畴，F和F'是$\mathscr{C}$中的对象，F在集合X上是自由的，F'在集合X'上是自由的，并且$|X|=|X'|$，则F与F'等价。

注：如果F和F'在同一集合X上是自由的，则满足定理中的假设条件。

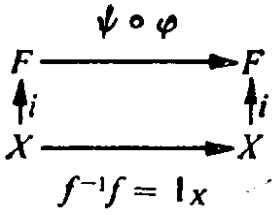
证明 因为F和F'是自由的，并且$|F|=|F'|$，从而有一一对应$f:X\to X'$和映射$i:X\to F$，$j:X'\to F'$。考虑映射$jf:X\to F'$。因为F是自由的，存在态射$\varphi:F\to F'$，使得图表

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & F' \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ X & \xrightarrow[f]{} & X' \end{array}$$

是交换的。类似的，由于一一对应f有逆$f^{-1}:X'\to X$，而F'是自由的，从而存在$\psi:F'\to F$，使得图表

$$\begin{array}{ccc} F' & \xrightarrow{\psi} & F \\ {\scriptstyle j}\uparrow & & \uparrow{\scriptstyle i} \\ X' & \xrightarrow[f^{-1}]{} & X \end{array}$$

是交换的。将二者组合在一起，便给出交换图表：



于是 $(\psi\circ\varphi)i = i1_X = i$. 但是 $1_F i = i$. 从而根据自由对象的唯一性，我们得出 $\psi\circ\varphi = 1_F$. 类似的推导给出 $\varphi\circ\psi = 1_{F'}$. 从而 F 和 F' 等价. ■

积、余积和自由对象都是用所谓泛映射性质（即利用某种唯一决定的态射的存在性）来定义的. 我们还已经看出，一个给定对象族的任意两个积（或者余积）事实上是等价的（定理7.3和定理 7.5）. 同样地，同一集合上的任意两个自由对象是等 价 的（定理7.8）. 而且，在定理7.3和7.8的证明中存在着明显的相似之处. 从而毫不奇怪地，上面提到的这些术语事实上均是一个简单概念的某些特殊情形.

定义7.9 范畴$\mathscr{C}$中的对象I叫作泛的（或叫初始的），是指对于$\mathscr{C}$的每个对象C，均存在唯一的态射$I\to C$. $\mathscr{C}$之对象T叫作余泛的（或叫终结的），是指对于$\mathscr{C}$的每个对象C，均存在唯一的态射$C\to T$.

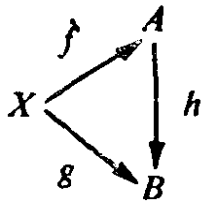
下面我们要证明，可以将积、余积和自由对象考虑成某个适当 选择的范畴中的 泛（或者余泛）对象. 但是这种刻划方式今后是不需要的，因为除了第III.4节，第III.5节，第 IV.5 节以及少数习题之外，我们不再提泛对象这件事. 如果读者愿意的话，他可以暂时略去下面的内容.

定理7.10 范畴$\mathscr{C}$ 中任意两个泛（或者余泛）对象均是等价的.

证明 假设I和J是$\mathscr{C}$中两个泛对象。由于I是泛对象，从而有唯一的态射$f:I\to J$。类似地，由于J是泛对象，也有唯一的态射$g:J\to I$。合成$g\circ f:I\to I$是$\mathscr{C}$的态射。但是$1_I:I\to I$也是$\mathscr{C}$的态射，而由I的泛性，可知只有唯一的态射$I\to I$，因此$g\circ f=1_I$。类似地，由J的泛性导致$f\circ g=1_J$。从而$f:I\to J$是等价。类似可证余泛对象的情形。 ∎

例 在群范畴$\mathscr{C}$中，一元群$\langle e\rangle$既是泛对象，也是余泛对象。

例 假设F为具体范畴$\mathscr{C}$中集合X上一个自由对象（对于$i:X\to F$）。如下定义一个新的范畴$\mathscr{D}$：$\mathscr{D}$的对象集合是{集合映射$f:X\to A$ |A为$\mathscr{C}$中对象（的凭借集合）}。$\mathscr{D}$中从$f:X\to A$到$g:X\to B$的态射定义为$\mathscr{C}$的态射$h:A\to B$并且使下面图表是交换的（即$h\circ f=g$）：



不难证明，$1_A:A\to A$是$\mathscr{D}$中从f到f的恒等态射。并且h为$\mathscr{D}$中的等价$\Longleftrightarrow h$是$\mathscr{C}$中的等价。由于F在集合X上是自由的，从而对于每个映射$f:X\to A$，均有唯一的态射$\bar{f}:F\to A$，使得$\bar{f}i=f$。这恰好等于说，$i:X\to F$是范畴$\mathscr{D}$中的泛对象。

例 假设$\{A_i\mid i\in I\}$是范畴$\mathscr{C}$中的对象族，如下定义一个范畴$\mathscr{E}$，它的对象集合是

$$\left\{(B,\{f_i\mid i\in I\})\ \middle|\ \begin{array}{l}B\text{为}\mathscr{C}\text{中的对象，对于每个}\\ i\in I,\ f_i:B\to A_i\text{是}\mathscr{C}\text{中的态射。}\end{array}\right\}$$

而$\mathscr{E}$中从$(B,\{f_i\mid i\in I\})$到$(D,\{g_i\mid i\in I\})$的态射是$\mathscr{C}$中一个态射$h:B\to D$，使得对每个$i\in I$均有$g_i\circ h=f_i$。证明1_B是$\mathscr{E}$中从$(B,\{f_i\})$到$(B,\{f_i\})$的恒等态射，并且：h是$\mathscr{E}$中的等价$\Longleftrightarrow h$是

$\mathscr{C}$中的等价。如果在$\mathscr{C}$中对象族$\{A_i \mid i\in I\}$存在积（对于映射π_k：$\Pi A_i \to A_k$ $(\forall k\in I)$），则对于$\mathscr{C}$中每个$(B,\{f_i\})$均存在唯一的态射$f: B\to \Pi A_i$，使得对每个$i\in I$均有$\pi_i\circ f = f_i$。而这恰好相当于说：$(\Pi A_i, \{\pi_i \mid i\in I\})$是范畴$\mathscr{C}$中的余泛对象。类似地，$\mathscr{C}$中一个对象族的余积可以看成是某个适当构作出来的范畴中的泛对象。

由于一个范畴中对象族$\{A_i \mid i\in I\}$的积ΠA_i可以看成是某个适当范畴中的余泛对象，从定理7.10立刻知道，ΠA_i不计等价是唯一决定的。对于余积和自由对象也有类似的结果。

习　题

1. 标点（Pointed）集合指的是(S, x)，其中S是集合而$x\in S$。标点集合之间的态射$(S, x)\to(S', x')$是三元组(f, x, x')，其中$f: S\to S'$是函数并且$f(x) = x'$。求证标点集合全体形成一个范畴。
2. 如果$f: A\to B$是范畴$\mathscr{C}$中的等价，而$g: B\to A$是态射，使得$g\circ f = 1_A$，$f\circ g = 1_B$，求证g是唯一的。
3. 在群范畴$\mathscr{G}$中，求证群$G_1\times G_2$与同态π_1：$G_1\times G_2\to G_1$和π_2：$G_1\times G_2\to G_2$（如定义2.2之前的例子所示）是$\{G_1, G_2\}$之积。
4. 在Abel群范畴$\mathscr{A}$中，求证群$A_1\times A_2$与同态$l_1: A_1\times A_2\longrightarrow A_1$和$l_2: A_1\times A_2\to A_2$（如定义2.2之前的例子所示）是$\{A_1, A_2\}$之积。
5. 集合范畴中每个集族$\{A_i \mid i\in I\}$均可定义余积。〔提示：考虑$\dot{\bigcup} A_i = \{(a, i)\in(\bigcup A_i)\times I \mid a\in A_i\}$及映射$A_i\to \dot{\bigcup} A_i$，$a\longmapsto(a, i)$。称$\dot{\bigcup} A_i$为集合$A_i$之非交并集。〕
6. (a) 求证（习题1中的）标点集合范畴$\mathscr{S}_*$中永远存在标点集合族的积，并刻划它。(b) 求证在范畴$\mathscr{S}_*$中，每个对象族均有余积（通常称作“楔积”（Wedge product））。刻划这个楔积。

7. 假设F为具体范畴$\mathscr{C}$中集合X上的自由对象(对于$i: X \to F$)。如果$\mathscr{C}$中包含某个对象，并且它的凭借集合至少包含两个元素，则i是集合上的单射。

8. 假设X为集合，F为群范畴中X上的自由对象（对于$i: X \to F$）（第9节中要证明F的存在性)。求证$i(X)$是群F的生成元集合〔提示：如果G是由$i(X)$生成的F之子群，则存在同态$\varphi: F \to G$，使得$\varphi i = i$。求证$F \xrightarrow{\varphi} G \xrightarrow{\subset} F$是恒等映射.〕。

8. 直积与直和

我们在本节中研究群范畴中的积和Abel群范畴中的余积。这些积和余积其所以重要，不仅因为可以用它们从已知群构作新群，而且还可以用特别的子群（这些子群的结构可能是已经知道的）来描述某些群的结构。

我们开始先把群G和H的直积$G \times H$的定义(见第40页）推广到任意（可能无限）群族$\{G_i \mid i \in I\}$上。如下定义（集合）Cartesian积$\prod_{i \in I} G_i$上的二元运算：如果$f, g \in \prod_{i \in I} G_i$（即$f, g: I \to \bigcup_{i \in I} G_i$，并且对每个$i \in I$，$f(i), g(i) \in G_i$)。则$fg: I \to \bigcup_{i \in I} G_i$是由$i \longmapsto f(i)g(i)$所给出的函数。由于每个$G_i$均是群，$f(i)g(i) \in G_i$（对每个$i$)，从而由引论中的定义5.1可知$fg \in \prod_{i \in I} G_i$.如果我们象在$I$有限时所做的那样，将$f \in \prod_{i \in I} G_i$等同于它的象（$a_i = f(i)$，对每个$i \in I$)，则$\prod_{i \in I} G_i$中的二元运算即是我们所熟悉的按分量相乘：

$\{a_i\}\{b_i\}=\{a_ib_i\}$。具有这种二元运算的$\prod_{i\in I}G_i$叫作群族$\{G_i\mid i\in I\}$的直积（或者叫完全直和）。如果$I=\{1,2,\cdots,n\}$，则$\prod_{i\in I}G_i$通常表示成$G_1\times G_2\times\cdots\times G_n$（或者用加法记号：$G_1\oplus G_2\oplus\cdots\oplus G_n$）。

定理8.1 如果$\{G_i\mid i\in I\}$是群族，则

(i) 直积$\prod_{i\in I}G_i$是群；

(ii) 对于每个$k\in I$，映射$\pi_k:\prod_{i\in I}G_i\to G_k$，$f\longmapsto f(k)$［或者$\{a_i\}\longmapsto a_k$］是群的满同态。

证明作为练习。 ∎

定理8.1中的映射π_k叫作该直积的正则射影。

定理8.2 令$\{G_i\mid i\in I\}$是群族而$\{\varphi_i:H\to G_i\mid i\in I\}$是群同态族，则存在唯一的同态$\varphi:H\to\prod_{i\in I}G_i$，使得对所有$i\in I$，$\pi_i\varphi=\varphi_i$。并且这个性质不计同构唯一决定了$\prod_{i\in I}G_i$。换句话说，$\prod_{i\in I}G_i$是群范畴中的积。

证明 根据引论中的定理5.2，集合映射$\varphi:H\to\prod_{i\in I}G_i$，$\varphi(a)=\{\varphi_i(a)\}_{i\in I}\in\prod_{i\in I}G_i$是满足$\pi_i\varphi=\varphi_i$（对所有$i\in I$）的唯一函数。容易验证$\varphi$是同态。从而$\prod_{i\in I}G_i$是（范畴意义下的）积，从而由定理7.3可知它决定到同构（等价）。 ∎

Abel群的直积显然仍是Abel群，从而Abel群的直积也是Abel

群范畴中的积。

定义8.3 群族 $\{G_i|i\in I\}$的（外）弱直积（表示成$\prod_{i\in I}{}^{W}G_i$）是集合

$$\{f\in\prod_{i\in I}G_i|\text{除了有限个以外对所有 }i\in I,$$

$$f(i)=e_i(G_i\text{ 中幺元素})\}$$

如果所有的群G_i均是（加法）Abei 群，则通常称$\prod_{i\in I}{}^{W}G_i$为（外）直和，并且表示成$\sum_{i\in I}G_i$。

如果I有限，则弱直积与直积一致。在一般情形下则有

定理8.4 如果$\{G_i|i\in I\}$是群族，则

(i) $\prod_{i\in I}{}^{W}G_i$ 是$\prod_{i\in I}G_i$的正规子群；

(ii) 对于每个$k\in I$，映射 $\iota_k:G_k\to\prod_{i\in I}{}^{W}G_i$，$\iota_k(a)=\{a_i\}_{i\in I}$，(其中$a_i=e$（对于$i\neq k$）而$a_k=a$）是群的单同态；

(iii) 对于每个$i\in I$，$l_i(G_i)$ 是$\prod_{i\in I}G_i$的正规子群。

证明作为练习。 ∎

定理8.4中的映射ι_k叫作正则嵌入。

定理8.5 假设$\{A_i|i\in I\}$是Abel群族（记成加法）。如果B是Abel群，而$\{\psi_i:A_i\to B|i\in I\}$是同态族，则有唯一的同态$\psi:\sum_{i\in I}A_i\to B$，使得对每个 $i\in I$均有$\psi\iota_i=\psi_i$，并且这一性质不计同构唯一

决定了$\sum_{i\in I}A_i$。换句话说，$\sum_{i\in I}A_i$是Abel群范畴中的余积。

注记：如果略去“Abel”一字，则定理不对，即外弱直积不是群范畴中的余积（习题4）。

定理8.5的证明 本证明中的群运算均记成加法。如果$0\neq\{a_i\}\in\sum A_i$，则只有有限多个a_i不为零，设它们为a_{i_1}，a_{i_2}，…，a_{i_r}。定义$\psi:\sum A_i\to B$，$\psi(0)=0$，$\psi(\{a_i\})=\psi_{i_1}(a_{i_1})+\psi_{i_2}(a_{i_2})+\cdots+\psi_{i_r}(a_{i_r})=\sum_{i\in I_0}\psi_i(a_i)$，其中$I_0$是集合$\{i_1,i_2,\cdots,i_r\}=\{i\in I|a_i\neq 0\}$。由于$B$是Abel群，可以证明$\psi$是同态并且对所有$i\in I$，$\psi l_i=\psi_i$。对于每个$\{a_i\}\in\sum A_i$，$\{a_i\}=\sum_{i\in I_0}l_i(a_i)$，$I_0$为上述的有限集合。如果$\xi:\sum A_i\to B$是同态，使得对所有$i$均有$\xi l_i=\psi_i$，则$\xi(\{a_i\})=\xi\left(\sum_{I_0}l_i(a)\right)=\sum_{I_0}\xi l_i(a_i)=\sum_{I_0}\psi_i(a_i)=\sum_{I_0}\psi l_i(a_i)=\psi\left(\sum_{I_0}l_i(a_i)\right)=\psi(\{a_i\})$，从而$\xi=\psi$，即$\psi$是唯一的。因此$\sum A_i$是Abel群范畴中的余积，从而由定理7.5可知它不计同构是唯一决定的。 ∎

下面我们研究在何种条件下群G同构于它的子群族的弱直积。

定理8.6 假设$\{N_i|i\in I\}$是群G的正规子群族，并且

(i) $G=\langle\bigcup_{i\in I}N_i\rangle$；

(ii) 对于每个$k\in I$，$N_k\cap\langle\bigcup_{i\neq k}N_i\rangle=\langle e\rangle$。则$G\cong\prod_{i\in I}{}^{w}N_i$。

在证明此定理之前，我们注意常常用到的一个特殊情形。将

定理5.3加以推广，便不难证明，如果$N_1, N_2, \cdots, N_r$是群 G 的正规子群，则$\langle N_1 \cup N_2 \cup \cdots \cup N_r \rangle = N_1 N_2 \cdots N_r = \{n_1 n_2 \cdots n_r \mid n_i \in N_i\}$。用加法记号，$N_1 N_2 \cdots N_r$写成$N_1 + N_2 + \cdots + N_r$. 读者记住下一系理可能是有益的，因为一般情况下的证明本质上是与之相同的。

系8.7 如果$N_1, N_2, \cdots, N_r$是群G的正规子群，$G = N_1 N_2 \cdots N_r$并且对每个$1 \leqslant k \leqslant r$，$N_k \cap (N_1 \cdots N_{k-1} N_{k+1} \cdots N_r) = \langle e \rangle$，则$G \cong N_1 \times N_2 \times \cdots N_r$。∎

定理8.6的证明 如果$\{a_i\} \in \prod^{W} N_i$，则除了有限个之外对于每个$i \in I$，$a_i = e$。以$I_0$表示有限集合$\{i \in I \mid a_i \neq e\}$。则$\prod_{i \in I_0} a_i$是 G 中的元素，因为对于 $a \in N_i$ 和 $b \in N_j (i \neq j)$，由定理5.3 (iv)$ab = ba$。从而映射$\varphi: \prod^{W} N_i \to G$, $\{a_i\} \longmapsto \prod_{i \in I_0} a_i \in G$（并且$\{e\} \to e\}$是同态，从而$\varphi l_i(a_i) = a_i$（对于$a_i \in N_i$）。

因为G是由诸子群N_i生成的，每个元素$a \in G$均是不同的N_i中元素的有限乘积。由于N_i和N_j（对于$i \neq j$）中元素是可交换的，a可以写成乘积$\prod_{i \in I_0} a_i$，其中$a_i \in N_i$，I_0是I的某个有限子集合。从而$\prod_{i \in I_0} l_i(a_i) \in \prod^{W} N_i, \varphi(\prod_{i \in I_0} l_i(a_i)) = \prod_{i \in I_0} \varphi l_i(a_i) = \prod_{i \in I_0} a_i = a$。因此$\varphi$是满同态。

假设$\varphi(\{a_i\}) = \prod_{i \in I_0} a_i = e \in G$。为方便起见，我们显然可以假定$I_0 = \{1, 2, \cdots, n\}$。于是$\prod_{i \in I_0} a_i = a_1 a_2 \cdots a_n = e$，$a_i \in N_i$。从而$a_1^{-1} = a_2 \cdots a_n \in N_1 \cap \langle \bigcup_{i=1} N_i \rangle = \langle e \rangle$，因此$a_1 = e$。重复这一推理即

可证对所有$i\in I$，$a_i=e$，从而φ是单同态。 ∎

定理8.6使我们给出

定义8.8 令$\{N_i\mid i\in I\}$是群G的正规子群族，$G=\langle\bigcup_{i\in I}N_i\rangle$，并且对于每个$k\in I$，$N_k\cap\langle\bigcup_{i\neq k}N_i\rangle=\langle e\rangle$。则$G$叫作$\{N_i\mid i\in I\}$的内弱直积（如果$G$是（加法）Abel群，则叫作内直和）。

作为定理8.6的一个容易的系理，我们可以对内弱直积作如下的刻划。

定理8.9 令$\{N_i\mid i\in I\}$是群G的正规子群族。则G是$\{N_i\mid i\in I\}$的内弱直积$\Longleftrightarrow$$G$的每个非幺元素均唯一写成乘积$a_{i_1}a_{i_2}\cdots a_{i_n}$，其中$i_1$，…，$i_n$是$I$中不同的元素，而对每个$1\leqslant k\leqslant n$，$e\neq a_{i_k}\in N_{i_k}$。

证明作为练习。 ∎

内弱直积和外弱直积之间有不同之处。如果群G是诸群N_i的内弱直积，根据定义，每个N_i实际上均是G的子群，并且G同构于外弱直积$\prod_{i\in I}{}^{W}N_i$。但是，外弱直积$\prod_{i\in I}{}^{W}N_i$实际上不包含群N_i，而只有一个子群（即$l_i(N_i)$，见定理8.4和习题10）和它同构。老实说，这一区别并不十分重要，如果不发生混淆的话，我们略去形容词“内”和“外”。事实上我们将使用如下的记号。

记号：我们以$G=\prod_{i\in I}{}^{W}N_i$表示群$G$是它的子群族$\{N_i\mid i\in I\}$的内弱直积。

定理8.10 令$\{f_i:G_i\to H_i\mid i\in I\}$是群的同态族，$f=\prod f_i$为

由 $\{a_i\}\longmapsto\{f_i(a_i)\}$ 给出的映射 $\prod_{i\in I}G_i\to\prod_{i\in I}H_i$。则 f 为群同态并且 $f(\prod_{i\in I}{}^{W}G_i)\subset\prod_{i\in I}{}^{W}H_i$, $Kerf=\prod_{i\in I}Kerf_i$ 而 $Imf=\prod_{i\in I}Imf_i$。从而：f 是单同态（满同态）$\Longleftrightarrow$ 每个 f_i 均是单同态（满同态）。

证明作为练习。 ∎

系8.11 假设 $\{G_i|i\in I\}$ 和 $\{N_i|i\in I\}$ 是群族，并且对于每个 $i\in I$，N_i 是 G_i 的正规子群，则

(i) $\prod_{i\in I}N_i$ 是 $\prod_{i\in I}G_i$ 的正规子群，并且 $\prod_{i\in I}G_i/\prod_{i\in I}N_i\cong\prod_{i\in I}G_i/N_i$。

(ii) $\prod_{i\in I}{}^{w}N_i$ 是 $\prod_{i\in I}{}^{w}G_i$ 的正规子群，并且 $\prod_{i\in I}{}^{w}G_i/\prod_{i\in I}{}^{w}N_i\cong\prod_{i\in I}{}^{w}G_i/N_i$。

证明 (i) 对于每个 i，令 π_i：$G_i\to G_i/N_i$ 为正则满同态。由定理8.10可知映射 $\prod\pi_i:\prod_{i\in I}G_i\to\prod_{i\in I}G_i/N_i$ 为满同态，其核为 $\prod_{i\in I}N_i$。因此由第一同构定理，$\prod G_i/\prod N_i\cong\prod G_i/N_i$。类似地可以证明(ii)。 ∎

习　题

1. S_3 不是它的任何真子群族的直积。Z_{p^n}（p 为素数，$n\geqslant 1$）和 $\mathbf{Z}$ 亦有此性质。
2. 给出群 H_i，K_j 的例子，使得 $H_1\times H_2\cong K_1\times K_2$，但是没有 H_i 同构于某个 K_j。

3. 假设G为(加法)Abel群，H和K是G的子群.求证$G\cong H\oplus K\Longleftrightarrow$存在同态$H\underset{l_1}{\overset{\pi_1}{\leftrightarrows}}G\underset{l_2}{\overset{\pi_2}{\rightleftarrows}}K$，使得$\pi_1 l_1=1_H$，$\pi_2 l_2=1_K$，$\pi_1 l_2=0$，$\pi_2 l_1=0$，其中0是将每个元素均映成零元素的映射，并且对每个$x\in G$，$l_1\pi_1(x)+l_2\pi_2(x)=x$。

4. 给出例子表明弱直积不是群范畴中的余积（提示：只需考虑两个因子$G\times H$的情形）。

5. 设G和H是有限循环群，则$G\times H$为循环群$\Longleftrightarrow(|G|,|H|)=1$。

6. 每个有限生成Abel群$G\neq\langle e\rangle$，如果它的每个元素（除了e之外）的阶数均为p（p为素数），则G必同构于n个Z_p的直和$Z_p\oplus Z_p\oplus\cdots\oplus Z_p$（对于某个$n\geqslant 1$）.〔提示：令$A=\{a_1,a_2,\cdots,a_n\}$是生成元集合，使得$A$的真子集合均不能生成$G$.证明$\langle a_i\rangle\cong Z_p$并且$G=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_n\rangle$.〕

7. 令H，K，N是群G的非平凡正规子群，并且假设$G=H\times K$。证明N或者在G的中心中，或者N与H和K中的一个非平凡地相交。给出例子表明，当G是非Abel群时，则上述两种情形实际上均可能发生。

8. 如果诸N_i中有一个不是正规子群，则系8.7不成立。

9. 如果群G是它的子群H和K的（内）直积，则$H\cong G/K$，$G/H\cong K$。

10. 如果$\{G_i|i\in I\}$是群族，则$\Pi^w G_i$是它的诸子群$\{l_i(G_i)|i\in I\}$的内弱直积。

11. 假设$\{N_i|i\in I\}$是群G的子群族，则G是$\{N_i|i\in I\}$的内弱直积$\Longleftrightarrow$

(i) 对于$i\neq j$和$a_i\in N_i$，$a_j\in N_j$，$a_ia_j=a_ja_i$；

(ii) G的每个非幺元素均可唯一地写成$a_{i_1}\cdots a_{i_n}$，其中i_1，…，i_n是I中的不同元素，并且对每个k，$e\neq a_{i_k}\in N_{i_k}$〔比较定理8.9.〕.

12. 群G的正规子群H叫作是直积因子（如果G是加法Abel群，则称作直和成分），是指G存在(正规)子群K，使得$G=H\times K$。(a)如果H是K的直积因子而K是G的直积因子，则H在G中正规〔比较习题5.10〕.(b)如果H是G的直积因子，则每个同态$H\to G$可以扩充成自同态$G\to G$.但是一个单同态不一定能扩充成自同构$G\to G$。

13. 设 $\{G_i \mid i\in I\}$ 是群族而$J\subset I$。则映射$\alpha: \prod_{j\in J} G_j \to \prod_{i\in I} G_i$, $\{a_j\} \mapsto \{b_j\}$（其中$b_j = a_j$，对于$j\in J$，$b_i = e_i$（G_i中幺元素），对于$i\notin J$）是群的单同态，并且 $\prod_{i\in I} G_i/\alpha(\prod_{j\in J} G_j) \cong \prod_{i\in I-J} G_i$。

14. 对于$i = 1, 2$，令$H_i \lhd G_i$。给出例子表明下面诸命题均可能不成立：

(a) $G_1\cong G_2$并且$H_1\cong H_2 \Rightarrow G_1/H_1\cong G_2/H_2$。

(b) $G_1\cong G_2$并且$G_1/H_1\cong G_2/H_2 \Rightarrow H_1\cong H_2$。

(c) $H_1\cong H_2$并且$G_1/H_1\cong G_2/H_2 \Rightarrow G_1\cong G_2$。

9. 自由群，自由积，生成元与关系

我们将要证明在群(具体) 范畴中存在着自由对象(自由群)，然后由此来发展用“生成元与关系”刻划群的方法。此外，我们还要指明在群范畴中如何构作余积（自由积)。

给了集合X，我们要构作一个群F，使得在定义7.7的意义下它在集合X上是自由的。如果$X = \phi$，F是平凡群$\langle e\rangle$。如果$X \neq \phi$，以X^{-1}表示与X非交的集合，并且$|X| = |X^{-1}|$。取一个一一对应$X \to X^{-1}$，并且以x^{-1}表示$x\in X$的象。最后再取一个与$X\cup X^{-1}$非交的一元集合$\{1\}$。X上的一个字是指一个序列$(a_1, a_2, \cdots)$，其中$a_i\in X\cup X^{-1}\cup\{1\}$，使得存在某个$n\in \boldsymbol{N}^*$，当$k\geqslant n$时，$a_k = 1$。常数序列 (1, 1, …) 叫作空字，并且表示成1(这种含混的记号今后不会引起混乱)。X上的字 $(a_1, a_2, \cdots)$ 叫作既约的，如果

(i) 对于每个$x\in X$，x和x^{-1}均不相邻（即对于所有$i\in \boldsymbol{N}^*$，$x\in X$，$a_i = x \Longrightarrow a_{i+1} \neq x^{-1}$，并且$a_i = x^{-1} \Longrightarrow a_{i+1} \neq x$)；

(ii) $a_k = 1 \Longrightarrow$ 对于每个$i\geqslant k$，$a_i = 1$。

特别地，空字1是既约的。

每个非空既约字均有形式$(x_1^{\lambda_1}, x_2^{\lambda_2}, \cdots, x_n^{\lambda_n}, 1, 1, \cdots)$，其中$n\in \mathbf{N}^*$，$x_i\in X$，$\lambda_i=\pm 1$（对于每个$x\in X$，约定$x^1$表示$x$）。此后我们将把此字记为$x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$。这个新的记号既紧凑又富有建议性。从序列相等的定义可知，两个既约字$x_1^{\lambda_1}\cdots x_m^{\lambda_m}$和$y_1^{\delta_1}\cdots y_n^{\delta_n}$（$x_i$，$y_j\in X$，$\lambda_i$，$\delta_j=\pm 1$）相等$\Longleftrightarrow$或者二者均为1，或者 $m=n$并且$x_i=y_i$，$\lambda_i=\delta_i(1\leqslant i\leqslant n)$。于是由$x\longmapsto x^1=x$给出的从$X$到$X$上全体既约字组成的集合$F(X)$上的映射是单射。我们将$X$等同于它的象，从而将$X$看成是$F(X)$的一个子集合。

接下来我们定义集合 $F=F(X)$ 上的二元运算。空字1的作用象幺元素（对每个 $w\in F$，$w1=1w=w$）。我们希望非空既约字的乘积是它们的连接，即

$(x_1^{\lambda_1}\cdots x_m^{\lambda_m})(y_1^{\delta_1}\cdots y_n^{\delta_n})=x_1^{\lambda_1}\cdots x_m^{\lambda_m}y_1^{\delta_1}\cdots y_n^{\delta_n}$。不幸的是，方程右边的字可能不是既约的（例如$x_m^{\lambda_m}=y_1^{-\delta_1}$时）。因此，我们在连接之后(如果必要的话)再消去形如xx^{-1}或者$x^{-1}x$的相邻项，将它定义为两个既约字的乘积.例如$(x_1x_2^{-1}x_3)(x_3^{-1}x_2x_4)=x_1x_4$。更确切地，如果$x_1^{\lambda_1}\cdots x_m^{\lambda_m}$和$y_1^{\delta_1}\cdots y_n^{\delta_n}$是$X$上的非空既约字，$m\leqslant n$，以$k$表示最大整数（$0\leqslant k\leqslant m$），使得 $x_{m-j}^{\lambda_{m-j}}=y_{j+1}^{-\delta_{j+1}}$（$0\leqslant j\leqslant k-1$）。则定义

$$(x_1^{\lambda_1}\cdots x_m^{\lambda_m})(y_1^{\delta_1}\cdots y_n^{\delta_n})=\begin{cases}x_1^{\lambda_1}\cdots x_{m-k}^{\lambda_{m-k}}y_{k+1}^{\delta_{k+1}}\cdots y_n^{\delta_n}, & \text{如果}k<m;\\ y_{m+1}^{\delta_{m+1}}\cdots y_n^{\delta_n} & \text{如果}k=m<n.\\ 1, & \text{如果}k=m=n.\end{cases}$$

对于$m>n$，乘积也可以类似地定义。这个定义保证既约字的积仍然是既约字。

定理9.1 如果X是非空集合，$F=F(X)$是X上全体既约字所

构成的集合，则F对于上述定义的二元运算为群，并且$F=\langle X\rangle$。

群$F=F(X)$叫作集合X上的自由群（“自由”一字的解释见下面定理9.2）。

证明 因为1是幺元素，而$x_1^{\delta_1}\cdots x_n^{\delta_n}$的逆元素是$x^{-\delta_n}\cdots x_1^{-\delta_1}$，从而只需验证结合律。为此，可以用归纳法和仔细地考查各种情形，也可以用下面更巧妙的机构：对于每个$x\in X$和$\delta=\pm1$，以$|x^\delta|$表示映射$F\to F$，$1\mapsto x^\delta$并且

$$x_1^{\delta_1}\cdots x_n^{\delta_n}\mapsto\begin{cases}x^\delta x_1^{\delta_1}\cdots x_n^{\delta_n}, & \text{如果}x^\delta\neq x_1^{-\delta_1};\\ x_2^{\delta_2}\cdots x_n^{\delta_n}, & \text{如果}x^\delta=x_1^{-\delta_1}\text{并且}n\geqslant 2;\\ 1, & \text{如果}x^\delta=x_1^{-\delta_1}\text{并且}n=1.\end{cases}$$

由于$|x|\,|x^{-1}|=1_F=|x^{-1}|\,|x|$，从而根据引论中（13）式，可知每个$|x^\delta|$都是$F$上的置换（一一对应），其逆映射是$|x^{-\delta}|$。以$A(F)$表示$F$上的全体置换所构成的群（见第39页），而$F_0$表示由$\{|x|\ |x\in X\}$生成的子群。则映射$\varphi$：$F\to F_0$，$1\to 1_F$，$x_1^{\delta_1}\cdots x_n^{\delta_n}\mapsto|x_1^{\delta_1}|\cdots|x_n^{\delta_n}|$显然是满射，并且对$w_1$，$w_2\in F$，有$\varphi(w_1w_2)=\varphi(w_1)\varphi(w_2)$。由于在映射$|x_1^{\delta_1}|\cdots|x_n^{\delta_n}|$之下，$1\mapsto x_1^{\delta_1}\cdots x_n^{\delta_n}$，从而$\varphi$是单射。但是$F_0$是群，从而在$F$中有结合律，并且$\varphi$为群同构。显然$F=\langle X\rangle$。∎

容易得到自由群的某些性质。例如若$|X|\geqslant 2$，则X上的自由群是非Abel群（x，$y\in X$，$x\neq y\Longrightarrow x^{-1}y^{-1}xy$是既约的$\Longrightarrow x^{-1}y^{-1}xy\neq 1\Longrightarrow xy\neq yx$）。类似地，自由群中每个元素（$\neq1$）均具有无限阶（习题1）。如果$X=\{a\}$，则$X$上的自由群是无限循环群$\langle a\rangle$（习题2）。一个很不平凡的结果是：自由群的每个子群本身也是某个子集上的自由群（见J.Rotman[19]）。

定理9.2 假设F是集合X上的自由群，$l:X\to F$是包含映射。

如果G是群而$f:X\to G$是集合映射，则存在唯一的群同态$\bar{f}:F\to G$，使得$\bar{f}l=f$。换句话说，F是群范畴中集合X上的自由对象。

注记：如果F'是群范畴中集合X上的另一个自由对象（对于$\lambda:X\to F'$），则由定理7.8和9.2可知存在同构$\varphi:F\cong F'$，使得$\varphi l=\lambda$。特别地，$\lambda(X)$是F'的生成元集合。这个事实也可以从自由对象的定义直接证得。

定理9.2的证明概要 定义$\bar{f}(1)=e$。如果$x_1^{\delta_1}\cdots x_n^{\delta_n}$是$X$上的非空既约字，定义$\bar{f}(x_1^{\delta_1}\cdots x_n^{\delta_n})=f(x_1)^{\delta_1}f(x_2)^{\delta_2}\cdots f(x_n)^{\delta_n}$。由于$G$是群，$\delta_i=\pm 1$，从而乘积$f(x_1)^{\delta_1}\cdots f(x_n)^{\delta_n}$是$G$中元素。证明$\bar{f}$是同态并且$\bar{f}l=f$。如果$g:F\to G$是任一同态，使得$gl=f$，则$g(x_1^{\delta_1}\cdots x_n^{\delta_n})=g(x_1^{\delta_1})\cdots g(x_n^{\delta_n})=g(x_1)^{\delta_1}\cdots g(x_n)^{\delta_n}=gl(x_1)^{\delta_1}\cdots gl(x_n)^{\delta}=f(x_1)^{\delta_1}\cdots f(x_n)^{\delta_n}=\bar{f}(x_1^{\delta_1}\cdots x_n^{\delta_n})$。因此$\bar{f}$是唯一的。 ∎

系9.3 每个群G都是某个自由群的同态象。

证明 设X是G的生成元集合，令F为集合X上的自由群。按照定理9.2，包含映射$X\to G$诱导出同态$\bar{f}:F\to G$，使得$x\mapsto x\in G$。由于$G=\langle X\rangle$，从定理9.2的证明过程可知$\bar{f}$是满同态。∎

系9.3和第一同构定理的直接推论是：每个群G均同构于商群F/N，其中$G=\langle X\rangle$，F是X上的自由群，而N是系9.3中满同态$F\to G$的核。因此，为了刻划G（在同构意义下），我们只需决定X，F和N。但是F是由X所决定的（在同构意义下）（定理7.8），而N作为F的子群，是由生成它的任意子集所决定的。现在，如果$w=x_1^{\delta_1}\cdots x_n^{\delta_n}\in F$是$N$的生成元，则在满同态$F\to G$之下，$w\mapsto x_1^{\delta_1}\cdots x_n^{\delta_n}=e\in G$。$G$中的方程$x_1^{\delta_1}\cdots x_n^{\delta_n}=e$叫做生成元$x_i$上的关系。显然，一个给定的群$G$可以由$G$的一个指定的生成元集合$X$与这些生

成元上一个适当的关系集合R所完全刻划。这个刻划是不唯一的，因为对于一个给定群G，X和R均可以有许多可能的选择（见习题6和9）。

反之，假如我们给了一个集合X和X上元素的一个（既约）字集合Y。问题：是否存在着群G，使得G由X生成并且所有的关系$w=e(w\in Y)$均是对的（其中$w=x_1^{\delta_1}\cdots x_n^{\delta_n}$现在是$G$中的乘积）？我们马上就会看到，答案是肯定的，只要允许X中不同的元素在群G中可以相等。例如若a，$b\in X$，而a^1b^{-1}是Y中的（既约）字，则在包含a，b并且满足$a^1b^{-1}=e$的每个群中$a=b$。

给了“生成元”集合X和X中元素的（既约）字集合Y，我们可以如下构作这样的一个群：令F是X上的自由群，N是F中由Y生成的正规子群[3]。令$G=F/N$，并且X等同于在映射 $X\subset F\to F/N$之下的象。如上所述，这可能会使 X中某些元素等同为同一元素。这时，G是由X（经过等同之后）生成的群。并且由构造方法可知满足所有的关系$w=e(w\in Y)$。（$w=x_1^{\delta_1}\cdots x_n^{\delta_n}\in Y\Longrightarrow x_1^{\delta_1}\cdots x_n^{\delta_n}\in N\Longrightarrow x_1^{\delta_1}N\cdots x_n^{\delta_n}N=N$，即在$G=F/N$中$x_1^{\delta_1}\cdots x_n^{\delta_n}=e$）。

定义9.4 假设X是集合而Y是X上的一个（既约）字集合。我们称群G是由生成元$x\in X$和关系$w=e(w\in Y)$所定义的群，如果$G\cong F/N$，其中F是X上的自由群，而N是F中由Y生成的正规子群。这时，称$(X|Y)$是群G的表现。

上面的讨论表明，由给定的生成元和关系所定义的群是永远存在的。进而，它在下列意义下是最大可能的这样的群。

3.由集合$S\subset F$生成的正规子群是F中所有包含S的正规子群之交，见习题5.2。

定理9.5 (Van Dyck)假设X是集合而Y是一个X上(既约)字集合。G是由生成元$x\in X$和关系$w=e(w\in Y)$所定义的。如果H是任一群，使得$H=\langle X\rangle$并且H满足全部关系 $w=e(w\in Y)$，则存在满同态$G\to H$。

注记：Y中的元素可以看作X上的字，G中的乘积和H中的乘积，可以按上下文区分开来。

定理9.5的证明 如果F是X上的自由群，则由系9.3可知，包含映射$X\to H$诱导出满同态$\varphi:F\to H$。因为H满足诸关系$w=e(w\in Y)$，从而 $Y\subset\mathrm{Ker}\varphi$。因此在$F$中由$Y$生成的正规子群包含在 $\mathrm{Ker}\varphi$中。根据系5.8，φ 诱导出满同态 $F/N\to H/0$。从而合成映射 $G\cong F/N\to H/0\cong H$是满同态。∎

下面是由生成元和关系定义的一些群的例子.这些例子表明，为了研究一个给定的表现，常常需要针对这一表现的某种专门的推理。在方便的时候，我们对于字将使用指数记号(例如用x^2y^{-3}代替$x^1x^1y^{-1}y^{-1}y^{-1}$)。

例 令G是由生成元a，b和关系$a^4=e$，$a^2b^{-2}=e$以及$abab^{-1}=e$所定义的群。由于8阶四元数群Q_8是由a，b生成的，并且满足这些关系(习题4.14)，根据定理9.5,可知存在满同态$\varphi:G\to Q_8$。于是 $|G|\geqslant|Q_8|=8$。以F表示$\{a,b\}$上的自由群，N是由$\{a^4,\ a^2b^{-2},\ abab^{-1}\}$生成的正规子群。不难证明，$F/N$中每个元素均有形式$a^ib^iN$，其中$0\leqslant i\leqslant 3$而$j=0,1$。于是 $|G|=|F/N|\leqslant 8$。因此 $|G|=8$ 而φ是同构。从而由上述生成元和关系定义的群是(同构于)Q_8。

例 由生成元a，b和关系$a^n=e(3\leqslant n\in\mathbb{N}^*)$,$b^2=e$以及$abab=e$(或者$ba=a^{-1}b$)定义的群是正多边形群$D_n$(习题8)。

例 由一个生成元b和一个关系 $b^m=e(m\in\mathbb{N}^*)$ 定义的群是

Z_m（习题9）。

例 集合X上的自由群F是由生成元$x \in X$(没有关系）所定义的群（根据定义2.7，$\langle \phi \rangle = \langle e \rangle$）。“自由”一词来源于$F$没有关系(relation-free)这一事实。

本节最后我们对群范畴中的余积（自由积）作简要地讨论。许多细节都留给读者，因为整个过程与构作自由群的过程是很相似的。

给了一个群族$\{G_i \mid i \in I\}$，我们可以假定（必要时重新加以标记）诸G_i是彼此非交的集合。假设$X = \bigcup_{i \in I} G_i$，令$\{1\}$是与$X$非交的一元集合。$X$上的字是任一序列$(a_1, a_2, \cdots)$，使得$a_i \in X \cup \{1\}$并且存在某个$n \in \mathbf{N}^*$，使得当$i \geqslant n$时，$a_i = 1$。字$(a_1, a_2, \cdots)$叫作既约的，是指

(i) 没有$a_i \in X$是a_i所在的群G_i中的幺元素；

(ii) 对于所有i，$i \geqslant 1$，a_i和a_{i+1}不在同一群G_j之中；

(iii) 对于所有$i \geqslant k$，$a_k = 1$导致$a_i = 1$。特别地，$1 = (1, 1, \cdots)$是既约的。每个既约字($\neq 1$)均可唯一地写成$a_1 a_2 \cdots a_n = (a_1, a_2, \cdots, a_n, 1, 1, \cdots)$，其中$a_i \in X$。

以$\prod_{i \in I}^{*} G_i$（当I有限时也记为$G_1 * G_2 * \cdots * G_n$）表示X上全体既约字所组成的集合。对于下述的二元运算，$\prod_{i \in I}^{*} G_i$形成群，叫作群族$\{G_i \mid i \in I\}$的自由积。二元运算定义为：1是幺元素，两个既约字($\neq 1$)之乘积基本上是将此二字连接在一起。但是两个既约字的连接可能不是既约的，从而要作必要的消元和紧缩。例如若$a_i, b_i \in G_i (i = 1, 2, 3)$，则$(a_1 a_2 a_3)(a_3^{-1} b_2 b_1 b_3) = a_1 c_2 b_1 b_3 = (a_1, c_2, b_1, b_3, 1, 1, \cdots)$，其中$c_2 = a_2 b_2 \in G_2$。最后，对于

每个$k\in I$，映射$l_k:G_k\to\prod_{i\in I}^{*}G_i$，$e\mapsto 1$，$a\mapsto a=(a,\ 1,\ 1,\cdots)$是群的单同态。因此有时我们将$G_k$等同于它在$\prod_{i\in I}^{*}G_i$中的同态象（例如在习题15中即是如此）。

定理9.6 假设$\{G_i|\ i\in I\}$是群族而$\prod_{i\in I}^{*}G_i$是它们的自由积。如果$\{\psi_i:G_i\to H\ |i\in I\}$是一个群同态族，则存在唯一的同态$\psi:\prod_{i\in I}^{*}G_i\to H$，使得对所有$i\in I$，$\psi l_i=\psi_i$，并且这一性质不计同构唯一决定了$\prod_{i\in I}^{*}G_i$。换句话说，$\prod_{i\in I}^{*}G_i$是群范畴中的余积。

证明概要 如果$a_1a_2\cdots a_n$是$\prod_{i\in I}^{*}G_i$中的既约字，其中$a_k\in G_{i_k}$，定义$\psi(a_1\cdots a_n)$为$\psi_{i_1}(a_1)\psi_{i_2}(a_2)\cdots\psi_{i_n}(a_n)\in H$。∎

习　题

1. 自由群F中的每个非幺元素都是无限阶的。
2. 求证集合$\{a\}$上的自由群是无限循环群，从而同构于$\mathbf{Z}$。
3. 设F是自由群，N是由集合$\{x^n|x\in F\}$（n为固定的整数）生成的子群，求证$N\lhd F$。
4. 令F为集合X上的自由群，$Y\subset X$。如果H是F中包含Y的最小正规子群，则F/H是自由群。
5. 由生成元a，b和关系$a^8=b^2a^4=ab^{-1}ab=e$生成的群，其阶数$\leqslant 16$。
6. 6阶循环群是由生成元a，b和关系$a^2=b^3=a^{-1}b^{-1}ab=e$所定义的群。
7. 求证由生成元a，b和关系$a^2=e$，$b^8=e$定义的群是无限非Abel群。
8. 由生成元a，b和关系$a^n=e(3\leqslant n\in\mathbf{N}^*)$，$b^2=e$，$abab=e$定义的群是正

多边形群D_n（见定理6.13）。

9. 由生成元b和关系$b^m=e(m\in\mathbf{N}^*)$定义的群是循环群Z_m。

10. 自由积运算是满足交换律和结合律的：对于任意群A，B，C，$A*B\cong B*A$，$A*(B*C)\cong(A*B)*C$。

11. 如果N是$A*B$的由A生成的正规子群，则$(A*B)/N\cong B$。

12. 如果G与H均有多于一个元素，则$G*H$是无限群，并且中心为$\langle e\rangle$。

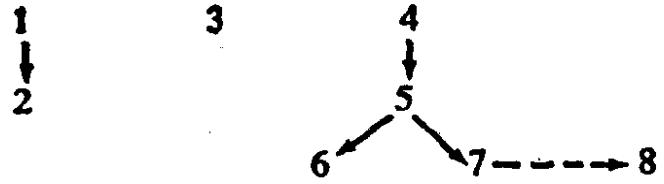
13. 自由群是一些无限循环群的自由积。

14. 如果G是由生成元a，b和关系$a^2=e$，$b^8=e$定义的群，则$G\cong Z_2*Z_8$。〔见习题12并比较习题6.〕

15. 如果f：$G_1\to G_2$，g：$H_1\to H_2$是群同态，则存在唯一的同态h：$G_1*H_1\to G_2*H_2$，使得$h|G_1=f$，$h|H_1=g$。

第II章　群的结构

我们继续按照在第I章引言中所描绘的计划来研究群。本章所突出的重点是：对于 Abel 群和各类与 Abel 群性质相似的（非 Abel）群，给出比较深刻的结构定理。这一章分成三部分，一部分中的结果可能用作另一部分的例子或推动力。但是各部分之间基本上是独立的，各节之间的关系如下



第 8 节中大部分内容与本章的其余部分是无关的。

1. 自由 Abel 群

我们将研究 Abel 群范畴中的自由对象。象通常在处理Abel群时习惯上所作的那样，本节中均采用加法记号。下面的表可能是有帮助的。

ab ……$a+b$

a^{-1} ……$-a$

e ……0

a^n ……na

ab^{-1} ……$a-b$

HK ……$H+K$

aH ……$a+H$

$G\times H$……$G\oplus H$

$H\vee K$……$H+K$

$\prod^{W}_{i\in I} G_i$ …… $\sum_{i\in I} G_i$

弱直积 ……直和

对于采用加法记号的任意群G，$(m+n)a=ma+na$ $(a\in G,$ $m,$ $n\in\mathbf{Z})$。如果G是Abel群，则$m(a+b)=ma+mb$。如果X是G的非空子集合，根据定理I.2.8，由X生成的子群$\langle X\rangle$采用加法记号则是由所有线性组合$n_1x_1+n_2x_2+\cdots+n_kx_k(n_i\in\mathbf{Z},\ x_i\in X)$所构成的。特别地，循环群$\langle x\rangle$是$\{nx\mid n\in\mathbf{Z}\}$。

Abel群F的一组基是F的一个子集合X，使得(i)$F=\langle X\rangle$，并且(ii)对于不同的x_1，x_2，…，$x_k\in X$和$n_i\in\mathbf{Z}$，

$n_1x_1+n_2x_2+\cdots+n_kx_k=0\Longrightarrow$ 对于每个i均有$n_i=0$。

读者不要被它与向量空间的基之间惑人的类比所哄骗（习题2）.

定理1.1 关于 Abel 群F的如下一些条件是彼此等价的。

(i) F具有一组非空的基。

(ii) F是一族无限循环群的（内）直和。

(iii) F是（同构于）一些整数加法群$\mathbf{Z}$的直和。

(iv) 存在着非空集合X和函数$l:X\to F$具有下列性质：给了

Abel群G和函数$f:X\to G$，则存在唯一的群同态$\bar{f}:F\to G$，使得$\bar{f}l=f$。换句话说，F是Abel群范畴中的自由对象。

满足定理1.1条件的Abel群F叫作（集合X上的）自由Abel群。我们也定义平凡群0是空集合ϕ上的自由Abel群。

定理1.1的证明 (i)$\Longrightarrow$(ii)：如果X是F的一组基，则对于每个$x\in X$，$nx=0\Longleftrightarrow n=0$。因此每个子群$\langle x\rangle$($x\in X$)均是无限循环群（由于$F$是Abel群，从而它是正规子群）。因为$F=\langle X\rangle$，我们也有$F=\langle\bigcup_{x\in X}\langle x\rangle\rangle$。假如对于某个$z\in X$，$\langle z\rangle\cap\langle\bigcup_{\substack{x\in X\\ x\neq z}}\langle x\rangle\rangle\neq 0$，则存在某个非零的$n\in\mathbb{Z}$，使得$nz=n_1x_1+\cdots+n_kx_k$，其中$z,x_1,\cdots,x_k$是$X$中不同的元素，它与$X$为一组基这一事实相矛盾。因此$\langle z\rangle\bigcap\langle\bigcup_{\substack{x\in X\\ x\neq z}}\langle x\rangle\rangle=0$。从而根据定义I.8.8便知$F=\sum_{x\in X}\langle x\rangle$。

(ii)⇒(iii)：定理I.3.2，I.8.6和I.8.10。

(iii)⇒(i)：假设$F\cong\Sigma\mathbb{Z}$，其中诸$\mathbb{Z}$由X作下标集合。对于每个$x\in X$，以θ_x表示$\Sigma\mathbb{Z}$中的元素$\{u_i\}$，其中$u_i=0$(对于$i\neq x$)，而$u_x=1$。验证$\{\theta_x\mid x\in X\}$是$\Sigma\mathbb{Z}$的一组基。然后利用同构$F\cong\Sigma\mathbb{Z}$得到F的一组基。

(i)⇒(iv)：设X是F的一组基，而l：$X\to F$是包含映射。假设给了一个映射$f:X\to G$。如果$u\in F$，由于X生成F，从而$u=n_1x_1+\cdots+n_kx_k(n_i\in\mathbb{Z},x_i\in X)$。如果$u=m_1x_1+\cdots+m_kx_k(m_k\in\mathbb{Z})$，则$\sum_{i=1}^{k}(n_i-m_i)x_i=0$，由于$X$是一组基，从而对每个$i$，$n_i=m_i$。

于是我们可以定义映射$\bar{f}:F\to G$，$\bar{f}(u)=\bar{f}\left(\sum_{i=1}^{k}n_ix_i\right)=n_1f(x_1)$

$+\cdots+n_kf(x_k)$，使得$\bar{f}l=f$。因为G是 Abel 群，易知$\bar{f}$是同态。又由于X生成F，从而每个同态$F\to G$均由它在X上的作用所完全决定。因此若$g:F\to G$是同态，使得$gl=f$，则对于每个$x\in X$，$g(x)=g(l(x))=f(x)=\bar{f}(x)$，从而$g=\bar{f}$，即$\bar{f}$是唯一的。因此由定义I.7.7可知在Abel群范畴中，F是集合X上的自由对象。

(iv)⇒(iii)：给了$l:X\to F$，构作直和$\Sigma\mathbb{Z}$，其中诸$\mathbb{Z}$以X为下标集合。如同(iii)⇒(i)的证明中所作的那样，令$Y=\{\theta_x|x\in X\}$是$\Sigma\mathbb{Z}$的一组基。在(iii)⇒(i)⇒(iv)的证明中，已经推出$\Sigma\mathbb{Z}$是集合Y上的自由对象。由于显然有$|X|=|Y|$，根据定理I.7.8可知$F\cong\Sigma\mathbb{Z}$。 ∎

给了任一集合X，定理1.1的证明指出如何构作以X为一组基的自由 Abel 群F。简言之，令F为直和$\Sigma\mathbb{Z}$，其中诸$\mathbb{Z}$以X为下标集合。正如(iii)⇒(i)的证明中所示，$\{\theta_x|x\in X\}$是$F=\Sigma\mathbb{Z}$的一组基，并且F是集合$\{\theta_x|x\in X\}$上的自由群。由于映射$l:X\to F$，$x\longmapsto\theta_x$是单射，由此易知，在定理1.1条件(iv)的意义下，F是X上的自由群。在这种情况下，我们将X与它在l下之象等同，从而$X\subset F$，而循环子群$\langle\theta_x\rangle=\{n\theta_x|n\in\mathbb{Z}\}=\mathbb{Z}\theta_x$写成$\langle x\rangle=\mathbb{Z}x$。在这种记号下，$F=\sum_{x\in X}\langle\theta_x\rangle$写成$F=\sum_{x\in X}\mathbb{Z}x$，而$F$中元素均有形式$n_1x_1+\cdots+n_kx_k$($n_i\in\mathbb{Z}$，$x_i\in X$)。特别地，$X=l(X)$是$F$的一组基。

定理1.2 自由 Abel 群F的任意两组基具有同样的势。

于是，自由 Abel 群F的任意一组基X的势$|X|$是F的一个不变量。$|X|$称作F的秩。

定理1.2的证明概要 先设F有一组基X，其中X具有有限势n。于是$F\cong\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$($n$个直和成分)。对于$F$的任一子群$G$，证

明$2G=\{2u\mid u\in G\}$是G的子群．验证同构$F\cong\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$在$2F$上的限制是同构$2F\cong 2\mathbb{Z}\oplus\cdots\oplus 2\mathbb{Z}$，于是由系I.8.11可知$F/2F\cong\mathbb{Z}/2\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/2\mathbb{Z}\cong Z_2\oplus\cdots\oplus Z_2$（$n$个直和成分）．因此$|F/2F|=2^n$．如果$Y$是$F$的另一组基，而$r$是任一整数，使得$|Y|\geqslant r$，则由类似的推理可以证明$|F/2F|\geqslant 2^r$，从而$2^r\leqslant 2^n$，即$r\leqslant n$．由此推出$|Y|=m\leqslant n$，从而$|F/2F|=2^m$．因此$2^m=2^n$，而$|X|=n=m=|Y|$．

如果F有一组基是无限的，从上一段可知，F的任一组基都是无限的．因此，为了完成证明，我们只需证明$|X|=|F|$，其中X为F的任一组无限的基．显然$|X|\leqslant|F|$．令$S=\bigcup_{n\in N^*}X^n$，其中$X^n=X\times X\times\cdots\times X$（$n$个因子）．对于每个$s=(x_1,\cdots,x_n)\in S$，以$G_s$表示子群$\langle x_1,\cdots,x_n\rangle$．于是$G_s\cong\mathbb{Z}y_1\oplus\cdots\oplus\mathbb{Z}y_t$，其中$y_1,\cdots,y_t$（$t\leqslant n$）是$\{x_1,\cdots,x_n\}$中两两相异元素．因此由引论中定理8.12可知$|G_s|=|\mathbb{Z}^t|=|\mathbb{Z}|=\aleph_0$．由于$F=\bigcup_{s\in S}G_s$，由引论中习题8.12我们有$|F|=\left|\bigcup_{s\in S}G_s\right|\leqslant|S|\aleph_0$．但是由引论中定理8.11和8.12，$|S|=|X|$，从而$|F|\leqslant|X|\aleph_0=|X|$．因此由Schroeder–Bernstein定理得到$|F|=|X|$． ∎

命题1.3 设F_1是集合X_1上的自由Abel群，F_2是集合X_2上的自由Abel群．则$F_1\cong F_2\Longleftrightarrow F_1$和$F_2$有同样的秩（即$|X_1|=|X_2|$）．

注记：命题1.3对于任意非Abel自由群（见第I.9节）也成立．见习题12．

命题1.3的证明概要 如果$\alpha:F_1\cong F_2$．则$\alpha(X_1)$是F_2的一组

基，从而由定理1.2可知 $|X_1|=|\alpha(X_1)|=|X_2|$。反过来则是定理I.7.8。 ∎

定理1.4 每个Abel群G均是秩$|X|$的自由Abel群的同态象，其中X是G的生成元集合。

证明 如果F是集合X上的自由Abel群。则$F=\sum_{x\in X}\mathbb{Z}x$并且rank$F=|X|$。根据定理1.1，包含映射$X\to G$诱导出一个同态$\bar{f}:F\to G$，使得$1x\longmapsto x\in G$，从而$X\subset \mathrm{Im}\bar{f}$。由于$X$生成$G$，从而必然有$\mathrm{Im}\bar{f}=G$。 ∎

现在我们要证明一个定理，它在分析有限生成Abel群的结构时（第2节）是非常有用的。为此我们需要

引理1.5 如果$\{x_1, \cdots, x_n\}$是自由Abel群的一组基并且$a\in\mathbb{Z}$，则对所有$i\neq j$，$\{x_1, \cdots, x_{j-1}, x_j+ax_i, x_{j+1}, \cdots, x_n\}$也是$F$的一组基。

证明 由于 $x_j=-ax_i+(x_j+ax_i)$，从而 $F=\langle x_1, \cdots, x_{j-1}, x_j+ax_i, x_{j+1}, \cdots, x_n\rangle$。如果$k_1x_1+\cdots+k_j(x_j+ax_i)+\cdots+k_nx_n=0(k_j\in\mathbb{Z})$，则$k_1x_1+\cdots+(k_i+k_ja)x_i+\cdots+k_jx_j+\cdots+k_nx_n=0$，由此推得对每个$t$，$k_t=0$。 ∎

定理1.6 如果F是有限秩n的自由Abel群，G是F的非零子群，则存在F的一组基$\{x_1, \cdots, x_n\}$，一个整数$r(1\leqslant r\leqslant n)$和一组正整数$d_1, \cdots, d_r$，使得$d_1|d_2|\cdots|d_r$，并且$G$是以$\{d_1x_1, \cdots, d_rx_r\}$为基的自由Abel群。

注记：秩（可能无限）为α的自由Abel群的每个子群也是自

由的，并且其秩β至多等于α，见定理IV.6.1.记号 "$d_1 | d_2 | \cdots | d_r$" 意味着"d_1除尽d_2，d_2除尽d_3等等"。

定理1.6的证明 如果$n=1$，则$F=\langle x_1\rangle \cong \mathbf{Z}$，而由定理I.3.5，I.3.1和I.3.2可知$G=\langle d_1x_1\rangle \cong \mathbf{Z}$($d_1\in \mathbf{N}^*$)。采用数学归纳法，假设定理对于秩小于$n$的所有自由 Abel 群均成立。以$S$表示集合

$$\left\{ s\in \mathbf{Z} \mid \begin{array}{l}\text{存在}F\text{的一组基}\{y_1, \cdots, y_n\}\text{，使}G\text{中} \\ \quad \text{有形如}sy_1+k_2y_2+\cdots+k_ny_n\ (k_i\in \mathbf{Z})\text{的元素。}\end{array} \right\}$$

注意在这种情形下，$\{y_2, y_1, y_3, \cdots, y_n\}$也是$F$的一组基，从而$k_2\in S$。类似地$k_i\in S$（对于$i=3, 4, \cdots, n$)。由于$G\neq 0$，从而$S\neq \varnothing$。因此$S$包含有最小的正整数$d_1$，并且对于 F 的某一组基$\{y_1, y_2, \cdots, y_n\}$，存在$v\in G$，使得 $v=d_1y_1+k_2y_2+\cdots+k_ny_n$。利用除法算式，对于每个 $i=2, \cdots, n$，有 $k_i=d_1q_i+r_i$，其中$0\leqslant r_i<d_1$。从而 $v=d_1(y_1+q_2y_2+\cdots+q_ny_n)+r_2y_2+\cdots+r_ny_n$。令 $x_1=y_1+q_2y_2+\cdots+q_ny_n$，由引理1.5可知$W=\{x_1, y_2, \cdots, y_n\}$是$F$的一组基。由于$v\in G$，$r_i<d_1$ 而将W中元素以任意次序重新排列，均是F的一组基，从而由d_1在 S 中的最小性质推出$0=r_2=r_3=\cdots=r_n$，因此$d_1x_1=v\in G$。

令$H=\langle y_2, y_3, \cdots, y_n\rangle$。则$H$是秩$n-1$的自由Abel群，并且$F=\langle x_1\rangle \oplus H$。进而我们断言 $G=\langle v\rangle \oplus (G\cap H)=\langle d_1x_1\rangle \oplus (G\cap H)$。由于$\{x_1, y_2, \cdots, y_n\}$是$F$的一组基，从而$\langle v\rangle \cap (G\cap H)=0$。如果$u=t_1x_1+t_2y_2+\cdots+t_ny_n\in G(t_i\in \mathbf{Z})$，由除法算式有 $t_1=d_1q_1+r_1$其中$0\leqslant r_1<d_1$。因此G中包含 $u-q_1v=r_1x_1+t_2y_2+\cdots+t_ny_n$。由$d_1$在$S$中的最小性质推出$r_1=0$，从而 $t_2y_2+\cdots+t_ny_n\in G\cap H$并且$u=q_1v+(t_2y_2+\cdots+t_ny_n)$。从而 $G=\langle v\rangle+(G\cap H)$，这就证明了我们的断言(定义I.8.8)。

如果$G\cap H=0$，则 $G=\langle d_1x_1\rangle$，从而定理成立。否则便有$G\cap H\neq 0$。这时由归纳假设可知存在H的一组基$\{x_2, x_3, \cdots, x_n\}$和正整数$r$，$d_2$，$d_3$，$\cdots$，$d_r$，使得$d_2|d_3|\cdots|d_r$，并且$G\cap H$是以$\{d_2x_2, \cdots, d_rx_r\}$为基的自由 Abel 群。由于 $F=\langle x_1\rangle\oplus H$而$G=\langle d_1x_1\rangle\oplus(G\cap H)$，易知 $\{x_1, x_2, \cdots, x_n\}$ 是F的一组基同时$\{d_1x_1, \cdots, d_rx_r\}$是$G$的一组基。为完成证明的归纳步骤，我们只需要证明$d_1|d_2$。根据除法算式，$d_2=qd_1+r_0$，$0\leqslant r_0<d_1$。根据引理1.5，$\{x_2, x_1+qx_2, x_3, \cdots, x_n\}$是$F$的一组基，而 $r_0x_2+d_1(x_1+qx_2)=d_1x_1+d_2x_2\in G$，由$d_1$在$S$中的最小性质推得$r_0=0$，从而$d_1|d_2$。 ∎

系1.7 如果G是由n个元素生成的有限生成Abel群，则 G 的每个子群H均可以由m个元素生成，其中$m\leqslant n$。

如果略去“Abel”一词，则此系不再成立(习题8)。

系1.7的证明 根据定理1.4，存在着秩n的自由Abel群和满同态$\pi:F\to G$。$\pi^{-1}(H)$是F的子群，根据定理1.6可知$\pi^{-1}(H)$是秩$m\leqslant n$的自由Abel群。$\pi^{-1}(H)$ 的任意一组基在π之下的象是由至多m个元素所构成的集合，此集合生成$\pi(\pi^{-1}(H))=H$。 ∎

习　题

1. (a) 如果G是 Abel 群而$m\in\mathbf{Z}$,则$mG=\{mu\,|\,u\in G\}$ 是G的子群。

   (b) 如果$G\cong\sum_{i\in I}G_i$，则$mG\cong\sum_{i\in I}mG_i$而$G/mG\cong\sum_{I\in i}G_i/mG_i$。

2. Abel群F的子集合X叫作线性无关的，是指：$n_1x_1+\cdots+n_kx_k=0(n_i\in\mathbf{Z}$，$x_1$，$\cdots$，$x_k$为$X$中不同的元素)$\Rightarrow$对每个$i$均有$n_i=0$。求证：

(a) X是线性无关的$\Longleftrightarrow$子群$\langle X\rangle$中每个非零元素均可以唯一写成形式$n_1x_1+\cdots+n_sx_s$ ($n_i\in\mathbf{Z}$, $n_i\neq 0$, x_1, x_2, $\cdots$, x_s为X的不同元素)。

(b) 如果F是秩n (有限) 的自由 Abel 群，则n元线性无关子集合不一定是一组基[提示：考虑$F=\mathbf{Z}$]。

(c) 如果F是自由 Abel 群，则F的线性无关子集合不一定能扩充成F的一组基。

(d) 如果 F是自由Abel群，则F的生成元集合 不一定包含 F 的 一 组基。但是如果F是由n个元素有限生成的自由 Abel 群，则 F 的秩m不超过n。

3. 设$X=\{a_i|i\in I\}$ 是一个集合。则X上的自由 Abel 群是 (同构于)由生成元集合X和关系 (用乘法记号) $\{a_ia_ja_i^{-1}a_j^{-1}=e|i,\ j\in I\}$ 所定义的群。

4. 自由 Abel 群是自由群(第I.9节)，当且仅当它是循环群。

5. 一族自由 Abel 群的直和是自由 Abel 群。(自由 Abel群的直积不必为自由Abel群，见L.Fuchs [13，第168页].)

6. 如果$F=\sum_{x\in X}\mathbf{Z}x$是自由 Abel 群，$G$是以$X'=X-\{x_0\}$(对于某个$x_0\in X$) 为基的子群， 则$F/G\cong\mathbf{Z}x_0$。将此结果推广到$X$的任意子集$X'$上去。

7. 对于每个正整数n，一个非零自由 Abel 群均有指数为n的子群。

8. 设G 是由实阵 $a=\begin{pmatrix}2&0\\0&1\end{pmatrix}$，$b=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 生成的乘法群。如果H是G中(主)对角元均为 1 的全部方阵所构成的集合，则H是一个子群但不是有限生成的。

9. 设G是有限生成 Abel 群，其中每个非零元素均是无限阶的。则 G 是自由 Abel 群。[提示：定理1.6]

10. (a) 求证有理数加法群$\mathbf{Q}$不是有限生成的。

(b) 求证$\mathbf{Q}$不是自由的。

(*c*) 如果将“有限生成”这一假设条件去掉，则习题9不再成立。

11. (*a*) 假定G是以x为变量的全体整系数多项式所形成的加法群。求证G同构于正有理数（乘法）群$\mathbf{Q}^*$.[提示：用算术基本定理来构作同构.]。

(*b*) 群$\mathbf{Q}^*$是以 $\{p \mid p$为$\mathbf{Z}$中素数$\}$ 为基的自由 Abel 群。

12. 令F是集合X上的自由（不必 Abel）群（见第I.9节），G 是集合Y上的自由群。又令F'是F中由 $\{aba^{-1}b^{-1} \mid a, b \in F\}$ 生成的子群，类似地定义G'。求证：

(*a*) $F' \lhd F$, $G' \lhd G$，并且F/F'和G/G'是 Abel 群 [见后面的定理7.8]。

(*b*) F/F'和 G/G' 分别是秩为$|X|$和$|Y|$的自由 Abel 群。[提示：$\{xF' \mid x \in X\}$ 是F/F'的一组基.]。

(*c*) $F \cong G \Longleftrightarrow |X| = |Y|$。[提示：如果$\varphi$：$F \cong G$，则 φ 诱导出同构 $F/F' \cong G/G'$。利用命题1.3和(*b*)。反过来则是定理I.7.8.]

2. 有限生成 Abel 群

开始我们先证明关于有限生成 Abel 群的两个不同的结构定理。然后由唯一性定理（2.6）推出，每个结构定理均提供一给定群的数值不变量集合（即：两个群有同样的不变量集合当且仅当它们是同构的）。因此，每个结构定理都导致全部有限生成 Abel 群完全的同构分类.象第 1 节一样，所有的群均记成加法。本节中的许多结果都可以推广到某些非有限生成的 Abel 群上（虽然证明可能完全不同），见L.Fuchs[13]或者I.Kaplansky[17]。

这里证明的所有结构定理都是主理想整环上有限生成模相应定理（第IV.6）的特殊情形。可能有些读者更愿意使用第IV.6节

的证明方法来代替这里所采用的方法，因为这里的方法在很大程度上依赖于定理1.6。

定理2.1 每个有限生成 Abel 群G均是(同构于)一些循环群的有限直和，并且这些循环群中如果有一些是有限的，总可以使它们的阶是m_1，m_2，…，m_t，其中$m_1>1$同时$m_1|m_2|\cdots|m_t$。

证明 如果$G\neq 0$，并且G是由n个元素所生成的，则根据定理1.4，存在秩n的自由Abel群F和满同态$\pi: F\to G$。如果π是同构，则$G\cong F\cong \mathbf{Z}\oplus\cdots\oplus\mathbf{Z}$($n$个直和成分)。不然，则由定理1.6可知，存在$F$的一组基$\{x_1, \cdots, x_n\}$和正整数$d_1$，…，$d_r$，使得$1\leqslant r\leqslant n$，$d_1|d_2|\cdots|d_r$，并且$\{d_1x_1, \cdots, d_rx_r\}$是$K=\mathrm{Ker}\pi$的一组基。现在

$F=\sum_{i=1}^{n}\langle x_i\rangle$，$K=\sum_{i=1}^{r}\langle d_ix_i\rangle$，其中$\langle x_i\rangle\cong\mathbf{Z}$，并且在同一个同构之下$\langle d_ix_i\rangle\cong d_i\mathbf{Z}=\{d_iu\,|\,u\in\mathbf{Z}\}$。对于$i=r+1$，$r+2$，…，$n$，令$d_i=0$，于是$K=\sum_{i=1}^{n}\langle d_ix_i\rangle$。然后由系I.5.7，I.5.8和I.8.11可知

$$G\cong F/K=\sum_{i=1}^{n}\langle x_i\rangle/\sum_{i=1}^{n}\langle d_ix_i\rangle\cong\sum_{i=1}^{n}\langle x_i\rangle/\langle d_ix_i\rangle$$

$$\cong\sum_{i=1}^{n}\mathbf{Z}/d_i\mathbf{Z}.$$

如果$d_i=1$，则$\mathbf{Z}/d_i\mathbf{Z}=\mathbf{Z}/\mathbf{Z}=0$；如果$d_i>1$，则$\mathbf{Z}/d_i\mathbf{Z}\cong Zd_i$；如果$d_i=0$，则$\mathbf{Z}/d_i\mathbf{Z}=\mathbf{Z}/0\cong\mathbf{Z}$。令$m_1$，…，$m_t$是诸$d_i$中不等于0和1的那些数(并且排列次序保持不变)，以s表示等于0的d_i之个数，则

$$G\cong Z_{m_1}\oplus\cdots\oplus Z_{m_t}\oplus(\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}),$$

其中$m_1>1$，$m_1|m_2|\cdots|m_t$，而$(\mathbf{Z}\oplus\cdots\oplus\mathbf{Z})$的秩为$s$。 ∎

定理2.2 每个有限生成 Abel 群 G均是(同构于)循环群的有限直和，这些循环群或者是无限的，或者阶为素数幂。

证明概要 本定理是定理2.1和下一引理的直接推论。习题4扼要的给出另一证明。 ∎

引理2.3 如果m是正整数，$m=p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$($p_1,\cdots,p_t$ 是不同的素数且每个$n_i>0$)，则 $Z_m\cong Z_{P_1^{n_1}}\oplus Z_{P_2^{n_2}}\oplus\cdots\oplus Z_{P_t^{n_t}}$。

证明概要 对于m的素因子个数t作数学归纳法，同时利用事实

$$Z_{rn}=Z_r\oplus Z_n \quad (\text{如果}(r,n)=1)$$

即可证明。现在证明后一事实：元素 $n=n1\in Z_n$ 的 阶 为 r (定理 I.3.4(vii))，从而$Z_r\cong\langle n1\rangle<Z_{rn}$，并且映射$\psi_1$：$Z_r\longrightarrow Z_{rn}$，$k\longmapsto nk$是单同态。类似地，映射$\psi_2$：$Z_n\longrightarrow Z_{rn}$，$k\longmapsto rk$也是单同态。从定理 I.8.5 的证明可知，映射 ψ：$Z_r\oplus Z_n\longrightarrow Z_{rn}$，$(x,y)\longmapsto\psi_1(x)+\psi_2(y)=nx+ry$ 是同态。由于$(r,n)=1$，存在$a,b\in\mathbf{Z}$，使得 $ra+nb=1$ (引论中定理6.5)。于是对每个 $k\in Z_{rn}$，$k=rak+nbk=\psi(bk,ak)$，即ψ是满同态。因为$|Z_r\oplus Z_n|=rn=|Z_{rn}|$，从而$\psi$必定为单同态。 ∎

系2.4 如果G是n阶有限 Abel 群，则对于每个正整数$m|n$，G均有m阶子群。

证明概要 利用定理2.2和以下两个事实：

(i) $G\cong\sum_{i=1}^{k}G_i\Rightarrow|G|=|G_1||G_2|\cdots|G_k|$；

(ii) 由下面的引理2.5(V)可知当 $i \leqslant r$ 时，$p^{r-i} Z_{p^r} \cong Z_{p^i}$。∎

注记：如果G不是Abel群，则系2.4可能不成立(习题I.6.8)。

下面在定理2.6中，我们要证明定理2.1和2.2的直和分解中诸循环子群的阶数实际上是由群 G所唯一决定的。为此，我们首先要收集一些关于Abel群各种各样的事实，这些事实在证明中将会用到。

引理2.5 假设G是Abel 群，m 为整数而p是素数。则下面四个均是G的子群：

(i) $mG = \{mu \mid u \in G\}$

(ii) $G[m] = \{u \in G \mid mu = 0\}$

(iii) $G(p) = \{u \in G \mid |u| = p^n$，对于某个$n \geqslant 0\}$。

(iv) $G_t = \{u \in G \mid |u|$有限$\}$

特别地，存在着下面一些同构：

(v) $Z_{p^n}[p] \cong Z_p (n \geqslant 1)$，$p^m Z_{p^n} \cong Z_{p^{n-m}} (m < n)$。

假定H和$G_i (i \in I)$均是Abel群。

(vi) 如果 g：$G \to \sum_{i \in I} G_i$是同构，则 g在mG和$G[m]$上的限制分别是同构$mG \cong \sum_{i \in I} mG_i$ 和$G[m] \cong \sum_{i \in I} G_i[m]$。

(vii) 如果f：$G \to H$ 是同构，则 f在G_t和$G(p)$上的限制分别是同构$G_t \cong H_t$和$G(p) \cong H(p)$。

证明概要 (i)—(iv)作为练习。其中G为Abel群这一假设是本质性的 (S_3给出(i)—(iii) 的反例，而习题I.3.5给出 (iv)的反例)。

(v) 根据定理 I.3.4(vii)，$p^{n-1} \in Z_{p^n}$ 的阶数是 p，从而 $\langle p^{n-1} \rangle \cong Z_p$ 并且$\langle p^{n-1} \rangle < Z_{p^n}[p]$。如果 $u \in Z_{p^n}[p]$，则在Z_{p^n}中pu

$=0$，从而在$\mathbb{Z}$中$pu\equiv 0(\mathrm{mod}p^n)$。但是$p^n\mid pu$推出$p^{n-1}\mid u$。因此在$Z_{p^n}$中$u\in\langle p^{n-1}\rangle$，从而$Z_{p^n}[p]<\langle p^{n-1}\rangle$ 对于第二个论断，注意由定理1.3.4(vii)可知$p^m\in Z_{p^n}$的阶数为p^{n-m}。因此 $p^mZ_{p^n}=\langle p^m\rangle\cong Z_{p^{n-m}}$。

(vi)作为练习。

(vii) 如果$f: G\to H$ 是同态而 $x\in G(p)$ 的阶数为 p^n，则$p^nf(x)=f(p^nx)=f(0)=0$。因此$f(x)\in H(p)$。从而$f: G(p)\to H(p)$。如果f是同构，则同样的推理表明 $f^{-1}: H(p)\to G(p)$。由于$ff^{-1}=1_{H(P)}$，因此$G(p)\cong H(p)$。(vii)的另一个论断可类似证明。 ∎

如果G是Abel群，则引理2.5中定义的子群G_t叫作G的扭子群。如果$G=G_t$，则G叫作扭群。如果 $G_t=0$，则G叫作无扭的。关于所有可数扭群的完全分类，可见I.Kaplansky[17]。

定理2.6 假设G是有限生成Abel群。则

(i) 存在唯一的非负整数s，使得将G 任意分解成循环群直和时，其无限循环群直和成分的个数均恰好是s。

(ii) 或者 G 是自由Abel群，或者存在唯一的一组(不必不同的)正整数$m_1,\cdots,m_t$，使得$m_1>1$，$m_1\mid m_2\mid\cdots\mid m_t$，并且

$$G\cong Z_{m_1}\oplus Z_{m_2}\oplus\cdots\oplus Z_{m_t}\oplus F$$

其中F是自由Abel群。

(iii) 或者G是自由 Abel 群，或者存在一组正整数 $p_1^{s_1},\cdots,p_k^{s_k}$，它不计次序是唯一的，使得 $p_1,\cdots,p_k$ 是(不必不同的)素数而$S_1,\cdots,S_k$是(不必不同的)正整数，并且

$$G\cong Z_{p_1^{s_1}}\oplus Z_{p_2^{s_2}}\oplus\cdots\oplus Z_{p_k^{s_k}}\oplus F$$

其中F是自由Abel群。

证明 (i) 将G任意分解成循环群的直和（定理2.1保证至少存在这样一个分解），均得到一个同构 $G\cong H\oplus F$，其中 H 是有限循环群的直和(可能是0)，而F是自由Abel群，其秩恰好是该分解中无限循环直和成分的个数 s。如果 l：$H\to H\oplus F$ 是正则嵌入 ($h\longmapsto(h,0)$)，显然$l(H)$是$H\oplus F$的扭子群。根据引理2.5，在同构 $G\cong H\oplus F$ 之下，$G_t\cong l(H)$。从而由系I.5.8得到 $G/G_t\cong(F\oplus H)/l(H)\cong F$。因此，$G$的任意一种分解均导致$G/G_t$是自由 Abel群，并且它的秩是该分解中无限循环直和成分的个数 s。由于 G/G_t与每个特别的分解无关，并且根据定理1.2，G/G_t 的秩是不变量，从而s是唯一决定的。

(iii) 假设G有两个分解：

$$G\cong\sum_{i=1}^{r}Z_{n_i}\oplus F \quad 和 \quad G\cong\sum_{j=1}^{d}Z_{k_j}\oplus F',$$

其中n_i, k_j 均是素数幂（可能会出现不同的素数），F和F'是自由 Abel 群。(由定理2.2可知至少存在这样一个分解)。我们必须证明$r=d$并且（在重新排列之后）$n_i=k_i$（对于每个i)。不难看出，$\Sigma Z_{n_i}\oplus F$的扭子群是(同构于)ΣZ_{n_i}，对于另一分解有类似结果。从而由引理2.5可知 $\sum_{i=1}^{r}Z_{n_i}\cong G_t\cong\sum_{j=1}^{d}Z_{k_j}$。对于每个素数$p$，$(\Sigma Z_{n_i})(p)$显然是(同构于)$n_i$为$p$之幂的那些 Z_{n_i}的直和，对于另一分解也有类似的结果。由引理2.5可知，对每个素数p均有$(\Sigma Z_{n_i})(p)\cong(\Sigma Z_{k_j})(p)$，从而我们可以假定 $G=G_t$，并且n_i,k_j 均是一固定素数p的幂（从而$G=G(p)$)。于是我们有

$$\sum_{i=1}^{r}Z_{p^{a_i}}\cong G\cong\sum_{j=1}^{d}Z_{p^{c_j}}\quad(1\leqslant a_1\leqslant a_2\leqslant\cdots\leqslant a_r,$$

$$1 \leqslant c_1 \leqslant c_2 \leqslant \cdots \leqslant c_d).$$

我们首先证明，在群的任意两个这样的分解中，必然$r=d$。从引理2.5和G的第一分解可知

$$G[p] \cong \sum_{i=1}^{r} Z_{p^{a_i}}[p] \cong Z_p \oplus \cdots \oplus Z_p \ (r\text{个直和成分})$$

从而$|G[p]| = p^r$。对第二个分解作类似的推理可知$|G[p]| = p^d$。因此$p^r = p^d$，即$r=d$。

以$v(1 \leqslant v \leqslant r)$表示整数，使得当$i<v$时$a_i = c_i$而$a_v \neq c_v$。我们不妨假定$a_v < c_v$。由于$a_i \leqslant a_v$时 $p^{a_v} Z_{p^{a_i}} = 0$。从而由第一分解式和引理2.5给出

$$p^{a_v} G \cong \sum_{i=1}^{r} p^{a_v} Z_{p^{a_i}} \cong \sum_{i=v+1}^{r} Z_{p^{a_i - a_v}},$$

其中$a_{v+1} - a_v \leqslant a_{v+2} - a_v \leqslant \cdots \leqslant a_r - a_v$。显然它至多有 $r-(v+1)+1 = r-v$个非零直和成分。类似地，由于 $i<v$时$a_i = c_i$，而$a_v < c_v$，从而第二分解式给出

$$p^{a_v} G \cong \sum_{i=v}^{r} Z_{p^{c_i - a_i}},$$

其中$1 \leqslant c_v - a_v \leqslant c_{v+1} - a_v \leqslant \cdots \leqslant c_r - a_v$。显然它至少有$r-v+1$个非零直和成分。因此，若将群$p^{a_v} G$以两种方式分解成素幂阶循环群的直和，则第一分解中直和成分的个数小于第二分解中直和成分的个数。这就与前一段所证明的结论（这里用于$p^{a_v} G$）相矛盾。于是对于每个i，必然$a_i = c_i$。

(ii) 假设G有两个分解

$G \cong Z_{m_1} \oplus \cdots \oplus Z_{m_t} \oplus F$，$G \cong Z_{k_1} \oplus \cdots \oplus Z_{k_d} \oplus F'$，其中$m_1 > 1$，$m_1 | m_2 | \cdots | m_t$，$k_1 > 1$，$k_1 | k_2 | \cdots | k_d$，而$F$和$F'$是自由Abel群（由

定理2.1可知至少存在这样的一个分解)。每个m_i，k_j都有素因子分解式，通过插入形如p^0的因子，我们可以假定在所有素因子分解式中出现同样一些(彼此不同的)素数，即

$$m_1=p_1^{a_{11}}p_2^{a_{12}}\cdots p_r^{a_{1r}},\quad k_1=p_1^{c_{11}}p_2^{c_{12}}\cdots p_r^{c_{1r}}$$
$$m_2=p_1^{a_{21}}p_2^{a_{22}}\cdots p_r^{a_{2r}},\quad k_2=p_1^{c_{21}}p_2^{c_{22}}\cdots p_r^{c_{2r}}$$
$$\vdots\qquad\qquad\qquad\vdots$$
$$m_t=p_1^{a_{t1}}p_2^{a_{t2}}\cdots p_r^{a_{tr}},\quad k_d=p_1^{c_{d1}}p_2^{c_{d2}}\cdots p_r^{c_{dr}}.$$

由于$m_1|m_2|\cdots|m_t$，可知对每个j，$0\leqslant a_{1j}\leqslant a_{2j}\leqslant\cdots\leqslant a_{tj}$。类似地对每个$j$ $0\leqslant c_{1j}\leqslant c_{2j}\leqslant\cdots\leqslant c_{dj}$。由引理2.3和2.5可知

$$\sum_{i,j}Z_{p_j^{a_{ij}}}\cong\sum_{i=1}^{t}Z_{m_i}\cong G_t\cong\sum_{i=1}^{d}Z_{k_i}\cong\sum_{i,j}Z_{p_j^{c_{ij}}},$$

其中某些直和成分可能是零。由此可知对每个$j=1,2,\cdots,r$，

$$\sum_{i=1}^{t}Z_{p_j^{a_{ij}}}\cong G(p_j)\cong\sum_{i=1}^{d}Z_{p_j^{c_{ij}}}.$$

由于$m_1>1$，从而存在某个p_j，使得$1\leqslant a_{1j}\leqslant\cdots\leqslant a_{tj}$，从而$\sum_{i=1}^{t}Z_{p_j^{a_{ij}}}$有$t$个非零直和成分。由(iii)知$\sum_{i=1}^{d}Z_{p_j^{c_{ij}}}$也恰好有$t$个非零直和成分，因此$t\leqslant d$。类似地，由$k_1>1$推得$d\leqslant t$，从而$d=t$。从(iii)便知现在对每个$i,j$均要$a_{ij}=c_{ij}$。这就导致$m_i=k_i$(对于$i=1,2,\cdots,t$)。 ∎

如果G是有限生成Abel群，则在定理2.6(ii)中唯一决定的整数$m_1,\cdots,m_t$叫作G的不变因子，而在定理2.6(iii)中唯一决定的那些素数幂叫作G的初等因子。

系2.7 两个有限生成Abel群G和H同构$\Longleftrightarrow G/G_t$和$H/H_t$有

相同的秩，并且G和H有同样的不变因子(或者初等因子)。

证明作为练习。 ∎

例 全体1500阶的有限Abel群可以按下述方法完全决定（不计同构)。由于有限群 G的初等因子之积是 $|G|$，而 $1500=2^2\cdot3\cdot5^3$，从而初等因子只有以下几种可能：$\{2,2,3,5^3\}$，$\{2,2,3,5,5^2\}$，$\{2,2,3,5,5,5\}$，$\{2^2,3,5^3\}$，$\{2^2,3,5,5^2\}$和$\{2^2,3,5,5,5\}$。这六种初等因子中的每个均决定出一个1500阶 Abel 群（例如$\{2,2,3,5^3\}$决定出 $Z_2\oplus Z_2\oplus Z_3\oplus Z_{5^3}$)。由定理2.2可知，每个1500阶 Abel 群均同构于这六个群中的一个，并且由系2.7可知这六个群彼此互不同构。

如果已经知道有限生成Abel群G的不变因子$m_1,\cdots,m_t$，那末由定理2.6的证明可知，G的初等因子是由出现在 $m_1,\cdots,m_t$ 素因子分解式中的全部素数幂$p^n(n>0)$所组成。反之，如果已经知道G的初等因子，它们排列成如下的形式(必要时插入某些形如p^0的项)：

$$\begin{array}{c} p_1^{n_{11}},p_2^{n_{12}},\cdots,p_r^{n_{1r}} \\ p_1^{n_{21}},p_2^{n_{22}},\cdots,p_r^{n_{2r}} \\ \vdots \qquad\qquad \vdots \\ p_1^{n_{t1}},p_2^{n_{t2}},\cdots,p_r^{n_{tr}}. \end{array}$$

其中$p_1,\cdots,p_r$是不同的素数，并且对每个$j=1,2,\cdots,r$，$0\leqslant n_{1j}\leqslant n_{2j}\leqslant\cdots\leqslant n_{tj}$（其中有某个$n_{ij}\neq0$)，最后对某个$j$有$n_{1j}\neq0$。根据初等因子定义(定理2.6(iii))，$G\cong\sum_{i=1}^{t}\sum_{j=1}^{r}Z_{p_j^{n_{ij}}}\oplus F$，其中$F$是自由Abel群(并且$p_j^{n_{ij}}=p_j^0=1$的那些有限的直和成分是0)。对于每个$i=1,2,\cdots,t$，令$m_i=p_1^{n_{i1}}p_2^{n_{i2}}\cdots p_r^{n_{ir}}$(即$m_i$是上面排列中第$i$行之积)。因为有某个 $n_{1j}\neq0$，从而$m_1>1$。并且由上述构作方

式可知$m_1 \mid m_2 \mid \cdots \mid m_t$。由引理2.3知$G \cong \sum_{i=1}^{s}\left(\sum_{j=1}^{r} Z_{p_j^{n_{ij}}}\right) \oplus F \cong$

$\sum_{i=1}^{t} Z_{m_i} \oplus F$。从而由定理2.6(ii)便知$m_1, \cdots, m_t$是$G$的不变因子。

例 如果G是群 $Z_5 \oplus Z_{15} \oplus Z_{25} \oplus Z_{36} \oplus Z_{54}$，由引理2.3可知 $G \cong Z_5 \oplus (Z_5 \oplus Z_3) \oplus Z_{25} \oplus (Z_9 \oplus Z_4) \oplus (Z_{27} \oplus Z_2)$。从而 G 的初等因子是$2, 2^2, 3, 3^2, 3^3, 5, 5, 5^2$，它可按上面所述排列成：

$2^0,\ 3\ ,\ 5$

$2\ ,\ 3^2,\ 5$

$2^2,\ 3^3,\ 5^2$。

从而G的不变因子是 $1 \cdot 3 \cdot 5 = 15$，$2 \cdot 3^2 \cdot 5 = 90$和$2^2 \cdot 3^3 \cdot 5^2 = 2700$，因此$G \cong Z_{15} \oplus Z_{90} \oplus Z_{2700}$。

还有一个题目也应当自然地放到本节之中，这就是：对于由生成元和关系所定义的有限生成Abel群，如何决定它的结构。但是由于处理这一问题的最好办法需要运用某些矩阵技巧，我们把它放到第Vll.2节的附录中。有兴趣的读者现在就可以阅读这一材料，只有很少困难或者根本就没有任何困难。

习　题

1. 求证一个有限Abel群若不是循环群，必包含一个子群同构于$Z_p \oplus Z_p$(对于某个素数p)。
2. 假设G是有限Abel群，x是G中具有最大阶的元素。求证$\langle x \rangle$是G的一个直和成分。由此给出定理2.1的另一证明。
3. 假设G是有限Abel$p$-群(习题7)，而$x \in G$具有最大阶数。如果$\overline{y} \in G/\langle x \rangle$的阶数是$p^r$，则存在陪集$\overline{y}$的一个代表元素 $y \in G$，使得$|y| = p^r$。〔注

意如果$|x| = p^t$，则$p^tG = 0$.〕

4. 利用习题3和7给出定理2.2的一个与定理2.1无关的证明.〔提示：如果G是一个p-群，令x是其中最大阶元素．根据归纳假设，$G/\langle x\rangle$是循环群的直和：$G/\langle x\rangle \cong \langle \overline{x_1}\rangle \oplus \cdots \oplus \langle \overline{x_n}\rangle$，其中$|\overline{x_i}| = p^{r_i}$并且$1 \leqslant r_1 \leqslant r_2 \leqslant \cdots \leqslant r_n$．取$\overline{x_i}$的代表元素$x_i$，使得$|x_i| = |\overline{x_i}|$．求证$G = \langle x_1\rangle \oplus \cdots \oplus \langle x_n\rangle \oplus \langle x\rangle$即是所需的分解.〕.

5. 如果G是有限生成Abel群，并且G/G_t的秩为n，而H是G的子群，使得H/H_t的秩为m．则$m \leqslant n$，并且$(G/H)/(G/H)_t$的秩为$n-m$．

6. 令$k, m \in \mathbf{N}^*$．如果$(k,m) = 1$，则$kZ_m = Z_m$并且$Z_m[k] = 0$．如果$k|m$，令$m = kd$，则$kZ_m \cong Z_d$并且$Z_m[k] \cong Z_k$．

7. 一个(子)群如果每个元素的阶数均是某一固定素数p之幂，它便叫作p-(子)群(注意：$|0| = 1 = p^0$)．令G是Abel扭群．

   (a) $G(p)$是G的唯一极大p-子群(即：G之每个p-子群均包含在$G(p)$之中)．

   (b) $G = \Sigma G(p)$，其中求和是对所有使$G(p) \neq 0$的素数p．〔提示：如果$|u| = p_1^{n_1} \cdots p_t^{n_t}$，令$m_i = |u|/p_i^{n_i}$．于是存在$c_i \in \mathbf{Z}$，使得$c_1m_1 + \cdots + c_tm_t = 1$，从而$u = c_1m_1u + \cdots + c_tm_tu$，而$c_im_iu \in G(p_i)$.〕

   (c) 如果H是另一个Abel扭群，则$G \cong H \Longleftrightarrow$对于每个素数$p$，$G(p) \cong H(p)$．

8. 有限Abel$p$-群(习题7)是由它的全部最大阶元素所生成．

9. Abel群$Z_{p^3} \oplus Z_{p^2}$有多少个p^2阶子群？

10. (a) 设G是有限Abel p-群(习题7)．求证：对每个$n \geqslant 0$，$p^{n+1}G \cap G[p]$是$p^nG \cap G[p]$的子群．

    (b) 求证：$(p^nG \cap G[p])/(p^{n+1}G \cap G[p])$是一些$Z_p$的直和.设其直和成分的个数为$k$．

    (c) 将G写成循环群的直和．求证(b)中的数k是p^{n+1}阶直和成分的个数．

11. 设G，H和K均是有限生成Abel群．

(*a*) 如果$G\oplus G\cong H\oplus H$，则$G\cong H$。

(*b*) 如果$G\oplus H\cong G\oplus K$，则$H\cong K$。

(*c*) 如果G_1是秩$\aleph_0$的自由Abel群，则 $G_1\oplus\mathbf{Z}\oplus\mathbf{Z}\cong G_1\oplus\mathbf{Z}$，但是$\mathbf{Z}\oplus\mathbf{Z}\not\cong\mathbf{Z}$。

注意：存在着可数无限生成的无扭Abel群G，使得$G\cong G\oplus G\oplus G$，但是$G\cong G\oplus G$，从而(*a*)对于$H=G\oplus G$不成立。见A.L.S.Corner [60]。还见习题3.11，3.12和IV.3.12。

12. (*a*) $Z_2\oplus Z_9\oplus Z_{85}$的初等因子是什么？不变因子是什么？对于$Z_{26}\oplus Z_{42}\oplus Z_{49}\oplus Z_{200}\oplus Z_{1000}$回答同样的问题。

(*b*) 不计同构决定所有的64阶Abel群。对于96阶作同样的问题。

(*c*) 决定所有阶数$\leqslant 20$的Abel群。

13. 求证$Z_m\oplus Z_n$的不变因子是(m,n)和$[m,n]$（最大公因数和最小公倍数）（当$(m,n)>1$时）或者mn（当$(m,n)=1$时）。

14. 如果H是有限Abel群G的子群，则G有子群同构于G/H。

15. $\mathbf{Q}/\mathbf{Z}$中每个有限子群都是循环群。〔见习题I.3.7和7.〕

3. Krull-Schmidt定理

群$\boldsymbol{Z}$和$\boldsymbol{Z}_{p^n}$(p为素数）均是不可分解的，这意味着它们都不是两个真子群的直和(习题 I.8.1)。从而定理2.2和2.6(iii) 可以重述为：每个有限生成Abel群都是有限个不可分解群的直和，并且这些不可分解的直和成分不计同构是唯一决定的。现在我们要将此结果推广到一大批(不必Abel的)群上去[1]。

在本章其余部分，我们又对于任意群恢复使用乘法记号。

---

1. 本节的结果今后是不需要的。

定义3.1 群G叫作不可分解的，如果$G\neq\langle e\rangle$并且G不是它的两个真子群的(内)直积.

因此，G是不可分解的$\Leftrightarrow G\neq\langle e\rangle$，并且$G\cong H\times K$导致$H=\langle e\rangle$或者$K=\langle e\rangle$(习题1).

例 每个单群(例如A_n，$n\neq 4$)都是不可分解的. 但是不可分解群不必是单群：$\boldsymbol{Z}$，$\boldsymbol{Z}_{p^n}$(p为素数)和S_n均是不可分解的，但都不是单群(习题2和I.8.1).

定义3.2 群G叫作满足[正规]子群的升链条件(ACC)，是指对于G的每个[正规]子群链$G_1<G_2<\cdots$，均存在一个整数n，使得当$i\geqslant n$时$G_i=G_n$. G叫作满足[正规]子群的降链条件(DCC)，是指对于G的每个[正规]子群链$G_1>G_2>\cdots$，均存在一个整数n，使得当$i\geqslant n$时$G_i=G_n$.

例 每个有限群都同时满足上述两个链条件. $\boldsymbol{Z}$满足升链条件但不满足降链条件(习题5). $Z(p^\infty)$满足降链条件但不满足升链条件(习题13).

定理3.3 如果群G满足正规子群的升链或者降链条件，则G是有限多个不可分解子群的直积.

证明概要 假设G不是有限个不可分解子群的直积. 令$S=\{H\mid H\lhd G$，H是G的直积因子(即存在G的某个子群T_H，使得$G=H\times T_H$)，并且H不是有限个不可分解子群的直积$\}$. 显然$G\in S$. 如果$H\in S$，则H不是不可分解的，从而H存在真子群K_H和J_H，使得$H=K_H\times J_H(=J_H\times K_H)$. 进而，这两个真子群之一(假定是$K_H$)必然属于$S$(特别地，由习题I.8.12可知$K_H\lhd G$). 令$f$：$S\to S$是映射$f(H)=K_H$. 由引论中的递归定理6.2(对于每个$n$均

取$f_n=f$)，可知存在函数φ：$\mathbf{N}\to S$，使得

$\varphi(0)=G$，并且$\varphi(n+1)=f(\varphi(n))=K_{\varphi(n)}(n\geqslant 0)$。如果用$G_n$表示$\varphi(n)$，则我们有$G$的一列子群$G_0$，$G_1$，$G_2$，…(所有这些子群均在$S$中)，使得

$$G=G_0,\ G_1=K_{G_0};\ G_2=K_{G_1};\ \cdots,\ G_{n+1}=K_{G_n};\ \cdots$$

由构造方式可知每个G_i均在G中正规，并且

$$G\supsetneqq G_1\supsetneqq G_2\supsetneqq G_3\supsetneqq\cdots.$$

如果G满足正规子群的降链条件，这就导致矛盾。进而，按部就班地用数学归纳法可以证明，对于每个$n\geqslant 1$，$G=G_n\times J_{G_{n-1}}\times J_{G_{n-2}}\times\cdots\times J_{G_0}$，其中每个$J_{G_i}$都是$G$的真子群。因此存在着正规子群的真升链：

$$J_{G_0}\subsetneqq J_{G_1}\times J_{G_0}\subsetneqq J_{G_2}\times JG_1\times J_{G_0}\subsetneqq\cdots.$$

如果G满足正规子群的升链条件，这又导致矛盾。 ∎

为了决定在什么条件下定理 3.3 中的分解是唯一的，我们需要一些定义和引理。群G的自同态f叫作正规自同态，是指对于所有a，$b\in G$，$af(b)a^{-1}=f(aba^{-1})$。

引理3.4 假设群G满足正规子群的升[降]链条件，而f是G的[正规]自同态。则f为自同构$\Longleftrightarrow f$为满同态[单同态]。

证明 假设G满足ACC而f为满同态。则正规子群的升链$\langle e\rangle<\mathrm{Ker}f<\mathrm{Ker}f^2<\cdots$（其中$f^k=ff\cdots f$）必然变成常链，即必然有$\mathrm{Ker}f^n=\mathrm{Ker}f^{n+1}$。由于$f$是满同态，从而$f^n$也是满同态。如果$a\in G$而$f(a)=e$，则有$b\in G$使$a=f^n(b)$并且$e=f(a)=f^{n+1}(b)$。从而$b\in\mathrm{Ker}f^{n+1}=\mathrm{Ker}f^n$，这又导致$a=f^n(b)=e$。从而$f$是单同态，即$f$是自同构。

假设G满足DCC并且f是单同态。对于每个$k\geqslant 1$，$\mathrm{Im}f^k$是G的

正规子群，这是因为f是正规自同态。从而降链$G>\mathrm{Im}f>\mathrm{Im}f^2>\cdots$必然变成常链，即必然有$\mathrm{Im}f^n=\mathrm{Im}f^{n+1}$。从而对于每个$a\in G$，均有$b\in G$使得$f^n(a)=f^{n+1}(b)$。由于$f$为单同态，从而$f^n$也是单同态，于是 $f^n(a)=f^{n+1}(b)=f^n(f(b))$导致 $a=f(b)$。于是f为满同态，即为自同构。 ∎

引理3.5 (Fitting) 如果群G同时满足正规子群的升链和降链条件，而f是G 的正规自同态，则存在某个 $n\geqslant 1$，使得$G=\mathrm{Ker}f^n\times\mathrm{Im}f^n$。

证明 由于f是正规自同态，从而每个$\mathrm{Im}f^k$ $(k\geqslant 1)$ 均在G中正规。于是我们有两个正规子群链：

$G>\mathrm{Im}f>\mathrm{Im}f^2>\cdots$和$\langle e\rangle<\mathrm{Ker}f<\mathrm{Ker}f^2<\cdots$

根据假设，存在n使得对每个$k\geqslant n$均有$\mathrm{Im}f^k=\mathrm{Im}f^n$和$\mathrm{Ker}f^k=\mathrm{Ker}f^n$，假设 $a\in\mathrm{Ker}f^n\cap\mathrm{Im}f^n$。则存在 $b\in G$使得$a=f^n(b)$并且$f^{2n}(b)=f^n(f^n(b))=f^n(a)=e$。从而$b\in\mathrm{Ker}f^{2n}=\mathrm{Ker}f^n$，于是 $a=f^n(b)=e$。因此$\mathrm{Ker}f^n\cap\mathrm{Im}f^n=\langle e\rangle$。对于任一 $c\in G$，$f^n(c)\in\mathrm{Im}f^n=\mathrm{Im}f^{2n}$，从而有$d\in G$，$f^n(c)=f^{2n}(d)$。因此$f^n(cf^n(d^{-1}))=f^n(c)f^{2n}(d^{-1})=f^n(c)f^{2n}(d)^{-1}=f^n(c)f^n(c)^{-1}=e$，于是$cf^n(d)^{-1}\in\mathrm{Ker}f^n$。由于$c=(cf^n(d^{-1}))f^n(d)$，从而$G=(\mathrm{Ker}f^n)(\mathrm{Im}f^n)$。因此由定义I.8.8便知$G=\mathrm{Ker}f^n\times\mathrm{Im}f^n$。 ∎

群G的自同态f 叫作幂零的，是指存在一个正整数n，使得对每个$g\in G$，$f^n(g)=e$。

系3.6 如果G是不可分解群，并且同时满足正规子群的升链和降链条件，又f为G 的正规自同态，则或者f 是幂零的，或者f是自同构。

证明 由Fitting引理，存在某个$n\geqslant 1$，使得 $G=\mathrm{Ker}f^n\times \mathrm{Im}f^n$。由于$G$是不可分解的，从而或者$\mathrm{Ker}f^n=\langle e\rangle$，或者$\mathrm{Im}f^n=\langle e\rangle$。后者导致$f$是幂零的。如果 $\mathrm{Ker}f^n=\langle e\rangle$，则$\mathrm{Ker}f=\langle e\rangle$，从而$f$是单同态，于是由引理3.4可知$f$是自同构。 ∎

如果f和g均是群G的自同态，我们以 $f+g$表示函数 $G\to G$，$a\longmapsto f(a)g(a)$。$f+g$ 一般不必是自同态（习题7）。但是易知运算$+$是满足结合律的，从而G上的所有自同态〔注〕所构成的集合对于$+$是一个幺半群（幺元素是自同态O_G：$G\longrightarrow G$，$a\longmapsto e$（对任意$a\in G$））。

系3.7 假设$G(\neq\langle e\rangle)$是不可分解群，并且同时满足正规子群的升链和降链条件。如果f_1，…，f_n是G的正规幂零自同态，使得每个 $f_{i_1}+\cdots+f_{i_r}$ $(1\leqslant i_1<i_2<\cdots<i_r\leqslant n)$ 均是自同态，则$f_1+f_2+\cdots+f_n$是幂零的。

证明概要 由于每个$f_{i_1}+\cdots+f_{i_r}$都是自同态，从而都是正规的（习题8(c)）。于是只要对于情形$n=2$证明了定理，则整个证明即可利用数学归纳法得到。如果 f_1+f_2 非幂零，由系3.6可知它是自同构。验证f_1+f_2的逆g也是正规自同态。如果$g_1=f_1g$，$g_2=f_2g$，则$1_G=g_1+g_2$，并且对于每个 $x\in G$，$x^{-1}=(g_1+g_2)(x^{-1})=g_1(x^{-1})g_2(x^{-1})$。于是 $x=[g_1(x^{-1})g_2(x^{-1})]^{-1}=g_2(x)g_1(x)=(g_2+g_1)(x)$，从而$1_G=g_2+g_1$。因此$g_1+g_2=g_2+g_1$，于是 $g_1(g_1+g_2)=g_1 1_G=1_G g_1=(g_1+g_2)g_1$，这又导致 $g_1g_2=g_2g_1$。现在即可递归证明：对每个$m\geqslant 1$，

$$(g_1+g_2)^m=\sum_{i=0}^{m}c_i g_1^i g_2^{m-i}(c_i\in\mathbf{Z})。$$

〔注〕：应当是“所有函数$G\longrightarrow G$” ——译者注

其中 c_i 是二项系数（见定理III.1.6），而 $c_i h$ 意味着 $h+h+\cdots+h$（c_i个）。由于每个f_i均幂零，从而$g_i=f_i g$有非平凡的核，由系3.6又推出g_i也幂零。对此对于充分大的m和所有 $a\in G$，$(g_1+g_2)^m(a)=\sum_{i=0}^{m} c_i g_1^i g_2^{m-i}(a)=\prod_{i=0}^{m} e^{c_i}=e$。但这与$g_1+g_2=1_G$以及$G\neq\langle e\rangle$这些事实相矛盾。∎

下面一个定理将使用如下的事实：如果群G是它的子群 $G_1\cdots$，G_S 的内直积，则由定理I.8.6 的证明可知存在同构φ：$G_1\times\cdots\times G_S\cong G$，$(g_1,\ \cdots,\ g_S)\longmapsto g_1g_2\cdots g_S$。因此，$G$的每个元素均可以唯一地写成乘积$g_1g_2\cdots g_S$ $(g_i\in G_i)$。对于每个i，映射π_i：$G\longrightarrow G_i$，$g_1g_2\cdots g_S\longmapsto g_i$是满同态（它是 φ^{-1}与正则射影 $G_1\times\cdots\times G_S\to G_i$之合成）。我们将把映射$\pi_i$看成是结合于内直积$G=G_1\times\cdots\times G_S$的正则满同态。

定理3.8 （Krull—Schmidt） 假设群G同时满足正规子群的升链和降链条件。如果$G=G_1\times G_2\times\cdots\times G_S$和$G=H_1\times H_2\times\cdots\times H_t$，其中$G_i$和$H_j$均是不可分解的，则$s=t$，并且在重新标记之后，对于每个$i$均有$G_i\cong H_i$，而对于每个$r<t$均有

$$G=G_1\times\cdots\times G_r\times H_{r+1}\times\cdots\times H_t.$$

注记：根据定理3.3可知G至少有一个这样的分解。此外，这里的唯一性命题比简单地说“不可分解因子不计同构是唯一决定的”要强。

定理3.8证明概要 令 $P(0)$是命题：$G=H_1\times\cdots\times H_t$。对于$1\leqslant r\leqslant min(s,\ t)$，令$P(r)$ 为命题：可以将H_1，…，H_t 重新标记，使得 $G_i\cong H_i$ $(1\leqslant i\leqslant r)$ 并且 $G=G_1\times\cdots\times G_r\times H_{r+1}\times\cdots\times H_t$（或者 $G=G_1\times\cdots\times G_t$，如果 $r=t$）。我们要归纳证明：对于

满足$0\leqslant r\leqslant min\ (s,\ t)$ 的所有r，$P(r)$ 均是对的。由假设可知$P(0)$是对的。现在假设$P(r-1)$是对的，即在重新标记之后，我们有$G_i\cong H_i$ $(1\leqslant i\leqslant r-1)$并且$G=G_1\times\cdots\times G_{r-1}\times H_r\times\cdots\times H_t$。令$\pi_1$，…，$\pi_S[\pi'_1$，…，$\pi'_t]$是结合于内直积

$$G=G_1\times\cdots\times G_S[G=G_1\times\cdots\times G_{r-1}\times H_r\times\cdots\times H_t]$$

的正则满同态（如在本定理之前的一段所述）。令$\lambda_i[\lambda'_i]$是将第i因子映到G的包含映射。对于每个i，令$\varphi_i=\lambda_i\pi_i$：$G\longrightarrow G$，$\psi_i=\lambda'_i\pi'_i$：$G\longrightarrow G$。验证下面一些恒等式成立：

$$\varphi_i\,|G_i=1_{G_i},\ \varphi_i\varphi_i=\varphi_i,\ \varphi_i\varphi_j=O_G(i\neq j)^{2},$$

$$\psi_1+\cdots+\psi_t=1_G,\ \psi_i\psi_i=\psi_i,\ \psi_i\psi_j=O_G(i\neq j),$$

$$\mathrm{Im}\varphi_i=G_i,\ \mathrm{Im}\psi_i=G_i(i<r),\ \mathrm{Im}\psi_i=H_i(i\geqslant r)。$$

由此可知对所有$i<r$均有$\varphi_r\psi_r=O_G$（因为$\psi_i(x)\in G_i$，从而$\varphi_r\psi_i(x)=\varphi_r1_{G_i}\psi_i(x)=\varphi_r\varphi_i\psi_i(x)=e$）。

上面这些恒等式表明$\varphi_r=\varphi_r1_G=\varphi_r(\psi_1+\cdots+\psi_t)=\varphi_r\psi_r+\cdots+\varphi_r\psi_t$。彼此不同的$\varphi_r\psi_i$之“和”均是正规自同态（习题8，9）。由于$\varphi_r\,|\,G_r=1_G$是$G_r$的（正规）自同态，并且$G_r$同时满足正规子群的升链和降链条件（习题6），系3.6和3.7导致$\varphi_r\psi_j|\,G_r$是$G_r\neq\langle e\rangle$的自同构（对于某个j $(r\leqslant j\leqslant t)$）。因此，对于每个$n\geqslant1$，$(\varphi_r\psi_j)^{n+1}$也是$G$的自同构。由于$G_r\neq\langle e\rangle$并且$(\varphi_r\psi_j)^{n+1}=\varphi_r(\psi_j\varphi_r)^n\psi_j$（对每个$n\geqslant1$），从而正规自同态$\psi_j\varphi_r|\,H_j:H_j\longrightarrow H_j$不可能幂零。由于$H_j$满足两个链条件（习题6），由系3.7可知$\psi_j\varphi_r|\,H_j$必然是$H_j$的自同构。因此$\psi_j|\,G_r:G_r\to H_j$是同构，并且$\varphi_r|\,H_j:H_j\to G_r$也是同构。重新标记$H_k$，使我们可设$j=r$并且$G_r\cong H_r$。于是我们证明了命题$P(r)$的前半部分。

2.见系3.7的前面一段。

由于 $G=G_1\times\cdots\times G_{r-1}\times H_r\times\cdots\times H_t$（归纳假设），子群$G_1G_2\cdots G_{r-1}H_{r+1}\cdots H_t$是内直积 $G_1\times\cdots\times G_{r-1}\times H_{r+1}\times\cdots\times H_t$。注意对于$j<r,\psi_r(G_j)=\psi_r\psi_j(G)=\langle e\rangle$而对于 $j>r,\psi_r(H_j)=\psi_r\psi_j(G)=\langle e\rangle$，从而$\psi_r\ (G_1\cdots G_{r-1}H_{r+1}\cdots H_t)=\langle e\rangle$。由于 $\psi_r|G_r$是同构，我们必须有 $G_r\cap(G_1\cdots G_{r-1}H_{r+1}\cdots H_t)=\langle e\rangle$。于是群 $G^*=G_1\cdots G_{r-1}G_rH_{r+1}\cdots H_t$是内直积：

$$G^*=G_1\times\cdots\times G_r\times H_{r+1}\times\cdots\times H_t。$$

如下定义映射θ：$G\to G$，每个元素$g\in G$均可以写成 $g=g_1\cdots g_{r-1}h_r\cdots h_t$，其中 $g_i\in G_i$，$h_j\in H_j$。令 $\theta(g)=g_1\cdots g_{r-1}\varphi_r(h_r)h_{r+1}\cdots h_t$。显然 $\mathrm{Im}\theta=G^*$。θ是单同态（见定理I.8.10），并且易知它是正规自同态。从而由引理3.4可知θ是自同构，于是 $G=\mathrm{Im}\theta=G^*=G_1\times\cdots\times G_r\times H_{r+1}\times\cdots\times H_t$。这就证明了$P(r)$的后半部分，也就完成了全部归纳推理。因此，在重新标记之后，我们有$G_i\cong H_i$ $(0\leqslant i\leqslant\min(s,t))$。如果 $\min(s,t)=s$，则 $G_1\times\cdots\times G_S=G=G_1\times\cdots\times G_S\times H_{S+1}\times\cdots\times H_t$，如果$\min(s,t)=t$，则$G_1\times\cdots\times G_s=G=G_1\times\cdots\times G_t$。由于$G_i\neq\langle e\rangle$，$H_j\neq\langle e\rangle$（对所有的$i,j$），从而不论在哪种情形下，都必需$s=t$。∎

习　题

1. 群G是不可分解的$\Longleftrightarrow G\neq\langle e\rangle$，并且由$G\cong H\times K$推得$H=\langle e\rangle$或者$K=\langle e\rangle$；
2. $n\geqslant2$时S_n是不可分解的.〔提示：如果$n\geqslant5$，则定理I.6.8，I.6.10和习题I.8.7可能是有帮助的.〕
3. 加法群$\mathbf{Q}$是不可分解的。
4. 不可分解群的非平凡同态象不一定是不可分解的。

5. (*a*) **Z**满足子群的ACC，但是不满足DCC。

(*b*) 每个有限生成Abel群都满足子群的ACC。

6. 设H，K是群G的正规子群，并且$G=H\times K$。

(*a*) 如果$N\lhd H$，则$N\lhd G$（比较习题I.5.10）。

(*b*) 如果G满足正规子群的ACC或者DCC，则H和K亦然。

7. 如果f和g是群G的自同态，则$f+g$不必为自同态。〔提示：令 $a=(123)$，$b=(132)\in S_8$，定义$f(x)=axa^{-1}$，$g(x)=bxb^{-1}$。〕

8. 假设f和g是群G的正规自同态。则

(*a*) fg为正规自同态。

(*b*) $H\lhd G$导致$f(H)\lhd G$。

(*c*) 如果$f+g$是自同态，则它必正规。

9. 令$G=G_1\times\cdots\times G_n$。对于每个$i$，令$\lambda_i:G_i\longrightarrow G$为包含映射，而$\pi_i:G\longrightarrow G_i$为正则射影（见第130页）。令$\varphi_i=\lambda_i\pi_i$。则任意$k(1\leqslant k\leqslant n)$个不同的$\varphi_i$之"和"$\varphi_{i_1}+\cdots+\varphi_{i_k}$都是$G$的正规自同态。

10. 利用 Krull-Schmidt 定理，对于有限 Abel 群证明定理 2.2 和定理2.6 (iii)。

11. 如果G和H是群，使得$G\times G=H\times H$，而G同时满足正规子群的 *ACC* 和*DCC*，则$G\cong H$〔见习题2.11〕。

12. 如果G，H，K和J是群，使得$G\cong H\times K$并且$G\cong H\times J$，而G 同时满足正规子群的ACC和DCC，则$K\cong J$〔见习题2.11〕。

13. 对于每个素数p，群$Z(p^\infty)$满足子群的降链条件，但是不满足升链条件〔见习题I.3.7〕。

4. 群在集合上的作用

本节中所谈的技巧将在下一节用于继续深入研究（非 Abel有

限）群的结构定理。

定义4.1 群G叫作作用于集合S上，是指存在一个函数$G\times S\longrightarrow S$（通常表示成$(g, x)\longmapsto gx$），使得对每个$x\in S$和$g_1$，$g_2\in G$，

$$ex=x,\ (g_1g_2)x=g_1(g_2x).$$

群G在一个给定集合S上可能有许多不同的作用方式，因此记号gx有些含混。但是在上下文中这不会产生任何困难。

例 对称群S_n在集合$I_n=\{1, 2, \cdots, n\}$上的作用由$(\sigma, x)\longmapsto\sigma(x)$给出。

例 令G是群而H是它的子群。群H在集合G上的作用由$(h, x)\longmapsto hx$给出，其中hx是G中的乘积。$h\in H$在G上的这种作用叫作(左)平移。如果K是G的另一个子群，而S是K在G中全体左陪集组成的集合，则H在S上的作用由平移：$(h, xK)\longmapsto hxK$给出。

例 令H是群G的子群。H在集合G上的作用由$(h, x)\longmapsto hxh^{-1}$给出。为了避免与$G$的乘积相混淆，$h\in H$的这个作用永远表示成$hxh^{-1}$而不是$hx$。$h\in H$在$G$上的这个作用叫作是用$h$作共轭，而元素$hxh^{-1}$叫作$x$的共轭元素。如果$K$是$G$的任一子群而$h\in H$，则$hKh^{-1}$是$G$中同构于$K$的子群（习题I.5.6）。从而$H$由共轭作用于$G$的全体子群所组成的集合$S$上：$(h, K)\longmapsto hKh^{-1}$。群$hKh^{-1}$叫作$K$的共轭子群。

定理4.2 假定群G作用于集合S上。

(i) S上由

$$x\sim x'\Longleftrightarrow gx=x'\ (\text{对于某个}g\in G)$$

定义的关系是等价关系。

(ii) 对于每个$x\in S$，$G_x=\{g\in G\mid gx=x\}$是G的子群。

证明作为练习。 ∎

定理4.2 (i) 中所给等价关系的等价类叫作G在S上的轨道[3]。$x\in S$的轨道表示成$\bar{x}$。子群G_x叫作x的固定子群。或者叫作固定x的子群等等。

例 如果群G共轭作用于自身之上，则$x\in G$的轨道$\{gxg^{-1}\mid g\in G\}$叫作x的共轭类。如果子群H共轭作用于G上，固定子群$H_x=\{h\in H\mid hxh^{-1}=x\}=\{h\in H\mid hx=xh\}$叫作$x$在$H$中的中心化子，并且表示成$C_H(x)$。如果$H=G$，则$C_G(x)$简称为$x$的中心化子。如果$H$共轭作用于$G$的全体子群所组成的集合$S$上，则$H$之固定$K\in S$的子群，即$\{h\in H\mid hKh^{-1}=K\}$叫作$K$在$H$中的正规化子，表示成$N_H(K)$。群$N_G(K)$则简称为$K$的正规化子。每个子群$K$显然在$N_G(K)$中正规。而$K\lhd G\Longleftrightarrow N_G(K)=G$。

定理4.3 如果群G作用于集合S之上，则$x\in S$的轨道的势等于指数$[G:G_x]$。

证明 令g，$h\in G$。由于

$$gx=hx\Longleftrightarrow g^{-1}hx=x\Longleftrightarrow g^{-1}h\in G_x\Longleftrightarrow hG_x=gG_x.$$

从而由$gG_x\longmapsto gx$给出的映射可定义出由G_x在G中的全体陪集所组成的集合到轨道$\bar{x}=\{gx\mid g\in G\}$之上的一一对应。因此$[G:G_x]=|\bar{x}|$。 ∎

系4.4 令G是有限群而K是G的子群。

3.这与我们前面在证明定理 I.6.3中采用的术语轨道是一致的，那里是一种特殊情形，即考虑S_n的循环子群$\langle\sigma\rangle$在集合I_n上的作用。

(i) $x\in G$的共轭元素个数等于$[G:C_G(x)]$，并且此数是$|G|$的因子。

(ii) 如果$\bar{x}_1$，…，$\bar{x}_n$ ($x_i\in G$) 是G的全部不同的共轭类，则

$$|G|=\sum_{i=1}^{n}[G:C_G(x_i)]$$

(iii) G中共轭于K的子群的个数是$[G:N_G(K)]$，并且此数是$|G|$的因子。

证明 (i) 和(iii) 由上一定理和Lagrange 定理I.4.6直接推出。由于共轭是G上的等价关系 (定理4.2)，G是共轭类$\bar{x}_1$，…，$\bar{x}_n$的非交并，从而由(i)即得出(ii)。 ∎

系4.4(ii)中的方程$|G|=\sum_{i=1}^{n}[G:C_G(x_i)]$叫作有限群$G$的类方程。

定理4.5 如果群G作用于集合S之上，则此作用诱导出一个同态$G\longrightarrow A(S)$，其中$A(S)$是S的全体置换所构成的群。

证明 如果$g\in G$，定义$\tau_g:S\longrightarrow S$，$x\longmapsto gx$。由于对每个$x\in S$均有$x=g(g^{-1}x)$，从而$\tau_g$是满射。类似地，由$gx=gy$($x$，$y\in S$) 导致$x=g^{-1}(gx)=g^{-1}(gy)=y$，从而$\tau_g$是单射，于是$\tau_g$是一一对应 (即是$S$上的置换)。由于$\tau_{gg'}=\tau_g\tau_{g'}:S\longrightarrow S$ (对所有g，$g'\in G$)，从而映射$G\longrightarrow A(S)$，$g\longmapsto\tau_g$是同态。 ∎

系4.6 (Cayley) 如果G是群，则存在单同态$G\longrightarrow A(G)$，从而每个群均同构于某个置换群。特别地，每个有限群G均同构于S_n的某个子群，其中$n=|G|$。

证明 假设G由左平移作用于自身之上，应用定理4.5便得到一个同态 $\tau: G \to A(G)$。如果 $\tau(g) = \tau_g = 1_G$，则对每个 $x \in G$均有 $gx = \tau_g(x) = x$。特别地$ge = e$，从而 $g = e$，即τ是单同态。为证最后论断只需注意：如果$|G| = n$，则$A(G) \cong S_n$。 ∎

让我们回忆一下，如果G是群，则G的全体自同构所组成的集合Aut$G$以函数合成作为二元运算形成群（习题I.2.15）。

系4.7 令G为群，

(i) 对于每个$g \in G$，经g共轭诱导出G的一个自同构。

(ii) 存在着同态$G \to \mathrm{Aut}G$，其核为 $C(G) = \{g \in G \mid gx = xg$. 对所有$x \in G\}$。

证明 (i) 如果G经共轭作用于自身之上，则由定理4.5的证明可知，对于每个$g \in G$，映射$\tau_g: G \to G$，$\tau_g(x) = gxg^{-1}$ 是一一对应。易知τ_g也是同态，从而是同构。

(ii) 令G经共轭作用于自身之上。从(i)可知定理4.5中同态$\tau: G \to A(G)$的象包含在Aut$G$之中。显然

$g \in \mathrm{Ker}\tau \Longleftrightarrow \tau_g = 1_G \Longleftrightarrow gxg^{-1} = \tau_g(x) = x$，对所有 $x \in G$。但是$gxg^{-1} = x \Longleftrightarrow gx = xg$。从而$\mathrm{Ker}\tau = C(G)$。 ∎

系4.7(i) 中的自同构τ_g 叫作由g诱导的内自同构。正规子群 $C(G) = \mathrm{Ker}\tau$叫作G的中心。元素 $g \in G$在$C(G)$ 中$\Longleftrightarrow g$的共轭类只包含一个元素g。因此，如果G是有限群并且 $x \in C(G)$，则$[G: C_G(x)] = 1$ （系4.4）。从而G的类方程 （系4.4(ii)）可以写成

$$|G| = |C(G)| + \sum_{i=1}^{m} [G: C_G(x_i)],$$

其中 $\bar{x}_1$，…，$\bar{x}_m$ ($x_i \in G - C(G)$) 是G 的不同共轭类并且 $[G: C_G$

$(x_i)]>1$.

命题4.8 假设H是群G的子群，G由左平移作用于由H在G中的全体左陪集所组成的集合S上。则诱导同态 $G\to A(S)$的核包含在H之中。

证明 诱导同态$G\longrightarrow A(S)$由$g\longmapsto\tau_g$给出，其中τ_g：$S\longrightarrow S$，而$\tau_g(xH)=gxH$。如果g在核中，则 $\tau_g=1_s$，从而对每个 $x\in G$，$gxH=xH$。特别对$x=e$，$geH=eH=H$，这导致$g\in H$。 ∎

系4.9 如果 H是G 的指数为n的子群，并且G没有非平凡的正规子群包含在H中，则G同构于S_n的某个子群。

证明 将命题4.8用于H。$G\longrightarrow A(S)$的核是G的正规子群并且包含在H中，由假设知它必为$\langle e\rangle$。从而$G\longrightarrow A(S)$ 是单同态。因此G同构于H的n个左陪集上的置换群(它显然同构于S_n)的某个子群。 ∎

系4.10 如果H是有限群G的子群并且指数为p，其中p是$|G|$的最小素因子，则$H\lhd G$。

证明 令S为H在G中的全体左陪集所组成的集合。则 $A(S)\cong S_p$，这是因为$[G:H]=p$。如果K是命题4.8中同态 $G\longrightarrow A(S)$的核，则K在G中正规并且包含在H中。此外，G/K同构于S_p的某个子群。因此$|G/K|\,|\,|1S_p|=p!$。但是$|G/K|=[G:K]$的每个因子必需除尽$|G|=|K|[G:K]$。由于(除了1之外)没有比 p 更小的数可以除尽$|G|$，因此我们必然有$|G/K|=p$或者1。但是$|G/K|=[G:K]=[G:H][H:K]=p[H:K]\geq p$。从而$|G/K|=p$并且$[H:K]=1$，即$H=K$。但是$K\lhd G$，从而$H\lhd G$。 ∎

习　题

1. 假设G是群而A是G的正规Abel子群，证明G/A共轭作用于A上，并且给出一个同态$G/A\to \mathrm{Aut}A$。
2. 如果H和K均是G的子群，并且$H\lhd K$，求证$K<N_G(H)$。
3. 如果群G中有元素a，而a恰好有两个共轭元素，则G有一个真正规子群$N\neq(e)$
4. 设H是G的子群，H的中心化子是集合$C_G(H)=\{g\in G\mid h_g=gh$，对每个$h\in H\}$，求证$C_G(H)$是$N_G(H)$的子群。
5. 如果H是G的子群，则商群$N_G(H)/C_G(H)$(见习题4)同构于$\mathrm{Aut}H$的某个子群。
6. 假设群G作用于集合S之上，$|S|\geqslant 2$，又假定G是可迁的，即给了任意的x，$y\in S$，均存在$g\in G$，使得$gx=y$.求证

   (a) 对于每个$x\in S$，x之轨道$\overline{x}$都是S，

   (b) 所有的固定子群$G_x(x\in S)$均彼此共轭。

   (c) 如果G有以下的性质：$\{g\in G\mid gx=x$，对所有$x\in S\}=\langle e\rangle$(假如对于某个$n$有$G<S_n$，并且$S=\{1,2,\cdots,n\}$，则$G$便具有此性质)，又如果$N\lhd G$，$N\lhd G_x$(对于某个$x\in S$)，则$N=\langle e\rangle$

   (d) 对于$x\in S$，$|S|=[G:G_x]$，从而$|S|\mid|G|$。
7. 假设G是群而InG是G的全体内自同构所构成的集合，求证$InG\lhd \mathrm{Aut}G$。
8. 给出Z_6的一个不是内自同构的自同构。
9. 如果$G/C(G)$是循环群，则G是Abel群。
10. 求证S_4的中心是$\langle e\rangle$.从而S_4同构于S_4的所有内自同构所形成的群。
11. 设群G中有元素a，$|a|\geqslant 3$，求证G有非恒等自同构[提示：习题1.2.2和系4.7]。
12. 任何有限群均同构于A_n的某个子群(对于某个n)。

13．如果群G包含一个指数有限的子群($\neq G$)，它必包含一个指数有限的正规子群($\neq G$)。

14．如果$|G|=p^n$，其中$p>n$，p为素数，而H为p阶子群，则$H \lhd G$。

15．如果p^n阶群G有一个p阶正规子群N(p为素数)，则N在G的中心中。

5．Sylow定理

有限 Abel 群已经在第 2 节中作了完全的同构分类，有限非Abel群则要复杂得多，而Sylow的几个定理是为理解任意有限群结构所作的最基本的一步。

促使我们进行研究的是如下的问题：如果正整数m除尽群G的阶数，G是否有m阶子群？这是Lagrange定理I.4.6的反问题。对于Abel群这是对的(系2.4)。但是对于任意的群可能不对(习题I.6.8)。我们先考虑m是素数这一特殊情形(定理5.2)，接下来便是Sylow 第一定理，它是说：当m是素数幂时，我们问题的答案是肯定的。这自然导致讨论最大素数幂阶的子群 (Sylow 第二和第三定理)。

引理5.1 如果p^n(p为素数)阶群 H 作用于有限集合S上，而$S_0=\{x\in S \mid hx=x$对于每个$h\in H\}$，则$|S|\equiv|S_0|(\mathrm{mod}p)$。

注记：这个引理(以及记号S_0)今后要经常使用[4]。

引理5.1的证明 轨道$\bar{x}$恰包含一个元素$\Longleftrightarrow x\in S_0$。因此$S$可以写成非交并：$S=S_0\cup\bar{x}_1\cup\bar{x}_2\cup\cdots\cup\bar{x}_n$，其中对每个$i$，$|\bar{x}_i|>1$。从而$|S|=|S_0|+|\bar{x}_1|+|\bar{x}_2|+\cdots+|\bar{x}_n|$。由于$|\bar{x}_i|>1$。

而 $|\bar{x}_i| = [H: H_{x_i}]$除尽 $|H| = p^n$，从而$p \mid |\bar{x}_i|$（对于每个i）。因此 $|S| \equiv |S_0| \pmod{p}$。∎

定理5.2 （Cauchy） 如果G是有限群并且素数$p \mid |G|$，则G中有p阶元素。

证明 （J.H.Mckay）令S为集合$\{(a_1, a_2, \cdots, a_p) \mid a_i \in G, a_1 a_2 \cdots a_p = e\}$。由于 $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$，从而 $|S| = n^{p-1}$，其中 $n = |G|$。因为$p \mid n$，从而 $|S| \equiv 0 \pmod{p}$。令群 Z_p 在集合S上的作用是循环置换，即对于$k \in Z_p$，$k(a_1, a_2, \cdots, a_p) = (a_{k+1}, a_{k+2}, \cdots, a_p, a_1, \cdots, a_k)$。验证$(a_{k+1}, a_{k+2}, \cdots, a_k) \in S$（利用如下的事实：在群中 $ab = e \Longrightarrow ba = (a^{-1}a)(ba) = a^{-1}(ab)a = e$）。验证对于0，$k$，$k' \in Z_p$和$x \in S$，$0x = x$，$(k + k')x = k(k'(x))$ 在集合上的群作用采用加法记号[4]）。因此可以定义Z_p在S上的作用。

现在$(a_1, \cdots, a_p) \in S_0 \Longleftrightarrow a_1 = a_2 = \cdots = a_p$。显然$(e, e, \cdots, e) \in S_0$。从而 $|S_0| \neq 0$。由引理5.1可知$0 \equiv |S| \equiv |S_0| \pmod{p}$。由于 $|S_0| \neq 0$，从而S_0中至少存在p个元素，即存在$a \neq e$，使得$(a, a, \cdots, a) \in S_0$，于是$a^p = e$。由于$p$为素数，从而$|a| = p$。∎

一个群如果每个元素的阶均是某个固定素数p的幂（$\geqslant 0$），则此群叫作p-群。如果H是群G的子群并且H是p-群，则H叫作 G 的p-子群。特别地，对于每个素数p，$|\langle e \rangle| = 1 = p^0$，从而$\langle e \rangle$是$G$的$p$-子群。

系5.3 有限群G是p-群$\Longleftrightarrow |G|$为p之幂。

证明 如果G是p-群而q是除尽$|G|$的素数，由 Cauchy定理知

---

4. 我感谢R.J.Nunke指给我这个证明的轮廓。

G中包含q阶元素。由于G中每个元素的阶均是p的幂，从而$q=p$。于是$|G|$是p的幂，反过来则是Lagrange定理I.4.6的直接推论。∎

系5.4 非平凡有限p-群G的中心$C(G)$必包含多于一个元素。

证明 考虑G的类方程(见136页)：

$$|G| = |C(G)| + \sum [G: C_G(x_i)].$$

由于每个$[G: C_G(x_i)]>1$，并且除尽$|G| = p^n (n\geqslant 1)$，从而p除尽每个$[G: C_G(x_i)]$和$|G|$，因此除尽$|C(G)|$。由于$|C(G)|\geqslant 1$，因此$C(G)$至少有p个元素。∎

引理5.5 如果H是有限群G的p-子群，则 $[N_G(H):H]\equiv[G:H](\mathrm{mod}p)$。

证明 令S是H在G中的全体左陪集组成的集合，而H在S上的作用是(左)平移。则$|S| = [G:H]$。并且

$xH\in S_0 \Longleftrightarrow hxH = xH$(对每个$h\in H$)$\Longleftrightarrow x^{-1}hxH = H$(对每个$h\in H$)$\Longleftrightarrow x^{-1}hx\in H$(对每个$h\in H$)$\Longleftrightarrow x^{-1}Hx = H\Longleftrightarrow xHx^{-1} = H$
$\Longleftrightarrow x\in N_G(H)$。

因此$|S_0|$是陪集$xH(x\in N_G(H))$的个数，即$|S_0| = [N_G(H):H]$。由引理5.1，$[N_G(H):H] = |S_0| \equiv |S| = [G:H](\mathrm{mod}p)$。∎

系5.6 如果H是有限群G的p-子群，并且$p|[G:H]$，则$N_G(H)\neq H$。

证明 $0\equiv[G:H]\equiv[N_G(H):H](\mathrm{mod}p)$。由于恒有$[N_G(H):H]\geqslant 1$，从而必然$[N_G(H):H]>1$，因此$N_G(H)\neq H$。∎

定理5.7 (Sylow第一定理)设G是$p^n m$阶群，其中$n\geqslant 1$，p为

素数，并且$(p, m)=1$。则对每个$1\leqslant i\leqslant n$，G均包含p^i阶子群，并且G的每个$p^i(i<n)$阶子群均是某个p^{i+1}阶子群的正规子群。

证明 由于$p\mid|G|$，由Cauchy定理可知它包含一个p阶元素a，从而包含p阶子群$\langle a\rangle$。现在归纳假设H是G的p^i阶子群$(1\leqslant i<n)$。则$p\mid[G:H]$，并且由引理5.5和系5.6可知H在$N_G(H)$中正规，$H\neq N_G(H)$和 $1<|N_G(H)/H|=[N_G(H):H]\equiv[G:H]\equiv 0(\mathrm{mod}p)$。从而$p\mid|N_G(H)/H|$，因此象以上所述一样$N_G(H)/H$包含一个 p阶子群。根据系I.5.12，这个子群有形式H_1/H，其中H_1为 $N_G(H)$ 的子群并且H_1包含H。由于$H\lhd N_G(H)$，从而$H\lhd H_1$。最后 $|H_1|=|H||H_1/H|=p^ip=p^{i+1}$。∎

群G的子群p叫作Sylow p-子群(p是素数)，是指p是G的最大p-子群(即若$P<H<G$，并且H为p-群，则$P=H$)。Sylow p-子群永远存在，虽然它可能是平凡的。进而，每个p-子群均包含在某个Sylow p-子群中(为了对于无限群证明这一点，需要Zorn引理)。定理5.7表明，对于每个素数$p\mid|G|$，有限群G必有非平凡的Sylow p-子群。此外我们有

系5.8 假设G是p^nm阶群，其中p为素数，$n\geqslant 1$并且$(m, p)=1$。令H是G的p-子群。则

(i) H是G的Sylow p-子群$\Longleftrightarrow|H|=p^n$

(ii) Sylow p-子群的每个共轭也是Sytow$p$-子群。

(iii) 如果只有一个Sylow p-子群P，则$P\lhd G$。

证明概要 (i) 由系I.4.6和5.3以及定理5.7。

(ii) 由习题I.5.6和(i)。

(iii) 由(ii)得出。∎

作为系5.8(ii)的逆，我们有

定理5.9 (Sylow第二定理)。如果H是有限群G的p-子群，而P是G的任意一个Sylow p-子群.则存在$x\in G$，使得$H<xPx^{-1}$。特别地，G的两个Sylow p-子群是彼此共轭的。

证明 设S是p在G中的全体左陪集所组成的集合，而H在S上的作用是(左)平移。由引理5.1，$|S_0|\equiv|S|=[G:P](\mathrm{mod}p)$。但是$p\nmid[G:p]$，因此$|S_0|\neq 0$，从而存在$xP\in S_0$。但是

$xP\in S_0\Longleftrightarrow hxP=xP$ (对所有$h\in H$) $\Longleftrightarrow x^{-1}hxP=P$(对所有$h\in H$)$\Longleftrightarrow x^{-1}Hx<P\Longleftrightarrow H<xPx^{-1}$。

如果H是Sytow p-子群，则$|H|=|P|=|xPx^{-1}|$，因此$H=xPx^{-1}$。 ∎

定理5.10 (Sylow第三定理)如果G是有限群而p是素数，则G的Sylow p-子群的个数是$|G|$的因子，并且具有形式$kp+1$(对于某个$k\geqslant 0$)。

证明 根据Sylow第二定理，Sylow p-子群的个数是它们之中任一个(设是P)的共轭子群个数。但是这个数是$[G:N_G(P)]$，从而为$|G|$的因子(系4.4)。令S为G的全体Sylow p-子群所组成的集合，P在S上的作用为共轭。则$Q\in S_0\Longleftrightarrow xQx^{-1}=Q$(对于所有$x\in P$)。而后一条件又等价于$P<N_G(Q)$。由于$P$和$Q$均是$G$的Sylow p-子群，从而也都是$N_G(Q)$的Sylow p-子群，因此它们在$N_G(Q)$中共轭。但是Q在$N_G(Q)$中正规，从而只可能$Q=P$。因此$S_0=\{P\}$，并且由引理5.1，$|S|\equiv|S_0|=1(\mathrm{mod}p)$，从而$|S|=kp+1$。 ∎

定理5.11 如果P是有限群G的Sytow$p$-子群，则$N_G(N_G(P))=N_G(P)$。

证明 p的每个共轭Q都是G的Sylow$p$-子群，从而Q也是G中包含Q的任意子群的Sylow$p$- 子群．由于$P \lhd N = N_G(P)$，由定理5.9可知P是N中唯一的Sylow$p$-子群．因此

$$x \in N_G(N) \Longrightarrow xNx^{-1} = N \Longrightarrow xPx^{-1} < N \Longrightarrow xPx^{-1} = P \Longrightarrow x \in N.$$

于是$N_G(N_G(P)) < N$．而$N_G(N_G(P)) > N$是显然成立的． ∎

习　题

1．如果$N \lhd G$，并且N和G/N均为p－群，则G为p－群．

2．如果G为有限p－群，$H \lhd G$，$H \neq \langle e \rangle$，则$H \cap C(G) \neq \langle e \rangle$．

3．令$|G| = p^n$，对于每个k，$0 \leqslant k \leqslant n$，$G$必有$p^k$阶正规子群．

4．如果G是无限p－群(p为素数)，则或者对于每个$n \geqslant 1$，G 均有p^n阶子群；或者存在$m \in \mathrm{N}^*$，使得G的每个有限子群的阶均$\leqslant p^m$．

5．如果P是有限群G的正规Sylow$p$－子群，而f；$G \to G$是自同态，则$f(P) < P$

6．如果H是有限群G的p^k阶正规子群，则H包含在G的每个Sytow$p$－子群之中．

7．求S_3，S_4，S_5的全部Sylow2-子群和Sylow3-子群．

8．如果对于每个素数p，有限群G的每个Sylow$p$-子群均正规，则G是它的诸Sylow子群的直积．

9．如果$|G| = p^n q$，其中$p > q$，p，q均是素数，则G 有唯一的正规子群，其指数为q．

10．每个12阶，28阶，56阶和200阶群一定包含一个正规Sylow 子群，从而均不是单群．

11．在168阶单群中，共有多少个7阶元素？

12．求证S_4的每个自同构均是内自同构，从而 $S_4 \cong \mathrm{Aut}S_4$．[提示：见习题

4.10. S_4的每个自同构诱导出S_4的Sytow3-子群组成的集合$\{P_1, P_2, P_3, P_4\}$上的一个置换.如果 $f\in \mathrm{Aut}S_4$ 使得$f(P_i)=P_i(1\leqslant i\leqslant 4)$, 则 $f=1_{S_4}$]

13. 每个p^2阶群(p为素数)G都是Abel群.[提示: 习题4.9和系5.4].

6. 有限群的分类

现在我们对于全部pq阶群 (p和q均是素数) 和全部小阶数群($n\leqslant 15$)作同构分类. 当然,这些都不是非常深刻的结果. 但是即使是为此所作的努力也将表明要决定任意(有限)群的结构是多么困难. 本节的结果在今后是不需要的.

命题6.1 假设p和q均是素数, $p>q$. 如果$q\nmid p-1$, 则每个pq阶群均同构于循环群Z_{pq}. 如果$q\mid p-1$, 则不计同构恰好有两个不同的pq阶群: 循环群Z_{pq}和非Abel 群K, 其中K是由元素c和d生成的, 并且

$$|c|=p,\ |d|=q,\ dc=c^s d,$$

其中$s\not\equiv 1(\mathrm{mod}\ p)$, $s^q\equiv 1(\mathrm{mod}\ p)$.

证明概要 命题中所描述的pq阶非Abel群 K 是存在的(习题2). 给了一个pq阶群G, 由Cauchy 定理5.2, G包含元素 a和b, $|a|=p$, $|b|=q$. 此外, $S=\langle a\rangle$在G中正规(由系4.10, 或者象下面那样通过计算Sylow$p$-子群). 陪集bS在群G/S中的阶数是q.由于$|G/S|=q$, 从而G/S是由bS生成的循环群, 即$G/S=\langle bS\rangle$. 因此G中每个元素均可写成形式b^ia^j, 从而$G=\langle a, b\rangle$.

Sylow$q$-子群的个数是$kq+1$并且它除尽pq。因此它必然为1或者p。如果它是1（当$q\nmid p-1$时必然如此），则$\langle b\rangle$也在G中正规。由Lagrange定理I.4.6可知$\langle a\rangle\cap\langle b\rangle=\langle e\rangle$。因此由定理I.3.2，I.8.6，I.8.10和习题I.8.5可知$G=\langle a\rangle\times\langle b\rangle\cong Z_p\oplus Z_q\cong Z_{pq}$。如果它是$p$(这只可能在$p|q-1$的时候)，则$bab^{-1}=a^r$(由于$\langle a\rangle\lhd G$)并且$r\not\equiv 1\pmod p$（否则由定理I.3.4(v)得出$G$是Abel群，从而只有唯一的Sylow$q$-子群)。由$bab^{-1}=a^r$，归纳地可推出$b^iab^{-i}=a^{r^i}$。特别取$i=q$，得出$a=a^{r^q}$，由定理I.3.4(V)，这导致$r^q\equiv 1\pmod p$。

为了完成证明，我们必需再证当$q|p-1$时，如果G是上一段所描绘的非Abel群，则G同构于K。我们需要一些数论结果。同余式$x^q\equiv 1\pmod p$恰好有q个 mod p不同的解（见J.E.Shockley[51；系6.1，第67页]）。如果r是其中一个解，而k是满足$r^k\equiv 1\pmod p$的最小正整数，则$k\mid q$。（见J.E.Shockley[51，定理8，第70页]）。在我们的情况下，$r\not\equiv 1\pmod p$，从而$k=q$。由此可知$1, r, r^2, \cdots, r^{q-1}$是$x^q\equiv 1\pmod p$的全部mod$p$不同的解。因此存在某个$t(1\leqslant t\leqslant q-1)$，使得$s\equiv r^t\pmod p$。如果$b_1=b^t\in G$，则$|b_1|=q$。我们在上面的讨论(以$b_1$代替$b$)表明：$G=\langle a, b_1\rangle$，$G$中每个元素均可以表示成$b_1^ia^j$，$|a|=p$，$b_1ab_1^{-1}=b^tab^{-t}=a^{r^t}=a^s$(定理I.3.4(v))。因此$b_1a=a^sb_1$。验证映射$G\longrightarrow K$，$a\longmapsto c$，$b_1\longmapsto d$是同构。∎

系6.2 如果p是奇素数，则每个$2p$阶群或者同构于循环群Z_{2p}，或者同构于正多边形群D_p。

证明 将命题6.1用于$q=2$。如果G不循环，关于s的条件给出$s\equiv -1\pmod p$。从而$G=\langle c, d\rangle$，$|d|=2$，$|c|=p$，而由定理

I.3.4(v)给出$dc=c^{-1}d$。从而由定理I.6.13便知$G\cong D_p$。 ∎

命题6.3 (不计同构)恰好存在两个不同的8阶非Abel群：四元数群Q_8和正多边形群D_4。

注记：四元数群Q_8由习题I.2.3所刻划。

证明概要 验证$D_4\ncong Q_8$(习题10)。如果8阶群G是非Abel的，则它不能有8阶元素，并且不能每个非恒等元素都是2阶的（习题I.1.13)。因此G包含4阶元素a。而$\langle a\rangle$的指数为2，从而$\langle a\rangle\lhd G$。取$b\notin\langle a\rangle$。由于$|G/\langle a\rangle|=2$，从而$b^2\in\langle a\rangle$。证明只有两种可能性：$b^2=a^2$或者$b^2=e$。由于$\langle a\rangle\lhd G$，$bab^{-1}\in\langle a\rangle$。唯一可能的是$bab^{-1}=a^3=a^{-1}$。从而$G$中每个元素均可以写成$b^ia^j$。于是$G=\langle a, b\rangle$。对于前一种情形则$|a|=4, b^2=a^2, ba=a^{-1}b$，从而由习题I.4.14可知$G\cong Q_8$。对于后一种情形则$|a|=4$，$|b|=2$，$ba=a^{-1}b$，从而由定理I.6.13有$G\cong D_4$。 ∎

命题6.4 (不计同构)共存在恰好三个不同的12阶非Abel群：正多边形群D_6，交错群A_4，以及由a，b生成的群T，其中$|a|=6$，$b^2=a^3$，$ba=a^{-1}b$。

证明概要 验证存在着上述的群T(习题5)，并且D_6，A_4和T彼此互不同构(习题6)。如果G是12阶非Abel群，以P表示G的一个Sylow3-子群。则$|P|=3$，$[G:P]=4$。由命题4.8可知存在同态$f:G\longrightarrow S_4$，其核$K\subset P$，从而$K=P$或者$K=\langle e\rangle$。如果$K=\langle e\rangle$，则f是单同态，而G同构于S_4中的一个12阶子群，由定理I.6.8可知它必然为A_4。如果$K=P$，则$P\lhd G$。这时P是G的唯一Sylow3-子群。从而G只包含两个3阶元素。设c为其中的一个3阶元素，则$[G:C_G(c)]=1$或者2，这是因为$[G:C_G(c)]$是c的共轭元

素个数，并且c的每个共轭元素均是3阶的．从而$C_G(c)$是12阶或者6阶群．根据 Cauchy 定理．无论在哪一种情形下，均存在2阶元素$d\in C_G(c)$．验证$|cd|=6$．

令$a=cd$，则$\langle a\rangle\lhd G$并且$|G/\langle a\rangle|=2$．从而存在元素$b\in G$，使得$b\notin\langle a\rangle$，$b\neq e$，$b^2\in\langle a\rangle$并且$bab^{-1}\in\langle a\rangle$．由于$G$是非 Abel 群并且$|a|=6$，从而只可能$bab^{-1}=a^5=a^{-1}$，即$ba=a^{-1}b$．对于$b^2\in\langle a\rangle$共有六种可能性：$b^2=a^2$或者$b^2=a^4$均导致矛盾．$b^2=a$或者$b^2=a^5$导致$|b|=12$，从而$G$是Abel群．因此只可能：

(i) $|a|=6$，$b^2=e$，$ba=a^{-1}b$，由定理I.6.13可知$G\cong D_6$；

(ii) $|a|=6$，$b^2=a^3$，$ba=a^{-1}b$，由习题5(b)可知$G\cong T$．

∎

下表列出小阶群的全部同构类．共有14个不同的16阶群和51个不同的32阶群，见M.Hall 和 J.K.Senior[16]．目前没有一个公式能够对于每个n给出n阶群的个数．

阶数	群	参考资料
1	$\langle e\rangle$	……
2	Z_2	习题I.4.3
3	Z_3	习题I.4.3
4	$Z_2\oplus Z_2$，Z_4	习题I.4.5
5	Z_5	习题I.4.3
6	Z_6，D_3	系6.2
7	Z_7	习题I.4.3
8	$Z_2\oplus Z_2\oplus Z_2$，$Z_2\oplus Z_4$，Z_8，Q_8，D_4	定理2.1，命题6.3
9	$Z_3\oplus Z_3$，Z_9	习题5.13，定理2.1
10	Z_{10}，D_5	系6.2
11	Z_{11}	习题I.4.3

12	$Z_2 \oplus Z_6, Z_{12}, A_4, D_6, T$	定理2.1，命题6.4
13	Z_{18}	习题I.4.3
14	Z_{14}, D_7	系6.2
15	Z_{15}	命题6.1

习　题

1. 假设G和H是群，$\theta: H \to \mathrm{Aut}G$是群同态．以$G \times_\theta H$表示集合$G \times H$赋以如下的二元运算：$(g, h)(g', h') = (g[\theta(h)g'], hh')$．求证$G \times_\theta H$是群，其幺元素为$(e, e)$，而$(g, h)^{-1} = (\theta(h^{-1})(g^{-1}), h^{-1})$．$G \times_\theta H$称作$G$和$H$的半直积．

2. 设$C_p = \langle a \rangle$和$C_q = \langle b \rangle$分别是p阶和q阶（乘法）循环群，其中p和q均为素数，$p > q$，$q \mid p-1$．设s是整数，使得$s \not\equiv 1 \pmod p$，$s^q \equiv 1 \pmod p$，（这导致$s \not\equiv 0 \pmod p$）．由初等数论可知这样的S是存在的（见J.E.Shockley[51；系6.1，第67页1]．求证

   (a) 映射$\alpha: C_p \to C_p$，$a^t \longmapsto a^{st}$是自同构．

   (b) 映射$\theta: C_q \to \mathrm{Aut}C_p$，$\theta(b^t) = \alpha^t$（$\alpha$见第（a）部分）是同态（$\alpha^\circ = 1_{C_p}$）．

   (c) 如果将a和b分别记为(a, e)和(e, b)，则群$C_p \times_\theta C_q$（见习题1）是pq阶群，此群由a和b生成，并且关系为：$|a| = p$，$|b| = q$，$ba = a^s b$，其中$s \not\equiv 1 \pmod p$并且$s^q \not\equiv 1 \pmod p$．群$C_p \times_\theta C_q$叫作亚循环(metacyclic)群．

3. 考虑集合$G = \{\pm 1, \pm i, \pm j, \pm k\}$，乘法为：$i^2 = j^2 = k^2 = -1$，$ij = k$，$jk = i$，$ki = j$，$ji = -k$，$kj = -i$，$ik = -j$，而乘以$\pm 1$则采用通常的法则．求证$G$是同构于$Q_8$的群．

4. 四元数群Q_8的中心是什么？求证$Q_8/C(Q_8)$是Abel群．

5. (a) 证明$S_3 \times Z_4$有12阶非Abel子群T，T由元素a和b生成，并且$|a| = 6$，$a^3 = b^2$，$ba = a^{-1}b$．

(b) 每个由a，b生成的12阶群，如果$|a|=6$，$a^3=b^2$并且$ba=a^{-1}b$，则它必然同构于T。

6. D_6，A_4和T彼此均不同构，其中T是命题6.4和习题5中所描述的12阶群。

7. 如果G是p^3（p为素数）阶非Abel群，则G的中心是由所有形如$aba^{-1}b^{-1}$（a，$b\in G$）的元素所生成的子群。

8. 假设p是奇素数。求证至多有两个p^3阶非Abel群〔其中一个是由a，b生成的，并且满足$|a|=p^2$，$|b|=p$，$b^{-1}ab=a^{1+p}$；而另一个是由a,b，c生成的，并且满足$|a|=|b|=|c|=p$，$c=a^{-1}b^{-1}ab$，$ca=ac$，$cb=bc$.〕。

9. 将所有18阶群作同构分类，对于20阶和30阶作同样的事情。

10. 求证D_4不同构于Q_8。〔提示：计算2阶元素的个数.〕

7. 幂零群与可解群

考虑关于有限群G的如下一些条件。

(i) G是它的Sylow子群的直积。

(ii) 如果$m\,||G|$，则G有m阶子群。

(iii) 如果$|G|=mn$，$(m,\ n)=1$，则G有m阶子群。

条件 (ii) 和 (iii) 可以考虑作 Sylow 第一定理的变型. 不难证明 (i)$\Longrightarrow$(ii)。而(ii)$\Longrightarrow$(iii) 是显然成立的. 从定理2.2容易推出，每个有限Abel 群满足 (i)。每个p-群显然也满足(i)。另一方面，A_4满足 (iii) 但是不满足 (ii)，而S_3满足 (ii) 但是不满足 (i)（习题1）。我们已经对于有限Abel群和p-群得出了深刻的结果，那么，将分别满足 (i)、(ii) 或 (iii) 的群类作为进

一步研究的对象便是很合适的。我们目前仅限于研究满足 (i) 或者 (iii) 的那些群。

我们首先用某种子群“正规列”来定义幂零群和可解群。对于有限群的情形，幂零群可以用条件 (i) 来刻划 (命题7.5)，而可解群可以用条件 (iii) 来刻划(命题7.14)。这种观点也表明幂零群可解群与交换性之间的联系。在第 8 节给出刻划幂零群和可解群的另一些方式。

我们处理可解群的方式是纯群论的。但是在历史上，可解群第一次出现时是与域上多项式求根问题有关联的 (见第v.9节)。

设G是群。G的中心$C(G)$是正规子群 (系4.7)。令$C_2(G)$是$C(G/C(G))$在正则射影 $G\to G/C(G)$ 之下的原象。则由定理I.5.11 (的证明) 可知$C_2(G)$在G中正规并且包含 $C(G)$。继续这个过程我们归纳地定义：$C_1(G)=C(G)$，而 $C_i(G)$ 是 $C(G/C_{i-1}(G))$在正则射影$G\to G/C_{i-1}(G)$之下的原象。因此我们得到G的一个正规子群列，叫作G的中心升链：$\langle e\rangle<C_1(G)<C_2(G)<\cdots$。

定义7.1 群G叫作幂零的，是指存在某个n，使得 $C_n(G)=G$。

每个Abel群G都是幂零的，因为$G=C(G)=C_1(G)$。

定理7.2 每个有限p-群都是幂零的。

证明 G和它的所有非平凡商群都是p-群。因此由系5.4可知它们均有非平凡的中心。由此推出，如果$G\neq C_i(G)$，则 $C_i(G)$严格包含在$C_{i+1}(G)$中。由于G是有限群，必然对某个n,使$C_n(G)$等于G。 ∎

定理7.3 有限多个幂零群的直积也是幂零的.

证明 为方便起见，假定$G=H\times K$，对于多于两个因子的情形证明是类似的. 我们归纳证明 $C_i(G)=C_i(H)\times C_i(K)$ ($i=1$的情形显然是对的). 令 π_H 是正则满同态 $H\to H/C_i(H)$. 类似地定义π_K. 验证正则满同态φ: $G\to G/C_i(G)$ 是下面一些同态的合成:

$$\begin{aligned} G=H\times K &\xrightarrow{\pi} H/C_i(H)\\ &\times K/C_i(K)\xrightarrow{\psi}\frac{H\times K}{C_i(H)\times C_i(K)}\\ &=\frac{H\times K}{C_i(H\times K)}=G/C_i(G), \end{aligned}$$

其中$\pi=\pi_H\times\pi_K$ (定理I.8.10)，而ψ是系 I.8.11中的同构. 于是

$$\begin{aligned} C_{i+1}(G)&=\varphi^{-1}[C(G/C_i(G))]\\ &=\pi^{-1}\psi^{-1}[C(G/C_i(G))]\\ &=\pi^{-1}[C(H/C_i(H)\times K/C_i(K))]\\ &=\pi^{-1}[C(H/C_i(H))\times C(K/C_i(K))]\\ &=\pi_H^{-1}[C(H/C_i(H))]\times\pi_K^{-1}[C(K/C_i(K))]\\ &=C_{i+1}(H)\times C_{i+1}(K). \end{aligned}$$

因此由归纳法证明了对每个i，$C_i(G)=C_i(H)\times C_i(K)$. 由于$H$和$K$均幂零，从而存在$n\in\mathbf{N}^*$，使得$C_n(H)=H$，同时$C_n(K)=K$,于是$C_n(G)=H\times K=G$. 即$G$是幂零群. ∎

引理7.4 如果H是幂零群G 的真子群，则H是它的正规化子$N_G(H)$的真子群.

证明 令 $C_0(G)=\langle e\rangle$，又设n是最大下标，使得 $C_n(G)<H$ (由于G 幂零而H是G 的真子群，可知这样的n 是存在的). 取$a\in C_{n+1}(G)$，$a\notin H$，则对每个 $h\in H$，在$G/C_n(G)$ 中 $C_nah=(C_na)$

$(C_nh)=(C_nh)(C_na)=C_nha$，这是因为根据$C_{n+1}(G)$的定义知$C_na$在中心中。从而$ah=h'ha$，其中$h'\in C_n(G)<H$，从而$aha^{-1}\in H$，即$a\in N_G(H)$。由于$a\notin H$，可知$H$是$N_G(H)$的真子群。 ∎

命题7.5 一个有限群是幂零的，当且仅当它是它的Sylow子群的直积。

证明 如果G是它的Sylow子群的直积，由定理7.2和7.3可知G是幂零的.如果G是幂零的，而P是G的Sylow$p$-子群（对于某个素数p），则或者$P=G$（这时便证毕），或者P是G的真子群。对于后一情形，由引理7.4可知P是$N_G(H)$的真子群。由定理5.11，$N_G(P)$是它自己的正规化子，从而由引理7.4可知必需$N_G(P)=G$。因而$P\lhd G$，于是由定理5.9知P是G中唯一的Sylow p-子群。令$|G|=p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$（$p_i$为不同的素数，$n_i>0$），又令$P_1$，$P_2$，…，$P_k$是$G$中对应的（真正规）Sylow子群。由于$|P_i|=p_i^{n_i}$（对每个$i$），$P_i\cap P_j=\langle e\rangle$（对于$i\neq j$）。根据定理I.5.3可知对于每个$x\in P_i$，$y\in P_j$（$i\neq j$），$xy=yx$。从而对于每个$i$，$P_1P_2\cdots P_{i-1}P_{i+1}\cdots P_k$是子群，并且其中每个元素的阶数均是$p_1^{n_1}\cdots p_{i-1}^{n_{i-1}}p_{i+1}^{n_{i+1}}\cdots p_k^{n_k}$的因子。从而$P_i\cap(P_1\cdots P_{i-1}P_{i+1}\cdots P_k)=\langle e\rangle$，于是$P_1P_2\cdots P_k=P_1\times P_2\times\cdots\times P_k$。由于$|G|=p_1^{n_1}\cdots p_k^{n_k}=|P_1\times\cdots\times P_k|=|P_1\cdots P_k|$，从而必然$G=P_1P_2\cdots P_k=P_1\times\cdots\times P_k$。 ∎

系7.6 如果G是有限幂零群而$m\mid|G|$，则G有m阶子群。

证明作为练习。 ∎

定义7.7 设G是群。由集合$\{aba^{-1}b^{-1}\mid a,b\in G\}$生成的$G$的子群叫作$G$的换位子群，并表示成$G'$。

元素$aba^{-1}b^{-1}(a,\ b\in G)$叫作换位子。换位子只是生成$G'$，因而$G'$可能会包含不是换位子的元素。$G$是Abel群的充要条件是$G'=\langle e\rangle$。所以在某种意义上，可用$G'$来衡量$G$与Abel群相距有多远。

定理7.8 如果G是群，则G'是G的正规子群并且G/G'是Abel群。如果N是G的正规子群，则G/N为Abel群$\Longleftrightarrow N\supset G'$。

证明 令$f:G\to G$是任一自同构。则

$$f(aba^{-1}b^{-1})=f(a)f(b)f(a)^{-1}f(b)^{-1}\in G'.$$

从而$f(G')<G'$。特别若f是由元素$a\in G$共轭的作用所给出的自同构，则$aG'a^{-1}=f(G')<G'$，于是根据定理I.5.1可知$G'\lhd G$。由于$(ab)(ba)^{-1}=aba^{-1}b^{-1}\in G'$，从而$abG'=baG'$，即$G/G'$是Abel群。如果$G/N$是Abel群，则$abN=baN$（对于所有$a,\ b\in G$），从而$ab(ba)^{-1}=aba^{-1}b^{-1}\in N$，即$N$包含全部换位子，从而$G'<N$。反方向则很容易。∎

令G是群，以$G^{(1)}$表示G'。然后对于$i\geqslant 1$，定义$G^{(i)}=(G^{(i-1)})'$。称$G^{(i)}$为G的第i导出子群。这给出G的一个子群列，并且每个均是它前一个的正规子群：$G>G^{(1)}>G^{(2)}>\cdots$，事实上，每个$G^{(i)}$均是G的正规子群（习题13）。

定义7.9 群G叫作可解的，是指存在某个n，使得$G^{(n)}=\langle e\rangle$。

每个Abel群显然是可解的。更一般地我们有

命题7.10 每个幂零群均可解。

证明 根据$C_i(G)$的定义，$C_i(G)/C_{i-1}(G)=C(G/C_{i-1}(G))$

是Abel群，从而当$i>1$时$C_i(G)'<C_{i-1}(G)$，而$C_1(G)'=C(G)'=\langle e\rangle$。对于某个$n$，$G=C_n(G)$。因而$C(G/C_{n-1}(G))=C_n(G)/C_{n-1}(G)=G/C_{n-1}(G)$ 是 Abel 群，从而 $G^{(1)}=G'<C_{n-1}(G)$。因此 $G^{(2)}=G^{(1)\prime}<C_{n-1}(G)'<C_{n-2}(G)$。类似地，$G^{(3)}<C_{n-2}(G)'<C_{n-3}(G)$，…，$G^{(n-1)}<C_2(G)'<C_1(G)$，$G^{(n)}<C_1(G)'=\langle e\rangle$。即$G$是可解的。 ∎

定理7.11 (i) 可解群的每个子群和同态象都是可解的。

(ii) 如果N是群G的正规子群，并且N和G/N均可解，则G也可解。

证明概要 (i) 如果$f:G\to H$是同态[满同态]，验证$f(G^{(i)})<H^{(i)}[f(G^{(i)})=H^{(i)}]$（对于每个$i$）。假设$f$ 是满同态，并且G是可解的。则存在某个 n，使得$\langle e\rangle=f(e)=f(G^{(n)})=H^{(n)}$，从而$H$是可解的。对于子群情形，其证明是类似的。

(ii) 设$f:G\to G/N$是正则满同态。由于 G/N是可解的，从而存在某个n，使得$f(G^{(n)})=(G/N)^{(n)}=\langle e\rangle$。于是$G^{(n)}<Kerf=N$。又由(i) 知 $G^{(n)}$是可解的，从而存在$k\in \boldsymbol{N}^*$，使得$G^{(n+k)}=(G^{(n)})^{(k)}=\langle e\rangle$，即$G$是可解的。 ∎

系7.12 $n\geqslant 5$时，对称群S_n不是可解的。

证明 如果S_n是可解的，则A_n也是可解的。由于A_n是非Abel群，从而 $A_n'\neq(1)$。但是A_n'在 A_n中正规（定理7.8），而A_n是单群（定理I.6.10），从而必然 $A_n'=A_n$。因此对所有 $i\geqslant 1$，$A_n^{(i)}=A_n\neq(1)$，即A_n不可解。 ∎

注记：本节以下内容在今后是不需要的。

为了对于有限可解群证明Sylow 定理的推广（正如本节第一

段所提到的)，我们需要一些定义和引理。群G的子群H叫作特征子群[完全不变子群]，是指对于每个自同构[自同态]$f:G\to G$，均有$f(H)<H$。显然，每个完全不变子群都是特征子群，而每个特征子群都是正规的(因为共轭运算是自同构)。群G的极小正规子群是指一个非平凡正规子群，它没有真子群在G中正规。

引理7.13 假设N是有限群G的正规子群，而H是G的任意子群。

(i) 如果H是N的特征子群，则H在G中正规。

(ii) G的每个正规Sylow p-子群都是完全不变的。

(iii) 如果G是可解的而N是极小正规子群，则N是Abel p-群(对于某个p)。

证明 (i) 由于对每个$a\in G$，$aNa^{-1}=N$，从而 a-共轭运算是N的自同构。由于H是N的特征子群，从而对每个$a\in G$，$aHa^{-1}<H$。于是由定理I.5.1可知H在G中正规。

(ii) 作为练习。

(iii) 易知N'在N中是完全不变的，从而由(i) 可知N'在G中正规。由于N是极小正规子群，所以或者$N'=\langle e\rangle$，或者$N'=N$。由于N是可解的 (定理7.11)，从而 $N'\neq N$，因此 $N'=\langle e\rangle$，即N为非平凡的Abel群。令P是N的非平凡Sylow p-子群(对于某个素数p)。由于N是Abel群，从而P在N中正规，因此由 (ii) 知P在N中是完全不变的。于是由 (i) 知P在 G 中正规。由于N是极小的而P是非平凡的，从而$P=N$。 ∎

命题7.14 (P.Hall) 令G为mn阶有限可解群，$(m,n)=1$。则

(i) G包含m阶子群。

(ii) G的任意两个m阶子群都是彼此共轭的。

(iii) 如果$k|m$，则G的每个k阶子群都包含在某个m阶子群之中。

注记：如果m是素数幂，则这个定理不过是Sylow诸定理中某些结果的重述。P.Hall还证明了(i)的逆命题：如果G是有限群，并且当$|G|=mn$，$(m, n)=1$时，G便有m阶子群，则G是可解的。证明超出了本书的范围（见M.Hall[15，第143页]）。

命题7.14的证明 证明是对于$|G|$作数学归纳法，阶数$\leqslant 5$的时候是平凡的。我们分两种情形：

情形**1**：G存在真正规子群H，使得$n\nmid H$。

(i) $|H|=m_1n_1$，其中$m_1|m$，$n_1|n$并且$n_1<n$。G/H是阶$(m/m_1)(n/n_1)(<mn)$的可解群，并且$(m/m_1, n/n_1)=1$。由归纳假设可知G/H包含一个(m/m_1)阶子群A/H（其中A是G的子群，见系I.5.12)。于是$|A|=|H|[A:H]=(m_1n_1)(m/m_1)=mn_1<mn$。而$A$是可解的（定理7.11)，由归纳假设，它包含$m$阶子群。

(ii) 假设B和C均是G的m阶子群。由于H在G中正规，HB也是子群（定理I.5.3)，它的阶数k必然除尽$|G|=mn$。由于$k=|HB|=|H||B|/|H\cap B|=m_1n_1m/|H\cap B|$，从而$k|H\cap B|=m_1n_1m$，因此$k|m_1n_1m$。但是$(m_1, n)=1$，从而有整数$x$，$y$，使得$m_1x+ny=1$，于是$mn_1m_1x+mn_1ny=mn_1$。从而$k|mn_1$。由Lagrange定理I.4.6，$m=|B|$，$m_1n_1=|H||k$。从而由$(m, n)=1$推出$mn_1|k$。因此$k=mn_1$。类似地，$|HC|=mn_1$。从而$HB/H$和$HC/H$均是$G/H$的$m/m_1$阶子群。由归纳假设知它们是彼此共轭的：即有$\bar{x}\in G/H$（$\bar{x}$是$x\in G$的陪集)，使得$\bar{x}(HB/H)\bar{x}^{-1}=HC$

/H。由此推出$xHBx^{-1}=HC$。从而xBx^{-1}和C均是HC的m阶子群，由归纳假设，它们在HC中共轭。从而B和C在G中共轭。

(iii) 如果G的子群K有阶数$k|m$，则$HK/H\cong K/H\cap K$的阶数除尽k。由于HK/H是G/H的子群，它的阶数也除尽$|G/H|=(m/m_1)(n/n_1)$。由$(k, n)=1$推出HK/H的阶数除尽m/m_1。根据归纳假设，存在G/H的一个m/m_1阶子群A/H包含HK/H（其中$A<G$）。显然K是A的子群。由于$|A|=|H||A/H|=m_1n_1(m/m_1)=mn_1<mn$，由归纳假设，$K$包含在$A$的（从而$G$的）某个$m$阶子群中。

情形2：G的每个真正规子群的阶数均可被n除尽。如果H是极小正规子群（因为G是有限群，这样的群是存在的），则由引理7.13 (iii) 可知$|H|=p^r$（对于某个素数p）。由于$(m, n)=1$，$n/|H|$，从而$n=p^r$，即H是G的Sylow$p$-子群。由于H在G中正规，从而H是G唯一的Sylow$p$-子群。这个推理过程表明H是G中仅有的极小正规子群（不然的话，就会对不同的素数p和q，有$n=p^r$同时$n=q^s$）。特别地，G的每个非平凡正规子群均包含H。

(i) 令K是G的正规子群，使得K/H是G/H的极小正规子群（系I.5.12）。由引理7.13 (iii) 可知$|K/H|=q^s$(q为素数并且$q\neq p$)，从而$|K|=p^rq^s$。设S是K的Sylow q-子群，而M是S在G中的正规化子。我们将证明$|M|=m$。由于H在K中正规，HS是K的子群。显然$H\cap S=\langle e\rangle$，从而$|HS|=|H||S|/|H\cap S|=p^rq^s=|K|$，从而$K=HS$。

因为K在G中正规并且$S<K$，则S在G中的每个共轭子群都在K中。由于S是K的Sylow子群，所有这些子群在K中就已经彼此共轭。令$N=N_K(S)$。则S在G中的共轭子群个数c是$[G:M]=[K:N]$（系4.4）。由于$S<N<K$，$K>HN>HS=K$，从而$K=HN$并

且$c=[G:M]=[K:N]=[HN:N]=[H:H\cap N]$（系I.5.9）。我们要证明$H\cap N=\langle e\rangle$，这导致$c=|H|=p^r$，从而$|M|=|G|/[G:M]=mp^r/p^r=m$。为此我们先证$H\cap N<C(K)$，再证$C(K)=\langle e\rangle$。

令$x\in H\cap N$而$k\in K$。由于$K=HS$，$k=hs(h\in H,\ s\in S)$。因为H是Abel群（引理7.13（iii））而$x\in H$，为了证明$xk=kx$从而$x\in C(K)$，我们只需证明$xs=sx$。现在$(xsx^{-1})s^{-1}\in S$（因为$x\in N=N_K(S)$）。但是$x(sx^{-1}s^{-1})\in H$（由于$x\in H$而$H\lhd G$）。因此$xsx^{-1}s^{-1}\in H\cap S=\langle e\rangle$，这导致$xs=sx$。

易知$C(K)$是K的特征子群。由于K在G中正规，根据引理7.13（i）可知$C(K)$在G中正规。如果$C(K)\neq\langle e\rangle$，则$C(K)$必然包含H。由此及$K=HS$导致S在K中正规。由引理7.13（ii）和（i）可知S在K中是完全不变的，从而在G中正规（因为$K\lhd G$）。这导致$H<S$，但这是不可能的。从而$C(K)=\langle e\rangle$。

（ii）令M象（i）中那样，假设B是G中m阶子群。现在$|BK|$可被$|B|=m$和$|K|=p^rq^s$所除尽。由于$(m,\ p)=1$，从而$|BK|$可被$p^rm=nm=|G|$除尽。因此$G=BK$。从而$G/K=BK/K=B/B\cap K$（系I.5.9），这导致$|B\cap K|=|B|/|G/K|=q^s$。从Sylow第二定理知$B\cap K$在K中与S共轭。进而，$B\cap K$在B中正规（因为$K\lhd G$），从而B包含在$N_G(B\cap K)$之中。证明共轭的子群有共轭的正规化子。从而$N_G(B\cap K)$和$N_G(S)=M$在G中共轭。因此$|N_G(B\cap K)|=|M|=m$。但是$|B|=m$，从而由$B<N_G(B\cap K)$导致$B=N_G(B\cap K)$。即B和M是共轭的。

（iii）令$D<G$，其中$|D|=k$，$k|m$。设M（阶数为m）和H（阶数为p^h，$(p,\ m)=1$）如（i）中所示。则$D\cap H=\langle e\rangle$而$|DH|=|D||H|/|D\cap H|=kp^r$。我们也有$|G|=kp^r$，$M\cap H=\langle e\rangle$和$MH=G$（因为$|MH|=|M||H|/|M\cap H|=mp^r=|G|$）。从而$M(DH)$

$=G$，因此 $|M\cap DH|=|M||DH|/|MDH|=m(kp^r)/mp^r=k$。令 $M^*=M\cap DH$。则M^*和D共轭（将（ii）用于群DH）。从而有 $a\in G$，$aM^*a^{-1}=D$。由于$M^*<M$，D包含在aMa^{-1}中，而aMa^{-1}与M共轭，因此是m阶子群。 ∎

在本节的最后让我们提一下长期未解决的 Burnside猜想：每个奇阶有限群都是可解的。这个著名的结果首先由 W.Feit 和 J. Thompson[61]于1963年证明。

习　题

1. (a) A_4不是它的Sylow子群的直积，但是A_4有如下的性质：$mn=12$，$(m, n)=1$则A_4有m阶子群。

   (b) S_3有1，2，3和6阶子群，但是它不是其Sylow子群的直积。

2. 设G是群而a，$b\in G$。将换位子$aba^{-1}b^{-1}\in G$表示成$[a,b]$。求证对于任意的a，b，$c\in G$，$[ab, c]=a[b, c]a^{-1}[a, c]$。

3. 如果H和K是群G的子群，令(H, K)是由$\{hkh^{-1}k^{-1}\mid h\in H, k\in K\}$所生成的$G$的子群。求证

   (a) (H, K)在$H\vee K$中正规。

   (b) 如果$(H, G')=\langle e\rangle$，则$(H', G)=\langle e\rangle$。

   (c) $H\lhd G\Longleftrightarrow(H, G)<H$。

   (d) 令$K\lhd G$并且$K<H$，则$H/K<C(G/K)\Longleftrightarrow(H, G)<K$。

4. 定义群G如下的子群链$\gamma_i(G)$：$\gamma_1(G)=G$，$\gamma_2(G)=(G, G)$，$\gamma_i(G)=(\gamma_{i-1}(G), G)$（见习题3）。求证$G$幂零$\Longleftrightarrow$存在某个$m$使得$\gamma_m(G)=\langle e\rangle$。

5. 幂零群的每个子群和商群都是幂零的。[提示：定理7.5 或者习题4.]

6. (Wielandt) 求证有限群G是幂零的$\Longleftrightarrow G$的每个极大真子群都是正规的。由此推出，每个极大真子群的指数都是素数。[提示：如果P是G的

Sylow p- 子群，求证每个子群如果包含 $N_G(p)$，则必是自身的正规化子，见定理5.11.〕

7. 如果N是幂零群G的非平凡正规子群，则$N \cap C(G) \neq \langle e \rangle$。

8. 如果D_n是正多边形群，生成元为n阶元素a和2阶元素b，则

   (a) $a^2 \in D'_n$

   (b) 如果n是奇数，则$D'_n \cong Z_n$。

   (c) 如果n是偶数，$n=2m$，则$D'_n \cong Z_m$。

   (d) D_n幂零$\Longleftrightarrow$$n$为2的幂。

9. 求证S_4的换位子群是A_4。什么是A_4的换位子群？

10. 当$n \leqslant 4$时S_4是可解的，但是S_8和S_4非幂零。

11. 非平凡有限可解群G必包含正规Abel子群$H \neq \langle e \rangle$。如果G不可解，则G必包含正规子群H，使得$H' = H$。

12. 不存在群G，使得$G' = S_4$。〔提示：习题9和5.12可能是有帮助的。〕

13. 如果G是群，则第i导出子群$G^{(i)}$是完全不变子群，从而$G^{(i)}$是正规子群。

14. 如果$N \lhd G$，$N \cap G' = \langle e \rangle$，则$N < C(G)$。

15. 如果H是有限可解群G的极大真子群，则$[G:H]$是素数幂。

16. 对于任意群G，$C(G)$是特征子群，但不一定是完全不变子群。

17. 如果G是Abel p-群，则子群$G[p]$（见引理2.5）在G中是完全不变的。

18. 如果G是有限幂零群，则G的每个极小正规子群均包含在$C(G)$中并且阶为素数。

8. 正规列与亚正规列

群的中心升列和导出子群列很有益处。这启示我们有必要去研究其它这样的序列。下面我们便着手这项工作，同时还要给出

幂零群与可解群的又一种刻划方式，并介绍著名的Jordan-Hölder定理。

定义8.1 群 G的亚正规列是子群链 $G=G_0>G_1>\cdots>G_n$，其中G_{i+1}在G_i中正规($0\leqslant i<n$)。商群G_i/G_{i+1} 均叫作该序列的因子，而序列中严格包含的个数（换句话说，即是非平凡因子的个数）叫作该序列的长度。如果G_i在G中正规（对于所有i)，则上述亚正规列称作正规列[5]。

亚正规列不一定是正规列（习题I.5.10)。

例 对于任意群G，导出列$G>G^{(1)}>\cdots>G^{(n)}$是正规列（见习题7.13)。如果G是幂零的，则中心升列$C_1(G)<\cdots<C_n(G)=G$是G的正规列。

定义8.2 假设$G=G_0>G_1>\cdots>G_n$是亚正规列。则形如 $G=G_0>\cdots>G_i>N>G_{i+1}>\cdots>G_n$或者$G=G_0>\cdots>G_n>N$的序列叫作原亚正规列的一步加细，是指$N\lhd G_i$并且$G_{i+1}\lhd N$(当 $i<n$时)。亚正规列S 通过有限多次一步加细而得到的任一亚正规列，均叫作S的细化。S的一个细化叫作真细化，是指它的长度大于S的长度。

定义8.3 亚正规列$G=G_0>G_1>\cdots>G_n=\langle e\rangle$叫作组成列，是指每个因子$G_i/G_{i+1}$都是单的。亚正规列$G=G_0>G_1>\cdots>G_n=\langle e\rangle$叫作可解列，是指每个因子均是 Abel 群。

在处理组成列时，下列事实经常被采用：如果N是群G的正规子群，则G/N的每个正规子群均有形式H/N，其中H是G 的正规子

5. 某些作者将我们这里的“亚正规列”叫作是“正规列”。

群并且包含N(系1.5.12)。因此当$G \neq N$时，G/N为单群$\Longleftrightarrow$ N在集合$\{M \mid M \lhd G,\ M \neq G\}$中极大（这样的子群$N$叫作$G$的极大正规子群）。

定理8.4 (i) 每个有限群G均有组成列。

(ii) 可解列的每个加细均是可解列。

(iii) 一个亚正规列是组成列当且仅当它没有真加细。

证明 (i) 假设G_1是G的极大正规子群，由系I.5.12可知G/G_1是单群。令G_2是G_1的极大正规子群，如此等等。由于G是有限群，这个过程必定终止于$G_n = \langle e \rangle$。因此$G > G_1 > \cdots > G_n = \langle e \rangle$是组成列。

(ii) 如果G_i/G_{i+1}为 Abel 群而$G_{i+1} \lhd H \lhd G_i$，则 H/G_{i+1} 是Abel群（因为它是G_i/G_{i+1}的子群），而G_i/H也是Abel群（因为根据第三同构定理I.5.10，它同构于商群$(G_i/G_{i+1})/(H/G_{i+1})$）。由此立刻推出结论。

(iii) 如果 $G_{i+1} \lneq H \lneq G_i$，则$H/G_{i+1}$是$G_i/G_{i+1}$ 的真正规子群，并且由系I.5.12可知，G_i/G_{i+1} 的每个真正规子群均有如此形式。然后再考虑到如下的事实即可证得结论：亚正规列$G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$有真加细$\Longleftrightarrow$存在子群$H$，使得

$G_{i+1} \lneq H \lneq G_i$(对于某个$i$)。∎

定理8.5 群G是可解的$\Longleftrightarrow$$G$有可解列。

证明 如果G可解，由定理7.8可知其导出列$G > G^{(1)} > G^{(2)} > \cdots > G^{(n)} = \langle e \rangle$也是可解的。如果$G = G_0 > G_1 > \cdots > G_n = \langle e \rangle$是$G$的可解列，则$G/G_1$为 Abel 群。从而由定理7.8可知$G_1 > G^{(1)}$。

同样由G_1/G_2为Abel群推出$G_2>G_1'>G^{(2)}$。继续下去，则可以归纳证得$G_i>G^{(i)}$(对于所有i)。特别地$\langle e\rangle=G_n>G^{(n)}$，从而$G$是可解的。∎

例 正多边形群D_n是可解群，因为$D_n>\langle a\rangle>\langle e\rangle$是可解列，其中$a$为$n$阶元素(从而$D_n/\langle a\rangle\cong Z_2$)。类似地，如果$|G|=pq(p>q$均为素数)，则$G$包含$p$阶元素$a$，并且$\langle a\rangle$在$G$中正规(系4.10)。因此$G>\langle a\rangle>\langle e\rangle$是可解列，即$G$是可解群。更一般地我们有

命题8.6 有限群G是可解的$\Longleftrightarrow G$有组成列，并且其因子均为素阶循环群。

证明 具有循环因子的（组成）列显然是可解列。反之，假设$G=G_0>G_1>\cdots>G_n=\langle e\rangle$是$G$的可解列，如果$G_0\neq G_1$，令$H_1$为$G=G_0$中包含$G_1$的极大正规子群。如果$H_1\neq G_1$，再令$H_2$为$H_1$中包含$G_1$的极大正规子群，如此等等。由于$G$有限，便给出序列$G>H_1>H_2>\cdots>H_k>G_1$，其中每个子群都是其前一个群的极大正规子群，从而每个因子都是单群。对于每一对$(G_i,\ G_{i+1})$都如此作，根据定理8.4(ii)，便给出原序列的可解加细$G=N_0>N_1>\cdots>H_r=\langle e\rangle$。序列中每个因子都是Abel单群，从而是素阶循环群（习题I.4.3)。因此$G>N_1>\cdots>N_r=\langle e\rangle$是组成列。∎

一个给定的群可以有许多亚正规列或者可解列。同样地，也可能有一些不同的组成列（习题1)。但是我们现在要证明，一个群的任意两个组成列在下面意义下是等价的。

定义8.7 群G的两个亚正规列S和T叫作等价的，如果在S和T的非平凡因子之间存在着一一对应，使对应的因子彼此同构。

两个等价的亚正规列不一定有同样多项，但是必须有同样的

长度（即有同样多的非平凡因子）。显然，亚正规列的等价是等价关系。

引理8.8 如果S是群G的组成列，则S的每个加细均与S等价。

证明 设S为$G=G_0>G_1>\cdots>G_n=\langle e\rangle$。由定理8.4 (iii)可知$S$没有真加细。因此，$S$的加细只能是再加入某些$G_i$。从而$S$的任一加细均与$S$有同样的非平凡因子，因此与$S$等价。∎

下一个引理纯粹是技术性的。从定理8.10的证明即可看出这一引理的价值。

引理8.9 (Zassenhaus) 设A^*,A,B^*,B均是群G的子群，并且A^*在A中正规，B^*在B中正规。则

(i) $A^*(A\cap B^*)$是$A^*(A\cap B)$的正规子群，

(ii) $B^*(A^*\cap B)$是$B^*(A\cap B)$的正规子群，

(iii) $A^*(A\cap B)/A^*(A\cap B^*)\cong B^*(A\cap B)/B^*(A^*\cap B)$。

证明 由于B^*在B中正规，从而$A\cap B^*=(A\cap B)\cap B^*$是$A\cap B$的正规子群(定理I.5.3(i))。类似地，$A^*\cap B$在$A\cap B$中正规。因此$D=(A^*\cap B)(A\cap B^*)$是$A\cap B$的正规子群（定理I.5.3(iii)和习题I.5.13)。定理I.5.3(iii)也导致$A^*(A\cap B)$和$B^*(A\cap B)$分别是A和B的子群。我们将要定义一个满同态$f:A^*(A\cap B)\to(A\cap B)/D$，并且核为$A^*(A\cap B^*)$。这就推出$A^*(A\cap B^*)$在$A^*(A\cap B)$中正规（定理I.5.5），并且$A^*(A\cap B)/A^*(A\cap B^*)\cong(A\cap B)/D$（系I.5.7)。

定义f：$A^*(A\cap B)\to(A\cap B)/D$如下：如果$a\in A^*$，$c\in A\cap B$，令$f(ac)=Dc$。则$f$是可定义的，因为$ac=a_1c_1$($a,a_1\in A^*$，$c,c_1\in A\cap B$)导致$c_1c^{-1}=a_1^{-1}a\in(A\cap B)\cap A^*=A^*\cap B<D$，从

而$Dc_1 = Dc$。 f 显然是满射。又f是满同态，因为$f[(a_1c_1)(a_2c_2)] = f(a_1a_3c_1c_2) = Dc_1c_2 = Dc_1Dc_2 = f(a_1c_1)f(a_2c_2)$，其中$a_i \in A^*$，$c_j \in A \cap B$，而$c_1a_2 = a_3c_1$，这是因为$A^*$在$A$中正规.最后$ac \in \mathrm{Ker}f \Leftrightarrow c \in D \Leftrightarrow c = a_1c_1$，$a_1 \in A^* \cap B, c_1 \in A \cap B^* \Leftrightarrow ac = (aa_1)c_1 \in A^*(A \cap B^*)$。因此$\mathrm{Ker}f = A^*(A \cap B^*)$。

由对称的推理过程表明$B^*(A^* \cap B)$在$B^*(A \cap B)$中正规，并且$B^*(A \cap B)/B^*(A^* \cap B) \cong (A \cap B)/D$。由此立即得出 (iii)。∎

定理8.10 (Schreier) 群G的任意两个亚正规列[正规列]均有等价的亚正规[正规]加细。

证明 设$G = G_0 > G_1 > \cdots > G_n$和$G = H_0 > H_1 > \cdots > H_m$均为亚正规[正规]列。令$G_{n+1} = \langle e \rangle = H_{m+1}$，并且对于每个$0 \leqslant i \leqslant n$，考虑群

$$G_i = G_{i+1}(G_i \cap H_0) > G_{i+1}(G_i \cap H_1) > \cdots > G_{i+1}(G_i \cap H_j) > G_{i+1}(G_i \cap H_{j+1}) > \cdots > G_{i+1}(G_i \cap H_m) > G_{i+1}(G_i \cap H_{m+1}) = G_{i+1}$$

对于每个$0 \leqslant j \leqslant m$，Zassenhaus 引理 (用于$G_{i+1}$，$G_i$，$H_{j+1}$和$H_j$)表明$G_{i+1}(G_i \cap H_{j+1})$在$G_{i+1}(G_i \cap H_j)$中正规。[如果两个原始列均是正规列，由定理I.5.3(iii)，习题I.5.2和I.5.13可知每个$G_{i+1}(G_i \cap H_j)$都在G中正规。]在每个G_i和G_{i+1}中间均插入这些群，然后用$G(i,j)$表示$G_{i+1}(G_i \cap H_j)$，便给出序列$G_0 > G_1 > \cdots > G_n$的亚正规[正规]加细。

$$G = G(0,0) > G(0,1) > \cdots > G(0,m) > G(1,0) > G(1,1) > G(1,2) > \cdots > G(1,m) > G(2,0) > \cdots > G(n-1,m) > G(n,0) > \cdots > G(n,m),$$

其中$G(i,0) = G_i$。注意这个加细列共有$(n+1)(m+1)$个(不必不

同的）项．由对称的推理过程得到 $G=H_0>H_1>\cdots>H_m$ 的一个加细（其中$H(i,j)=H_{j+1}(G_i\cap H_j)$，$H(0,j)=H_j$）：

$$G=H(0,0)>H(1,0)>\cdots>H(n,0)>H(0,1)>H(1,1)>H(2,1)>\cdots>H(n,1)>H(0,2)>\cdots>H(n,m-1)>H(0,m)>\cdots>H(n,m).$$

这个加细列也有$(n+1)(m+1)$项．对于每对$(i,j)$$(0\leqslant i\leqslant n,\ 0\leqslant j\leqslant m)$，由Zassenhaus 引理8.9（用于$G_{i+1},G_i,H_{j+1}$和$H_j$）可知有同构：

$$\frac{G(i,\ j)}{G(i,j+1)}=\frac{G_{i+1}(G_i\cap H_j)}{G_{i+1}(G_i\cap H_{j+1})}\cong\frac{H_{j+1}(G_i\cap H_j)}{H_{j+1}(G_{i+1}\cap H_j)}=\frac{H(i,j)}{H(i+1,j)}.$$

这就给出因子之间所希望的一一对应，从而证明了这两个加细列是等价的．∎

定理8.11 （Jordan-Hölder） 群 G 的任意两个组成列均彼此等价．因此，每个群的组成列都唯一地决定了一串单群．

注记：此定理并没有谈到一给定群之组成列的存在性．

证明 因为组成列是亚正规列，根据定理8.10，任意两个组成列均有等价的加细．但是由引理8.8，组成列S的加细等价于S．从而任意两个组成列都是等价的．∎

Jordan-Hölder定理指明，单群的某些知识可能是有用的．事实上，近年来寻找和研究（有限）单群成为一些群论学家的很活跃的主要课题，并且取得了显著的成果．虽然已经判定和刻划了许多个单群族，但是迄今还没有将所有有限单群作完全的分类〔注〕．

〔注〕 这个问题于1981年已经得到完全的解决——译者

当然，交错群$A_n(n\neq 4)$形成一个单群族（定理I.6.10）。可以证明，在阶数小于200的群中，(不计同构) 只有两个非Abel 单群，即A_5和S_7的一个168阶子群(见习题13—20)。关于单群的进一步讨论可见J.Rotman[19]。

习　题

1. (a) 求D_4的由4个子群组成的正规列。
   (b) 求群D_4的全部组成列。
   (c) 对于群A_4作(b)。
   (d) 对于群$S_3\times Z_2$作(b)。
   (e) 求S_4和D_6的全部组成因子。

2. 如果$G=G_0>G_1>\cdots>G_n$是有限群G的亚正规列，则$|G|=\left(\prod_{i=0}^{n-1}|G_i/G_{i+1}|\right)|G_n|$。

3. 如果N是群G的正规单子群，而G/N有组成列，则G也有组成列。

4. 一个群的组成列是具有极大（有限）长度的亚正规列。

5. 一个Abel群具有组成列的充要条件是它为有限群。

6. 如果$H\lhd G$，其中G有组成列，则G必有组成列使H为其中之一项。

7. 具有组成列的可解群必为有限群。

8. 如果H和K均是G的可解子群，并且$H\lhd G$,则HK是G的可解子群。

9. 每个p^2q阶群(p，q为素数) 均可解。

10. 群G是幂零的$\Longleftrightarrow G$存在正规列$G=G_0>G_1>\cdots>G_n=\langle e\rangle$，使得对每个$i$，$G_i/G_{i+1}<C(G/G_{i+1})$。

11. (a) 证明定理7.11对于幂零群是不对的[考虑S_3]。
    (b) 如果$H<C(G)$并且G/H幂零，则G幂零。

12. 将Jordan-Hölder定理用于群Z_n来证明引论中的算术基本定理6.7。

13. 每个60阶单群均同构于A_5.〔提示：利用系4.9.如果$H<G$，则〔$G:H$〕$\geqslant 5$(因为当$n\leqslant 4$时$|S_n|<60$)．如果〔$G:H$〕$=5$，由定理I.6.8可知$G\cong A_5$.如果假设G没有指数为5的子群，则导致矛盾.〕

14. 不存在阶数小于60的非Abel单群.

15. 令G是S_7中由(1234567)和(26)(34)生成的子群.求证$|G|=168$.

下面习题16—20扼要地描绘了下列事实的一个证明：习题15中的群G是单群.象在定义4.1后面第一个例子那样，我们将G作用于集合$S=\{1,2,3,4,5,6,7\}$之上，并且利用习题4.6.

16. 群G是可迁的（见习题4.6）.

17. 对于每个$x\in S$，G_x是G的极大（真）子群．这个事实的证明可分成如下几步依次进行：(a) G的一个区组(block)是S的子集T，使得对每个$g\in G$，或者$gT\cap T=\phi$，或者$gT=T$，其中$gT=\{gx|x\in T\}$.证明：如果T是区组，则$|T|$可除尽7.〔提示：令$H=\{g\in G|gT=T\}$，证明对于$x\in T$，$G_x<H$并且〔$H:G_x$〕$=|T|$.从而$|T|$除尽〔$G:G_x$〕$=$〔$G:H$〕〔$H:G_x$〕.但是由习题4.6(a)和定理4.3知道〔$G:G_x$〕$=7$.〕

(b) 如果G_x不是极大子群，则有G的一个区组T，使得$|T|\neq 7$，而这与(a)相矛盾.〔提示：如果$G_x\leqq H<G$，求证H在S上不可迁（因为$1\leqslant$〔$H:G_x$〕$<|S|$，则可迁性与习题4.6(d)相矛盾).令$T=\{hx|h\in H\}$.由于H不可迁，从而$|T|<|S|=7$，又由于$H\neq G_x$，从而$|T|>1$．证明T是一个区组.〕

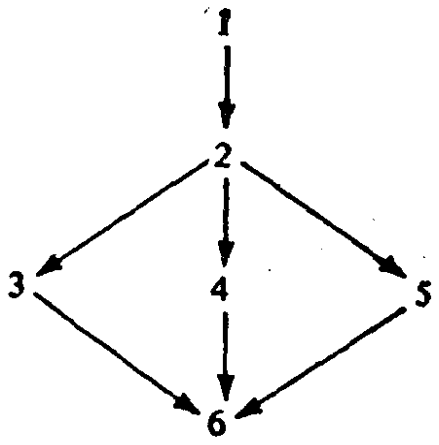
18. 如果(1)$\neq N\lhd G$，则$7||N|$.〔提示：习题4.6(c)$\Longrightarrow G_x\leqq NG_x$（对于每个$x\in S$)$\Longrightarrow NG_x=G$(对于每个$x\in S$，由习题17)$\Longleftrightarrow N$在$S$上可迁$\Longrightarrow 7||N|$(由习题4.6(d)).〕

19. 群G包含一个7阶子群P，使得G中包含P的最小正规子群必为G自己.

20. 如果(1)$\neq N<G$，则$N=G$.从而G是单群.〔利用习题I.5.19和习题18来证明$P<N$.再利用习题19.〕

第III章　环

除了群以外，另一个代数基本对象是环。（在一给定类中的）所有环的同构分类问题比群还要复杂。在第IX章中我们将给出这方面的部分结果。本章的大部分内容是介绍环论中一些事实，这些事实是在代数各领域中最常用到的。前两节处理环，同态和理想。这些内容中有许多（不是全部）只不过是群论中相应内容到环上的直接推广。第3节和第4节是谈交换环，这种环在许多方面很象整数环。在第3节研究可除性，因子分解，欧氏环，主理想整环和唯一因子分解。第 4 节把从整数环构作有理数域的通常方法加以推广，并且较为详细的考虑了任意交换环的商环。最后两节研究环R上的n 元多项式环。特别地，我们在第 6 节中，对于多项式环再次研究了第 3 节中的那些概念。



这一章各节之间的依赖关系大致如右图所示：第 6 节只需要第 4 节和第 5 节的一部分结果。

1. 环 与 同 态

我们要定义环论中一些基本概念，给出许多例子，并提供一些常常要用到的计算性结果。学习本节的唯一困难是：需要在短时间内熟悉大量的术语。

定义1.1 环是一个非空子集R与两个二元运算(通常表示成加法(+)和乘法)，使得：

(i) $(R,+)$是Abel群；

(ii) 对于所有$a,b,c\in R$，$(ab)c=a(bc)$（乘法结合律）；

(iii) $a(b+c)=ab+ac$，$(a+b)c=ac+bc$(左、右分配律)。

假如此外还满足

(iv) 对所有$a,b\in R$，$ab=ba$，

则称R为交换环。如果R包含元素1_R，使得

(v) 对所有$a\in R$，均有$1_Ra=a1_R=a$，

则称R为具有幺元素的环（或叫含幺环）。

注记：符号1_R也用来表示恒等映射$1_R: R\to R$。但是在课文中使用时不会产生混淆。

环中加法群的幺元素叫作环的零元素，表示成0。如果R是环，$a\in R$，而$n\in\mathbb{Z}$，则na具有通常加法群中的意义（定义I.1.8)。例如当$n>0$时$na=a+a+\cdots+a$(n个)。在给出环的例子之前，我们有

定理1.2 设R是环，则

(i) 对所有$a\in R$，$0a=a0=0$。

(ii) 对所有a，$b\in R$，$(-a)b=a(-b)=-(ab)$。

(iii) 对所有$a,b\in R$，$(-a)(-b)=ab$。

(iv) 对所有$n\in\mathbb{Z}$和$a,b\in R$，$(na)b=a(nb)=n(ab)$。

(v) 对所有$a_i,b_j\in R$，$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j$。

证明概要 (i) $0a=(0+0)a=0a+0a$，从而$0a=0$。

(ii) $ab+(-a)b=(a+(-a))b=0b=0$，由定理I.1.2 (iii)便知$(-a)b=-(ab)$。从(ii)可推出(iii)。用归纳法可以证明(v)。而(iv)是(v)的特殊情形。∎

下面三个定义中要引进更多的术语。然后便给出一些例子。

定义1.3 环R中的非零元素a叫作左〔右〕零因子，是指存在非零元素$b\in R$，使得$ab=0$〔$ba=0$〕。R中同时是左零因子和右零因子的元素叫作R的零因子。

不难验证，环R没有左右零因子的充要条件是在R中具有左、右消去律，即对于所有的$a,b,c\in R$，并且$a\neq 0$，则

$ab=ac$或者$ba=ca\Rightarrow b=c$

定义1.4 含幺环R中元素a叫作左〔右〕可逆的，如果存在$c\in R$〔$b\in R$〕，使得$ca=1_R$〔$ab=1_R$〕。这时，元素c和b分别叫作a的左逆和右逆。如果元素$a\in R$同时左可逆和右可逆，便称为可逆元素或者叫作单位。

注记：(i) 含幺环R中单位a的左逆和右逆元素必然相等（因为$ab=1_R=ca$导致$b=1_Rb=(ca)b=c(ab)=c1_R=c$）。

(ii) 含幺环R中的全部单位所成的集合形成乘法群。

定义1.5 含幺交换环R中如果没有零因子，并且$1_R \neq 0$，便称R是整环，含幺环D中如果$1_D \neq 0$，并且每个非零元素均是单位，则称D是除法环或者体。交换除法环叫作域。

注记：(i) 每个零环和每个体均至少有两个元素(即0和1_R)。

(ii) 含幺环R是体的充要条件是R的非零元素全体形成乘法群（见定义1.4后面的注记(ii)）。

(iii) 每个域F都是整环，因为$ab=0$和$a\neq 0$导致$b=1_F b$
$=(a^{-1}a)b=a^{-1}(ab)=a^{-1}0=0$

例 整数环是整环。偶数集合E是不具有幺元素的交换环。$\boldsymbol{Q}$(有理数集合)，$\boldsymbol{R}$(实数集合)与$\boldsymbol{C}$(复数集合) 对于通常的加法和乘法运算均是域。当$n\geqslant 2$时，$\boldsymbol{Q}$(或者$\boldsymbol{R}$，$\boldsymbol{C}$) 上$n\times n$的方阵全体形成含幺非交换环，这个环中的单位恰好是非异方阵。

例 对于每个正整数n，模n整数集合Z_n是环。详见定理I.1.5后面的例子。如果n不是素数，比如设$n=kr$，$k>1$，$r>1$，则$\bar{k}\neq\bar{0}$，$\bar{r}\neq\bar{0}$，但是$\bar{k}\,\bar{r}=\overline{kr}=\bar{n}=\bar{0}$(在$Z_n$中)，从而$\bar{k}$和$\bar{r}$均是零因子。如果$p$为素数，由习题I.1.7可知$Z_p$是域。

例 设A是Abel群，而End$A$是全部自同态$f: A\to A$所形成的集合。在End$A$中定义加法为$(f+g)(a)=f(a)+g(a)$。验证$f+g\in$End$A$。由于A是Abel群，这就使得End$A$也是Abel群。假定End$A$中乘法是函数的合成。则End$A$是含幺(可能不交换)环。其中幺元素是恒等自同态$1_A: A\to A$。

例 令G是(乘法)群，而R是环。以$R(G)$表示加法群$\sum_{g\in G} R$(即对每个$g\in G$都有一个R)，为方便起见，我们对于$R(G)$中元

素采用新的记号。$R(G)$中元素$x=\{r_g\}_{g\in G}$只有有限多个非零坐标。设它们是$r_{g_1},\cdots,r_{g_n}(g_i\in G)$。我们将$x$表示成形式和$r_{g_1}g_1+r_{g_2}g_2+\cdots+r_{g_n}g_n$或者$\sum_{i=1}^{n} r_{g_i}g_i$。我们也允许某些$rg_i$是零，从而$R(G)$中的一个元素可能有形式上不同的写法（例如$r_1g_1+0g_2=r_1g_1$。采用这种记号，群$R(G)$中的加法可以写成

$$\sum_{i=1}^{n} rg_ig_i+\sum_{i=1}^{n} s_{g_i}g_i=\sum_{i=1}^{n}(r_{g_i}+s_{g_i})g_i。$$

（必要时插入一些零系数，我们总可以假定两个形式和包含有同样的下标$g_1,\cdots g_n$）。在$R(G)$中定义乘法为

$$\Big(\sum_{i=1}^{n} r_ig_i\Big)\Big(\sum_{j=1}^{m} s_jg_j\Big)=\sum_{i=1}^{n}\sum_{j=1}^{m}(r_is_j)(g_ig_j)。$$

由于在R和G中均已分别定义了乘积r_is_j和g_ig_j，从而上式是有意义的，并且正如我们所希望的，右边的表达式是形式和。对于这两种运算$R(G)$是环，叫作G在R上的群环。$R(G)$为交换环的充要条件是R和G分别是交换环和变换群。如果1_R和e分别是R和G的幺元素，则1_Re是$R(G)$的幺元素。

例 令$\boldsymbol{R}$为实数域，S是符号集合$\{1,i,j,k\}$。令K是加法Abel群$\boldsymbol{R}\oplus\boldsymbol{R}\oplus\boldsymbol{R}\oplus\boldsymbol{R}$，并且将$K$中元素写成形式和$(a_0,a_1,a_2,a_3)=a_0\mathbf{1}+a_1i+a_2j+a_3k$。于是：

$$a_0\mathbf{1}+a_1i+a_2j+a_3k=b_0\mathbf{1}+b_1i+b_2j+b_3k\Longleftrightarrow a_i=b_i\quad(0\leqslant i\leqslant 3)$$

我们又规定$a_0\mathbf{1}\in K$等同于$a_0\in\boldsymbol{R}$，并且系数为零的项可以略去不写（例如$4+2j=4\cdot 1+0i+2j+0k$而$i=0+1i+0j+0k$）。然后在

K中定义加法

$$(a_0+a_1i+a_2j+a_3k)+(b_0+b_1i+b_2j+b_3k)$$
$$=(a_0+b_0)+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k.$$

同时在K中定义乘法

$$(a_0+a_1i+a_2j+a_3k)(b_0+b_1i+b_2j+b_3k)$$
$$=(a_0b_0-a_1b_1-a_2b_2-a_3b_3)+(a_0b_1+a_1b_0+a_2b_3$$
$$-a_3b_2)i+(a_0b_2+a_2b_0+a_3b_1-a_1b_3)j$$
$$+(a_0b_3+a_3b_0+a_1b_2-a_2b_1)k.$$

将两个形式和逐项相乘并遵从如下一些法则，即可得到上述乘积公式：

(i) 结合律；

(ii) $ri=ir$, $rj=jr$, $rk=kr$(对于所有$r\in\mathbb{R}$)；

(iii) $i^2=j^2=k^2=ijk=-1$, $ij=-ji=k$, $jk=-kj=i$, $ki=-ik=j$.

K对于这个乘法是非交换的体，非零元素$a_0+a_1i+a_2j+a_3k$的乘法逆是$(a_0/d)-(a_1/d)i-(a_2/d)j-(a_3/d)k$，其中$d=a_0^2+a_1^2+a_2^2+a_3^2$，$K$叫作实四元数体．我们也可以把实四元数体看成2阶复矩阵环的某个子环（习题8）．

定义1.1表明，环R对于乘法形成半群（如果R有幺元素，则形成幺半群）．从而可以利用定义I.1.8在R中定义指数运算．对于每个$a\in R$和$n\in\mathbb{N}^*$，我们有$a^n=a\cdots a$(n个因子)，并且若R为含幺环，则$a^0=1_R$，根据定理I.1.9便有

$$a^ma^n=a^{m+n},\quad (a^m)^n=a^{mn}.$$

在环R中采用通常的方式定义减法：$a-b=a+(-b)$．显然对所有$a,b,c\in R$，均有$a(b-c)=ab-ac$，$(a-b)c=ac-bc$．

下一定理在计算中常常是有用的，让我们回忆一下，如果k和

n是整数并且$0 \leqslant k \leqslant n$，则二项式系数为$\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$，其中$0! = 1$而$n! = n(n-1)(n-2)\cdots 2\cdot 1$（对于$n \geqslant 1$）。$\binom{n}{k}$是整数（习题10）。

定理1.6 （二项式定理）令R是含幺环，n为正整数，$a, b, a_1, a_2, \cdots, a_s \in R$。

(i) 如果$ab = ba$，则 $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$。

(ii) 如果对所有i和j，$a_i a_j = a_j a_i$，则

$$(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{(i_1!)\cdots(i_s!)} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s},$$

其中求和是过全体满足 $i_1 + i_2 + \cdots + i_s = n$ 的n数组$(i_1, i_2, \cdots, i_s)$

证明概要 (i) 对于n用数学归纳法，同时利用事实 $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ （对于$k < n$）（习题10(c)）。其中分配律和a与b的可交换性是关键。

(ii) 对s作数学归纳法。情形$s=2$即是第(i)部分，因为$(a_1 + a_2)^n = \sum_{k=0}^{n} \binom{n}{k} a_1^k a_2^{n-k} = \sum_{k+j=n} \frac{n!}{k!\,j!} a_1^k a_2^j$。如果定理对于$s$成立，注意从第(i)部分可知

$$\begin{aligned}(a_1 + \cdots + a_s + a_{s+1})^n &= ((a_1 + \cdots + a_s) + a_{s+1})^n \\ &= \sum_{k=0}^{n} \binom{n}{k} (a_1 + \cdots + a_s)^k a_{s+1}^{n-k}\end{aligned}$$

$$= \sum_{k+j=n} \frac{n!}{k!j!}(a_1 + \cdots + a_s)^k a_{s+1}^j$$

然后利用归纳假设和一些计算即可证明。∎

定义1.7 令R和S为环，函数$f: R \to S$叫作环同态，是指对所有$a, b \in R$，

$$f(a+b) = f(a) + f(b) \quad f(ab) = f(a)f(b)$$

注记：不难看出，全部环组成的类与全部环同态形成一个(具体) 范畴。

在上下文很清楚的时候，我们常常把“环同态”简单地称之为“同态”。特别地，环的同态也是其凭借(underlying)加法群的同态。从而可以使用同样的术语：环的单同态[满同态，同构]即是环的一个同态，它同时是单射[满射，一一对应]。环的单同态$R \to S$有时叫作R在S中的嵌入。同构$R \to R$叫作R的自同构。

环同态 $f: R \to S$ 的核就是指f作为加法群映射的核，即 $\operatorname{Ker} f = \{r \in R \mid f(r) = 0\}$。类似地，$f$ 的象是$\operatorname{Im} f = \{s \in S \mid$ 存在某个$r \in R$，使得$s = f(r)\}$。如果R和S均有幺元素1_R和1_S，我们不需要一个环同态将1_R映成1_S（见习题15，16)。

例 正则映射 $\boldsymbol{Z} \to Z_m$，$k \mapsto \bar{k}$是环的满同态。映射 $Z_3 \to Z_6$，$\bar{k} \mapsto \overline{4k}$可以定义出环的单同态。

例 假设G和H是乘法群，$f: G \to H$是群同态。令R是环并且定义群环上的映射：

$$\bar{f}: R(G) \to R(H), \quad \bar{f}\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} r_i f(g_i).$$

则$\bar{f}$是环同态。

定义1.8 令R 是环。如果存在最小正整数n，使得对于所有

$a\in R$，$na=0$，则称R的特征是n。（写成：Char $R=n$）。如果不存在这样的n，则称R的特征是零。

定理1.9 设R是含幺环，并且其特征$n>0$。

(i) 如果φ：$\mathbb{Z}\to R$是由$m\mapsto m1_R$给出的映射，则φ是环同态，并且核为$\langle n\rangle=\{kn\mid k\in\mathbb{Z}\}$。

(ii) n是满足$n1_R=0$的最小正整数。

(iii) 如果R没有零因子（特别若R是整环），则n是素数。

证明概要 (ii)如果k是满足$k1_R=0$的最小正整数，则由定理1.2可知对于每个$a\in R$，$ka=k(1_Ra)=(k1_R)a=0a=0$。

(iii) 如果$n=kr$，其中$1<k<n$，$1<r<n$，则$0=n1_R=(kr)1_R1_R=(k1_R)(r1_R)$导致$k1_R=0$或者$r1_R=0$，这就与(ii)相矛盾。∎

定理1.10 每个环R都可以嵌到含幺环S中。环S（不是唯一的）可以取成特征是零，也可以取成与R的特征相同。

证明概要 令S为加法Abel群$R\oplus\mathbb{Z}$，在S中定义乘法为

$(r_1,\ k_1)(r_2,\ k_2)=(r_1r_2+k_2r_1+k_1r_2,\ k_1k_2)$ $(r_i\in R, k_i\in\mathbb{Z})$。证明$S$是含幺环，其中$1_S=(0,\ 1)$，$S$的特征是零，并且映射$R\to S$，$r\mapsto(r,\ 0)$是环的单同态（即嵌入）。如果Char $R=n>0$，取$S=R\oplus Z_n$，而乘法定义为

$$(r_1,\ \bar{k}_1)(r_2,\bar{k}_2)=(r_1r_2+k_2r_1+k_1r_2,\ \bar{k}_1\bar{k}_2)$$

其中$r_i\in R$而$\bar{k}_i\in Z_n$是$k_i\in\mathbb{Z}$在正则映射之下的象。类似可以证明同样结果，并且Char $S=n$。∎

习　题

1. (*a*) 设G是(加法)Abel群. 在G中定义乘法运算为 $ab=0$ (对所有a, $b\in G$). 则G是环.

(*b*) 设 S 是某个固定集合U的全部子集所构成的集合, 定义 $A+B=(A-B)\cup(B-A)$, $AB=A\cap B$.则S是环. S是否为交换环? 它是否有幺元素?

2. 设 $\{R_i|i\in I\}$ 是一族含幺环. 定义乘法为按坐标相乘, 便可将 Abel群的直和 $\sum_{i\in I}R_i$作成环. $\sum_{i\in I}R_i$是否具有幺元素?

3. 环R叫作Boole环, 是指$a^2=a$ (对于每个$a\in R$). 证明每个Boole环都是交换环并且$a+a=0$ (对于所有$a\in R$). 〔关于Boole 环的例子见习题 1 (*b*). 〕

4. 设R是环而S是非空集合. 则群 $M(S, R)$ (习题I.1.2) 对于如下定义的乘法是环: $f,g\in M(S,R)$ 的乘积是函数$S\to R$, $S\mapsto f(s)g(s)$.

5. 如果A是Abel群$\mathbf{Z}\oplus\mathbf{Z}$, 则End A是非交换环.

6. (具有多于一个元素的) 有限环如果没有零因子, 则必是体 (特别地, 有限整环是域.)

7. 设R是环 (具有多于一个元素), 并且对于每个非零$a\in R$, 均有唯一的$b\in R$, 使得$aba=a$. 求证:

(*a*) R没有零因子.

(*b*) $bab=b$.

(*c*) R有幺元素.

(*d*) R是体.

8. 令R是所有形如 $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ 的二阶复矩阵所构成的集合, 其中 $\overline{z}$和$\overline{w}$分别是z和w的复共轭 (即$c=a+b\sqrt{-1}\Longleftrightarrow\overline{c}=a-b\sqrt{-1}$). 则 R

是体，并且同构于实四元数体K。〔提示：定义同构$K\to R$，方法是令1，i，j，$k\in K$的象分别为矩阵

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}\sqrt{-1}&0\\0&\sqrt{-1}\end{pmatrix},\ \begin{pmatrix}0&1\\-1&0\end{pmatrix},\ \begin{pmatrix}0&\sqrt{-1}\\\sqrt{-1}&0\end{pmatrix}.$$〕

9. (*a*) 实四元数体K的子集$G=\{1,\ -1,\ i,\ -i,\ j,\ -j,\ k,\ -k\}$对于乘法形成群。

(*b*) G同构于四元数群（习题I.4.14和I.2.3）。

(*c*) 环K与群环$\mathbf{R}(G)$有什么区别（$\mathbf{R}$是实数域）？

10. 令k，n是整数，$0\leqslant k\leqslant n$，而$\binom{n}{k}$是二项式系数$n!/k!(n-k)!$，其中$0!=1$而$n!=n(n-1)(n-2)\cdots 2\cdot 1$（对于$n>0$）。求证

(*a*) $\binom{n}{k}=\binom{n}{n-k}$

(*b*) $\binom{n}{k}<\binom{n}{k+1}$（对于$k+1\leqslant n/2$）

(*c*) $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$（对于$k<n$）

(*d*) $\binom{n}{k}$是整数。

(*e*) 如果p是素数并且$1\leqslant k\leqslant p^n-1$，则$\binom{p^n}{k}$可以被$p$除尽。

〔提示：(*b*)注意$\binom{n}{k+1}=\binom{n}{k}\frac{n-k}{k+1}$。(*d*)注意$\binom{m}{0}=\binom{m}{m}=1$然后利用(*c*)部分结果对$n$作数学归纳法。〕

11. 令R是特征p的含幺交换环。如果$a,b\in R$，则对每个整数$n\geqslant 0$，$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$。〔见定理1.6和习题10。注意如果$p=2$则$b=-b$.〕

12. 环中元素a叫作幂零的，如果对于某个n有$a^n=0$。证明在交换环中，如果a和b是幂零的，则$a+b$也是幂零的。证明对于非交换环，这个结果可能不对。

13．在环R中下列二条件是等价的。

（a） R不具有非零的幂零元素（见习题12）。

（b） 如果$a\in R$并且$a^2=0$，则$a=0$。

14．令 R 是具有素特征 p 的交换环，映射 $R\to R$，$r\mapsto r^p$ 是环同态，称作Frobenius同态〔见习题11〕。

15．（a） 给出环的非零同态f：$R\to S$ 的例子，使得 $f(1_R)\neq 1_S$，其中1_R 和1_S分别是环R和S中幺元素。

（b） 如果f：$R\to S$是含幺环之间的满同态，则$f(1_R)=1_S$。

（c） 如果f：$R\to S$是含幺环之间的同态，u是 R中的单位，并且$f(u)$也是S中的单位，则$f(1_R)=1_S$并且$f(u^{-1})=f(u)^{-1}$。〔注意：不难给出如下的例子：即使u是R中的单位，$f(u)$也不一定为S中单位。〕

16．设f：$R\to S$是环同态，并且对某个非零元素$r\in R$，$f(r)\neq 0$。如果R有幺元素而S没有零因子，则S是含幺环，并且其幺元素是$f(1_R)$。

17．（a） 如果R是环，则如下定义的R^{OP}也是环。R^{OP} 的凭借集合恰好为R并且R^{OP}中加法与R中加法一致。R^{OP}中乘法（表示成$\circ$）定义为$a\circ b=ba$，其中ba是R中乘积。R^{OP}叫作R的反环。

（b） R具有幺元素$\Leftrightarrow R^{OP}$具有幺元素。

（c） R为体$\Leftrightarrow R^{OP}$为体。

（d） $(R^{OP})^{OP}=R$。

（e） 如果S是环，则$R\cong S\Leftrightarrow R^{OP}\cong S^{OP}$。

18．设$\mathbf{Q}$是有理数域而R是任意环。如果f，g：$\mathbf{Q}\to R$是环同态，使得$f|\mathbf{Z}=g|\mathbf{Z}$，则$f=g$。〔提示：证明对$n\in\mathbf{Z}(n\neq 0)$，$f(1/n)g(n)=g(1)$，从而$f(1/n)=g(1/n)$。〕

2. 理　想

就象正规子群在群论中起着很重要的作用一样，理想在环的

研究中起着类似的作用。我们首先讲理想的基本性质，其中包括刻划主理想（定理2.5)和各种同构定理(2.9—2.13，它们对应于群的同构定理)。然后用多种方式刻划素理想和极大理想，讨论环范畴中的直积，并证明中国剩余定理。

定义2.1 假设R是环而S是R的非空子集合，并且S对于R中的加法和乘法运算是封闭的，便称S是R的子环。设I是环R的子环。如果

$$r\in R,\ x\in I\Rightarrow rx\in I.$$

则I叫作是环R的左理想。如果

$$r\in R,\ x\in I\Rightarrow xr\in I.$$

则I叫作是环R的右理想。如果I同时是左理想和右理想，便称I是一个理想。

如果有一个关于左理想的命题，不难看出，关于右理想的一个类似的命题也是成立的。

例 设R是环，R的中心是集合$C=\{c\in R\mid cr=rc,$对所有$r\in R\}$。易知C是R的子环，但不一定是理想(习题6)。

例 如果f：$R\to S$是环的同态，则$\mathrm{Ker}\,f$是R中的理想（见下面的定理2.8)。$\mathrm{Im}\,f$是S的子环，但$\mathrm{Im}\,f$不一定是S的理想。

例 对于每个整数n，循环子群$\langle n\rangle=\{kn\mid k\in\mathbf{Z}\}$是$\mathbf{Z}$中的理想。

例 设R是体D上全体n阶方阵所形成的环，I_k是R中只可能在第k列有非零元素的方阵所形成的集合。求证I_k是R的左理想，但不是右理想。如果J_k是R中只可能在第k行有非零元素的方阵所形成的集合，则J_k是右理想但不是左理想。

例 环R自身和只有零元素的集合（表示成0)为理想。这是

每个环 R均具有的两个理想. 零理想0也叫作平凡理想.

注记　设I是R 的一个(左)理想. 如果 $I\neq 0$, $I\neq R$, I叫作真〔左〕理想. 注意如果R有幺元素1_R而I是R的〔左〕理想,则$I=R\Longleftrightarrow 1_R\in I$. 从而 R 的非零〔左〕理想I是真〔左〕理想$\Longleftrightarrow I$不包含R中的单位 (因为若$u\in R$是单位并且$u\in I$, 则$1_R=u^{-1}u\in I$). 特别地, 体D没有真左〔或右〕理想, 因为 D 中每个非零元素都是单位. 关于它的逆命题见习题7.体上n阶方阵环有真左理想和真右理想(见上面所述), 但是没有真 (双侧) 理想 (习题9).

定理2.2　环R的非空子集I是左〔右〕理想$\Longleftrightarrow$

(i)　$a,b\in I\Rightarrow a-b\in I$, 并且

(ii)　$a\in I$, $r\in R\Rightarrow ra\in I[ar\in I]$.

证明作为练习. 见定理$I.2.5$.∎

系2.3　令$\{A_i\mid i\in I\}$是环R中的〔左〕理想族. 则$\bigcap_{i\in I}A_i$ 也 是〔左〕理想.

证明作为练习. ∎

定义2.4　设X是环R的子集合. 令$\{A_i\mid i\in I\}$是R中所有包含X的〔左〕理想. 则 $\bigcap_{i\in I}A_i$叫作由X 生成的〔左〕理想. 这 个 理 想表示成(X).

X中的元素叫作理想(X)的生成元. 如果$X=\{x_1,\cdots,x_n\}$, 则理想X表示成$(x_1,x_2,\cdots,x_n)$, 并且(X) 叫作有限生成的. 由一个元素生成的理想(x)叫作主理想.如果一个环的每个理想都是主理想, 这个环便叫作主理想环. 是主理想环的整环叫 作 主 理 想整

环[2]。

定理2.5 设R是环，$a\in R$，$X\subset R$。

(i) 主理想(a)为

$$\{ra+as+na+\sum_{i=1}^{m}r_ias_i\mid r,s,r_i,s_i\in R,\ m\in \boldsymbol{N}^*,n\in \boldsymbol{Z}\}.$$

(ii) 如果R含有幺元素，则$(a)=\left\{\sum_{i=1}^{n}r_ias_i\mid r_i,\ s_i\in R,\ n\in \boldsymbol{N}^*\right\}$。

(iii) 如果a属于R的中心，则$(a)=\{ra+na\mid r\in R,n\in \boldsymbol{Z}\}$。

(iv) $Ra=\{ra\mid r\in R\}$和$aR=\{ar\mid r\in R\}$分别是R中的左理想和右理想（它们可能不包含a）。如果R有幺元素，则$a\in Ra$，$a\in aR$。

(v) 如果R有幺元素并且a属于R的中心，则$Ra=(a)=aR$。

(vi) 如果R有幺元素而 X 包含在 R 的中心之中，则理想$(X)=\{r_1a_1+\cdots+r_na_n\mid n\in \boldsymbol{N}^*,\ r_i\in R,\ a_i\in X\}$。

注记：在交换环中永远满足(iii)中的假设条件。

证明概要 (i) 证明集合

$$I=\left\{ra+as+na+\sum_{i=1}^{m}r_ias_i\mid r,s,r_i,s_i\in R,\ n\in \boldsymbol{Z},m\in \boldsymbol{N}^*\right\}$$

是理想，$a\in I$，并且，对于包含a的每个理想I'，$I\subset I'$。从而$I=(a)$。

(ii) 由以下事实即得：$ra=ra1_R$，$as=1_Ras$，而$na=n(1_Ra)=(n1_R)a$，其中$n1_R\in R$。∎

---

2. 有些文献中也用“主理想环”一词表示我们这里的主理想整环。

假设$A_1, A_2, \cdots, A_n$是环R的非空子集合，我们以 $A_1 + A_2 + \cdots + A_n$表示集合$\{a_1 + a_2 + \cdots + a_n | a_i \in A_i (1 \leqslant i \leqslant n)\}$。假设$A$和$B$是$R$的非空子集合，我们以$AB$表示集合 $\{a_1 b_1 + \cdots + a_n b_n | n \in \boldsymbol{N}^*, a_i \in A, b_i \in B\}$。如果$A$是由一个元素$a$构成的，则将$AB$记为$aB$。类似地，如果$B = \{b\}$，则将$AB$记为$Ab$。注意若$B$[或者$A$]是对于加法封闭的，则$aB = \{ab | b \in B\}$[或者 $Ab = \{ab | a \in A\}$]。更一般地，以$A_1 A_2 \cdots A_n$表示集合 $\left\{ \sum_{\lambda=1}^{l} a_1^{(\lambda)} a_2^{(\lambda)} \cdots a_n^{(\lambda)} | a_i^{(\lambda)} \in A_i \ (1 \leqslant i \leqslant n)(1 \leqslant \lambda \leqslant l), \ l \in \boldsymbol{N}^* \right\}$特别若所有的$A_i (1 \leqslant i \leqslant n)$ 均是同一个集合A，则以A^n表示$A_1 A_2 \cdots A_n = AA \cdots A$。

定理2.6 假设 $A, A_1, A_2, \cdots, A_n$, B 和C 均是环R的[左]理想。则

(i) $A_1 + A_2 + \cdots + A_n$和$A_1 A_2 \cdots A_n$是〔左〕理想。

(ii) $(A + B) + C = A + (B + C)$。

(iii) $(AB)C = ABC = A(BC)$。

(iv) $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$, $(A_1 + A_2 + \cdots + A_n)C = A_1 C + A_2 C + \cdots + A_n C$。

证明概要 (i) 利用定理2.2。(iii) 利用定义和稍微复杂但是相当直接的推理即可证明。(iv) 先证$A(B + C) = AB + AC$和$(A + B)C = AC + BC$，然后用数学归纳法。∎

理想在环论中所起的作用，与正规子群在群论中所起的作用相近。例如，设R是环而I是R的理想。由于R的加法群是Abel群，从而I是正规子群。从定理I.5.4便知可以定义商群R/I，其中的加法为

$$(a + I) + (b + I) = (a + b) + I。$$

事实上，可以将R/I作成环。

定理2.7 设R是环而I是R的理想。则加法商群R/I对于由

$$(a+I)(b+I)=ab+I$$

所给出的乘法是一个环。如果R是交换环或者具有幺元素，则R/I也是如此。

证明概要 只要我们证明了上述乘法是可以定义的，然后即可按通常步骤证明R是环等事项（例如，若R有幺元素1_R，则1_R+I是R/I的幺元素）。假设$a+I=a'+I$，$b+I=b'+I$，我们必须证明$ab+I=a'b'+I$，由于$a'\in a'+I=a+I$，从而$a'=a+i$(对某个$i\in I$)。类似地$b'=b+j(j\in I)$。从而$a'+b'=(a+i)(b+j)=ab+ib+aj+ij$。由于$I$是理想，

$$a'b'-ab=ib+aj+ij\in I.$$

因此由系I.4.3，可知$a'b'+I=ab+I$，即R/I中上述乘法是可定义的。∎

如果与群的情形加以比较，便会猜想到理想与环的同态有密切的关系。

定理2.8 如果f：$R\to S$是环的同态，则f的核是R的理想。反之，如果I是R的理想，则映射π：$R\to R/I$，$r\longmapsto r+I$是环的满同态并且核是I。

映射π叫作正则满同态（或叫作正则射影）。

证明 $\mathrm{Ker}f$是R的加法子群。如果$x\in\mathrm{Ker}f$并且$r\in R$，则$f(rx)=f(r)f(x)=f(r)0=0$，从而$rx\in\mathrm{Ker}f$，类似地可证$xr\in\mathrm{Ker}f$，因此Kerf是理想。根据定理I.5.5，映射π是群的满同态，并且核为I。由于对所有a，$b\in R$，$\pi(ab)=ab+I=(a+I)(b+I)$

$=\pi(a)\pi(b)$，从而π也是环的满同态。∎

从上述结果自然会想到，只要把正规子群和群分别改成理想与环，那么关于群的各种同构定理(定理 I.5.6—I.5.12) 均可移植到环上来。在每种情况下，对于加法 Abel 群来说，所希望的同构已经知道是存在的。但是所涉及到的群事实上均是环，而正规子群均是理想，因此只需再验证那些群同构也是环同态，从而也就是环同构了。注意：在证明群的各种同构定理时，群和陪集均写成乘法形式，而现在环的加法群与理想的陪集均写成加法形式。

定理2.9 如果f：$R\to S$是环的同态而I是R的理想，并且I包含在f的核之中，则存在唯一的环同态$\bar{f}$：$R/I\to S$，使得$\bar{f}(a+I)=f(a)$(对所有$a\in R$)。此外，$\mathrm{Im}\,\bar{f}=\mathrm{Im}f$，$\mathrm{Ker}\bar{f}=(\mathrm{Ker}f)/I$。最后，$\bar{f}$是同构$\Longleftrightarrow f$是满同态并且$I=\mathrm{Ker}f$。

证明作为练习。见定理I.5.6.∎

系2.10 (第一同构定理) 如果f：$R\to S$是环的同态，则f诱导出环同构$R/\mathrm{Ker}f\cong\mathrm{Im}f$。

证明作为练习。见系I.5.7.∎

系2.11 如果f：$R\to S$是环同态，I是R的理想，J是S的理想，并且$f(I)\subset J$，则f诱导出环同态$\bar{f}$：$R/I\to S/J$，$a+I\longmapsto f(a)+J$。进而，$\bar{f}$是同构$\Longleftrightarrow\mathrm{Im}f+J=S$同时$f^{-1}(J)=I$。特别地，如果$f$是满同态，并且$f(I)=J$，$\mathrm{Ker}f\subset I$，则$\bar{f}$是同构。

证明作为练习。见系I.5.8.∎

定理2.12 假设I和J均是环R的理想。

(i)（第二同构定理）。存在着环同构$I/(I\cap J)\cong(I+J)/J$。

(ii)（第三同构定理）。如果$I\subset J$，则J/I是R/I中的理想，并且有环同构$(R/I)/(J/I)\cong R/J$。

证明作为练习。见系I.5.9和I.5.10.∎

定理2.13 如果I是环R的理想，则R中包含I的全部理想所构成的集合与R/I中全部理想所构成的集合之间存在着由$J\longmapsto J/I$给出的一一对应。从而R/I中每个理想都有形式J/I，其中J是R的理想，并且J包含I。

证明作为练习。见定理I.5.11，系I.5.12和习题13.∎

下面我们将以多种方式刻划两类理想(素理想和极大理想)，它们在今后是经常遇到的。

定义2.14 环R的理想P叫作素理想，是指$P\neq R$，并且对于R中任意两个理想A，B，

$$AB\subset P\Rightarrow A\subset P\text{或者}B\subset P。$$

由于历史原因和技术上的原因，我们在定义素理想时将理想R除掉。下面给出素理想的一种很有益处的刻划方式。在习题14中还要给出另一些刻划方式。

定理2.15 如果P是环R的理想，$P\neq R$，并且对于所有的a，$b\in R$，

$$ab\in P\Rightarrow a\in P\quad\text{或者}b\in P,\tag{1}$$

则P是素理想，反之，如果P是素理想而R是交换环，则P满足条件(1)。

注记：逆命题中的交换性质是必需的(习题9(b))。

证明 如果A和B是理想，使得$AB\subset P$，并且$A\not\subset P$，则存在元素$a\in A-P$。对于每个$b\in B$，$ab\in AB\subset P$，从而$a\in P$或者$b\in P$。但是$a\notin P$，因此必然$b\in P$ (对于每个 $b\in B$)，即$B\subset P$。从而P是素理想。反过来，如果 P是一个理想并且 $ab\in P$，由定义2.4可知主理想(ab)包含在P之中。如果R 是交换环，则由定理2.5导致$(a)(b)\subset(ab)$，从而$(a)(b)\subset P$。如果P是素理想，则或者$(a)\subset P$或者$(b)\subset P$，从而$a\in P$或者$b\in P$。∎

例 任意整环中的零理想均是素理想，因为$ab=0\Longleftrightarrow a=0$或者$b=0$。如果$p$是素数，则$\mathbb{Z}$中的主理想$(p)$是素理想，因为

$ab\in(p)\Rightarrow p\mid ab\Rightarrow p\mid a$或者$p\mid b\Rightarrow a\in(p)$或者$b\in(p)$。

定理2.16 在含幺($1_R\neq 0$)交换环R中，理想 P是素理想$\Longleftrightarrow$商环R/P是整环。

证明 R/P是交换环。根据定理 2.7，幺元素是1_R+P，零元素为$0+P=P$。如果P是素理想，则$1_R+P\neq P$(因为$P\neq R$)。此外，R/P没有零因子，因为

$$(a+P)(b+P)=P \Rightarrow ab+P=P\Rightarrow ab\in P \Rightarrow a\in P$$
$$\text{或者}\quad b\in P \Rightarrow a+P=P \quad\text{或者}\quad b+P=P.$$

因此R/P是整环。反之，如果 R/P是整环，则 $1_R+P\neq 0+P$，从而$1\notin P$，即$P\neq R$。由于R/P没有零因子，从而

$ab\in P\Rightarrow ab+P=P\Rightarrow(a+P)(b+P)=P\Rightarrow a+P=P$ 或者$b+P=P\Rightarrow a\in P$或者$b\in P$。

由定理2.15便知P是素理想。∎

定义2.17 环R中的理想〔左理想〕M叫作极大理想，是指$M\neq R$并且对于每个理想〔左理想〕N，如果$M\subset N\subset R$，则或者$N=M$或者$N=R$。

例 $\boldsymbol{Z}$的理想(3)是极大的，但是(4)不是极大理想，因为(4)$\subsetneq$(2)$\subsetneq\boldsymbol{Z}$。

注记：如果R是环而$\mathscr{S}$是集合$\{I\mid I$为R的理想并且$I\neq R\}$，则$\mathscr{S}$由集合论的包含关系赋以半序。于是：M为极大理想(定义2.17)$\Longleftrightarrow$在引论第7节的意义下M是半序集合$\mathscr{S}$中的极大元。更一般地，有时称理想I对于某个给定的性质是极大的，意思是：在集合$\{I\mid I$为R的理想并且具有上述给定的性质$\}$中，I对于集合论的包含序（这是半序）是极大元。在这种情形下，I在定义2.17意义下不一定是极大的。

定理2.18 在非零含幺环R中永远存在极大〔左〕理想。事实上，R中每个〔左〕理想(除了R本身以外)均包含在某个极大〔左〕理想之中。

证明 由于0是理想而$0\neq R$，可知只需证明第二个命题即可。证明是Zorn引理的直接应用。设A是R中的〔左〕理想，并且$A\neq R$，以$\mathscr{S}$表示集合$\{R$中的〔左〕理想$B\mid A\subset B\neq R\}$。由于$A\in\mathscr{S}$，从而$\mathscr{S}$是非空集合。由集合论包含关系将$\mathscr{S}$赋以半序(即$B_1\leqslant B_2\Longleftrightarrow B_1\subset B_2$)。为了利用Zorn引理，我们必须证明：$\mathscr{S}$中的每个〔左〕理想链$\mathscr{C}=\{C_i\mid i\in I\}$在$\mathscr{S}$中均有上界。令$C=\bigcup_{i\in I}C_i$。我们要证$C$是$R$中的〔左〕理想：如果$a$，$b\in C$，则存在$i$，$j\in I$，使得$a\in C_i$，$b\in C_j$。由于$\mathscr{C}$是链，从而或者$C_i\subset C_j$或者$C_j\subset C_i$。不妨设后者成立。于是$a$，$b\in C_j$。由于$C_j$是左理想，从而$a-b\in C_j$，并

且$ra \in C_i$（对于所有$r \in R$）（如果C_i是理想，则也有$ar \in C_i$）。因此由a，$b \in C$推出$a-b$和ra均属于$C_i \subset C$。从而由定理2.2可知C是〔左〕理想。由于$A \subset C_i$（对于每个i），从而$A \subset \cup C_i = C$。又因为每个C_i均属于$\mathscr{S}$，从而$C_i \neq R$（对于每个$i \in I$）。因此$1_R \notin C_i$（对于每个$i \in I$），因否则便有$C_i = R$。从而$1_R \notin \cup C_i = C$，于是$C \neq R$，即$C \in \mathscr{S}$，显然C是链$\mathscr{C}$的上界。于是满足Zorn引理的假设条件，从而$\mathscr{S}$包含极大元。但是$\mathscr{S}$中极大元显然是R中包含A的极大〔左〕理想。∎

定理2.19 如果R是交换环，并且$R^2 = R$（特别当R有幺元素时满足此条件），则R中每个极大理想M均是素理想。

注记：定理2.19的逆不成立，例如在$\mathbb{Z}$中0是素理想但不是极大理想。还见习题9。

证明 假设$ab \in M$，但是$a \notin M$，$b \notin M$。则理想$M+(a)$和$M+(b)$均真包含M。由极大性可知$M+(a) = R = M+(b)$。由于R是交换环而$ab \in M$，由定理2.5推出$(a)(b) \subset (ab) \subset M$。从而$R = R^2 = (M+(a))(M+(b)) \subset M^2 + (a)M + M(b) + (a)(b) \subset M$。这就与$M \neq R$这一事实相矛盾（因为$M$是极大理想）。因此$a \in M$或者$b \in M$。由定理2.15便知$M$是素理想。∎

象素理想一样，极大理想也可以由它的商环来刻划。

定理2.20 设M是含幺环R的理想，$1_R \neq 0$。

(i) 如果M是极大理想而R是交换环，则商环R/M是域。

(ii) 如果商环R/M是体，则M为极大理想。

注记：如果R不具有幺元素，则(i)不再成立（习题19）。如果M是极大理想而R不是交换环，则R/M不一定是体（习题9）。

证明 (i) 如果M是极大理想，则M为素理想（定理2.19），由定理2.16便知R/M是整环。因此我们只需证明：如果$a+M\neq M$，则$a+M$在R/M中有乘法逆元素。现在由$a+M\neq M$推出$a\notin M$，从而M真包含在理想$M+(a)$之中。但是M为极大理想，从而必然$M+(a)=R$。由于R是变换环，由定理2.5(v)可知$1_R=m+ra$（对于某个$m\in M$和$r\in R$）。于是$1_R-ra=m\in M$，从而

$$1_R+M=ra+M=(r+M)(a+M)。$$

因此$r+M$是$a+M$在R/M中的乘法逆元素，所以R/M是域。

(ii) 如果R/M是体，则$1_R+M\neq 0+M$，从而$1_R\notin M$，即$M\neq R$。如果N是理想，使得$M\subsetneq N$，令$a\in N-M$。则$a+M$在R/M中有乘法逆元素。假设$(a+M)(b+M)=1_R+M$。于是$ab+M=1_R+M$，即$ab-1_R=c\in M$。但是$a\in N$而$M\subset N$，从而$1_R\in N$，因此$N=R$，即M是极大理想。∎

系2.21 设R是含幺($1_R\neq 0$)交换环，则关于R的以下诸条件是彼此等价的。

(i) R是域；

(ii) R没有真理想；

(iii) 0是R中的极大理想；

(iv) 每个非零的环同态$R\to S$都是单同态。

注记：系2.21对于体是不对的(习题9)。

证明 这些结果可以直接证明（习题7），也可以按下面方式来作。根据定理2.20，$R\cong R/0$是域$\Longleftrightarrow$0为R中极大理想。但是后者显然又等价于R没有真理想。最后，对于每个理想$I(\neq R)$，正则映射π：$R\to R/I$是非零环同态，其核为I（定理2.8）。由于π是单同态$\Longleftrightarrow I=0$，从而(iv)$\Longleftrightarrow R$没有真理想。∎

现在我们考虑环范畴中的(直)积。利用群中的相应事实，容易证明它们的存在性和基本性质。但是，环的余积则更为复杂，而且环范畴中的余积也不如Abel 群范畴中的余积（直和）那样有用。

定理2.22 设$\{R_i \mid i\in I\}$是环的非空族，$\prod_{i\in I} R_i$是加法Abel 群R_i的直积。

(i) $\prod_{i\in I} R_i$对于由$\{a_i\}_{i\in I}\{b_i\}_{i\in I}=\{a_ib_i\}_{i\in I}$ 所定义的乘法是环。

(ii) 如果R_i具有幺元素或者是可交换的（对于每个$i\in I$），则$\prod_{i\in I} R_i$也是如此。

(iii) 对于每个$k\in I$，正则射影 π_k：$\prod_{i\in I} R_i \to R_k$，$\{a_i\}\longmapsto a_k$是环的满同态。

(iv)对于每个$k\in I$，正则单射 l_k：$R_k\to\prod_{i\in I} R_i$，$a_k\longmapsto\{a_i\}$(其中$i\neq k$时$a_i=0$)是环的单同态。

证明作为练习．■

$\prod_{i\in I} R_i$叫作是环族$\{R_i \mid i\in I\}$的(外) 直积。如果下标集合 I是有限的，设$I=\{1, 2, \cdots, n\}$，有时我们把$\prod_{i\in I} R_i$记成$R_1\times R_2\times\cdots\times R_n$。

如果$\{R_i \mid i\in I\}$是一族环，对于每个$i\in I$，A_i是R_i的理想。不难看出，$\prod_{i\in I} A_i$是$\prod_{i\in I} R_i$的理想。如果对所有$i\neq k$，$A_i=0$，则理想$\prod_{i\in I} A_i$恰好是$l_k(A_k)$。如果下标集合I是有限的，并且每个R_i都有幺元素，则$\prod_{i\in I} R_i$中每个理想都有形式$\prod_{i\in I} A_i$，其中A_i是R_i的理想(习题1·2)。

定理2.23 设$\{R_i \mid i\in I\}$是环的非空族，S是环，而$\{\varphi_i: S\to R_i \mid i\in I\}$是环的同态族。则存在唯一的环同态$\varphi: S\to\prod_{i\in I} R_i$，使得对所有$i\in I$，$\pi_i\varphi=\varphi_i$。环$\prod_{i\in I} R_i$不计同构由这个性质所唯一决定。换句话说，$\prod_{i\in I} R_i$是环范畴中的积。

证明概要 根据定理I.8.2，存在唯一的群同态$\varphi: S\to\prod_{i\in I} R_i$，使得$\pi_i\varphi=\varphi_i$(对所有$i\in I$)。验证$\varphi$也是环同态。因此$\prod_{i\in I} R_i$是环范畴中的积(定义I.7.2)，再由定理I.7.3可知它不计同构是唯一决定的。∎

定理2.24 设A_1，A_2，…，A_n是环R中的理想，使得：(i) $A_1+A_2+\cdots+A_n=R$，(ii) 对于每个k $(1\leqslant k\leqslant n)$，$A_k\cap(A_1+\cdots+A_{k-1}+A_{k+1}+\cdots+A_n)=0$。则存在环同构$R\cong A_1\times A_2\times\cdots\times A_n$。

证明 从定理I.8.6的证明可知映射$\varphi: A_1\times A_2\times\cdots\times A_n\to R$，$(a_1, \cdots, a_n)\longmapsto a_1+a_2+\cdots+a_n$是加法Abel群同构。我们

只需要验证φ是环同态。注意如果$i\neq j$，$a_i\in A_i$，$a_j\in A_j$，由(ii)可知$a_ia_j\in A_i\cap A_j=0$。从而对于a_i，$b_i\in A_i$：

$$(a_1+a_2+\cdots+a_n)(b_1+b_2+\cdots+b_n)$$
$$=a_1b_1+\cdots+a_nb_n。$$

因此φ是环同态。∎

如果R是环而A_1，…，A_n是R的理想，并且满足定理2.24中的假设条件，则R叫作诸理想A_i的(内) 直积。与群的情形一样，内直积与外直积是有区别的。如果环R是诸理想A_1，…，A_n的内直积，则每个A_i实际上都是R的理想，而R同构于外直积 $A_1\times\cdots\times A_n$。但是外直积$A_1\times\cdots\times A_n$不包含$A_i$，而只是有一个与$A_i$同构的成份(即$l_i(A_i)$，见定理 2.22)。由于这个区别在实际中是不重要的，所以当课文很清楚的时候，我们略去形容词“内”和“外”，从而采用下面的符号。

符号：我们用$R=\Pi A_i$或者 $R=A_1\times A_2\times\cdots\times A_n$表示环$R$是其理想$A_1$，…，$A_n$的内直积。

习题24中给出有限直积的另一种刻划方式。

在本节最后我们给出一个结果，这个结果在第viii章和第ix章中要用到。设A是环 R的理想，a，$b\in R$。元素a叫作模A同余于b(表示成$a\equiv b(\mathrm{mod}A)$)，是指$a-b\in A$。因此

$$a\equiv b(\mathrm{mod}A)\Longleftrightarrow a-b\in A\Longleftrightarrow a+A=b+A。$$

由定理2.7知R/A是环，从而

$$a_1\equiv a_2(\mathrm{mod}A),b_1\equiv b_2(\mathrm{mod}A)\Rightarrow a_1+b_1\equiv a_2+b_2(\mathrm{mod}A),$$
$$a_1b_1\equiv a_2b_2(\mathrm{mod}A)。$$

定理2.25 (中国剩余定理) 设A_1，…，A_n是环R的理想，并且$R^2+A_i=R$(对所有i)和$A_i+A_j=R$(对所有$i\neq j$)。如果b_1，

…，$b_n \in R$，则存在$b \in R$使得

$$b \equiv b_i (\mathrm{mod} A_i)(1 \leqslant i \leqslant n)$$

进而，c也是上面同余方程组的解$\Leftrightarrow b \equiv c\ (\mathrm{mod} A_1 \cap A_2 \cap \cdots \cap A_n)$。

注记：如果R有幺元素，则$R^2 = R$，从而对R的每个理想A，等式$R^2 + A = R$均成立。

证明概要 因为$A_1 + A_2 = R$，$A_1 + A_3 = R$，从而

$$R^2 = (A_1 + A_2)\ (A_1 + A_3) = A_1^2 + A_1 A_3 + A_2 A_1 + A_2 A_3 \subset A_1 + A_2 A_3 \subset A_1 + (A_2 \cap A_3).$$

再由$R = A_1 + R^2$可知

$$R = A_1 + R^2 \subset A_1 + (A_1 + (A_2 \cap A_3)) = A_1 + (A_2 \cap A_3) \subset R.$$

因此$R = A_1 + (A_2 \cap A_3)$。现在归纳假设

$$R = A_1 + (A_2 \cap A_3 \cap \cdots \cap A_{k-1}),$$

则

$$R^2 = (A_1 + (A_2 \cap \cdots \cap A_{k-1}))(A_1 + A_k) \subset A_1 + (A_2 \cap \cdots \cap A_k).$$

因此

$$R = R^2 + A_1 \subset A_1 + (A_2 \cap \cdots \cap A_k) \subset R.$$

从而$R = A_1 + (A_2 \cap \cdots \cap A_k)$。这样我们便归纳证明了$R = A_1 + (A_2 \cap \cdots \cap A_n) = A_1 + (\bigcap_{i \neq 1} A_i)$。类似的推理可知对每个$k = 1, 2, \cdots, n$，均有$R = A_k + (\bigcap_{i \neq k} A_i)$。从而对每个$k$，均存在元素$a_k \in A_k$和$r_k \in \bigcap_{i \neq k} A_i$，使得$b_k = a_k + r_k$。并且

$$r_k \equiv b_k (\mathrm{mod} A_k) \quad r_k \equiv 0 (\mathrm{mod} A_i)(\text{对于} i \neq k).$$

令$b=r_1+r_2+\cdots+r_n$，用定理前面的注记可以验证$b\equiv b_i(\mathrm{mod}A_i)$（对每个$i$）。最后，如果$c\in A$，使得$c\equiv b_i(\mathrm{mod}A_i)$（对于每个$i$），则$b\equiv c(\mathrm{mod}A_i)$（对于每个$i$），因此$b-c\in A_i$（对于每个$i$）。所以$b-c\in\bigcap_{i=1}^{n}A_i$，即$b\equiv c(\mathrm{mod}\bigcap_{i=1}^{n}A_i)$。∎

这个定理其所以命名为中国剩余定理，是因为它推广了初等数论中的下面一个事实，而这个事实是中国数学家于公元前一世纪就已经知道了。

系2.26 设m_1，m_2，…，m_n是正整数，并且$(m_i, m_j)=1$（当$i\neq j$时）。如果b_1，b_2，…，b_n是任意整数，则同余方程组

$$x\equiv b_1(\mathrm{mod}m_1),\ x\equiv b_2(\mathrm{mod}m_2),\ \cdots,\ x\equiv b_n(\mathrm{mod}m_n)$$

有整数解，并且解是模$m=m_1m_2\cdots m_n$唯一决定的。

证明概要 令$A_i=(m_i)$，则$\bigcap_{i=1}^{n}A_i=(m)$。证明由$(m_i,m_j)=1$推出$A_i+A_j=\boldsymbol{Z}$。然后用定理2.25。∎

系2.27 如果A_1，…，A_n是环R中理想，则存在环的单同态

$$\theta:\ R/(A_1\cap\cdots\cap A_n)\to R/A_1\times R/A_2\times\cdots\times R/A_n。$$

如果$R^2+A_i=R$（对所有i），$A_i+A_j=R$（对所有$i\neq j$），则θ是环同构。

证明概要 由定理2.23可知正则满同态$\pi_k:\ R\to R/A_k$（$1\leqslant k\leqslant n$）诱导出环同态$\theta_1:\ R\to R/A_1\times\cdots\times R/A_k$，其中$\theta_1(r)=(r+A_1,\ \cdots,\ r+A_n)$。显然$Ker\theta_1=A_1\cap\cdots\cap A_n$。因此$\theta_1$诱导出环的单同态$\theta:\ R/(A_1\cap\cdots\cap A_n)\to R/A_1\times\cdots\times R/A_n$。（定理2.9）。映射$\theta$不必为满射（习题26）。但是如果定理2.25中的假设条件成

立，并且$(b_1+A_1, \cdots, b_n+A_n)\in R/A_1\times\cdots\times R/A_n$，则存在$b\in R$，使得$b\equiv b_i(\mathrm{mod}A_i)$（对于所有$i$）因此$\theta(b+\bigcap_i A_i)=(b+A_1, \cdots, b+A_n)=(b_1+A_1, \cdots, b_n+A_n)$，从而$\theta$是满同态。∎

习　题

1. 交换环中全体幂零元素形成一个理想〔见习题1.12〕.
2. 假设I是交换环R中的理想，而令$\mathrm{Rad}I=\{r\in R\mid r^n\in I$，对于某个$n\}$，求证Rad I 是理想。
3. 如果R是环，$a\in R$，则$J=\{r\in R\mid ra=0\}$是R的左理想，而$K=\{r\in R\mid ar=0\}$是R的右理想。
4. 如果I是R的左理想，则$A(I)=\{r\in R\mid rx=0$对于每个$x\in I\}$是R的理想。
5. 如果I是环R中理想，令$〔R:I〕=\{r\in R\mid xr\in I$，对于每个$x\in R\}$。求证$〔R:I〕$是$R$的理想并且包含$I$。
6. (a) 设S是域F上二阶方阵全体形成的环，则S的中心是由所有形如$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$的方阵构成的。

   (b) S的中心不是S的理想。

   (c) 什么是体上全体n阶方阵形成的环的中心？
7. (a) 含幺环R是体$\Longleftrightarrow R$没有真左理想。〔命题I.1.3可能是有帮助的.〕

   (b) 如果S是环（可能不具有幺元素），并且S没有真左理想，则或者$S^2=0$，或者S是体。〔提示：证明$\{a\in S\mid Sa=0\}$是理想。如果$cd\neq 0$，证明$\{r\in S\mid rd=0\}=0$。求$e\in S$，使得$ed=d$，然后证明e是（双侧）幺元素.〕
8. 设R是含幺环，S是R上全体n阶方阵形成的环。则J是S的理想$\Longleftrightarrow$存在R的某个理想I，使得J是所有I上全体n阶方阵形成的环。〔提示：给

了J，以I表示集合$\{r\in R|r$是J中某方阵第一行第一列处的元素$\}$。利用初等方阵$E_{r,s}(1\leqslant r,\ s\leqslant n)$，其中$E_{r,s}$在第$r$行第$s$列位置处的元素为1，而其余地方的元素均为0。注意对于方阵$A=(a_{ij})$，方阵$E_{p,r}AE_{s,q}$在第p行第q列处的元素为a_{rs}而其余元素均为0。〕

9. 设S是体D上全体n阶方阵形成的环。$n\geqslant 2$。

(a) S没有真理想（即0是极大理想）。〔提示：利用习题8或者直接论证，并使用习题8中提到的方阵$E_{r,s}$。〕

(b) S有零因子。于是：(i) $S\cong S/0$不是体，并且 (ii) 0是素理想但不满足定理2.15中的条件(1)。

10. (a) 证明$\mathbf{Z}$是主理想环〔见定理I.3.1〕。

(b) 主理想环的同态象也是主理想环。

(c) 对于每个$m>0$，Z_m是主理想环。

11. 如果N是交换环R中全体幂零元素所构成的理想(见习题1)，则环R/N中只有0是幂零元素。

12. 假设环R没有幺元素也没有零因子。令S是定理1.10的证明中所用的环，它的加法群是$R\times\mathbf{Z}$。令$A=\{(r,\ n)\in S|rx+nx=0$(对于每个$x\in R\}$。

(a) A是S的理想。

(b) S/A有幺元素，并且包含一个同构于R的子环。

(c) S/A无零因子。

13. 设f：$R\to S$是环同态，I是R的理想，J是S的理想。则

(a) $f^{-1}(J)$是R的理想并且包含$Kerf$。

(b) 如果f是满同态，则$f(I)$是S的理想，如果f不是满射，则$f(I)$不一定是S的理想。

14. 如果P是环R的理想，而R不必是交换环，则下列诸条件是彼此等价的。

(a) P是素理想。

(b) 如果$r,\ s\in R$，使得$rRs\subset P$，则$r\in P$或者$s\in P$。〔提示：如果(a)成立而$rRs\subset P$，则$(RrR)(RsR)\subset P$，从而$RrR\subset P$或者$RsR\subset P$，假

设$RrR\subset P$. 如果$A=(r)$，则$A^3\subset RrR\subset P$，从而$r\in A\subset P$.〕

(c) 如果(r)和(s)是R的主理想并且$(r)(s)\in P$，则$r\in P$或者$s\in P$.

(d) 如果U和V是R的右理想并且$UV\subset P$，则$U\subset P$或者$V\subset P$.

(e) 如果U和V是R的左理想并且$UV\subset P$，则$U\subset P$或者$V\subset P$.

15. 含幺交换环中的零元素与全体零因子构成的集合至少包含一个素理想.

16. 设R是含幺交换环，并且假设R的理想A包含在$P_1\cup\cdots\cup P_n$中，其中P_1，…，P_n均是素理想. 求证存在某个i使得$A\subset P_i$.〔提示：不然的话，我们可以假定$A\cap P_j\not\subset\bigcup_{i\neq j}P_i$（对于每个$j$）. 令$a_j\in(A\cap P_j)-(\bigcup_{i\neq j}P_i)$. 则$a_1+a_2a_3\cdots a_n$属于$A$但不属于$P_1\cup\cdots\cup P_n$.〕

17. 设f：$R\twoheadrightarrow S$是环的满同态，其核为K.

(a) 如果P是R的素理想并且包含K，则$f(P)$是S的素理想〔见习题3〕.

(b) 如果Q是S的素理想，则$f^{-1}(Q)$是R中的素理想并且包含K.

(c) 在R的全体包含K的素理想和S的全体素理想之间存在着一一对应：$P\mapsto f(P)$.

(d) 如果I是环R的理想，则R/I中每个素理想都有形式P/I，其中P是R中包含I的素理想.

18. 含幺交换环R中的理想$M\neq R$是极大的$\Longleftrightarrow$对于每个$r\in R-M$，均存在$x\in R$，使得$1_R-rx\in M$.

19. 偶整数环E有极大理想M，使得E/M不是域.

20. 在环$\mathbf{Z}$中，关于非零理想I的下列诸条件是彼此等价的：(i) I是素理想；(ii) I是极大理想；(iii) $I=(p)$，其中p是素数.

21. 决定环Z_m中全部素理想和极大理想.

22. (a) 如果R_1，…，R_n是含幺环而I是$R_1\times\cdots\times R_n$中的理想，则$I=A_1\times\cdots\times A_n$，其中每个$A_i$是$R_i$的理想.〔提示：给了$I$，令$A_i=\pi_i(I)$，其中$\pi_i$：$R_1\times\cdots\times R_n\twoheadrightarrow R_i$为正则满同态.〕

(b) 证明：若环R_i不具有幺元素，则(a)中的结论不一定正确.

23. 环R中的元素e叫作幂等元素，是指$e^2=e$。环R之中心中的元素叫作中心元素。如果e是含幺环R中的中心幂等元素，则

(a) 1_R-e是中心幂等元素；

(b) eR和$(1_R-e)R$均是R的理想，并且$R=eR\times(1_R-e)R$。

24. 环R的幂等元素e_1，…，e_n〔见习题23〕叫作正交的，如果$e_ie_j=0$(当$i\neq j$时)。设R，R_1，…，R_n均是含幺环，则下列诸条件是彼此等价的：

(a) $R\cong R_1\times\cdots\times R_n$。

(b) R包含一个正交中心幂等元素集合〔习题23〕$\{e_1,\cdots,e_n\}$，使得$e_1+e_2+\cdots+e_n=1_R$并且$e_iR\cong R_i$(对每个i)。

(c) R是内直积$R=A_1\times\cdots\times A_n$，其中每个$A_i$均为$R$的理想，并且$A_i\cong R_i$。

〔提示：(a)⇒(b)：元素$\overline{e_1}=(1_{R_1},0,\cdots,0)$，$\overline{e_2}=(0,1_{R_1},0,\cdots,0)$，…，$\overline{e_n}=(0,\cdots,0,1_{R_n})$是$S=R_1\times\cdots\times R_n$中的正交中心幂等元素，并且$\overline{e_1}+\cdots+\overline{e_n}=1_S$，$\overline{e_i}S\cong R_i$。(b)⇒(c)：注意$A_i=e_iR$是$R$的主理想$(e_i)$，而$e_iR$本身是具有幺元素$e_i$的环〕

25. 如果$m\in\mathbf{Z}$有素因子分解式$m=p_1^{k_1}\cdots p_t^{k_t}$($k_i>0$，$p_1$，…，$p_t$为不同的素数)，则有环同构$Z_m\cong Z_{p_1^{k_1}}\times\cdots\times Z_{p_t^{k_t}}$。〔提示：系2.27。〕

26. 如果$R=\mathbf{Z}$，$A_1=(6)$，$A_2=(4)$，则系2.27中的映射θ：$R/A_1\cap A_2\to R/A_1\times R/A_2$不是满射。

3. 交换环中的因子分解

我们在本节中要把整数环中的可除性，最大公因子和素数等概念推广到任意交换环上，并且研究某种整环，这种整环具有一种类似于算术基本定理(引论中定理6.7)的性质。主要结果是：每个主理想整环都是这种唯一因子分解整环。此外我们还研究一

种交换环(欧氏环),这种交换环具有类似于欧氏除法算式的性质.

定义3.1 交换环R中非零元素a叫作可以整除元素$b\in R$(表示成:$a\mid b$),是指存在$x\in R$,使得$ax=b$.元素a,$b\in R$叫作相伴的,是指$a\mid b$同时$b\mid a$.

现在我们要表明,关于整除性的所有命题均可用主理想的术语来叙述.

定理3.2 设a,b,u是含幺交换环R中的元素.

(i) $a\mid b\Longleftrightarrow(b)\subset(a)$.

(ii) a和b是相伴的$\Longleftrightarrow(a)=(b)$.

(iii)u是单位$\Longleftrightarrow u\mid r$(对所有$r\in R$).

(iv)u是单位$\Longleftrightarrow(u)=R$.

(v) 关系"a与b相伴"是R上的等价关系.

(vi) 如果$a=br$,其中$r\in R$是单位,则a和b相伴.如果R为整环,则反过来也成立.

证明作为练习.定理2.5(v)对于(i)和(ii)可能是有帮助的.∎

定义3.3 设R是含幺交换环.R中的元素c叫作不可约的,是指

(i) c是非零元素并且不是单位;

(ii) $c=ab\Longrightarrow a$或者b是单位.

R中元素p叫作素元,是指

(i) $p\neq 0$,并且不是单位;

(ii) $p\mid ab\Longrightarrow p\mid a$或者$p\mid b$.

例 如果p是通常的素数,则p和$-p$均是$\mathbb{Z}$中的不可约元与素元(在定义3.3的意义下).在环$\mathbb{Z}_6$中,易知2是素元,但$2\in\mathbb{Z}_6$不

是不可约元，因为$2=2\cdot4$而2和4均不是Z_6中的单位（它们甚至于是零因子）。习题3给出不是素元的不可约元的例子。

环 R 中的素元和不可约元分别与R中的素理想和极大理想有紧密的联系。

定理3.4 设p和c是整环R中的非零元素。

(i) p为素元$\Longleftrightarrow(p)$是非零素理想。

(ii) c为不可约元$\Longleftrightarrow(c)$在R的全体真主理想所组成的集合S中极大。

(iii) R的每个素元均是不可约元。

(iv) 如果R为主理想整环，则p为素元$\Longleftrightarrow p$为不可约元。

(v) R中与不可约元〔素元〕相伴的元素仍旧是不可约元〔素元〕。

(vi) R中不可约元的因子只可能是与它相伴的元素和R中的单位。

注记：从下面的证明中可以看出，定理 3.4 的一部分结果对于任意含幺交换环均成立。

证明 (i) 利用定义3.3和定理2.15。

(ii) 如果c是不可约元，由定理3.2知(c)是R的真理想。如果$(c)\subset(d)$，则$c=dx$。由于 c 不可约，可知或者d是单位（从而$(d)=R$），或者x是单位（由定理3.2这时$(c)=(d)$）。于是(c)在S中极大。反之，如果(c)在S中极大，由定理3.2可知c不是 R中单位并且根据假设$c\neq0$。如果$c=ab$，则$(c)\subset(a)$，从而或者$(c)=(a)$，或者$(a)=R$。在$(a)=R$时，a是单位(定理3.2)。在 $(c)=(a)$时，$a=cy$，从而 $c=ab=cyb$。由于R是整环，$1=yb$，从而b为单位。因此c是不可约的。

(iii) 如果$p=ab$，则$p|a$或者$p|b$。假设$p|a$。则$px=a, p=ab=pxb$，从而$1=xb$，于是b是单位。

(iv) 如果p不可约，从(ii)，定理2.19和(i)即可证明p是素元。

(v) 如果c不可约而d与c相伴，则$c=du$其中$u\in R$是单位(定理3.2)。如果$d=ab$，则$c=abu$，从而a是单位或者bu是单位。但是若bu是单位，则b也是单位。因此d是不可约的。

(vi) 如果c不可约而$a|c$，则$(c)\subset(a)$，由(ii)可知$(c)=(a)$或者$(a)=R$。因此或者a与c相伴，或者由定理3.2推出a是单位。∎

现在我们在任意整环中发展类似于环$\mathbb{Z}$中整除性和素整数的一些概念。让我们回忆一下，根据算术基本定理（引论的定理6.7），$\mathbb{Z}$中每个元素均是有限个不可约元（即素整数和它们加上负号）的乘积。并且这个分解本质上是唯一的（不考虑这些不可约因子的次序）。以$\mathbb{Z}$为样板我们有

定义3.5 整环R叫作是唯一因子分解整环，是指：

(i) R中每个非零非单位a均可以写成$a=c_1c_2\cdots c_n$，其中$c_1, c_2, \cdots, c_n$均是不可约元。

(ii) 如果$a=c_1c_2\cdots c_n$，$a=d_1d_2\cdots d_m$(c_i和d_i均是不可约元)，则$n=m$，并且存在$\{1, 2, \cdots, n\}$的一个置换σ，使得对于每个i，c_i与$d_{\sigma(i)}$相伴。

注记：由(ii)可知，唯一因子分解整环中每个不可约元必是素元。于是由定理3.4(iii)可知不可约元和素元这两个概念是一致的。

定义3.5不是毫无意义的，因为存在着这样的整环：其中每个元素均是不可约元的有限乘积，但是这个分解式不是唯一的（即定义3.5的(ii)不再成立），见习题4。事实上，在历史上其所以产

生“理想”这个概念，原因之一就是在某些代数整数环中具有因子分解不唯一的元素，但是在这些整数环中对于理想发现了某种类型的唯一因子分解定理．见第VIII章．

从不可约元与主理想之间的关系（定理3.4）以及整数环作为样板，可以猜测每个主理想整环均是唯一因式分解整环．为了证明这是对的，我们需要：

引理3.6 如果R是主理想环而$(a_1)\subset(a_2)\subset\cdots$是$R$中的理想链，则存在某个正整数$n$，使得当$j\geqslant n$时$(a_j)=(a_n)$．

证明 令$A=\bigcup_{i\geqslant 1}(a_i)$．我们证明$A$是理想：如果$b$，$c\in A$，则$b\in(a_i)$，$c\in(a_j)$．不妨假设$i\geqslant j$，则$(a_j)\subset(a_i)$而$b$，$c\in(a_i)$．由于$(a_i)$是理想，$b-c\in(a_i)\subset A$．类似地对于$r\in R$和$b\in A$，则$b\in(a_i)$，从而$rb\in(a_i)\subset A$和$br\in(a_i)\subset A$．由定理2.2便知$A$是理想．由假设知$A$是主理想，设$A=(a)$．由于$a\in A=\cup(a_i)$，从而存在某个$n$，使得$a\in(a_n)$．由定义2.4可知$(a)\subset(a_n)$．因此当$j\geqslant n$时，$(a)\subset(a_n)\subset(a_j)\subset A=(a)$．即$(a_j)=(a_n)$．

定理3.7 每个主理想整环R都是唯一因子分解整环．

注记：定理3.7的逆命题不再成立．例如可以证明多项式环$\mathbb{Z}[x]$是唯一因子分解整环（见后面的定理6.14），但不是主理想整环（习题6.1）．

证明概要 假设S是集合$\{0\neq r\in R\mid r$不是单位，并且r不能写成有限个不可约元的乘积$\}$．我们先证明S是空集合，从而R中每个非单位$r\neq 0$均可写成有限个不可约元的乘积．假设S不是空集合，令$a\in S$．由定理3.2(iv)可知(a)是真理想，由定理2.18又知

它包含在一个极大理想(c)之中。由定理3.4(ii)可知$c\in R$是不可约元。因为$(a)\subset(c)$，从而$c|a$。于是对每个$a\in S$，均可以选取a的一个不可约因子c_a(选择公理)。由于R是整环，由c_a唯一决定一个非零元素$x_a\in R$，使得$c_a x_a=a$。我们现在证明$x_a\in S$：如果x_a是单位，由定理3.2(vi)和3.4(v)可知$a=c_a x_a$将会是不可约元。如果x_a不是单位并且不属于S，则x_a可以分解成不可约元的乘积，从而a亦是不可约元的乘积。但是$a\in S$，这就导出矛盾。因此$x_a\in S$。进而我们再证$(a)\subsetneq(x_a)$：由于$x_a|a$，由定理3.2(i)可知$(a)\subset(x_a)$。但是$(a)=(x_a)\Longrightarrow x_a=ay(y\in R)$，从而$a=x_a c_a=ayc_a$，即$1=yc_a$。这就与$c_a$不可约从而不是单位这一事实相矛盾。因此$(a)\subsetneq(x_a)$。

上面所述的事实表明，可以定义一个函数f：$S\to S$，$f(a)=x_a$。根据引论中的递归定理6.2(取$f=f_n$对于所有n)，存在函数φ：$\boldsymbol{N}\to S$，使得

$$\varphi(0)=a,\quad \varphi(n+1)=f(\varphi(n))=x_{\varphi(n)}\quad (n\geqslant 0)$$

记$\varphi(n)=a_n$，我们得到S中元素序列：a，a_1，a_2，…使得

$$a_1=x_a,\quad a_2=x_{a_1},\cdots,\quad a_{n+1}=x_{a_n},\cdots$$

于是由前一段所述，存在理想升链

$$(a)\subsetneq(a_1)\subsetneq(a_2)\subsetneq(a_3)\subsetneq\cdots,$$

这与引理3.6相矛盾。因此集合S是空集，即R中每个非零非单元均可分解成有限个不可约元的乘积。

最后，如果$c_1c_2\cdots c_n=a=d_1d_2\cdots d_m$($c_i$，$d_i$均不可约)，由定理3.4(iv)，$c_1|d_i$(对于某个$i$)。因为$c_1$不是单位，由定理3.4(vi)可知它与某个$d_i$相伴合。然后按部就班采用数学归纳法即可证明分解的唯一性。∎

还有一类整环是我们今后经常遇到的，它们具有一般整环不

一定保持的一种性质.

定义3.8 令$\boldsymbol{N}$是非负整数集合而R是交换环. 我们称R为欧氏环, 是指存在一个函数φ: $R-\{0\}\to\boldsymbol{N}$, 使得:

(i) 如果a, $b\in R$, 并且$ab\neq 0$, 则$\varphi(a)\leqslant\varphi(ab)$.

(ii) 如果a, $b\in R$, 并且$b\neq 0$, 则存在q, $r\in R$, 使得$a=qb+r$, 其中$r=0$或者$r\neq 0$而$\varphi(r)<\varphi(b)$.

是整环的欧氏环叫作欧氏整环.

例 整数环$\boldsymbol{Z}$对于$\varphi(x)=|x|$是欧氏整环.

例 如果F为域, 令$\varphi(x)=1$ (对所有$0\neq x\in F$). 则F是欧氏整环.

例 如果F为域, 则单变量多项式环 $F[x]$是欧氏整环, 其中取$\varphi(f)$为f的次数. 见下面的系6.4.

例 令$\boldsymbol{Z}[i]=\{a+bi\mid a, b\in\boldsymbol{Z}\}$. 它是整环,叫作高斯整环. 定义$\varphi(a+bi)=a^2+b^2$. 显然$a+bi\neq 0\Longrightarrow\varphi(a+bi)\neq 0$. 不难证明定义中的条件(i)是满足的. 请读者证明φ也满足条件 (ii) (习题6).

定理3.9 每个欧氏环 R 均是含幺主理想环. 从而每个欧氏整环均是唯一因子分解整环.

注记: 定理3.9的逆命题不再成立,因为存在主理想整环不是欧氏整环(习题8)

证明 如果I是R中的非零理想, 取$a\in I$, 使得$\varphi(a)$是非负整数集合$\{\varphi(x)\mid x\neq 0, x\in I\}$中的最小整数. 如果$b\in I$, 则 $b=qa+r$, $r=0$或者$r\neq 0$而$\varphi(r)<\varphi(a)$. 由于$b\in I$并且$qa\in I$, 因此$r\in I$. 但是$\varphi(r)<\varphi(a)$ 与 a 的选取相矛盾, 从而必然 $r=0$, 即 $b=qa$

由定理2.5可知 $I \subset Ra \subset (a) \subset I$。因此$I = Ra = (a)$，即$R$是主理想环。

由于R自身是理想，存在$a \in R$使得 $R = Ra$。于是$a = ea = ae$(对于某个$e \in R$)。如果$b \in R = Ra$，则$b = xa$(对于某个$x \in R$)。因此 $be = (xa)e = x(ae) = xa = b$，即$e$是$R$的幺元素。定理的最后论断现在是定理3.7的直接推论。∎

在本节的最后，我们对整除性再作某些进一步的考查，这些考查今后会偶尔用到(第5，6节和第II。6节)。

定义3.10 假设X是交换环R的非空子集。元素 $d \in R$ 叫作X的最大公因子，是指

(i) $d \mid a$(对于每个$a \in X$)；

(ii) $c \mid a$(对于所有$a \in X$) $\Longrightarrow c \mid d$。

最大公因子不是永远存在的。例如在偶整数环E中，2没有因子，从而2和4没有(最大)公因子。即使 $a_1, \cdots, a_n$ 的最大公因子存在，它也不一定是唯一的。但是由(ii)可知，X 的任意两个最大公因子显然是相伴的。此外，不难看出，与X 的某个最大公因子相伴的元素也是X的最大公因子。如果R有幺元素而$a_1, a_2, \cdots, a_n$以1_R作为最大公因子，则称$a_1, a_2, \cdots, a_n$是互素的。

定理3.11 假设$a_1, \cdots, a_n$是含幺交换环R中的元素。

(i) $d \in R$是$\{a_1, \cdots, a_n\}$ 的最大公因子并且 $d = r_1 a_1 + \cdots + r_n a_n$(对于某些$r_i \in R$) $\Longleftrightarrow (d) = (a_1) + (a_2) + \cdots + (a_n)$。

(ii) 如果R是主理想环，则 $a_1, \cdots, a_n$ 的最大公因子是存在的，并且每个最大公因子都可写成形式$r_1 a_1 + \cdots + r_n a_n (r_i \in R)$。

(iii) 如果R是唯一因子分解整环，则$a_1, \cdots, a_n$ 的最大公因

子是存在的。

注记：定理3.11(i)并不意味着a_1，…，a_n的每个最大公因子均可表示成a_1，…，a_n的R-线性组合。一般来说这是不对的(习题6.15)，还见习题12。

证明概要 (i) 利用定义10和定理2.5。

(ii) 由(i)推出。

(iii) 每个a_i有因子分解：$a_i = c_1^{m_{i1}} c_2^{m_{i2}} \cdots c_t^{m_{it}}$，其中$c_1$，…，$c_t$是彼此不同的不可约元，而$m_{ij} \geqslant 0$。证明$d = c_1^{k_1} c_2^{k_2} \cdots c_t^{k_t}$是$a_1$，…，$a_n$的最大公因子，其中$k_j = \min\{m_{1j}, m_{2j}, m_{3j}, \cdots, m_{nj}\}$。∎

习　题

1. 主理想整环中的非零理想是极大理想当且仅当它是素理想。
2. 整环R是唯一因子分解整环$\Longleftrightarrow$$R$中每个非零素理想均包含一个非零主素理想。
3. 令R是实数域的子环$\{a + b\sqrt{10} \mid a, b \in \mathbf{Z}\}$
   (a) 映射N：$R \longrightarrow \mathbf{Z}$，$a + b\sqrt{10} \longmapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$ 满足：$N(uv) = N(u)\ N(v)$ (对所有$u, v \in R$)；$N(u) = 0 \Longleftrightarrow u = 0$
   (b) u是R中单位$\Longleftrightarrow N(u) = \pm 1$
   (c) 2，3，$4 + \sqrt{10}$，$4 - \sqrt{10}$均是R中不可约元。
   (d) 2，3，$4 + \sqrt{10}$，$4 - \sqrt{10}$不是 R 中素元。[提示：$3 \cdot 2 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$.]
4. 证明在习题3所述的整环中，每个元均可以分解成不可约元的乘积，但是分解不一定是唯一的(在定义3.5(ii)的意义下)。
5. 设R是主理想整环。

(a) 每个真理想均是极大理想的乘积$P_1P_2\cdots P_n$，并且不计因子次序这个乘积是唯一的。

(b) R中理想P叫作准素的，是指$ab\in R$，$a\notin P\Rightarrow b^n\in P$（对于某个$n$）。证明$P$准素$\Longleftrightarrow$存在某个$n$，使得$P=(p^n)$，其中$p\in R$是素元（=不可约元）或者$p=0$。

(c) 如果P_1，P_2，…，P_n均是准素理想，并且$P_i=(p_i^{n_i})$其中诸p_i是彼此不相伴的素元，则$P_1P_2\cdots P_n=P_1\cap P_2\cdots\cap P_n$。

(d) R中每个真理想均可（不计次序唯一地）表示成有限个准素理想之交。

6. (a) 如果a和n是整数，$n>0$，则存在整数q和r使得$a=qn+r$，其中$|r|\leqslant n/2$。

(b) 高斯整数环$\mathbf{Z}[i]$对于$\varphi(a+bi)=a^2+b^2$是一个欧氏整环[提示：为了证明定义2.5(ii)成立，先令$y=a+bi$,并假设x是正整数。从(a)部分知有整数q_i，r_i，使得$a=q_1x+r_1$，$b=q_2x+r_2$，其中$|r_1|\leqslant x/2$，$|r_2|\leqslant x/2$。令$q=q_1+q_2i$，$r=r_1+r_2i$，则$y=q\mathrm{x}+r$，其中$r=0$或者$\varphi(r)<\varphi(x)$。对于一般情形，注意对于$\mathrm{x}=c+di\neq 0$和$\overline{x}=c-di$必然$x\overline{x}>0$。从而有q，$r_0\in\mathbf{Z}[i]$，使得$y\overline{x}=q(x\overline{x})+r_0$，其中$r_0=0$或者$\varphi(r_0)<\varphi(x\overline{x})$。令$r=y-qx$，则$y=qx+r$，而$r=0$或者$\varphi(r)<\varphi(x)$.]

7. 什么是高斯整数环$\mathbf{Z}[i]$中的单位？

8. 设R是复数域的子环$\{a+b(1+\sqrt{19}i)/2\mid a,\ b\in\mathbf{Z}\}$。
则R是主理想整环但不是欧氏整环。

9. 设R是唯一因子分解整环而d是R中非零元素。则只有有限个不同的素理想包含理想(d)。[提示：$(d)\subset(k)\Rightarrow k\mid d$.]

10. 如果R是唯一因子分解整环而a，$b\in R$是互素的，并且$a\mid bc$，则$a\mid c$。

11. 设R是欧氏环而$a\in R$。则a是R中单位$\Longleftrightarrow\varphi(a)=\varphi(1_R)$。

12. 含幺交换主理想环中每个非空(可能是无限个元素的）集合均有最大公因子。

13. (欧氏算法)设R是对于函数$\varphi: R-\{0\}\longrightarrow \mathbf{N}$的欧氏整环。如果$a,b\in R$而$b\neq 0$，下面是求$a$和$b$的最大公因子的一种方法：重复使用定义 3.8 (ii)我们有：

$$a=q_0b+r_1,\ r_1=0\text{或者}\varphi(r_1)<\varphi(b);$$

$$b=q_1r_1+r_2,\ r_2=0\text{或者}\varphi(r_2)<\varphi(r_1);$$

$$r_1=q_2r_2+r_3,\ r_3=0\text{或者}\varphi(r_3)<\varphi(r_2);$$

$$\vdots$$

$$r_k=q_{k+1}r_{k+1}+r_{k+2},\ r_{k+2}=0\text{或者}\varphi(r_{k+2})<\varphi(r_{k+1});$$

假设$r_0=b$，并且以n表示使$r_{n+1}=0$的最小整数(由于$\varphi(r_k)$形成非负整数的严格递降序列，从而这样的n是存在的)。证明r_n是a和b的最大公因子。

4. 分式环和局部化

在本节的第一部分我们把由整数环构作有理数域的办法作很大程度的推广，然后用泛映射性质来刻划由任意交换环所构作的分式环（定理4.5)。本节的最后部分是谈分式环的(素)理想结构并介绍在一个素理想处的局部化，这部分内容今后只是偶然用到。

定义4.1 环R的非空子集合S叫作乘法集合，是指 $a,\ b\in S\Rightarrow ab\in S$。

例 在含幺（$1\neq 0$）环中，全体非零因子所形成的集合是乘法集合。特别地，整环中所有非零元素构成一个乘法集合。任意含幺环中全体单位构成一个乘法集合。如果P是交换环 R 中的素理想，则由定理2.15可知P和$S=R-P$ 均是乘法集合。

从整数环$\mathbf{Z}$和有理数域$\mathbf{Q}$中最容易看出我们即将要作的事情

的动机。非零整数构成的集合 S 显然是$\mathbb{Z}$的一个乘法集合。直观上，可以将域$\mathbb{Q}$想象为由全体a/b ($a\in\mathbb{Z}$，$b\in S$) 所组成的，并且满足如下的要求

$$a/b=c/d\Leftrightarrow ad=bc\ (\text{或者}ad-bc=0)。$$

更确切地说，可以按下述办法构作$\mathbb{Q}$（以后再提供证明细节）：在集合$\mathbb{Z}\times S$ 上定义关系：

$$(a,\ b)\sim(c,\ d)\Leftrightarrow ad-bc=0$$

不难看出这是等价关系。$\mathbb{Q}$定义成$\mathbb{Z}\times S$ 对此等价关系的等价类集合。(a,b)的等价类表示成a/b，然后按通常的方式定义加法和乘法。可以证明这些运算的可定义性，并且由此$\mathbb{Q}$是一个域。易知映射$\mathbb{Z}\to\mathbb{Q}$，$a\longmapsto a/1$ 是单同态（嵌入）。

现在我们要将刚才所描绘的构造推广到任意交换环 R（可能没有幺元素）和它的任意乘法集合 S 上去。我们将构作一个含幺交换环$S^{-1}R$和同态φ_s：$R\to S^{-1}R$。如果 S 是整环R中全体非零元素所组成的集合，则$S^{-1}R$是域（如果 $R=\mathbb{Z}$，则$S^{-1}R=\mathbb{Q}$），并且φ_S是R 到 $S^{-1}R$中的嵌入。

定理4.2 设S是交换环R的乘法集合。在集合$R\times S$上定义关系：

$$(r,\ s)\sim(r',\ s')\Leftrightarrow s_1(rs'-r's)=0(\text{对于某个}s_1\in S)。$$

则这是等价关系。进而，如果R没有零因子并且$0\notin S$，则

$$(r,\ s)\sim(r',\ s')\Leftrightarrow(rs'-r's)=0$$

证明作为练习。∎

设S是交换环R的一个乘法集合，而$\sim$是定理4.2 中的等价关系。$(r,\ s)\in R\times S$ 的等价类表示成r/s。$R\times S$ 对于$\sim$的全部等价类构成的集合表示成$S^{-1}R$。验证：

(i) $r/s=r'/s' \Longleftrightarrow s_1(rs'-r's)=0$（对于某个$s_1\in S$）。

(ii)$tr/ts=r/s$（对于每个$r\in R$和s，$t\in S$）。

(iii)如果$0\in S$，则$S^{-1}R$只有一个等价类。

定理4.3 设S是交换环R的乘法集合，令$S^{-1}R$是$R\times S$对于定理4.2的等价关系的等价类集合。

(i) $S^{-1}R$是含幺交换环，其中加法和乘法定义为

$$r/s+r'/s'=(rs'+r's)/ss',\quad (r/s)(r'/s')=rr'/ss'$$

(ii)如果R不为零环并且没有零因子，而$0\notin S$，则$S^{-1}R$是整环。

(iii)如果R不是零环并且没有零因子，而S是R中全体非零元素所构成的集合，则$S^{-1}R$是域。

证明概要 (i) 一旦我们证明了$S^{-1}R$中的加法和乘法均是可以定义的二元运算（即与r，s，r'，s'的选取无关），则其余部分的证明便可按照通常程序进行。特别地，对于每个s，$s'\in S$，$0/s=0/s'$，并且$0/s$是$S^{-1}R$的零元素。r/s的加法逆元素是$(-r)/s$。对于每个s，$s'\in S$，$s/s=s'/s'$，而s/s是$S^{-1}R$中的幺元素。

为证加法是可以定义的，首先注意$(rs'+r's)/ss'$是$S^{-1}R$中的元素，这是因为S是乘法集合。如果$r/s=r_1/s_1$，$r'/s'=r_1'/s_1'$，我们需要证明$(rs'+r's)/ss'=(r_1s_1'+r_1's_1)/s_1s_1'$由假设可知存在$s_2$，$s_3\in S$使得

$$s_2(rs_1-r_1s)=0,\quad s_3(r's_1'-r_1's')=0$$

第一个方程乘以$s_3s's_1'$，第二个方程乘以s_2ss_1然后相加便得到

$$s_2s_3[(rs'+r's)s_1s_1'-(r_1s_1'+r_1's_1)ss']=0$$

因此$(rs'+r's)/ss'=(r_1s_1'+r_1's_1)s_1s_1'$（由于$s_2s_3\in S$）。类似地证明乘法也是与$r$，$s$，$r'$，$s'$的选取无关。

(ii)如果R没有零因子而$0 \notin S$,则$r/s = 0/s \Longleftrightarrow r = 0$(在$R$中)。从而$(r/s)(r'/s') = 0$ (在$S^{-1}R$中)$\Longleftrightarrow rr' = 0$ (在R 中)$\Longleftrightarrow r = 0$或者$r' = 0$。因此$S^{-1}R$ 为整环。

(iii)如果$r \neq 0$, 则$r/s \in S^{-1}R$的乘法逆元素是$s/r \in S^{-1}R$。∎

定理4.3中的环$S^{-1}R$叫作R对于S的分式环。一个重要的特殊情形是R为整环而$S = R - \{0\}$。这时$S^{-1}R$为域 (定理4.3 (iii)),叫作整环R 的商域。因此对于$R = \mathbb{Z}$, 其商域恰好是有理数域$\mathbb{Q}$。更一般地, 假设 R 是任意非零交换环, 而S为不是零因子的全部非零元素组成的集合。如果S非空 (当R 有幺元素时便是这样),则$S^{-1}R$叫作环R的全商环[3]

定理4.3(iii)可以重新叙述为: 如果非零环R 没有零因子,则R 的全商环是域。显然, 整环的全商环恰好是它的商域。

如果φ: $\mathbb{Z} \to \mathbb{Q}$是由$n \longmapsto n/1$给出的映射,则$\varphi$显然是单同态,即将$\mathbb{Z}$映入到$\mathbb{Q}$之中。进而, 对于每个非零整数$n$, $\varphi(n)$ 是$\mathbb{Q}$中的单位。更一般地我们有:

定理4.4 设S是交换环R的乘法集合。

(i) 映射φ_S: $R \to S^{-1}R$, $r \longmapsto rs/s$ (对于任一$s \in S$) 定义出一个环同态, 使得对于每个$s \in S$, $\varphi_S(s)$是 $S^{-1}R$中的单位。

(ii)如果$0 \notin S$, 并且S 不包含零因子, 则 φ_S 是单同态。特别地, 任意整环均可嵌在它的商域中。

(iii)如果R有幺元素, 而S是由单位所构成的, 则φ_S 是同构。特别地, 域F 的全商环 (即是商域) 同构于F。

证明概要 (i) 如果s, $s' \in S$, 则$rs/s = rs'/s'$, 从而φ_S是可

3.对于非交换环有类似的定义, 见定义IX.4.7。

定义的．验证φ_S是环同态，并且对每个 $s\in S$，$s/s^2\in S^{-1}R$是$s^2/s\in\varphi_S(s)$的乘法逆元素．

(ii)如果$\varphi_S(r)=rs/s=0$（在$S^{-1}R$中），则$rs/s=0/s$，从而$rs^2s_1=0$（对于某个$s_1\in S$）．由于$s^2s_1\in S$，从而$s^2s_1\neq 0$．因为S没有零因子，从而必然$r=0$．

(iii)从(ii)知 φ_S 是单同态．如果 $r/s\in S^{-1}R$，其中s是R中单位，则$r/s=\varphi_S(rs^{-1})$，因此φ_S为满同态．∎

根据定理4.4(ii)，习惯上我们将整环R等同于它在φ_S作用下的象，从而将R看作它商域的子环．由于这时 $1_R\in S$，从而 $r\in R$ 可等同于$r/1_R\in S^{-1}R$．

下一个定理表明，分式环可以用泛映射性质来完全地刻划．有时将这个定理作为分式环的定义．

定理4.5 假设S是交换环 R 的乘法集合，令T是任意一个含幺交换环．如果f：$R\to T$是环同态，并且对于所有$s\in S$，$f(s)$ 都是T中的单位．则存在唯一的环同态$\bar{f}$：$S^{-1}R\to T$，使得$\bar{f}\varphi_S=f$．环 $S^{-1}R$ 由这个性质所完全决定(不计同构)．

证明概要 验证映射 $\bar{f}$：$S^{-1}R\to T$，$\bar{f}(r/s)=f(r)f(s)^{-1}$可以定义出一个环同态，使得 $\bar{f}\varphi_S=f$．如果g：$S^{-1}R\to T$是另一个同态使得$g\varphi_S=f$，那么对每个$s\in S$，$g(\varphi_S(s))$是 T 中的单位．从而由习题1.15，对于每个$s\in S$，$g(\varphi_S(s)^{-1})=g(\varphi_S(s))^{-1}$．现在对每个$s\in S$，$\varphi_S(s)=s^2/s$，从而 $\varphi_S(s)^{-1}=s/s^2\in S^{-1}R$．因此对每个$r/s\in S^{-1}R$，

$$\begin{aligned}g(r/s)&=g(\varphi_S(r)\varphi_S(s)^{-1})=g(\varphi_S(r))g(\varphi_S(s)^{-1})\\&=g(\varphi_S(r))g(\varphi_S(s))^{-1}=f(r)f(s)^{-1}\\&=\bar{f}(r/s).\end{aligned}$$

于是$\bar{f}=g$。

为证定理的最后命题，令$\mathscr{C}$是如下的范畴：它的对象集合是$\{(f, T)\mid T$为含幺交换环，$f: R\to T$是环同态，并且对于每个$s\in S$，$f(s)$均是T中单位$\}$。$\mathscr{C}$中从(f_1, T_1)到(f_2, T_2)的态射定义为环同态$g: T_1\to T_2$，使得$gf_1=f_2$。验证$\mathscr{C}$是范畴，并且$\mathscr{C}$中的态射$g: (f_1, T_1)\to(f_2, T_2)$是等价$\Longleftrightarrow g: T_1\to T_2$是环同构。上一段已表明$(\varphi_S, S^{-1}R)$是范畴$\mathscr{C}$中的泛对象，从而根据定理I.7.10可知$S^{-1}R$不计同构是完全决定的。∎

系4.6 将整环R看成它的商域F的子环。如果E是域而$f: R\to E$是环的单同态，则存在唯一的域的单同态$\bar{f}: F\to E$，使得$\bar{f}\mid R=f$。特别地，任意域E_1如果包含R，则必包含同构于F的一个子域F_1，使得$R\subset F_1\subset E_1$。

证明概要 令$S=R-\{0\}$，将定理4.5用于$f: R\to E$。于是存在同态$\bar{f}: S^{-1}R=F\to E$，使得$\bar{f}\varphi_S=f$。验证$\bar{f}$是单同态。由于R等同于$\varphi_S(R)$，这意味着$\bar{f}\mid R=f$。定理的最后命题是$f: R\to E_1$为包含映射这一特殊情形。∎

定理4.7—4.11谈分式环的理想结构。这部分内容只在第VIII 6节中用到。定理4.13今后要被引用，它不依赖于定理4.7—4.11。

定理4.7 设S是交换环R的乘法集合。

(i) 如果I是R中理想，则$S^{-1}I=\{a/s\mid a\in I, s\in S\}$是$S^{-1}R$的理想。

(ii) 如果J是R中另一理想，则

$$S^{-1}(I+J)=S^{-1}I+S^{-1}J,\quad S^{-1}(IJ)=(S^{-1}I)(S^{-1}J),$$

$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$。

注记：$S^{-1}I$叫作I在$S^{-1}R$中的扩充。注意由$r/s \in S^{-1}I$不能推出$r \in I$，因为可能有$a/s = r/s$，其中$a \in I$，$r \notin I$。

证明概要 利用$S^{-1}R$中如下的事实：

$$\sum_{i=1}^{n}(c_i/s) = \Big(\sum_{i=1}^{n} c_i\Big)\Big/ s,$$

$$\sum_{j=1}^{m}(a_j b_j/s) = \sum_{j=1}^{m}(a_j/s)(b_j s/s),$$

$$\sum_{k=1}^{t}(c_k/s_k) = \Big(\sum_{k=1}^{t} c_k s_1 s_2 \cdots s_{k-1} s_{k+1} \cdots s_t\Big)\Big/ s_1 s_2 \cdots s_t.$$ ∎

定理4.8 设S是含幺交换环R的乘法集合。令I是R的理想。则$S^{-1}I = S^{-1}R \Longleftrightarrow S \cap I \neq \varnothing$。

证明 如果$s \in S \cap I$，则$1_{S^{-1}R} = s/s \in S^{-1}I$，从而$S^{-1}I = S^{-1}R$。反之，如果$S^{-1}I = S^{-1}R$，则$\varphi_S^{-1}(S^{-1}I) = R$，从而$\varphi_S(1_R) = a/s$（其中$a \in I$，$s \in S$）。由于$\varphi_S(1_R) = 1_R s/s$，我们有$s^2 s_1 = ass_1$（对于某个$s_1 \in S$），但是$s^2 s_1 \in S$，而$ass_1 \in I$，从而推出$S \cap I \neq \varnothing$。∎

为了刻划分式环的素理想，我们需要一个引理。回忆：如果J是分式环$S^{-1}R$中的理想，则$\varphi_S^{-1}(J)$是R中的理想（习题 2.13）。有时将$\varphi_S^{-1}(J)$叫作J在R中的限制。

引理4.9 设S是含幺交换环R的乘法集合。I是R的理想。则

(i) $I \subset \varphi_S^{-1}(S^{-1}I)$。

(ii) 如果$I = \varphi^{-1}S(J)$，其中J为$S^{-1}R$的理想，则$S^{-1}I = J$。

换句话说，$S^{-1}R$中每个理想均有形式$S^{-1}I$，其中I是R的某个理想。

(iii) 如果P是R的素理想而$S\cap P=\varnothing$，则$S^{-1}P$是$S^{-1}R$的素理想并且$\varphi_S^{-1}(S^{-1}P)=P$。

证明 (i) 如果$a\in I$，则对每个$s\in S$，$as\in I$。从而$\varphi_S(a)=as/s\in S^{-1}I$，于是$a\in\varphi_S^{-1}(S^{-1}I)$。因此$I\subset\varphi_S^{-1}(S^{-1}I)$。

(ii) 因为$I=\varphi_S^{-1}(J)$，$S^{-1}I$中每个元素均有形式r/s，其中$\varphi_S(r)\in J$。因此$r/s=(1_R/s)(rs/s)=(1_R/s)\varphi_S(r)\in J$，即$S^{-1}I\subset J$。反之，如果$r/s\in J$，则$\varphi_S(r)=rs/s=(r/s)(s^2/s)\in J$，从而$r\in\varphi_S^{-1}(J)=I$。因此$r/s\in S^{-1}I$，于是$J\subset S^{-1}I$。

(iii) 根据定理4.8，$S^{-1}P$是理想并且$S^{-1}P\neq S^{-1}R$。如果$(r/s)(r'/s')\in S^{-1}P$，则$rr'/ss'=a/t$，其中$a\in P$，$t\in S$。从而$s_1trr'=s_1ss'a\in P$（对于某个$s_1\in S$）。由于$s_1t\in S$而$S\cap P=\varnothing$，从定理2.15推出$rr'\in P$，从而$r\in P$或者$r'\in P$。因此$r/s\in S^{-1}P$或者$r'/s'\in S^{-1}P$。再由定理2.15可知$S^{-1}P$是素理想。最后，由(i)知$P\subset\varphi_S^{-1}(S^{-1}P)$。反之，如果$r\in\varphi_S^{-1}(S^{-1}P)$，则$\varphi_S(r)\in S^{-1}P$。因此$\varphi_S(r)=rs/s=a/t$，其中$a\in P$而$s$，$t\in S$。从而$s_1str=s_1sa\in P$，(对于某个$s_1\in S$)。因为$s_1st\in S$，而$S\cap P=\varnothing$，由定理2.15知$r\in P$。因此$\varphi_S^{-1}(S^{-1}P)\subset P$。∎

定理4.10 设S是含幺交换环R的乘法集合。则在集合$u=\{R$的素理想$P\mid P\cap S=\varnothing\}$和$v=\{S^{-1}R$的素理想$\}$之间存在着由$P\longmapsto S^{-1}P$给出的一一对应。

证明 由引理4.9 (iii) 可知$P\longmapsto S^{-1}P$定义了一个单射$u\to v$。只需再证明它也是满射。令J是$S^{-1}R$的素理想，又令$P=\varphi_S^{-1}(J)$。由引理4.9(ii)可知$S^{-1}P=J$。从而只需证明P是素理想。〔注〕

〔注〕：还需证明$P\cap S=\varnothing$，这可由定理4.8得出。——译者

如果$ab \in P$，则$\varphi_S(a)\varphi_S(b) = \varphi_S(ab) \in J$，这是因为$P = \varphi_S^{-1}(J)$。由于$J$为$S^{-1}R$的素理想，由定理2.15可知或者$\varphi_S(a) \in J$或者$\varphi_S(b) \in J$。因此或者$a \in \varphi_S^{-1}(J) = P$，或者$b \in P$，再由定理2.15即知$P$为素理想。∎

设R是含幺交换环，P为R的素理想。由定理2.15可知$S = R - P$是R的乘法集合。分式环$S^{-1}R$叫作R在P处的局部化，并且表示成R_P。如果I是R的理想，则R_P的理想$S^{-1}I$表示成I_P。

定理4.11 设P是含幺交换环R的素理想。

(i) 在集合{R的素理想$P' \mid P' \subset P$}与集合{R_P的素理想}之间存在着由$Q \longmapsto Q_P$给出的一一对应。

(ii) P_P是R_P的唯一极大理想。

证明 因为包含在P中的R的理想恰好是与$S = R - P$不相交的那些理想，从而(i)是定理4.10的直接推论。如果M是R_P的极大理想，由定理2.19可知M是素理想，从而$M = Q_P$，其中Q是R的某个素理想并且$Q \subset P$。但是$Q \subset P$导致$Q_P \subset P_P$。由定理4.8知$P_P \neq R_P$，从而必然$Q_P = P_P$。即P_P是R_P中唯一极大理想。∎

象定理4.11中的R_P那样具有唯一极大理想的环有其自身的兴趣。

定义4.12 含幺交换环叫作局部环，是指它有唯一极大理想。

注记：由于含幺环中每个理想均包含在某个极大理想中（定理2.18），从而局部环R的唯一极大理想必然包含R的每个理想（当然除了R自身之外）。

例 如果p是素数而$n \geqslant 1$，则Z_{p^n}是局部环，其唯一极大理想是(p)。

定理4.13 如果R是含幺交换环，则下列诸条件是彼此等价的。

(i) R是局部环。

(ii) R中所有的非单位均包含在某一理想$M(\neq R)$之中。

(iii) R的非单位全体形成理想。

证明概要 如果I是R的理想并且$a\in I$，由定理2.5可知$(a)\subset I$。从而$I\neq R\Longleftrightarrow I$中元素均不是单位。由此事实即给出(ii)⇒(iii)和(iii)⇒(i)。

(i)⇒(ii)：如果$a\in R$不是单位，则$(a)\neq R$。由定义4.12后面的注记可知(a)（从而a）包含在R的唯一极大理想之中。∎

习　题

1. 对于每个$n\geqslant 2$决定环Z_n的全商环。
2. 设S是含幺交换环R的乘法集合。而T是环$S^{-1}R$的乘法集合。令$S_*=\{r\in R\mid r/s\in T$，对于某个$s\in S\}$。则$S_*$是$R$的乘法集合，并且存在环同态$S_*^{-1}R\cong T^{-1}(S^{-1}R)$。
3. (a) 正偶数集合E是$\mathbf{Z}$的乘法集合，并且$E^{-1}\mathbf{Z}$是有理数域。

   (b) 叙述并证明关于$\mathbf{Z}$的乘法集合应满足的条件，以保证$S^{-1}\mathbf{Z}$是有理数域。
4. 如果$S'=\{2,4\}$，$R=Z_6$，则$S^{-1}R$同构于域Z_3，从而定理4.3 (ii)的逆命题是不成立的。
5. 设R是整环，其商域为F。如果T是整环，使得$R\subset T\subset F$，则F是（同构于）T的商域。
6. 设S是整环R的乘法集合，$0\notin S$。如果R为主理想整环或者唯一因子分解整环，则$S^{-1}R$亦然。

7. 设R_1和R_2为整环，其商域分别为F_1和F_2.如果f：$R_1\to R_2$是同构，则f可扩充成同构$F_1\cong F_2$.〔提示：系.4.6.〕

8. 设R是含幺交换环，I是R的理想，π：$R\to R/I$是正则射影.

(a) 如果S是R的乘法集合，则$\pi S=\pi(S)$是R/I的乘法集合.

(b) 映射θ：$S^{-1}R\to(\pi S)^{-1}(R/I)$，$r/s\longmapsto\pi(r)/\pi(s)$ 可定义出一个函数.

(c) θ是环同态，其核为$S^{-1}I$，从而诱导出环同构$S^{-1}R/S^{-1}I\cong(\pi S)^{-1}(R/I)$.

9. 设S是含幺交换环R的乘法集合.如果I是 R的理想，则 $S^{-1}(\mathrm{Rad}\,I)=\mathrm{Rad}(S^{-1}I)$.〔见习题2.2.〕

10. 设R为整环，对于每个极大理想M（当然它也是素理想），将R_M看成是R的商域的子环.证明$\bigcap R_M=R$，其中交运算过R的全部极大理想.

11. 设p是$\mathbf{Z}$中素数，则 (p) 为素理想.在Z_p和局部化$Z_{(p)}$之间有什么关系？

12. 含幺交换环R是局部环$\Longleftrightarrow$若r，$s\in R$，$r+s=1_R$，则r和s至少有一个为单位.

13. 环$R=\{r/s\mid r,\ s\in\mathbf{Z},p\nmid s\}$（其中$p$为固定素数）是局部环.

14. 如果M是含幺交换环R中的极大理想，n为正整数，则环 R/M^n 有唯一素理想，从而是局部环.

15. 在含幺交换环R中，下列诸条件是彼此等价的：

(i) R有唯一素理想；

(ii) 非单位必为幂零元素（见习题1.12）；

(iii) R有一个极小素理想，这个极小素理想包含所有零因子.并且R中非单位均是零因子.

16. 局部环的非零同态象仍为局部环.

5. 多项式环与形式幂级数环

我们开始先给出环R上单变量多项式的定义与记号。其次定义R上 n 变量多项式环并讲述它的基本性质。本节的最后部分简要地介绍一下 R 上单变量形式幂级数环，这部分内容今后不需要。

定理5.1 设R是环。以$R[x]$表示集合 $\{(a_0, a_1, \cdots) | a_i \in R$，只有有限个$a_i \neq 0\}$

(i) $R[x]$对于如下定义的加法和乘法是环

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots)$$

$$(a_0, a_1, \cdots)(b_0, b_1, \cdots) = (c_0, c_1, \cdots,)$$

其中

$$c_n = \sum_{i=0}^{n} a_{n-i} b_i = a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1} + a_0 b_n$$

$$= \sum_{k+j=n} a_k b_j .$$

(ii) 如果R是交换环，或者是含幺环，或者是无零因子环，或者是整环，则$R[x]$也分别如此。

(iii) 映射$R \to R[x]$，$r \longmapsto (r, 0, 0, \cdots)$ 是环的单同态。

证明作为练习。如果 R 有幺元素 1_R，则 $(1_R, 0, 0, \cdots)$ 是$R[x]$中的幺元素。注意若 $(a_0, a_1, \cdots)$，$(b_0, b_1, \cdots) \in R[x]$，而$k$和$j$分别是使$a_k \neq 0$，$b_j \neq 0$的最小下标，则

$(a_0,a_1,\cdots)(b_0,b_1,\cdots)=(0,\cdots,0,a_kb_j,a_{k+1}b_j+a_kb_{j+1},\cdots)$. ∎

定理5.1中的环$R[x]$叫作R上的多项式环. 它的元素叫作多项式. 现在解释一下记号$R[x]$. 按照定理5.1(iii), 我们今后将R等同于它在$R[x]$中的同构象, 并且将$(r,0,0,\cdots)$简记成r. 注意$r(a_0,a_1,\cdots)=(ra_0,ra_1,\cdots)$. 我们现在给出多项式的更为熟悉的记号.

定理5.2 设R是含幺环, 以x表示$R[x]$中的元素$(0,1_R,0,0,\cdots)$. 则

(i) $x^n=(0,0,\cdots,0,1_R,0,\cdots)$, 其中$1_R$是第$(n+1)$个坐标.

(ii) 如果$r\in R$, 则对每个$n\geqslant 0$, $rx^n=x^nr=(0,\cdots,0,r,0,\cdots)$, 其中$r$是第$(n+1)$个坐标.

(iii) 对于$R[x]$中每个非零多项式f, 均存在一个整数$n\in\boldsymbol{N}$和元素$a_0,\cdots,a_n\in R$, 使得$f=a_0x^0+a_1x^1+\cdots+a_nx^n$. 整数$n$和元素$a_i$在下列意义下是唯一的: 如果又有$f=b_0x^0+b_1x^1+\cdots+b_mx^m$$(b_i\in R)$, 则$m\geqslant n$, 并且$a_i=b_i(1\leqslant i\leqslant n)$, 而$b_i=0(n<i\leqslant m)$.

证明概要 利用数学归纳法即可证明(i). 直接计算可得(ii)、(iii) 如果$f=(a_0,a_1,\cdots)\in R[x]$, 则必然存在一个最大下标$n$使得$a_n\neq 0$. 于是$a_0,a_1,\cdots,a_n\in R$即为所需元素. ∎

如果R有幺元素, 则$x^0=1_R$(象在任何一个含幺环中那样), 从而多项式$f=a_0x^0+a_1x^1+\cdots+a_nx^n$可以写成$f=a_0+a_1x+\cdots+a_nx^n$. 为方便起见, 可以将定理5.2中的记号按下述方式推广到不具有幺元素的环中. 如果R是没有幺元素的环, 根据定理1.10, R可以嵌入含幺环S之中, 将R等同于它在嵌入映射之下的象, 则R是S的子环. 从而$R[x]$显然是$S[x]$的子环, 所以每个多项式$f=(a_0,a_1,$

…）$\in R[x]$可以唯一地写成 $f=a_0+a_1x+\cdots+a_nx^n$，其中 $a_i\in R\subset S$，$a_n\neq 0$，而$x=(0,1_S,0,0,\cdots)\in S[x]$。这种情形与$R$ 有么元素时的情形仅有一个重要的区别：在这种情形下元素 x 不属于 $R[x]$。

从今以后，（含么或者不含么）环R上的多项式f 永远写成形式$f=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ $(a_i\in R)$。采用这种符号，$R[x]$中的加法和乘法由类似的法则给出：

$$\sum_{i=0}^{n}a_ix^i+\sum_{i=0}^{n}b_ix^i=\sum_{i=0}^{n}(a_i+b_i)x^i$$

$$\Big(\sum_{i=0}^{n}a_ix^i\Big)\Big(\sum_{j=1}^{m}b_jx^j\Big)=\sum_{k=0}^{m+n}c_kx^k,\ \text{其中}$$

$$c_k=\sum_{i+j=k}a_ib_j。$$

如果$f=\sum_{i=0}^{n}a_ix^i\in R[x]$，则元素$a_i\in R$叫作$f$的系数。元素 a_0叫作常数项。R中的元素均有形式 $r=(r,0,0,\cdots)=rx^0$，它们叫作常数多项式。如果$f=\sum_{i=0}^{n}a_ix^i=a_0+a_1x+\cdots+a_nx^n=a_nx^n+\cdots+a_1x+a_0$，并且$a_n\neq 0$，称$a_n$为$f$的首项系数。如果 R 有么元素而首项系数为1_R，便称f为首 1 多项式。

设R是（含么）环。由于历史上的原因，元素 $x=(0,1_R,0,\cdots)\in R[x]$ 叫作未定元。称多项式为关于未定元 x 的多项式。如果S是另一个（含么）环，则未定元$x\in S[x]$与$R[x]$中的未定元x不是同一个元素。但是在课文中，这个模糊的记号不致于造成混乱。

如果R是任意环，为方便起见，有时要将一个 R 上多项式环

与另一个R上多项式环区别开来。在这种情形下，一个多项式环中的未定元用x，而另一个多项式环中的未定元则用不同的符号y。后一个多项式环表示成$R[y]$，它的元素有形式$a_0+a_1y+\cdots+a_ny^n$。

现在我们定义多个未定元的多项式。为方便起见，这里的讨论只限于未定元个数有限的情形。关于一般的情形见习题4。定义基于如下的事实：一个未定元的多项式可以看成是具有特殊性质的序列，即函数$\boldsymbol{N}\to R$。对于每个正整数n，令$\boldsymbol{N}^n=\boldsymbol{N}\times\cdots\times\boldsymbol{N}$（$n$个因子）。$\boldsymbol{N}^n$中的元素是由$\boldsymbol{N}$中元素构成的有序$n$数组。$\boldsymbol{N}^n$对于逐项相加运算显然是一个加法交换幺半群。

定理5.3 设R是环，以$R[x_1,\cdots,x_n]$表示集合

{函数f：$\boldsymbol{N}^n\to R$|只有有限个元素$u\in\boldsymbol{N}^n$，使得$f(u)\neq 0$}。

(i) $R[x_1,\cdots,x_n]$对于如下定义的加法和乘法是环：

$$(f+g)(u)=f(u)+g(u),\quad (fg)(u)=\sum_{\substack{v+w=u\\ v,w\in\boldsymbol{N}^n}} f(v)\,g(w),$$

其中$f,g\in R[x_1,\cdots,x_n]$，$u\in\boldsymbol{N}^n$。

(ii) 如果R是交换环，或者是含幺环，或者是无零因子环，或者是整环，则$R[x_1,\cdots,x_n]$也分别如此。

(iii) 映射$R\to R[x_1,\cdots,x_n]$，$r\longmapsto f_r$是环的单同态，其中$f_r(0,\cdots,0)=r$，而对所有其余$u\in\boldsymbol{N}^n$，$f_r(u)=0$。

证明作为练习。∎

定理5.3中的环$R[x_1,\cdots,x_n]$叫作R上n个未定元的多项式环。R等同于它在定理5.3(iii)之映射下的同构象，从而可看成是$R[x_1,\cdots,x_n]$的子环。如果$n=1$，则$R[x_1]$恰好是定理5.1中的多项式环。正象$n=1$的情形那样，对于$R[x_1,\cdots,x_n]$中的元素也有

更方便的符号。

令 n 是正整数，对于每个 $i=1,2,\cdots,n$，令

$$\varepsilon_i=(0,\cdots,0,1,0,\cdots,0)\in \boldsymbol{N}^n$$

其中 1 是 ε_i 的第 i 坐标。如果 $k\in \boldsymbol{N}$，令 $k\varepsilon_i=(0,\cdots,0,k,0,\cdots,0)$。则 $\boldsymbol{N}^n$ 中每个元素均可写成形式 $k_1\varepsilon_1+k_2\varepsilon_2+\cdots+k_n\varepsilon_n$。

定理5.4 设 R 是含幺环而 n 是正整数。对于每个 $i=1,2,\cdots,n$，令 x_i 为 $R[x_1,\cdots,x_n]$ 中按下述方式定义的元素：$x_i(\varepsilon_i)=1_R$，而对于 $u\neq\varepsilon_i$，$x_i(u)=0$。则

(i) 对于每个整数 $k\in \boldsymbol{N}$，$x_i^k(k\varepsilon_i)=1_R$ 而对于 $u\neq k\varepsilon_i$，$x_i^k(u)=0$。

(ii) 对于每个 $(k_1,\cdots,k_n)\in \boldsymbol{N}^n$，$x_1^{k_1}x_2^{k_2}x_3^{k_3}(k_1\varepsilon_1+\cdots+k_n\varepsilon_n)=1_R$ 而对于 $u\neq k_1\varepsilon_1+\cdots+k_n\varepsilon_n$，$x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}(u)=0$。

(iii) $x_i^s x_j^t=x_j^t x_i^s$（对于所有 $s,t\in \boldsymbol{N}$ 和 $i,j=1,2,\cdots,n$）

(iv) $x_i^t r=rx_i^t$（对所有 $r\in R$ 和 $t\in \boldsymbol{N}$）

(v) 对于 $R[x_1,\cdots,x_n]$ 中每个非零多项式 f，均存在 $\boldsymbol{N}^n$ 中唯一决定的一组非零元素 $(k_{11},k_{12},\cdots,k_{1n})$，$(k_{21},k_{22},\cdots,k_{2n})$，$\cdots$，$(k_{m1},k_{m2},\cdots,k_{mn})$ 和唯一决定的一组元素 $a_0,a_1,\cdots,a_m\in R$，使得

$$f=a_0x_1^0x_2^0\cdots x_n^0+a_1x_1^{k_{11}}x_2^{k_{12}}\cdots x_n^{k_{1n}}+a_2x_1^{k_{21}}x_2^{k_{22}}\cdots x_n^{k_{2n}}+\cdots+a_mx_1^{k_{m1}}x_2^{k_{m2}}\cdots x_n^{k_{mn}}.$$

证明概要 (v) 令 $(k_{11},\cdots,k_{1n})$，$\cdots$，$(k_{m1},\cdots,k_{mn})$ 是使 f 不为零的那些 $\boldsymbol{N}^n$ 中非零元素。令 $a_0=f(0,\cdots,0)$，而对于 $1\leqslant i\leqslant m$，令 $a_i=f(k_{i1},k_{i2},\cdots,k_{in})$。∎

如果 R 是含幺环，则象定理5.4中那样，元素 $x_1,x_2,\cdots,x_n\in R[x_1,\cdots,x_n]$ 叫做未定元。与一个未定元的情形一样，在方便的

时候，我们也用$x_1,\cdots,x_n$以外的符号来表示未定元。定理5.4(v)中的元素$a_0,a_1,\cdots,a_m$叫作多项式f的系数。形如$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$（$a\in R$）的多项式叫作关于$x_1,\cdots,x_n$的单项式。定理5.4（v）表明，每个多项式均是单项式的和。习惯上我们略去每个单项式中指数为0的那些x_i。例如$a_0x_1^0x_2^0x_3^0+a_1x_1^2x_2^0x_3+a_2x_1x_2^3x_3$写成$a_0+a_1x_1^2x_3+a_2x_1x_2^3x_3$。定理5.4中的符号和术语均可以推广到多项式环$R[x_1,\cdots,x_n]$上来，其中$R$可能没有幺元素（象一个未定元的情形那样）。环$R$嵌入含幺环$S$中，而$R[x_1,\cdots,x_n]$看作$S[x_1,\cdots,x_n]$的子环。如果$R$没有幺元素，则未定元$x_1,x_2,\cdots,x_n$和单项式$x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$（$k_i\in\boldsymbol{N}$）都不是$R[x_1,\cdots,x_n]$中的元素。

如果R是任意环，则不难看出，映射$R[x_1]\to R[x_1,\cdots,x_n]$，

$$\sum_{i=0}^{m}a_ix_1^i\longmapsto\sum_{i=0}^{m}a_ix_1^ix_2^0\cdots x_n^0=\sum_{i=0}^{m}a_ix_1^i\in R[x_1,\cdots,x_n]$$

是环的单同态。类似地，对于$\{1,2,\cdots,n\}$的任意子集合$\{i_1\cdots,i_k\}$，存在着单同态$R[x_{i_1},\cdots,x_{i_k}]\to R[x_1,\cdots,x_n]$。通常将$R[x_{i_1},\cdots x_{i_k}]$等同于它的同构象，从而看成是$R[x_1,\cdots,x_n]$的子环。

设$\varphi:R\to S$是环的同态，$f\in R[x_1,\cdots,x_n]$，而$s_1,s_2,\cdots,s_n\in S$。根据定理5.4，$f=\sum_{i=0}^{m}a_ix_1^{k_{i1}}\cdots x_n^{k_{in}}$，其中$a_i\in R$而$k_{ij}\in\boldsymbol{N}$。去掉指数为0的全部$x_i$，然后$\varphi f(s_1,s_2,\cdots,s_n)$定义为$\sum_{i=0}^{m}\varphi(a_i)s_1^{k_{i1}}\cdots s_n^{k_{in}}\in S$。即$\varphi f(s_1,\cdots,s_n)$是用$\varphi(a_i)$代替$a_i$而用$s_i^{k_{ij}}$代替$x_i^{k_{ij}}$（$k_{ij}>0$）之后而得到的。由于$a_i$和$k_{ij}$均是唯一决定的（定理5.4），从而$\varphi f(S_1,\cdots,S_n)$可以定义成$S$中的元素。如果$R$是$S$的子环而$\varphi$是包含映射，我们仍用$f(s_1,\cdots,s_n)$表示$\varphi f(s_1,\cdots,s_n)$。

与许多代数结构一样，多项式环$R[x_1,\cdots,x_n]$也可以用泛映射性质来刻划。在加上一些适当的假设之后，下一定理和它的系对于非交换环的情形也是对的（习题5）。它们对于无限多未定元的多项式环也是对的（习题4）。

定理5.5 设R和S是含幺交换环，$\varphi:R\to S$为环的同态，使得$\varphi(1_R)=1_S$、如果$s_1,s_2,\cdots,s_n\in S$，则存在唯一的环同态$\bar{\varphi}:R[x_1,\cdots,x_n]\to S$，使得$\bar{\varphi}|R=\varphi$并且$\bar{\varphi}(x_i)=s_i$ $(1\leqslant i\leqslant n)$。这个性质不计同构完全决定了多项式环$R[x_1,\cdots,x_n]$。

证明概要 如果$f\in R[x_1,\cdots,x_n]$，则由定理5.4有

$$f=\sum_{i=0}^{m}a_i x_1^{k_{i1}}\cdots x_n^{k_{in}}\quad(a_i\in R,k_{ij}\in \boldsymbol{N})$$

由$\bar{\varphi}(f)=\varphi f(s_1,\cdots,s_n)$给出的映射$\bar{\varphi}$显然是可以定义的，并且$\bar{\varphi}|R=\varphi$，$\bar{\varphi}(x_i)=s_i$。利用$\varphi$为同态、指数运算法则以及二项式定理1.6可以验证$\bar{\varphi}$是环同态。反过来，假设$\psi:R[x_1,\cdots,x_n]\to S$是同态，使得$\psi|R=\varphi$和$\psi(x_i)=s_i$（对于每个$i$），则

$$\begin{aligned}\psi(f)&=\psi\Big(\sum_{i=0}^{m}a_i x_1^{k_{i1}}\cdots x_n^{k_{in}}\Big)\\&=\sum_{i=0}^{m}\psi(a_i)\psi(x_1^{k_{i1}})\cdots\psi(x_n^{k_{in}})\\&=\sum_{i=0}^{m}\varphi(a_i)\psi(x_1)^{k_{i1}}\cdots\psi(x_n)^{k_{in}}\\&=\sum_{i=0}^{m}\varphi(a_i)s_1^{k_{i1}}\cdots s_n^{k_{in}}\\&=\varphi f(s_1,s_2,\cdots,s_n)=\bar{\varphi}(f).\end{aligned}$$

从而$\psi=\bar{\varphi}$，即$\bar{\varphi}$是唯一的。最后，为了证明$R[x_1,\cdots,x_n]$由这个映射性质所完全决定，如下定义一个范畴$\mathscr{C}$：对象是$\{(\psi,K,s_1,$

$\cdots, s_n)\mid K$为含幺交换环，$s_i \in K$，$\psi: R \to K$是环同态，并且 $\psi(1_R) = 1_K\}$、$\mathscr{C}$中从 $(\psi, K, s_1, \cdots, s_n)$ 到 $(\theta, T, t_1, \cdots, t_n)$ 的态射是环同态$\zeta: K \to T$，使得$\zeta(1_K) = 1_T, \zeta\psi = \theta$，并且$\zeta(s_i) = t_i (1 \leqslant i \leqslant n)$。验证：$\zeta$是$\mathscr{C}$中的等价$\Longleftrightarrow\zeta$为环同构。如果$l: R \to R[x_1, \cdots, x_n]$是包含映射，则由本证明的第一部分可知 $(l, R[x_1, \cdots, x_n], x_1, \cdots x_n)$ 是 $\mathscr{C}$中的泛对象。从而由定理 I.7.10 可知不计同构$R[x_1, \cdots, x_n]$是完全决定的。∎

系5.6 如果$\varphi: R \to S$是交换环的同态而$s_1, \cdots, s_n \in S$，则映射$R[x_1, \cdots, x_n] \to S$，$f \longmapsto \varphi f(s_1, \cdots, s_n)$ 是环同态。

证明概要 由定理5.5的证明可知，即使 R 和 S 没有幺元素时，$f \longrightarrow \varphi f(S_1, \cdots, S_n)$ 也定义出一个环同态。∎

注记：系5.6中的映射$R[x_1, \cdots, x_n] \longrightarrow S$ 叫作取值同态或代换同态。如果R和S不是交换环，则系5.6可能不对。这一点很重要，因为我们经常无意识地使用系 5.6。例如我们经常遇到如下的推理：如果$f = gh (f, g, h \in R[x])$，$c \in R$，则 $f(c) = g(c)h(c)$但是在R不是交换环的时候，这是不对的（习题 6）。

定理5.5的另一个推论可用下面例子加以说明。设 R 是含幺交换环。考虑多项式

$$f = x^2y + x^3y + x^4 + xy + y^2 + r \in R[x, y].$$

注意 $f = y^2 + (x^2 + x^3 + x)y + (x^4 + r)$，从而 $f \in R[x][y]$。类似地，$f = x^4 + yx^3 + yx^2 + yx + (y^2 + r) \in R[y][x]$。这建议我们：$R[x, y]$同时同构于$R[x][y]$和 $R[y][x]$。更一般地，我们有：

系5.7 设R是含幺交换环，n是正整数。对于每个$k (1 \leqslant k \leqslant n)$，均存在环同构 $R[x_1, \cdots, x_k][x_{k+1} \cdots, x_n] \cong R[x_1, \cdots, x_n] \cong R$

$[x_{k+1},\cdots,x_n][x_1,\cdots,x_k]$。

证明 可以采用直接构作同构的办法证明此系，也可以按下述方式用定理5.5的泛映射性质来证明，给了含幺交换环之间的同态$\varphi: R\to S$。又给了元素$s_1,\cdots,s_n\in S$，由定理5.5可知存在着同态$\bar{\varphi}: R[x_1,\cdots,x_k]\to S$，使得$\bar{\varphi}|R=\varphi$，$\bar{\varphi}(x_i)=s_i$ $(1\leqslant i\leqslant k)$。在定理5.5中，以$R[x_1,\cdots,x_k]$代替$R$则给出同态$\bar{\bar{\varphi}}: R[x_1,\cdots,x_k][x_{k+1},\cdots,x_n]\to S$，使得$\bar{\bar{\varphi}}|R[x_1,\cdots,x_k]=\bar{\varphi}$并且$\bar{\bar{\varphi}}(x_i)=s_i$ $(k+1\leqslant i\leqslant n)$。由构作方式可知$\bar{\bar{\varphi}}|R=\bar{\varphi}|R=\varphi$并且$\bar{\bar{\varphi}}(x_i)=s_i(1\leqslant i\leqslant n)$。假设$\psi: R[x_1,\cdots,x_k][x_{k+1},\cdots,x_n]\to S$是同态，并且使得$\psi|R=\varphi$和$\psi(x_i)=s_i(1\leqslant i\leqslant n)$。则使用定理5.5中证明唯一性时的推理方法便可证明$\psi|R[x_1,\cdots,x_k]=\bar{\varphi}$。从而由定理5.5的唯一性命题（用于$R[x_1,\cdots,x_k]$）导致$\psi=\bar{\bar{\varphi}}$。因此$R[x_1,\cdots,x_k][x_{k+1},\cdots,x_n]$即有所需的泛映射性质，由定理5.5即知$R[x_1,\cdots,x_k][x_{k+1},\cdots,x_n]\cong R[x_1,\cdots,x_n]$。类似地证明另一个同构。∎

因此，通常将$R[x_1,\cdots,x_k]$看成是$R[x_1,\cdots,x_n]$的子环（见第228页），习惯上将系5.6中彼此同构的几个多项式环等同起来。例如可写成$R[x_1,\cdots,x_k][x_{k+1},\cdots,x_n]=R[x_1,\cdots,x_n]$。

在本章的最后我们简要地介绍一下形式幂级数环，这部分内容今后不需要。

命题5.8 设R是环，以$R[[x]]$表示全体R中元素序列$(a_0,a_1,\cdots)$所组成的集合。则

(i) $R[[x]]$对于如下定义的加法和乘法形成环：

$$(a_0,a_1,\cdots)+(b_0,b_1,\cdots)=(a_0+b_0,a_1+b_1\cdots)$$

$(a_0,a_1,\cdots)(b_0,b_1,\cdots)=(c_0,c_1,\cdots)$，其中

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} = \sum_{k+j=n} a_k b_j .$$

(ii) 多项式环$R[x]$是$R[[x]]$的子环.

(iii) 如果R是交换环，或者是含幺环，或者是无零因子环，或者是整环，则$R[[x]]$也分别如此.

证明作为练习，见定理5.1 ∎

命题5.8中的环$R[[x]]$叫作环R上的形式幂级数环. 它的元素叫作幂级数. 如果R有幺元素，则多项式$x=(0,1_R,0,\cdots)\in R[[x]]$叫作未定元. 不难验证$x^i r = r x^i$（对所有$r\in R$和$i\in \mathbf{N}$）. 如果$(a_0,a_1,\cdots)\in R[[x]]$，则对于每个$n$，$(a_0,a_1,\cdots,a_n,0,0,\cdots)$是多项式，从而由定理5.2可知$(a_0,\cdots,a_n,0,0,\cdots)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$. 因此我们修改成如下的记号：幂级数$(a_0,a_1,\cdots)\in R[[x]]$表示成形式和$\sum_{i=0}^{\infty} a_i x^i$. 元素$a_i$叫作系数而$a_0$叫作常数项. 与多项式情形一样，即使$R$不具有幺元素时，我们也可以使用上述记号（这时$x\notin R[[x]]$）.

命题5.9 设R是含幺环，$f=\sum_{i=0}^{\infty} a_i x^i \in R[[x]]$. 则

(i) f为$R[[x]]$中单位$\Longleftrightarrow$它的常数项a_0是R中单位.

(ii) 如果a_0在R中不可约，则f在$R[[x]]$中也不可约.

注记：如果$f\in R[[x]]$实际上是多项式，并且常数项为不可约元或者单位，则f在多项式环$R[x]$中不一定为不可约元或者单位（习题8）.

证明 (i) 如果存在$g=\sum b_i x^i \in R[[x]]$，

使得 $fg=gf=1_R\in R[[x]]$,

立刻推出$a_0b_0=b_0a_0=1_R$,从而a_0为R中单位。现在假定a_0为R中的单位。如果存在元素$g=\sum b_ix^i\in R[[x]]$,使得$fg=1_R$,则有如下的方程:

$$\begin{aligned}
&a_0b_0=1_R,\\
&a_0b_1+a_1b_0=0,\\
&\qquad\vdots\\
&a_0b_n+a_1b_{n-1}+\cdots+a_nb_0=0,\\
&\qquad\vdots
\end{aligned}$$

反之,如果在 R 中存在这个方程组的解 $(b_0,b_1,b_2,\cdots)$,则$g=\sum_{i=0}^{\infty}b_ix^i\in R[[x]]$显然有性质 $fg=1_R$。由于 a_0为单位(乘法逆元素是a_0^{-1}),则第一方程可解:$b_0=a_0^{-1}$.类似地,$b_1=a_0^{-1}(-a_0b_0)=a_0^{-1}(-a_1a_0^{-1})$。然后归纳:如果$b_0,\cdots,b_{n-1}$ 由诸 a_i 决定,则$a_0b_n=-a_1b_{n-1}-\cdots-a_nb_0$导致 $b_n=a_0^{-1}(-a_1b_{n-1}-\cdots-a_1b_0)$。因此若 a_0 为单位,则方程组可解,从而存在 g 使得 $fg=1_R\in R[[x]]$。类似的推理表明也存在$h\in R[[x]]$,使得$hf=1_R$。但是$h=h1_R=h(fg)=(hf)g=1_Rg=g$,从而$g$是$f$的双侧逆元素,于是$f$为$R[[x]]$中的单位。

(ii) 是(i) 的直接推论。 ∎

系5.10 如果R是体,则$R[[x]]$中元素为单位的充要条件是该元素有非零常数项。主理想(x) 恰好由 $R[[x]]$ 中全部非单位所构成,并且它是$R[[x]]$ 中唯一极大理想。从而当 R 是域的时候,$R[[x]]$是局部环。

证明 第一个论断是根据命题5.9(i) 和事实:R中非零元素

均为单位。因为 x 属于$R[[x]]$的中心，由定理2.5 可知

$$(x)=\{xf \mid f\in R[[x]]\}.$$

从而（x）中每个元素 xf 的常数项均为0，即xf不是单位。反过来，每个非单位$f\in R[[x]]$必然有形式$f=\sum_{i=0}^{\infty}a_ix^i$，其中 $a_0=0$。令$g=\sum_{i=0}^{\infty}b_ix^i$，其中 $b_i=a_{i+1}$（对于每个 i）。于是 $xg=f$，即$f\in(x)$。从而（x）恰好为非单位集合，最后，因为$1_R\notin(x)$，从而$(x)\neq R[[x]]$。进而，$R[[x]]$的每个理想$I(\neq R[[x]])$必然由非单位组成的（第184页的注记）。于是$R[[x]]$的每个真理想均包含于（x）之中。从而（x）是$R[[x]]$的唯一极大理想。∎

习　题

1. (a) 如果$\varphi: R\to S$是环同态，则映射$\bar{\varphi}: R[[x]]\to S[[x]]$，$\bar{\varphi}(\Sigma a_ix^i)=\Sigma\varphi(a_i)x^i$是环同态，并且$\bar{\varphi}(R[x])\subset S[x]$。

   (b) $\bar{\varphi}$为单同态[或者满同态]$\Longleftrightarrow\varphi$为单同态[或者满同态]。这时 $\bar{\varphi}: R[x]\to S[x]$也是单同态[或者满同态]。

   (c) 将 (a) 和 (c) 中结果推广到多项式环$R[x_1,\cdots,x_n]$和$S[x_1,\cdots,x_n]$的情形。

2. 以$\mathrm{Mat}_n R$表示环R上全体n阶方阵构成的环。则对于每个$n\geqslant 1$，

   (a) $(\mathrm{Mat}_n R)[x]\cong\mathrm{Mat}_n R[x]$。

   (b) $(\mathrm{Mat}_n R)[[x]]\cong\mathrm{Mat}_n R[[x]]$。

3. 设R是环而G是以x为生成元的无限乘法循环群。群环$R(G)$(见175页)是否同构于R上一个未定元的多项式环？

4. (a) 令S为非空集，又令$\mathbf{N}^S$为集合｛函数$\varphi: S\to N$|至多存在有限个元素$s\in S$，使得$\varphi(s)\neq 0$｝。则$\mathbf{N}^S$对于下述乘积是乘法交换幺半群。

$(\varphi\psi)(s)=\varphi(s)+\psi(s)$ $(\varphi,\psi\in\mathbf{N}^S,\ s\in S)$，$\mathbf{N}^S$ 中的幺元素是零函数。

(b) 对于每个$x\in S$和$i\in\mathbf{N}$，令 $x^i\in\mathbf{N}^S$ 定义为 $x^i(x)=i$，而对$s\neq x$，$x^i(s)=0$。如果$\varphi\in\mathbf{N}^S$并且只有S中元素$x_1,\cdots,x_n$使$\varphi(x_i)\neq 0$。则在$\mathbf{N}^S$中$\varphi=x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$，其中$i_j=\varphi(x_j)$。

(c) 如果R是含幺环，以$R[S]$表示集合 {函数$f:\mathbf{N}^S\to R$ | 至多存在有限个$\varphi\in\mathbf{N}^S$，使得$f(\varphi)\neq 0$}。则$R[S]$是含幺环，其中加法和乘法分别定义成：

$$(f+g)(\varphi)=f(\varphi)+g(\varphi)\quad(f,g\in R[S],\ \varphi\in\mathbf{N}^S),$$

$$(fg)(\varphi)=\sum f(\theta)g(\xi)\quad(f,g\in R[S],\ \theta,\xi,\ \varphi\in\mathbf{N}^S),$$

其中求和过 $\{(\theta,\xi)\mid\theta\xi=\varphi\}$。$R[S]$叫作$R$上关于$S$的多项式环。

(d) 对于每个$\varphi=x^{i_1}\cdots x^{i_n}\in\mathbf{N}^S$和每个$r\in R$，我们用$rx^{i_1}\cdots x^{i_n}\in\mathbf{N}^S$表示函数$\mathbf{N}^S\to R$，它在$\varphi$处取值为$r$而在其他处取值为0，则$R[S]$中每个非零元素$f$均可写成形式$f=\sum_{i=0}^{m}x_1^{k_{1i}}x_2^{k_{2i}}\cdots x_n^{k_{ni}}$，其中$r_i\in R$，$x_i\in S$，$k_{ij}\in\mathbf{N}$，所有这些元素均是唯一决定的。

(e) 如果$|S|=n$（有限），则$R[S]\cong R[x_1,\cdots,x_n]$。[提示：如果$\mathbf{N}^n$象在课文中那样看成是加法交换幺半群，则存在幺半群同构$\mathbf{N}^S\cong\mathbf{N}^n$，$\varphi\to(\varphi(s_1),\cdots\varphi(s_n))$，其中$S=\{s_1,\cdots,s_n\}$。]

(f) 叙述并证明定理5.5对于$R[S]$的模拟。

5. 设R和S是含幺环，$\varphi:R\to S$是环同态，并且$\varphi(1_R)=1_S$，又存在S_1，$s_2,\cdots,s_n\in S$，使得$s_is_j=s_js_i$（对于所有i,j）和$\varphi(r)s_i=s_i\varphi(r)$（对于所有$r\in R$和所有$i$），则存在唯一的同态$\bar{\varphi}:R[x_1,\cdots,x_n]\to S$，使得$\bar{\varphi}|R=\varphi$并且$\bar{\varphi}(x_i)=s_i$。这个性质不计同构完全决定了$R[x_1,\cdots,x_n]$。

6. (a) 如果R是$\mathbf{Z}$上所有2阶方阵组成的环，则对于每个$A\in R$，

$$(x+A)(x-A)=x^2-A^2\in R[x].$$

(b) 存在c，$A\in R$，使得$(c+A)(c-A)\neq c^2-A^2$。

因此当环不是交换环时，系5.6可能不成立.

7. 如果R是含幺交换环而$f=a_nx^n+\cdots+a_0$是$R[x]$中的零因子，则存在非零元素$b\in R$，使得$ba_n=ba_{n-1}=\cdots=ba_0=0$.

8. (a) 多项式$x+1$是形式幂级数环$\mathbf{Z}[[x]]$中的单位，但不是$\mathbf{Z}[x]$中的单位.

(b) x^2+3x+2在$\mathbf{Z}[[x]]$中不可约，但在$\mathbf{Z}[x]$中不是不可约的.

9. 如果F是域，则(x)是$F[x]$中的极大理想，但它不是唯一的极大理想(比较系5.10).

10. (a) 如果F为域，则$F[[x]]$中每个非零元素均有形式x^iu，其中$u\in F[[x]]$是单位.

(b) $F[[x]]$为主理想整环，它只有如下一些理想：0，$F[[x]]=(1_F)=(x^0)$，和(x^k)(对于每个$k\geqslant 1$)

11. 令$\mathscr{C}$为全体含幺交换环和全体满足$f(1_R)=1_S$的环同态$f:R\to S$所组成的范畴，则多项式环$\mathbf{Z}[x_1,\cdots,x_n]$是范畴$\mathscr{C}$中在集合$\{x_1,\cdots,x_n\}$上的自由对象.[提示：对于$\mathscr{C}$中每个$R$，映射$\mathbf{Z}\to R$，$n\longmapsto n1_R$是环同态.再使用定理5.5.]

6. 多项式环中的因子分解

我们现在对于交换环上的多项式环考虑第3节介绍的那些论题(整除性，不可约性和唯一因子分解).首先介绍两个基本工具：多项式的次数和除法算式.然后研究多项式的一次因式，求这样的因式相当于求多项式的根.最后我们考虑高次不可约因式：证明Eisenstein不可约判别法.同时还证明：如果D是唯一因子

分解整环，则多项式整环$D[x_1,\cdots,x_n]$也是如此。

设R为环。非零单项式$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\in R[x_1,\cdots,x_n]$的次数是指非负整数$k_1+k_2+\cdots+k_n$。如果$f$是$R[x_1,\cdots,x_n]$中的非零多项式，则$f=\sum_{i=0}^{m}a_i{x_1}^{k_{i1}}\cdots x_n^{k_{in}}$(定理5.4)。多项式$f$的（全）次数是诸单项式$a_ix_1^{k_{i1}}\cdots x_n^{k_{in}}$ $(a_i\neq 0)$ 的次数的最大值。f的(全)次数表示成$\deg f$。显然，非零多项式的次数为$0\Longleftrightarrow f$为常数多项式：$f=a_0=a_0x_1^0\cdots x_n^0$。一个多项式如果是一些同次数$(=k)$的单项式之和，便称该多项式为$k$次齐次多项式。注意对于每个$k(1\leqslant k\leqslant n)$，$R[x_1,\cdots,x_{k-1},x_{k+1},\cdots,x_n]$是$R[x_1,\cdots,x_n]$的子环（见第228页）。将$f$看作环$R[x_1,\cdots,x_{k-1},x_{k+1},\cdots,x_n]$上一个未定元$x_k$的多项式时，它的次数叫作$f$对于$x_k$的次数。

例 多项式$3x_1^2x_2^2x_3^2+3x_1x_3^4-6x_2^3x_3\in\mathbb{Z}[x]$对于$x_1,x_2$和$x_3$的次数分别为2,3和4，而全次数是6。

由于技术上的原因，为方便起见我们定义零多项式的次数为$-\infty$，并且对于符号$\deg 0=-\infty$采用如下的规定：对于任何整数n，$(-\infty)<n$，$(-\infty)+n=-\infty=n+(-\infty)$，$(-\infty)+(-\infty)=-\infty$。

定理6.1 设R是环而$f,g\in R[x_1,\cdots,x_n]$。则

(i) $\deg(f+g)\leqslant\max(\deg f,\deg g)$。

(ii) $\deg(fg)\leqslant\deg f+\deg g$。

(iii) 如果R没有零因子，则$\deg(fg)=\deg f+\deg g$。

(iv) 如果$n=1$，并且f或者g的首项系数不是R中的零因子(比如当它是单位的时候)，则$\deg(fg)=\deg f+\deg g$。

注记：如果$\deg f$改成f对于x_k的次数，则定理也是对的。

证明概要 由于我们今后主要应用$n=1$的情形，我们只对此

情形加以证明。(i)的证明是容易的。在 $f=0$或者 $g=0$的时候，(ii)也显然是对的。如果 $0\neq f=\sum_{i=0}^{n}a_ix^i$ 次数为n，$0\neq g=\sum_{i=0}^{m}b_ix^i$ 的次数为 m，则 $fg=a_0b_0+\cdots+(a_{n-1}b_m+a_nb_{m-1})x^{n+m-1}+a_nb_mx^{n+m}$ 的次数至多为 $m+n$。由于 $a_n\neq 0\neq b_m$，从而fg的次数为 $m+n\Longleftarrow a_n$和b_m至少有一个不是零因子。∎

定理6.2 （除法算式） 设R是含幺环，$f,g\in R[x]$均为非零多项式，并且g的首项系数是R中的单位。则存在唯一决定的多项式$q,r\in R[x]$，使得

$$f=qg+r \qquad \text{并且}\deg r<\deg g.$$

证明 如果 $\deg g>\deg f$，取 $q=0$，$r=f$即可。如果 $\deg g\leqslant\deg f$，则$f=\sum_{i=0}^{n}a_ix^i$，$g=\sum_{i=0}^{m}b_ix^i$，其中 $a_n\neq 0$，$b_m\neq 0$，$m\leqslant n$，并且b_m为R中单位。现在对于$n=\deg f$ 采用数学归纳法。如果$n=0$，则$m=0$，$f=a_0$，$g=b_0$并且b_0是单位。令$q=a_0b_0^{-1}$，$r=0$，则 $\deg r<\deg g$ 并且 $qg+r=(a_0b_0^{-1})b_0=a_0=f$。

现在假设对于每个次数小于$n=\deg f$的多项式，满足定理条件的q和r都是存在的。通过直接计算可知，多项式$(a_nb_m^{-1}x^{n-m})g$的次数为n并且首项系数为a_n。从而

$$f-(a_nb_m^{-1}x^{n-m})g=(a_nx^n+\cdots+a_0)-(a_nx^n+\cdots+a_nb_m^{-1}b_0x^{n-m})$$

是次数小于n的多项式。根据归纳假设，存在多项式q'和r，使得

$f-(a_nb_m^{-1}x^{n-m})g=q'g+r$ 并且 $\deg r<\deg g$。于是令 $g=a_nb_m^{-1}x^{n-m}+q'$，则

$$f=(a_nb_m^{-1}x^{n-m})g+q'g+r=qg+r.$$

（唯一性） 假设$f=g_1q+r_1$，$f=g_2q+r_2$，其中$\deg r_1<\deg g$，

$\deg r_2 < \deg g$。则 $q_1 g + r_1 = q_2 g + r_2 \Rightarrow (q_1 - q_2)g = r_2 - r_1$。由于$g$的首项系数$b_m$是单位，从而由定理6.1推出

$\deg(q_1 - q_2) + \deg g = \deg(q_1 - q_2)g = \deg(r_2 - r_1)$。因为$\deg(r_2 - r_1) \leqslant \max(\deg r_2, \deg r_1) < \deg g$，从而只有$\deg(q_1 - q_2) = (-\infty) = \deg(r_2 - r_1)$的时候上面的等式才能成立。换句话说，我们有$q_1 - q_2 = 0$同时$r_2 - r_1 = 0$。∎

系6.3 （余数定理） 如果R是含幺环而

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$$

对于每个$c \in R$，则存在唯一的$q(x) \in R[x]$，使得$f(x) = q(x)(x - c) + f(c)$。

证明 $f = 0$时取$q = 0$即可。现设$f \neq 0$。由定理6.2可知存在唯一的多项式$q(x), r(x) \in R[x]$，使得$f(x) = q(x)(x - c) + r(x)$，其中$\deg r(x) < \deg(x - c) = 1$。因此$r(x) = r$是常数多项式（可能为0）。如果$q(x) = \sum_{j=1}^{n-1} b_j x^j$，则 $f(x) = q(x)(x - c) + r = -b_0 c + \sum_{k=1}^{n-1}(-b_k c + b_{k-1})x^k + b_{n-1}x^n + r$，从而

$$\begin{aligned} f(c) &= -b_0 c + \sum_{k=1}^{n-1}(-b_k c + b_{k-1})c^k + b_{n-1}c^n + r \\ &= -\sum_{k=0}^{n-1} b_k c^{k+1} + \sum_{k=1}^{n} b_{k-1} c^k + r \\ &= 0 + r = r. \end{aligned}$$

∎

系6.4 如果F是域，则多项式环$F[x]$是欧氏整环，从而$F[x]$是主理想整环和唯一因子分解整环。$F[x]$中的单位恰好是其中全部非零常数。

证明概要 由定理5.1知$F[x]$是整环。定义φ：$F[x]-\{0\}\to \boldsymbol{N}$，$\varphi(f)=\deg f$。由于$F$中非零元素均是单位，由定理 6.1(iv)和6.2便知$F[x]$是欧氏整环。因此 $F[x]$是主理想整环和唯一因子分解整环(定理3.9)。最后，定理6.1(iv)推出$F[x]$中每个单位f的次数均为0，从而f是非零常数。反过来显然是对的。∎

如果F是域，则当$n\geqslant 2$时$F[x_1,\cdots,x_n]$不是主理想整环（习题1)，但它是唯一因子分解整环（下面的定理6.14)。在证明后一事实之前，我们先讨论多项式环中关于1次因子的某些事实。

定义6.5 设 R 是交换环S的子环，$f=\sum_{i=0}^{m} a_i x_1^{k_{i1}}\cdots x_n^{k_{in}}\in R[x_1,\cdots,x_n]$是一个多项式，$c_1,\cdots,c_n\in S$使得$f(c_1,c_2,\cdots,c_n)=0$，我们称$(c_1,c_2,\cdots,c_n)$为$f$的根或者$f$的零点（或者叫作多项式方程$f(x_1,\cdots,x_n)=0$的一个解)。[4.〔注〕]

定理6.6 设R是含幺交换环，$f\in R[x]$，则$c\in R$是f的根$\Longleftrightarrow$$x-c$可以整除$f$。

证明概要 由系6.3我们有 $f(x)=q(x)(x-c)+f(c)$。如果$(x-c)\mid f(x)$，则 $h(x)(x-c)=f(x)=q(x)(x-c)+f(c)$，其中$h\in R[x]$，从而$(h(x)-q(x))(x-c)=f(c)$。但是$R$为交换环，由

---

4. 定义中的交换性不是本质的，但是对于非交换环S我们要区分“左根”和“右根”(对于后一情形，多项式f要写成$f=\sum x_1^{k_{i1}}\cdots x_n^{k_{in}}a_i$)。

〔注〕 更确切地，将$(c_1,c_2,\cdots,c_n)$称为f在S中的根，或者叫作f在S中的零点，或者叫作多项式方程$f(x_1,\cdots,x_n)=0$在S中的一个解。 ——译者

系5.6(取$\varphi=1_R$)可知 $f(c)=(h(c)-q(c))(c-c)=0$. 反过来则不需要交换性，但是仍需应用系6.3. ∎

定理6.7 如果D是整环，并且包含在整环E之中，而$f\in D[x]$的次数为n，则f在E中至多有n个不同的根.

证明概要 设 $c_1,c_2,\cdots$ 是f 在 E 中全体相异的根. 由定理6.6，$f(x)=q_1(x)(x-c_1)$，从而由系5.6，$0=f(c_2)=q(c_2)(c_2-c_1)$. 由于$c_2\neq c_1$而E是整环，可知$q_1(c_2)=0$. 于是$x-c_2$整除q_2，于是$f(x)=q_3(x)(x-c_2)(x-c_1)$. 现在采用归纳法便可证明：如果$c_1,c_2,\cdots,c_m$是$f$在$E$中相异的根，则$g_m=(x-c_1)(x-c_2)\cdots(x-c_m)$整除$f$. 但是由定理6.1，$\deg g_m=m$. 再由定理6.1即可知$m\leqslant n$. ∎

注记：如果不假设交换性，定理6.7可能会不对. 例如x^2+1在实四元数体中有无穷多个不同的根(包括$\pm i$，$\pm j$和$\pm k$).

如果D是唯一因子分解整环，它的商域为F，$f\in D[x]$，则可以用下面命题求f在F中的根.

命题6.8 设D是唯一因子分解整环，其商域为F. 令 $f=\sum_{i=0}^{n}a_ix^i\in D[x]$. 如果$u=c/d\in F$，其中$c,d\in D$，$c$和$d$互素，并且$u$是$f$的根. 则 $c\mid a_0$同时 $d\mid a_n$.

证明概要 $f(u)=0$推出$a_0d^n=c\left(\sum_{i=1}^{n}(-a_i)c^{i-1}d^{n-i}\right)$和$-a_nc^n=\left(\sum_{i=0}^{n-1}c^id^{n-i-1}\right)d$. 因此，如果 $(c,d)=1_R$，则由习题 3.10 可知$c\mid a_0$并且$d\mid a_n$. ∎

例 如果 $f=x^4-2x^3-7x^2-(11/3)x-4/3\in\mathbf{Q}[x]$，则$f$与$3f=3x^4-6x^3-21x^2-11x-4\in\mathbf{Z}[x]$ 在$\mathbf{Q}$中有同样的根。根据命题6.8，$3f$只可能有如下的有理根：$\pm1,\pm2,\pm4,\pm1/3,\pm2/3$和$\pm4/3$。代入验证可知其中只有4是它的有理根。

设D为整环而 $f\in D[x]$。如果 $c\in D$ 是f的根，重复使用定理6.6和定理6.7可知存在最大整数$m(0\leqslant m\leqslant\deg f)$，使得

$$f(x)=(x-c)^m g(x)$$

其中$g(x)\in R[x]$而且 $(x-c)\nmid g(x)$(即$g(c)\neq0$)。整数m叫作f的根 c 的重数。如果c的重数为1，c叫作单根。如果c的重数$m>1$，c叫作重根。为了决定何时多项式有重根，我们需要：

引理6.9 设D 是整环，$f=\sum_{i=0}^{n}a_ix^i\in D[x]$。令 $f'\in D[x]$是多项式$f'=\sum_{k=1}^{n}ka_kx^{k-1}=a_1+2a_2x+3a_3x^2+\cdots+na_nx^{n-1}$，则对所有$f,g\in D[x]$和$c\in D$：

(i) $(cf)'=cf'$

(ii) $(f+g)'=f'+g'$

(iii) $(fg)'=f'g+fg'$

(iv) $(g^n)'=ng^{n-1}g'$

证明作为练习。∎

多项式f'叫作f的形式微商。我们加上“形式”一词是为了强调这里f'的定义不涉及极限概念。

根据定义3.3，非零多项式$f\in R[x]$叫作不可约的，是指 f不是单位并且对于每个分解式$f=gh$，g或h至少有一个是 $R[x]$中的单位。

定理6.10 假设D是整环，并且是整环E的子环。令$f\in D[X]$，$c\in E$。

(i) c为f的重根$\Longleftrightarrow f(c)=0$同时$f'(c)=0$。

(ii) 如果D是域并且f和f'互素，则f在E中无重根。

(iii) 如果D是域，f在$D[x]$中不可约，而E包含f的一个根，则f在E中无重根$\Longleftrightarrow f'\neq 0$。

证明 (i) $f(x)=(x-c)^m g(x)$，其中m为f的根c的重数($m\geqslant 0$) 而$g(c)\neq 0$。由引理6.9可知$f'(x)=m(x-c)^{m-1}g(x)+(x-c)^m g'(x)$。如果$c$是$f$的重根，则$m>1$，于是$f'(c)=0$。反之若$f(c)=0$，则$m\geqslant 1$(定理6.6)。如果$m=1$，则$f'(x)=g(x)+(x-c)g'(x)$。因此若$f'(c)=0$，则由系5.6便知$0=f'(c)=g(c)$，这就导出矛盾。因此$m>1$。

(ii) 由系6.4和定理3.11可知有$k,h\in D[x]\subset E[x]$，使得$kf+hf'=1_D$。如果c为f的重根，由系5.6和(i)可知$1_D=k(c)f(c)+h(c)f'(c)=0$，这就导致矛盾。从而c是单根。

(iii) 如果f不可约而$f'\neq 0$，则f和f'互素，因为$\deg f'<\deg f$。因此由(ii)可知f在E中无重根。反之，假设f在E中无重根而b是f在E中的根。如果$f'(b)=0$，由(i)知b为重根，这就导致矛盾。从而$f'\neq 0$。∎

以上我们完成了对多项式线性因子的讨论。我们现在考虑更一般的问题，即决定多项式环$D[x]$中的单位和不可约元，其中D是整环。一般来说这是件相当困难的事情，但是有些事实是容易建立起来的。

(i) $D[x]$中的单位恰好是常数多项式，同时这些常数还必须是D中的单位[见系6.4的证明]。

(ii) 如果$c\in D$而c在D中不可约，则常数多项式c在$D[x]$中也不可约[利用定理6.1和(i)]。

(iii) 一次多项式的首项系数如果是 D 中的单位，则它在$D[x]$中不可约。特别地，域上每个一次多项式都不可约。

(iv) 假设D是整环E的子环并且 $f\in D[x]\subset E[x]$。则f可能在$E[x]$中不可约但在$D[x]$中可约，也可能f在$D[x]$中不可约但在$E[x]$中可约。这可见下面的例子。

例 由上面的(iii)可知$2x+2$在$\mathbf{Q}[x]$中不可约，但是$2x+2=2(x+1)$，而由(i)知2和$x+1$均不是$\mathbf{Z}[x]$中的单位，从而$2x+2$在$\mathbf{Z}[x]$中可约。x^2+1在实数域中不可约，但是在复数域中可以分解成$(x+i)(x-i)$。由(i)可知 $(x+i)$ 和 $(x-i)$ 均不是$\mathbf{C}[x]$中单位，从而(x^2+1)在$\mathbf{C}[x]$中可约。

为了在这一领域得到稍多一些的一般结果，以下我们只限于讨论唯一因子分解整环D上的多项式。事实上我们要证明$D[x_1,\cdots,x_n]$也是唯一因子分解整环。证明需要一些予备知识，这些予备知识也提供了对于$D[x]$中不可约性的一个判别法则。

设D是唯一因子分解整环，$f=\sum_{i=0}^{n}a_ix^i$是$D[x]$中的非零多项式。系数$a_0,a_1,\cdots,a_n$的最大公因子叫作f的容量(Content)，并表示成$C(f)$。严格说来，符号$C(f)$有些混淆，因为最大公因子不是唯一的。但是，f的任意两个容量必然是相伴的，而与f的容量相伴的元素也必然是f的容量。我们以$b\approx c$表示b和c在D中相伴。则$\approx$是D上的等价关系，并且由于D是整环，从而$b\approx c\Longleftrightarrow b=cu$，其中$u$为$D$中单位(定理3.2(vi))。如果$a\in D$而$f\in D[x]$，则$C(af)\approx aC(f)$ (习题4)。如果$f\in D[x]$而 $C(f)$为D中单位，我们称f是本原多项式。显然，对于每个多项式 $g\in D[x]$，$g=C(g)g_1$，其中

g_1是本原多项式。

引理6.11 (Gauss) 如果 D 是唯一因子分解整环而 $f,g\in D[x]$，则 $C(fg)\approx C(f)C(g)$。特别地，本原多项式的乘积仍是本原多项式。

证明 $f=C(f)f_1$，$g=C(g)g_1$，其中 f_1,g_1为本原多项式。则 $C(fg)=C(C(f)f_1C(g)g_1)\approx C(f)C(g)C(f_1g_1)$。从而我们只需要证$f_1g_1$本原(即$C(f_1g_1)$是单位)即可。如果 $f_1=\sum_{i=0}^{m}a_ix^i$，

$g_1=\sum_{j=0}^{n}b_jx^j$，则 $f_1g_1=\sum_{k=0}^{m+n}c_kx^k$，其中$c_k=\sum_{i+j=k}a_ib_j$ 如果f_1g_1不本原，则存在R中不可约元p，使得$p\mid c_k$(对于所有k)。由于$C(f_1)$是单位，从而 $p\nmid C(f_1)$，于是存在整数s，使得

$p\mid a_i$(对于$i<s$) 而$p\nmid a_s$。

类似地，存在整数t，使得

$p\mid b_j$ (对于$j<t$) 而$p\nmid b_t$。

但是 p 整除 $c_{s+t}=a_0b_{s+t}+\cdots+a_{s-1}b_{t+1}+a_sb_t+a_{s+1}b_{t-1}+\cdots+a_{s+t}b_0$，从而$p$必然整除 a_sb_t。因为D中不可约元均是素元，从而$p\mid a_s$或者$p\mid b_t$。这就导出矛盾。因此f_1g_1是本原的。∎

引理6.12 令D为唯一因子分解整环，其商域为F，令f和g是$D[x]$中的本原多项式，则f与g在$D[x]$中相伴$\Longleftrightarrow$它们在 $F[x]$中相伴。

证明 如果f与g在整环$F[x]$中相伴，则$f=gu$，其中u是$F[x]$中单位 (定理3.2(vi))。根据系6.4可知$u\in F$，从而 $u=b/c$，其中$b,c\in D$，$c\neq 0$。因此$cf=bg$。由于$C(f)$和$C(g)$均是D中单位，

从而

$c \approx cC(f) \approx C(cf) = C(bg) \approx bC(g) \approx b$. 因此$b = cv$, 其中$v$是$D$中的单位, 并且$cf = bg = vcg$. 从而$f = vg$ (因为$c \neq 0$), 于是f和g在$D[x]$中相伴. 反过来显然是成立的. ∎

引理6.13 设D是唯一因子分解整环, 其商域为F, f是$D[x]$中正次数本原多项式. 那末f在$D[x]$中不可约$\Longleftrightarrow f$在$F[x]$中不可约.

证明概要 假设f在$D[x]$中不可约并且$f = gh$, 其中$g, h \in F[x]$并且$\deg g \geqslant 1$, $\deg h \geqslant 1$. 则$g = \sum_{i=0}^{n} (a_i/b_i)x^i$, $h = \sum_{j=0}^{m} (c_j/d_j)x^j$, 其中$a_i, b_i, c_j, d_j \in D$并且$b_i \neq 0, d_j \neq 0$. 令$b = b_0 b_1 \cdots b_n$并且对于每个$i$, 令$b_i^* = b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n$. 如果$g_1 = \sum_{i=0}^{n} a_i b_i^* x^i \in D[x]$, 则$g_1 = ag_2$其中$a = C(g_1)$, $g_2 \in D[x]$并且g_2是本原多项式. 验证$g = (1_D/b)g_1 = (a/b)g_2$并且$\deg g = \deg g_2$. 类似地有$h = (c/d)h_2$, 其中$c, d \in D$, $h_2 \in D[x]$, h_2本原而$\deg h = \deg h_2$. 于是$f = gh = (a/b)(c/d)g_2h_2$, 从而$bdf = acg_2h_2$. 由假设$f$是本原的, 又由引理6.11知$g_2h_2$也是本原的, 从而

$$bd \approx bdC(f) \approx C(bdf)$$
$$= C(acg_2h_2) \approx acC(g_2h_2) \approx ac$$

象在引理6.12的证明中所作的那样, 由bd和ac在D中相伴, 推出f和g_2h_2在$D[x]$中相伴. 从而f在$D[x]$中可约, 而这就导致矛盾. 因此f在$F[x]$中不可约.

反之, 如果f在$F[x]$中不可约但是$f = gh$, 其中$g, h \in D[x]$, 由系6.4 可知g和h之中必有一个 (设为g) 是常数. 因此 $C(f) =$

$gC(h)$。由于f是本原的，g必定为D中的单位，从而也是 $D[x]$中的单位。因此$f(x)$在$D[x]$中不可约。 ∎

定理6.14 如果D是唯一因子分解整环，则多项式环$D[x_1,\cdots,x_n]$也是唯一因子分解整环。

注： 由于域F显然是唯一因子分解整环，从而$F[x_1,\cdots,x_n]$是唯一因子分解整环。

证明概要 我们只需证明 $D[x]$ 是唯一因子分解整环即可。因为由系5.7知 $D[x_1,\cdots,x_n]=D[x_1,\cdots,x_{n-1}][x_n]$，从而用数学归纳法即可给出完全的证明。如果 $f\in D[x]$ 有正次数，则 $f=C(f)f_1$，f_1为$D[x]$中正次数的本原多项式。由于D是唯一因子分解整环，从而$C(f)$或者是单位，或者$C(f)=c_1c_2\cdots c_m$其中每个c_i在D中均不可约，因此在 $D[x]$中也不可约。令F是D的商域。由于 $F[x]$ 是唯一因子分解整环(系6.4)，并且包含 $D[x]$，从而 $f_1=p_1^*p_2^*\cdots p_n^*$，其中每个$p_i^*$均是$F[x]$中的不可约多项式。从引理6.13的证明可知对于每个i，$p_i^*=(a_i/b_i)p_i$，其中$a_i,b_i\in D$，$b_i\neq 0$，$a_i/b_i\in F$，$p_i\in D[x]$，并且p_i是本原的。每个p_i在$F[x]$中显然是不可约的，从而由引理6.13可知每个p_i在$D[x]$中也是不可约的。如果令$a=a_1a_2\cdots a_n$，$b=b_1b_2\cdots b_n$，则$f_1=(a/b)p_1p_2\cdots p_n$。从而$bf_1=ap_1p_2\cdots p_n$。由于 f_1 和 $p_1p_2\cdots p_n$ 均是本原的(引理6.11)，从而(象在引理6.12的证明中所作的那样) a和b在 D中相伴。因此 $a/b=u$，其中u为D中单位。所以当$C(f)$不是单位的时候，$f=C(f)f_1=c_1c_2\cdots c_m(up_1)p_2\cdots p_n$，其中每个$c_i$，$p_i$与$up_1$在$D[x]$中均不可约。同样地，如果$C(f)$是单位，则$f$也是$D[x]$中一些不可约元素的乘积。

(唯一性) 假设f是 $D[x]$ 中正次数的非本原多项式。验证f

分解成不可约元之乘积的任一分解式均可写成 $f=c_1c_2\cdots c_mp_1\cdots p_n$，其中每个 c_i均是 D 中不可约元，$C(f)=c_1\cdots c_m$，而每个p_i均是$D[x]$中正次数的不可约元(从而为本原的)。假设$f=d_1\cdots d_rq_1\cdots q_s$，其中每个 d_j在D中均不可约，$C(f)=d_1\cdots d_r$，并且每个 q_j均是$D[x]$中正次数的不可约本原多项式。则$c_1c_2\cdots c_n$和$d_1d_2\cdots d_r$在D中相伴。从D中的唯一因子分解性质可以推出$n=r$，并且(在重新标号之后) 每个c_i与d_i相伴。从而 $p_1p_2\cdots p_n$和$q_1q_2\cdots q_s$在$D[x]$中相伴，于是也在 $F[x]$ 中相伴。根据引理6.13，每个p_i和q_j在$F[x]$中均是不可约的，由$F[x]$中的唯一因子分解性质(系6.4) 推得$n=s$，并且 (在重新标号之后) 每个p_i在$F[x]$中均与q_i相伴。根据引理6.12，便知p_i与q_i在$D[x]$中相伴。∎

定理6.15 (Eisenstein 判别法) 假设 D是唯一因子分解整环，其商域为F。如果$f=\sum_{i=0}^{n}a_ix^i\in D[x]$，$\deg f\geqslant 1$，并且$p$为$D$中的不可约元，使得

$$p\nmid a_n;\ p\mid a_i(0\leqslant i\leqslant n-1);\ p^2\nmid a_0.$$

则f在$F[x]$中不可约。又如果f是本原的，则f在$D[x]$中不可约。

证明 $f=C(f)f_1$，其中f_1为$D[x]$中本原多项式而 $C(f)\in D$ (特别当f为本原多项式时，$f_1=f$)，由于 $C(f)$是F中的单位 (系6.4)。只需证f_1在$F[x]$中不可约即可。根据引理6.13，我们只需证明f_1在$D[x]$中不可约即可。假如不然的话，即$f_1=gh$，其中

$$g=b_rx^r+\cdots+b_0\in D[x],\ \deg g=r\geqslant 1,$$

$$h=c_sx^s+\cdots+c_0\in D[x],\ \deg h=s\geqslant 1.$$

现在p不能除尽$C(f)$(因为$p\nmid a_n$)，从而 $f_1=\sum_{i=0}^{n}a_i^*x^i$ 的诸系数对

于p满足与f的诸系数相同的整除性条件。如果p能够整除$a_0^* = b_0c_0$，由于D中每个不可约元均是素元，从而或者$p|b_0$或者$p|c_0$。假设$p|b_0$，由于$p^2\nmid a_0^*$，c_0不能被p所整除。但是g有某个系数b_k不能被p所整除（不然的话，p将能整除$gh=f_1$的每个系数，这就导出矛盾）。令k是满足下列条件的整数：

$p|b_i$(对于$i<k$)但是$p\nmid b_k$。

则$1\leqslant k\leqslant r<n$。由于$a_k^* = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}C_1 + b_kc_0$，并且$p|a_k^*$，从而$p$必然整除$b_kc_0$，于是$p$必然能够整除$b_k$或者$c_0$。但这是不可能的，从而$f_1$必然在$D[x]$中不可约。∎

例 如果$f = 2x^5 - 6x^3 + 9x^2 - 15 \in \mathbf{Z}[x]$，取$p=3$，由Eisenstein判别法可知$f$在$\mathbf{Q}[x]$和$\mathbf{Z}[x]$中均不可约。

例 令$f = y^3 + x^2y^2 + x^3y + x \in R[x,y]$，其中$R$为唯一因子分解整环。则$x$在$R[x]$中不可约，从而$f$看作为$(R[x])[y]$中的元素是本原的。于是由定理6.14和Eisenstein判别法（取$p=x$，$D=R[x]$）可知f在$R[x][y]=R[x,y]$中是不可约的。

Eisenstein 判别法的另一个应用可见习题10。对于只有有限多单位的唯一因子分解整环（例如$\mathbf{Z}$），Kronecker 给出一个寻求在这种整环上一个多项式的全部不可约因子的方法，但是方法比较复杂（习题13）。关于其他例子和技巧可见习题6—9。

习　题

1. (a) 如果D是整环而c是D中的一个不可约元，则$D[x]$不是主理想整环。〔提示：考虑由x和c生成的理想(x, c)。〕

(b) $\mathbf{Z}[x]$不是主理想整环。

(c) 如果F是域而$n\geqslant 2$，则$F[x_1, \cdots, x_n]$不是主理想整环。〔提示：证

明x_1在$F[x_1, \cdots, x_{n-1}]$中不可约.]

2. 如果F是域而$f, g \in F[x]$并且$\deg g \geqslant 1$，则存在唯一决定的多项式$f_0, f_1, \cdots, f_r \in F[x]$，使得$\deg f_i < \deg g$（对每个$i$）并且

$$f = f_0 + f_1 g + f_2 g^2 + \cdots + f_r g^r.$$

3. 假设$f(x)$是整环D上的正次数多项式.

(a) 如果$\mathrm{char} D = 0$，则$f' \neq 0$

(b) 如果$\mathrm{char} D = p \neq 0$，则$f' = 0 \Longleftrightarrow f$为$x^p$的多项式（即$f = a_0 + a_1 x^p + a_2 x^{2p} + \cdots a_j x^{jp}$）.

4. 如果D是唯一因子分解整环，$a \in D$，$f \in D[x]$，则$C(af)$和$aC(f)$在D中相伴.

5. 令R为含幺交换环，$f = \sum_{i=0}^{n} a_i x^i \in R[x]$. 则$f$是$R[x]$中的单位$\Longleftrightarrow a_0$是$R$中单位而$a_1, \cdots, a_n$均是$R$的幂零元素（习题1.12）

6. 设$p \in \mathbf{Z}$是素数，F是域，$c \in F$，则$x^p - c$在$F[x]$中不可约的充要条件是$x^p - c$在F中无根.[提示：考虑$\mathrm{char} F = p$和$\mathrm{char} F \neq p$两种情形.]

7. 如果$f = \Sigma a_i x^i \in \mathbf{Z}[x]$，$p$是素数，令$\overline{f} = \Sigma \overline{a_i} x^i \in Z_p[x]$，其中$\overline{a}$是$a$在正则满同态$\mathbf{Z} \to Z_p$之下的象.

(a) 如果f是首1多项式并且$\overline{f}$在$Z_p[x]$中不可约(对于某个素数p)，则f在$\mathbf{Z}[x]$中也不可约.

(b) 给出例子表明：若f不是首1多项式的时候，(a) 可能不再成立.

(c) 将(a) 推广到任一唯一因子分解整环上的多项式的情形.

8. (a) 令$c \in F$，其中F是特征为p（p为素数）的域，则$x^p - x - c$在$F[x]$中不可约$\Longleftrightarrow x^p - x - c$在$F$中无根.

(b) 如果$\mathrm{char} F = 0$，则(a) 不再成立.

9. 设$f = \sum_{i=0}^{n} a_i x^i \in \mathbf{Z}[x]$，$\deg f = n$. 又设对某个$k$（$0 < k < n$）和某个素数$p$满足：$p \nmid a_n$，$p \nmid a_k$，$p \mid a_i$（$0 \leqslant i \leqslant k-1$）并且$p^2 \nmid a_0$. 求证$f$有一个次数至少为$k$的因子$g$，并且$g$在$\mathbf{Z}[x]$中不可约.

10. (*a*) 假设D是整环而$c\in D$. 令$f(x)=\sum_{i=0}^{n}a_ix^i\in D[x]$并且$f(x-c)=\sum_{i=0}^{n}a_i(x-c)^i\in D[x]$. 则$f(x)$在$D[x]$中不可约的充要条件是$f(x-c)$在$D[x]$中不可约.

(*b*) 对于每个素数p, 分圆多项式$f=x^{p-1}+x^{p-2}+\cdots+x+1$在$\mathbf{Z}[x]$中不可约. 〔提示: 注意$f=(x^p-1)/(x-1)$, 从而$f(x+1)=((x+1)^p-1)/x$. 用二项式定理1.6和Eisenstein判别法证明$f(x+1)$在$\mathbf{Z}[x]$中不可约.〕

11. 如果$c_0, c_1, \cdots, c_n$是整环D中两两相异的元素, $d_0, \cdots, d_n$是D中任意元素, 则在$D[x]$中至多有一个$n+1$次多项式f, 使得$f(c_i)=d_i$ $(0\leqslant i\leqslant n)$. 〔关于$f$的存在性见习题12.〕

12. Lagrange 插值公式 如果F是域, $a_0, a_1, \cdots, a_n$是F中两两相异的元素, $c_0, c_1, \cdots, c_n$是F中任意元素, 则

$$f(x)=\sum_{i=0}^{n}\frac{(x-a_0)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_0)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)}c_i$$

是$F[x]$中唯一的多项式, 使得$f(a_i)=c_i$ $(0\leqslant i\leqslant n)$〔参见习题11.〕

13. 设D为唯一因子分解整环并且只有有限多个单位. F是它的商域. 如果$f\in D[x]$的次数为n, 而$c_0, c_1, \cdots, c_n$是D中$n+1$个不同的元素, 那末根据习题11, f由$f(c_0), f(c_1), \cdots, f(c_n)$所完全决定. 下面是求$f$在$D[x]$中全部不可约因子的*Kronecker*方法.

(*a*) 只需求次数$\leqslant n/2$的因子g即可.

(*b*) 如果g是f的因子, 则对于每个$c\in D$, $g(c)$均是$f(c)$的因子.

(*c*) 以m表示$\leqslant n/2$的最大整数. 取D中不同的元素$c_0, c_1, \cdots, c_m$. 再选取$d_0, d_1, \cdots, d_m\in D$, 使得对每个$i$, d_i在D中是$f(c_i)$的因子. 利用习题12构作一个多项式$g\in F[x]$, 使得$g(c_i)=d_i$ $(0\leqslant i\leqslant m)$. 根据习题11可知$g$是唯一的.

(*d*) 检查(*c*)中的多项式g是否为f在$F[x]$中的因子。如果不是，则再重新选择d_0，…，d_m并且重复过程(*c*)（由于D是唯一因子分解整环并且只有有限多个单位，从而d_0，…，d_m只有有限多种选取方法)。如果g是f的因子，假设$f=gh$，再对g和h重复整个过程。

(*e*) 经过有限步骤之后，便可求出f在$F[x]$中的全部（不可约）因子。如果$g\in F[x]$是这样一个（正次数的）因子，取$r\in D$使$rg\in D[x]$（例如令r为g之诸系数的分母的乘积)。则$r^{-1}(rg)$从而rg也是f的因子。于是$rg=C(rg)g_1$，其中$g_1\in D[x]$本原并且在$F[x]$中不可约。根据引理6.13，g_1是f在$D[x]$中的一个不可约因子。采用这种方法可以得到f的全部非常数的不可约因子。然后便很容易发现它的常数因子。

14. 假设R是含幺交换环，c，$b\in R$，c为单位。

(*a*) 证明$x\longmapsto cx+b$诱导出$R[x]$中唯一的一个自同构，使它在R上为恒等映射。这个自同构的逆是什么？

(*b*) 如果D是整环，证明$D[x]$的自同构如果在D上为恒等自同构，则必有(*a*) 中所描述的形式。

15. 如果F是域，则x和y在多项式整环$F[x,y]$中是互素的，但是$F[x,y]=(1_F)\supsetneq(x)+(y)$[比较定理3.11(i)]。

16. 假设$f=a_nx^n+\cdots+a_0$是实数域$\mathbf{R}$上的多项式，并且令$\varphi=|a_n|x^n+\cdots+|a_0|\in R[x]$。

(*a*) 如果$|u_i|\leqslant d_i$ $(1\leqslant i\leqslant n)$则$|f(u_1,\ \cdots,\ u_n)|\leqslant\varphi(d_1,\ \cdots,d_n)$。

[注意$|a+b|\leqslant|a|+|b|$；并且：$|a|\leqslant a'$，$|b|\leqslant b'\Rightarrow|ab|\leqslant a'b'$]。

(*b*) 给了b，$c\in\mathbf{R}$，$c>0$，则存在$M\in\mathbf{R}$，使得对于每个$h\in\mathbf{R}$，$|h|\leqslant c$，均有$|f(a+h)-f(a)|\leqslant M|h|$。[提示：利用(*a*)。]

(*c*) (中值定理)。如果$a<b$，$f(a)<d<f(b)$，则存在$c\in\mathbf{R}$使得$a<c<b$并且$f(c)=d$。[提示：取c为$S=\{x|a<x<b,\ f(x)\leqslant d\}$的上端。并利用(*b*)。]

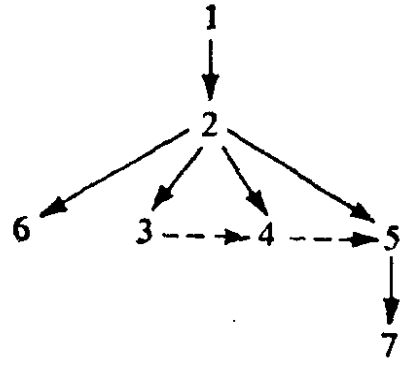
(*d*) $\mathbf{R}[x]$中每个奇次多项式g均有实根。[提示：取适当的a，$b\in\mathbf{R}$，使得$g(a)<0$，$g(b)>0$。然后用(*c*)。]

第IV章　模

环上的模是Abel群的一种推广（后者是$\mathbb{Z}$上的模）。它们是进一步研究代数学的基础。第1节主要是将群论中的各种概念和结果移植到模上来。虽然在任意环上模的（同构）分类是相当困难的，但是对于环上的自由模（第2节）和主理想整环上的有限生成模（第6节）我们给出本质上完全的结果。自由模有很广泛的应用（例如体上的向量空间即是它的特殊情形），在第2节要对它进行充分的研究。第3节中考虑投射模（这是自由模的一种推广），这节的内容只在第VIII．6节和第IX章中用到。

除了第2节和第6节之外，我们把注意力更多地集中于与模有关的一些外部结构，而不是模本身的内部结构。对于模理论中的某些范畴特性，例如正合序列（第1节）和模同态（第4节），我们具有特殊的兴趣。此外，我们还研究与模有关的各种构造：例如张量积（第5节）等。第7节介绍含幺交换环K上的代数。

本章诸节之间的内部联系大致如下图所示：其中虚线箭头$A\cdots\rightarrow B$表示第A节中某些结果在第B节中使用，但是第B节与第A节本质上是独立的。



1. 模，同态和正合序列

环上的模是Abel群的一种推广（后者是$\mathbb{Z}$上的模）. 所以在这一节的第一部分主要是将群论中的各种概念和结果移植到模上来，本节的其余部分给出关于正合序列的一些基本事实.

定义1.1 设R是环. 一个（左）R-模是指一个加法Abel群A与一个函数$R\times A\to A$（以ra表示(r, a)的象），使得对于所有$r, s\in R$和$a, b\in A$：

(i) $r(a+b)=ra+rb$.

(ii) $(r+s)a=ra+sa$.

(iii) $r(sa)=(rs)a$.

如果R有幺元素1_R并且

(iv) $1_Ra=a$，对于每个$a\in A$，

则A称作幺作用R-模. 如果R是体，则幺作用R-模也叫作（左）向量空间.

类似地，利用一个函数$A\times R\to A$（表示成$(a,r)\longmapsto ar$）并且满足与(i)－(iv)相类似的性质，可以定义（幺作用）右R-模. 从现在起，如果不作特别说明，则“R-模”均指的是“左R-模”. 容易看出，将所有关于左R-模的定理加以必要的修改，均可适用于右R-模.

一个给定的群A可以有许多不同的R-模结构（左模或者右模）. 如果R是交换环，不难验证，通过定义$ar=ra$（对于所有

$a\in A$，$r\in R$)，每个左R-模A均给出一个右R-模结构（在(iii)中则需要环R的交换性．这种思想可以推广到任意环上，见习题16)．除非特别声明，在交换环R上的每个模均以为既是左模又是右模，即$ar=ra$（对于每个$r\in R$，$a\in A$)．

如果R-模A的零元素为0_A，而环R的零元素为0_R，则不难证明，对于每个$r\in A$，$a\in A$：

$$r0_A=0_A,\quad 0_Ra=0_A.$$

今后我们将0_A，0_R，$0\in\mathbb{Z}$以及平凡模$\{0\}$均表示成0．

同样不难验证，对于每个$r\in R$，$n\in\mathbb{Z}$和$a\in A$：

$$(-r)a=-(ra)=r(-a)\quad n(ra)=r(na).$$

其中na是在群论中所定义的（定义I.1.8，但是这里用加法符号)．

例 每个加法Abel群G是幺作用$\mathbb{Z}$-模，其中na（$n\in\mathbb{Z}$，$a\in G$）由定义I.1.8给出．

例 如果S是环而R是子环，则S是R-模（但是反过来则不对!)，其中$ra(r\in R,\ a\in S)$是S中的乘法．特别地，环$R[x_1,\cdots,x_m]$和$R[[x]]$都是R-模．

例 如果I是环R的左理想，则I是左R-模，其中$ra(r\in R,\ a\in I)$是R中的乘积．特别地，0和R均是R-模．此外，由于I是R的加法子群，R/I也是（Abel）群．并且R/I也是R-模，其中$r_1(r_1+I)=rr_1+I$．但是除非I是双侧理想，否则R/I不是环．

例 设R和S为环，φ：$R\to S$为环同态．则每个S-模A可以作成R-模，办法是定义rx（$x\in A$）为$\varphi(r)x$．我们称A的这个R-模结构是通过φ的回拉（Pullback）所给出的．

例 设A是Abel群，EndA是自同态环(见第174页)．则A是幺作用（End$A$)-模，其中fa定义为$f(a)$(对于$a\in A$，$f\in$End$A$)．

例 如果R是环，则每个Abel群A均可以作成具有平凡模结

构的R-模，即对于所有$r\in R$和$a\in A$定义$ra=0$。

定义1.2 设A和B是环R上的模。函数f：$A\to B$叫作R-模同态，是指对于所有a，$c\in A$和$r\in R$：

$$f(a+c)=f(a)+f(c),\quad f(ra)=rf(a).$$

如果R是体，则R-模同态叫作线性变换。

在课文中清楚的时候，我们就把R-模同态简称作同态。注意：R-模同态f：$A\to B$一定是加法Abel群的同态，从而我们又有类似的一些术语：如果f作为集合映射是单射，满射或者一一对应，则f分别称作R-模单同态，R-模满同态或者R-模同构。f的核是指作为Abel群同态的核，即 $\mathrm{Ker}f=\{a\in A\mid f(a)=0\}$。类似地，$f$的象集合是$\mathrm{Im}f=\{b\in B\mid b=f(a)$，对于某个$a\in A\}$ 最后，从定理I.2.3推出：

(i) f是R-模单同态$\Longleftrightarrow\ker f=0$。

(ii) f：$A\to B$是R-模同构$\Longleftrightarrow$存在着R-模同态g：$B\to A$，使得$gf=1_A$，$fg=1_B$。

例 对于任意模，零映射0：$A\to B$，$a\longmapsto 0(a\in A)$是模同态。Abel群的每个同态均是$\mathbb{Z}$-模同态。如果R是环，则映射$R[x]\to R[x]$，$f\longmapsto xf$(例如$(x^2+1)\longmapsto x(x^2+1)$)是$R$-模同态，但不是环同态。

注记：对于一个给定的环R，所有R-模（或者所有幺作用R-模）与R-模同态显然形成一个（具体）范畴。事实上，我们可以用范畴语言严格地定义满同态和单同态（即只有对象和态射但是没有元素）。见习题2。

定义1.3 设R是环，A是R-模而B是A的非空子集合。我们

称B是A的子模，是指B是A的加法子群，并且对于所有$r\in R$和$b\in B$，$rb\in B$。体上向量空间的子模叫作子空间。

注意子模本身是模。含幺环上的幺作用模的子模也必然是幺作用模。

例 如果R是环，$f: A\to B$是R-模同态，则$\ker f$是A的子模而$\mathrm{Im}f$是B的子模。如果c是B的子模，则$f^{-1}(c)=\{a\in A\mid f(a)\in c\}$是$A$的子模。

例 设I是环R的左理想，A是R-模，而S是A的非空子集。则$IS=\left\{\sum_{i=1}^{n} r_i a_i \mid r_i\in I,\ a_i\in S,\ n\in \mathbf{N}^*\right\}$是$A$的子模（习题3）。类似地，如果$a\in A$，则$Ia=\{ra\mid r\in I\}$是$A$的子模。

例 如果$\{B_i\mid i\in I\}$是模A的子模族，则不难看出$\bigcap_{i\in I} B_i$也是A的子模。

定义1.4 如果X是环R上的模A的一个子集合，A的所有包含X的子模之交叫作由X生成（或者张成）的子模。

如果X是有限的，并且X生成模B，则称B是有限生成模。如果$X=\varnothing$，则X显然生成零模，如果X是一元集合，$X=\{a\}$，则由X生成的子模叫作由a生成的循环（子）模。最后，如果$\{B_i\mid i\in I\}$是A的子模族，则由$X=\bigcup_{i\in I} B_i$生成的子模叫作模B_i $(i\in I)$之和。如果指标集合I是有限的，则B_1，…，B_n的和也表示成$B_1+B_2+\cdots+B_n$。

定理1.5 设R是环，A是R-模，X是A的子集，$\{B_i\mid i\in I\}$是A的子模族，$a\in A$。令$Ra=\{ra\mid r\in R\}$。则

(i) Ra是A的子模，并且映射$R\to Ra, r\longmapsto ra$是R-模满同态.

(ii) 由a生成的循环子模C是$\{ra+na \mid r\in R,\ n\in \mathbf{Z}\}$如果$R$有幺元素并且$C$是幺作用模，则$C=Ra$.

(iii) 由X生成的子模D是

$$\left\{\sum_{i=1}^{s} r_i a_i + \sum_{j=1}^{t} n_j b_j \mid s,t\in \mathbf{N}^*,\ a_i,\ b_j\in X,\ r_i\in R, n_j\in \mathbf{Z}\right\}.$$

如果R有幺元素并且A是幺作用模，则

$$D=RX=\left\{\sum_{i=1}^{s} r_i a_i \mid s\in \mathbf{N}^*,\ a_i\in X,\ r_i\in R\right\}.$$

(iv) $\{B_i \mid i\in I\}$之和为$\{b_{i_1}+\cdots+b_{i_m} \mid b_{i_k}\in B_{i_k},\ n\in \mathbf{N}^*\}$.

证明 作为练习. 注意如果R有幺元素1_R并且A是幺作用模，则对每个$n\in \mathbf{Z}$，$n1_R\in R$，并且对于每个$a\in A$，$na=(n1_R)a$. ∎

定理1.6 设B是环R上模A的子模. 则商群A/B是R-模，其中R在A/B上的作用定义为：

$$r(a+B)=ra+B \quad (r\in R,\ a\in A).$$

映射π：$A\to A/B$，$a\longmapsto a+B$是R-模满同态，并且核是B.

映射π叫作正则满同态（或者叫作射影）.

证明概要 由于A是Abel加法群，B是正规子群，从而A/B可以作成Abel群. 如果$a+B=a'+B$，则$a-a'\in B$. 由于B是子模，可知对每个$r\in R$，$ra-ra'=r(a-a')\in B$. 因此由系 I.4.3可知$ra+B=ra'+B$. 从而可以定义出R在A/B上的作用. 证明的其余部分是容易的. ∎

以上述诸结果可以毫不奇怪地想到，关于群的各种同构定理（定理I.5.6—I.5.12）经过必要的修改，对于模也是成立的. 在证明的每一步中，我们只需检查每个子群或同态事实上均是子

模或模同态. 为方便起见，我们将这些结果列在下面。

定理1.7 如果R是环，$f: A\to B$是R-模同态，C是$\ker f$的子模，则存在唯一的R-模同态$\bar{f}: A/C\to B$，使得对于每个$a\in A$，$\bar{f}(a+C)=f(a)$。其次，$\mathrm{Im}\,\bar{f}=\mathrm{Im}f$，$\ker\bar{f}=\ker f/C$。最后，$\bar{f}$是$R$-模同构$\Longleftrightarrow f$是$R$-模满同态并且$C=\ker f$。特别地，$A/\ker f\cong\mathrm{Im}f$。

证明见定理I.5.6.和系I.5.7. ∎

系1.8 如果R是环，A'和B'分别是R-模A和B的子模，$f: A\to B$是R-模同态，并且$f(A')\subset B'$，则f诱导出一个R-模同态$\bar{f}: A/A'\to B/B'$，$a+A'\longmapsto f(a)+B'$。进而，$\bar{f}$是R-模同构$\Longleftrightarrow\mathrm{Im}f+B'=B$并且$f^{-1}(B')\subset A'$。特别地，如果$f$是满同态并且$f(A')=B'$，$\ker f\subset A'$，则$\bar{f}$是$R$-模同构。

证明见系I.5.8。∎

定理1.9 设B和C是环R上模A的子模。

(i) 存在R-模同构$B/(B\cap C)\cong(B+C)/C$。

(ii) 如果$C\subset B$，则B/C是A/C的子模，并且有R-模同构$(A/C)/(B/C)\cong A/B$。

证明见系I.5.9和I.5.10。∎

定理1.10 如果R是环，B是R-模A的子模，则在集合$\{A$的子模$C\mid C\supset B\}$和集合$\{A/B$的全部子模$\}$之间存在着一一对应：$C\longmapsto C/B$。从而A/B的每个子模均有形式C/B，其中C是A的一个子模，使得$C\supset B$。

证明见定理I.5.11和系I.5.12. ∎

下面我们证明在R-模范畴中，积和余积是永远存在的。

定理1.11 设R是环，$\{A_i \mid i\in I\}$是非空R-模族。$\prod_{i\in I} A_i$是 Abel群A_i的直积，$\sum_{i\in I} A_i$是Abel群A_i的直和。则

(i) $\prod_{i\in I} A_i$是R-模，其中R的作用为：$r\{a_i\}=\{ra_i\}$。

(ii) $\sum_{i\in I} A_i$是$\prod_{i\in I} A_i$的子模。

(iii) 对于每个$k\in I$，正则射影π_k：$\Pi A_i \to A_k$（定理I.8.1）是R-模满同态。

(iv) 对于每个$k\in I$，正则嵌入ι_k：$A_k \to \Sigma A_i$（定理I.8.4)是R-模单同态。

证明作为练习。 ∎

$\prod_{i\in I} A_i$叫作R-模族$\{A_i \mid i\in I\}$的（外）直积，而$\sum_{i\in I} A_i$叫作它的（外）直和。如果下标集合是有限的，例如$I=\{1, 2, \cdots, n\}$，则直积和直和是一致的，并且记成$A_1\oplus A_2\oplus\cdots\oplus A_n$。映射$\pi_k$和$\iota_k$分别称作正则射影和正则嵌入。

定理1.12 如果R是环，$\{A_i \mid i\in I\}$是R-模族，C是R-模，$\{\varphi_i: C\to A_i \mid i\in I\}$是一族$R$-模同态，则存在唯一的$R$-模同态$\varphi$：$C\to \prod_{i\in I} A_i$，使得对每个$i\in I$，$\pi_i\varphi=\varphi_i$。并且不计同构$\prod_{i\in I} A_i$由此性质所唯一决定。换句话说，$\prod_{i\in I} A_i$是$R$-模范畴中的积。

证明 由定理I.8.2可知存在唯一的群同态φ：$C\to \prod_i A_i$，

$\varphi(c)=\{\varphi_i(c)\}_{i\in I}$具有所需性质。由于每个$\varphi_i$均是$R$-模同态，从而$\varphi(rc)=\{\varphi_i(rc)\}_{i\in I}=\{r\varphi_i(c)\}_{i\in I}=r\{\varphi_i(c)\}_{i\in I}=r\varphi(c)$，即$\varphi$也是$R$-模同态，因此$\Pi A_i$是$R$-模范畴中的积（定义I.7.2.）。于是由定理I.7.3可知它不计同构是唯一决定的。∎

定理1.13 如果R是环，$\{A_i\mid i\in I\}$是R-模族，D是R-模，$\{\psi_i: A_i\to D\mid i\in I\}$是一族$R$-模同态，则存在唯一的$R$-模同态$\psi$：$\sum_{i\in I}A_i\to D$，使得对于每个$i\in I$，$\psi\iota_i=\psi_i$。$\sum_{i\in I}A_i$不计同构由此性质所唯一决定。换句话说，$\sum_{i\in I}A_i$是$R$-模范畴中的余积。

证明 由定理I.8.5可知存在唯一的Abel群同态$\psi:\Sigma A_i\to D$，它具有所需性质，其中ψ由$\psi(\{a_i\})=\sum_i\psi_i(a_i)$给出，而求和是遍历有限下标集合$\{i\mid a_i\neq 0\}$。不难看出$\psi$是$R$-模同态，从而$\Sigma A_i$是$R$-模范畴中的余积（定义I.7.4），于是由定理I.7.5可知它不计同构是唯一决定的。∎

由于直和经常出现，所以需要对它作进一步的刻划。首先我们注意，如果f和g都是从R-模A到R-模B的R-模同态，则由$a\longmapsto f(a)+g(a)$给出的映射$f+g: A\to B$也是R-模同态。不难验证，所有R-模同态$A\to B$组成的集合$\mathrm{Hom}_R(A, B)$对于上述加法是Abel群（习题7）。此外，模同态的加法对于函数合成运算是有分配律的，即：

$$h(f+g)=hf+hg,\quad (f+g)k=fk+gk,$$

其中$f, g: A\to B$，$h: B\to C$，$k: D\to A$。

定理1.14 设R是环，A，A_1，…，A_n为R-模。则$A\cong A_1\oplus$

$A_2 \oplus \cdots \oplus A_n \Longleftrightarrow$对于每个$1 \leqslant i \leqslant n$，均存在$R$-模同态$\pi_i: A \to A_i$和$\iota_i: A_i \to A$，使得

(i) $\pi_i \iota_i = 1_{A_i}$ $(1 \leqslant i \leqslant n)$；

(ii) $\pi_j \iota_i = 0$ (如果$i \neq j$)；

(iii) $\iota_1 \pi_1 + \iota_2 \pi_2 + \cdots + \iota_n \pi_n = 1_A$。

证明 ($\Longrightarrow$) 如果A是模$A_1 \oplus A_2 \oplus \cdots \oplus A_n$，则正则嵌入$\iota_i$和正则射影$\pi_i$满足(i)－(iii)，读者很容易证明它们。同样地，如果$A \cong A_1 \oplus A_2 \oplus \cdots \oplus A_n$并且同构为$f$：$A \cong A_1 \oplus A_2 \oplus \cdots \oplus A_n$，则同态$\pi_i f$：$A \to A_i$和$f^{-1}\iota_i$：$A_i \to A$满足(i)－(iii)。

($\Longleftarrow$) 设 π_i：$A \to A_i$ 和 ι_i：$A_i \to A$ $(1 \leqslant i \leqslant n)$ 满足 (i)－(iii)。以π'_i：$A_1 \oplus \cdots \oplus A_n \to A_i$和$\iota'_i$：$A_i \to A_1 \oplus \cdots \oplus A_n$分别表示正则射影和正则嵌入。令$\varphi$：$A_1 \oplus \cdots \oplus A_n \to A$为$\varphi = \iota_1 \pi'_1 + \iota_2 \pi'_2 + \cdots + \iota_n \pi'_n$，$\psi$：$A \to A_1 \oplus \cdots \oplus A_n$为$\psi = \iota'_1 \pi_1 + \iota'_2 \pi_2 + \cdots + \iota'_n \pi_n$。则

$$\varphi\psi = \Big(\sum_{i=1}^{n} \iota_i \pi'_i\Big)\Big(\sum_{j=1}^{n} \iota'_j \pi_j\Big) = \sum_{i=1}^{n}\sum_{j=1}^{n} \iota_i \pi'_i \iota'_j \pi_j$$

$$= \sum_{i=1}^{n} \iota_i \pi'_i \iota'_i \pi_i = \sum_{i=1}^{n} \iota_i 1_{A_i} \pi_i = \sum_{i=1}^{n} \iota_i \pi_i = 1_A。$$

类似地，$\psi\varphi = \sum_{i=1}^{n}\sum_{j=1}^{n} \iota'_i \pi_i \iota_j \pi'_j = \sum_{i=1}^{n} \iota'_i \pi'_i = 1_{A_1 \oplus \cdots \oplus A_n}$ 于是由定理I.2.3可知φ是同构。∎

定理1.15 设R是环，$\{A_i \mid i \in I\}$是R-模A的一族子模，并且

(i) A是族$\{A_i \mid i \in I\}$之和；

(ii) 对于每个$k \in I$均有$A_k \cap A_k^* = 0$，其中A_k^*是族$\{A_i \mid i \neq k\}$之和。

则存在同构$A \cong \sum_{i \in I} A_i$。

证明作为练习。见定理I.8.6。■

模A叫作是它的一族子模$\{A_i \mid i\in I\}$的(内)直和，是指A和$\{A_i\}$满足定理1.15中的假设条件。与群范畴中一样，内直和与外直和有不同之处。如果模A是模A_i的内直和，则由定义可知每个A_i实际上都是A的子模，而A只是同构于外直和$\sum_{i\in I} A_i$。但是外直和$\sum_{i\in I} A_i$不包含模A_i，而只是包含一个与A_i同构的子模（即是$l_i(A_i)$，见定理1.11和习题I.8.10）。由于这个区别在实用中是不重要的，在课文中清楚的时候，我们略去修饰词“内”和“外”，而使用下面的记号。

记号：我们以$A=\sum_{i\in I} A_i$表示模A是它的子模族$\{A_i \mid i\in I\}$的内直和。

定义1.16 一对模同态$A\xrightarrow{f} B\xrightarrow{g}C$叫作在$B$处正合，是指$\mathrm{Im}f=\mathrm{Ker}g$。模同态有限序列$A_0\xrightarrow{f_1}A_1\xrightarrow{f_2}A_2\xrightarrow{f_3}\cdots\xrightarrow{f_{n-1}}A_{n-1}\xrightarrow{f_n}A_n$叫作正合的，是指$\mathrm{Im}f_i=\mathrm{Ker}f_{i+1}$ $(1\leqslant i\leqslant n-1)$。模同态无限序列$\cdots\xrightarrow{f_{i-1}}A_{i-1}\xrightarrow{f_i}A_i\xrightarrow{f_{i+1}}A_{i+1}\xrightarrow{f_{i+2}}\cdots$叫作正合的，是指对每个$i\in\mathbb{Z}$，$\mathrm{Im}f_i=\mathrm{Ker}f_{i+1}$。

有时为了方便，我们采用不够确切的语言，即将一个模同态的正合序列称作模的正合序列。

例 首先注意，对于任意模A，存在唯一的模同态$0\longrightarrow A$和$A\longrightarrow 0$。如果A和B是任意两个模，则序列$0\longrightarrow A\xrightarrow{\iota} A\oplus B\xrightarrow{\pi}B\longrightarrow 0$和$0\longrightarrow B\xrightarrow{\iota} A\oplus B\xrightarrow{\pi}A\longrightarrow 0$是正合的，其中$\iota$和

π分别是正则嵌入和正则射影。类似地，如果C是D的子模，则序列 $0\longrightarrow C\xrightarrow{i} D\xrightarrow{p}D/C\longrightarrow 0$ 是正合的，其中i是包含映射，p是正则满同态。如果f：$A\longrightarrow B$是模同态，则$A/\mathrm{Ker}f$和$B/\mathrm{Im}f$分别叫作f的余象和余核，并且分别表示成 $\mathrm{Coim}f$ 和 $\mathrm{Coker}f$。下面三个序列均是正合的：$0\longrightarrow \mathrm{Ker}f\longrightarrow A\longrightarrow \mathrm{Coim}f\longrightarrow 0$，$0\longrightarrow \mathrm{Im}f\longrightarrow B\longrightarrow \mathrm{Coker}f\longrightarrow 0$，$0\longrightarrow \mathrm{Ker}f\longrightarrow A\xrightarrow{f}B\longrightarrow \mathrm{Coker}f\longrightarrow 0$，其中未标出的映射都是显然的包含映射或者射影。

注记：$0\longrightarrow A\xrightarrow{f}B$ 是模同态正合序列$\Longleftrightarrow f$ 是模的单同态。类似地，$B\xrightarrow{g}C\longrightarrow 0$ 是正合的$\Longleftrightarrow g$是模的满同态。如果 $A\xrightarrow{f} B\xrightarrow{g}C$是正合的，则$gf=0$。最后，如果$A\xrightarrow{f} B\xrightarrow{g} C\longrightarrow 0$是正合的，则$\mathrm{Coker}f=B/\mathrm{Im}f=B/\mathrm{Ker}g=\mathrm{Coim}g\cong C$。形如$0\longrightarrow A\longrightarrow B\longrightarrow C\longrightarrow 0$ 的正合序列叫作短正合序列。注意这时f为单同态而g为满同态。以上所作的注记表明，一个短正合序列不过是提供另一种方式来表达B的一个子模（$A\cong\mathrm{Im}f$）和它的商模（$B/\mathrm{Im}f=B/\mathrm{Ker}g\cong C$）。

引理1.17 设R是环，并且

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0
\end{array}$$

是R-模与R-模同态组成的交换图表，并且两行均是短正合序列。则

(i) α和γ是单同态$\Rightarrow\beta$是单同态；

(ii) α和γ是满同态$\Rightarrow\beta$是满同态；

(iii) α和γ是同构$\Rightarrow\beta$是同构。

证明 (i) 设 $b\in B$并且$\beta(b)=0$. 我们需要证明$b=0$. 由图表的交换性，可知

$$\gamma g(b)=g'\beta(b)=g'(0)=0.$$

但是γ是单同态，从而$g(b)=0$. 由图表的上一行在B处的正合性，我们有 $b\in\mathrm{Ker}g=\mathrm{Im}f$. 假定 $b=f(a)$，$a\in A$. 又由图表的交换性，我们有

$$f'\alpha(a)=\beta f(a)=\beta(b)=0.$$

由下一行在 A' 处的正合性知f' 为单同态(定理 I.2.3(i))，从而$\alpha(a)=0$. 但是α为单同态，于是$a=0$. 从而$b=f(a)=f(0)=0$. 所以β是单同态.

(ii) 设$b'\in B'$，则$g'(b')\in C'$. 由于γ是满同态，从而有 $c\in C$，使得$g'(b')=\gamma(c)$. 从上一行在 c 处的正合性可知g是满同态. 于是有$b\in B$，使得$c=g(b)$. 由图表的交换性我们有

$$g'\beta(b)=\gamma g(b)=\gamma(c)=g'(b').$$

从而 $g'(\beta(b)-b')=0$，由正合性给出$\beta(b)-b'\in\mathrm{Ker}g'=\mathrm{Im}f'$，设 $f'(a')=\beta(b)-b'$, $a'\in A'$. 由于α是满同态，从而有$a\in A$，使得$a'=\alpha(a)$. 考虑$b-f(a)\in B$，我们有

$$\beta(b-f(a))=\beta(b)-\beta f(a).$$

由图表的交换性，$\beta f(a)=f'\alpha(a)=f'(a')=\beta(b)-b'$. 从而

$$\beta(b-f(a))=\beta(b)-\beta f(b)=\beta(b)-(\beta(b)-b')=b'.$$

从而β是满同态.

(iii) 是(i)和(ii)的直接推论. ∎

两个短正合序列叫作同构的，是指存在下面形式的模同态交换图表：

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0
\end{array}$$

并且f,g和h都是同构。在这种情形下，不难证明图表

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \uparrow{\scriptstyle f^{-1}} & & \uparrow{\scriptstyle g^{-1}} & & \uparrow{\scriptstyle h^{-1}} & & \\ 0 & \to & A' & \to & B' & \to & C' & \to & 0 \end{array}$$

也是交换的(其中两行上的映射与前一交换图表相同)。事实上，短正合序列的同构是等价关系(习题14)。

定理1.18 设R是环，$0\longrightarrow A_1\xrightarrow{f}B\xrightarrow{g}A_2\longrightarrow 0$是$R$-模同态的短正合序列，则下面三个条件是彼此等价的。

(i) 存在R-模同态h：$A_2\to B$，使得$gh=1_{A_2}$；

(ii) 存在R-模同态k：$B\to A_1$，使得$kf=1_{A_1}$；

(iii) 所给的序列同构于短正合序列$0\to A_1\xrightarrow{\iota_1}A_1\oplus A_2\xrightarrow{\pi_2}A_2\to 0$，并且从$A_1$到$A_1$和从$A_2$到$A_2$的垂直同构均是恒等映射。特别地，$B\cong A_1\oplus A_2$。

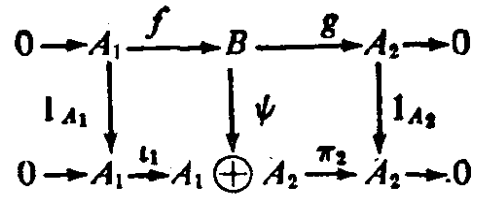
满足定理1.18中几个等价条件的短正合序列叫作分裂(split)的正合序列。

证明概要 (i)⇒(iii)：按照定理1.13，同态f和h诱导出模同态φ：$A_1\oplus A_2\to B$，$(a_1,a_2)\longmapsto f(a_1)+h(a_2)$。验证图表

$$\begin{array}{ccccccccc} 0 & \to & A_1 & \xrightarrow{\iota_1} & A_1\oplus A_2 & \xrightarrow{\pi_2} & A_2 & \to & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ 0 & \to & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \to & 0 \end{array}$$

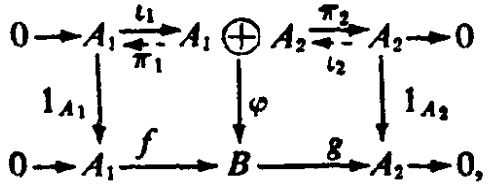
是交换的(利用$gf=0$和$gh=1_{A_2}$)。由引理1.17可知φ是同构。

(ii)⇒(iii)：图表



是交换的，其中ψ是由$\psi(b)=(k(b),\ g(b))$给出的模同态（见定理1.12）。由引理1.17可知ψ是同构。

(iii)⇒(i),(ii)给了交换图表



其中两行均是正合的并且φ是同构。定义$h:\ A_2\to B$为$\varphi\iota_2$，$k:\ B\to A_1$为$\pi_1\varphi^{-1}$。利用图表的交换性以及$\pi_i\iota_i=1_{A_i}$和$\varphi^{-1}\varphi=1_{A_1\oplus A_2}$可证$kf=1_{A_1}$和$gh=1_{A_2}$。 ∎

习　题

注：R是环

1. 如果A是Abel群，n是正整数，使得对每个$n\in A$均有$na=0$，则A是幺作用Z_n-模。其中Z_n在A上的作用为$\overline{k}a=ka$，这里$k\in\mathbf{Z}$，而$k\longmapsto\overline{k}\in Z_n$，$\mathbf{Z}\to Z_n$是正则射影。

2. 设$f:\ A\to B$是R-模同态。

   (a) f是单同态⟺对于每一对R-模同态$g,h:\ D\to A$，如果$fg=fh$，则必然$g=h$。

   〔提示：为证(⟸)，令$D=\mathrm{Ker}f$，取g为包含映射而h为零映射。〕

   (b) f是满同态⟺对于每一对R-模同态$k,\ t:\ B\to C$，如果$kf=tf$，则必然$k=t$。

〔提示：为证($\Longleftarrow$)，令k是正则满同态$B\to B/\mathrm{Im}f$而t为零映射.〕

3. 设I是环R的左理想，A是R-模.

(a) 如果S是A的非空子集合，则 $IS=\left\{\sum_{i=1}^{n} r_i a_i \mid n\in \mathbf{N}^*;\ r_i\in I,\ a_i\in S\right\}$是$A$的子模。注意如果$S=\{a\}$，则$IS=Ia=\{ra\mid r\in I\}$.

(b) 如果I是双侧理想，则A/IA是R/I-模，其中 R/I的作用为$(r+I)(a+IA)=ra+IA$.

4. 如果R是含幺环，则每个幺作用循环R-模均同构于形如R/J的R-模，其中J是R的一个左理想.

5. 如果R是含幺环，非零幺作用R-模叫作是单的，是指它只有两个子模：0和A.

(a) 每个单R-模都是循环模.

(b) 如果A是单R-模，则A 的每个R-模自同态或者是零映射，或者是同构.

6. 一个有限生成R-模作为Abel群不一定是有限生成的〔提示：习题 II.1.10〕.

7. (a) 如果A和B是R-模，则全体R-模同态$A\to B$所构成的集合$\mathrm{Hom}_R(A,B)$是Abel群，其中$f+g$定义为 $(f+g)(a)=f(a)+g(a)\in B(\forall a\in A)$. 幺元素是零映射.

(b) $\mathrm{Hom}_R(A,A)$ 是含幺环，其中乘法为函数的合成. 这称作A的自同态环.

(c) A 是左 $\mathrm{Hom}_R(A,A)$-模，其中 fa 定义为 $fa=f(a)$ $(a\in A,\ f\in \mathrm{Hom}_R(A,A))$.

8. 证明定理I.8.10和系I.8.11对于R-模也有类似的命题.

9. 如果f：$A\to A$是R-模同态，并且$ff=f$，则$A=\mathrm{Ker}f\oplus\mathrm{Im}f$.

10. 设$A,A_1,\cdots,A_n$是R-模. 则$A\cong A_1\oplus\cdots\oplus A_n\Longleftrightarrow$对于每个$1\leqslant i\leqslant n$，均存在$R$-模同态$\varphi_i$：$A\to A$，使得$\mathrm{Im}\varphi_i\cong A_i$，$\varphi_i\varphi_j=0$（当$i\neq j$时），并且$\varphi_1+\varphi_2+\cdots+\varphi_n=1_A$.〔提示：如果$A\cong A_1\oplus\cdots\oplus A_n$，令$\pi_i$，$\iota_i$如定理

1.14中所示，然后取$\varphi_i=\iota_i\pi_i$。反之，给了$\{\varphi_i\}$，证明$\varphi_i\varphi_i=\varphi_i$。令$\psi_i=\varphi_i|\mathrm{Im}\varphi_i$：$\mathrm{Im}\varphi_i\to A$，在定理1.14中将$A, A_i, \pi_i, \iota_i$分别取成$A, \mathrm{Im}\varphi_i, \varphi_i$和$\psi_i$即可。〕

11. (*a*) 如果A是交换环R上的模，$a\in A$，则$\mathscr{O}_a=\{r\in R|ra=0\}$是$R$的理想，如果$\mathscr{O}_a\neq 0$，称$a$是$A$的扭元素。

(*b*) 如果R是整环，则A中扭元素全体组成的集合$T(A)$是A的子模（称作扭子模）。

(*c*) 求证若交换环R不是整环，则(*b*)可能不成立。

在(*d*)－(*f*)中R是整环。

(*d*) 如果f：$A\to B$是R-模同态，则$f(T(A))\subset T(B)$。从而f在$T(A)$的限制f_T是R-模同态$T(A)\to T(B)$。

(*e*) 如果$0\to A\xrightarrow{f}B\xrightarrow{g}C$是$R$-模正合序列，则$0\to T(A)\xrightarrow{f_T}T(B)\xrightarrow{g_T}T(C)$也是$R$-模正合序列。

(*f*) 如果g：$B\to C$是R-模满同态，则g_T：$T(B)\to T(C)$不必为满同态。〔提示：考虑Abel群。〕

12. (五项引理) 令

$$\begin{array}{ccccccccc} A_1 & \to & A_2 & \to & A_3 & \to & A_4 & \to & A_5 \\ \downarrow{\scriptstyle\alpha_1} & & \downarrow{\scriptstyle\alpha_2} & & \downarrow{\scriptstyle\alpha_3} & & \downarrow{\scriptstyle\alpha_4} & & \downarrow{\scriptstyle\alpha_5} \\ B_1 & \to & B_2 & \to & B_3 & \to & B_4 & \to & B_5 \end{array}$$

是R-模和R-模同态的交换图表，并且两行都是正合的。求证：

(*a*) α_1为满同态并且α_2和α_4是单同态$\Longrightarrow\alpha_3$是单同态；

(*b*) α_5是单同态并且α_2和α_4是满同态$\Longrightarrow\alpha_3$是满同态。

13. (*a*) 如果$0\to A\to B\xrightarrow{f}C\to 0$和$0\to C\xrightarrow{g}D\to E\to 0$均是模的短正合序列，则$0\to A\to B\xrightarrow{gf}D\to E\to 0$是正合序列。

(*b*) 求证每个正合序列都可以象(*a*)中那样由一些适当的短正合序列黏接而成。

14. 证明短正合序列的同构是等价关系。

15. 如果f：$A\to B$和g：$B\to A$是R-模同态，使得$gf=1_A$，则$B=\mathrm{Im}f\oplus\mathrm{Ker}g$。

16. 设R是环，而R^{OP}是它的反环（习题III.1.7).如果A是左R-模，则A是右R^{OP}-模，其中对于$a\in A$，$r\in R^{OP}$，定义$ar=ra$（右边的$r\in R$)。类似地，如果A是右R-模，则它也是左R^{OP}-模。

17. (a) 如果R为含幺环而A是R-模，则A有子模B和C，使得B为幺作用模，$RC=0$并且$A=B\oplus C$。〔提示：令$B=\{1_Ra\mid a\in A\}$，$C=\{a\in A_1\mid 1_Ra=0\}$。并注意对每个$a\in A$，$a-1_Ra\in C$。〕

(b) 设A_1是另一个R-模，并且$A_1=B_1\oplus C_1$(其中B_1为幺作用模而$RC_1=0$)。如果f：$A\to A_1$是R-模同态，则$f(B)\subset B_1$并且$f(C)\subset C_1$。

(c) 如果(b)中的映射f是满同态(或者同构)，则$f|B$：$B\to B_1$和$f|C$：$C\to C_1$也是满同态(或者同构)。

18. 设R是不含幺的环，将R嵌入含幺环S中。并且S的特征是零(见定理III.1.10的证明)。将R等同于它在S中的象。

(a) 求证S中每个元素可以唯一地表示成形式$r1_S+n1_S$($r\in R$，$n\in\mathbf{Z}$)。

(b) 如果A是R-模，$a\in A$，求证存在唯一的R-模同态f：$S\to A$，使得$f(1_S)=a$。〔提示：令$f(r1_S+n1_S)=ra+na$。〕

2. 自由模和向量空间

在这一节中我们研究某个环上的模范畴中的自由对象，自由模在数学许多领域中都有广泛的应用，而体上的向量空间是它的最重要的例子（定理2.4)。自由Abel群是自由模的一个特殊情形(即是$\mathbf{Z}$-模)，它可以作为本节第一部分的样板。本节其余部分是讨论自由模的维数(或者秩)（定理2.6—2.12)，并研究向量空间

维数的一些特殊性质(定理和系2.13—2.16)。

R-模 A的子集合X叫作线性无关的，是指对于两两不同的元素$x_1,\cdots, x_n\in X$和$r_i\in R$,

$r_1x_1+r_2x_2+\cdots+r_nx_n=0\Rightarrow$对于每个$i, r_i=0$。不线性无关的集合叫作线性相关的。如果$A$作为$R$-模由集合$Y$生成，我们就称$Y$张成$A$。如果$R$是含幺环而$A$是幺作用模，则$Y$张成$A\Longleftrightarrow A$中每个元素均可以写成线性组合的形式：$r_1y_1+r_2y_2+\cdots+r_ny_n$，其中$r_i\in R$，$y_i\in Y$，见定理1.5。$A$的一个线性无关子集合如果张成$A$，它就叫作 A的一组基。注意空集合是线性无关的，并且是零模的基(见定义1.4)。

定理2.1 设R是含幺环。则关于幺作用R-模F的下列诸条件是彼此等价的：

(i) F有一组非空的基；

(ii) F是一族循环R-模的内直和，此族中每个循环R-模均同构于左R-模R；

(iii) 作为R-模F同构于一些左R-模R的直和；

(iv) 存在非空集合X和函数ι：$X\to F$ 具有下面的性质：给了任意一个幺作用R-模 A和函数 f：$X\to A$，均有唯一的 R-模同态 $\bar{f}$：$F\to A$，使得 $\bar{f}\iota=f$。换句话说，F是幺作用 R-模范畴中的自由对象。

这个定理的证明在下面。含幺环 R上的幺作用模 F 如果满足定理2.1中的等价条件，就叫作集合 X上的自由R-模。根据定理2.1(iv)，F是幺作用左R-模范畴中的自由对象。但是这样的 F不一定是全体R-模的范畴中的自由对象(习题15)。按照定义，零模是空集合上的自由模。

也可以在全体左R-模组成的范畴中定义自由模，其中R为任意的环(可能没有幺元素)，见习题2。这样一个自由对象不同构于一些R的直和，即使在R有幺元素时也会如此(习题2)。在下面仔细作了注解的一些情形中，某些结果在全体左R-模的范畴中对于自由模也是对的。但是除非特别指明，“自由模”一词总是指在定理2.1意义下的幺作用自由模。

定理2.1的证明概要 (i)⇒(ii)：设X是F的一组基，$x\in X$。由定理1.5可知映射$R\to Rx$，$r\longmapsto rx$是R-模满同态。如果$rx=0$，由线性无关性可知$r=0$。从而这个映射是单同态，于是有左R-模同构$R\cong Rx$。证明F是循环模$Rx(x\in X)$的内直和。

(ii)⇒(iii)：定理1.15和习题1.8。

(iii)⇒(i)：设$F\cong\sum R$，并且诸分量R以X作为下标集合。对于每个$x\in X$，令$\theta_x=\{r_i\}\in\sum R$，其中当$i\neq x$时$r_i=0$，而$r_x=1_R$。验证$\{\theta_x|x\in X\}$是$\sum R$的一组基，再用同构$F\cong\sum R$即给出$F$的一组基。

(i)⇒(iv)：令X是F的一组基，ι：$X\to F$是包含映射。假如我们给了一个映射f：$X\to A$。如果$u\in F$，则$u=\sum_{i=1}^{n}r_ix_i(r_i\in R,\ x_i\in X)$，这是因为$X$张成$F$。如果$u=\sum_{i=1}^{n}s_ix_i$ $(s_i\in R)$，则$\sum_i(r_i-s_i)x_i=0$，由线性无关性可知对每个i，$r_i=s_i$。从而可以定义映射

$$\bar{f}:\ F\to A,\ \bar{f}(u)=\bar{f}\left(\sum_{i=1}^{n}r_ix_i\right)=\sum_{i=1}^{n}r_if(x_i),$$

并且$\bar{f}\iota=f$。验证$\bar{f}$是R-模同态。由于X生成F，每个R-模同态$F\to A$都由它在X上的作用唯一决定。因此若g：$F\to A$是R-模同态并且$g\iota=f$，则对每个$x\in X$，$g(x)=g(\iota(x))=f(x)=\bar{f}(x)$，从而

$g=\bar{f}$，即$\bar{f}$是唯一的。于是由定义1.7.7可知在幺作用R-模范畴中F是集合X上的自由对象。

(iv)⇒(iii)：给了 ι：$X\to F$，构作直和 ΣR，其中对于每个$x\in X$均对应一个直和分量R。令$Y=\{\theta_x|x\in X\}$是证明(iii)⇒(i)时所述的(幺作用)R-模ΣR的那组基。从 (iii)⇒(i)⇒(iv)的证明可知ΣR 是 R-模范畴中集合Y上的自由对象(对于包含映射 $Y\to\Sigma R$)。由于$|X|=|Y|$，从定理 I.7.8的证明可知存在 R-模同构 f：$F\cong\Sigma R$，使得　　$f(\iota(X))=Y$。 ∎

注记：(*a*) 如果F是集合X上的自由R-模(ι：$X\to F$)，则从定理2.1中(iv)⇒(iii)的证明可知$\iota(X)$实际上是F的一组基。

(*b*) 反之，由定理2.1中 (i)⇒(iv) 的证明可知。如果X是含幺环R上的幺作用模F的一组基，则F对于包含映射ι：$X\to F$是X上的自由模。

(*c*) 如果X是任一非空集合而R是含幺环，则从定理2.1的证明过程可以看到如何构作集合X上的一个自由R-模。简言之，令F是直和ΣR,其中分量R以X为下标集合。使用该证明中的记号，$\{\theta_x|x\in X\}$是F的一组基，从而 $F=\sum_{x\in X}R\theta_x$。由于映射 ι：$X\to F$，$X\longmapsto\theta_x$是单射，不难看出，F在定理2.1条件(iv)的意义下是X上的自由模。在这种情形下，我们通常将X等同于它在ι之下的象，从而用x来代替θ_x，于是$X\subset F$。采用这种记号，则 $F=\sum_{x\in X}R\theta_x$ 可以写成$\sum_{x\in X}Rx$，从而F中的元素有形式 $r_1x_1+\cdots+r_nx_n(r_i\in R,\ x_i\in X)$。特别地，$X=\iota(X)$ 是F的一组基。

(*d*) 习题2中要证明，对于任意环R(可能没有幺元素)，全体

R-模组成的范畴中也存在一给定集合上的自由模。

系2.2 （含幺）环R上的每个（幺作用）模A均是一个自由R-模F的同态象。如果A是有限生成的，则F也可以取成是有限生成的。

注记：如果将系2.2的括号中的词去掉，并且“自由模”指的是任意环上全体左模组成的范畴中的自由模（由习题2所定义的），则系2.2和它的证明仍旧正确。

系2.2的证明概要 设X是A的生成元集合，F是集合X上的自由R-模。则包含映射$X\to A$诱导出R-模同态$\bar{f}$：$F\to A$，使得 $X\subset \mathrm{Im}\,\bar{f}$（定理2.1(iv)）。由于$X$生成$A$，我们必然有$\mathrm{Im}\bar{f}=A$。 ∎

注记：与自由Abel群的情形不同，任意环上的自由模的子模不一定是自由的。例如$\{0, 2, 4\}$是Z_6的子模，但显然不是自由Z_6-模。比较定理II. 1.6和下面的定理6.1。

体 D 上的向量空间（定义1）是很重要的，这有许多方面的原因。例如，D 上的每个向量空间事实上都是自由D-模。为了证明这一点我们需要

引理2.3 体D上向量空间V的极大线性无关子集合X是 V 的一组基。

证明 设W是由集合X张成的V的子空间。由于X是线性无关的并且张成W，从而X是 W 的一组基。如果$W=V$则证毕。若不然，则存在非零元素$a\in V$，$a\notin W$。考虑集合$X\cup\{a\}$。如果$ra+r_1x_1+\cdots+r_nx_n=0$ $(r, r_i\in D, x_i\in X)$ 而 $r\neq 0$，则 $a=r^{-1}(ra)=-r^{-1}r_1x_1-\cdots r^{-1}r_nx_n\in W$，这就与$a$的选取相矛盾。从而$r=0$，而这又推出 $r_i=0$ $(1\leqslant i\leqslant n)$，这是因为 X 是线性无关的。从而

$X\cup\{a\}$也是V的线性无关子集合，而这又与X的极大性相矛盾。因此$W=V$。即X是一组基。∎

定理2.4 体D上的每个向量空间V都有基，从而是自由D-模。更一般的，V的每个线性无关子集合都包含在V的一组基中。

注记：定理2.4的逆也是对的。即：如果含幺环D上每个幺作用模都是自由模，则D是体(习题3.14)。

定理2.4的证明概要 第一个论断是第二个论断的直接推论，因为空集合是每个向量空间的线性无关子集合。现在我们假定X是V的任意线性无关子集合。令$\mathcal{S}=\{V$的线性无关子集合$C|C\supset X\}$。显然$X\in\mathcal{S}$，从而$\mathcal{S}\neq\phi$。集合$\mathcal{S}$中赋以集合论的包含序。如果$\{C_i|i\in I\}$是$\mathcal{S}$中的链，证明集合$C=\bigcup_{i\in I}C_i$也是线性无关的，从而是$\mathcal{S}$中的元素。C显然是链$\{C_i|i\in I\}$的上界。由Zorn引理，$\mathcal{S}$包含极大元B。B包含X并且是V的极大线性无关子集合。由引理2.3即知B是V的一组基。∎

定理2.5 如果V是体D上的向量空间，X是V的子集合并且张成V，则X包含V的一组基。

证明概要 令$\mathcal{S}$是X的全体线性无关子集合所组成的集合，并赋以包含序。由Zorn引理导致X存在极大线性无关子集合Y。X中每个元素均是Y中元素的线性组合（不然的话，就会象在引理2.3中那样构作出X的一个线性无关子集合真包含Y，这就与Y的极大性相矛盾）。由于X张成V，从而Y也张成V。于是Y是V的一组基。∎

对于自由Abel群($\mathbb{Z}$-模)，我们知道，自由$\mathbb{Z}$-模的任意两组

基具有同样的势（定理II.1.2）。不幸的是，对于任意含幺环上的自由模这是不成立的(习题13)。现在我们要证明：体上的向量空间和含幺交换环上的自由模均有这个性质。

定理2.6 设R为含幺环。F是自由R-模并且具有一组无限的基X，则F的每一组基都与X有同样的势。

证明 如果Y是F的另一组基，我们先证Y也是无限的。假如Y是有限的。由于Y生成F，并且Y中每个元素都是X中有限个元素的线性组合，从而存在X的一个有限子集合$\{x_1, \cdots, x_m\}$生成F。因为X是无限的，于是存在$x \in X - \{x_1, \cdots, x_m\}$。从而有$r_i \in R$，使得 $x = r_1x_1 + \cdots + r_mx_m$，而这与$X$的线性无关性相矛盾。于是$Y$是无限的。

令$K(Y)$是Y的全体有限子集合所构成的集合。定义映射

$f: X \to K(Y)$，$x \longmapsto \{y_1, \cdots, y_n\}$

其中 $x = r_1y_1 + \cdots + r_ny_n$，且对每个$i$，$r_i \neq 0$。由于$Y$是一组基，$\{y_i\}$是唯一确定的，从而$f$是可定义的函数（它不必是单射）。如果 $\mathrm{Im}f$ 有限，则$\bigcup_{S \in \mathrm{Im}f} S$是$Y$的有限子集合并且生成 X 从而也生成F，象上一段所证明的那样，这就与Y的线性无关性相矛盾。从而$\mathrm{Im}f$是无限的。

现在我们证明：对于每个$T \in \mathrm{Im}f \subset K(Y)$，$f^{-1}(T)$是$X$ 的有限子集合。如果$x \in f^{-1}(T)$，则x包含在由T生成的F的子模 F_T 之中，即$f^{-1}(T) \subset F_T$(见定理1.5)。由于T是有限的，并且每个$y \in T$均是X中有限个元素的线性组合，从而存在X的一个有限子集合S，使得$F_T \subset F_S$。因此$x \in f^{-1}(T)$ 导致$x \in F_S$，从而x 是 S 中元素的线性组合（定理1.5）。由于$x \in X$，$S \subset X$，这就推出$x \in S$,否则

便与X的线性无关性相矛盾。因此$f^{-1}(T)\subset S$，即$f^{-1}(T)$是有限的。

对于每个$T\in \mathrm{Im}f$，令$f^{-1}(T)=\{x_1,\cdots,x_n\}$，定义单射

$$g_T:\ f^{-1}(T)\to \mathrm{Im}f\times \boldsymbol{N},\ x_k\longmapsto (T,\ k)。$$

证明集合$f^{-1}(T)(T\in \mathrm{Im}f)$形成$X$的一个分拆。从而可以定义单射

$$X\to \mathrm{Im}f\times \boldsymbol{N},\ x\longmapsto g_T(x),\ 其中x\in f^{-1}(T)。$$

于是$|X|\leqslant|\mathrm{Im}f\times \boldsymbol{N}|$。由引论中的定义8.3，定理8.11和系8.13可知

$$\begin{aligned}|X|&\leqslant|\mathrm{Im}f\times \boldsymbol{N}|=|\mathrm{Im}f|\,\aleph_0\\&=|\mathrm{Im}f|\leqslant|K(Y)|=|Y|。\end{aligned}$$

在上述推理过程中交换X和Y的位置，可证$|Y|\leqslant|X|$。于是由Schroeder—Bernstein定理即知$|X|=|Y|$。■

定理2.7 如果V是体D上的向量空间，则V的任意两组基有相同的势。

证明 设X和Y是V的两组基。如果X或者Y是无限的，由定理2.6可知$|X|=|Y|$。以下设X和Y均是有限的。假定$X=\{x_1,\cdots,x_n\}$，$Y=\{y_1,\cdots,y_m\}$。因为X和Y都是基，从而有$r_i\in D$，使得$0\neq y_m=r_1x_1+\cdots+r_nx_n$。如果$r_k$是第一个非零系数，则$x_k=r_k^{-1}y_m-r_k^{-1}r_{k+1}x_{k+1}-\cdots-r_k^{-1}r_nx_n$。于是集合$X'=\{y_m,\ x_1,\ \cdots,\ x_{k-1},\ x_{k+1},\ \cdots,\ x_n\}$张成$V$(因为$X$张成$V$)。特别地，

$y_{m-1}=s_my_m+t_1x_1+\cdots+t_{k-1}x_{k-1}+t_{k+1}x_{k+1}+\cdots+t_nx_n$ $(s_m,\ t_i\in D)$。$\{t_i\}$不全为零(不然的话便有$y_{m-1}-s_my_m=0$，这就与Y的线性无关性相矛盾)。如果t_j是其中第一个不为零的，则x_j是

y_{m-1}，y_m 和 $\{x_i|i\neq j,\ k\}$ 的线性组合。从而集合 $\{y_{m-1},\ y_m\}\cup\{x_i|i\neq j,\ k\}$ 张成 V（因为 X' 张成 V）。特别地，y_{m-2} 是 y_{m-1}，y_m 和 $\{x_i|i\neq j,\ k\}$ 的线性组合。上面这种“填 y 去 x”过程可以重复下去，在第 k 步完成之后，我们得到由 y_m，y_{m-1}，…，y_{m-k+1} 和 $n-k$ 个 x_i 所组成的一个集合，并且此集合张成 V。如果 $n<m$，则第 n 步作完之后将得到“$\{y_m,\cdots,y_{m-n+1}\}$ 张成 V”的结论。由于 $m-n+1\geqslant 2$，从而 y_1 将会是 $y_m,\cdots,y_{m-n+1}$ 的线性组合，这就与 Y 的线性无关性相矛盾。从而必然有 $m\leqslant n$。交换 X 和 Y 的位置，类似的推理给出 $n\leqslant m$。从而 $m=n$。∎

定义2.8 设 R 是含幺环，如果对于每个自由 R-模 F，F 的任意两组基均有同样的势。我们便称 R 具有不变维数性质。而 F 的任意一组基的势叫作 F 在 R 上的维数（或者秩）。

定理2.7是说，体具有不变维数性质，我们遵照通常的作法，即对于体上的向量空间使用“维数”一词，而对其它环上的自由模则使用“秩”。体 D 上的向量空间 V 的维数表示成 $\dim_D V$。我们将在系2.12之后研究 $\dim_D V$ 的性质。2.9—2.12中的结果除了第IV.6节和VII.5节之外今后是不需要的。

命题2.9 设 E 和 F 均是环 R 上的自由模，而且 R 有不变维数性质。则 $E\cong F\Longleftrightarrow E$ 和 F 有相同的秩。

证明作为练习。见命题II.1.3。∎

引理2.10 设 R 是含幺环，$I(\neq R)$ 是 R 的理想，F 是自由 R-模，而 X 是 F 的一组基。$\pi:F\to F/IF$ 是正则满同态。则 F/IF 是自由 R/I-模，而 $\pi(X)$ 是 F/IF 的一组基，并且 $|\pi(X)|=|X|$。

(让我们回忆：$IF=\left\{\sum_{i=1}^{n} r_i a_i \mid r_i \in I,\ a_i \in F,\ n \in \boldsymbol{N}^+\right\}$，而$R/I$在$F/IF$上的作用为$(r+I)(a+IF)=ra+IF$(习题3))。

证明 如果$u+IF \in F/IF$，则 $u=\sum_{j=1}^{n} r_j x_j$，$r_j \in R$，$x_j \in X$，这是因为$u \in F$而X是F的一组基。从而$u+IF=\left(\sum_j r_j x_j\right)+IF=\sum_j (r_j x_j+IF)=\sum_j (r_j+I)(x_j+IF)=\sum_j (r_j+I)\pi(x_j)$，于是$\Pi(X)$生成$R/I$-模$F/IF$。另一方面，如果 $\sum_{k=1}^{m} (r_k+I)\pi(x_k)=0$，其中$r_k \in R$，$x_1,\cdots,x_m$为$X$中不同的元素，则 $0=\sum_k (r_k+I)\pi(x_k)=\sum_k (r_k+I)(x_k+IF)=\sum_k r_k x_k+IF$，从而$\sum_k r_k x_k \in IF$。于是$\sum_k r_k x_k=\sum_j s_j u_j$，其中$s_j \in I$，$u_j \in F$。由于每个$u_j$均是$X$中元素的线性组合而$I$是理想，从而$\sum_j s_j u_j$是$X$中元素的线性组合并且系数均属于$I$，从而$\sum_{k=1}^{m} r_k x_k=\sum_j s_j u_j=\sum_{t=1}^{d} c_t y_t$，其中$c_t \in I$，$y_t \in X$。由$X$的线性无关性导致(必要时重新加标号和插入一些项$ox_k$，$ox_t$)$m=d$，并且对每个$k$，$x_k=y_k$和$r_k=c_k$。于是在$R/I$中对于每个$k$，$r_k+I=0$，从而$\pi(X)$在$R/I$上是线性无关的。于是$F/IF$是自由$R/I$-模，并且$\pi(X)$是它的一组基(定理2.1)。最后，如果$x$，$x' \in X$，并且在$F/IF$中$\pi(x)=\pi(x')$，则$(1_R+I)\pi(x)-(1_R+I)\pi(x')=0$。如$x \neq x'$，则上述推理导致$1_R \in I$，而这与$I \neq R$相矛盾。因此$x=x'$，即映射 $\pi: X \to \pi(X)$ 是一一对应，从而 $|X|=|\pi(X)|$。 ∎

命题2.11 如果f：$R\to S$是含幺环的非零满同态，并且 S 有不变维数性质，则R也有不变维数性质.

证明 令$I=\mathrm{Ker}f$. 则$S\cong R/I$（系III.2.10）. 令X和Y均是自由R-模F的基，$\pi:F\to F/IF$是正则满同态. 由引理2.10可知 F/IF是自由R/I-模（从而也是自由S-模），并且 $\pi(X)$和$\pi(Y)$均是它的基，而且$|X|=|\pi(X)|$，$|Y|=|\pi(Y)|$. 由于 S 有不变维数性质，从而 $|\pi(X)|=|\pi(Y)|$. 于是$|X|=|Y|$，即 R也有不变维数性质. ∎

系2.12 如果 R 是一个以体作为同态象的含幺环，那么，R 具有不变维数的性质. 特别地，每一个含幺交换环具有不变维数的性质.

证明 第一个陈述从定理2.7和命题2.11得到. 如果R是含幺交换环，那么，R包含一个极大理想M（定理III.2.18）且R/M是一个域（定理III.2.20）. 于是第二个陈述是第一个陈述的特殊情况. ∎

现在让我们回到体上向量空间，即研究它的维数性质. 体 D 上的向量空间V叫做有限维的，是指$\dim_D V$是有限的.

定理2.13 设W是体D上向量空间V的子空间. 则

(i) $\dim_D W\leqslant\dim_D V$;

(ii) 如果$\dim_D W=\dim_D V$并且$\dim_D V$有限，则$W=V$;

(iii) $\dim_D V=\dim_D W+\dim_D(V/W)$.

证明概要 (i) 设Y是W的一组基. 根据定理 2.4 可知存在V的一组基X包含Y. 因此$\dim_D W=|Y|\leqslant|X|=\dim_D V$.

(ii) 如果$|Y|=|X|$ 而X是有限的，因为$Y\subset X$，从而必然Y

$=X$，于是$W=V$。

(iii) 我们要证$U=\{x\in W\mid x\in X-Y\}$是$V/W$的一组基。由此即可推出（由引论中定义8.3）$\dim_D V=|X|=|Y|+|X-Y|=|Y|+|U|=\dim_D W+\dim_D(V/W)$。如果$v\in V$，则$v=\sum_i r_i y_i+\sum_j s_j x_j$（$r_i$，$s_i\in D$，$y_i\in Y$，$x_j\in X-Y$），从而$v+W=\sum_j s_j(x_j+W)$。因此$U$张成$V/W$。如果$\sum_j r_j(x_j+W)=0$（$r_j\in D$，$x_j\in X-Y$），则$\sum_j r_j x_j\in W$，从而$\sum_j r_j x_j=\sum_k s_k y_k$（$s_k\in D$，$y_k\in Y$）。这就推出$r_j=0$，$s_k=0$（对每个$j$和$k$），因为否则就会与$X=Y\cup(X-Y)$的线性无关性相矛盾。因此$U$是线性无关的，并且$|U|=|X-Y|$。∎

系2.14 如果$f: V\to V'$是体D上向量空间之间的线性变换，则存在V的一组基X，使得$X\cap \mathrm{Ker}f$是$\mathrm{Ker}f$的一组基，并且$\{f(x)\mid f(x)\neq 0,\ x\in X\}$是$\mathrm{Im}f$的一组基。特别地，

$$\dim_D V=\dim_D(\mathrm{Ker}f)+\dim_D(Imf)。$$

证明概要 为证第一个论断，取$W=\ker f$，并且令Y和X如定理2.13的证明中所示。第二个论断由定理2.13(iii)推得，因为由定理1.7我们有$V/W\cong \mathrm{Im}f$。∎

系2.15 如果V和W均是体D上某向量空间的有限维子空间，则

$$\dim_D V+\dim_D W=\dim_D(V\cap W)+\dim_D(V+W)。$$

证明概要 令X是$V\cap W$的一组基，Y是V的一组(有限）基并

且包含X，Z是W的一组(有限)基并且包含X(定理2.4)。证明$X \cup (Y-X) \cup (Z-X)$是$V+W$的一组基。于是

$$\dim_D(V+W) = |X| + |Y-X| + |Z-X| = \dim_D(V \cap W) + (\dim_D V - \dim_D(V \cap W)) + (\dim_D W - \dim_D(V \cap W)). \blacksquare$$

让我们回忆：如果体R包含在体S之中，则S是R上的向量空间，并且rs($s \in S$，$r \in R$)是S中的乘积。下面一个定理在第V章研究域扩张时是需要的。

定理2.16 设R，S，T均是体并且$R \subset S \subset T$。则

$$\dim_R T = (\dim_S T)(\dim_R S).$$

此外，$\dim_R T$有限$\Longleftrightarrow$$\dim_S T$和$\dim_R S$均有限。

证明 设U是T在S上的一组基，V是S在R上的一组基。我们只需证明$\{vu \mid v \in V, u \in U\}$是$T$在$R$上的一组基。这是因为：由$U$在$S$上的线性无关性可知诸元素$vu$是两两不同的，从而$\dim_R T = |U| \cdot |V| = (\dim_S T) \cdot (\dim_R S)$。而定理中最后一个论断由下面事实直接推出：两个有限势的乘积仍是有限势，而无限势与有限势的乘积是无限势(引论中的定理8.11)。

如果$u \in T$，则$u = \sum_{i=1}^{n} s_i u_i$($s_i \in S$，$u_i \in U$)，这是因为$U$张成$S$-向量空间$T$。由于$S$是$R$-向量空间，从而每个$s_i$可以写成$s_i = \sum_{j=1}^{m_j} r_{ij} v_j$($r_{ij} \in R$，$v_j \in V$)，因此$u = \sum_i s_i u_i = \sum_i \left(\sum_j r_{ij} v_j \right) u_i = \sum_i \sum_j r_{ij} v_j u_i$。于是$\{vu \mid v \in V, u \in U\}$张成$R$-向量空间$T$。

假设$\sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij}(v_j u_i) = 0$ ($r_{ij} \in R$，$v_j \in V$，$u_i \in U$)。对于每

个i，令 $s_i=\sum_{j=1}^{m} r_{ij}v_j \in S$，则 $0=\sum_i \sum_j r_{ij}(v_j u_i)=\sum_i\Big(\sum_j r_{ij} v_j\Big)u_i=\sum_i s_i u_i$。由$U$在$S$上的线性无关性可知对每个 i，$0=s_i=\sum_j r_{ij}v_j$。又由V在R上的线性无关性可知对于每个i和j，$r_{ij}=0$。因此$\{vu \mid v\in V,\ u\in U\}$在$R$上是线性无关的，从而是一组基。∎

习　题

1. (*a*) 体R上的向量空间V中一个向量集合 $\{x_1, \cdots, x_n\}$ 是线性相关的$\Longleftrightarrow$存在某个x_k，它是前面一些$x_i(1\leqslant i<k)$的线性组合。

   (*b*) 如果 $\{x_1, x_2, x_3\}$ 是V 的线性无关子集合，则集合 $\{x_1+x_2, x_2+x_3, x_3+x_1\}$ 是线性无关的$\Longleftrightarrow$Char$R\neq 2$〔见定义III.1.8〕。

2. 设R是任意环(可能没有幺元素)，X 是非空集合。在本题中我们称 R-模F是X上的自由R-模，是指对于全体左R-模组成的范畴，F是X上的自由对象。于是由定义1.7.7，F是X上的自由R-模，是指存在函数 $\iota: X\to F$，使得对每个左R-模A和函数$f: X\to A$，均存在唯一的R-模同态$\bar{f}: F\to A$，满足$\bar{f}\iota=f$。

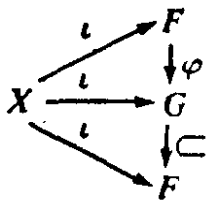
   (*a*) 设$\{X_i \mid i\in I\}$是一族两两非交的集合，并且对于每个$i\in I$，令F_i是x_i上的自由R-模(对于$\iota_i: X_i\to F_i$)。令$X=\bigcup_{i\in I} X_i$，$F=\sum_{i\in I} F_i$，而$\phi_i: F_i\to F$是正则嵌入。定义$\iota: X\to F$，$\iota(x)=\phi_i\iota_i(x)$ (对于$x\in X_i$)(由于$\{X_i\}$两两非交可知ι是可定义的)。证明F是X上的自由R-模。〔提示：定理1.13可能会有用处。〕

   (*b*) 设R是含幺环。并设Abel群$\mathbf{Z}$具有平凡的R- 模结构 (即对于每个$r\in R$，$m\in\mathbf{Z}$，$rm=0$)。于是$R\oplus\mathbf{Z}$也是R-模，其中$r(r', m)=(rr', 0)$(对于r，$r'\in R$，$m\in\mathbf{Z}$)。如果$X=\{t\}$是一元集合。令$\iota: X\to R\oplus\mathbf{Z}$是由$\iota(t)=(1_R, 1)$给出的映射。证明$R\oplus\mathbf{Z}$是$X$上的自由$R$-模。〔提示：

给了f：$X\to A$，令$A=B\oplus C$如习题1.17中所示，于是$f(t)=b+c$ ($b\in B$，$c\in C$)。定义$f(r,\ m)=rb+mc$。〕

(c) 如果R是任意环而X是任意集合，则存在X 上的自由模。〔提示：因为X是集合$\{t\}(t\in X)$的非交并，根据(a) 我们不妨假设X只有一个元素。如果R是含幺环，则利用(b)。如果R没有幺元素，象定理III.1.10的证明中所作的那样，将R嵌入含幺环S中并且S 的特征为零。利用习题1.18证明S是X上的自由R-模。〕

3. 设R是任意环(可能没有幺元素)，象习题2中那样，F 是集合X上的自由R-模(对于ι：$X\to F$)。求证$\iota(X)$是R- 模F的一个生成元集合。〔提示：令G是由$\iota(X)$生成的F的子模，利用“自由模” 的定义证明存在模同态φ，使得图表



是交换的。从而$\varphi=1_F$。〕

4. 设R是主理想整环，A是幺作用左R-模，$p\in R$是素元（即不可约元)。令$pA=\{pa\mid a\in A\}$，$A[p]=\{a\in A\mid pa=0\}$。则

(a) $R/(p)$是域(定理III.2.20和III.3.4)。

(b) pA和$A[p]$均是A的子模。

(c) A/pA是$R/(p)$上的向量空间，其中$(r+(p))(a+pA)=ra+pA$。

(d) $A[p]$是$R/(p)$上的向量空间，其中$(r+(p))a=ra$。

5. 设V是体D上的向量空间，S是V的全体子空间所组成的集合， 并赋以集合论的包含序。

(a) S是完备格(见引论中的习题7.2。V_1与V_2的上端和下端分别为V_1+V_2和$V_1\cap V_2$)。

(b) S是有补格，即对于每个$V_1\in S$，均存在$V_2\in S$，使得$V=V_1+V_2$并且$V_1\cap V_2=0$，从而$V=V_1\oplus V_2$。

(c) S是模格。即：如果V_1，V_2，$V_3\in S$并且$V_3\subset V_1$，则

$$V_1 \cap (V_2 + V_3) = (V_1 \cap V_2) + V_3.$$

6. 设$\mathbf{R}$和$\mathbf{C}$分别为实数域和复数域. 则

(*a*) $\dim_{\mathbf{R}}\mathbf{C} = 2$, $\dim_{\mathbf{R}}\mathbf{R} = 1$.

(*b*) 不存在域K, 使得$\mathbf{R} \subsetneq K \subsetneq \mathbf{C}$.

7. 如果G是阶数大于2的群, 则G有非平凡的自同构. 〔提示: 习题II.4.11和上面的习题4(*d*). 〕

8. 如果V是有限维向量空间, 而V^m是向量空间

$$V \oplus V \oplus \cdots \oplus V \qquad (m\text{个}V),$$

则对于每个$m \geqslant 1$, V^m均是有限维向量空间, 并且$\dim V^m = m(\dim V)$.

9. 如果R是具有维数不变性质的环, F_1和F_2是自由R-模, 则$\operatorname{rank}(F_1 \oplus F_2) = \operatorname{rank} F_1 + \operatorname{rank} F_2$.

10. 设R是没有零因子的环, 并且对于每个r, $s \in R$, 均存在a, $b \in R$ (不同时为零), 使得$ar + bs = 0$.

(*a*) 如果$R = K \oplus L$(模直和), 则$K = 0$或者$L = 0$.

(*b*) 如果R为含幺环, 则R具有不变维数性质.

11. 设环R具有不变维数性质, F是自由R-模并且秩α是无限的, 则对于每个势β, $0 \leqslant \beta \leqslant \alpha$, F均有无穷多个秩β的真自由子模.

12. 如果F是含幺环上的自由模, 并且具有有限势$n \geqslant 1$的基, 也具有势$n+1$的基, 则对于每个$m \geqslant n$ ($m \in \mathbf{N}^*$), F都具有势为m的基.

13. 设K为含幺环, F是自由K-模并且具有可数无限的一组基$\{e_1, e_2, \cdots\}$. 则由习题1.7(*b*)可知$R = \operatorname{Hom}_K(F, F)$是环. 求证: 对于任一正整数$n$, 自由左$R$-模$R$均有$n$个元素组成的一组基. 也就是说, 对于任一正整数$n$均有$R$-模同构$R \cong R \oplus \cdots \oplus R$($n$个分量). 〔提示: $\{1_R\}$是一元基. $\{f_1, f_2\}$是二元基, 其中$f_1(e_{2n}) = e_n$, $f_1(e_{2n-1}) = 0$, $f_2(e_{2n}) = 0$, $f_2(e_{2n-1}) = e_n$. 注意对于每个$g \in R$, $g = g_1 f_1 + g_2 f_2$, 其中$g_1(e_n) = g(e_{2n})$, $g_2(e_n) = g(e_{2n-1})$.〕

14. 设$f: V \to V'$是有限维向量空间V和V'之间的线性变换, 并且$\dim V = \dim V'$. 则下列诸条件是彼此等价的.

(i) f是同构；

(ii) f是满同态；

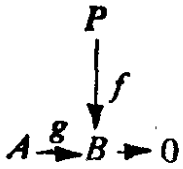
(iii) f是单同态.〔提示：系2.14〕

15. 设R是含幺环. 证明在所有左R-模所形成的范畴中，R不是任何集合上的自由模.(定义见习题2.)〔提示：考虑具有平凡R-模结构的非零Abel群A(即对于每个$r\in R$和$a\in A$，$ra=0$). 注意从R到A的模同态只有零映射.〕

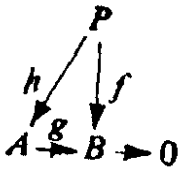
3. 投射模和内射模

每个自由模都是投射模，任意投射模(不必是自由的)都有与自由模相同的某些性质.投射模在范畴讲述方式中是特别有益的，因为它只用模和同态来定义. 此外我们也研究投射模的对偶概念——内射模.

定义3.1 环R上的模P叫作投射模，是指任意给了下面一个R-模同态图表

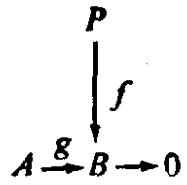


并且底行是正合的(即g是满同态)，均存在R-模同态h：$P\to A$，使得图表

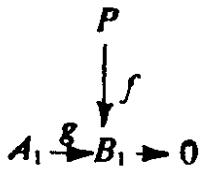


是交换的(即$gh=f$)。

下面几个定理给出投射模的一些例子。我们首先注意，如果R是含幺环而P是幺作用模，则P是投射模$\Leftrightarrow$对于每一对幺作用模A，B和R-模同态的图表



其中g是满同态，均存在同态h：$P\to A$，使得$gh=f$。因为由习题1.17知道$A=A_1\oplus A_2$，$B=B_1\oplus B_2$，其中A_1和B_1均是幺作用模，而$RA_2=0=RB_2$。习题1.17还表明$f(P)\subset B_1$，并且$g|A_1:A_1\to B_1$是满同态，从而我们有幺作用模的图表：



于是“存在h：$P\to A$使$gh=f$”等价于“存在h：$P\to A_1$使$gh=f$”。

定理3.2 含幺环R上的自由模F是投射模。

注记：如果去掉“含幺”二字并且F是全体左R-模组成的范畴中的自由模（定义见习题2.2），则此定理仍旧成立，并且可以逐字逐句地照搬下面的证明，不同之处只是用习题2.2代替定理2.1，同时去掉所有的“幺作用”一词。

定理3.2的证明 按照本定理前面所作的注解，我们可以假定所给的是幺作用R-模的同态图表：

其中g是满同态而F是集合X上的自由R-模$(\iota: X\to F)$。对于每个$x\in X$，$f(\iota(x))\in B$。由于g为满同态，从而存在$a_x\in A$，使得$g(a_x)=f(\iota(x))$。由于F是自由模，映射$X\to A$，$x\longmapsto a_x$诱导出R-模同态$h: F\to A$，使得对每个$x\in X$，$h(\iota(x))=a_x$。从而对每个$x\in X$，$gh\iota(x)=g(a_x)=f\iota(x)$，于是$gh\iota=f\iota: X\to B$。由定理2.1(iv)的唯一性部分，我们有$gh=f$。因此$F$是投射模。∎

系3.3 环R上的每个模A均是某个投射R-模的同态象。

证明 由定理3.2和系2.2直接得到。∎

定理3.4 设R是环。关于R-模P的以下几个条件是彼此等价的。

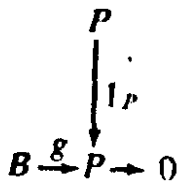
(i) P是投射模；

(ii) 每个短正合序列$0\to A\xrightarrow{f}B\xrightarrow{g}P\to 0$都是分裂正合序列(从而$B\cong A\oplus P$)；

(iii) 存在自由R-模F和R-模K，使得$F\cong K\oplus P$。

注记：如果R是含幺环而P是幺作用模，则条件(iii)中“自由模”一词可以解释成是定理2.1的意思。否则便是习题2.2的意思。无论哪种情形证明是一样的。

定理3.4的证明 (i)$\Longrightarrow$(ii)：考虑图表

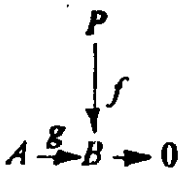


由假设可知底行是正合的。由于P是投射模，从而存在R-模同态$h: P\longrightarrow B$，使得$gh=1_P$。因此由定理1.18可知短正合序列$0\longrightarrow$

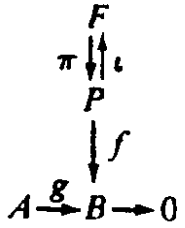
$A \xrightarrow{f} B \underset{h}{\overset{g}{\rightleftarrows}} P \longrightarrow 0$是分裂正合序列，并且$B \cong A \oplus P$。

(ii)$\Longrightarrow$(iii)：由系2.2可知存在自由R-模F 和满同态 g：$F \longrightarrow P$。如果$k = \ker g$，则 $0 \longrightarrow K \xrightarrow{\subset} F \xrightarrow{g} P \longrightarrow 0$是正合的。由假设它也是分裂的，从而由定理1.18即知$F \cong K \oplus P$。

(iii)$\Longrightarrow$(i)：设π 是合成映射 $F \cong K \oplus P \longrightarrow P$，其中第二个映射为正则射影。类似地，令$\iota$是合成$P \longrightarrow K \oplus P \cong F$，其中第一个映射是正则嵌入。给了$R$-模同态图表



并且底行是正合的，考虑图表



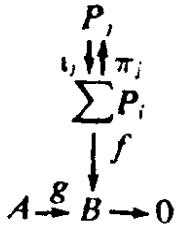
由定理3.2知F是投射模，从而有R-模同态h_1：$F \longrightarrow A$，使得$gh_1 = f\pi$。令$h = h_1\iota$：$P \longrightarrow A$。则$gh = gh_1\iota = (f\pi)\iota = f(\pi\iota) = f1_P = f$，从而$P$是投射模。∎

例 如果$R = Z_6$，则Z_3和Z_2都是Z_6-模(见习题1.1)，并且有Z_6-模同构$Z_6 \cong Z_2 + Z_3$。从而Z_2和Z_3 均是投射Z_6-模，但均不是自由Z_6-模。

命题3.5 设R是环。R-模直和$\sum_{i \in I} P_i$是投射模$\Longleftrightarrow$每个P_i都是投射模。

证明概要 假设$\sum P_i$是投射模。由于定理3.4中在证明(iii)

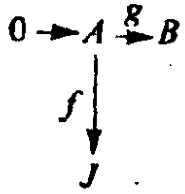
$\Longrightarrow$(i)的时候只用到F是投射模这一事实，从而若将其中的 F,K 和P 分别取成$\sum_{i\in I} P_i$，$\sum_{i\neq j} P_i$和P_j，则结论仍然成立。反过来也可以用类似的技巧证明，即采用图表



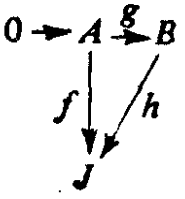
如果每个P_i都是投射模，则对于每个j 均存在 $h_j: P_j \longrightarrow A$ 使得 $gh_j = f\iota_j$。由定理1.13可知存在唯一同态h：$\sum P_i \longrightarrow A$，使得对每个$j$，$h\iota_j = h_j$。验证$gh = f$。∎

让我们回忆：在范畴理论中所定义的某个概念（即用对象和态射定义的概念）的对偶就是通过“倒转所有箭头”而得到的概念。将这种思想稍加引伸，我们可以说：单同态是满同态的对偶，这是因为：$A \longrightarrow B$为单同态$\Longleftrightarrow 0 \longrightarrow A \longrightarrow B$ 为正合的；另一方面，$B \longrightarrow A$为满同态$\Longleftrightarrow B \longrightarrow A \longrightarrow 0$为正合的（箭头倒转！）。这就使我们如下定义投射模的对偶概念。

定义3.6 环R上的模J叫作内射模，是指任意给了R-模同态图表



其中顶行是正合的（即g为单同态），则必然存在 R-模同态 h：$B \longrightarrow J$，使得图表



是交换的(即$hg=f$)。

定义3.1后面一段注解现在类似地也可用于含幺环上幺作用内射模的情形。我们不会感到惊奇的是，前面许多(不是全部)命题的对偶均可以得到证明。例如，由于在范畴理论中积是余积(直和)的对偶概念，从而命题3.5的对偶是

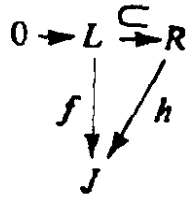
命题3.7 R-模直积$\prod_{i\in I} J_i$是内射模$\Longleftrightarrow$每个J_i都是内射模。

证明作为练习。见命题3.5。∎

由于自由模的概念没有对偶(习题13)，从而对于内射模没有定理3.2或者3.4(iii)的类似结果。但是系3.3具有对偶，事实上，系3.3是说，对于每个模A均存在投射模P和正合序列$P\longrightarrow A\longrightarrow 0$。此命题的对偶应当是：对于每个模$A$均存在内射模$J$和正合序列$0\longrightarrow A\longrightarrow J$。换句话说，每个模均可以嵌入某个内射模中。本节其余部分就是对于含幺环上的幺作用模来证明这一事实，这部分今后是不需要的。一旦证明了这点，便很容易证得定理3.4(i)和(ii)的对偶(命题3.13)。开始我们先用环R的左理想(子模)来刻划内射R-模。

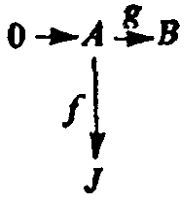
引理3.8 设R是含幺环。幺作用R-模J是内射模$\Longleftrightarrow$对于R的每个左理想L，R-模同态$L\longrightarrow J$均可扩充成R-模同态$R\longrightarrow J$。

证明概要 所谓$f: L\longrightarrow J$可以扩充到R，就是意味着存在同态$h: R\longrightarrow J$，使图表



是交换的。如果J是内射模，这样的h显然是存在的。反之，假设

J有所述的扩充性质，并且我们给了如下的模同态图表



其中顶行是正合的。为证J是内射模，我们必需求出同态h：$B\longrightarrow J$，使得$hg=f$。令

$$\mathscr{S}=\{R\text{-模同态}h\text{：}C\longrightarrow J\mid \mathrm{Im}g\subset C\subset B\}.$$

由于fg^{-1}：$\mathrm{Im}g\longrightarrow J$是$\mathscr{S}$中元素（$g$是单同态），从而$\mathscr{S}$是非空集合。将$\mathscr{S}$赋以如下的半序：$h_1\leqslant h_2 \iff \mathrm{Dom}h_1\subset \mathrm{Dom}h_2$ 并且 $h_2|\mathrm{Dom}h_1=h_1$。验证$\mathscr{S}$满足 Zorn 引理的假设，从而 $\mathscr{S}$ 包含极大元h：$H\longrightarrow J$，其中 $hg=f$。我们只需再证 $H=B$，即可完成整个证明。

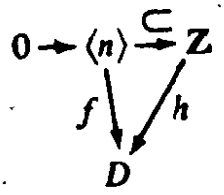
如果 $H\neq B$，令$b\in B-H$，则$L=\{r\in R\mid rb\in H\}$是R的左理想。可以定义 R-模同态$L\to J$，$r\mapsto h(rb)$。由假设可知存在R-模同态 $k:R\to J$，使得对每个 $r\in L$，$k(r)=h(rb)$。令$c=k(1_R)$，定义映射 $\bar{h}:H+Rb=J$，$a+rb\mapsto h(a)+rc$。现在证明 $\bar{h}$ 的可定义性：如果$a_1+r_1b=a_2+r_2b\in H+Rb$，则 $a_1-a_2=(r_2-r_1)b\in H\cap Rb$。从而 $r_2-r_1\in L$ 而 $h(a_1)-h(a_2)=h(a_1-a_2)=h((r_2-r_1)b)=k(r_2-r_1)=(r_2-r_1)k(1_R)=(r_2-r_1)c$。因此 $\bar{h}(a_1+r_1b)=h(a_1)+r_1c=h(a_2)+r_2c=\bar{h}(a_2+r_2b)$，这就证明了$\bar{h}$的可定义性。验证 $\bar{h}$：$H+Rb\to J$是R-模同态，并且是$\mathscr{S}$中的元素。这就与h的极大性相矛盾（因为$b\in H$从而$H\subsetneq H+Rb$）。于是 $H=B$，即J是内射模。∎

Abel群D叫作可除群，是指对于任意给定的$y\in D$和$0\neq n\in\mathbb{Z}$，均有$x\in D$，使得$nx=y$。例如加法群$\mathbb{Q}$是可除群，但$\mathbb{Z}$不是可除群（习题4）。不难证明，Abel群的直和是可除群$\iff$它的每个直

和分量都是可除群。还可以证明：每个可除群的同态象也是可除群（习题7）。

引理3.9 Abel群D是可除群$\Longleftrightarrow D$是内射（幺作用）$\mathbb{Z}$-模。

证明 如果D是内射模，$y\in D$，$0\neq n\in\mathbb{Z}$，令f：$\langle n\rangle\to D$ 是由$n\mapsto y$所唯一决定的同态（由定理 I.3.2和II.1.1可知$\langle n\rangle$是自由$\mathbb{Z}$-模）。由于D是内射模，从而有同态h：$\mathbb{Z}\to D$使得图表



是交换的。如果$x=h(1)$，则 $nx=nh(1)=h(n)=f(n)=y$。因此D是可除群。为证（$\Longrightarrow$），注意$\mathbb{Z}$的左理想均是循环群 $\langle n\rangle$,$n\in\mathbb{Z}$。如果D是可除群而f：$\langle n\rangle\to D$ 是同态，则存在$x\in D$使得$nx=f(n)$。定义h：$\mathbb{Z}\to D$，$1\mapsto x$，证明h是同态并且是f的扩充。从而由引理3.8可知D是内射模。 ∎

注记：习题11给出可除Abel群（即内射幺作用 $\mathbb{Z}$- 模）的一个完全刻划。

引理3.10 每个Abel群A均可以嵌到可除Abel群之中。

证明 根据定理II.1.4，存在自由$\mathbb{Z}$-模F和满同态$F\to A$，其核为K，于是$F/K\cong A$。由于F是一些$\mathbb{Z}$的直和（定理II.1.1），并且$\mathbb{Z}\subset\mathbb{Q}$，从而$F$可以嵌到由一些$\mathbb{Q}$所作成的直和$D$之中（定理I.8.10）。但是由命题3.7，引理3.9和引理3.9前面的注记知道D 是可除群。如果f：$F\to D$是嵌入单同态，则由系 I.5.8知道f诱导出同构$F/K\cong f(F)/f(K)$，因此合成$A\cong F/K\cong f(F)/f(K)\subset D/f(K)$

是单同态。但是$D/f(K)$是可除群的同态象，从而也是可除群.∎

如果R是含幺环而J是Abel群，则$\mathrm{Hom}_Z(R, J)$（即全体$\mathbb{Z}$-模同态$R\to J$所组成的集合）也是Abel群（习题1.7)。验证$\mathrm{Hom}_Z(R, J)$是幺作用左R-模，其中R的作用定义为$(rf)(x)=f(xr)$ $(r, x\in R, f\in \mathrm{Hom}_Z(R, J))$。

引理3.11 如果J是可除Abel群，R是含幺环，则$\mathrm{Hom}_Z(R, J)$是内射左R-模。

证明概要 根据引理3.8可知我们只需证明：对于R的每个左理想L，任意R-模同态$f: L\to \mathrm{Hom}_Z(R, J)$均可以扩充成$R$-模同态$h: R\to \mathrm{Hom}_Z(R, J)$。由$g(a)=[f(a)](1_R)$给出的映射$g: L\to J$是群同态。由引理3.9知道$J$是内射$\mathbb{Z}$-模，并且我们有图表

$$\begin{array}{ccc} 0\to L & \subseteq & R \\ {\scriptstyle g}\downarrow & & \\ J & & \end{array}$$

从而有群同态$\bar{g}: R\to J$，使得$\bar{g}|L=g$。定义$h: R\to \mathrm{Hom}_Z(R, J)$，$r\mapsto h(r)$，其中$h(r): R\to J$是由$[h(r)](x)=\bar{g}(xr)(x\in R)$所给出的映射。验证$h$的可定义性（即每个$h(r)$均是群同态$R\to J$)，验证$h$是群同态$R\to \mathrm{Hom}_Z(R, J)$。如果$s, r, x\in R$，则

$$h(sr)(x)=\bar{g}(x(sr))=\bar{g}((xs)r)=h(r)(xs).$$

根据$\mathrm{Hom}_Z(R, J)$所定义的R-模结构，我们有$h(r)(xs)=[sh(r)](x)$，从而$h(sr)=sh(r)$，于是h为R-模同态。最后，假设$r\in L$，$x\in R$。则$xr\in L$，而

$$h(r)(x)=\bar{g}(xr)=g(xr)=[f(xr)](1_R).$$

因为f是R-模同态而$\mathrm{Hom}_Z(R, J)$是R-模，从而

$$[f(xr)](1_R)=[xf(r)](1_R)=f(r)(1_Rx)=f(r)(x).$$

因此对于$r\in L$，$h(r)=f(r)$，即h是f的扩充。 ∎

现在我们可以证明系3.3和定理3.4的对偶。

命题3.12 含幺环R上的每个幺作用模A均可以嵌到某个内射R-模之中。

证明概要 因为A是Abel群，由引理3.10可知存在可除群J和群的单同态f：$A\to J$。不难看出，映射

$$\bar{f}:\ \mathrm{Hom}_Z(R,\ A)\to\mathrm{Hom}_Z(R,\ J),$$

对于$g\in\mathrm{Hom}_Z(R,\ A)$，$\bar{f}(g)=fg\in\mathrm{Hom}_Z(R,\ J)$

是R-模单同态。由于每个R-模同态均是$\mathbb{Z}$-模同态，我们有$\mathrm{Hom}_R(R,\ A)\subset\mathrm{Hom}_Z(R,\ A)$。事实上，不难看出$\mathrm{Hom}_R(R,\ A)$是$\mathrm{Hom}_Z(R,A)$的$R$-子模。最后，验证映射

$$A\to\mathrm{Hom}_R(R,A),\ \ a\longmapsto f_a,\ \ f_a(r)=ra.$$

是R-模单同态（事实上它是同构）。合成这些映射便得到R-模单同态

$$A\to\mathrm{Hom}_R(R,A)\xrightarrow{\subset}\mathrm{Hom}_Z(R,\ A)\xrightarrow{\bar{f}}\mathrm{Hom}_Z(R,\ J).$$

由引理3.11知$\mathrm{Hom}_Z(R,\ J)$是内射R-模，从而我们已经将A嵌到内射模之中。 ∎

命题3.13 设R是含幺环。则关于幺作用R-模J的下列诸条件是彼此等价的：

(i) J是内射模；

(ii) 每个短正合序列$0\to J\xrightarrow{f}B\xrightarrow{g}C\to 0$都是分裂正合序列（从而$B=J\oplus C$）；

(iii) 如果J是某个R-模B的子模，则J必为B的直和成份。

证明概要 (i)$\Longrightarrow$(ii)。将定理3.4中(i)$\Longrightarrow$(ii)的证明

对偶化即可。

(ii)$\Longrightarrow$(iii)：由于序列 $0\to J\xrightarrow{\subset} B\xrightarrow{\pi} B/J\to 0$是分裂正合的，从而存在同态 g：$B/J\to B$，使得 $\pi g=1_{B/J}$。由定理 1.18 ((i)$\Longrightarrow$(iii)) 可知有同构$J\oplus B/J\cong B$，$(x, y)\longmapsto x+g(y)$。容易得出B是J和$g(B/J)$的内直和。

(iii)$\Longrightarrow$(i)：由命题 3.12 可知J是某个内射模Q的子模。再由命题3.7和这里的 (iii) 推出J是内射模。 ∎

习　题

注：R是环。如果R为含幺环，则所有R-模均假定是幺作用的。

1. 关于[含幺]环R的以下诸条件是彼此等价的：
   (a) 每个[幺作用]R-模都是投射模；
   (b) 每个[幺作用]R-模的短正合序列都是分裂正合的；
   (c) 每个[幺作用]R-模都是内射模。
2. 设R是含幺环。则R-模A是内射的$\Longleftrightarrow$对于R的每个左理想L和R-模同态g：$L\to A$，均存在$a\in A$，使得$g(r)=ra$（对于每个$r\in L$）。
3. 体D上每个向量空间既是投射D-模也是内射D-模。[见习题1.]
4. (a) 对于每个素数p，$\mathbf{Z}(p^\infty)$（见习题I.1.10）是可除群。
   (b) 非零有限Abel群都不是可除群。
   (c) 非零自由Abel群都不是可除群。
   (d) $\mathbf{Q}$是可除Abel群。
5. $\mathbf{Q}$不是投射$\mathbf{Z}$-模。
6. 如果G是Abel群，则$G=D\oplus N$，其中D是可除群，而N是简约的（即指N没有非平凡的可除子群）。[提示：令D是由G的全体可除子群的并集所生成的子群。]
7. 不用引理3.9证明：

(a) 可除Abel群的每个同态象均是可除群。

(b) 可除Abel群的每个直和成份（习题I.8.12）也是可除群。

(c) 可除Abel群的直和也是可除群。

8. 无扭可除Abel群D必是一些有理数加法群$\mathbf{Q}$的直和。[提示：如果$0\neq n\in\mathbf{Z}$，$a\in D$，则存在唯一的$b\in D$，使得$nb=a$。将b记为$\left(\frac{1}{n}a\right)$。对于$m$，$n\in\mathbf{Z}$，$(n\neq 0)$，定义$(m/n)a=m(1/n)a$。则$D$是$\mathbf{Q}$上的向量空间。然后使用定理2.4.]

9. (a) 如果D是可除群，则D_t也是可除群，从而$D=D_t\oplus E$，其中E是无扭群。

10. 设p是素数，D是可除Abel$p$-群。则D是一些$\mathbf{Z}(p^\infty)$的直和。[提示：令X是Z_p上向量空间$D[p]$的一组基（见习题2.4）。如果$x\in X$，则存在x_1，x_2，x_3，$\cdots\in D$，使得$x_1=x$，$|x_1|=p$，$px_2=x_1$，$px_3=x_2$，$\cdots$，$px_{n+1}=x_n$，$\cdots$。如果H_x是由这些x_i生成的子群，则$H_x\cong\mathbf{Z}(p^\infty)$（习题I.3.7）。证明$D\cong\sum_{x\in X}H_x$。]

11. 每个可除Abel群都是一些有理数加法群$\mathbf{Q}$和一些$\mathbf{Z}(p^\infty)$（对于某些可能不同的素数p）的直和。[提示：将习题9用于D，然后将习题7和8用于所得到的无扭直和成份。而由习题7，10和II.2.7。又知另一个直和成份D_t是各种$\mathbf{Z}(p^\infty)$的直和。]

12. 令G，H，K均是可除Abel群。

(a) 如果$G\oplus G\cong H\oplus H$，则$G\cong H$[见习题11]。

(b) 如果$G\oplus H\cong G\oplus K$，则$H\cong K$[见习题11和II.2.11]。

13. 假如我们试图将环R上自由模的概念加以对偶化（不妨称这种对象是“余自由的”(co-free)），那末其定义应当有如下形式：R-模F叫作集合X上的余自由模，是指存在函数ι：$F\to X$，使得对于每个R-模A和函数f：$A\to X$，均有唯一的模同态$\overline{f}$：$A\to F$满足$\iota\overline{f}=f$（见定理2.1(iv)）。求证对于每个集合X，如果$|X|\geqslant 2$，则没有这样的R-模F。如果$|X|=1$，则只有0是余自由模。[提示：如果F存在并且$|X|\geqslant 2$，

考虑0的可能映象然后构作f：$R\to X$使得对每个同态$\overline{f}$：$R\to F$ 均有 $\overline{i}f\neq f$，即可导出矛盾。]

14. 如果D是含幺环并且每个幺作用D-模都是自由模，则D是体。[提示：由习题III.2.7和定理III.2.18可知只需证明D 没有非零极大左理想.注意D的每个左理想均是自由 D-模，从而由定理 3.2，习题1和命题3.13可知它均是模D的直和成份。]

4. Hom 和对偶性

我们首先讨论 $\mathrm{Hom}_R(A, B)$ 与诱导映射，正合序列，直和以及直积有关的一些性质。本节的后一部分处理对偶性，它与前一部分本质上是相互独立的。

回忆：如果A和B是环R上的模，则$\mathrm{Hom}_R(A, B)$是所有R-模同态$A\to B$所形成的集合。如果$R=\mathbb{Z}$，通常我们将$\mathrm{Hom}_Z(A,B)$写成$\mathrm{Hom}(A, B)$。$\mathrm{Hom}_R(A, B)$ 是加法Abel群，并且加法与函数合成运算满足分配律 （见第261页）。

定理4.1 设A，B,C,D是环R上的模。φ：$C\to A$ 和ψ：$B\to D$是R-模同态。则映射

$$\theta\colon \mathrm{Hom}_R(A, B)\to\mathrm{Hom}_R(C, D),\ f\mapsto\psi f\varphi$$

是Abel群的同态。

证明概要 由于R-模同态的合成仍是R-模同态，从而θ是可定义的。再由 R- 模同态的合成与加法满足分配律，可知 θ 是同态。 ∎

通常将定理4.1中的映射θ写成$\mathrm{Hom}(\varphi, \psi)$，并且叫作由$\varphi$和$\psi$所诱导的同态。注意对于同态$\varphi_1: E\to C$，$\varphi_2: C\to A$，$\psi_1: B\to D$和$\psi_2: D\to F$，我们有

$$\mathrm{Hom}(\varphi_1,\psi_2)\mathrm{Hom}(\varphi_2, \psi_1)=\mathrm{Hom}(\varphi_2\varphi_1, \psi_2\psi_1):$$

$$\mathrm{Hom}_R(A,B)\to\mathrm{Hom}_R(E,F).$$

诱导同态有两个重要的特殊情况。如果$B=D$并且$\psi=1_B$，则诱导同态$\mathrm{Hom}(\varphi, 1_B): \mathrm{Hom}_R(A, B)\to\mathrm{Hom}_R(C,B)$为$f\mapsto f\varphi$，这记成$\bar{\varphi}$。类似地，如果$A=C$并且$\varphi=1_A$，则诱导同态$\mathrm{Hom}(1_A, \psi): \mathrm{Hom}_R(A, B)\to\mathrm{Hom}_R(A, D)$为$f\mapsto\psi f$，这记成$\bar{\psi}$。

现在我们考查Hom_R与正合序列有关的性质。

定理4.2 设R是环，则$0\to A\xrightarrow{\varphi} B\xrightarrow{\psi} C$是$R$-模正合序列$\Longleftrightarrow$对于每个$R$-模$D$，

$$0\to\mathrm{Hom}_R(D,A)\xrightarrow{\bar{\varphi}}\mathrm{Hom}_R(D, B)\xrightarrow{\bar{\psi}}\mathrm{Hom}_R(D,C)$$

是Abel群的正合序列。

证明 如果$0\to A\xrightarrow{\varphi} B\xrightarrow{\psi} C$是正合的，我们需要证明：(i) $\mathrm{Ker}\bar{\varphi}=0$（即$\bar{\varphi}$是单同态）；(ii) $\mathrm{Im}\bar{\varphi}\subset\mathrm{Ker}\bar{\psi}$；(iii) $\mathrm{Ker}\bar{\psi}\subset\mathrm{Im}\bar{\varphi}$。

(i) $f\in\mathrm{Ker}\bar{\varphi}\Longrightarrow\varphi f=0\Longrightarrow\varphi f(x)=0$（对于每个$x\in D$）。由于$0\to A\xrightarrow{\varphi} B$正合，$\varphi$是单同态，从而对于每个$x\in D$，$f(x)=0$，即$f=0$。因此$\mathrm{Ker}\bar{\varphi}=0$。

(ii) 由正合性可知$\mathrm{Im}\varphi=\mathrm{Ker}\psi$，从而$\psi\varphi=0$，于是$\bar{\psi}\,\bar{\varphi}=\overline{\psi\varphi}=0$。因此$\mathrm{Im}\bar{\varphi}\subset\mathrm{Ker}\bar{\psi}$。

(iii) $g\in\mathrm{Ker}\bar{\psi}\Longrightarrow\psi g=0\Longrightarrow\mathrm{Im}g\subset\mathrm{Ker}\psi=\mathrm{Im}\varphi$。由于$\varphi$是单同态，从而$\varphi: A\to\mathrm{Im}\varphi$是同构。如果$h$是合成映射$D\xrightarrow{g}\mathrm{Im}\,g\subset\mathrm{Im}\,\varphi\xrightarrow{\varphi^{-1}}A$，则$h\in\mathrm{Hom}_R(D, A)$并且$g=\varphi h=\bar{\varphi}(h)$。从而$\mathrm{Ker}\bar{\psi}\subset\mathrm{Im}\bar{\varphi}$。

反之，假设对于每个D，其诱导映射的Hom序列都是正合的。首先令$D=\mathrm{Ker}\varphi$，并且令i：$D\to A$是包含映射。由于$\mathrm{Ker}\bar{\varphi}=0$(正合性)，$\bar{\varphi}(i)=\varphi i=0$，从而$0=D=\mathrm{Ker}\varphi$。因此$0\to A\xrightarrow{\varphi}B$是正合的。其次，令$D=A$。由于$\mathrm{Ker}\bar{\psi}=\mathrm{Im}\bar{\varphi}$，我们有$0=\bar{\psi}\bar{\varphi}(1_A)=\psi\varphi 1_A=\psi\varphi$，从而$\mathrm{Im}\varphi\subset\mathrm{Ker}\psi$。最后令$D=\mathrm{Ker}\psi$，并且令$j$：$D\to B$是包含映射。由于$0=\psi j=\bar{\psi}(j)$以及$\mathrm{Ker}\bar{\psi}=\mathrm{Im}\bar{\varphi}$，从而存在某个$f$：$D\to A$使得$j=\bar{\varphi}(f)=\varphi f$。因此对于每个$x\in D=\mathrm{Ker}\psi$均有$x=j(x)=\varphi f(x)\in\mathrm{Im}\varphi$，于是$\mathrm{Ker}\psi\subset\mathrm{Im}\varphi$。从而$\mathrm{Ker}\psi=\mathrm{Im}\varphi$，即$0\to A\xrightarrow{\varphi}B\xrightarrow{\psi}C$是正合的。 ∎

命题4.3 设R是环。则$A\xrightarrow{\theta}B\xrightarrow{\rho}C\to 0$为$R$-模正合序列$\Longleftrightarrow$对于每个$R$-模$D$，

$$0\to\mathrm{Hom}_R(C,D)\xrightarrow{\bar{\rho}}\mathrm{Hom}_R(B,D)\xrightarrow{\bar{\theta}}\mathrm{Hom}_R(A,D)$$

均是Abel群的正合序列。

证明概要 如果$A\xrightarrow{\theta}B\xrightarrow{\rho}C\to 0$是正合的，我们需要证明$\mathrm{Ker}\bar{\theta}\subset\mathrm{Im}\bar{\rho}$。如果$f\in\mathrm{Ker}\bar{\theta}$，则$0=\bar{\theta}(f)=f\theta$，从而$0=f(\mathrm{Im}\theta)=f(\mathrm{Ker}\rho)$。由定理1.7可知$f$诱导出同态$\bar{f}$：$B/\mathrm{Ker}\rho\to D$，使得$\bar{f}(b+\mathrm{Ker}\rho)=f(b)$。再由定理1.7可知存在同构$\varphi$：$B/\mathrm{Ker}\rho\cong C$，使得$\varphi(b+\mathrm{Ker}\rho)=\rho(b)$。于是映射$\bar{f}\varphi^{-1}$：$C\to D$是$R$-模同态，并且$\bar{\rho}(\bar{f}\varphi^{-1})=f$。于是$\mathrm{Ker}\bar{\theta}\subset\mathrm{Im}\bar{\rho}$。然后类似于定理4.2即可完成($\Longrightarrow$)部分的证明。

反之，假设对于每个D，其Hom序列都是正合的。令$D=C/\mathrm{Im}\zeta$，π：$C\to D$是正则射影。则$\bar{\zeta}(\pi)=\pi\zeta=0$，从而由$\mathrm{Ker}\bar{\zeta}=0$导致$\pi=0$。于是$C=\mathrm{Im}\zeta$，即$B\xrightarrow{\zeta}C\to 0$是正合的。然后考虑$D=B/\mathrm{Im}\theta$和正则满同态$B\to D$即可类似地证明$\mathrm{Ker}\zeta\subset\mathrm{Im}\theta$。最后取$D=C$，则$0=\bar{\theta}\bar{\zeta}(1_C)=\zeta\theta$，从而$\mathrm{Im}\theta\subset\mathrm{Ker}\zeta$。因此$A\xrightarrow{\theta}B\xrightarrow{\zeta}C\to 0$是正合

的。 ∎

人们有时把上面两个结果综合起来，说成：$\mathrm{Hom}_R(A, B)$是左正合的。一般来说，短正合序列$0\to A\to B\to C\to 0$并不诱导出短正合序列 $0\to\mathrm{Hom}_R(D, A)\to\mathrm{Hom}_R(D, B)\to\mathrm{Hom}_R(D, C)\to 0$和$0\to\mathrm{Hom}_R(C, D)\to\mathrm{Hom}_R(B, D)\to\mathrm{Hom}_R(A, D)\to 0$（见习题3）。但是，下面三个定理表明，在某些情况下所诱导出的这些序列是正合的。

命题4.4 关于环R上模的下列诸条件是彼此等价的。

(i) $0\to A\xrightarrow{\varphi}B\xrightarrow{\psi}C\to 0$是分裂的$R$-模正合序列；

(ii) 对于每个R-模D，$0\to\mathrm{Hom}_R(D, A)\xrightarrow{\bar{\varphi}}\mathrm{Hom}_R(D, B)\xrightarrow{\bar{\psi}}\mathrm{Hom}_R(D, C)\to 0$是分裂的Abel群正合序列；

(iii) 对于每个R-模D，$0\to\mathrm{Hom}_R(C, D)\xrightarrow{\bar{\psi}}\mathrm{Hom}_R(B, D)\xrightarrow{\bar{\varphi}}\mathrm{Hom}_R(A, D)\to 0$是分裂的Abel群正合序列。

证明概要 (i)$\Longrightarrow$(iii)：由定理1.18可知存在同态$\alpha: B\to A$使得$\alpha\varphi=1_A$。验证其诱导同态

$$\bar{\alpha}: \mathrm{Hom}_R(A, D)\to\mathrm{Hom}_R(B, D)$$

满足$\bar{\varphi}\,\bar{\alpha}=1_{\mathrm{Hom}_R(A, D)}$。从而$\varphi$是满同态（引论中的定理3.1），由命题4.3和定理1.18即知该Hom_R序列是分裂正合的。

(iii)$\Longrightarrow$(i)：如果$D=A$，而$f: B\to A$满足$1_A=\bar{\varphi}(f)=f\varphi$，则$\varphi$是单同态（引论中的定理3.1）。由命题4.3和定理1.18即知$0\to A\xrightarrow{\varphi}B\xrightarrow{\psi}C\to 0$是分裂正合序列。类似地证明(i)$\Longrightarrow$(ii)和(ii)$\Longrightarrow$(i)。 ∎

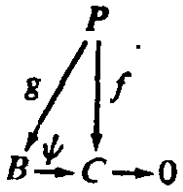
定理4.5 关于环R上模P的下列条件是彼此等价的。

(i) P是投射模；

(ii) 如果ψ：$B\to C$是R-模满同态，则$\bar{\psi}$：$\mathrm{Hom}_R(P, B)\to\mathrm{Hom}_R(P, C)$是Abel群的满同态。

(iii) 如果$0\to A\xrightarrow{\varphi}B\xrightarrow{\psi}C\to 0$是$R$-模短正合序列，则$0\to\mathrm{Hom}_R(P, A)\xrightarrow{\bar{\varphi}}\mathrm{Hom}_R(P, B)\xrightarrow{\bar{\psi}}\mathrm{Hom}_R(P, C)\to 0$是Abel群的短正合序列。

证明概要 (i)$\Longleftrightarrow$(ii)：映射$\bar{\psi}$：$\mathrm{Hom}_R(P, B)\to\mathrm{Hom}_R(P, C)(g\mapsto\psi g)$是满同态$\Longleftrightarrow$对于每个$R$-模同态$f$：$P\to C$，均有$R$-模同态$g$：$P\to B$，使得图表是交换的（即：$f=\psi g=\bar{\psi}(g)$）。



(ii)$\Longrightarrow$(iii)：定理4.2。

(iii)$\Longrightarrow$(ii)：给了满同态ψ：$B\to C$。令$A=\mathrm{Ker}\psi$，然后将(ii)用于短正合序列$0\to A\xrightarrow{\subset}B\xrightarrow{\psi}C\to 0$即可。∎

命题4.6 关于环R上模J的下列诸条件是彼此等价的。

(i) J是内射模；

(ii) 如果θ：$A\to B$是R-模单同态，则$\bar{\theta}$：$\mathrm{Hom}_R(B, J)\to\mathrm{Hom}_R(A, J)$是Abel群的满同态；

(iii) 如果$0\to A\xrightarrow{\theta}B\xrightarrow{\zeta}C\to 0$是$R$-模短正合序列，则$0\to\mathrm{Hom}_R(C, J)\xrightarrow{\bar{\zeta}}\mathrm{Hom}_R(B, J)\xrightarrow{\bar{\theta}}\mathrm{Hom}_R(A, J)\to 0$是Abel群的短正合序列。

证明 为定理4.5的对偶。留给读者练习。∎

定理4.7 设A，B，$\{A_i\mid i\in I\}$，$\{B_j\mid j\in J\}$均是环R上的模。

则有如下的Abel群同构：

(i) $\mathrm{Hom}_R\left(\sum_{i\in I} A_i,\ B\right) \cong \prod_{i\in I} \mathrm{Hom}_R(A_i,\ B)$；

(ii) $\mathrm{Hom}_R\left(A,\ \prod_{j\in J} B_j\right) \cong \prod_{j\in J} \mathrm{Hom}_R(A,\ B_j)$。

注记：如果I和J均是有限的，则$\sum_{i\in I} A_i = \prod_{i\in I} A_i$，$\sum_{j\in J} B_i = \prod_{j\in J} B_j$。如果$I$和$J$是无限的，则直积$\Pi$改成直和$\Sigma$之后，定理可能不成立（见习题10）。

定理4.7的证明概要 (i) 对于每个$i\in I$，令$\iota_i: A_i \to \sum_{i\in I} A_i$为正则射影(定理1.11)。给了$\{g_i\}\in \prod_{i\in I} \mathrm{Hom}_R(A_i,\ B)$，存在唯一的$R$-模同态$g: \sum_{i\in I} A_i \to B$，使得对每个$i\in I$，$g\iota_i = g_i$（定理1.13）。验证映射

$\psi: \Pi\mathrm{Hom}_R(A_i,\ B) \to \mathrm{Hom}_R(\Sigma A_i,\ B), \{g_i\} \longmapsto g$ 是同态。证明映射

$\varphi: \mathrm{Hom}_R(\Sigma A_i,\ B) \to \Pi\mathrm{Hom}_R(A_i,\ B),\ f \longmapsto \{f\iota_i\}$ 是同态，并且$\varphi\psi$和$\psi\varphi$均为恒等映射。从而φ为同构。

(ii) 类似地证明，只是用定理1.12代替定理1.13。∎

为了处理对偶性和其他一些概念，我们需要考虑Abel群$\mathrm{Hom}_R(A,\ B)$上一些可能的模结构。我们先引进双重模。设R和S是环。Abel群A叫作R-S双重模，是指A既是左R-模又是右S-模，并且

$r(as) = (ra)s$（对每个$a\in A$，$r\in R$，$s\in S$）。我们有时写成

${}_RA_S$ 以表示A是R-S双重模。类似地，用${}_RB$ 表示左R-模B，用C_S表示右S-模C。

例 每个环R的乘法均满足结合律，从而是R-R 双重模。交换环R上的每个左模A都是 R-R 双重模，其中 $ra=ar$ $(a\in A, r\in R)$。

定理4.8 设R和S是环，而${}_RA$，${}_RB_S$，${}_RC_S$和${}_RD$如上所述。

(i) $\mathrm{Hom}_R(A, B)$ 是右 S-模，其中S的作用为：$(fs)(a)=(f(a))s$ $(s\in S, a\in A, f\in \mathrm{Hom}_R(A, B))$。

(ii) 如果$\varphi: A\to A'$是左R-模同态，则诱导映射$\bar{\varphi}$：$\mathrm{Hom}_R(A', B)\to\mathrm{Hom}_R(A, B)$ 是右S-模同态。

(iii) $\mathrm{Hom}_R(C, D)$ 是左S-模，其中S的作用为：$(sg)(c)=g(cs)$ $(s\in S, c\in C, g\in \mathrm{Hom}_R(C, D))$。

(iv) 如果$\psi: D\to D'$为左R-模同态，则$\bar{\psi}$：$\mathrm{Hom}_R(C, D)\to \mathrm{Hom}_R(C, D')$ 是左S-模同态。

证明概要 (i) 验证fs定义出模同态。证明 $\mathrm{Hom}_R(A, B)$ 为右 S-模是冗长而乏味的，但是每一步都很简单。类似地证明(iii)。

(ii) 由定理4.1知道$\bar{\varphi}$是Abel群同态。如果$f\in \mathrm{Hom}_R(A', B)$，$a\in A$，$s\in S$，则

$$\begin{aligned}\bar{\varphi}(fs)(a)&=((fs)\varphi)(a)=(fs)(\varphi(a))\\&=(f(\varphi(a)))s=(f\varphi(a))s\\&=((\bar{\varphi}f)(a))s.\end{aligned}$$

于是$\bar{\varphi}(fs)=(\bar{\varphi}f)s$，即$\bar{\varphi}$是右$S$-模同态。类似地证明(iv)。∎

注记：作为定理4.8的一个重要特例是：R为交换环，于是每个R-模C均是R-R 双重模，其中 $rc=cr$ $(r\in R, c\in C)$。这时，

对于每个$r\in R$，$a\in A$和$f\in \mathrm{Hom}_R(A, B)$，我们均有

$$(rf)(a)=f(ar)=f(ra)=rf(a)=(f(a))r$$
$$=(fr)(a).$$

从而$\mathrm{Hom}_R(A, B)$也是R-R双重模，其中$rf=fr$ ($r\in R$，$f\in \mathrm{Hom}_R(A, B)$)。

定理4.9 如果A是含幺环R上的幺作用左模，则有左R-模同构$A\cong \mathrm{Hom}_R(R, A)$。

证明概要 由于R是R-R双重模，可以由定理4.8 (iii) 给出$\mathrm{Hom}_R(R, A)$的左模结构。验证映射

$$\varphi: \mathrm{Hom}_R(R, A)\longrightarrow A,\ f\longmapsto f(1_R)$$

是R-模同态，定义映射ψ：$A\longrightarrow \mathrm{Hom}_R(R, A)$，$a\longmapsto f_a$，其中$f_a(r)=ra$。验证$\psi$是可定义的，并且是$R$-模同态，而且$\varphi\psi=1_A$，$\psi\varphi=1_{\mathrm{Hom}_R(R,A)}$。∎

令A是环R上的左模。由于R是R-R双重模，由定理4.8 (i) 可知$\mathrm{Hom}_R(A, R)$是右R-模，称作A的对偶模，并且表示成A^*。A^*中的元素有时叫作线性泛函。类似地，如果B是右R-模，则B的对偶B^*是左R-模$\mathrm{Hom}_R(B, R)$ (习题4(a))。

定理4.10 设A，B和C是环R上的左模，

(i) 如果φ：$A\to C$是左R-模同态，则诱导映射$\bar{\varphi}$：$C^*=\mathrm{Hom}_R(C, R)\to \mathrm{Hom}_R(A, R)=A^*$是右$R$-模同态。

(ii) 存在R-模同构$(A\oplus C)^*\cong A^*\oplus C^*$。

(iii) 如果R是体，而$0\to A\xrightarrow{\theta} B\xrightarrow{\zeta} C\to 0$是左向量空间的短正合序列，则$0\to C^*\xrightarrow{\bar{\zeta}} B^*\xrightarrow{\bar{\theta}} A^*\to 0$是右向量空间的短正合序列。

证明作为练习。参见定理2.4，3.2，4.1，4.5和4.7。(i)中的映射$\bar{\varphi}$叫作φ的对偶映射。∎

如果A是环R上的左模，$a\in A$，$f\in A^*=\mathrm{Hom}_R(A, R)$，我们常常将$f(a)\in R$表示成$\langle a, f\rangle$，由于$f$是左$R$-模同态，从而

$$\langle r_1a_1+r_2a_2, f\rangle=r_1\langle a_1, f\rangle+r_2\langle a_2, f\rangle \quad (r_i\in R,\ f\in A^*,\ a_i\in A) \tag{1}$$

类似地，由于A^*是左R-模，其中$(fr)(a)=f(a)r$，我们有

$$\langle a, f_1r_1+f_2r_2\rangle=\langle a, f_1\rangle r_1+\langle a, f_2\rangle r_2 \quad (r_i\in R,\ f_i\in A^*\ a\in A) \tag{2}$$

在下面证明中我们对线性泛函使用尖括号记法，同时还使用Kronecker符号δ_{ij}：对于任意下标集合I和含幺环R，符号$\delta_{ij}(i, j\in I)$在$i\neq j$时表示$0\in R$，而在$i=j$时表示$1_R\in R$。

定理4.11 设F是含幺环上的自由左模，令X是F的一组基，并且对于每个$x\in X$，令f_x：$F\to R$由$f_x(y)=\delta_{x,y}$，$(y\in X)$所定义。则

(i) $\{f_x|x\in X\}$是F^*的线性无关子集合，并且势为$|X|$；

(ii) 如果X是有限的，则F^*是以$\{f_x|x\in X\}$为基的自由右R-模。

注记：由于F是以X为基的自由模，从而同态f_x是可定义的（定理2.1）。在(ii)中，我们称$\{f_x|x\in X\}$是X的对偶基。由定理2.4可知，本定理对于体上任意向量空间V显然是对的。特别若V是有限维的，则由命题2.9和定理4.11推出$\dim V=\dim V^*$，$V\cong V^*$。但是如果V是无限维的，则$\dim V^*>\dim V$（习题12）。更一般地，如果F是任意环（例如$\mathbb{Z}$）上的自由模，则F^*不一定为自由模（见习题10）。

定理4.11的证明 (i)如果$f_{x_1}r_1+f_{x_2}r_2+\cdots+f_{x_n}r_n=0(r_i\in R, x_i\in X)$，则对于每个$0\leqslant j\leqslant n$，

$$0=\langle x_j,\ 0\rangle=\langle xj,\ \sum_{i=0}^{n} f_{xi}r_i\rangle=\sum_i \langle x_j,\ f_{xi}\rangle r_i=\sum_i \delta_{ij}r_i$$

$=r_j$。

由于$r_j=0$（对每个j），可知$\{f_x\mid x\in X\}$是线性无关的。如果$x\neq y\in X$，则$f_x(x)=1_R\neq 0=f_y(x)$，从而$f_x\neq f_y$。因此$|X|=|\{f_x\mid x\in X\}|$。

(ii) 如果X是有限的，假设$X=\{x_1,\ \cdots,\ x_n\}$，$f\in F^*$，令$s_i=f(x_i)=\langle x_i,\ f\rangle\in R$。我们用$f_i$表示$f_{x_i}$。如果$u\in F$，则$u=r_1x_1+r_2x_2+\cdots+r_nx_n\in F$ $(r_i\in R)$。从而

$$\begin{aligned}\langle u,\ \sum_{j=1}^{n} f_j s_j\rangle &=\langle \sum_{i=1}^{n} r_i x_i,\ \sum_j f_j s_j\rangle=\sum_i\sum_j r_i\langle x_i,\ f_j\rangle s_j\\ &=\sum_i\sum_j r_i\delta_{ij}s_j=\sum_i r_i s_i=\sum_i r_i\langle x_i,\ f\rangle\\ &=\langle\sum_i r_i x_i,\ f\rangle=\langle u,\ f\rangle。\end{aligned}$$

因此$f=f_1s_1+f_2s_2+\cdots+f_ns_n$，而$\{f_i\}=\{f_x\mid x\in X\}$生成$F^*$。从而$\{f_x\mid x\in X\}$是一组基，即$F^*$是自由模。∎

可以将对偶再作对偶。如果A是左R-模，则A^*是右R-模，而$A^{**}=(A^*)^*=\mathrm{Hom}_R(\mathrm{Hom}_R(A,\ R),\ R)$（其中第一个$\mathrm{Hom}_R$是表示全部右$R$-模同态）是左$R$-模（见习题4(a)）。$A^{**}$叫做是$A$的两次对偶。

定理4.12 设A是环R上的左模。

(i) 存在R-模同态θ：$A\to A^{**}$。

(ii) 如果R是含幺环而A是自由R-模，则θ是单同态。

(iii) 如果R是含幺环而A是具有一组有限基的自由R-模，则

θ是同构.

如果θ：$A\to A^{**}$是同构，我们称A为反射模.

证明 (i) 对于每个$a\in A$，令$\theta(a)$：$A^*\to R$由$[\theta(a)](f)=\langle a, f\rangle\in R$所定义. 由定理4.10后面的(2)式可知$\theta(a)$是右$R$-模同态（即$\theta(a)\in A^{**}$）. 从定理4.10后面的(1)式可知，由$a\longmapsto\theta(a)$给出的映射$\theta$：$A\to A^{**}$是左$R$-模同态.

(ii) 设X是A的一组基. 如果$a\in A$，则$a=r_1x_1+r_2x_2+\cdots+r_nx_n$ ($r_i\in R$，$x_i\in X$). 如果$\theta(a)=0$，则对每个$f\in A^*$，

$$0=\langle a, f\rangle=\langle\sum_{i=1}^{n}r_ix_i, f\rangle=\sum_i r_i\langle x_i, f\rangle.$$

特别对$f=f_{x_j}$ ($1\leqslant j\leqslant n$) 我们有

$$0=\sum_i r_i\langle x_i, f_{x_j}\rangle=\sum_i r_i\delta_{ij}=r_j.$$

因此$a=\sum_j r_jx_j=\sum_i 0x_i=0$，而$\theta$是单同态.

(iii) 如果X是A的一组有限基，则A^*是对偶基$\{f_x\mid x\in X\}$上的自由模（定理4.11）. 类似地，A^{**}是（有限）对偶基$\{g_x\mid x\in X\}$上的自由模，其中对于每个$x\in X$，g_x：$A^*\to R$是由条件$g_x(f_y)=\delta_{xy}$ ($y\in X$) 所唯一决定的同态. 但是$\theta(x)\in A^{**}$是同态$A^*\to R$，并且对于每个$y\in X$均有

$$\theta(x)(f_y)=\langle x, f_y\rangle=\delta_{xy}=g_x(f_y).$$

于是$g_x=\theta(x)$，而$\{\theta(x)\mid x\in X\}$是A^{**}的一组基. 由此推出$Im\theta=A^{**}$，即θ是满同态. ∎

习　题

注：R是环

1. (a) 对于任意Abel群A和正整数m，Hom $(Z_m, A)\cong A[m]=\{a\in A\mid$

$ma=0\}$。

(b) $\mathrm{Hom}\ (Z_m,\ Z_n)\cong Z_{(m,n)}$。

(c) 对于Z-模Z_m，我们有$Z^*{}_m=0$。

(d) 对于每个$k\geqslant 1$，Z_m是Z_{mk}一模（习题1.1）。作为Z_{mk}-模有$Z^*{}_m\cong Z_m$。

2. 如果A，B是Abel群，m，n为整数，使得$mA=0=nB$，则$\mathrm{Hom}\ (A,\ B)$中每个元素的阶均可整除$(m,\ n)$。

3. 设π：$\mathbf{Z}\to Z_2$是正则满同态。则诱导映射$\bar{\pi}$：$\mathrm{Hom}\ (Z_2,\ \mathbf{Z})\to\mathrm{Hom}(Z_2,\ Z_2)$是零映射。由于$\mathrm{Hom}(Z_2,\ Z_2)\neq 0$（练习1$(b)$），从而$\bar{\pi}$不是满同态。

4. 设R，S为环，A_R，${}_SB_R$，${}_SC_R$，D_R如课文中所示。以Hom_R表示全体右R-模同态所组成的集合。

(a) $\mathrm{Hom}_R\ (A,\ B)$是左S-模，其中S的作用为$(sf)(a)=s(f(a))$。

(b) 如果φ：$A\to A'$是右R-模同态，则诱导映射$\bar{\varphi}$：$\mathrm{Hom}_R\ (A',\ B)\to\mathrm{Hom}_R\ (A,\ B)$是左$S$-模同态。

(c) $\mathrm{Hom}_R\ (C,\ D)$是右S-模，其中S的作用为$(gs)(c)=g(sc)$。

(d) 如果ψ：$D\to D'$是右R-模同态，则$\bar{\psi}$：$\mathrm{Hom}_R(C,\ D)\to\mathrm{Hom}_R(C,\ D')$是右$S$-模同态。

5. 设R是含幺环，则有环同构$\mathrm{Hom}_R(R,\ R)\cong R^{op}$，其中$\mathrm{Hom}_R$表示左$R$-模同态（见习题III.1.17和1.7）。特别地，如果R是交换环，则有环同构$\mathrm{Hom}_R(R,\ R)\cong R$。

6. 设S是体上向量空间V的一个非空子集合，S的零化子是V^*的子集$S^0=\{f\in V^*\mid \langle s,\ f\rangle=0$，对于每个$s\in S\}$。

(a) $0^0=V^*$，$V^0=0$；$S\neq\{0\}\Rightarrow S^0\neq V^*$。

(b) 如果W为V的子空间，则W^0是V^*的子空间。

(c) 如果W是V的子空间并且$\dim V$有限，则$\dim W^0=\dim V-\dim W$。

(d) 设W和V如(c)中所示。则存在同构$W^*\cong V^*/W^0$。

(e) 设W和V如(c)中所示。并且在定理4.12的同构θ之下将V等同于

V^{**}，则$(W^0)^0 = W \subset V^{**}$。

7. 如果V是体上的向量空间而$f \in V^*$，令$W = \{a \in V \mid \langle a, f\rangle = 0\}$，则$W$是$V$的子空间，如果$\dim V$是有限的，那末$\dim W$是多少？

8. 如果R是含幺环，我们以${}_RR$和R_R分别表示左R-模R和右R-模R。则$({}_RR)^* = R_R$，$(R_R)^* = {}_RR$。

9. 对于每个左R-模同态f：$A \to B$，图表

$$\begin{array}{ccc} A & \xrightarrow{\theta_A} & A^{**} \\ f\downarrow & & \downarrow f^* \\ B & \xrightarrow{\theta_B} & B^{**} \end{array}$$

均是交换的，其中θ_A和θ_B如定理4.12所示，f^*是指映射$\bar{f}$：$\mathrm{Hom}_R(B, R) \to \mathrm{Hom}_R(A, R)$在$A^{**} = \mathrm{Hom}_R(\mathrm{Hom}_R(A, R), R)$上所诱导的映射。

10. 设$F = \sum_{x \in X} \mathbf{Z}x$是自由$\mathbf{Z}$-模，其中$X$是一组无限基。则$\{f_x \mid x \in X\}$（定理4.11）不形成$F^*$的基〔提示：由定理4.7和4.9可知$F^* \cong \prod_{x \in X} \mathbf{Z}x$。但是在这个同构之下$f_x \longmapsto \{\delta_{x,y}\} \in \sum_{x \in X} \mathbf{Z}x$。〕。

注：$F^* = \prod_{x \in X} \mathbf{Z}x$不是自由$\mathbf{Z}$-模。见L.Fuchs〔13；第168页〕。

11. 如果R是含幺环而P是有限生成的幺作用投射左R-模，则

(a) P^*是有限生成的投射右R-模。

(b) P是反射模。

如果去掉“有限生成”一词，则此命题不再成立。见习题10。

12. 设F是域，X为无限集合，V是集合X上的自由左F-模（向量空间）。令F^X表示全体函数f：$X \to F$所形成的集合。

(a) F^X是F上的(右)向量空间，其中

$(f+g)(x) = f(x) + g(x)$；$(fr)(x) = rf(x))$。

(b) 存在向量空间同构$V^* \cong F^X$.

(c) $\dim_F F^X = |F|^{|X|}$ (见引论中的习题8.10).

(d) $\dim_F V^* > \dim_F V$ 〔提示：由引论中的习题 8.10 和定理 8.10 可知 $\dim_F V^* = \dim_F F^X = |F|^{|X|} \geqslant 2^{|X|} = |P(X)| > |X| = \dim_F V$.〕

5. 张量积

环R上的模A_R和${}_RB$的张量积$A \otimes_R B$是一个Abel群. 它在多线性代数中起着重要作用. 将张量积$A \otimes_R B$看成是某个范畴中的泛对象常常是很有益的 (定理5.2). 另一方面，也经常将$A \otimes_R B$看成是$\mathrm{Hom}_R(A, B)$的某种对偶记号. 我们现在着手作这些事情，即考虑如下几件事情：$A \otimes_R B$的诱导映射与模结构的关系，张量积与正合序列以及直和有关的一些性质.

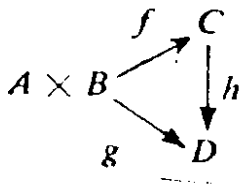
如果A_R和${}_RB$是环R上的模，C是（加法）Abel群，则从$A \times B$到C的准线性映射是满足下列条件的函数$f: A \times B \to C$，对于每个$a, a_i \in A$, $b, b_i \in B$和$r \in R$,

$$f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b) \tag{3}$$

$$f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2) \tag{4}$$

$$f(ar, b) = f(a, rb). \tag{5}$$

对于固定的A_R, ${}_RB$，考虑如下的范畴$\mathcal{M}(A, B)$：其对象集合是$A \times B$上的全体准线性映射，而$\mathcal{M}(A, B)$中从准线性映射$f: A \times B \to C$到准线性映射$g: A \times B \to D$的态射定义为群同态$h: C \to D$，使得图表



是交换的。验证$\mathcal{M}(A, B)$是范畴，1_C是从f到f的恒等态射。h是$\mathcal{M}(A, B)$中的等价$\Longleftrightarrow h$是群同构。我们在定理5.2中要构作范畴$\mathcal{M}(A, B)$中的泛对象(见定义I.7.9)。但首先我们需要

定义5.1 设A是环R上左模而B是右R-模。F是集合$A\times B$上的自由 Abel 群。令K是由下列形式的元素全体所生成的F的子群(对每个$a, a'\in A, b, b'\in B, r\in R$)：

(i) $(a+a', b)-(a, b)-(a', b)$;

(ii) $(a, b+b')-(a, b)-(a, b')$;

(iii) $(ar, b)-(a, rb)$.

商群F/K叫作A和B的张量积，并且表示成$A\otimes_R B$ ($R=\mathbf{Z}$时也简记成$A\otimes B$)。F中元素(a, b)的陪集$(a, b)+K$表示成$a\otimes b$。$(0, 0)$的陪集表示成0。

由于F是由集合$A\times B$所生成的，从而商群$F/K=A\otimes_R B$是由全体形如$a\otimes b$ ($a\in A$, $b\in B$)的元素(陪集)所生成。但并不是$A\otimes_R B$中每个元素都具有形式$a\otimes b$(习题4)。F中每个元素都可写成有限和$\sum_{i=1}^{r} n_i(a_i, b_i)$ ($n_i\in\mathbf{Z}$, $a_i\in A$, $b_i\in B$)，从而它在$A\otimes_R B=F/K$中的陪集具有形式$\sum_{i=1}^{r} n_i(a_i\otimes b_i)$。此外，由于每个陪集可以选取不同的代表元素，因此可能在$A\otimes_R B$中$a\otimes b=a'\otimes b'$但是$a\neq a'$, $b\neq b'$(习题4)。还可能在$A\neq 0$并且$B\neq 0$的时候$A\otimes_R B=0$(习题3)。

由定义5.1可知$A\otimes_R B$的生成元$a\otimes b$之间满足下面的关系(对于所有$a, a_i\in A, b, b_i\in B, r\in R$)：

$$(a_1+a_2)\otimes b=a_1\otimes b+a_2\otimes b; \tag{6}$$

$$a\otimes(b_1+b_2)=a\otimes b_1+a\otimes b_2; \tag{7}$$

$$xr\otimes b=a\otimes rb. \tag{8}$$

这些事实均可以直接证明。例如：由于$(a_1+a_2,\ b)-(a_1,\ b)-(a_2,\ b)\in K$，即是“零陪集”中的元素，从而

$$[(a_1+a_2,\ b)+K]-[(a_1,\ b)+K]-[(a_2,\ b)+K]=K$$

或者用符号$(a,\ b)+k=a\otimes b$，即知

$$(a_1+a_2)\otimes b-a_1\otimes b-a_2\otimes b=0.$$

事实上，$A\otimes_R B$的另一种定义方式即是：它是Abel群，其生成元集合是全体符号$a\otimes b(a\in A,\ b\in B)$，而且有生成关系(6)—(8)。此外，由于0是群中唯一满足$x+x=x$的元素，不难看出，对于每个$a\in A,\ b\in B$：

$$a\otimes 0=0\otimes b=0\otimes 0=0.$$

给了环R上的模A_R和${}_RB$，不难验证映射

$$i:\ A\times B\to A\otimes_R B,\ (a,\ b)\mapsto a\otimes b$$

是准线性映射，它叫作正则准线性映射。它的重要性在于

定理5.2 假设A_R和${}_RB$是环R上的模，C是Abel群。如果g：$A\times B\to C$是准线性映射，则存在唯一的群同态$\bar{g}$：$A\otimes_R B\to C$，使得$\bar{g}\,i=g$，其中i：$A\times B\to A\otimes_R B$是正则准线性映射。并且若不计同构，则$A\otimes_R B$由此性质所唯一决定。换句话说，在全体$A\times B$上准线性映射所组成的范畴$\mathcal{M}(A,\ B)$中，$i$：$A\times B\to A\otimes_R B$是泛对象。

证明概要 设F是集合$A\times B$上的自由Abel群，K是定义5.1中所描述的子群。由于F是自由群，由定理2.1(iv)可知$(a,\ b)\mapsto g(a,\ b)\in C$唯一决定一个同态$g_1$：$F\to C$。利用$g$是准线性映射可证$g_1$将$K$的每个生成元都映到零元素，从而$K\subset\ker g_1$。由定理1.7，

g_1诱导出同态$\bar{g}$：$F/K\to C$，使得$\bar{g}[(a,b)+K]=g_1[(a,b)]=g(a,b)$。但是$F/K=A\otimes_R B$，$(a,b)+K=a\otimes b$。因此$\bar{g}$：$A\otimes_R B\to C$是同态，使得$\bar{g}\,i(a,b)=\bar{g}\,(a\otimes b)=g(a,b)$（对每个$(a,b)\in A\times B$），即$\bar{g}\,i=g$。如果又有同态$h$：$A\otimes_R B\to C$使得$hi=g$，则对于$A\otimes_R B$的每个生成元$a\otimes b$，

$$h(a\otimes b)=hi(a,b)=g(a,b)=\bar{g}\,i(a,b)=\bar{g}\,(a\otimes b).$$

即同态h和$\bar{g}$在$A\otimes_R B$的生成元集合上一致，从而必然$h=\bar{g}$，即$\bar{g}$是唯一的。这就表明i：$A\times B\to A\otimes_R B$是范畴$\mathscr{M}(A,B)$中的泛对象。因此由定理I.7.10可知不计同构（等价）$A\otimes_R B$由此唯一决定。∎

系5.3 如果A_R，A'_R，${}_RB$，${}_RB'$均是环R上的模，f：$A\to A'$，g：$B\to B'$是R-模同态，则存在唯一的群同态$A\otimes_R B\to A'\otimes_R B'$，使得对每个$a\in A$，$b\in B$，$a\otimes b\mapsto f(a)\otimes g(b)$。

证明概要 证明$(a,b)\longmapsto f(a)\otimes g(b)$定义了一个准线性映射$h$：$A\times B\to C=A'\otimes_R B'$。由定理5.3可知存在唯一的同态$\bar{h}$：$A\otimes_R B\to A'\otimes_R B'$，使得对每个$a\in A$和$b\in B$，$\bar{h}\,(a\otimes b)=\bar{h}i(a,b)=h(a,b)=f(a)\otimes g(b)$。∎

系5.3中的那个唯一决定的同态表示成$f\otimes g$：$A\otimes_R B\to A'\otimes_R B'$。如果$f'$：$A'_R\to A''_R$和$g'$：${}_RB'\to {}_RB''$也是$R$-模同态，不难证明

$$(f'\otimes g')(f\otimes g)=(f'f\otimes g'g)\text{：}A\otimes_R B\to A''\otimes_R B''.$$

由此即可推出：如果f和g均是R-模同构，则$f\otimes g$是群同构，并且其逆是$f^{-1}\otimes g^{-1}$。

命题5.4 如果$A\xrightarrow{f}B\xrightarrow{g}C\to 0$是环$R$上左模的正合序列，而$D$是右$R$-模，则

$$D\otimes_R A\xrightarrow{1_D\otimes f} D\otimes_R B\xrightarrow{1_D\otimes g} D\otimes_R C\to 0$$

是Abel群的正合序列。(类似地，

$$A\otimes_R D\xrightarrow{f\otimes 1_D} B\otimes_R D\xrightarrow{g\otimes 1_D} C\otimes_R D\to 0$$

也是Abel群的正合序列。)

证明 我们需要证明：(i) $\mathrm{Im}(1_D\otimes g)=D\otimes_R C$；(ii) $\mathrm{Im}(1_D\otimes f)\subset\mathrm{Ker}(1_D\otimes g)$；(iii) $\mathrm{Ker}(1_D\otimes g)\subset\mathrm{Im}(1_D\otimes f)$。

(i) 根据假设g是满同态，从而$D\otimes_R C$中每个元素$d\otimes c$均有形式$d\otimes g(b)=(1_D\otimes g)(d\otimes b)$，$b\in B$。因此$\mathrm{Im}(1_D\otimes g)$包含 $D\otimes_R C$的所有生成元素。从而$\mathrm{Im}(1_D\otimes g)=D\otimes_R C$。

(ii) 由于$\mathrm{Ker}g=\mathrm{Im}f$，从而$gf=0$，于是$(1_D\otimes g)(1_D\otimes f)=1_D\otimes gf=1_D\otimes 0=0$，从而$\mathrm{Im}(1_D\otimes f)\subset\mathrm{Ker}(1_D\otimes g)$。

(iii) 令π：$D\otimes_R B\to(D\otimes_R B)/\mathrm{Im}(1_D\otimes f)$是正则满同态。由(ii)和定理1.7可知存在同态$\alpha$:$(D\otimes_R B)/\mathrm{Im}(1_D\otimes f)\to D\otimes_R C$,使得$\alpha(\pi(d\otimes b))=(1_D\otimes g)(d\otimes b)=d\otimes g(b)$.我们要证明$\alpha$是同构。由此及定理1.7可以推出$\mathrm{Ker}(1_D\otimes g)=\mathrm{Im}(1_D\otimes f)$,从而完成了证明。

首先证明映射

β：$D\times C\to(D\otimes_R B)/\mathrm{Im}(1_D\otimes f)$，$(d,\ c)\longmapsto\pi(d\otimes b)$，(其中$g(b)=c$)与$b$ 的选取无关。(由于g是满同态，从而至少存在一个这样的b。)如果$g(b')=c$，则$g(b-b')=0$，从而 $b-b'\in\mathrm{Ker}g=\mathrm{Im}f$，因此有$a\in A$，使得$b-b'=f(a)$。由于 $d\otimes f(a)\in\mathrm{Im}(1_D\otimes f)$，$\pi(d\otimes f(a))=0$。从而

$$\pi(d\otimes b)=\pi(d\otimes(b'+f(a)))=\pi(d\otimes b'+d\otimes f(a))$$
$$=\pi(d\otimes b')+\pi(d\otimes f(a))=\pi(d\otimes b').$$

所以β是可定义的，验证β是准线性映射。于是由定理5.2可知存在唯一的同态$\bar{\beta}$：$D\otimes_R C\to(D\otimes_R B)/\mathrm{Im}(1_D\otimes f)$，使得 $\bar{\beta}(d\otimes c)$

$= \bar{\beta} i(d, c) = \beta(d,c) = \pi(d \otimes c)$，其中$g(b) = c$。所以对于$D \otimes_R C$的每个生成元素$d \otimes c$，$\alpha\bar{\beta}(d \otimes c) = \alpha(\pi(d \otimes b)) = d \otimes g(b) = d \otimes c$，因此$\alpha\bar{\beta}$为恒等映射。类似地可证$\bar{\beta}\alpha$也是恒等映射，从而$\alpha$是同构。■

注记：如果$h: A_R \to A'_R$，$k: {}_RB \to {}_RB'$是模的满同态，则由命题5.4可知$1_A \otimes k$和$h \otimes 1_B$均是群的满同态。由于$h \otimes k = (1_{A'} \otimes k)(h \otimes 1_B)$，因此$h \otimes k: A \otimes_R B \to A' \otimes_R B'$也是满同态。但是如果$h$和$k$是单同态，则$h \otimes 1_B$和$1_A \otimes k$不必为单同态（习题7）。

定理5.5 设R和S是环，记号${}_SA_R$，${}_RB$，C_R，和${}_RD_S$如前所示。则

(i) $A \otimes_R B$是左S-模，其中$s(a \otimes b) = sa \otimes b (s \in S, a \in A, b \in B)$。

(ii) 如果$f: A \to A'$是S-R双重模的同态，$g: B \to B'$是R-模同态，则诱导映射$f \otimes g: A \otimes_R B \to A' \otimes_R B'$是左$S$-模的同态。

(iii) $C \otimes_R D$是右S-模，其中$(c \otimes d)s = c \otimes ds (s \in S, c \in C, d \in D)$。

(iv) 如果$h: C \to C'$是R-模同态，$k: D \to D'$是R—S双重模同态，则诱导映射$h \otimes k: C \otimes_R D \to C' \otimes_R D'$是右$S$-模同态。

证明概要 (i) 对于每个$s \in S$，映射

$$A \times B \to A \otimes_R B, \quad (a, b) \longmapsto sa \otimes b$$

是R-准线性映射，从而诱导出唯一的群同态$\alpha s: A \otimes_R B \to A \otimes_R B$，使得$\alpha s(a \otimes b) = sa \otimes b$。对于每个元素$u = \sum_{i=1}^{n} a_i \otimes b_i \in A \otimes_R B$，定义$su$为元素$\alpha_s(u) = \sum_{i=1}^{n} \alpha_s(a_i \otimes b_i) = \sum_{i=1}^{n} sa_i \otimes b_i$。由于$\alpha_s$是同态，

从而S的这个作用是可定义的（即与u写成生成元之和的方式无关）。现在不难验证$A\otimes_R B$是左S-模。■

注记：定理5.5的一个重要特例为：R是交换环，这时每个R-模A均是R-R双重模，其中$ra=ar(r\in R,\ a\in A)$。这时$A\otimes_R B$也是R-R双重模，其中$r(a\otimes b)=ra\otimes b=a\otimes rb=a\otimes br=(a\otimes b)r$ $(r\in R,\ a\in A,\ b\in B)$。

如果R是交换环，则R-模的张量积还可以用将定理5.2稍加修改的一种有益的形式来刻划。设A，B，C是交换环R上的模。从$A\times B$到C的双线性映射是函数f：$A\times B\to C$，使得对于每个a，$a_i\in A$，b，$b_i\in B$，$r\in R$，

$$f(a_1+a_2,\ b)=f(a_1,\ b)+f(a_2,\ b) \tag{9}$$

$$f(a,\ b_1+b_2)=f(a,\ b_1)+f(a,\ b_2) \tag{10}$$

$$f(ra,\ b)=rf(a,\ b)=f(a,\ rb) \tag{11}$$

条件(9)和(10)就是(3)和(4)，由(11)显然推出前面的(5)，从而每个双线性映射都是准线性映射。

例 如果A^*是交换环R上模A的对偶，则映射$A\times A^*\to R$，$(a,\ f)\longmapsto f(a)=\langle a,\ f\rangle$是双线性的。

例 如果A和B是交换环R上的模，则$A\otimes_R B$也是R-模，并且不难看出，正则准线性映射i：$A\times B\to A\otimes_R B$是双线性的；这时$i$叫作正则双线性映射。

定理5.6 如果A、B、C是交换环R上的模，g：$A\times B\to C$是双线性映射，则存在唯一的R-模同态$\bar{g}$：$A\otimes_R B\to C$，使得$\bar{g}i=g$，其中i：$A\times B\to A\otimes_R B$是正则双线性映射。并且若不计同构，则模$A\otimes_R B$由这一性质所唯一确定。

证明概要 验证由定理5.2给出的Abel群的唯一同态$\bar{g}$：$A\otimes$

${}_RB\to C$实际上是R-模同态。为证定理最后论断，令$\mathscr{B}(A,B)$是$A\times B$上全体双线性映射所形成的范畴（即在$\mathscr{M}(A,B)$的定义中将群C，D和群同态h：$C\to D$分别改成模和模同态）。于是由本定理第一部分已证出i：$A\times B\to A\otimes_R B$是$\mathscr{B}(A,B)$中的泛对象，从而由定理I.7.10可知$A\otimes_R B$不计同构是唯一确定的。∎

当R是含幺交换环的时候，定理5.6提供出定义$A\otimes_R B$的另一种方式：令F_1是集合$A\times B$上的自由R-模，而K_1是由下列形式的全部元素所生成的子模：

$$(a+a',\ b)-(a,\ b)-(a',\ b);$$

$$(a,\ b+b')-(a,\ b)-(a,\ b');$$

$$(ra,\ b)-r(a,\ b);$$

$$(a,\ rb)-r(a,\ b).$$

其中a，$a'\in A$，b，$b'\in B$，$r\in R$（比较定义5.1）。我们断言：存在R-模同构$A\otimes_R B\cong F_1/K_1$。模仿定理5.2的证明即知映射$A\times B\to F_1/K_1$，$(a,\ b)\longmapsto 1_R(a,\ b)+K_1$是范畴$\mathscr{B}(A,\ B)$中的泛对象。于是由定理5.6可知$A\otimes_R B\cong F_1/K_1$。

现在我们回到任意环上的模。

定理5.7 如果R是含幺环，A_R和${}_RB$均是幺作用R-模，则有R-模同构

$$A\otimes_R R\cong A,\quad R\otimes_R B\cong B.$$

证明概要 由于R是R-R双重模，由定理5.5可知$R\otimes_R B$是左R-模。$(r,\ b)\longmapsto rb$给出一个准线性映射$R\times B\to B$。由定理5.2可知存在群同态α：$R\otimes_R B\to B$，使得$\alpha(r\otimes b)=rb$。验证α事实上是左R-模的同态。然后验证映射β：$B\to R\otimes_R B$，$b\longmapsto 1_R\otimes b$是$R$-模同态，并且$\alpha\beta=1_B$，$\beta\alpha=1_R\otimes_{R}{}_B$。于是$\alpha$：$R\otimes_R B\cong B$。类似地

构作同构$A\otimes_R R\cong A$。 ∎

如果R和S是环，A_R，${}_RB_S$，${}_SC$是（双重）模，则由定理 5.5 知$A\otimes_R B$是右S-模而$B\otimes_S C$是左R-模，从而可以定义Abel群$(A\otimes_R B)\otimes_S C$和$A\otimes_R(B\otimes_S C)$。

定理5.8 如果R和S是环而 A_R，${}_RB_S$，${}_SC$是（双 重）模，则有同构

$$(A\otimes_R B)\otimes_S C\cong A\otimes_R(B\otimes_S C).$$

证明 根据定义，$(A\otimes_R B)\otimes_S C$中每个元素v是有限和$\sum_{i=1}^{n} u_i\otimes c_i$($u_i\in A\otimes_R B$，$c_i\in C$)。而每个$u_i\in A\otimes_R B$又是有限和$\sum_{j=1}^{m_i} a_{ij}\otimes b_{ij}$($a_{ij}\in A$，$b_{ij}\in B$)，于是我们有

$$v=\sum_i u_i\otimes c_i=\sum_i\Big(\sum_j a_{ij}\otimes b_{ij}\Big)\otimes c_i=\sum_i\sum_j[(a_{ij}\otimes b_{ij})\otimes c_i].$$

从而$(A\otimes_R B)\otimes_S C$是由集合 $\{(a\otimes b)\otimes c\mid a\in A,\ b\in B,\ c\in C\}$所生成的。类似地，$A\otimes_R(B\otimes_S C)$是由集合$\{a\otimes(b\otimes c)\mid a\in A,\ b\in B,\ c\in C\}$所生成的。验证$\Big(\sum_{i=1}^{n} a_i\otimes b_i,\ c\Big)\longmapsto\sum_{i=1}^{n}[a_i\otimes(b_i\otimes c)]$定义出一个$S$-准线性映射 $(A\otimes_R B)\times C\to A\otimes_R(B\otimes_S C)$。从而由定理5.2可知存在同态

$$\alpha:\ (A\otimes_R B)\otimes_S C\to A\otimes_R(B\otimes_S C).$$

使得$\alpha[(a\otimes b)\otimes c]=a\otimes(b\otimes c)(a\in A,\ b\in B,\ c\in C)$。类似地，存在$R$-准线性映射$A\times(B\otimes_S C)\to(A\otimes_R B)\otimes_S C$，它诱导出同态

$$\beta:\ A\otimes_R(B\otimes_S C)\to(A\otimes_R B)\otimes_S C.$$

使得$\beta[a\otimes(b\otimes c)]=(a\otimes b)\otimes c$　　$(a\in A,\ b\in B,\ c\in C)$。对于$(A\otimes_R B)\otimes_S C$的每个生成元素$(a\otimes b)\otimes c$，$\beta\alpha[(a\otimes b)\otimes c]=(a\otimes b)\otimes c$，从而$\beta\alpha$是$(A\otimes_R B)\otimes_S C$上的恒等映射。类似地可以推出$\alpha\beta$是$A\otimes_R(B\otimes_S C)$上的恒等映射。从而$\alpha$和$\beta$均是同构。∎

在定理5.8的同构之下，今后我们将$(A\otimes_R B)\otimes_S C$等同于$A\otimes_R(B\otimes_S C)$。现在可以递归地定义$n$重张量积：

$$A'\otimes_{R_1}A^2\otimes_{R_2}\otimes\cdots\otimes_{R_n}A^{n+1},$$

其中R_1，$\cdots R_n$是环，而A'_{R_1}，${}_{R_1}A^2{}_{R_2}$，$\cdots$，${}_{R_n}A^{n+1}$是(双重)模。这种递归定义的张量积还可以用泛n重线性映射来刻划(习题10)。

定理5.9　设R是环，A和$\{A_i\mid i\in I\}$均是右R-模，B和$\{B_j\mid j\in J\}$均是左R-模。则有群同构

$$\Big(\sum_{i\in I}A_i\Big)\otimes_R B\cong\sum_{i\in I}(A_i\otimes_R B);$$

$$A\otimes_R\Big(\sum_{j\in J}B_j\Big)\cong\sum_{j\in J}(A\otimes_R B_j).$$

证明　令l_k，π_k分别是$\sum_{i\in I}A_i$的正则嵌入和正则射影。由定理I.8.5可知，同态族$l_k\otimes 1_B$：$A_k\otimes_R B\to\Big(\sum_{i\in I}A_i\Big)\otimes_R B$诱导出同态$\alpha$：$\sum_{i\in I}(A_i\otimes_R B)\to\Big(\sum_{i\in I}A_i\Big)\otimes_R B$，使得$\alpha[\{a_i\otimes b\}]=\sum_{i\in I_0}(l_i(a_i)\otimes b)=\Big(\sum_{i\in I_0}l_i(a_i)\Big)\otimes b$，其中$I_0=\{i\in I\mid a_i\otimes b\neq 0\}$。由$(u,\ b)\longmapsto\{\pi_i(u)\otimes b\}_{i\in I}$定义出一个准线性映射$\Big(\sum_{i\in I}A_i\Big)\times B\to\sum_{i\in I}(A_i\otimes_R B)$，它诱导出同态$\beta$：$\Big(\sum A_i\Big)\otimes_R B\to\sum(A_i\otimes_R B)$，使得$\beta(u\otimes b)=\{\pi_i(u)\otimes b\}_{i\in I}$。我们要证明$\alpha\beta$和$\beta\alpha$分别是恒等映射，从而$\alpha$是同构。

如果$u\in\sum A_i$，$I_0=\{i\in I\mid \pi_i(u)\neq 0\}$，

则 $u=\sum_{i\in I_0} l_i\pi_i(u)$。因此对于$(\sum A_i)\otimes_R B$的每个生成元素$u\otimes b$，

$$\alpha\beta(u\otimes b)=\alpha[\{\pi_i(u)\otimes b\}]$$
$$=\Big(\sum_{i\in I_0} l_i\pi_i(u)\Big)\otimes b=u\otimes b.$$

从而$\alpha\beta$是恒等映射。

对于每个$j\in I$，令l_j^*：$A_j\otimes_R B\to\sum_i(A_i\otimes_R B)$是正则嵌入，验证$\sum_i(A_i\otimes_R B)$由$\{l_j^*(a\otimes b)=\{\pi_i l_j(a)\otimes b\}_{i\in I}\mid j\in I, a\in A_j, b\in B\}$所生成。对于每个这样的生成元素，当$i\neq j$时$(\pi_i l_j(a))\otimes b=0$，而$(\pi_j l_j(a))\otimes b=a\otimes b$，于是

$$\beta\alpha[l_j^*(a\otimes b)]=\beta\alpha[\{\pi_i l_j(a)\otimes b\}]$$
$$=\beta[l_j\pi_j l_j(a)\otimes b]=\beta[l_j(a)\otimes b]$$
$$=\{\pi_i l_j(a)\otimes b\}_{i\in I}$$
$$=l_j^*(a\otimes b).$$

从而映射$\beta\alpha$必定是恒等映射。类似地证明第二个同构。∎

定理5.10 （伴随结合性）设R和S是环，A_R，$_RB_S$，C_S为（双重）模。则有Abel群同构：

α：$\mathrm{Hom}_S(A\otimes_R B, C)\cong\mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$。

其中对每个f：$A\otimes_R B\to C$，定义αf为

$$[(\alpha f)(a)](b)=f(a\otimes b).$$

注：$\mathrm{Hom}_R(-,-)$和$\mathrm{Hom}_S(-,-)$均是右模同态集合。而$\mathrm{Hom}_S(B,C)$上的R-模结构是（见习题4.4(c)）：

$$(gr)(b)=g(rb)\quad(r\in R,\ b\in B,\ g\in \mathrm{Hom}_S(B,\ C)).$$

定理5.10的证明概要 证明是利用有关定义的一个直接练习。也就是要检查以下诸项：

(i) 对于每个 $a\in A$，$f\in \mathrm{Hom}_S(A\otimes_R B,\ C)$，$(\alpha f)(a)$：$B\to C$是$S$-模同态。

(ii) (αf)：$A\to \mathrm{Hom}_S(B,\ C)$是$R$-模同态。因此函数$\alpha$是可定义的。

(iii) α是群同态（即$\alpha(f_1+f_2)=\alpha(f_1)+\alpha(f_2)$）。为证$\alpha$是同构，要构作逆映射 β：$\mathrm{Hom}_R(A,\ \mathrm{Hom}_S(B,\ C))\to \mathrm{Hom}_S(A\otimes_R B,\ C)$，它定义为

$(\beta g)(a\otimes b)=[g(a)](b)$，$(a\in A,\ b\in B,\ g\in \mathrm{Hom}_R(A,\ \mathrm{Hom}_S(B,\ C))$。验证：

(iv) 上面在生成元素上定义的βg决定出唯一的S-模同态 $A\otimes_R B\to C$。

(v) β是同态。

(vi) $\beta\alpha$和$\alpha\beta$均为恒等映射。因此α是同构。∎

在本节的最后我们研究自由模的张量积。除了少数几个习题之外，这部份内容只在第IX.6节中用到。

定理5.11 设R是含幺环。如果A是幺作用右R-模而F是以Y为基的自由左R-模，则$A\otimes_R F$中每个元素u均可唯一地写成形式 $u=\sum_{i=1}^{n} a_i\otimes y_i$，其中$a_i\in A$而$\{y_i\}$是$Y$中两两相异的元素。

注记：给了$u=\sum_{k=1}^{t} a_k\otimes y_k$和 $v=\sum_{j=1}^{m} b_j\otimes z_j$（$a_k$，$b_j\in A$，$y_k$，$z_j\in Y$）。必要时插入一些形如$0\otimes y(y\in Y)$ 的项，可以认为 $u=$

$\sum_{i=1}^{n} a_i\otimes y_i$，$v=\sum_{i=1}^{n} b_i\otimes y_i$。而定理5.11中的“唯一性”一词即指：如果$\sum_{i=1}^{n} a_i\otimes y_i=\sum_{i=1}^{n} b_i\otimes y_i$，则对于每个$i$，$a_i=b_i$。特别地，如果$\sum_{i=1}^{n} a_i\otimes y_i=0=\sum_{i=1}^{n} 0\otimes y_i$，则$a_i=0(1\leqslant i\leqslant n)$。

定理5.11的证明 考虑直和$\sum_{y\in Y} A_y$，其中$A_y\cong A$（对于每个$y\in Y$）。先如下构作同构θ：$A\otimes_R F\cong\sum_{y\in Y} A_y$：由于Y是一组基，可知对于每个$y\in Y$，$\{y\}$是线性无关集合。从而$R$-模满同态$\varphi$：$R\to Ry$，$r\longmapsto ry$（定理1.5）事实上是同构。因此由定理5.7可知，对于每个$y\in Y$，有同构

$$A\otimes_R Ry\xrightarrow{I_A\otimes\varphi^{-1}}A\otimes_R R\cong A=A_y,$$

于是由定理5.9和I.8.10便知存在同构

$$\theta:\ A\otimes_R F=A\otimes_R\Big(\sum_{y\in Y} Ry\Big)\cong\sum_{y\in Y} A\otimes_R Ry\cong\sum_{y\in Y} A_y.$$

验证对于每个$a\in A$，$z\in Y$，$\theta(a\otimes z)=\{u_y\}\in\sum A_y$，其中$u_z=a$而$y\neq z$时$u_y=0$。换句话说，$\theta(a\otimes z)=l_z(a)$，其中$l_z$：$A_z\to\sum A$是正则嵌入。现在每个非零元素$v\in\sum A$，均是有限和$v=l_{y_1}(a_1)+\cdots+l_{y_n}(a_n)=\theta(a_1\otimes y_1)+\cdots+\theta(a_n\otimes y_n)$，其中$y_1$，…，$y_n$为Y中不同的元素而$a_i$是$A$中唯一确定的非零元素。从而$A\otimes_R F$中每个元素（它必然是$\theta^{-1}(v)$，其中$v$为$\sum A$，中某个元素）均可唯一地写成$\sum_{i=1}^{n} a_i\otimes y_i$。∎

系5.12 如果R是含幺环，A_R和${}_RB$分别是以X和Y为基的自

由R-模，则$A\otimes_R B$是以$W=\{x\otimes y\mid x\in X,\ y\in Y\}$为基的自由(右)$R$-模。($W$的势为$|X||Y|$)

注记：由于R是R-R双重模，从而一些R的直和也是R-R双重模。特别地，每个自由左R-模也是自由右R-模并且反过来也是对的。但是一般来说，自由（左）R-模不是R-R双重模范畴中的自由对象（习题12)。

系5.12的证明概要 根据定理5.11的证明和定理2.1（对于右R-模）可知，存在群同构

$$\theta:\ A\otimes_R B\cong\sum_{y\in Y}A_y=\sum_{y\in Y}A=\sum_{y\in Y}\Big(\sum_{x\in X}xR\Big).$$

根据上面的注记可知B是R-R双重模，从而由定理5.5可知$A\otimes_R B$是右R-模。验证θ是右R-模同构，并且$\theta(W)$是自由右R-模$\sum_Y(\sum_X xR)$的一组基。因此$A\otimes_R B$是以W为基的自由右R-模。由定理5.11知W中元素是两两相异的，从而$|W|=|X||Y|$。∎

系5.13 设S是含幺环，R是S的子环并且$1_S\in R$。如果F是以X为基的自由左R-模，则$S\otimes_R F$是以$\{1_S\otimes x\mid x\in X\}$（势是$|X|$）为基的自由左$S$-模。

证明概要 S显然是S-R双重模，从而由定理5.5可知$S\otimes_R F$是左S-模。从定理5.11的证明可知有群同构$\theta:\ S\otimes_R F\cong\sum_{x\in X}S_x$，其中每个$S_x$均是$S$。此外，如果对于$z\in X$，令$\iota_z:\ S=S_z\to\sum_{x\in X}S_x$是正则嵌入，则对每个$z\in X$，$\theta(1_S\otimes z)=\iota_z(1_S)$。验证$\theta$事实上是左$S$-模同构。显然$\{\iota_x(1_S)\mid x\in X\}$（势为$|X|$）是自由左$S$-模$\sum_{x\in X}S_x$

的一组基，从而$S\otimes_R F$是以$\{1_S\otimes x \mid x\in X\}$（势是$|X|$）为基的自由$S$-模。 ∎

习　题

注：R是环。$\otimes$为$\otimes_Z$

1. 如果$R=\mathbf{Z}$，则定义5.1中的条件(iii)是多余的(即由(i)和(ii)可以推出(iii))。

2. 设A和B是Abel群。

   (a) 对于每个$m>0$，$A\otimes Z_m\cong A/mA$。

   (b) $Z_m\otimes Z_n\cong Z_c$，其中$c=(m,n)$。

   (c) 刻划$A\otimes B$，其中A和B均是有限生成Abel群。

3. 如果A是扭Abel群，$\mathbf{Q}$是有理数(加法)群，则

   (a) $A\otimes\mathbf{Q}=0$。

   (b) $\mathbf{Q}\otimes\mathbf{Q}=\mathbf{Q}$。

4. 给出例子表明以下论述是可能发生的（对适当的环R和模A_R，$_RB$）。

   (a) $A\otimes_R B\neq A\otimes_Z B$。

   (b) $u\in A\otimes_R B$，但是$u\neq a\otimes b$（对任意$a\in A$，$b\in B$）。

   (c) $a\otimes b=a_1\otimes b_1$，但是$a\neq a_1$，$b\neq b_1$。

5. 如果A'是右R-模A的子模，B'是左R-模B的子模，则$A/A'\otimes_R B/B'\cong(A\otimes_R B)/C$，其中$C$是由$\{a'\otimes b,\ a\otimes b' \mid a\in A,\ a'\in A',\ b\in B,\ b'\in B'\}$所生成的$A\otimes_R B$的子群。

6. 令$f:\ A_R\to A'_R$，$g:\ {}_RB\to {}_RB'$是R-模同态，试问由系5.3给出的同态$f\otimes g$和Abel群张量积

$$\mathrm{Hom}_R(A,\ A')\otimes\mathrm{Hom}_R(B,\ B')$$

   中元素$f\otimes g$有什么不同？

7. 通常的单射$\alpha:Z_2\to Z_4$是Abel群的单同态。证明$1\otimes\alpha:\ Z_2\otimes Z_2\to Z_2\otimes Z_4$是零映射（但是$Z_2\otimes Z_2\neq 0$，$Z_2\otimes Z_4\neq 0$，见习题2）。

8. 设 $0\longrightarrow A\xrightarrow{f}B\xrightarrow{g}C\longrightarrow 0$是左$R$-模的短正合序列，$D$是右$R$-模。则只要下列条件有一条成立，$0\longrightarrow D\otimes_R A\xrightarrow{1_D\otimes f} D\otimes_R B\xrightarrow{1_D\otimes g} D\otimes_R C\longrightarrow 0$便也是正合序列。

(a) $0\longrightarrow A\xrightarrow{f}B\xrightarrow{g}C\longrightarrow 0$是分裂正合序列。

(b) R是含幺环而D是自由右R-模。

(c) R是含幺环而D是投射幺作用右R-模。

9. (a) 如果I是含幺环R的右理想，B是左R-模，则有群同构 $R/I\otimes_R B\cong B/IB$，其中IB是由$\{rb\mid r\in I,\ b\in B\}$生成的$B$的子群。

(b) 如果R是交换环而I，J是它的理想，则有R-模同构 $R/I\otimes_R R/J\cong R/(I+J)$。

10. 如果R和S是环，${}_RA$，${}_RB_S$，${}_SC$是（双重）模，D是 Abel群，定义准线性映射为满足下列诸条件的函数f：$A\times B\times C\longrightarrow D$。

(i) $f(a+a',\ b,\ c)=f(a,\ b,\ c)+f(a',\ b,\ c)$；

(ii) $f(a,\ b+b',\ c)=f(a,\ b,\ c)+f(a,\ b',\ c)$；

(iii) $f(a,\ b,\ c+c')=f(a,\ b,\ c)+f(a,\ b,\ c')$；

(iv) $f(ar,\ b,\ c)=f(a,\ rb,\ c)\quad (r\in R)$；

(v) $f(a,\ bs,\ c)=f(a,\ b,\ sc)\quad (s\in S)$。

求证：

(a) 映射i：$A\times B\times C\longrightarrow (A\otimes_R B)\otimes_S C$，$(a,\ b,\ c)\longmapsto (a\otimes b)\otimes c$是准线性映射。

(b) 准线性映射 i 是泛映射。即给了准线性映射g：$A\times B\times C\longrightarrow D$，存在唯一的群同态$\overline{g}$：$(A\otimes_R B)\otimes_S C\longrightarrow D$，使得$\overline{g}i=g$。

(c) 映射j：$A\times B\times C\longrightarrow A\otimes_R(B\otimes_S C)$，$(a,\ b,\ c)\longmapsto a\otimes(b\otimes c)$也是准线性的泛映射。

(d) 由(b)，(c)和定理I.7.10可证$(A\otimes_R B)\otimes_S C\cong A\otimes_R(E\otimes_S C)$。

(e) 以显然的方式在n个（双重）模（$n\geqslant 4$）上定义准线性函数，并简要叙述如何把上面结果推广到（在$n-1$个环上）n个（双重）模的情形。

(f) 如果$R=S$，R是交换环，而A，B，C，D均是R-模，定义三重线性映射$A\times B\times C\longrightarrow D$，并且将(a)，(b)和(c)中的结果推广到这种映射上来。

11. 令A，B，C是交换环R上的模。则

(a) 集合$\mathscr{L}(A, B; C)=\{$全体R-双线性映射 $A\times B\to C\}$是R-模，其中$(f+g)(a, b)=f(a, b)+g(a, b)$，$(rf)(a, b)=rf(a, b)$。

(b) 下列几个R-模均同构于$\mathscr{L}(A, B; C)$：

(i) $\mathrm{Hom}_R(A\otimes_R B, C)$；

(ii) $\mathrm{Hom}_R(A, \mathrm{Hom}_R(B, C))$；

(iii) $\mathrm{Hom}_R(B, \mathrm{Hom}_R(A, C))$。

12. 假设R是含幺环。以$\mathscr{C}$表示全体幺作用R-R双重模与双重模同态（即群同态f：$A\to B$满足$f(ras)=rf(a)s$，r，$s\in R$）所构成的范畴。令$X=\{1_R\}$，ι：$X\to R$是包含映射。

(a) 如果R是非交换环，则R（对于ι：$X\to R$）不是范畴$\mathscr{C}$中在集合X上的自由对象。

(b) $R\otimes_Z R$是R-R双重模（定理5.5）。如果ι：$X\to R\otimes_Z R$由$1_R\longmapsto 1_R\otimes 1_R$给出，则在范畴$\mathscr{C}$中$R\otimes_Z R$是集合$X$上的自由对象。

6. 主理想整环上的模

本节主要目的是决定主理想整环上有限生成模的结构，这部分内容只用于第VII.2节和第VII.4节。事实上，有限生成Abel群的所有结构定理（第II.1和II.2节）均可以看作是这种模的结构定理，而且第II.1节和第II.2节中的许多证明均可以直接推广到R-模上，其中R为欧氏整环。但是，为了推广到R是任意主理想整

环的情形，需要将某些证明作相当大的修改。所以我们在这里将使用不同的方式来证明结构定理。与Abel群的情形一样，我们要证明：每个有限生成模均可用两种方式分解为循环子模的直和(定理6.12)。对于一给定的模，每种分解均提供出一个不变量组(即：两个模有同样的不变量组$\Leftrightarrow$它们同构（系6.13))。因此，每一种分解方法都给出主理想整环上有限生成模一个完全的同构分类。在本节中“模”均指的是“幺作用模”

我们从主理想整环R上的自由模开始。由系2.12知R具有不变维数性质，从而可以定义自由R-模的秩(定义2.8)。特别地，两个自由R-模是同构的$\Leftrightarrow$它们有相同的秩(命题2.9)。此外，我们还可以将定理II.1.6作如下的推广。

定理6.1 设F是主理想整环R上的自由模。G是F的子模。则G也是自由R-模并且$\mathrm{rank}G \leqslant \mathrm{rank}F$。

证明概要 设$\{x_i | i \in I\}$是F的一组基。则$F = \sum_{i \in I} Rx_i$，其中每个Rx_i（作为左模）均同构于R。将集合I赋以良序$\leqslant$（引论第7节)。对于每个$i \in I$，i的直接后继表示成$i+1$（引论中习题7.7)。令$J = I \cup \{\alpha\}$，其中$\alpha \notin I$。并且定义$i < \alpha$（对于每个$i \in I$)。于是J也是良序集合，并且I中每个元素在J中均有直接后继。[1]对于每个$j \in J$定义F_j为由集合$\{x_i | i < j\}$生成的F的子模。验证这些子模F_j有下列性质：

(i) $j < k \Longleftrightarrow F_j \subset F_k$;

(ii) $\bigcup_{j \in J} F_j = F$;

[1] 构作集合J的技术上的原因是：I中某个（至多一个）元素在I中可能没有直接后继。例如当I是有限集合的时候就是这样。

(iii) 对于每个$i\in I$，$F_{i+1}/F_i\cong Rx_i\cong R$。

[将定理1.7用于正则射影$F_{i+1}=\sum_{k<i+1}Rx_k\longrightarrow Rx_i$。]

对于每个$j\in J$，令$G_i=G\cap F_j$，验证：

(iv) $j<k\Longrightarrow G_j\subset G_k$；

(v) $\bigcup_{j\in J}G_j=G$；

(vi) 对于每个$i\in I$，$G_i=G_{i+1}\cap F_i$。

由性质(vi)和定理1.9(i)推出$G_{i+1}/G_i=G_{i+1}/(G_{i+1}\cap F_i)\cong(G_{i+1}+F_i)/F_i$。但是$(G_{i+1}+F_i)/F_i$是$F_{i+1}/F_i$的子模。于是由(iii)可知$G_{i+1}/G_i$同构于$R$的子模。但是$R$的每个子模均是$R$的理想，从而有形式$(c)=Rc$，其中$c\in R$。如果$c\neq 0$，则定理1.5(i)中的$R$-模满同态事实上是同构。因此$R$的每个子模（从而每个$G_{i+1}/G_i$）均是自由模，并且秩为0或者1。由定理3.2和3.4可知对于每个$i\in I$，序列$0\to G_i\xrightarrow{\subset}G_{i+1}\longrightarrow G_{i+1}/G_i\longrightarrow 0$是分裂正合的。从而由定理1.18和习题1.15推出每个G_{i+1}都是内直和$G_{i+1}=G_i\oplus Rb_i$，其中$b_i\in G_{i+1}-G_i$。并且如果$G_{i+1}\neq G_i$，则$Rb_i\cong R$，而$G_{i+1}=G_i$时（即$G_{i+1}/G_i=0$时）取$b_i=0$。因此对每个$i\in I$均定义了$b_i\in G$。令$B=\{b_i\mid b_i\neq 0\}$。则$|B|\leqslant|I|=\mathrm{rank}F$。为完成证明，我们只需再证$B$是$G$的一组基。

假设$u=\sum_j r_jb_j=0$（$j\in I$，$r_j\in R$是有限和）。如果r_j不全为零，令k是使$r_k\neq 0$的最大下标。则$u=\sum_{j<k}r_jb_j+r_kb_k\in G_k\oplus Rb_k=G_{k+1}$。如果$u=0$，则$r_k=0$这就导致矛盾。所以对于每个$j$，$r_j$均为零，即$B$是线性无关的。

最后需要证明B张成G。由（v）可知这只需证明：对于每个$k \in J$，B的子集合$B_k = \{b_j \in B \mid j<k\}$张成$G_k$。我们使用超限归纳法（引论中定理7.1）。假设对于所有的$j<k$，B_j张成G_j。令$u \in G_k$。如果有$j \in I$，使$k = j+1$，则$G_k = G_{j+1} = G_j \oplus Rb_j$，而$u = v + rb_j$，$v \in G_j$。由归纳假设知$v$是有限和$v = \sum r_i b_i$，其中$r_i \in R$，$b_i \in B_j \subset B_k$。因此$u = \sum r_i b_i + rb_k$，于是$B_k$张成$G_k$。现在假设对每个$j \in I$，$k \neq j+1$（这种情形可能会发生，见引论中定理7.1前面的例子）。由于$u \in G_k = G \cap F_k$，从而$u = \sum r_j x_j$（有限和），其中$j<k$。令t是使$r_t \neq 0$的最大下标，则$u \in F_{t+1}$，并且根据假设可知$t+1<k$。因此$u \in G \cap F_{t+1} = G_{t+1}$，其中$t+1<k$。由归纳假设可知$u$是$B_{t+1}$中元素的线性组合，而$B_{t+1}$是$B_k$的子集合，从而$B_k$张成$G_k$。∎

系6.2 设R是主理想整环。A是由n个元素生成的R-模。则A的每个子模均可由m个元素生成，其中$m \leqslant n$。

证明作为练习。见系II.1.7和系2.2。 ∎

系6.3 主理想整环上的幺作用模A是自由模 $\Longleftrightarrow$ A是投射模。

证明 （$\Longrightarrow$）：定理3.2。

（$\Longleftarrow$）：存在短正合序列$0 \longrightarrow K \xrightarrow{\subset} F \xrightarrow{f} A \longrightarrow 0$，其中$F$是自由模，$f$为满同态而$K = \ker f$（系2.2）。如果$A$是投射模，由定理3.4可知$F \cong K \oplus A$。于是$A$同构于$F$的一个子模。由定理6.1即知$A$是自由模。 ∎

现在研究群中元素的阶和Abel群的扭子群到模上的推广。

定理6.4 设A是整环R上的左模，对于每个$a \in A$，令$\mathscr{O}_a =$

$\{r\in R|_{ra=0}\}$。

(i) 对于每个$a\in A$，$\mathscr{O}_a$是R的理想。

(ii) $A_t=\{a\in A\mid\mathscr{O}_a\neq 0\}$是$A$的子模。

(iii) 对于每个$a\in A$，有左模同构

$$R/\mathscr{O}_a\cong Ra=\{ra\mid r\in R\}。$$

令R是主理想整环而p是R中元素

(iv) 如果$p^ia=0$（等价地：$(p^i)\subset\mathscr{O}_a$），则$\mathscr{O}_a=(p^j)$，（对某个$j$，$0\leqslant j\leqslant i$）。

(v) 如果$\mathscr{O}_a=(p^i)$，则对于每个$0\leqslant j<i$，$p^ja\neq 0$。

注记：由定理III.3.4可知在主理想整环中，素元和不可约元是等同的概念。

证明概要 (iii)：利用定理1.5(i)和1.7。

(iv)：由假设可知$\mathscr{O}_a=(r)$，$r\in R$。由于$p^i\in\mathscr{O}_a$，从而$r\mid p^i$。由R中唯一因子分解特性（定理III.3.7）可知$r=p^ju$（$0\leqslant j\leqslant i$），并且u是单位。于是$\mathscr{O}_a=(r)=(p^ju)=(p^j)$（定理III.3.2）。

(v)：如果$p^ja=0$，$j<i$。则$p^j\in\mathscr{O}_a=(p^i)$，于是$p^i\mid p^j$而这与$R$中唯一因子分解性质相矛盾。∎

设A是整环上的模。定理6.4中的理想$\mathscr{O}_a$叫作$a\in A$的**零化理想**。定理6.4中的子模A_t叫作A的**扭子模**。如果$A=A_t$，A叫作**扭模**，如果$A_t=0$，则A叫做**无扭模**。每个自由模均是无扭模，但是反过来不对（习题2）。

设A是主理想整环R上的模。$a\in A$的零化理想是R中的主理想，设$\mathscr{O}_a=(r)$，则称a有**阶**r。元素r唯一确定到相差一个单位因子（定理III.3.2）。由a生成的循环子模Ra（定理1.5）叫作r**阶循环子模**。定理6.4(iii)表明，$a\in A$的阶为0（即Ra是0阶循环子模）$\Longleftrightarrow Ra\cong R$（即$Ra$是秩1自由模）。另一方面，$a\in A$有阶$r$

并且r是单位$\Leftrightarrow a=0$（因为$a=1_R a=r^{-1}(ra)=r^{-1}0=0$）。

例 如果R是主理想整环，$r\in R$，则商环$R/(r)$是以$a=1_R+(r)$为生成元的循环R-模。显然$\mathscr{O}_a=(r)$，从而a有阶r而$R/(r)$是r阶循环模。定理6.4(iii)表明，主理想整环R上的每个循环模C均同构于$R/(r)$，其中$(r)=\mathscr{O}_a$，而a是C的生成元。

例 令$R=\mathbb{Z}$。A为（加法）Abel群。假设$a\in A$的群论的阶（定义I.3.3）是有限的。则$\mathscr{O}_a=(n)$，其中$|n|$是a的群论阶。如果$a\in A$有无限阶，则$\mathscr{O}_a=(0)$。不管是哪种情形，$\mathbb{Z}a$均是由a生成的循环子群$\langle a\rangle$（定理I.2.8）。此外，如果$\mathscr{O}_a=(n)$，$n\neq 0$，则$\mathbb{Z}a\cong\mathbb{Z}/(n)\cong Z_n$；如果$\mathscr{O}_a=(0)$，则$\mathbb{Z}a\cong\mathbb{Z}/(0)\cong\mathbb{Z}$。

定理6.5 主理想整环R上的有限生成无扭模A是自由模。

注记："A是有限生成的"这一条件不可缺少（习题II,1.10）。

定理6.5的证明 我们可以假定$A\neq 0$。令X是A的一个由非零生成元素组成的有限集合。如果$x\in X$，则$rx=0$ $(r\in R)\Longleftrightarrow r=0$，这是因为$A$是无扭的。从而$X$具有非空子集$S=\{x_1,\cdots,x_k\}$对于下述性质是极大的：

$r_1x_1+\cdots+r_kx_k=0$ $(r_i\in R)\Longrightarrow r_i=0$（对于每个$i$），由$S$生成的子模$F$显然是以$S$为基的自由$R$-模。如果$y\in X-S$，由极大性可知存在不全为零的$r_*$，$r_1$，$\cdots$，$r_k\in R$，使得$r_*y+r_1x_1+\cdots+r_kx_k=0$。于是$r_*y=-\sum_{i=1}^{k}r_ix_i\in F$。此外我们有$r_*\neq 0$，这是由于若$r_*=0$，则全部$r_i$（$1\leqslant i\leqslant k$）均为零。因为$X$是有限的，从而有非零$r\in R$（即$r=\prod_{y\in X-S}r_*$），使得$rX=\{rx\mid x\in X\}$包含在$F$之中。于是$rA=\{ra\mid a\in A\}\subset F$。不难看出，映射$f$：$A\to A$，$a\longmapsto ra$是$R$-模

同态，其象为rA。由于A是无扭的，从而$\ker f=0$，于是$A\cong \mathrm{Im}f=rA\subset F$。于是由定理6.1可知$A$是自由$R$-模。∎

现在可以把确定主理想整环上有限生成模A的结构这件事情分成三步来作：先证A是扭模与自由模的直和（定理6.6）；再证每个扭模均是一些“p—准素模”的直和（定理6.7）；最后证明每个p—准素模均是循环模的直和(定理6.9)。

定理6.6 如果A是主理想整环R上的有限生成模，则$A=A_t\oplus F$，其中F是秩有限的自由R-模，并且$F\cong A/A_t$。

证明概要 商模A/A_t是无扭的，这是因为对于每个$r\neq 0$，

$r(a+A_t)=A_t\Longrightarrow ra\in A_t\Longrightarrow r_1(ra)=0$(对某个$r_1\neq 0$) $\Longrightarrow a\in A_t$。

此外，由于A是有限生成的，从而A/At也是有限生成的。因此由定理6.5便知A/A_t是秩有限的自由模。最后，正合序列$0\longrightarrow A_t\xrightarrow{\subset}A\longrightarrow A/A_t\longrightarrow 0$是分裂正合的，并且$A\cong A_t\oplus A/A_t$（定理3.2和3.4)。在定理3.4的同构$A_t\oplus A/A_t\cong A$之下，$A_t$的象是$A_t$，而$A/A_t$的象是$A$的一个子模$F$，$F$必然是秩有限的自由模。因此$A$是内直和$A=A_t\oplus F$(见定理1.15) ∎

定理6.7 设A是主理想环R上的扭模。并且对于每个素元$p\in R$，令$A(p)=\{a\in A\mid a$的阶是p的方幂$\}$。

(i) 对于每个素元p，$A(p)$均是A的子模。

(ii) $A=\sum A(p)$，其中求和过R的全部素元p。又若A是有限生成的，则只有有限多个$A(p)$不为零。

证明 (i) 令a，$b\in A(p)$。如果$\mathscr{O}_a=(p^r)$，$\mathscr{O}_b=(p^s)$。令$k=\max(r,s)$。则$p^k(a+b)=0$，从而由定理6.4(iv)可知$\mathscr{O}_{a+b}=$

(p^i)，$0\leqslant i\leqslant k$。因此$a,b\in A(p)\Longrightarrow a+b\in A(p)$。类似地可证：$a\in A(p)$，$r\in R\Longrightarrow ra\in A(p)$。从而$A(p)$是子模。

(ii) 令$0\neq a\in A$，$\mathscr{O}_a=(r)$。根据定理III.3.7我们有$r=p_1^{n_1}\cdots p_k^{n_k}$，其中$\{p_i\}$是$R$中两两不同的素元，而$n_i>0$ $(1\leqslant i\leqslant k)$。对于每个$i$，令$r_i=p_1^{n_1}\cdots p_{i-1}^{n_{i-1}}p_{i+1}^{n_{i+1}}\cdots p_k^{n_k}$。则 $(r_1,\cdots,r_k)=1$，从而存在$s_1,\cdots s_k\in R$，使得$s_1r_1+\cdots+s_kr_k=1_R$（定理III.3.11）。从而 $a=1_Ra=s_1r_1a+\cdots+s_kr_ka$。但是 $p_i^{n_i}s_ir_ia=s_ira=0$，因此 $s_ir_ia\in A(p_i)$。这就证明了子模$A(p)$（p过R中素元）生成模A。

设p是R中素元，A_1是由全部$A(q)(q\neq p)$所生成的A之子模。假设$a\in A(p)\cap A_1$。则 $p^ma=0$（对于某个 $m\geqslant 0$），并且 $a=a_1+\cdots+a_t$，$a_i\in A(q_i)$，其中素元q_1，…，q_t 均不为p。由于 $a_i\in A(q_i)$，从而有整数m_i，使得 $q_i^{m_i}a_i=0$，从而 $(q_1^{m_1}\cdots q_t^{m_t})a=0$。如果$d=q_1^{m_1}\cdots q_t^{m_t}$，则 $(p^m,d)=1$，从而$rp^m+sd=1_R(r,s\in R)$。于是 $a=1_Ra=rp^ma+sda=0$。因此$A(p)\cap A_1=0$。从而由定理1.15可知$A=\sum A(p)$。定理最后一个论断是由于：具有无限多个非零直和成份的模不可能是有限生成的。这是因为每个生成元只有有限多个非零的坐标。∎

为了决定有限生成模 $A(p)$的结构，我们还需要一个引理。对于R-模A和$r\in R$，我们令$rA=\{ra\mid a\in A\}$。

引理6.8 设A是主理想整环R上的模，$p\in R$为素元，n为正整数，$p^nA=0$但是$p^{n-1}A\neq 0$。设a为A中阶为p^n的元素。

(i) 如果$A\neq Ra$，则存在非零元素$b\in A$，使得$Ra\cap Rb=0$。

(ii) 存在A的子模C，使得$A=Ra\oplus C$。

注记：下面给出的证明是初等的。习题7给出(ii)的一个更简洁的证明，其中使用了内射模概念。

引理6.8的证明 (G. S. Monk) (i) 如果 $A \neq Ra$，则存在 $c \in A - Ra$。由于 $p^n c \in p^n A = 0$，故存在一个最小的正整数 j，使得 $p^j c \in Ra$。于是 $p^{j-1} c \notin Ra$，而 $p^j c = r_1 a (r_1 \in R)$。由于 R 是唯一因子分解整环，$r_1 = rp^k$，其中 $k \geqslant 0$，$r \in R$ 并且 $p \nmid r$。从而 $0 = p^n c = p^{n-j}(p^j c) = p^{n-j} r p^k a$。由于 $p \nmid r$，从而 $p^{n-1} a \neq 0$（定理6.4(v)），从而必然有 $n - j + k \geqslant n$，即 $k \geqslant j \geqslant 1$。因此 $b = p^{j-1} c - r p^{k-1} a \in A$。进而，$b \neq 0$（由于 $p^{j-1} c \notin Ra$）并且 $pb = p^j c - r p^k a = p^j c - r_1 a = 0$。如果 $Ra \cap Rb \neq 0$，则存在 $s \in R$，使得 $sb \in Ra$，而 $sb \neq 0$。由 $sb \neq 0$ 以及 $pb = 0$ 可知 $p \nmid s$。从而 $(s, p^n) = 1$，于是 $sx + p^n y = 1_R$，其中 x，$y \in R$。（定理III.3.11）。由 $p^n A = 0$ 给出 $b = 1_R b = sxb + p^n yb = x(sb) \in Ra$。从而 $p^{j-1} c = b + r p^{k-1} a \in Ra$。如果 $j - 1 \neq 0$，这就与 j 的极小性相矛盾。如果 $j - 1 = 0$，这又与 $c \notin Ra$ 相矛盾。因此 $Ra \cap Rb = 0$。

(ii) 如果 $A = Ra$，令 $c = 0$ 即可。如果 $A \neq Ra$，令 $\mathscr{S} = \{A$ 的子模 $B \mid Ra \cap B = 0\}$。由(i)知有非零元素 $b \in A$，使 $Ra \cap Rb = 0$，从而 $\mathscr{S}$ 是非空的。将 $\mathscr{S}$ 赋以集合论的包含序。验证 $\mathscr{S}$ 中每个链均有上界（$\in \mathscr{S}$）。由Zorn引理可知 A 存在子模 C，使得 C 在 $\mathscr{S}$ 中是极大元。考虑商模 A/C。显然 $p^n(A/C) = 0$，$p^n(a + C) = 0$。由于 $Ra \cap C = 0$，$p^{n-1} a \neq 0$，从而 $p^{n-1}(a + C) \neq C$。于是 $a + C$ 为 A/C 中阶 p^n 的元素。如果 A/C 不是由 $a + C$ 生成的循环 R-模（即 $A/C \neq R(a + C)$），由(i)知存在 $d + C \in A/C$，使得 $d + C \neq C$ 而 $R(a + C) \cap R(d + C) = C$。但是 $Ra \cap C = 0$，从而 $Ra \cap (Rd + C) = 0$。由于 $d \notin C$，$Rd + C \in \mathscr{S}$，并且 $Rd + C$ 真包含 C，这就与 C 之极大性相矛盾。因此 A/C 是由 $a + C$ 生成的循环 R-模（即 $A/C = R(a + C)$）。从而 $A = Ra + C$，于是由定理1.15可知 $A = Ra \oplus C$。 ∎

定理6.9 假设A是主理想整环R上的有限生成模，并且A中每个元素的阶均为R中素元p的幂次。则A是阶为$p^{n_1}, \cdots, p^{n_k}$的一些循环R-模的直和，其中$n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k \geqslant 1$。

证明 对于A的生成元个数r作数学归纳法。$r=1$的情形显然正确。如果$r>1$，则A由元素$a_1, \cdots, a_r$生成，它们的阶分别是p^{m_1}，p^{m_2}，p^{m_3}，$\cdots p^{m_r}$。我们不妨假定

$$n_1 = \max\{n_1, m_2, \cdots, m_r\}。$$

则$p^{n_1}A=0$而$p^{n_1-1}A \neq 0$。根据引理6.8可知A有子模C，使得$A = Ra_1 \oplus C$。令π：$A \to C$为正则满同态。由于A是由a_1，$\cdots$，a_r生成的，从而C由$\pi(a_1)$，$\pi(a_2)$，$\cdots$，$\pi(a_r)$生成。但是$\pi(a_1)=0$，从而C是由不超过$r-1$个元素所生成的。于是由归纳假设可知C是阶数分别为p^{n_2}，p^{n_3}，$\cdots$，p^{n_k}的一些循环R-模的直和，其中$n_2 \geqslant n_3 \geqslant \cdots \geqslant n_k \geqslant 1$。从而$C$中包含$n_2$阶的元素。由于$p^{n_1}A=0$，因此$p^{n_1}C=0$，于是$n_1 \geqslant n_2$。由于$Ra_1$是$p^{n_1}$阶循环$R$-模，从而$R$是阶数分别为$p^{n_1}$，$p^{n_2}$，$\cdots$，$p^{n_k}$的一些循环$R$-模的直和，其中$n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k \geqslant 1$。∎

定理6.6、6.7和6.9直接推出主理想整环上有限生成模的结构定理（见下面的定理6.12(ii)）。象Abel群的情形一样（第II.2节），还有将有限生成模分解成循环子模直和的另一种办法。为了得到这个第二种分解方法并证明两种分解方式的唯一性定理，我们还需要两个引理。

引理6.10 设$A, B, A_i (i \in I)$均是主理想整环R上的模。$r \in R$，$p \in R$，其中p为素元。

(i) $rA = \{ra \mid a \in A\}$和$A[r] = \{a \in A \mid ra = 0\}$均是$A$的子模。

(ii) $R/(p)$是域，$A[p]$是$R/(p)$上的向量空间。

(iii) 对于每个正整数n，均有R-模同构

$$(R/(P^n))[P]\cong R/(P),\quad P^m(R/(P^n))\cong R/(P^{n-m})(0\leqslant m\leqslant n).$$

(iv) 如果 $A\cong\sum_{i\in I}A_i$，则 $rA\cong\sum_{i\in I}rA_i$，$A[r]\cong\sum_{i\in I}A_i[r]$。

(v) 如果f：$A\to B$是R-模同构，则f：$A_t\cong B_t$，并且f：$A(p)\cong B(p)$。

证明概要 (ii) 习题2.4。(v) 见引理II.2.5(vii)。(iii) 参考定理6.5之前的第一个例子。验证 $(R/(p^n))[p]$ 作为 R-模（从而作为$R/(p)$上向量空间）是由一个非零元素$p^{n-1}+(p^n)$生成的，从而由定理2.5和2.1可知$(R/(p^n))[p]\cong R/(p)$。$R/(p^n)$中由$p^m+(p^n)$ 生成的子模是 $p^m(R/(p^n))$。由于 $p^m+(p^n)$的阶为p^{n-m}，从而由定理6.4(iii)便知$p^m(R/(p^n))\cong R/(p^{n-m})$。∎

引理6.11 设R为主理想整环。如果$r\in R$分解成$r=p_1^{n_1}\cdots p_k^{n_k}$，其中 $p_1,\cdots,p_k\in R$ 为两两不同的素元，$n_i>0(1\leqslant i\leqslant k)$，则有$R$-模同构

$$R/(r)\cong R/(p_1^{n_1})\oplus\cdots\oplus R/(p_k^{n_k}).$$

于是，每个r阶循环R-模均是阶数分别为$p_1^{n_1},\cdots,p_k^{n_k}$的$k$个循环$R$-模的直和。

证明概要 我们只需证明：如果$s,t\in R$，$(s,t)=1$，则$R/(st)\cong R/(s)\oplus R/(t)$。由此对$r$的分解式中不同素因子的个数作归纳法即证得引理的第一部分。而引理的第二部分则是下述事实的直接推论：根据定理6.4，对于每个$c\in R$，$R/(c)$均是阶为c的循环R-模。

映射θ：$R\to R$，$x\longmapsto tx$是R-模单同态，并且将理想(s)映成理想(st)。由系1.8可知它诱导出R-模同态 $R/(s)\to R/(st)$，$x+$

$(s)\longmapsto tx+(st)$. 类似地，也有同态$R/(t)\to R/(st)$，$x+(t)\longmapsto sx+(st)$. 从定理1.13的证明可知我们有R-模同态$\alpha: R/(s)\oplus R/(t)\to R/(st)$，$(x+(s),y+(t))\longmapsto[tx+sy]+(st)$. 由于$(s,t)=1_R$，从而有$u,v\in R$，使得$su+tv=1_R$(定理IV.3.11). 如果$c\in R$，则$c=suc+tvc$，于是$\alpha(vc+(s),uc+(t))=c+(st)$. 因此$\alpha$是满同态. 为证$\alpha$是单同态，我们只需证明

$\alpha(x+(s),y+(t))=0\Longrightarrow x\in(s)$并且$y\in(t)$: 如果$\alpha(x+(s),y+(t))=0$，则有$b\in R$，使得$tx+sy=stb\in(st)$. 于是$utx+usy=ustb$. 但是$y=1_Ry=(su+tv)y$，从而$utx+(y-tvy)=ustb$，$y=ustb-utx+tvy\in(t)$. 类似地可证$x\in(s)$. ∎

定理6.12 设A是主理想整环R上的有限生成模.

(i) A是一个秩有限的自由子模F与有限个循环扭模的直和. 进而，如果存在循环扭模直和成份，则可以使得它们的阶分别为$r_1,\cdots,r_t$，其中$r_1,\cdots,r_t$是R中(不必两两相异)非零非单位元素，并且$r_1|r_2|\cdots|r_t$. F的秩和理想$(r_1)\cdots,(r_t)$是由A所唯一确定的.

(ii) A是一个秩有限的自由子模E与有限个循环扭模的直和. 进而，如果存在循环扭模直和成份，则可以使得它们的阶分别为$p_1^{s_1},\cdots,p_k^{s_k}$，其中$p_1,\cdots,p_k$是$R$中（不必两两相异）的素元，而$s_1,\cdots,s_k$是（不必两两相异的)正整数. E的秩与理想$(p_1^{s_1}),\cdots,(p_k^{s_k})$是由$A$所唯一确定的.

注：记号$r_1|r_2|\cdots|r_t$表示r_1可整除r_2，r_2可整除r_3等等. 象在Abel群情形一样，定理6.12中的元素$r_1,\cdots,r_t$叫作模A的不变因子. 而$p_1^{s_1},\cdots,p_k^{s_k}$叫作模$A$的初等因子.

定理6.12的证明概要 关于(ii)中所述类型的直和分解的存在性是定理6.6,6.7和6.9的直接推论. 因此A是一个自由模和有

限个循环R-模的直和，并且其中每个循环R-模的阶都是某素元的方幂。在Abel群的情形，这些素数的幂恰好是A的初等因子。然后可以将从Abel群的初等因子计算不变因子的方法基本上原封不动地搬到这里来，从而就证明了（i）中所述形式的直和分解的存在性，需要改动的只是：$Z_{p^n}=Z/(p^n)$（p为素数）所起的作用改成用A的p^n阶循环扭子模，这里的p是R中的素元。根据定理6.4(iii)，这样一个扭模同构于$R/(p^n)$。此外，还需用引理6.11代替引理II.2.3。

关于(i)和(ii)中直和分解唯一性的证明，本质上与Abel群情形下的证明是一样的(定理II.2.6)，只需作如下一些修改。首先，R中的素因子分解式中每个不可约元唯一决定到相差单位因子(定义III.3.5和定理III.3.7)。这在$\mathbb{Z}$中不会引起任何麻烦，因为$\mathbb{Z}$中单位只有± 1而素数定义为正整数。但是在任意主理想整环R中，元素$a\in R$可能阶为p，同时阶为q，其中p和q为不同的素元。这时由于$(p)=\mathscr{O}_a=(q)$，从而由定理III.3.2即知p和q是相伴的，即$q=pu$，其中$u\in R$是单位。所以在叙述(i)和(ii)中的唯一性命题时，我们谈理想而不谈元素。注意$a\neq 0$导致$\mathscr{O}_a\neq R$。并且循环模Ra是自由的$\Longleftrightarrow\mathscr{O}_a=(0)$。因此(i)中的元素$r_i$均不为零也不是单位。另一个修改之处是：象前面那样，每个有限循环直和成份$Z_n\cong Z/(n)(n>1)$改成循环扭模$R/(r)(r\in R$是非零非单位元素)。把由一些无限循环直和成份$\mathbb{Z}$所生成的子群改成秩有限的一个自由R-模。用引理6.10和6.11代替引理II.2.3和II.2.5。而将第120页证明$r=d$的推理方法改成为利用如下事实：$A[p]$是$R/(p)$上的向量空间，从而直和成份$R/(p)$的个数恰好等于$\dim_{R/(p)}A[p]$，而由定理2.7可知它是不变量。∎

系6.13 主理想整环上的两个有限生成模 A 和 B 是同构的 $\Longleftrightarrow A/A_t$ 和 B/B_t 有同样的秩，并且 A 和 B 具有同样的不变因子（或者初等因子）。

证明作为练习。∎

习　题

注：若不特别声明，R 均是主理想整环，而模均是幺作用的。

1. 如果 R 是含幺交换环，并且每个自由 R-模的每个子模均是自由的，则 R 是主理想整环。〔提示：R 的每个理想 I 是自由 R-模。如果 $u,v\in I(u\neq 0,v\neq 0)$，则 $uv+(-v)u=0$，所以 I 有一元形成的基，即 I 是主理想。〕
2. 任意含幺整环上的每个自由模都是无扭的。但是逆命题则不成立（习题 II.1.10）。
3. 设 A 是阶为 $r\in R$ 的循环 R-模。
   (a) 如果 $s\in R$，$(s,r)=1$，则 $sA=A$，$A[s]=0$。
   (b) 如果 $s|r$，设 $sk=r$，则 $sA\cong R/(k)$，$A[s]\cong R/(s)$。
4. 如果 A 是阶为 r 的循环 R-模，则
   (i) A 的每个子模均是循环的，并且其阶可整除 r；
   (ii) 对于每个包含 (r) 的理想 (s)，A 恰好有一个 s 阶循环子模。
5. 如果 A 是有限生成扭模，则 $\{r\in R|rA=0\}$ 是 R 中非零理想。设此理想为 (r_1)，我们称 r_1 是 A 的极小零化子。设 A 是有限 Abel 群，$m\in\mathbf{Z}$ 是它的极小零化子。证明：如果 A 的一个循环子群其阶是 m 的真因子，则该子群不一定是 A 的直和成份。
6. 如果 A 和 B 是 R 上循环模，其阶分别为 r 和 s，其中 r,s 均不为零，并且 $(r,s)\neq 1$。则 $A\oplus B$ 的不变因子是 r 与 s 的最大公约元和最小公倍元。
7. 设 A 和 $a\in A$ 满足引理 6.8 的假设。
   (a) A 的每个 R-子模均是 $R/(p^n)$-模，其中 $(r+(p^n))a=ra$。反之，A 的每个 $R/(p^n)$-子模经 $R\to R/(p^n)$ 拉回之后也是 R-子模。

(*b*) 子模Ra同构于$R/(p^n)$.

(*c*) 环 $R/(p^n)$ 的真理想只有由$p^i+(p^n)$ $(1\leqslant i\leqslant n-1)$ 生成的那些理想.

(*d*) $R/(p^n)$ (从而 Ra) 是内射 $R/(p^n)$-模. 〔提示: 用 (*c*) 和引理 3.8.〕

(*e*) 存在A的一个R-子模C, 使得$A=Ra\oplus C$. 〔提示: 命题3.13.〕

7. 代　　数

我们在本节里介绍代数及其基本性质. 在讨论中大量地使用张量积. 在第IX章中还要对代数作进一步研究.

定义7.1 设K是含幺交换环. 一个K-代数(或者叫作K上的代数) A是指具有以下性质的环A:

(i) $(A,+)$ 是幺作用 (左) K-模;

(ii) $k(ab)=(ka)b=a(kb)$ (对所有$k\in K$, a, $b\in A$).

一个K-代数A如果是体, 便称它是除法代数.

代数的经典理论是研究域K上的代数. 这样的代数是K上的向量空间, 从而可以用各种线性代数的结果. 域K上的代数如果作为K上的向量空间是有限维的, 便称作K上有限维代数.

例 每个环R均是加法Abel群, 从而为$\mathbb{Z}$-模. 不难看出, R事实上是$\mathbb{Z}$-代数.

例 如果K是含幺交换环, 则多项式环 $K[x_1,\cdots,x_n]$ 和幂级数环$K[[x]]$均是K-代数 (对于通常的K-模结构).

例 如果V是域F上的向量空间, 则自同态环$\mathrm{Hom}_F(V,V)$(习

题1.7）是F-代数，其中 $\mathrm{Hom}_F(V,V)$ 的F-模结构在定理4.8后面的注记中讨论过。

例 设A是含幺环，K是A的中心的子环，并且$1_A\in K$。则A是K-代数，其中K-模结构由A中的乘法给出。特别地，每个含幺交换环K均是K-代数。

例 复数域$\mathbb{C}$和实四元数体均是实数域$\mathbb{R}$上的除法代数。

例 设G是乘法群而K是含幺交换环。则群环$K(G)$事实上是K-代数，其K-模结构由下式给出：

$$k(\sum r_i g_i)=\sum(kr_i)g_i \qquad (k,r_i\in K,g_i\in G).$$

$K(G)$叫作G在K上的群代数。

例 如果K是含幺交换环，则K上全体n阶方阵形成的环$\mathrm{Mat}_n K$是K-代数，K在K-模上的作用以通常方式给出。更一般地，如果A是K-代数，则$\mathrm{Mat}_n A$也是K-代数。

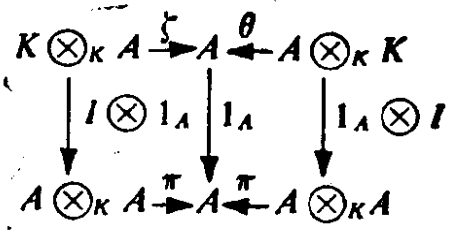
注记：因为K是交换环，所以每个左K-模（从而每个K-代数）A也是右K-模，其中 $ka=ak$（对于$a\in A,k\in K$）。在下面定理7.2和7.4中作张量积时，需要这项未被明显提到的事实。

下一定理给出定义K-代数的另一种方式，它是基于如下的事实：对于任意环R，在生成元$r\otimes s$上由$r\otimes s\longmapsto rs$所决定的唯一映射$R\otimes_{\mathbb{Z}}R\to R$是加法Abel群的同态。由于环均是$\mathbb{Z}$-代数，从而上述事实是下面定理的特殊情形。

定理7.2 设K是含幺交换环，A是幺作用左K-模。则A是K-代数$\Leftrightarrow$存在K-模同态π：$A\otimes_K A\to A$，使得图表

$$\begin{array}{ccc} A\otimes_K A\otimes_K A & \xrightarrow{\pi\otimes 1_A} & A\otimes_K A \\ \downarrow{\scriptstyle 1_A\otimes\pi} & & \downarrow{\scriptstyle \pi} \\ A\otimes_K A & \xrightarrow{\pi} & A \end{array}$$

是交换的。在这种情形下，K-代数A有幺元素$\Longleftrightarrow$存在K-模同态I：$K\to A$，使得图表



是交换的，其中ζ和θ是定理5.7中的同构。

证明概要 如果A是K-代数，则映射$A\times A\to A$，$(a,b)\longmapsto ab$是K-双线性的，于是由定理5.6可知存在K-模同态

$$\pi: A\otimes_K A\to A.$$

验证π具有所需要的性质。如果A有1_A，则不难看出映射I：$K\to A$，$k\longmapsto k1_A$是具有所需要性质的K-模同态。反之，给了A和映射π：$A\otimes_K A\to A$，定义$ab=\pi(a\otimes b)$，验证A是K-代数。如果I：$K\to A$也给定，则$I(1_K)$是A中幺元素。∎

定理7.2中的同态π叫作K-代数A的积映射。而同态I叫作单位映射。

定义7.3 设K是含幺交换环，A和B是K-代数。

(i) A的子代数是A的一个子环并且同时也是A的K-子模。

(ii) A的（左、右或者双侧）代数理想是环A的一个（左、右或者双侧）理想，并且同时也是A的K-子模。

(iii) K-代数同态（同构）f：$A\to B$是环同态（同构）同时也是K-模同态（同构）。

注记：如果A是K-代数，环A的理想不一定是A的代数理想（习题4）。但是如果A有幺元素，则对于每个$k\in K$和$a\in A$，

$$ka = k(1_A a) = (k1_A)a,\quad ka = (ka)1_A = a(k1_A).$$

其中$k1_A \in A$. 因此对于环A的左（右）理想J，我们有

$$kJ = (k1_A)J \subset J \qquad (kJ = J(k1_A) \subset J).$$

所以，如果A有幺元素，则每个(左、右或者双侧)理想也是(左、右或者双侧）代数理想。

现在可以用显然的方式定义K-代数A对于代数理想I的商代数，类似地定义一族K-代数的直积与直和。

另一种构作新代数的方法是使用张量积. 我们首先注意，如果A和B是K-模，则有K-模同构α：$A \otimes_K B \to B \otimes_K A$，使得$\alpha(a \otimes b) = b \otimes a (a \in A,\ b \in B)$，见习题 2 。

定理7.4 设A和B是交换环K上的（具有幺元素的）代数。π是合成映射

$$(A \otimes_K B) \otimes_K (A \otimes_K B) \xrightarrow{1_A \otimes \alpha \otimes 1_B} (A \otimes_K A) \otimes_K (B \otimes_K B)$$

$$\xrightarrow{\pi_A \times \pi_B} A \otimes_K B,$$

其中π_A和π_B分别是A和B的积映射. 则$A \otimes_K B$是（具有幺元素的）K-代数，并且以π为积映射。

证明作为练习. 注意对于$A \otimes_K B$的生成元素$a \otimes b$和$a_1 \otimes b_1$，其乘积定义为

$$(a \otimes b)(a_1 \otimes b_1) = \pi(a \otimes b \otimes a_1 \otimes b_1) = aa_1 \otimes bb_1.$$

因此若A和B分别有幺元素1_A和1_B，则$1_A \otimes 1_B$是$A \otimes_K B$中的幺元素。∎

定理7.4中的K-代数$A \otimes_K B$叫作K-代数A和B的张量积. 在研究域K上除法代数结构的时候（第IX. 6节），代数的张量积是很有益处的。

习　题

注：K永远为含幺交换环。

1. 设$\mathscr{C}$是如下的范畴：其对象为全体含幺交换K-代数，而态射为全体K-代数同态$f: A\to B$，使得$f(1_A)=1_B$。则$\mathscr{C}$中任意两个K-代数A和B均有余积。〔提示：考虑$A\to A\otimes_K B\leftarrow B$，其中$a\longmapsto a\otimes 1_B$，而$b\longmapsto 1_A\otimes b$。〕

2. 如果A和B是幺作用K-模〔K-代数〕，则存在K-模〔K-代数〕同构α：$A\otimes_K B\to B\otimes_K A$，使得$\alpha(a\otimes b)=b\otimes a$（对于每个$a\in A$，$b\in B$）。

3. 设A是含幺环。则A是含幺K-代数$\Longleftrightarrow$存在K到A的中心之中的环同态，使得$1_K\longrightarrow 1_A$。

4. 设A是有理数域$\mathbf{Q}$上的一维向量空间。如果我们定义$ab=0$（对于每个a，$b\in A$），则A是$\mathbf{Q}$-代数。A的每个真加法子群均是环A的理想，但不是代数理想。

5. 设$\mathscr{C}$是习题1中的范畴。如果X为集合$\{x_1,\cdots,x_n\}$，则在范畴$\mathscr{C}$中，多项式代数$K[x_1,\cdots,x_n]$是集合X上的自由对象。〔提示：给了$\mathscr{C}$中一个代数A和映射$g: \{x_1,\cdots,x_n\}\to A$，将定理Ⅱ.5.5用于单位映射$I: K\to A$和元素$g(x_1),\cdots,g(x_n)\in A$。〕

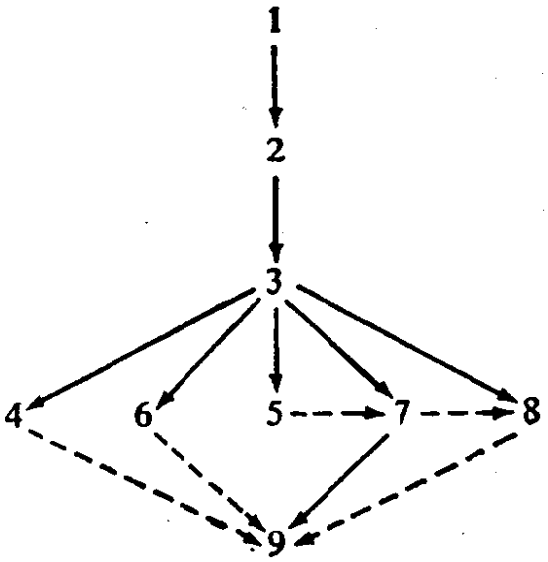
第V章　域和伽罗华理论

本章第一个主要论题是域的结构理论。我们将利用一个指定的子域K来研究域F(F叫作K的扩域)。在第1节中论述域扩张的一些基本事实。特别地，要讲述代数扩张和超越扩张之间的区别。在本章的多数地方，我们只处理代数扩张，第VI章将考虑任意的域扩张。我们彻底分析了某些域和域扩张的结构，其中包括：单扩张(第1节)，分裂域(正规扩张)和代数闭包(第3节)，有限域(第5节)以及可分代数扩张(第3、6节)。

域扩张的伽罗华理论(本章另一个主要论题)在历史上起源于方程论的一个经典问题，这将在第4节和第9节中加以详细讨论。伽罗华理论的各种结果有许多重要的应用，特别是用来研究代数数论(见E. Artin〔48〕)和代数几何(见S. Lang〔54〕)。

伽罗华理论的关键思想是：对于每个域的扩张$K \subset F$，我们都有一个由固定K中每个元素的F之自同构所形成的群(叫该扩张的伽罗华群)。而域的伽罗华扩张可以用它的伽罗华群来定义(第2节)，或者用该扩张的内部结构来定义(第3节)。伽罗华理论的基本定理(第2节)是说：在域的(有限维)伽罗华扩域的所有中间域和该扩张的伽罗华群的所有子群之间存在着一一对应关系。这个定理使我们能够把关于域，多项式和域的扩张方面的许多性质和问题转成用群论的语言来叙述。于是，如果群论中相应的问题能

够解决，则域论中的原始问题也就得到解决。例如，上一段中所提到的方程论中那个古典问题便是如此得到解决的。我们还将要刻划伽罗华群是有限循环群（第7节）和可解群（第9节）的那些伽罗华扩张。



本章诸节之间的内部联系大致如右图所示：其中虚线箭头 $A\cdots\cdots\rightarrow B$ 表示第 B 节使用第 A 节中的少数结果，但是第 B 节与第 A 节本质上是独立的。

1. 域的扩张

我们先给出研究域扩张所需要的一些基本事实，随后讨论单扩张。最后证明代数扩张的一些重要性质。在附录中我们解决古代所提出来的几个著名的几何难题，比如用圆规直尺来三等分角的问题。（这部分在后面不用）

定义1.1 如果域 K 是域 F 的子域，我们便称 F 是 K 的扩域（或者叫作 K 的扩张）。

如果 F 是 K 的扩域，不难看出 $1_K = 1_F$。此外，F 是 K 的向量空间（定义 IV.1.1）。在本章中我们永远将 K-向量空间 F 的维数表示成 $[F:K]$，而不象过去那样表示成 $\dim_K F$。按照 $[F:K]$ 是有限或者无限，我们分别将 F 称作 K 的有限维扩张或者无限维扩张。

定理1.2 假设 F 是 E的扩域而 E 是 K 的扩域。则 $[F:K]=[F:E][E:K]$。此外，$[F:K]$ 有限的充要条件是$[F:E]$和$[E:K]$均有限。

证明 这是定理IV.2.16的重述。 ∎

对于定理1.2中的情形 $K\subset E\subset F$，我们将E称作K和F的中间域。

如果F是域而 $X\subset F$，那末 X 所生成的子域（或子环）指的是F中包含X的全部子域（或子环）的交。如果F是K的扩域而$X\subset F$，那末由 $K\cup X$生成的子域（或子环）称作 X在 K上所生成的子域（或者子环）。并且表示成 $K(X)$（或者$K[X]$）。注意 $K[X]$ 必定是整环。

如果$X=\{u_1,\cdots,u_n\}$，则F的子域$K(X)$（或子环$K[X]$）也表示成$K(u_1,\cdots u_n)$（或$K[u_1,\cdots,u_n]$）。域$K(u_1,\cdots,u_n)$ 叫作K的有限生成扩域（但是在K上不必是有限维的，见习题2）。如果$X=\{u\}$，则$K(u)$叫作K的单扩张。不难验证，$K(u_1,\cdots,u_n)$ 和 $K[u_1,\cdots,u_n]$ 都与 u_i 之间的次序无关，并且 $K(u_1,\cdots,u_{n-1})(u_n)=K(u_1\cdots,u_n)$，$K[u_1,\cdots,u_{n-1}][u_n]=K[u_1,\cdots,u_n]$（习题4）。这些事实在今后要经常用到，每次都不再多作解释。

记号：如果F是域，$u,v\in F$，而$v\neq 0$，则元素 $uv^{-1}\in F$ 有时表示成u/v。

定理1.3 如果F是域K的扩域，$u,u_i\in F$，而$X\subset F$，则

(i) 子环$K[u]$等于$\{f(u)\mid f\in K[x]\}$。

(ii) 子环 $K[u_1,\cdots,u_m]$ 等于 $\{g(u_1,\cdots,u_m)\mid g\in K[x_1,\cdots,x_n]\}$。

(iii) 子环 $K[X]$ 等于 $\{h(u_1,\cdots,u_n)\mid u_i\in X,\ n$为自然数，$h\in K[x_1,\cdots,x_n]\}$。

(iv) 子域$K(u)$等于$\{f(u)/g(u)=f(u)g(u)^{-1}\mid f,\ g\in K[x]$，并且$g(u)\neq 0\}$。

(v) 子域$K(u_1,\cdots,u_m)$等于

$$\{h(u_1,\cdots,u_m)/k(u_1,\cdots,u_m)$$
$$=h(u_1,\cdots,u_m)k(u_1,\cdots,u_m)^{-1}\mid$$
$$h,k\in K[x_1,\cdots,x_m]\text{并且}k(u_1,\cdots,u_m)\neq 0\}。$$

(vi) 子域$K(X)$等于

$$\{f(u_1,\cdots,u_n)/g(u_1,\cdots,u_n)\mid n\in \boldsymbol{N}^*,$$
$$f,g\in K[x_1,\cdots,x_n],\ u_1,\cdots,u_n\in X,$$
$$g(u_1,\cdots,u_n)\neq 0\}。$$

(vii) 对于每个 $v\in K(X)$（或者$v\in K[X]$），均存在X的有限子集X'，使得$v\in K(X')$（或者$v\in K[X']$）。

证明概要 (vi) 每个域如果包含K和X，则必然包含集合

$$E=\{f(u_1,\cdots,u_n)/g(u_1,\cdots,u_n)\mid n\in \boldsymbol{N}^*,$$
$$f,g\in K[x_1,\cdots,x_n],\ u_i\in X,\ g(u_1,\cdots,u_n)\neq 0\},$$

因此$K(X)\supset E$。反之，如果 $f,g\in K[x_1,\cdots,x_m]$而 $f_1,g_1\in K[x_1,\cdots,x_n]$，我们定义$K[x_1,\cdots,x_{m+n}]$中的元素

$$h(x_1,\cdots,x_{m+n})=f(x_1,\cdots,x_m)g_1(x_{m+1},\cdots,x_{m+n})$$
$$-g(x_1,\cdots,x_m)f_1(x_{m+1},\cdots,x_{m+n}),$$
$$k(x_1,\cdots,x_{m+n})=g(x_1,\cdots,x_m)g_1(x_{m+1},\cdots,x_{m+n})。$$

那末对于任何 $u_1,\cdots,u_m,\ v_1,\cdots,v_n\in X$，如果 $g(u_1,\cdots,u_m)\neq 0$，$g_1(v_1,\cdots,v_m)\neq 0$，便有

$$\frac{f(u_1\cdots,u_m)}{g(u_1,\cdots,u_m)}-\frac{f_1(v_1,\cdots,v_n)}{g_1(v_1,\cdots,v_n)}$$

$$=\frac{h(u_1,\cdots,u_m,v_1,\cdots,v_n)}{k(u_1,\cdots,u_m,v_1,\cdots,v_n)}\in E\ .$$

因此E对于加法形成群(定理I.2.5)。类似地，E 中非零元素全体对于乘法形成群。从而E是域。由于 $X\subset E$ 并且 $K\subset E$，我们有$K(X)\subset E$。因此$K(X)=E$。

(vii) 如果$u\in K(X)$，由(vi)便知$u=f(u_1,\cdots,u_n)/g(u_1,\cdots,u_n)\in K(X')$，其中$X'=\{u_1,\cdots,u_n\}\subset X$。 ∎

如果 L 和 M 均是域F的子域，那末由集合 $L\cup M$ 所生成的子域叫作L和M在F中的合成，表示成 LM。由定义立即推出 $LM=L(M)=M(L)$。不难证明，如果 K 是 $L\cap M$ 的子域，并且 $M=K(S)$，其中$S\subset M$，则$LM=L(S)$（习题5)。关于$[L:K]$，$[M:K]$和$[LM:K]$之间的维数关系可见习题20和21。有限多个子域 E_1，$E_2,\cdots,E_n$的合成定义为由集合$E_1\cup E_2\cup\cdots\cup E_n$所生成的子域，并且表示成$E_1E_2\cdots E_n$(见习题5)。

下一步要区分域扩张的两种本质不同的情形。

定义1.4 假设F是域K的扩域。F 中元素u叫作在K上是代数的，是指u是某个非零多项式$f\in K[x]$ 的根。如果u不是任何一个非零多项式$f\in K[x]$的根，我们称u在K上是超越的。如果 F中每个元素都在K上是代数的，便称F为K的代数扩张，如果 F中至少有一个元素在K上是超越的，便称F为K的超越扩张。

注记：如果$u\in K$，则u是$x-u\in M[x]$的根，因此在K上是代数的。如果 $u\in F$ 在K的某个子域K'上是代数的，由于 $K'[x]\subset K[x]$，从而u在K上也是代数的。如果$u\in F$是$f\in K[x]$的根，而f的首项系数$c\neq 0$，则u也是多项式$c^{-1}f$的根，而$c^{-1}f$为 $K[x]$中的首1多项式。超越扩张可以包含(除了K自身中元素之外的)在K上代

数的元素。

例 以$\boldsymbol{Q}$,$\boldsymbol{R}$,$\boldsymbol{C}$分别表示有理数域，实数域和复数域。则$i\in\boldsymbol{C}$在$\boldsymbol{Q}$上是代数的，从而在$\boldsymbol{R}$上也是代数的。事实上$\boldsymbol{C}=\boldsymbol{R}(i)$。另一方面，$\pi$和$e\in\boldsymbol{R}$在$\boldsymbol{Q}$上都是超越的。关于这一不平凡的事实，请参见 I.Herstein[4]。

例 如果K是域，则多项式环$K[x_1,\cdots,x_n]$是整环（定理III.5.3）。$K[x_1,\cdots,x_n]$的商域表示成$K(x_1,\cdots,x_n)$。它等于$\{f/g|f,g\in K[x_1,\cdots,x_n]$并且$g\neq 0\}$，而运算为通常的加法和乘法（见定理III.4.3）。$K(x_1,\cdots,x_n)$叫作K上关于$x_1,\cdots,x_n$的有理函数域。在域的扩张

$$K\subset K(x_1,\cdots,x_n)$$

中，不难看出每个x_i在K上都是超越的。事实上，$K(x_1,\cdots,x_n)$中每个元素如果不属于K本身，那末它在K上必然是超越的（习题6）。

在下面两个定理中，我们要刻划全部单扩张（不计同构）。

定理1.5 如果F是K的扩域而$u\in F$在K上超越，则存在一个域的同构$K(u)\cong K(x)$，并且此同构在K上的限制是恒等自同构。

证明概要 由于u是超越的，从而对每个非零的$f,g\in K[x]$，$f(u)\neq 0$，$g(u)\neq 0$。从而映射$\varphi: K(x)\longrightarrow F$，$f/g\longmapsto f(u)/g(u)=f(u)g(u)^{-1}$可以定义出域的单同态，并且$\varphi$在K上是恒等映射。但是由定理1.3可知$Im\varphi=K(u)$，于是$K(x)\cong K(u)$。 ∎

定理1.6 如果F是K的扩域，$u\in F$在K上是代数的，则

(i) $K(u)=K[u]$;

(ii) $K(u)\cong K[x]/(f)$，其中$f\in K[x]$是$n(\geqslant 1)$次不可约的首1多项式，它由条件“$f(u)=0$”和“$g(u)=0(g\in K[x])\Longleftrightarrow f|g$”

所唯一决定。

(iii) $[K(u):K]=n$;

(iv) $\{1_K,u,u^2,\cdots,u^{n-1}\}$是$K$上向量空间$K(u)$的一组基。

(v) $K(u)$中每个元素都可以唯一地写成 $a_0+a_1u+\cdots+a_{n-1}u^{n-1}(a_i\in K)$。

证明 (i)和(ii)根据定理III.5.5和1.3，可知映射 $\varphi:K[x]\longrightarrow K[u]$，$g\longmapsto g(u)$是环的满同态。由于$K[x]$是主理想环（系III.6.4），从而$\mathrm{Ker}\varphi=(f)$，其中 $f\in K[x]$，并且$f(u)=0$。由于u是代数的，从而$\mathrm{Ker}\varphi\neq 0$，又由于$\varphi\neq 0$，从而 $\mathrm{Ker}\varphi\neq K[x]$。于是$f\neq 0$，并且$\deg f\geqslant 1$。进而，如果$c$是$f$的首项系数，则$c$是$K[x]$中的单位(系III.6.4)，从而$c^{-1}f$为首1多项式，并且$(f)=(c^{-1}f)$(定理 III.3.2)。于是我们可以假定 f 是首1的。由第一同构定理(系III.2.10)，我们有

$$K[x]/(f)=K[x]/\mathrm{Ker}\varphi\cong\mathrm{Im}\varphi=K[u].$$

由于$K[u]$为整环，根据定理III.2.16可知(f)是$K[x]$中的素理想。由定理III.3.4推出f是不可约的，从而(f)是极大理想。从而$K[x]/(f)$是域(定理III.2.20)。由于$K(u)$是F之包含K和u的最小子域，并且$K(u)\supset K[u]\cong K[x]/(f)$，从而必然 $K(u)=K[u]$。由于f是首1的并且

$$g(u)=0\Longleftrightarrow g\in\mathrm{Ker}\varphi=(f)\Longleftrightarrow f\mid g.$$

可知f是唯一的。

(iv) 根据定理1.3，$K(u)=K[u]$中每个元素均有形式$g(u)$，其中 $g\in K[x]$。利用除法算式，$g=qf+h$，其中 $q,h\in K[x]$，并且$\deg h<\deg f$。因此$g(u)=q(u)f(u)+h(u)=h(u)=b_0+b_1u+\cdots+b_mu^m$，其中$m<n=\deg f$。从而 $\{1_K,u,\cdots,u^{n-1}\}$ 张成K-向量空间$K(u)$。为了看出$\{1_K,u,\cdots,u^{n-1}\}$在K上是线性无关的，即是

一组基，我们假定

$$a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} = 0 \quad (a_i \in K)$$

则$g = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in K[x]$以$u$为根并且$\deg g \leqslant n-1$。由(ii)知$f \mid g$，而$\deg f = n$，从而必然$g = 0$。即对于所有$i$，$a_i = 0$，因而$\{1_k, u, \cdots, u^{n-1}\}$是线性无关的。因此$\{1_K, u, \cdots, u^{n-1}\}$是$K(u)$的一组基。

(iii)是(iv)的直接推论。

(iv)和(v)是等价的(作为练习)。 ∎

定义1.7 令F是K的扩域，$u \in F$在K上是代数的。则定理1.6中的首1多项式f叫作u的不可约多项式(或极小多项式)。而$\deg f = [K(u):K]$叫作u在K上的次数。

下面的例子表明如何利用定理1.6和其证明中所用的技巧作具体的计算。

例 多项式$x^3 - 3x - 1$在$\mathbb{Q}$上是不可约的（定理III.6.6和命题III.6.8)。并且它有实根u(习题III.6.16(d))根据定理1.6，u在$\mathbb{Q}$上的次数是3，并且$\{1, u, u^2\}$是$\mathbb{Q}(u)$在$\mathbb{Q}$上的一组基。元素$u^4 + 2u^3 + 3 \in \mathbb{Q}(u) = \mathbb{Q}[u]$可以表示成基元素(在$\mathbb{Q}$上）的线性组合。其方法如下：使用环$[x]$中的除法算式（即通常所谓的“长除法”)可知

$$x^4 + 2x^3 + 3 = (x+2)(x^3 - 3x - 1) + (3x^2 + 7x + 5).$$

从而

$$\begin{aligned} u^4 + 2u^3 + 3 &= (u+2)(u^3 - 3u - 1) + (3u^2 + 7u + 5) \\ &= (u+2) \cdot 0 + (3u^2 + 7u + 5) \\ &= 3u^2 + 7u + 5. \end{aligned}$$

$3u^2 + 7u + 5$在$\mathbb{Q}(u)$中的乘法逆元素可以按下面方法计算：由于

x^3-3x-1在$\mathbb{Q}[x]$中不可约，从而多项式x^3-3x-1和$3x^2+7x+5$在$\mathbb{Q}[x]$中是互素的。根据定理 III.3.11 可知存在$g(x)$，$h(x)\in\mathbb{Q}[x]$，使得

$$(x^3-3x-1)g(x)+(3x^2+7x+5)h(x)=1.$$

由于$u^3-3u-1=0$，从而我们有

$$(3u^2+7u+5)h(u)=1.$$

即$h(u)\in\mathbb{Q}(u)$是$3u^2+7u+5$的逆元素。多项式g和h可以用欧氏算式（习题 III.3.13）具体地计算出来：$g(x)=-(7/37)x+29/111$，$h(x)=(7/111)x^2-(26/111)x+28/111$。于是$h(u)=(7/111)u^2-(26/111)u+28/111$。

假设E是K的扩域，F是L的扩域，并且$\sigma: K\to L$是域的同构。在研究域的扩张的时候，经常遇到这样一个问题：在什么条件下，σ可以扩充成E到F上的同构？换句话说，是否存在一个同构$\tau: E\to F$，使得$\tau|K=\sigma$？现在我们对于单扩张的情形给出这个问题的答案，并且由此还得到判别两个单扩张$K(u)$和$K(v)$是否同构的一种方法（还见习题16）。

让我们回忆一下，如果$\sigma: R\to S$是环的同态，则映射$R[x]\to S[x]$，$\sum_i r_i x^i \longmapsto \sum_i \sigma(r_i)x^i$也是环同态（习题III.5.1）。这个映射显然是$\sigma$的扩充。我们将这个扩充映射$R[x]\to S[x]$仍记为$\sigma$，并且以$\sigma f$表示$f\in R[x]$的象元素。

定理1.8 假设$\sigma: K\to L$是域的同构，u是K的某扩域中的元素，v是L的某扩域中的元素。又假定下列两个条件当中有一个是成立的：

(i) u在K上是超越的，并且v在L上是超越的。

(ii) u是不可约多项式$f\in K[x]$的根，而v是$\sigma f\in L[x]$的根。则σ可以扩充成域同构$K(u)\cong L(v)$，并且将u映成v.

证明概要 (i) 由定理前面的注记，可知σ可以扩充成同构$K[x]\cong L[x]$.证明这个映射通过$h/g\longmapsto \sigma h/\sigma(g)$又可扩充成同构$K(x)\longrightarrow L(x)$。根据定理1.5，我们有$K(u)\cong K(x)\cong L(x)\cong L(v)$。而这些同构的合成便是$\sigma$的扩充，并且将$u$映成$v$.

(ii) 不妨假定f是首1的。由于$\sigma:K[x]\cong L[x]$，这导致$\sigma f\in L[x]$也是不可约的首1多项式。从定理1.6的证明可知映射

$$\varphi:K[x]/(f)\longrightarrow K[u]=K(u),\ \varphi[g+(f)]=g(u).$$

$$\psi:L(x)/(\sigma f)\longrightarrow L[v]=L(v),\ \psi[h+(\sigma f)]=h(v)$$

均是同构。又由系III.2.11可知映射

$$\theta:K[x]/(f)\longrightarrow L[x]/(\sigma f),\ \theta[g+(f)]=\sigma g+(\sigma f)$$

是同构。从而合成映射

$$K(u)\xrightarrow{\varphi^{-1}} K[x]/(f)\xrightarrow{\theta} L[x]/(\sigma f)\xrightarrow{\psi} L(v)$$

是域的同构，并且$g(u)\longmapsto(\sigma g)(v)$。特别地，$\psi\theta\varphi^{-1}$在$K$上与$\sigma$一致，并且将$u$映为$v$（因为由习题III.1.15知$\sigma(1_K)=1_L$）。∎

系1.9 假设E和F均是K的扩域，而$u\in E$和$v\in F$均在K上是代数的。则u和v是同一个不可约多项式$f\in K[x]$的根的充要条件是存在域的同构$K(u)\cong K(v)$，它将u映成v并且在K上为恒等映射。

证明 ($\Longrightarrow$) 在定理1.8中取$\sigma=1_K$（从而对每个$f\in K[x]$，$\sigma f=f$）。

($\Longleftarrow$) 假设$\sigma:K(u)\cong K(v)$，其中$\sigma(u)=v$，并且对每个$k\in K$，$\sigma(k)=k$。令$f\in K[x]$是代数元素u的极小多项式。如果f

$= \sum_{i=0}^{n} k_i x^i$，则$0 = f(u) = \sum_{i=0}^{n} k_i u^i$。因此 $0 = \sigma\left(\sum_{i=0}^{n} k_i u^i\right) = \sum_i \sigma(k_i u^i) = \sum_i \sigma(k_i)\sigma(u^i) = \sum_i k_i \sigma(u^i) = \sum_i k_i v^i = f(v)$。∎

至此为止，我们总是谈多项式$f \in K[x]$在K的某个给定扩域F中的根。下一定理表明，预先给出F实际上不是必要的。

定理1.10 如果K是域而$f \in K[x]$是n次多项式，则存在 K的单扩张$F = K(u)$，使得

(i) $u \in F$是f的根；

(ii) $[K(u):K] \leqslant n$，并且等式成立的充要条件是f在$K[x]$中不可约；

(iii) 如果f在$K[x]$ 中不可约，则 不 计 K- 同构（即在K上为恒等映射的同构） $K(u)$ 是唯一决定的。

注记：根据 (iii)，我们通常可称域F是将不可约多项式 $f \in K[x]$ 的一个根添加到域K 中所得到的。

证明概要 我们可以假定f是不可约的（不然的话，将f改成它的一个不可约因子）。于是 (f) 是 $K[x]$ 中 的极大理想（定理III.3.4和系III.6.4），而商环$F = K[x]/(f)$是域（定理III.2.20）。此外，正则射影$\pi: K[x] \to K[x]/(f) = F$ 在K上的限制是单射（因为只有 0 是$K[x]$之极大理想中的常数）。从而F包含有 $\pi(K) \cong K$。于是F可看成是K的扩域（这需要将 K 等同于 $\pi(K)$）。对于 $x \in K[x]$，令$u = \pi(x) \in F$。验证$F = K(u)$ 并且在F中$f(u) = 0$。于是由定理1.6推出 (ii) 而由系1.9给出 (iii)。 ∎

在本节的其余部分，我们将讨论域的代数扩张的一些重要的基本事实。

定理1.11 如果F是K的有限维扩域，则F是K上有限生成的代数扩张。

证明 如果$[F:K]=n$，$u\in F$，则$n+1$元集合$\{1_K, u, u^2, \cdots, u^n\}$必然是线性相关的。从而存在不全为零的$a_i\in K$，使得$a_0+a_1u+\cdots+a_nu^n=0$。从而$u$在$K$上是代数的。因为$u$是$F$中任意元素，从而$F$是$K$的代数扩张。如果$\{v_1,\cdots,v_n\}$是$F$在$K$上的一组基，不难看出$F=K(v_1,\cdots,v_n)$。∎

定理1.12 如果F是K的扩域而X是F的子集，使得$F=K(X)$，并且X中每个元素在K上都是代数的，则F是K的代数扩张。又若X为有限集合，则F是K的有限维扩张。

证明 如果$v\in F$，则存在某些$u_i\in X$，使得$v\in K(u_1,\cdots,u_n)$（定理1.3），并且有子域塔：

$K\subset K(u_1)\subset K(u_1,u_2)\subset\cdots\subset K(u_1,\cdots,u_{n-1})\subset K(u_1,\cdots,u_n)$。对于每个$i\geqslant 2$，因为$u_i$在$K$上是代数的，从而必然在$K(u_1,\cdots,u_{i-1})$上也是代数的。假设$u_i$在$K(u_1,\cdots,u_{i-1})$上的次数为$r_i$。由于$K(u_1\cdots,n_{i-1})(u_i)=K(u_1,\cdots,u_i)$，由定理1.6我们有$[K(u_1,\cdots,u_i):K(u_1,\cdots,u_{i-1})]=r_i$。再令$r_1$为$u_1$在$K$上的次数。重复使用定理1.2，即可证明$[K(u_1,\cdots,u_n):K]=r_1r_2\cdots r_n$。根据定理1.11可知$K(u_1,\cdots,u_n)$（从而$v$）在$K$上是代数的。由于$v$为$F$中的任意元素，从而$F$是$K$的代数扩张。如果$X=\{u_1,\cdots,u_n\}$是有限集合，用同样方法（取$F=K(u_1,\cdots,u_n)$）可以证明$[F:K]=r_1r_2\cdots r_n$是有限的。∎

定理1.13 如果F是E的代数扩张，而E是K的代数扩张，则F

是K的代数扩张.

证明 设$u\in F$. 由于u在E上是代数的，从而有$b_i\in E(b^n\neq 0)$，使得$b_nu^n+\cdots+b_1u+b_0=0$。因此u在子域$K(b_0,\cdots,b_n)$上是代数的. 从而对于域塔

$$K\subset K(b_0,\cdots,b_n)\subset K(b_0,\cdots,b_n)(u),$$

由定理1.6可知$[K(b_0,\cdots,b_n)(u):K(b_0,\cdots,b_n)]$是有限的（因为$u$在$K(b_0,\cdots,b_n)$上是代数的），而由定理1.12可知$[K(b_0,\cdots,b_n):K]$是有限的（因为每个$b_i$在$K$上均是代数的）。因此$[K(b_0,\cdots,b_n)(u):K]$是有限的（定理1.2）。于是$u\in K(b_0,\cdots,b_n)(u)$在$K$上是代数的（定理1.11）。由于$u$是$F$中的任意元素，从而$F$是$K$的代数扩张。∎

定理1.14 假设F是K的扩张，而E是F中在K上代数的全部元素所构成的集合。则E是F的子域（E当然是K的代数扩张）。

子域E显然是K在F中的唯一极大代数扩张。

证明 如果u，$v\in E$，根据定理1.12，$K(u,v)$是K的代数扩张。由于$u-v$和$uv^{-1}(v\neq 0)$也在$K(u,v)$中，从而$u-v$，$uv^{-1}\in E$。这表明E是域（见定理I.2.5）。∎

附录：圆规直尺作图

我们现在使用域的扩张来解决古代两个著名的数学问题。

(A) 是否可以用圆规直尺三等分任意的角？

(B) 是否可以用圆规直尺将一个正立方体加倍（即构作出正

立方体的一条边，使该正立方体的体积为另一给定的正立方体积的二倍)?

我们假定读者熟悉标准的圆规直尺作图方法，几乎每本平面几何教科书都要讲授的.例如:给了一条直线L和L外一点P，可构作出唯一的一条直线通过P并且与L平行（或者与L垂直）. 这里和今后所谈“可构作”，均是指“可以用圆规直尺作出”的意思.

进一步，我们将按下述方式采用解析几何的观点. 我们显然可以用圆规直尺构作出两个相互垂直的直线（两个坐标轴）. 选取一个单位长度之后我们可以构作平面上所有的整坐标点（即它们恰好为平行于两个坐标轴的适当直线的交点).现在我们就会看到，上述两个问题的解归结于：平面上还有哪些点可以用圆规直尺构作出来.

如果F是域$\mathbb{R}$的一个子域，则我们把实平面的子集{点(c,d)| $c\in F$, $d\in F$}称作F-平面. 如果P和Q是F-平面中两个不同的点，则通过P和Q的唯一直线叫作一条F-直线，而以P为圆心和线段PQ的长度为半径的圆叫作一个F-圆. 不难证明，每个F-直线都有形如$ax+by+c=0$ (a, b, $c\in F$) 的方程，而每个F-圆都有形如$x^2+y^2+ax+by+c=0$ (a, b, $c\in F$) 的方程（习题 24).

引理1.15 如果F为实数域$\mathbb{R}$的子域，并且令L_1和L_2为两条不平行的F-直线，c_1和c_2是两个不同的F-圆. 则

(i) $L_1\cap L_2$是F-平面中的点;

(ii) $L_1\cap C_1=\phi$，或者存在某个元素$u\in F(u\geqslant 0)$，使得$L_1\cap C_1$是$F(\sqrt{u})$-平面中的一点或者两点.

(iii) $C_1\cap C_2=\phi$，或者存在某个元素$u\in F(u\geqslant 0)$，使得$C_1\cap C_2$是$F(\sqrt{u})$-平面中的一点或者两点.

证明概要 (i) 作为练习。

(iii) 如果圆C_1是$x^2+y^2+a_1x+b_1y+c=0$，圆C_2是$x^2+y^2+a_2x+b_2y+c_2=0$(由引理前面的注记，可取$a_i,b_i,c_i\in F$)，证明$C_1\cap C_2$也是C_1，C_2与直线L：$(a_1-a_2)x+(b_1-b_2)y+(c_1-c_2)=0$之交。证明$L$是$F$-直线。于是便将情形(iii)归结为情形(ii)。

(ii) 假设L_1有方程$dx+ey+f=0$ (d, e, $f\in F$)。$d=0$的情形留给读者作为练习。如果$d\neq 0$，我们不妨假定$d=1$(为什么?)，从而$x=(-ey-f)$。如果$(x, y)\in L_1\cap C_1$，则通过变量代换给出C_1的方程为$0=(-ey-f)^2+y^2+a_1(-ey-f)+b_1y+c_1=Ay^2+By+c=0$，其中$A$，$B$，$C\in F$。如果$A=0$，则$y\in F$，从而$x\in F$，于是$x$，$y\in F(\sqrt{1})=F$。如果$A\neq 0$，又不妨假定$A=1$，则$y^2+By+c=0$，配方后得到$(y+B/2)^2+(c-B^2/4)=0$。从而或者$L_1\cap C_1=\phi$，或者$x$，$y\in F(\sqrt{u})$，其中$u=-c+B^2/4\geqslant 0$。 ∎

实数c称作可构作的，是指它可以从整坐标点出发，通过有限次的圆规直尺作图构作出来。显然，c (或者$(c,0)$)的可构作性等价于长为$|c|$的直线(利用圆规直尺)的可构作性。进而，平面上点(c, d)可以由圆规直尺构作出来，当且仅当c和d都是可构作的实数。整数显然是可构作的，由此不难证明下列诸事实(见习题25)：

(i) 每个有理数均是可构作的；

(ii) 如果$c>0$是可构作的，则$\sqrt{c}$是可构作的；

(iii) 如果c和d是可构作的，则$c\pm d$，cd和$c/d(d\neq 0)$都是可构作的，从而全体可构作数形成实数域的一个子域，并且它包含有理数域。

命题1.16 如果实数 c 是可构作的，则 c 在有理数域 $\mathbb{Q}$ 上是代数的，并且它的次数是 2 的方幂。

证明 上面的注记表明，我们可以从 $\mathbb{Q}$-平面出发。c 是可构作的，指的是从 $\mathbb{Q}$-平面开始，通过有限次允许的圆规直尺作图能够构作出 $(c,0)$ 来。而在构作的过程中，该平面中的每个点都是构作时所使用的直线与圆彼此之间的交点，因为这是只用圆规直尺给出新点的唯一办法。在这个过程中，第一步是构作直线或者圆，它们都是由两个点所完全决定的（对于圆则是由圆心 P 和半径 PT 所决定的）。这些点可以取成 $\mathbb{Q}$-平面上的点，也可以随意选取，但是对于后一情形，我们也可以取成是 $\mathbb{Q}$-平面中的点。类似地，在以后的每一步，决定直线和圆的两点或者取自 $\mathbb{Q}$-平面，或者取为前面各步中已经构作出的点。按照引理 1.15，构作出来的第一个新点属于 $\mathbb{Q}(\sqrt{u})$-平面，其中 $u\in\mathbb{Q}$，或者等价地说成：属于 $\mathbb{Q}(v)$-平面，其中 $v^2\in\mathbb{Q}$。这样一个扩域对于 $\mathbb{Q}$ 的次数是 $1=2^\circ$ 或者 2（视 v 是否属于 $\mathbb{Q}$ 而定）。类似地，构作出来的下一个新点在 $\mathbb{Q}(v,w)$-平面中，其中 $\mathbb{Q}(v,w)=\mathbb{Q}(v)(w)$，$w^2\in\mathbb{Q}(v)$。由此可知，经过有限次圆规直尺作图我们得到一个长度有限的域塔：

$$\mathbb{Q}\subset\mathbb{Q}(v_1)\subset\mathbb{Q}(v_1,v_2)\subset\cdots\subset\mathbb{Q}(v_1,\cdots,v_n)。$$

其中 $v_i^2\in\mathbb{Q}(v_1,\cdots,v_{i-1})$，并且 $[\mathbb{Q}(v_1,\cdots,v_i):\mathbb{Q}(v_1,\cdots,v_{i-1})]=1$ 或者 2 $(2\leqslant i\leqslant n)$。因此，按照这个过程构作出来的点 $(c,0)$ 在 F-平面上，其中 $F=\mathbb{Q}(v_1,\cdots,v_n)$。根据定理 1.2，$[F:\mathbb{Q}]$ 是 2 的方幂。从而 c 在 $\mathbb{Q}$ 上是代数的（定理 1.11）。由 $\mathbb{Q}\subset\mathbb{Q}(c)\subset F$ 导致 $[\mathbb{Q}(c):\mathbb{Q}]$ 能够整除 $[F:\mathbb{Q}]$（定理 1.2），从而 c 在 $\mathbb{Q}$ 上的次数 $[\mathbb{Q}(c):\mathbb{Q}]$ 也是 2 的方幂。∎

系1.17 60°角不能用圆规直尺三等分。

证明 假如可以三等分60°角，我们便可以构作一个锐角是20°的直角三角形。从而便能够构作实数cos20°（习题25）。但是从平面三角学我们知道，对于任意角度α

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha.$$

如果$\alpha = 20°$，则$\cos 3\alpha = \cos 60° = \frac{1}{2}$，从而cos20°是方程$\frac{1}{2} = 4x^3 - 3x$的根，因此也是多项式$8x^3 - 6x - 1$的根。然而，这个多项式在$\mathbb{Q}[x]$中是不可约的（见定理III.6.6和命题III.6.8）。从而cos20°在$\mathbb{Q}$上的次数是3，根据命题1.16，它是不能构作的。∎

系1.18 不能用圆规直尺将边长为1的正立方体加倍（即构作体积为2的正立方体）。

证明 如果S是体积为2的正立方体的边长，则S是$x^3 - 2$的根，利用Eisenstein判别法（定理III.6.15），可知$x^3 - 2$在$\mathbb{Q}[x]$中是不可约的。从而由命题1.16便知S是不可构作的。∎

习　题

注记：若不特别说明，则F永远为域K的扩域，而$\mathbf{Q}, \mathbf{R}, \mathbf{C}$分别表示有理数域、实数域和复数域。

1. (a) $[F:K] = 1 \Longleftrightarrow F = K$。

   (b) 如果$[F:K]$是素数，则在F和K之间不再有中间域。

   (c) 如果$u \in F$在K上的次数是n，则n整除$[F:K]$。

2. 给出有限生成但维数不有限的域的扩张的例子。[提示：考虑超越扩张。]

3. 如果u_1, …, $u_n \in F$, 则域$K(u_1, \cdots, u_n)$是(同构于)环$K[u_1, \cdots, u_n]$的商域.

4. (a) 对于任意u_1, …, $u_n \in F$ 和任意置换 $\sigma \in S_n$, $K(u_1, \cdots, u_n) = K(u_{\sigma 1}, \cdots, u_{\sigma n})$.

(b) $K(u_1, \cdots, u_{n-1})(u_n) = K(u_1, \cdots, u_n)$.

(c) 叙述并证明对于$K[u_1, \cdots, u_n]$的类似于(a)和(b)的命题.

(d) 如果每个u_i在K上均是代数的, 则$K(u_1, \cdots, u_n) = K[u_1, \cdots, u_n]$.

5. 设L和M是F的子域而LM是它们的合成.

(a) 如果$K \subset L \cap M$并且$M = K(S)$, 其中$S \subset M$, 则$LM = L(S)$.

(b) 何时LM等于集合论中的并集$L \cup M$?

(c) 如果E_1, …, E_n均是F的子域, 求证

$$E_1E_2\cdots E_n = E_1(E_2(E_3(\cdots(E_{n-1}(E_n))\cdots).$$

6. $K(x_1, \cdots, x_n)$中每个不属于K的元素在K上均是超越的.

7. 如果v在$K(u)$上是代数的, 其中$u \in F$, 并且v在K上是超越的, 则u在$K(v)$上是代数的.

8. 如果$u \in F$在K上是代数的并且次数为奇数, 则u^2在K上也是奇次代数数, 并且$K(u) = K(u^2)$.

9. 如果$x^n - a \in K[x]$是不可约的, 并且$u \in F$是$x^n - a$的根, 而m整除n, 求证u^m在K上的次数为n/m. u^m在K上的不可约多项式是什么?

10. 如果F是K的代数扩张而D是整环, 并且$K \subset D \subset F$, 则D是域.

11. (a) 给出域扩张$K \subset F$的例子, 使得$u, v \in F$在K上是超越的, 但是$K(u,v) \supsetneq K(x_1, x_2)$. [提示: 考虑$v$对于域$K(u)$的性状.]

(b) 叙述并证明定理1.5到n个超越元素u_1, …, u_n情形的推广.

12. 如果$d \geqslant 0$为整数但不是平方数, 刻划域$\mathbf{Q}(\sqrt{d})$. 并求出一个生成此域的元素集合.

13. (a) 考虑$\mathbf{Q}$的扩域$\mathbf{Q}(u)$, 其中u是$x^3 - 6x^2 + 9x + 3$的实根. (为什么此多项式不可约?)将下列元素用基$\{1, u, u^2\}$表达出来: u^4, u^5, $3u^5 -$

u^4+2，$(u+1)^{-1}$，$(u^2-6u+8)^{-1}$。

(*b*) 如果u是x^5+2x+2的实根，用$\mathbf{Q}(u)$的基$\{1, u, u^2, u^3, u^4\}$表达下列元素：$(u^2+2)(u^3+3u)$，u^{-1}，$u^4(u^4+3u^2+7u+5)$，$(u+2)(u^2+3)^{-1}$。

14. (*a*) 如果$F=\mathbf{Q}(\sqrt{2}, \sqrt{3})$，求$[F:\mathbf{Q}]$和$F$在$\mathbf{Q}$上的一组基。

(*b*) 对于域$F=\mathbf{Q}(i, \sqrt{3}, \omega)$作同样的事情。其中$i\in\mathbf{C}$，$i^2=-1$，而$\omega$是三次复单位根。

15. 在域$K(x)$中，令$u=x^3/(x+1)$。求证$K(x)$是域$K(u)$的单扩张。$[K(x):K(u)]=?$

16. 域$\mathbf{C}$，$\mathbf{Q}(i)$和$\mathbf{Q}(\sqrt{2})$作为$\mathbf{Q}$上的向量空间是同构的。但作为域则彼此互不同构。

17. 求域Z_2上一个2次不可约多项式f。将f的一个根u添加到Z_2中，得到一个4元域$Z_2(u)$。利用同样方式构作一个8元域。

18. 一个复数如果在$\mathbf{Q}$上是代数的，便称它是一个代数数。又若它是$\mathbf{Z}[x]$中某个首1多项式的根，便称它是一个代数整数。

(*a*) 如果u是一个代数数，则存在整数n，使nu是代数整数。

(*b*) 如果$r\in\mathbf{Q}$是代数整数，则$r\in\mathbf{Z}$。

(*c*) 如果u是代数整数，$n\in\mathbf{Z}$，则$u+n$和nu均是代数整数。

(*d*) 两个代数整数的和与积仍旧是代数整数。

19. 如果$u, v\in F$在K上分别是m次和n次代数的，则$[K(u, v):K]\leqslant mn$。又如果$(m, n)=1$，则$[K(u, v):K]=mn$。

20. 设L和M是扩张$K\subset F$的中间域。

(*a*) $[LM:K]$有限$\Longleftrightarrow$$[L:K]$和$[M:K]$均有限。

(*b*) 如果$[LM:K]$有限，则$[L:K]$和$[M:K]$均可以整除$[LM:K]$，并且

$$[LM:K]\leqslant[L:K][M:K].$$

(*c*) 如果$[L:K]$和$[M:K]$均有限并且互素，则

$$[LM:K]=[L:K]\cdot[M:K].$$

(*d*) 如果L和M均是K的代数扩张，则LM也是K上的代数扩张。

21. (*a*) 令L和M是扩张$K\subset F$的中间域，并且在K上都是有限维的。假设$[LM:K]=[L:K][M:K]$，求证$L\cap M=K$。

(*b*) 如果$[L:K]$或者$[M:K]$是2，则(*a*)的逆命题也成立。

(*c*) 利用2的实立方根和复立方根给出一个例子，使得$L\cap M=K$，$[L:K]=[M:K]=3$，但是$[LM:K]<9$。

22. F是K的代数扩张$\Longleftrightarrow$对于每个中间域E和每个单同态$\sigma:E\longrightarrow E$，如果$\sigma$在$K$上是恒等映射，则$\sigma$必为$E$的自同构。

23. 如果$u\in F$在$K(X)$上是代数的，其中$X\subset F$，则存在有限子集合$X'\subset X$，使得u在$K(X')$上是代数的。

24. 假设F是$\mathbf{R}$的子域，而P和Q均是F-平面中的点。

(*a*) 过P和Q的直线有如下形式的方程：$ax+by+c=0$，其中a，b，$c\in F$。

(*b*) 中心为P和半径为线段PQ的圆有如下形式的方程：$x^2+y^2+ax+by+c=0$，其中a，b，$c\in F$。

25. 设c和d是可构作的实数。则

(*a*) $c+d$和$c-d$也是可构作的；

(*b*) 如果$d\neq 0$，则c/d也是可构作的。[提示：如果$(x,0)$是x轴与一直线的交点，该直线过$(0,1)$并且与连接$(0,d)$和$(c,0)$两点的直线平行，则$x=c/d$。]

(*c*) cd是可构作的。[提示：利用(*b*)。]

(*d*) 可构作的实数形成$\mathbf{R}$的一个子域并且包含$\mathbf{Q}$。

(*e*) 如果$c\geqslant 0$，则$\sqrt{c}$是可构作的。[提示：过点$(1,0)$作垂直于x轴的直线。该直线在以$\left(\frac{c+1}{2},0\right)$为圆心和$\frac{c+1}{2}$为半径的上半圆中所截得线段之长度即为$\sqrt{c}$。]

26. 设E_1和E_2是F的子域而X是F的子集合，如果E_1中每个元素在E_2上均是代数的，则$E_1(X)$中每个元素在$E_2(X)$上均是代数的。[提示：$E_1(X)\subset(E_2(X))(E_1)$，并利用定理1.12。]

2. 基本定理

我们要定义任意域的伽罗华群，然后用它来定义伽罗华扩张．本节的其余部分是证明伽罗华理论的基本定理(定理2.5)，它可以使我们将关于域，多项式和域扩张方面的问题转化成群论的语言．本节后面的附录讨论对称有理函数，并且给出一些扩张的例子，使它们的伽罗华群为任意事先给定的有限群．

假设F是域．全部(域)自同构$F\to F$所组成的集合$\mathrm{Aut}F$对于函数的合成运算形成一个群(习题1)．它一般不是Abel群．伽罗华的重要发现是：关于域(特别是关于域上多项式的根)的许多问题事实上等价于该域自同构群中的某些群论问题．而在这些问题中，它们通常不仅与域有关，也与F的(适当选取的)子域有关．换句话说，与域的扩张有关．

如果F是K的扩域，我们在第1节中已经看到，F的K-模(向量空间)结构是非常重要的．从而自然去考虑F中也是K-模映射的那些自同构．所有这些自同构所组成的集合显然是$\mathrm{Aut}F$的子群．

更一般地，假设E和F均是域K的扩域．如果$\sigma:E\to F$是域的非零同态，由习题III.1.15可知$\sigma(1_E)=1_F$．如果σ又是K-模同态，则对于每个$k\in K$，

$$\sigma(k)=\sigma(k1_E)=k\sigma(1_E)=k\cdot 1_F=k.$$

反过来，如果域同态$\sigma:E\to F$将K逐元固定(即对于每个$k\in K$，$\sigma(k)=k$)，则σ不为零，并且对于每个$u\in E$，

$$\sigma(ku)=\sigma(k)\sigma(u)=k\sigma(u).$$

从而σ是K-模同态。

定义2.1 设E和F是域K的扩域。则非零映射$\sigma: E \to F$叫作一个K-同态，是指它即是域同态同时又是K-模同态。类似地，一个域自同构$\sigma \in \mathrm{Aut}F$如果又是K-同态，便称σ为F的一个K-自同构。F之全体K-自同构所形成的群叫作F在K上的伽罗华群，并且表示成$\mathrm{Aut}_K F$。

注记：我们也可以类似地定义K-单同态和K-同构。今后我们将把$\mathrm{Aut}_K F$的幺元素和它的一元子群都写成1。

例 假设$F = K(x)$，其中K是任意域。对于每个$a \in K$，$a \neq 0$，映射$\sigma_a: F \to F$，$f(x)/g(x) \longmapsto f(ax)/g(ax)$是$F$的$K$-自同构（这可直接证明，也可以利用系III.2.21(iv)，III.4.6，III.5.6，以及定理III.4.4(ii)）。如果K是无限域，则存在无限多个不同的自同构σ_a，因而$\mathrm{Aut}_K F$是无限群。类似地，对于每个$b \in K$，映射$\tau_b: F \to F$，$f(x)/g(x) \longmapsto f(x+b)/g(x+b)$是$F$的$K$-自同构。如果$a \neq 1_K$而$b \neq 0$，则$\sigma_a \tau_b \neq \tau_b \sigma_a$，从而$\mathrm{Aut}_K F$是非交换群。还参见习题6。

定理2.2 假设F是K的扩域，$f \in K[x]$。如果$u \in F$是f的根而$\sigma \in \mathrm{Aut}_K F$，则$\sigma(u) \in F$也是$f$的根。

证明 如果$f = \sum_{i=1}^{n} k_i x^i$，则$f(u) = 0$导致$0 = \sigma(f(u)) = \sigma(\sum k_i u^i) = \sum \sigma(k_i)\sigma(u^i) = \sum k_i \sigma(u)^i = f(\sigma(u))$。∎

定理2.2的一个重要应用是：如果u在K上是代数的，并且它的极小多项式$f \in K[x]$的次数是n，则每个自同构$\sigma \in \mathrm{Aut}_K K(u)$由它在$u$上的作用所完全确定（因为根据定理1.6，$\{1_K, u, \cdots, u^{n-1}\}$

是$K(u)$在K上的一组基)。按照定理2.2，$\sigma(u)$是f的根。从而$|\mathrm{Aut}_K K(u)| \leqslant m$，其中$m$是$f$在$K(u)$中相异根的个数(由定理III.6.7可知$m \leqslant n$)。

例 如果$F=K$，则$\mathrm{Aut}_K F$只包含恒等映射。但是反命题是不对的。例如令u为2的实立方根(从而$\boldsymbol{Q} \subsetneq \boldsymbol{Q}(u) \subset \boldsymbol{R}$)，则$\mathrm{Aut}_Q Q(u)$是一元群，因为$u$的象只能是$x^3-2$之根，而它的其余两个根是复根。类似地，$\mathrm{Aut}_Q R$是一元群(习题2)。

例 $\boldsymbol{C}=\boldsymbol{R}(i)$而$\pm i$是$x^2+1$的根。则$\mathrm{Aut}_Q C$的阶至多为2。不难证明，复共轭($a+bi \longmapsto a-bi$)是$\boldsymbol{C}$的$\boldsymbol{R}$-自同构且并不是恒等自同构，从而$|\mathrm{Aut}_R \boldsymbol{C}|=2$，于是$\mathrm{Aut}_R \boldsymbol{C} \cong Z_2$。类似地可知$\mathrm{Aut}_Q Q(\sqrt{3}) \cong Z_2$。

例 如果$F=Q(\sqrt{2}, \sqrt{3})=Q(\sqrt{2})(\sqrt{3})$。由于$x^2-3$在$Q(\sqrt{2})$上不可约，从定理1.2的证明和定理1.6可知$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$是$F$在$Q$上的一组基。因此，如果$\sigma \in \mathrm{Aut}_Q F$，则$\sigma$由$\sigma(\sqrt{2})$和$\sigma(\sqrt{3})$所完全确定。按照定理2.2，$\sigma(\sqrt{2})=\pm\sqrt{2}$，$\sigma(\sqrt{3})=\pm\sqrt{3}$，这意味着至多有四个不同的$K$-自同构。验证这四种可能情况实际上均是$F$的$Q$-自同构，并且$\mathrm{Aut}_Q F \cong Z_2 \oplus Z_2$。

我们在附录中(命题2.16)要证明，对于任意一个给定的有限群G，都有一个域的扩张以G为它的伽罗华群。但是，如果预先指明一个域(例如Q)，是否每个有限群都是该域对于它的某个扩域的伽罗华群，这是一个未解决的问题。

伽罗华理论的基本思想是在域扩张$K \subset F$的中间域和伽罗华群$\mathrm{Aut}_K F$的子群之间建立某种对应关系。虽然我们最感兴趣的是F在K上有限维的情形，但是我们将作尽可能一般化的讨论。为了建立这种对应关系，第一步是下面的定理。

定理2.3 假设F是K的扩域，E是一个中间域，H是$\mathrm{Aut}_K F$的一个子群．则

(i) $H'=\{v\in F\mid \sigma(v)=v$，对于每个$\sigma\in H\}$是一个中间域；

(ii) $E'=\{\sigma\in \mathrm{Aut}_K F\mid \sigma(u)=u$，对于每个$u\in E\}=\mathrm{Aut}_E F$是$\mathrm{Aut}_K F$的一个子群．

证明作为练习． ∎

域H'叫作H在F中的固定域(虽然这是很标准的术语，对于它却没有通用的符号，但是我们这里采用"加撇"的记号会有益处的)．同样地，在觉得方便的时候，我们仍用E'表示定理中的群$\mathrm{Aut}_E F$．如果将$\mathrm{Aut}_K F$表示成G，则不难看出，一方面我们有

$$F'=\mathrm{Aut}_F F=1,\quad K'=\mathrm{Aut}_K F=G.$$

另方面我们有$1'=F$(即F是一元子群的固定域)．但是$G'=K$不一定成立(例如对于定理2.2后面的第一个例子，便有$G=1$而$G'=F\neq K$．还见习题2)．

定义2.4 设F是K的扩域，并且伽罗华群$\mathrm{Aut}_K F$的固定域是K自身，则称F是K的伽罗华扩张(或伽罗华扩域)，或者称F在K上是伽罗华的[1]．

注记：F在K上是伽罗华的$\Longleftrightarrow$对于每个$u\in F-K$，均存在K-自同构$\sigma\in \mathrm{Aut}_K F$，使得$\sigma(u)\neq u$．如果$F$是$K$的任意扩域而$K_0$是$\mathrm{Aut}_K F$的固定域(可能$K_0\neq K$)，那末不难看出，$F$在$K_0$上是伽罗华

1. 通常要求一个伽罗华扩张是有限维的，或者至少是代数的，并且通常用在第3节将要讨论的正规性和可分性来定义它．对于有限维的情形，我们的定义与通常的定义等价．我们这里的定义本质上是由Artin给出的，不过他将这样的扩张叫作"正规的"．由于(当$\mathrm{char}F\neq 0$时)"正规"一词与许多其他作者所用的"正规"定义不一致，所以我们选用了Artin的基本方法，但是保留了比较传统的术语．

的，并且$K \subset K_0$，$\mathrm{Aut}_K F = \mathrm{Aut}_{K_0} F$。

例 $\mathbb{C}$在$\mathbb{R}$上是伽罗华的。$\mathbb{Q}(\sqrt{3})$在$\mathbb{Q}$上是伽罗华的（习题5）。如果K是无限域，则$K(x)$在K上是伽罗华的（习题9）。

现在我们可以叙述伽罗华理论基本定理了。虽然离证明此定理还有一定距离，但是它可以使读者看到，我们今后的讨论将把人们导致何方。如果L和M是某个扩张的两个中间域，并且$L \subset M$，我们将维数$[M:L]$叫作L和M的相对维数。类似地，如果H和J是该伽罗华群的两个子群，并且$H < J$，我们将指数$[J:H]$叫作H和J的相对指数。

定理2.5 （伽罗华理论基本定理） 如果F是K的有限维伽罗华扩张，则在该扩张的全部中间域所构成的集合与伽罗华群$\mathrm{Aut}_K F$的全部子群所构成的集合之间存在着一一对应（由$E \longmapsto E' = \mathrm{Aut}_E F$给出），并且

(i) 两个中间域的相对维数等于对应子群的相对指数。特别地$|\mathrm{Aut}_K F| = [F:K]$。

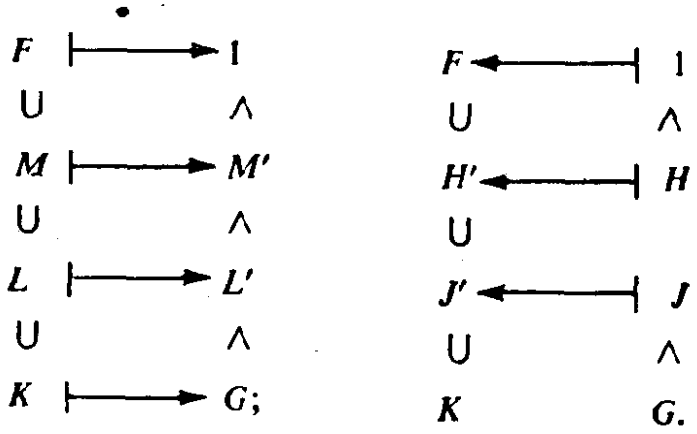
(ii) F在每个中间域E上都是伽罗华的。另一方面，E在K上是伽罗华的充要条件是对应的子群$E' = \mathrm{Aut}_E F$是$G = \mathrm{Aut}_K F$的正规子群。并且在这种情形下，G/E'是（同构于）E在K上的伽罗华群$\mathrm{Aut}_K E$。

本定理的证明需要相当多的预备知识（详细证明见引理2.14后面）。本节的其余部分就是讲授这些知识，而将构作伽罗华扩域和任意维数的伽罗华代数扩张问题放到下一节去。读者应当注意，我们在本节中证明的许多命题对于以后更一般情形也是适用的。

正如基本定理的叙述中所表明的，所谓伽罗华对应是将每个

中间域E对应F在E上的伽罗华群$\mathrm{Aut}_E F$. 反过来，这个一一对应的逆则是将其伽罗华群的每个子群对应于它在F中的固定域. 利用定理2.3中的“加撇”符号是很方便的. 于是将$\mathrm{Aut}_E F$表示成E'，而将H在F中的固定域表示成H'.

将这些加撇运算形象地绘成如下的图表，可能是有帮助的. 令L和M是扩张$K\subset F$的中间域，而J和H是其伽罗华群$G=\mathrm{Aut}_K F$的



子群. 关于加撇运算的基本事实可以形式化地由下面引理给出.

引理2.6 假设F是K的扩域，而L和M是中间域. 令H和J是$G=\mathrm{Aut}_K F$的子群. 则

(i) $F'=1$, $K'=G$;

(i′) $1'=F$;

(ii) $L\subset M\Longrightarrow M'<L'$;

(ii′) $H<J\Longrightarrow J'\subset H'$;

(iii) $L\subset L''$, $H<H''$ (其中$L''=(L')'$, $H''=(H')'$);

(iv) $L'=L'''$, $H'=H'''$.

证明概要 (i)—(iii)直接从定义得到. 为了证明(iv)的第一部分，注意由(iii)和(ii)推出$L'''<L'$，而在(iii)中以L'代替H即得到$L'<L'''$. 另一部分可以类似地证明. ∎

注记：完全有可能L''真包含L(以及H''真包含H)。根据定义可知若$G'=K$，则F在K上是伽罗华的。由于必然$K'=G$，因此F在K上是伽罗华的，当且仅当$K=K''$。类似地，F在中间域E上是伽罗华的，当且仅当$E=E''$。

设X是一个中间域或者为其伽罗华群的一个子群。如果$X=X''$，便称X是闭的。于是，F在K上是伽罗华的，当且仅当K是闭的。

定理2.7 如果F是K的扩域，则在该扩张的闭中间域与其伽罗华群的闭子群之间存在着由$E\longmapsto E'=\mathrm{Aut}_E F$给出的一一对应。

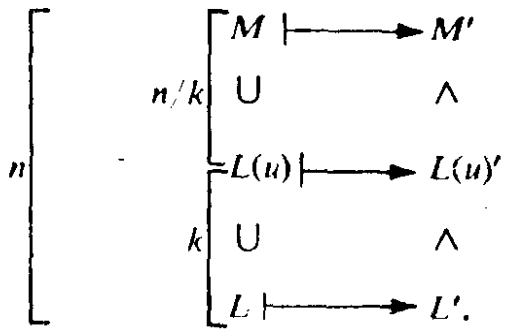
证明 作为练习。此一一对应的逆是：将每个闭子群H对应于它的固定域H'。注意由引理2.6 (iv) 可知，所有加撇的对象都是闭的。 ∎

要想使这一定理发挥效力，我们需要更明确地知道哪些中间域和子群是闭的。事实上，我们将要证明，在伽罗华代数扩张中，所有的中间域都是闭的。而对于有限维的情形，其伽罗华群的所有子群也都是闭的。开始先证明某些技术性的引理，这些引理使我们能估计各种相对维数。

引理2.8 假设F是K的扩域，L和M是中间域，并且$L\subset M$。如果$[M:L]$有限，则$[L':M']\leqslant[M:L]$。特别地，如果$[F:K]$有限，则$|\mathrm{Aut}_K F|\leqslant[F:K]$。

证明 对于$n=[M:L]$采用数学归纳法。$n=1$的情形显然是对的。如果$n>1$，并且定理对于所有$i<n$都是对的。取$u\in M$，$u\notin L$。因为$[M:L]$有限，从而u在L上是代数的（定理1.11），并且u的极小多项式$f\in L[x]$具有次数$k>1$。根据定理1.6和1.1可知

$[L(u):L]=k$, $[M:L(u)]=n/k$。从而我们有下面的图表：



现在分两种情形。如果 $k<n$，则 $1<n/k<n$。由归纳假设可知 $[L':L(u)']\leqslant k$, $[L(u)':M']\leqslant n/k$。从而 $[L':M']=[L':L(u)'][L(u)':M']\leqslant k(n/k)=n=[M:L]$，从而引理获证。另一方面，如果 $k=n$，则 $[M:L(u)]=1$ 即 $M=L(u)$。对于这种情形，为了完成证明，我们将构作一个从集合 $S=\{M'在L'中的左陪集\}$ 到集合 $T=\{多项式f\in L[x]在F中的根\}$ 的单射，由此得出 $|S|\leqslant|T|$。根据定理III.6.7我们有 $|T|\leqslant n$，而根据定义 $|S|=[L':M']$，这就表明 $[L':M']\leqslant|T|\leqslant n=[M:L]$。由此立即得到引理的最后论断，这是因为 $|\mathrm{Aut}_K F|=[\mathrm{Aut}_K F:1]=[K':F']\leqslant[F:K]$。

令 $\tau M'$ 是 M' 在 L' 中的一个左陪集。如果 $\sigma\in M'=\mathrm{Aut}_M F$，因为 $u\in M$，从而 $\tau\sigma(u)=\tau(u)$。从而陪集 $\tau M'$ 中每个元素在 u 上的作用是相同的，即均将 u 映成 $\tau(u)$。因为 $\tau\in L'=\mathrm{Aut}_L F$，而 u 是 $f\in L[x]$ 的根，由定理2.2可知 $\tau(u)$ 也是 f 的根。由此我们可以定义映射 $S\longmapsto T$，$\tau M'\longmapsto\tau(u)$，如果 $\tau(u)=\tau_0(u)$（τ，$\tau_0\in L'$），则 $\tau_0^{-1}\tau(u)=u$，从而 $\tau_0^{-1}\tau$ 固定 u。因此 $\tau_0^{-1}\tau$ 逐元固定 $L(u)=M$（见定理1.6(iv)），从而 $\tau_0^{-1}\tau\in M'$。于是由系I.4.3可知 $\tau_0 M'=\tau M'$，因而映射 $S\longmapsto T$ 是单射。 ∎

附录中给出引理2.8的某些重要应用。我们现在证明关于伽罗

华群的子群的一个类似的引理。

引理2.9 假设F是K的扩域，H和J是伽罗华群$\mathrm{Aut}_K F$的子群，并且$H<J$。如果$[J:H]$是有限的，则$[H':J']\leqslant[J:H]$。

证明 令$[J:H]=n$，并假设$[H':J']>n$。则存在u_1，u_2，…，$u_{n+1}\in H'$，使得它们在J'上是线性无关的。以$\{\tau_1,\tau_2,\cdots,\tau_n\}$表示$H$在$J$中的左陪集之完全代表系（即$J=\tau_1 H\cup\tau_2 H\cup\cdots\cup\tau_n H$，并且$\tau_j^{-1}\tau_i\in H\Longleftrightarrow i=j$）。考虑系数$\tau_i(u_j)$属于域$F$的$n+1$元$n$个方程的齐次线性方程组

$$\begin{aligned}
&\tau_1(u_1)x_1+\tau_1(u_2)x_2+\tau_1(u_3)x_3+\cdots+\tau_1(u_{n+1})x_{n+1}=0\\
&\tau_2(u_1)x_1+\tau_2(u_2)x_2+\tau_2(u_3)x_3+\cdots+\tau_2(u_{n+1})x_{n+1}=0\\
&\qquad\vdots\\
&\tau_n(u_1)x_1+\tau_n(u_2)x_2+\tau_n(u_3)x_3+\cdots+\tau_n(u_{n+1})x_{n+1}=0\qquad(1)
\end{aligned}$$

这样一个方程组永远有非平凡群（即有不全为0的解$(x_1,x_2,\cdots,x_{n+1})$，见习题 VII.2.4(*d*)。在全部非平凡解中取一组解$x_1=a_1,\cdots,x_{n+1}=a_{n+1}$，使得不为零的$a_i$的个数最少。必要时重新加以标号，我们可以假定$x_1=a_1,\cdots,x_r=a_r,x_{r+1}=\cdots=x_{n+1}=0$（其中诸$a_i\neq 0$）。将这组解的每个数均乘以$a_1^{-1}$之后，仍是该方程组的解。因此我们还可以假定$a_1=1_F$。

下面我们要证明，假设$u_1,\cdots,u_{n+1}\in H'$在J'上是线性无关的（即$[H':J']>n$），则导致存在$\sigma\in J$，使得$x_1=\sigma a_1,x_2=\sigma a_2,\cdots,x_r=\sigma a_r,x_{r+1}=\cdots=x_{n+1}=0$也是方程组(1)的解，并且$\sigma a_2\neq a_2$。因为两组解的差仍然是解，从而$x_1=a_1-\sigma a_1,x_2=a_2-\sigma a_2,\cdots,x_r=a_r-\sigma a_r,x_{r+1}=\cdots=x_{n+1}=0$也是(1)的解。但是

$a_1-\sigma a_1=1_F-1_F=0$而$a_2\neq\sigma a_2$，从而$x_1=0$，$x_2=a_2-\sigma a_2$，…，$x_r=a_r-\sigma a_r$，$x_{r+1}=\cdots=x_{n+1}=0$是(1)的一组非平凡解（因为$x_2\neq0$），并且非零分量至多有$r-1$个。这就与解$x_1=a_1$，…，$x_r=a_r$，$x_{r+1}=\cdots=x_{n+1}=0$中非零分量个数极小性相矛盾。从而$[H':J']\leqslant n$。

为了完成证明，我们必需寻求具有所需性质的$\sigma\in J$。根据定义，诸τ_i中恰有一个（设为τ_1）属于H。因此每个i,$\tau_1(u_i)=u_i$。由于$\{a_i\}$是(1)的解，由该方程组的第1个方程给出

$$u_1a_1+u_2a_2+\cdots+u_ra_r=0$$

因为$\{u_i\}$在J'上是线性无关的，并且$\{a_i\}$不全为零，从而必有某个a_i（设为a_2）不属于J'。于是存在$\sigma\in J$，使得$\sigma a_2\neq a_2$。

现在考虑方程组

$$\begin{aligned}
&\sigma\tau_1(u_1)x_1+\sigma\tau_1(u_2)x_2+\cdots+\sigma\tau_1(u_{n+1})x_{n+1}=0\\
&\sigma\tau_2(u_1)x_1+\sigma\tau_2(u_2)x_2+\cdots+\sigma\tau_2(u_{n+1})x_{n+1}=0\\
&\vdots\\
&\sigma\tau_n(u_1)x_1+\sigma\tau_n(u_2)x_2+\cdots+\sigma\tau_n(u_{n+1})x_{n+1}=0 \qquad (2)
\end{aligned}$$

由于σ是自同构而$x_1=a_1$，…，$x_r=a_r$，$x_{r+1}=\cdots=x_{n+1}=0$是(1)的解，易知$x_1=\sigma a_1$，…，$x_r=\sigma a_r$，$x_{r+1}=\cdots=x_{n+1}=0$是(2)的解。我们断言方程组(2)不计诸方程的次序即是方程组(1)（从而$x_1=\sigma a_1$，…，$x_r=\sigma a_r$，$x_{r+1}=\cdots=x_{n+1}=0$也是(1)的解）。为此首先应当验证下面两个事实。

(i) 对于每个$\sigma\in J$，$\{\sigma\tau_1,\ \sigma\tau_2,\ \cdots\sigma\tau_n\}\subset J$是$H$在$J$中的陪集完全代表系。

(ii) 如果ξ和θ是H在J中同一陪集中的元素，则（由于$u_i\in H'$）$\xi(u_i)=\theta(u_i)(1\leqslant i\leqslant n+1)$。

于是从(i)可知存在$\{1,\ 2,\ \cdots,\ n+1\}$的一个置换$\{i_1,\ \cdots,$

$i_{n+1}\}$，使得对于每个$k=1$，2，…，$n+1$，$\sigma\tau_k$和τ_{i_k}在H对于J的同一陪集中。由(ii)便知(2)的第k个方程即是(1)的第i_k个方程。 ∎

引理2.10 假设F是K的扩域，L和M是中间域并且$L\subset M$，而H和J是伽罗华群$\mathrm{Aut}_K F$的子群并且$H<J$。

(i) 如果L是闭的并且$[M:L]$有限，则M也是闭的并且 $[L':M']=[M:L]$。

(ii) 如果H是闭的并且$[J:H]$有限，则J也是闭的并且 $[H':J']=[J:H]$。

(iii) 如果F是K的有限维伽罗华扩张，则每个中间域和其伽罗华群的每个子群都是闭的，并且$|\mathrm{Aut}_K F|=[F:K]$。

注意由(ii)（令$H=1$）推出：$\mathrm{Aut}_K F$的每个有限子群都是闭的。

证明概要 (ii) 依次使用$J\subset J''$，$H=H''$，引理2.8与引理2.9，给出

$$[J:H]\leqslant[J'':H]=[J'':H'']\leqslant[H':J']\leqslant[J:H].$$

由此导出$J=J''$和$[H':J']=[J:H]$。类似地证明(i)。

(iii) 如果E是中间域，则$[E:K]$是有限的（因为$[F:K]$是有限的）。由于F在K是伽罗华的，而K是闭的，由(i)推出E是闭的，并且$[K':E']=[E:K]$。特别若$E=F$，则$|\mathrm{Aut}_K F|=[\mathrm{Aut}_K F:1]=[K':F']=[F:K]$是有限的。从而$\mathrm{Aut}_K F$的每个子群都是有限的。由于1是闭的，由(ii)即知J是闭的。 ∎

基本定理2.5的第(i)部分可以很容易地从定理2.7与引理2.10推出来。为了证明定理2.5的第(ii)部分，我们必须决定：在伽罗华对应中，哪些中间域对应着伽罗华群的正规子群。这就是下面的引理。

假设E是扩张$K\subset F$的中间域，我们称E（对于K和F）是稳定的，是指每个K-自同构$\sigma\in \mathrm{Aut}_K F$都将$E$映射到自身之中．如果$E$是稳定的而$\sigma^{-1}\in \mathrm{Aut}_K F$是$\sigma$的逆自同构，则$\sigma^{-1}$也将$E$映到自身之中．由此可知，$\sigma|E$事实上是$E$的$K$-自同构（即$\sigma|E\in \mathrm{Aut}_K E$）．并且它的逆是$\sigma^{-1}|E$．对于有限维扩张的情形，我们将要证明：$E$是稳定的$\Longleftrightarrow E$在$K$上是伽罗华的．

引理2.11 假设F是K的扩域，

(i) 如果E是此扩域的稳定中间域，则$E'=\mathrm{Aut}_E F$是伽罗华群$\mathrm{Aut}_K F$的正规子群；

(ii) 如果H是$\mathrm{Aut}_K F$的正规子群，则H的固定域H'是此扩张的稳定中间域．

证明 (i) 如果$u\in E$而$\sigma\in \mathrm{Aut}_K F$，由稳定性可知$\sigma(u)\in E$，从而对每个$\tau\in E'=\mathrm{Aut}_E F$，$\tau\sigma(u)=\sigma(u)$．因此对每个$\sigma\in \mathrm{Aut}_K F$，$\tau\in E'$和$u\in E$，$\sigma^{-1}\tau\sigma(u)=\sigma^{-1}\sigma(u)=u$．从而$\sigma^{-1}\tau\sigma\in E'$，即$E'$在$\mathrm{Aut}_K F$中正规．

(ii) 如果$\sigma\in \mathrm{Aut}_K F$，$\tau\in H$，由正规性可知$\sigma^{-1}\tau\sigma\in E'$．因此对每个$u\in H'$，$\sigma^{-1}\tau\sigma(u)=u$．从而对每个$\tau\in H$，$\tau\sigma(u)=\sigma(u)$．于是对每个$u\in H'$，$\sigma(u)\in H'$，这就意味着$H'$是稳定的． ∎

下面三个引理较为详细地展示了稳定中间域和伽罗华扩张之间的关系，以及它们与伽罗华群之间的关系．

引理2.12 如果F是K的伽罗华扩域而E是此扩张的稳定中间域，则E在K上是伽罗华的．

证明 如果$u\in E-K$，则存在$\sigma\in \mathrm{Aut}_K F$，使得$\sigma(u)\neq u$，这是因为$F$在$K$上是伽罗华的．但是由稳定性可知$\sigma|E\in \mathrm{Aut}_K E$．因

此由定义2.4后面的注记，可知E在K上是伽罗华的。 ∎

引理2.13 如果F是K的扩域而E是此扩张的中间域，并且E是K的伽罗华代数扩张，则E（对于F和K）是稳定的。

注记：关于E是代数扩张这一假设是不可缺少的，见习题13.

证明 如果$u\in E$,令$f\in K[x]$是u的极小多项式,而令$u=u_1$，$u_2,\cdots,u_r$是f在E中不同的根。由定理III.6.7可知 $r\leqslant n=\deg f$.如果$\tau\in \mathrm{Aut}_K E$,由定理2.2可知τ是$\{u_i\}$的一个置换。从而首1多项式$g(x)=(x-u_1)(x-u_2)\cdots(x-u_r)\in E(x)$的系数被每个$\tau\in \mathrm{Aut}_K E$所固定。由于$E$在$K$上是伽罗华的，从而必然 $g\in K[x]$。现在$u=u_1$是g的根，因此$f\mid g$（定理1.6(ii)）。由于g是首1的并且$\deg g\leqslant\deg f$，从而$f=g$。所以f的全部根是彼此不同的,并且全在E中。现在若$\sigma\in \mathrm{Aut}_K F$，由定理2.2知$\sigma(u)$是$f$的根，从而$\sigma(u)\in E$。因此$E$对于$F$和$K$是稳定的。 ∎

令E是扩张$K\subset F$的中间域。K-自同构$\tau\in \mathrm{Aut}_K E$叫作可以扩充到F，是指存在$\sigma\in \mathrm{Aut}_K F$，使得$\sigma|E=\tau$。不难看出，可以扩充的$K$-自同构全体形成$\mathrm{Aut}_K E$的一个子群。注意若$E$是稳定的，则$E'=\mathrm{Aut}_E F$是$G=\mathrm{Aut}_K F$的正规子群（引理2.11），从而可以定义商群$G/E'$。

引理2.14 假设F是K的扩域，E是此扩张的稳定中间域。则商群$\mathrm{Aut}_K F/\mathrm{Aut}_E F$同构于可以扩充到$F$的全部$E$的$K$-自同构所构成之群。

证明概要 由于E是稳定的，映射$\sigma\longmapsto\sigma|E$定义出群同态$\mathrm{Aut}_K F\longrightarrow\mathrm{Aut}_K E$，它的象显然是可以扩充到$F$的全部$E$的$K$-自同构所成之群。而核是$\mathrm{Aut}_E F$，然后利用第一同构定理I.5.7即可。 ∎

定理2.5(伽罗华理论基本定理)的证明 定理2.7表明在该扩张的闭中间域和其伽罗华群的闭子群之间存在着一一对应。但是在我们的情形下，由引理2.10(iii)可知所有的中间域和子群都是闭的。从而由引理2.10(i)立刻推出定理的(i)。

(ii) 由于E是闭的 (即$E=E''$)，从而F在E上是伽罗华的。由于E在K上是有限维的 (因为F是如此)，由定理1.11便知E在K上是代数的。因此，如果E在K上是伽罗华的，则由引理2.13可知E是稳定的。由引理2.11(i)便知$E'=\mathrm{Aut}_E F$在$\mathrm{Aut}_K F$中正规。反之，如果E'在$\mathrm{Aut}_K F$中正规，则E''是稳定的中间域(引理2.11 (ii))。但是 $E=E''$，因为所有的中间域都是闭的，从而由引理2.12可知E在K上是伽罗华的。

假设E是中间域，并且在K上是伽罗华的 (从而E'在$\mathrm{Aut}_K F$中正规)。由于E和E'是闭的并且$G'=K$ (F在K上是伽罗华的)，从而由引理2.10导致 $|G/E'|=[G:E']=[E'':G']=[E:K]$。根据引理2.14，$G/E'=\mathrm{Aut}_K F/\mathrm{Aut}_E F$同构于$\mathrm{Aut}_K E$的一个 ($[E:K]$阶的)子群。但是本定理第(i)部分表明$|\mathrm{Aut}_K E|=[E:K]$ (因为 E 在K上是伽罗华的)。这就得出$G/E'\cong\mathrm{Aut}_K E$。 ∎

伽罗华理论的现代发展主要归功于Emil Artin虽然我们的处理方式在很大程度上依赖于Artin (再经过I. Kaplansky 的整理)，但是Artin的方法与这里相比，侧重处仍有所不同。Artin 的基本对象是一个给定的域F连同F的一个(有限)自同构群。然后构作 F 的一个子域K即G的固定域。

定理2.15 (Artin) 设F是域，G是F的自同构群，K是G在 F 中的固定域。则F在K上是伽罗华的。如果G 有限，则 F 是K的有

限维伽罗华扩张，并且以G为伽罗华群。

证明 在任何情况下G均是$\mathrm{Aut}_K F$的子群。如果$u \in F-K$,则存在$\sigma \in G$，使得$\sigma(u) \neq u$。因此$\mathrm{Aut}_K F$的固定子域是K，从而F在K上是伽罗华的。如果G有限，则引理2.9(取$H=1$，$J=G$)表明$[F:K]=[1':G']\leqslant[G:1]=|G|$。由于$F$在$K$上是有限维的，由引理2.10(iii)可知$G=G''$。因为由假设$G'=K$(从而$G''=K'$)从而$\mathrm{Aut}_K F=K'=G''=G$。 ∎

附录：对称有理函数

设K是域，$K[x_1, \cdots, x_n]$是多项式整环，而$K(x_1, \cdots, x_n)$是有理函数域（见定理1.5前面的例子）。由定义知$K(x_1, \cdots, x_n)$是$K[x_1, \cdots, x_n]$的商域，从而$K[x_1, \cdots, x_n] \subset K(x_1, \cdots, x_n)$(象通常那样将$f$与$f/1_K$等同)。令$S_n$为$n$个字母上的对称群。有理函数$\varphi \in K(x_1, \cdots, x_n)$叫作在$K$上对于$x_1, \cdots, x_n$是对称的，是指对每个$\sigma \in S_n$,

$$\varphi(x_1, x_2, \cdots, x_n)=\varphi(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)})。$$

每个常数多项式显然是对称函数。如果$n=4$，则多项式$f_1=x_1+x_2+x_3+x_4$，$f_2=x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4$，$f_3=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$ 和 $f_4=x_1x_2x_3x_4$ 均是对称函数。更一般地，下面一些多项式叫作K上对于$x_1, \cdots, x_n$的初等对称函数：

$$f_1=x_1+x_2+\cdots+x_n=\sum_{i=1}^{n} x_i;$$

$$f_2=\sum_{1\leqslant i<j\leqslant n}x_ix_j;$$

$$f_3=\sum_{1\leqslant i<j<k\leqslant n}x_ix_jx_k;$$

$$\vdots$$

$$f_k=\sum_{1\leqslant i_1<\cdots<i_k\leqslant n}x_{i_1}x_{i_2}\cdots x_{i_k};$$

$$\vdots$$

$$f_n=x_1x_2\cdots x_n.$$

由于这些f_i恰好是多项式$g(y)\in K[x_1,\cdots,x_n][y]$中关于$y$的诸系数，其中

$$\begin{aligned}g(y)&=(y-x_1)(y-x_2)(y-x_3)\cdots(y-x_n)\\&=y^n-f_1y^{n-1}+f_2y^{n-2}-\cdots\\&\quad+(-1)^{n-1}f_{n-1}y+(-1)^nf_n.\end{aligned}$$

由此即可证明f_i均是对称函数。

如果$\sigma\in S_n$，则映射$x_i\longmapsto x_{\sigma(i)}(1\leqslant i\leqslant n)$和

$$f(x_1,\cdots,x_n)/g(x_1,\cdots,x_n)\longmapsto f(x_{\sigma(1)},\cdots,x_{\sigma(n)})/g(x_{\sigma(1)},\cdots,x_{\sigma(n)})$$

定义出域$K(x_1,\cdots,x_n)$的一个K-自同构，我们仍旧将它表示成σ(习题16)。映射$S_n\longmapsto \mathrm{Aut}_KK(x_1,\cdots,x_n)$，$\sigma\longmapsto\sigma$显然是群的单同态，从而$S_n$可看成是伽罗华群$\mathrm{Aut}_KK(x_1,\cdots,x_n)$的子群。$S_n$在$K(x_1,\cdots,x_n)$中的固定域$E$显然恰好是由对称函数所组成的。于是，所有对称函数构成的集合E是$K(x_1,\cdots,x_n)$的一个子域，并且它包含K。于是由Artin定理2.15可知$K(x_1,\cdots,x_n)$是E的伽罗华扩张，其伽罗华群为S_n，并且维数是$n!$。

命题2.16 如果G是有限群，则存在一个域的伽罗华扩张，使它的伽罗华群与G同构。

证明 Cayley定理II.4.6是说，如果$n=|G|$，则G同构于S_n的一个子群（这个子群也表示成G）。令K为任意域，E是$K(x_1, \cdots, x_n)$中的对称有理函数域，本命题前面的讨论表明，$K(x_1, \cdots, x_n)$是E的伽罗华扩张，并且其伽罗华群为S_n。从基本定理2.5的证明可知，$K(x_1, \cdots, x_n)$是G的固定域E_1的伽罗华扩张，并且$\mathrm{Aut}_{E_1}K(x_1, \cdots, x_n)=G$。∎

本附录的其余部分是要证明关于对称函数的两个经典定理（这些内容只在第9节附录中用到）。在整个讨论中，n为正整数，K为任意域，E是$K(x_1, \cdots, x_n)$中的对称有理函数子域，$f_1, \cdots, f_n \in E$是在K上$x_1, \cdots, x_n$的初等对称函数。于是我们有域塔：

$$K \subset K(f_1, \cdots, f_n) \subset E \subset K(x_1, \cdots, x_n)。$$

在定理2.18中我们将证明$E=K(f_1, \cdots, f_n)$。

如果$u_1, \cdots, u_r \in K(x_1, \cdots, x_n)$，根据定理1.3，$K(u_1, \cdots, u_r)$中每个元素均有形式$g(u_1, \cdots, u_r)/h(u_1, \cdots, u_r)$，其中$g$，$h \in K[x_1, \cdots, x_r]$。从而我们通常把$K(u_1, \cdots, u_r)$和$K[u_1, \cdots, u_r]$中的元素分别叫作在$K$上关于$u_1$，$\cdots$，$u_r$的有理函数和多项式从而命题$E=K(f_1, \cdots, f_n)$可以叙述为：每个有理对称函数事实上均是初等对称函数$f_1, \cdots, f_n$在K上的有理函数。为了证明$E=K(f_1, \cdots, f_n)$我们需要

引理2.17 设K是域，f_1，$\cdots$，f_n是K上关于x_1，$\cdots$，x_n的初等对称函数，k是整数并且$1 \leqslant k \leqslant n-1$。如果$h_1, \cdots, h_k \in K[x_1, \cdots, x_n]$是关于$x_1, \cdots, x_k$的初等对称函数，则每个$h_j$均可以写成$K$中关于$f_1$，$\cdots$，$f_n$和$x_{k+1}$，$x_{k+2}$，$\cdots$，$x_n$的多项式。

证明概要 如果$k=n-1$，则定理是对的，因为这时$h_1=f-x_n$，$h_j=f_j-h_{j-1}x_n(2\leqslant j\leqslant n)$。然后反次序地对于$k$作数学归纳法：即假定定理当$k=r+1$时是正确的并且$r+1\leqslant n-1$。以$g_1,\cdots,g_{r+1}$表示关于$x_1,\cdots,x_{r+1}$的初等对称函数，而$h_1,\cdots,h_r$是关于$x_1,\cdots,x_r$的初等对称函数。由于$h_1=g_1-x_{r+1}$，$h_j=g_j-h_{j-1}x_{r+1}$ $(2\leqslant j\leqslant r)$，从而定理对于$k=r$也是正确的。 ∎

定理2.18 如果K是域，E是$K(x_1,\cdots,x_n)$中全体对称有理函数所构成的子域，$f_1,\cdots,f_n$是初等对称函数，则$E=K(f_1,\cdots,f_n)$。

证明概要 由于$[K(x_1,\cdots,x_n):E]=n!$ 而$K(f_1\cdots,f_n)\subset E\subset K(x_1,\cdots,x_n)$，根据定理1.2，只需证明$[K(x_1,\cdots,x_n):K(f_1,\cdots,f_n)]\leqslant n!$ 即可。令$F=K(f_1,\cdots,f_n)$并考虑下面的域塔：

$$F\subset F(x_n)\subset F(x_{n-1},\ x_n)\subset\cdots\subset F(x_2,\cdots,x_n)$$
$$\subset F(x_1,\cdots,x_n)=K(x_1,\cdots,x_n)。$$

由于$F(x_k,\ x_{k+1},\ \cdots,\ x_n)=F(x_{k+1},\cdots,x_n)(x_k)$，根据定理1.2和1.6，我们只需证明：$x_n$在$F$上是代数的并且次数$\leqslant n$，同时对每个$k<n$，$x_k$在$F(x_{k+1},\ \cdots,\ x_n)$上是代数的并且次数$\leqslant k$。为了作到这些，令$g_n(y)\in F[y]$是多项式

$$g_n(y)=(y-x_1)(y-x_2)\cdots(y-x_n)$$
$$=y^n-f_1y^{n-1}+\cdots+(-1)^nf_n。$$

由于$g_n\in F[y]$的次数为n，并且x_n是g_n的根，从而由定理1.6可知x_n在$F=K(f_1,\cdots,f_n)$上是代数的，并且次数$\leqslant n$。现在对于每个$k(1\leqslant k\leqslant n)$，定义首1多项式：

$$g_k(y)=g_n(y)/(y-x_{k+1})\cdots(y-x_n)$$
$$=(y-x_1)(y-x_2)\cdots(y-x_k)。$$

$g_k(y)$的次数显然是k，x_k为$g_k(y)$的根，并且$g_k(y)$的系数恰好是关于$x_1,\cdots,x_k$的初等对称函数。根据引理2.17，每个$g_k(y)$都属于$F(x_{k+1},\cdots,x_n)[y]$，从而x_k在$F(x_{k+1},\cdots,x_n)$上是代数的，并且次数$\leqslant k$。 ∎

现在我们要证明定理2.18对于对称多项式函数的模拟，即：K上关于$x_1,\cdots,x_n$的每个对称多项式事实上均是K上初等对称函数的多项式。换句话说，$K[x_1,\cdots,x_n]$中每个对称多项式均属于$K[f_1,\cdots,f_n]$。首先我们需要

引理2.19 设K是域，E是$K(x_1,\cdots,x_n)$中全部对称有理函数所组成的子域。则集合$X=\{x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\mid 0\leqslant i_k<k$，对于每个$k\}$是$K(x_1,\cdots,x_n)$在$E$上的一组基。

证明概要 由于$[K(x_1,\cdots,x_n):E]=n!$而$|X|=n!$，只需证明X张成$K(x_1,\cdots,x_n)$即可（见定理Ⅳ.2.5）。考虑域塔$E\subset E(x_n)\subset E(x_{n-1},x_n)\subset\cdots\subset E(x_1,\cdots,x_n)=K(x_1,\cdots,x_n)$。由于$x_n$在$E$上是代数的并且次数$\leqslant n$（根据定理2.18的证明），从而集合$\{x_n^j\mid 0\leqslant j<n\}$在$E$上张成$E(x_n)$（定理1.6）。由于$E(x_{n-1},x_n)=E(x_n)(x_{n-1})$，而$x_{n-1}$在$E(x_n)$上是代数的并且次数$\leqslant n-1$，从而集合$\{x_{n-1}^i\mid 0\leqslant i\leqslant n-1\}$在$E(x_n)$上张成$E(x_{n-1},x_n)$。从定理Ⅳ.2.16证明中第2段的推理方法可知，集合$\{x_{n-1}^i x_n^j\mid 0\leqslant j<n-1,\ 0\leqslant j<n\}$在$E$上张成$E(x_{n-1},x_n)$。这给出归纳证明的第一步。然后用类似的推理即可完成证明。∎

命题2.20 设K是域，$f_1,\cdots,f_n$是$K(x_1,\cdots,x_n)$中的初等对称函数。

(i) $K[x_1,\cdots,x_n]$中每个多项式均可唯一地写成系数属于

$K[f_1, \cdots, f_n]$的$n!$个元素 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$($0 \leqslant i_k < k$对于每个$k$) 的线性组合；

(ii) $K[x_1, \cdots, x_n]$中每个对称多项式都属于$K[f_1, \cdots, f_n]$。

证明 设$g_k(y)$($k=1, \cdots, n$)如定理2.18的证明中所示。那里已经证明了$g_k(y)$的系数是关于$f_1, \cdots, f_n$和$x_{k+1}, \cdots, x_n$的(K上)多项式。由于g_k是k次首1多项式并且$g_k(x_k)=0$，从而x_k^k可以表示成K上关于$f_1, \cdots, f_n$，$x_{k+1}, \cdots, x_n$和 x_k^i($i \leqslant k-1$)的一个多项式。如果我们从 $k=1$开始一步一步地将 x_k^k 的这个表达式代到多项式 $h \in K[x_1, \cdots, x_n]$中，结果得到关于$f_1, \cdots, f_n$，$x_1, \cdots, x_n$ 的一个多项式，其中每个 x_k 的最高指数是$k-1$。换句话说，h是系数属于$K[f_1, \cdots, f_n]$的$n!$个元素$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$($i_k < k$,对于每个$k$)的线性组合。此外，这些系数多项式是唯一确定的，因为由引理2.19，

$$\{x_1^{i_1}\cdots x_n^{i_n} \mid 0 \leqslant i_k < k, \text{ 对于每个} k\}$$

在 $E=K(f_1, \cdots, f_n)$上是线性无关的。这就证明了 (i)，并且也证明了：如果多项式 $h \in K[x_1, \cdots, x_n]$ 是系数属于 $K(f_1, \cdots, f_n)$ 的 $x_1^{i_1}\cdots x_n^{i_n}$($i_k < k$)的线性组合，则其系数事实上是$K[f_1, \cdots, f_n]$ 中的多项式。特别地，如果h是对称多项式 (即$h \in E = K(f_1, \cdots, f_n)$)，则$h = hx_1^0x_2^0\cdots x_n^0$必然属于$K[f_1, \cdots, f_n]$。这就证明了(ii)。∎

习　题

注：若不加说明，则F永远是域K的扩域，而E是该扩张的中间域。

1. (a) 如果F是域而$\sigma: F \longmapsto F$是(环)同态，则或者$\sigma=0$，或者σ是单同态。如果$\sigma \neq 0$，则$\sigma(1_F)=1_F$。

(b) 全体域自同构$F \to F$所形成的集合$\mathrm{Aut}F$对于函数合成运算形成群。

(c) F的全体K-自同构所形成的集合$\mathrm{Aut}_K F$是$\mathrm{Aut}F$的子群。

2. $\mathrm{Aut}_{\mathbf{Q}}\mathbf{R}$为一元群.〔提示：由于$\mathbf{R}$中每个正数都是平方数，从而$\mathbf{R}$的自同构一定把正数映成正数，从而它保持$\mathbf{R}$中的大小次序．再将一给定的实数夹在适当的一些有理数之中.〕

3. 如果$0\leqslant d\in\mathbf{Q}$，则$\mathrm{Aut}_{\mathbf{Q}}\mathbf{Q}(\sqrt{d})$为一元群或者同构于$Z_2$.

4. 什么是$\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$在$\mathbf{Q}$上的伽罗华群？

5. (*a*) 如果$0\leqslant d\in\mathbf{Q}$，则$\mathbf{Q}(\sqrt{d})$在$\mathbf{Q}$上是伽罗华的.

(*b*) $\mathbf{C}$在$\mathbf{R}$上是伽罗华的.

6. 令$f/g\in K(x)$，其中$f/g\notin K$，并且f和g在$K[x]$中互素，考虑K的扩域$K(x)$.

(*a*) x在$K(f/g)$上是代数的，并且$[K(x):K(f/g)]=\max(\deg f,\deg g)$.〔提示：$x$是非零多项式$\varphi(y)=(f/g)g(y)-f(y)\in K(f/g)[y]$的根.证明$\deg\varphi=\max(\deg f,\deg g)$.按下列方法证明$\varphi$是不可约的：由于$f/g$在$K$上是超越的(为什么？)，为方便起见，我们可以将$K(f/g)$改成$K(z)$ (z是未定元)，并且认为$\varphi=zg(y)-f(y)\in K(z)[y]$. 由引理III.6.13可知，如果$\varphi$在$K[z][y]$中不可约，则在$K(z)[y]$中也不可约．而$\varphi$在$K[z][y]$中确实是不可约的，这是由于$\varphi$对于$z$是一次的而$f$和$g$互素.〕

(*b*) 如果$E\neq K$为中间域，则$[K(x):E]$有限.

(*c*) 映射$x\longmapsto f/g$诱导出同态$\sigma:K(x)\longrightarrow K(x)$，使得$\varphi(x)/\psi(x)\longmapsto\varphi(f/g)/\psi(f/g)$.$\sigma$是$K(x)$的$K$-自同构$\Longleftrightarrow\max(\deg f,\deg g)=1$.

(*d*) $\mathrm{Aut}_K K(x)$是由映射

$$x\longmapsto(ax+b)/(cx+d),\quad a,b,c,d\in K,\quad ad-bc\neq 0.$$

(象(*c*)中那样)所诱导的全部自同构所组成.

7. 令G是$\mathrm{Aut}_K K(x)$的三元子集合，其中三个元素即是象6(*c*)中那样分别通过$x\longmapsto x$，$x\longmapsto 1_K/(1_K-x)$，$x\longmapsto(x-1_K)/x$所诱导的三个自同构.求证G是$\mathrm{Aut}_K K(x)$的子群.决定G的固定域.

8. 假定$\mathrm{char}K=0$，令G是$\mathrm{Aut}_K K(x)$的子群，由通过$x\longmapsto x+1_K$诱导的自同构所生成.则G是无限循环群.决定G的固定域E.

$[K(x):E]=?$

9. (a) 如果K是无限域，则$K(x)$在K上是伽罗华的.〔提示：如果 $K(x)$ 在K上不是伽罗华的，由习题6(b)知$K(x)$在$\mathrm{Aut}_K K(x)$ 的固定域E上是有限维的.但是由习题6(d)，$\mathrm{Aut}_E K(x)=\mathrm{Aut}_K K(x)$是无限的. 这就与引理2.8相矛盾.〕

(b) 如果K是有限域，则$K(x)$在K上不是伽罗华的.〔提示：如果 $K(x)$在K上是伽罗华的，由引理2.9知$\mathrm{Aut}_K K(x)$将会是无限群. 但是由习题6(d)可知$\mathrm{Aut}_K K(x)$是有限的.〕

10. 如果K是无限域，则 $\mathrm{Aut}_K K(x)$ 只有它自身和有限子群是它的闭子群.〔提示：见习题6(b)和9.〕

11. 对于域$\mathbf{Q}$及其扩域$\mathbf{Q}(x)$，其中间域$\mathbf{Q}(x^2)$是闭的，但是$\mathbf{Q}(x^3)$不是闭的.

12. 如果E是扩张$K\subset F$的中间域，使得E在K上以及F在E上均是伽罗华的，并且每个$\sigma\in\mathrm{Aut}_K E$均可扩充到$F$上，则$F$在$K$上是伽罗华的.

13. 对于无限域K的扩张$K(x,y)$，其中间域 $K(x)$ 在 K 上是伽罗华的，但 $K(x)$ (对于$K(x,y)$和K) 不是稳定的.〔见习题9.将此结果与引理2.13加以比较.〕

14. 设F是K的有限维伽罗华扩张，L和M是两个中间域.则

(a) $\mathrm{Aut}_{LM}F=\mathrm{Aut}_L F\cap\mathrm{Aut}_M F$.

(b) $\mathrm{Aut}_{L\cap M}F=\mathrm{Aut}_L F\vee\mathrm{Aut}_M F$.

(c) 如果$\mathrm{Aut}_L F\cap\mathrm{Aut}_M F=1$，会有什么结论？

15. 如果F是K的有限维伽罗华扩张，E是一个中间域，则存在唯一的一个最小域L，使得$E\subset L\subset F$，并且L在K上是伽罗华的. 此外我们有

$$\mathrm{Aut}_L F=\bigcap_{\sigma\in\mathrm{Aut}_K F}\sigma(\mathrm{Aut}_E F)\sigma^{-1}.$$

16. 如果$\sigma\in S_n$，则由

$$f(x_1,\cdots,x_n)/g(x_1,\cdots,x_n)\longmapsto f(x_{\sigma(1)},\cdots,x_{\sigma(n)})/g(x_{\sigma(1)},\cdots,x_{\sigma(n)})$$

给出的映射$K(x_1,\cdots,x_n)\longrightarrow K(x_1,\cdots,x_n)$是$K(x_1,\cdots,x_n)$ 的K-自同构.

3. 分裂域，代数闭包和正规性

我们现在转而研究如何判别和构作伽罗华扩张。利用分裂域能够使我们解决这个问题，而这也是本节的主题。我们首先讲述分裂域和代数闭包（后者为分裂域的一个特殊情形）的基本性质，然后采用并不明显地提到伽罗华群的一种办法来刻划伽罗华代数扩张（定理3.11），并且将基本定理推广到无限维伽罗华代数扩张的情形（定理3.12）。最后讨论正规性和分裂域的其它刻划方法。在附录中我们证明了所谓代数基本定理（复数域上每个多项式方程都有解）。

设F是域而$f \in F[x]$是正次数的多项式。我们称f在F上分裂（或者称在$F[x]$中分裂），指的是f可以写成$F[x]$中线性因子的乘积，即$f = u_0(x-u_1)(x-u_2)\cdots(x-u_n)$，其中$u_i \in F$。

定义3.1 设K是域而$f \in K[x]$是正次数多项式。K的一个扩域F叫作多项式f在K上的分裂域，指的是f在$F[x]$中分裂并且$F = K(u_1, \cdots, u_n)$，其$u_1, \cdots, u_n$是f在F中的全部根。

以S表示$K[x]$中一些正次数多项式所构成的集合。K的一个扩域F叫作多项式集合S在K上的分裂域，指的是S中每个多项式都在$F[x]$中分裂，并且F是由S中所有多项式的根在K上所生成的域。

例 $\mathbb{Q}$上的多项式x^2-2只有两个根：$\sqrt{2}$和$-\sqrt{2}$。$(x^2-2)=(x-\sqrt{2})(x+\sqrt{-2})$。从而$\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\sqrt{2}, -\sqrt{2})$

是x^2-2在$\mathbb{Q}$上分裂域.类似地,$\mathbb{C}$是x^2+1在$\mathbb{R}$上的分裂域，然而，如果u是不可约多项式$f\in K[x]$的根．$K(u)$不一定就是f的分裂域．例如若u是2的实立方根（其它立方根是复的），则$\mathbb{Q}(u)\subset\mathbb{R}$，从而$\mathbb{Q}(u)$不是$x^3-2$在$\mathbb{Q}$上的分裂域．

注记：如果F是S在K上的分裂域，则$F=K(X)$,其中X是$K[x]$之子集合S中所有多项式的全部根所构成的集合．由定理1.12立刻推出，F在K上是代数的（如果S是有限集合，则X也是有限集合，从而F在K上也是有限维的）．注意若S是有限集合，例如$S=\{f_1, f_2, \cdots, f_n\}$，则$S$的分裂域与一个多项式$f=f_1f_2\cdots f_n$的分裂域是一回事（习题1）．这一事实今后常常用到而不加以说明．于是，关于多项式集合S的分裂域，我们主要对于S由一个多项式或者无限个多项式组成的这两种情形感兴趣．我们将要证明，每个[有限维]伽罗华代数扩张事实上都是一个多项式[有限]集合的一种特殊类型的分裂域．

现在要回答一个显然会提出的问题：是否每个多项式集合均具有分裂域？对于一个多项式的情形（或者等价地，对于一个多项式有限集合的情形），答案是相当容易的．

定理3.2 如果K是域而$f\in K[x]$的次数$n\geqslant 1$，则f存在分裂域F并且$[F:K]\leqslant n!$

证明概要 对于$n=\deg f$采用数学归纳法．如果$n=1$或者f在K上分裂，则$F=K$是分裂域．如果$n>1$，并且f在K上不分裂，令$g\in K[x]$是f的一个次数>1的不可约因子．由定理1.10可知存在K的单扩张$K(u)$，使得g是u的根，从而$[K(u):K]=\deg g>1$．由定理III.6.6，$f=(x-u)h$，其中$h\in K(u)[x]$并且次数是$n-1$.根据归纳假设，存在h在$K(u)$上的分裂域F，并且F对于$K(u)$的维

数$\leqslant(n-1)!$．证明F是f在K上的分裂域（习题3），并且维数$[F:K]=[F:K(u)][K(u):K]\leqslant(n-1)!\ (\deg g)\leqslant n!$． ∎

关于多项式无限集合的分裂域存在性的证明则要困难得多．我们这里采用一种间接的证明，即引进这类分裂域的一种特殊情形（定理3.4）．这一特殊情形本身也具有重要意义．

注：如果读者只对一个多项式的分裂域（即有限维分裂域）感兴趣，他可以由此跳到定理3.8．定理3.12也可以略去，并且定理 3.8—3.16 也可以只阅读有限维的情形．这些结果的证明都是或者分成两种情形（有限维和无限维），或者直接应用于两种情形．唯一的例外是定理3.14中对于(ii)$\Longrightarrow$(i) 的证明，它的另一种证明方法见习题25．

定理3.3 关于域F上的下列一些条件是彼此等价的．

(i) 每个不是常数的多项式$f\in F[x]$在F中都有根；

(ii) 每个不是常数的多项式$f\in F[x]$在F中都分裂；

(iii) $F[x]$中每个不可约多项式都是一次的；

(iv) （除F自身之外）不存在F的代数扩域；

(v) 存在F的一个子域K，使得F在K上是代数的，并且$K[x]$中每个多项式均在$F[x]$中分裂．

证明 作为练习，并参见第III.6节和定理1.6，1.10，1.12和1.13． ∎

满足定理3.3中等价条件的域叫作代数封闭的．例如我们将要证明复数域$\mathbf{C}$是代数封闭的（定理3.19）．

定理3.4 如果F是K的扩域，则下列二条件是等价的．

(i) F在K上是代数的，并且F是代数封闭的；

(ii) F是$K[x]$中全体（不可约）多项式所组成的集合在K上的分裂域。

证明作为练习，还参见习题9，10。 ∎

域K的扩域F如果满足定理3.4中的等价条件，便称作是K的一个代数闭包。例如$\boldsymbol{C}=\boldsymbol{R}(i)$是$\boldsymbol{R}$的一个代数闭包。如果$F$是$K$的一个代数闭包而$S$是$K[x]$中任意一个多项式集合，则$K$和$S$中多项式的全部根所生成的$F$的子域$E$显然是$S$在$K$上的分裂域（定理3.3和3.4）。所以，域$K$上任意分裂域的存在性等价于$K$的代数闭包的存在性。

证明每个域K均有代数闭包的主要困难不在代数方面，而是在集合论方面。其基本思想是将Zorn引理运用于适当选取的一个K的代数扩域集合[2]。为此我们需要

引理3.5 如果F是K的代数扩域，则$|F|\leqslant \aleph_0|K|$，

证明概要 令T是$K[x]$中全部正次数首1多项式所组成的集合。我们先证明$|T|=\aleph_0|K|$。对于每个$u\in \boldsymbol{N}^*$，以T_n表示T中全部n次多项式所组成的集合。则$|T_n|=|K^n|$，其中$K^n=K\times K\times\cdots\times K$（$n$个因子），这是因为每个多项式$f=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in T_n$由它的$n$个系数$a_0$，$a_1$，…，$a_{n-1}\in K$所完全确定。对于每个$n\in \boldsymbol{N}^*$，令$f_n:T_n\to K^n$是一个一一映射。由于集合$T_n$是两两非交的，$K^n$也是两两非交的，从而可以定义一一映射$f:T=\bigcup\limits_{n\in \boldsymbol{N}^*}T_n\to\bigcup\limits_{n\in \boldsymbol{N}^*}K^n$，$f(u)=f_n(u)$（对于$u\in T_n$）。因此由引论中的定理8.12(ii)我们有$|T|=\left|\bigcup\limits_{n\in \boldsymbol{N}^*}K^n\right|=\aleph_0|K|$。

2. 任何一个熟悉集合论悖论的人（引论，第2节）都能猜想到，K的全部代数扩域所组成的类不是一个集合，从而不能用Zorn引理这样的推理方式。

其次我们证明$|F|\leqslant|T|$，这就完成整个引理的证明。对于每个不可约的$f\in T$，将f在F中的彼此不同的根赋以一定的次序。如下定义一个映射$F\to T\times \boldsymbol{N}^*$：如果$a\in F$，由假设知$a$在$K$上是代数的，从而存在唯一的不可约首1多项式$f\in T$，使得$f(a)=0$（定理1.6）。我们将$a\in F$对应于$(f, i)\in T\times \boldsymbol{N}^*$，其中$a$对于预先选好的次序是$f$在$F$中的第$i$个根。验证映射$F\to T\times \boldsymbol{N}^*$是可以如此定义的，并且是单射。由于$T$是无限集合，由引论中的定理8.11可知$|F|\leqslant|T\times \boldsymbol{N}^*|=|T||\boldsymbol{N}^*|=|T|\aleph_0=|T|$。 ∎

定理3.6 每个域K都有代数闭包。K的任意两个代数闭包都是K-自同构的。

证明概要 选取一个集合S，使得$\aleph_0|K|<|S|$（由引论中的定理8.5可知这总是可以作到的）。由于$|K|\leqslant\aleph_0|K|$（引论中定理8.11），由引论中的定义8.4可知存在一个单射$\theta:K\to S$。所以我们可以假定$K\subset S$（因为不然的话，将S代之以$S-\mathrm{Im}\theta$与K的并集）。

令$\mathscr{S}$是类{域E|E是S的一个子集合，并且E是K的代数扩域}。类$\mathscr{S}$中这样一个域E由S的子集合E和E中的加法和乘法运算所完全确定。但是加法和乘法分别是函数φ：$E\times E\to E$和ψ：$E\times E\to E$。从而φ和ψ均可以等同于它们的图，即$E\times E\times E\subset S\times S\times S$的某个子集合（见引论第4节）。于是$\tau$：$E\mapsto(E, \varphi, \psi)$给出一个从$\mathscr{S}$到集合$P$的单射，其中$P$是集合$S\times(S\times S\times S)\times(S\times S\times S)$的全部子集构成的集合。由于$\mathrm{Im}\tau$是集合$P$的子类，从而$\mathrm{Im}\,\tau$事实上是一个集合。由于$\mathscr{S}$是$\mathrm{Im}\tau$在函数$\tau^{-1}$：$\mathrm{Im}\tau\to\mathscr{S}$之下的原象，从而集合论的公理保证事实上$\mathscr{S}$也是一个集合。

注意$\mathscr{S}\neq\varnothing$，这是因为$K\in\mathscr{S}$。按下列方式将集合$\mathscr{S}$赋以半序：$E_1\leqslant E_2\Longleftrightarrow E_2$是$E_1$的扩域。验证$\mathscr{S}$中每个链均有上界（可取

成链中所有域之并)。于是由Zorn引理，$\mathscr{S}$中存在着极大元F。

我们断言F是代数封闭的。如果不然，则存在F的一个真代数扩张$F_0=F(u)$，其中u是f的根并且$u\notin F$（定理1.10)。根据定理1.13，F_0也是K的代数扩张。于是由引理3.5便有$|F_0-F|\leqslant|F_0|\leqslant\aleph_0|K|<|S|$。由于 $|F|\leqslant|F_0|<|S|$ 而 $|S|=|(S-F)\cup F|=|S-F|+|F|$，根据引论中的定理8.10可知必然$|S|=|S-F|$。因此$|F_0-F|<|S-F|$，并且 F 上的恒等映射可以扩充成集合之间的单射$\zeta:F_0\to S$。从而通过定义 $\zeta(a)+\zeta(b)=\zeta(a+b)$ 和 $\zeta(a)\cdot\zeta(b)=\zeta(ab)$ 可以将$F_1=\mathrm{Im}\zeta$作成域。F_1显然是 F 的扩张。$F_1\subset S$，并且$\zeta:F_0\to F_1$ 是域的F-自同构。由于 F_0 是F的（从而也是 K 的）真代数扩张，从而F_1也是K的真代数扩张。这就意味着$F_1\in\mathscr{S}$，并且$F<F_1$，从而与F的极大性相矛盾。因此F是代数封闭的，并且在K上是代数的，从而是 K 的代数闭包。定理的唯一性命题将在下面系3.9中证明。 ∎

系3.7 如果K是域而S是$K[x]$中一个正次数多项式集合，则存在S在K上的分裂域。

证明作为练习。 ∎

现在我们转到分裂域和代数闭包的唯一性问题。其答案是下面关于同构可扩充性的结果（见定理1.8和它前面的注记)的直接推论。

定理3.8 令$\sigma:K\to L$是域的同构，$S=\{f_i\}$是$K[x]$中一个（正次数)多项式集合，而 $S'=\{\sigma f_i\}$是$L[x]$ 中对应的多项式集合。如果F是S在K上的分裂域而M是S'在L上的分裂域，则 σ可以扩充成同构$F\cong M$。

证明概要 先设S是由一个多项式$f\in K[x]$所组成的集合．我们对于$n=[F:K]$作数学归纳法．如果$n=1$，则$F=K$，而f在K上分裂．由此推出σf在L上也分裂，于是$L=M$．从而σ自己便是所需要的同构$F=K\xrightarrow{\sigma}L=M$．如果$n>1$，则$f$必然有次数大于1的不可约因子$g$．以$u$表示$g$在$F$中的一个根．然后证明$\sigma g$在$L[x]$中不可约．如果$v$是$\sigma g$在$M$中的一个根，由定理1.8可知$\sigma$可以扩充成同构$\tau:K(u)\cong L(v)$，并且$\tau(u)=v$．由于$[K(u):K]=\deg g>1$（定理1.6），从而$[F:K(u)]<n$（定理1.2）．因为$F$是$f$在$K(u)$上的分裂域而$M$是$\sigma f$在$L(v)$上的分裂域（习题2），由归纳假设便导致$\tau$可以扩充成同构$F\cong M$．

如果S是任意的，令

$\mathscr{S}=\{(E,\ N,\ \tau)\mid E$为$F$和$K$的中间域，$N$为$M$和$L$的中间域，

$\tau:E\to N$是域同构并且是σ的扩充$\}$

定义：$(E_1,\ N_1,\ \tau_1)\leqslant(E_2,\ N_2,\ \tau_2)\Longleftrightarrow E_1\subset E_2$，$N_1\subset N_2$，$\tau_2|E_1=\tau_1$．验证$\mathscr{S}$是非空半序集合，每个链在$\mathscr{S}$中均有上界．由Zorn引理可知$\mathscr{S}$有极大元$(F_0,\ M_0,\ \tau_0)$．我们断言$F_0=F$，$M_0=M$，从而$\tau_0:F\to M$即为所希望的$\sigma$之扩充．如果$F_0\neq F$，则有$f\in S$在$F_0$上不分裂．由于$f$的所有根都在$F$中，从而$F$包含$f$在$F_0$上的一个分裂域$F_1$．类似地，$M$包含$\tau_0 f=\sigma f$在$M_0$上的一个分裂域．由本证明的第一部分可知$\tau_0$可以扩充成同构$\tau_1:F_1\cong M_1$．而这就意味着$(F_1,\ M_1,\ \tau_1)\in\mathscr{S}$，并且$(F_0,\ M_0,\ \tau_0)<(F_1,\ M_1,\ \tau_1)$，这就与$(F_0,\ M_0,\ \tau_0)$的极大性相矛盾．如果$M_0\neq M$，则可利用$\tau_0^{-1}$并进行类似的推理． ∎

系3.9 设K是域而S是$K[x]$中一个（正次数）多项式集合．则S在K上的任意两个分裂域都是K-同构的．特别地，K的任意两

代数闭包都是K-同构的。

证明概要 在定理3.8中取$\sigma=1_k$。而最后一个论断是定理3.4(ii)的直接推论。 ∎

为了用分裂域来刻划伽罗华扩张，我们首先要考虑只在特征不为零的域中才会出现的一种现象。让我们回忆一下，如果K是任意域，f是$K[x]$中的非零多项式，c是f的根，则$f=(x-c)^m g(x)$，其中$g(c)\neq 0$，而m是唯一确定的正整数。根据$m=1$或者$m>1$，元素c分别叫作f的单根或重根。(见第242页)。

定义3.10 设K是域而$f\in K[x]$是不可约多项式，如果E是f在K上的某个分裂域，而f在E中的根全是单根，我们便称f是可分的。

设F是K的扩域，而u是F在K上的代数元素，假若u在K上的不可约多项式是可分的，我们便称u在K上是可分的。如果F中每个元素在K上是可分的，则F叫作K的可分扩张。

注记：(i) 从系3.9不难看出，一个可分多项式$f\in K[x]$在f的任意分裂域中都没有重根。

(ii) 定理III.6.10表明，$K[x]$中的一个不可约多项式是可分的，当且仅当它的导函数不为零。因此，若$\mathrm{char}\,K=0$，则K上的每个不可约多项式都是可分的(习题III.6.3)。所以，特征零域的每个代数扩域都是可分的。

(iii) 这里只是对于不可约多项式定义了可分性。

(iv) 根据定义3.10，K的可分扩域在K上必须是代数的。对于可能不必是代数扩张的域也可以定义可分性，并且在代数扩张的情形下两个定义是一致的(第VI.2节)。但是在本章中我们只使用定义3.10。

例 $x^2+1\in\mathbf{Q}[x]$是可分的，因为在$\mathbf{C}[x]$中$x^2+1=(x+i)(x-i)$。另一方面，多项式x^2+1在Z_2上没有单根，事实上它甚至是可约的，因为在$Z_2[x]$中$x^2+1=(x+1)^2$。

定理3.11 如果F是K的扩域，则下列诸命题是彼此等价的。

(i) F在K上是代数伽罗华扩张；

(ii) F在K上可分，并且F是$K[x]$中某个多项式集合S在K上的分裂域；

(iii) F是$K[x]$中某个可分多项式集合T在K上的分裂域。

注记：如果F在K上是有限维的，则命题(ii)和(iii)还可以稍微加强。例如(iii)可以改成：F是某个多项式$f\in K[x]$在K上的分裂域，而f的每个不可约因子都是可分的(习题13)。

证明 (i)$\Longrightarrow$(ii)和(iii)：如果$u\in F$的极小多项式是f，可以将引理2.13(取$E=F$)之证明的第一部分逐字逐句地搬过来，即可证明f在$F[x]$中分裂成不同的线性因子之乘积。从而u在K上是可分的。令$\{v_i|i\in I\}$是F在K上的一组基，对于每个$i\in I$，令$f_i\in K[x]$是v_i的极小多项式。前面的注记表明每个f_i在$F[x]$中均是可分的并且都分裂。从而F是$S=\{f_i|i\in I\}$在K上的分裂域。

(ii)$\Longrightarrow$(iii)：令$f\in S$，而$g\in K[x]$是f的一个首1的不可约因子。由于f在$F[x]$中分裂，g必然是某个$u\in F$的极小多项式。因为F在K上是可分的，可知g必然是可分的。取T为S中多项式的所有首1不可约因子(在$K[x]$中)所构成的可分多项式集合，则F是T在K上的分裂域。

(iii)$\Longrightarrow$(i)：F在K上是代数的，这是因为K上的任何分裂域均是代数扩张。如果$u\in F-K$，根据分裂域的定义和定理1.3(vii)，便知$u\in K(v_1,\cdots,v_n)$，其中每个v_i是某个$f_i\in T$的根。

因此$u \in E = K(u_1, \cdots, u_r)$，其中$\{u_i\}$是$f_1 \cdots f_n$在$F$中的全部根。由定理1.12便知$[E:K]$是有限的。由于每个$f_i$都在$F$中分裂，从而$E$是有限集合$\{f_1, \cdots, f_n\}$在$K$上的分裂域，或者等价地说成：$E$是$f = f_1 f_2 \cdots f_n$在$K$上的分裂域。现在假定定理对于有限维的情形是对的，则E在K上是伽罗华的，从而存在$\tau \in \mathrm{Aut}_K E$，使得$\tau(u) \neq u$。由于$F$是$T$在$E$上的分裂域(习题2)，根据定理3.8可知$\tau$可以扩充成一个自同构$\sigma \in \mathrm{Aut}_K F$，使得$\sigma(u) = \tau(u) \neq u$。因此$u$(这是$F - K$中任意元素)不属于$\mathrm{Aut}_K F$的固定域，即$F$在$K$上是伽罗华的。

上一段的推导表明，我们只需在$[F:K]$有限的情形下证明本定理即可。在这种情形下，存在有限个多项式$g_1, \cdots, g_t \in T$，使得F是$\{g_1, \cdots, g_t\}$在K上的分裂域(不然的话，F在K上将会是无限维的)。此外，由引理2.8可知$\mathrm{Aut}_K F$是有限群。如果K_0为$\mathrm{Aut}_K F$的固定域，由Artin定理2.15和基本定理，可知F是K_0的伽罗华扩张，并且$[F:K_0] = |\mathrm{Aut}_K F|$。所以，为了证明$F$在$K$上是伽罗华的(即$K = K_0$)，只需证明$[F:K] = |\mathrm{Aut}_K F|$。

我们对于$n = [F:K]$采用数学归纳法。$n = 1$的情形显然成立。如果$n > 1$，则必有某个g_i(设为g_1)的次数$s > 1$(不然的话，每个g_i的根都属于K，于是$F = K$)。令$u \in F$为g_1的根，由定理1.6可知$[K(u):K] = \deg g_1 = s$。由于g_1是可分的，g_1共有s个不同的根。由引理2.8(取$L = K$，$M = K(u)$，$f = g_1$)证明的第二段可知，存在着从$H = \mathrm{Aut}_{K(u)} F$在$\mathrm{Aut}_K F$中的全体左陪集组成的集合到$g_1$在$F$中的$S$个根组成的集合的一个单射，这个单射由$\sigma H \longmapsto \sigma(u)$给出。于是$[\mathrm{Aut}_k F:H] \leqslant s$。现在如果$v \in F$是$g_1$的另一个根，由系1.9可知存在着同构$\tau: K(u) \cong K(v)$，使得$\tau(v) = u$并且$\tau | K = \mathbf{1}_k$。因为$F$是$\{g_1, \cdots, g_t\}$在$K(u)$上和在$K(v)$上的分裂域(习题2)，从而$\tau$可以扩充成自同构$\sigma \in \mathrm{Aut}_K F$，使得$\sigma(u) = v$(定理3.8)。于是，$g_1$的

每个根都是H的某个陪集的象，从而$[\mathrm{Aut}_K F:H]=s$.' 进一步，F是多项式$\{g_i\}$（在 $K(u)[x]$中）的全部不可约因子h_i组成的集合在$K(u)$上的分裂域(习题4)。每个h_i显然是可分的，因为它除尽某个 g_i。由于 $[F:K(u)]=n/s<n$，从归纳假设推出 $[F:K(u)]=|\mathrm{Aut}_{K(u)}F|=|H|$，因而

$$[F:K]=[F:K(u)][K(u):K]=|H|s$$
$$=|H|[\mathrm{Aut}_K F:H]=|\mathrm{Aut}_K F|.$$

这就完成了证明。 ∎

定理3.12 （基本定理之推广） 如果 F 是K的代数伽罗华扩域，则

(i′) 在该扩张的全部中间域所构成的集合与伽罗华群$\mathrm{Aut}_K F$的全部闭子群所构成的集合之间存在着一一对应（由 $E\longmapsto E'=\mathrm{Aut}_E F$给出），并且：

(ii′) F在每个中间域E上都是伽罗华的。而 E 在K上是伽罗华的$\Longleftrightarrow$对应的子群E'在 $G=\mathrm{Aut}_K F$中正规。在后一情形下，G/E'是同构于E在K上的伽罗华群$\mathrm{Aut}_K E$的。

注记：将这个定理与定理2.5 相比较。对于无限的情形，基本定理的(i)不再成立(习题16)。如果$[F:K]$是无限的，则永远存在$\mathrm{Aut}_K F$的一个不闭的子群。这一事实的证明与Krull[64]所作的考查有关：如果F在K上是代数的，可以按下述方式将$\mathrm{Aut}_K F$作成为紧拓扑群：即一个子群是拓扑闭子群$\Longleftrightarrow$它在第 2 节的意义下是闭的(即$H=H''$)。不难证明，每个无限的紧拓扑群都存在不拓扑闭的子群。更进一步的讨论和例子可见P.J.McCarthy[40；第60—63页]。还可见下面的习题5.11。

定理3.12的证明 从定理2.7可知，为了建立一一对应关系，

我们只需证明每个中间域E都是闭的。根据定理3.11，F是一个可分多项式集合T在K上的分裂域。因此F也是T在E上的分裂域（习题2）。于是再根据定理3.11，F在E上是伽罗华的，从而E是闭的。

(ii′) 因为每个中间域E在K上都是代数的，将定理 2.5(ii)之证明的第一段用到这里来，即可证明：E在K上是伽罗华的$\Longleftrightarrow$$E'$在$\mathrm{Aut}_K F$中正规。

如果$E=E''$在K上是伽罗华的，并且E'在$G=\mathrm{Aut}_K F$中正规，则由引理2.11可知E是稳定的中间域。从而由引理2.14导致$G/E'=\mathrm{Aut}_K F/\mathrm{Aut}_E F$同构于$\mathrm{Aut}_K E$的一个子群，这个子群是由可以扩充到$F$的那些自同构所组成的。但是$F$是$K$上的分裂域(定理3.11)，从而它也是$E$上的分裂域(习题2)。因此，由定理3.8可知$\mathrm{Aut}_K E$中的每个自同构均可扩充到$F$，并且$G/E'\cong\mathrm{Aut}_K E$。 ∎

现在我们回到分裂域上来，要用我们已经使用过若干次的一个性质来刻划它们。

定义3.13 K的代数扩域F叫作在K上正规的（或者叫作K的正规扩张），指的是：$K[x]$中每个不可约多项式只要在F中有根，则它必然在$F[x]$中分裂。

定理3.14 如果F是K的代数扩域，则下列诸命题彼此等价。

(i) F在K上正规；

(ii) F是$K[x]$中某个多项式集合在K上的分裂域；

(iii) 如果$\overline{K}$是K的代数闭包并且包含F，则对于每个域之间的K-单同构$\sigma: F\to\overline{K}$，必然$\mathrm{Im}\sigma=F$，从而σ实际上是F的K-自同构。

注记：如果在(iii)中将代数闭包$\overline{K}$改成K的任何一个包含F的

正规扩域，则定理仍旧正确(习题21)。对于有限维的情形可以直接证明(ii)$\Longrightarrow$(i)，参见习题25。

证明 (i)$\Longrightarrow$(ii)：假设$\{u_i \mid i\in I\}$是F在K上的一组基，而f_i是u_i的极小多项式。则F是$\{f_i\in K[x] \mid i\in I\}$在$K$上的分裂域。

(ii)$\Longrightarrow$(iii)：令F是$\{f_i \mid i\in I\}$在K上的分裂域，$\sigma: F\longrightarrow \overline{K}$是域的$K$-单同态。如果$u\in F$是$f_j$的根，则$\sigma(u)$也是$f_j$的根(象定理2.2的证明一样)。根据假设，$f_j$在$F$中分裂，假定$f_j = c(x-u_1)\cdots(x-u_n)$($u_i\in F$，$c\in K$)。由于$\overline{K}[x]$是唯一因子分解整环（系III.6.4)，对于每个$i$，$\sigma(u_i)$必然是$u_1,\cdots,u_n$当中的一个。因为$\sigma$是单射，从而$\{\sigma(u_i)\}$必然是$\{u_i\}$的一个置换。但是$F$是由所有$f_i$的全部根在$K$上所生成的。由定理 1.3 可知 $\sigma(F)=F$，从而 $\sigma\in \mathrm{Aut}_k F$。

(iii)$\Longrightarrow$(ii)：令$\overline{K}$是F的代数闭包(定理 3.6)。则$\overline{K}$在K上是代数的(定理1.13)。从而$\overline{K}$是K的代数闭包并且包含 F（定理3.4)。令$f\in K[x]$不可约并且有根$u\in F$。由构造方法可知$\overline{K}$包含f的全部根。如果$v\in\overline{K}$是f的任意一个根，则存在着域的 K-同构σ：$K(u)\cong K(v)$，使得$\sigma(u)=v$(系1.9)，由定理3.4，3.8和习题2可知σ可以扩充成$\overline{K}$的K-自同构。从而$\sigma|F$是单同态$F\longrightarrow\overline{K}$，并且由假设可知$\sigma(F)=F$。因此$v=\sigma(u)\in F$，这表明$f$在$F$中分裂。从而$F$在$K$上是正规的。∎

系3.15 设F是K的代数扩域。则F在K上是伽罗华的$\Longleftrightarrow$$F$在$K$上正规可分。如果$\mathrm{char}K=0$，则$F$在$K$上是伽罗华的$\Longleftrightarrow$$F$ 在 K上是正规的。

证明作为练习。利用定理3.11和3.14。∎

定理3.16 如果E是K的代数扩域，则存在E的一个扩域 F，使得

(i) F在K上正规；

(ii) F没有包含E的真子域，使得它在K上也是正规的；

(iii) 如果E在K上是可分的，则F在K上是伽罗华的；

(iv) $[F:K]$有限$\Longleftrightarrow$$[E:K]$有限。

最后，F不计E-同构是唯一确定的。

定理3.16中的域F有时称作E在K上的正规闭包。

证明 (i) 令 $X=\{u_i \mid i\in I\}$ 是E在K上的一组基，而令 $f_i\in K[x]$是u_i的极小多项式。如果F是$S=\{f_i \mid i\in I\}$ 在E上的分裂域，则F也是S在K上的分裂域(习题3)，由定理3.14 即知F在K上是正规的。

(iii) 如果E在K上可分，则每个f_i 都是可分的。从而由定理3.11便知F在K上是伽罗华的。

(iv) 如果$[E:K]$有限，则X从而S也都是有限的。由定义3.1后面的注记即可推出$[F:K]$也是有限的。

(ii) F的子域F_0如果包含E，则必然包含 $f_i\in S$的根u_i (对于每个i)。如果F_0在K上正规(从而由定义，每个f_i在F_0中都分裂)，则$F\subset F_0$，因此$F=F_0$。

最后令F_1是E的另一个扩域并且满足性质(i)和(ii)。由于F_1在K上是正规的并且包含所有的u_i，从而F_1必然包含S在K上的分裂域F_2，并且$E\subset F_2$。而F_2在K上是正规的 (定理3.14)，于是由(ii)推出$F_2=F_1$。所以F和F_1都是S 在K上的分裂域，从而也都是S在E上的分裂域(习题2)。由定理3.8 即知E上的恒等映射可以扩充成E-同构$F\cong F_1$。∎

附录：代数基本定理

代数基本定理是说：复数域$\boldsymbol{C}$是代数封闭的（即$\boldsymbol{C}$上的每个多项式方程都在$\boldsymbol{C}$中可解）。目前关于这一事实的所有证明都在一定程度上依赖于分析方面的一些结果。我们将需要：

（A）每个正实数都有正实数平方根；

（B）$\boldsymbol{R}[x]$中每个奇次多项式在$\boldsymbol{R}$中均有根（也就是说，$\boldsymbol{R}[x]$中次数大于1的不可约多项式必然是偶次的）。

从有理数构作实数集合的方法可以直接推出（A）。而（B）则是微积分中值定理的一个系理，见习题 III.6.16。开始我们先证明一个定理（即后面的命题6.15）的特殊情形。

引理3.17 如果F是无限域K的有限维可分扩张，则存在某个$u\in F$，使得$F=K(u)$。

证明概要 根据定理3.16，存在着K的一个有限维伽罗华扩域F_1包含F。基本定理2.5推出$\mathrm{Aut}_K F_1$是有限的，并且扩张$K\subset F_1$只有有限多个中间域。从而扩张$K\subset F$也只有有限多个中间域。

由于$[F:K]$是有限的，我们可以选取$u\in F$，使得$[K(u):K]$极大。如果$K(u)\neq F$，则存在$v\in F-K(u)$。考虑形如$K(u+av)$（$a\in K$）的全部中间域。因为K是无限的，而中间域只有有限多个，从而存在$a,b\in K$，$a\neq b$，但是$K(u+av)=K(u+bv)$。因此$(a-b)v=(u+av)-(u+bv)\in K(u+av)$。由于$a\neq b$，我们有$v=(a-b)^{-1}(a-b)v\in K(u+av)$，从而$u=(u+av)-av\in K(u+av)$，

因此$K\subset K(u)\subsetneq K(u+av)$，于是$[K(u+av):K]>[K(u):K]$。这就与$u$的选取方法相矛盾。从而$K(u)=F$。∎

引理3.18 不存在复数域上维数是2的扩域。

证明概要 不难看出，如果F是$\boldsymbol{C}$上的2维扩域，则对于每个$u\in F-\boldsymbol{C}$均有$F=\boldsymbol{C}(u)$。从定理1.6可知u是2次不可约首1多项式$f\in\boldsymbol{C}[x]$的根。从而为了完成证明，我们只需证明这样的f不可能存在。

对于每个$a+bi\in\boldsymbol{C}=\boldsymbol{R}(i)$，由(A)知$|(a+\sqrt{a^2+b^2})/2|$和$|(-a+\sqrt{a^2+b^2})/2|$分别有正实平方根$c$和$d$。验证：适当地选择符号可有$(\pm c\pm di)^2=a+bi$。从而$\boldsymbol{C}$中每个元素在$\boldsymbol{C}$中均有平方根。所以若$f=x^2+sx+t\in\boldsymbol{C}[x]$，则$f$在$\boldsymbol{C}$中有根$(-s\pm\sqrt{s^2-4t})/2$，于是$f$在$\boldsymbol{C}$上分裂。因此$\boldsymbol{C}[x]$中没有2次不可约首1多项式。∎

定理3.19 （代数基本定理） 复数域是代数封闭的。

证明 为了证明每个非常数多项式$f\in\boldsymbol{C}[x]$在$\boldsymbol{C}$上分裂，由定理1.10可知只需证明：除自身之外$\boldsymbol{C}$没有其它有限维代数扩张。由于$[\boldsymbol{C}:\boldsymbol{R}]=2$而 char $\boldsymbol{R}=0$，可知$\boldsymbol{C}$的每个有限维扩域E_1均是$\boldsymbol{R}$的有限维可分扩张（定理1.2）。从而由定理3.16，E_1包含在$\boldsymbol{R}$的某个有限维伽罗华扩域F之中。为了得到最后结论$E_1=\boldsymbol{C}$，我们只需证明$F=\boldsymbol{C}$即可。

基本定理2.5表明$\mathrm{Aut}_{\boldsymbol{R}}F$是有限群。由定理II.5.7和2.5可知$\mathrm{Aut}_{\boldsymbol{R}}F$有$2^n(n\geqslant 0)$阶的Sylow 2-子群$H$，并且$[\mathrm{Aut}_{\boldsymbol{R}}F:H]$为奇数，从而$H$的固定域$E$的维数也是奇数$[H:R]=[\mathrm{Aut}_{\boldsymbol{R}}F:H]$。由于Char$\boldsymbol{R}=0$，$E$在$\boldsymbol{R}$上是可分的，由引理3.17即知$E=\boldsymbol{R}(u)$。从而$u$的不可约多项式的次数为奇数$[E:\boldsymbol{R}]=[\boldsymbol{R}(u):\boldsymbol{R}]$（定理1.6）。

由(B)便知这个次数必为1。从而$u\in\boldsymbol{R}$，而$[\mathrm{Aut}_{\boldsymbol{R}}F:H]=[E:\boldsymbol{R}]=1$。于是$\mathrm{Aut}_{\boldsymbol{R}}F=H$而$|\mathrm{Aut}_{\boldsymbol{R}}F|=2^n$。从而$\mathrm{Aut}_{\boldsymbol{R}}F$的子群$\mathrm{Aut}_{\boldsymbol{C}}F$的阶数是$2^m(0\leqslant m\leqslant n)$。

假设$m>0$，由Sylow第一定理II.5.7$\mathrm{Aut}_{\boldsymbol{C}}F$有指数为2的子群$J$。令$E_0$是$J$的固定域。根据基本定理，$E_0$为$\boldsymbol{C}$的扩张，其维数是$[\mathrm{Aut}_{\boldsymbol{C}}F:J]=2$，而这与引理3.18相矛盾。因此$m=0$，从而$\mathrm{Aut}_{\boldsymbol{C}}F=1$。由基本定理2.5推得$[F:\boldsymbol{C}]=[\mathrm{Aut}_{\boldsymbol{C}}F:1]=|\mathrm{Aut}_{\boldsymbol{C}}F|=1$，即$F=\boldsymbol{C}$。∎

系3.20 实数域的每个真代数扩域均同构于复数域。

证明 如果F是$\boldsymbol{R}$的真代数扩张，并且$u\in F-\boldsymbol{R}$有次数大于1的极小多项式$f\in\boldsymbol{R}[x]$，由定理3.19可知f在$\boldsymbol{C}$上分裂。如果$v\in\boldsymbol{C}$是f的根，由系1.9可知$\boldsymbol{R}$上的恒等映射可以扩充成同构$\boldsymbol{R}(u)\cong\boldsymbol{R}(v)\subset\boldsymbol{C}$。由于$[\boldsymbol{R}(v):\boldsymbol{R}]=[\boldsymbol{R}(u):\boldsymbol{R}]>1$而$[\boldsymbol{C}:\boldsymbol{R}]=2$，我们必然有$[\boldsymbol{R}(v):\boldsymbol{R}]=2$和$\boldsymbol{R}(v)=\boldsymbol{C}$。因此$F$是代数封闭域$\boldsymbol{R}(u)\cong\boldsymbol{C}$的代数扩张。但是代数封闭域没有除自身之外的代数扩张(定理3.3)，从而$F=\boldsymbol{R}(u)\cong\boldsymbol{C}$。∎

习　题

注：若不加说明，则F永远是域K的扩域，而S是$K[x]$中一个(正次数)多项式集合。

1. F是$K[x]$中多项式有限集合$\{f_1,\cdots,f_n\}$在K上的分裂域$\Leftrightarrow F$是一个多项式$f=f_1f_2\cdots f_n$在K上的分裂域。
2. 如果F是S在K上的分裂域而E是中间域，则F也是S在E上的分裂域。
3. (a) 令E是扩张$K\subset F$的中间域，并且假定$E=K(u_1,\cdots,u_r)$，其中$\{u_i\}$

是$f\in K[x]$的某些根.则F是f在K上的分裂域$\Longleftrightarrow F$是f在E上的分裂域.

(b) 将(a)推广到任意多项式集合的分裂域上去.

4. 如果F是S在K上的分裂域,而T是S中多项式的全部不可约因子构成的集合,则F也是T在K上的分裂域.

5. 如果$f\in K[x]$的次数为n而F是f在K上的分裂域，则$[F:K]$整除$n!$.

6. 设K是域，如果对于每个扩域F，包含在F之中的K之极大代数扩张(见定理1.14)必为K自身，则K是代数封闭的.

7. 如果F是代数封闭的，而$E=\{a\in F\mid a$在K上是代数的$\}$，则E是K的代数闭包〔见定理1.14〕.

8. 有限域K不是代数封闭的.[提示：如果$K=\{a_0,\cdots a_n\}$，考虑$a_1+(x-a_0)(x-a_1)\cdots(x-a_n)\in K[x]$，其中$a_1\neq 0$.]

9. F是K的代数闭包$\Longleftrightarrow F$在K上是代数的,并且对于K的每个代数扩张E，均存在K-单同态$E\to F$.

10. F是K的代数闭包$\Longleftrightarrow F$在K上是代数的，并且对于每个域同构$\sigma:K_1\to K$和K_1的每个代数扩域E，σ均可以扩充成一个单同态$E\to F$.

11. (a) 如果$u_1,\cdots,u_n\in F$在K上均可分，则$K(u_1,\cdots,u_n)$为K的可分扩张.

(b) 如果F是由K上一些（可能无限个）可分元素生成的，则F是K的可分扩张.

12. 令E是一个中间域.

(a) 如果$u\in F$在K上可分，则u在E上也是可分的.

(b) 如果F在K上可分，则F在E上可分并且E在K上可分.

13. 设$[F:K]$有限.则下列一些条件是彼此等价的：

(i) F在K上是伽罗华的；

(ii) F在K上可分，并且是某个$f\in K[x]$的分裂域；

(iii) F是某个多项式$f\in K[x]$在K上的分裂域，并且f的不可约因子是可分的.

14. 如果L和M是中间域，并且L是K的有限维伽罗华扩张，则LM也是M

的有限维伽罗华扩张，并且$\mathrm{Aut}_M LM \cong \mathrm{Aut}_{L\cap M} L$。

15. 设E是中间域。

(a) 如果F是K的伽罗华代数扩张，则F是E的伽罗华代数扩张[习题2.9和2.11表明“代数”这一假定条件是必要的]。

(b) 如果F在E上是伽罗华的，E在K上也是伽罗华的，并且F是$K[x]$中一些多项式在E上的分裂域，则F在K上也是伽罗华的[见习题2.12]。

16. 设F是有理数域$\mathbf{Q}$的代数闭包，又令$E(\subset F)$是集合$S=\{x^2+a \mid a\in\mathbf{Q}\}$在$\mathbf{Q}$上的分裂域，从而$E$是$\mathbf{Q}$的伽罗华代数扩张（定理3.11）。则

(a) $E=\mathbf{Q}(X)$，其中$X=\{\sqrt{p} \mid p=-1$或者p为素数$\}$。

(b) 如果$\sigma\in\mathrm{Aut}_{\mathbf{Q}}E$，则$\sigma^2=1_E$。因此群$\mathrm{Aut}_{\mathbf{Q}}E$事实上是$Z_2$上的一个向量空间[见习题I.1.13和IV.1.1]。

(c) $\mathrm{Aut}_{\mathbf{Q}}E$无限并且不可数。[提示：对于$X$的每个子集合$Y$，均存在$\sigma\in\mathrm{Aut}_{\mathbf{Q}}E$，使得$\sigma(\sqrt{p})=-\sqrt{p}$（对于$\sqrt{p}\in Y$）和$\sigma(\sqrt{p})=\sqrt{p}$（对于$\sqrt{p}\in X-Y$）。因此由引论的定理8.5可知$|\mathrm{Aut}_{\mathbf{Q}}E|=|P(X)|>|X|$。但是$|X|=\aleph_0$。]

(d) 如果B是$\mathrm{Aut}_{\mathbf{Q}}E$在$Z_2$上的一组基，则$B$是无限不可数集合。

(e) $\mathrm{Aut}_{\mathbf{Q}}E$有无限不可数个指数为2的子群。[提示：如果$b\in B$，则$B-\{b\}$生成一个指数为2的子群。]

(f) 集合$\{\mathbf{Q}$的扩域$F \mid F\subset E, [F:\mathbf{Q}]=2\}$是可数的。

(g) $\mathrm{Aut}_{\mathbf{Q}}E$中指数为2的闭子群组成可数集合。

(h) $[E:\mathbf{Q}]\leqslant\aleph_0$，从而$[E:\mathbf{Q}]<|\mathrm{Aut}_{\mathbf{Q}}E|$。

17. 如果中间域E在K上正规，则E（对于F和K）是稳定的。

18. 设F在K上正规而E是中间域。则E在K上正规$\Longleftrightarrow E$是稳定的[见习题17]。此外我们有$(\mathrm{Aut}_K F)/E'\cong\mathrm{Aut}_K E$。

19. 基本定理(2.5或者3.12)的(ii)或者(ii)′等价于：中间域E在K上正规$\Longleftrightarrow$其对应的子群E'在$G=\mathrm{Aut}_K F$中正规。此外，在这种情形下我们有$G/E'\cong\mathrm{Aut}_K F$[见习题18]。

20. 如果F在中间域E上正规而E在K上正规，则F在K上不一定正规。[提

示：令$\sqrt[4]{2}$是2的4次实根，考虑$\mathbf{Q}(\sqrt[4]{2})\supset\mathbf{Q}(\sqrt{2})\supset\mathbf{Q}$并利用习题23.]将之与习题2进行比较.

21. 设F在K上是代数的.则F在K上正规$\Longleftrightarrow$对于每个域上的K-单同态σ：$F\to N$，其中N是K之包含F的任一正规扩张，则必有$\sigma(F)=F$，从而σ是F的K-自同构.[提示：将定理3.14的证明稍加修改，并利用定理3.16.]

22. 如果F在K上是代数的，并且F中每个元素均属于某个中间域E，而E在K上正规，则F在K上也正规.

23. 如果$[F:K]=2$，则F在K上正规.

24. K的代数扩张F在K上是正规的$\Longleftrightarrow$对于每个不可约多项式$f\in K[x]$，f在$F[x]$中分解成不可约因子的乘积之后，这些不可约因子均有相同的次数.

25. 设F是$f\in K[x]$的分裂域.不用定理3.14来证明F在K上是正规的.[提示：如果不可约多项式$g(x)\in K[x]$有根$u\in F$，但是在F中不分裂，便可证明存在K-同构$\varphi:K(u)\cong K(v)$，其中$v\notin F$而v是g的根.证明φ可以扩充成同构$F\cong F(v)$.这就与$[F:K]<[F(v):K]$这一事实相矛盾.]

4. 多项式的伽罗华群

这一节的主要目的是为前几节所介绍的概念提供一些应用和例子.除了两个地方之外，本节材料今后是不需要的.这两个地方就是定义4.1和定理4.12，而后者又与定理4.2有关.在第9节考虑多项式方程的根式可解性的时候要利用到它们.

定义4.1 设 K是域。多项式 $f \in K[x]$的伽罗华群指的是群 $\mathrm{Aut}_K F$，其中F是f在K上的分裂域。

按照系3.9，可知f的伽罗华群与F 的选取是无关的。在给出例子之前我们先介绍一些有益的事实。让我们回忆一下，对称群 S_n的子群 G叫作可迁的，是指对于任何$i \neq j(1 \leqslant i, j \leqslant n)$，均存在 $\sigma \in G$，使得$\sigma(i) = j$。

定理4.2 设K是域而多项式$f \in K[x]$的伽罗华群为G。

(i) G同构于某个对称群S_n的一个子群；

(ii) 如果f是n次(不可约) 可分多项式，则n整除$|G|$，并且G同构于S_n的一个可迁子群。

证明概要 (i) 如果$u_1, \cdots, u_n$是f在某个分裂域F中的全部相异根($1 \leqslant n \leqslant \deg f$)，由定理2.2可知每个$\sigma \in \mathrm{Aut}_K F$均诱导出$\{u_1, \cdots, u_n\}$的唯一的一个置换(但反过来不一定正确!)。将$S_n$看成$\{u_1, \cdots, u_n\}$的全部置换所形成的群，证明：通过将$\sigma \in \mathrm{Aut}_K F$映成它所诱导出的置换可以定义出一个单同态$\mathrm{Aut}_K F \to S_n$(注意$F = K(u_1, \cdots, u_n)$)。

(ii) F在K上是伽罗华的 (定理3.11)，并且 $[K(u_1):K] = n = \deg f$(定理1.6)。因此由基本定理2.5便知 G 有一个指数为n的子群，从而$n \mid |G|$。对于任意$i \neq j$，均存在K-同构$\sigma: K(u_i) \cong K(u_j)$，使得$\sigma(u_i) = u_j$(系1.9)。由定理3.8可将$\sigma$扩充成$F$的 K-自同构，从而G同构于S_n的一个可迁子群。∎

今后我们常常把多项式f的伽罗华群等同于 S_n 中那个同构的子群，从而可以看成是f的根上的置换群。进一步，对于我们今后所讨论的多项式 $f \in K[x]$，在多数情形下它 (在某个分裂域中) 的全部根是彼此不同的。这时f的每个不可约因子均是可分的。从

而由定理3.11（和习题3.13)可知f的分裂域F在K上是伽罗华的．如果所有这种多项式的伽罗华群都可以计算，便能够（至少在原则上）计算任意多项式的伽罗华群（习题1)。

系4.3 设K是域而$f\in K[x]$是2次不可约多项式，并且f的伽罗华群为G.如果f是可分的(当char $K\neq 2$时必然如此),则 $G\cong Z_2$；否则$G=1$。

证明概要 注意$S_2=Z_2$。利用定义3.10后面的注记(ii) 以及定理4.2. ∎

由定理4.2(ii)立刻得到如下的事实：3 次可分多项式的伽罗华群是S_3 或者A_3（因为只有它们才是S_3的可迁子群)。为了得到更精确一些的结果，我们需作更一般的考虑。

定义4.4 设K是域并且char $K\neq 2$。$f\in K[x]$是n 次多项式并且(在f的某个分裂域F中) 有n个不同的根$u_1,\cdots,u_n$。令 $\Delta=\prod_{i<j}(u_i-u_j)=(u_1-u_2)(u_1-u_3)\cdots(u_{n-1}-u_n)\in F$.我们将元素 $D=\Delta^2$称作f 的判别式。

注意Δ是分裂域F中的元素，所以$D=\Delta^2$自然也属于 F。但是我们有

命题4.5 假设K,f,F和Δ如定义4.4中所示。

(i) f的判别式实际上属于K;

(ii) 对于每个$\sigma\in \mathrm{Aut}_K F<S_n$,$\sigma$是偶置换的充要条件是$\sigma(\Delta)=\Delta$，而$\sigma$是奇置换的充要条件是$\sigma(\Delta)=-\Delta$。

证明概要 关于(ii) 可见定理I.6.7的证明。由(ii) 可知对

于每个$\sigma\in \mathrm{Aut}_K F$，$\sigma(\Delta^2)=\sigma(\Delta)^2=(\pm\Delta)^2=\Delta^2$。由于$F$在$K$上是伽罗华的，从而$\Delta^2\in K$(定理3.11和习题3.13)。∎

系4.6 假设K,f,F,Δ如定义4.4所示（从而F在K上是伽罗华的)，并且将$G=\mathrm{Aut}_K F$考虑成是S_n的子群。在伽罗华对应中（定理2.5)，子域$K(\Delta)$对应于子群$G\cap A_n$。特别地，G只包含偶置换的充要条件是$\Delta\in K$。

证明作为练习。∎

系4.7 设K是域而$f\in K[x]$为3次(不可约)可分多项式。则f的伽罗华群为S_3或者A_3。如果char $K\neq 2$，则f的伽罗华群为A_3的充要条件是f的判别式是K中元素的平方。

证明作为练习。利用定理4.2和系4.6.∎

如果基域K是实数域的子域，则可以利用三次多项式$f\in K[x]$的判别式来判别f有多少个实根（习题2)。

假设f如系4.7中所示。如果f的伽罗华群是$A_3\cong Z_3$，当然便不存在中间域。如果是S_3，则共有4个真的中间域：$K(\Delta)$，$K(u_1)$,$K(u_2)$和$K(u_3)$。其中u_1,u_2,u_3是f的根。$K(\Delta)$对应于A_3，而$K(u_i)$对应于S_3的子群$\{(1),(jk)\}(i\neq j,k)$，后一子群的阶数是2，指数是3(习题3)。

如果char $K\neq 2$，可以把计算3次可分多项式的伽罗华群这一问题归结为先计算判别式，然后决定它是否为K中元素的平方。下列结果有时是有益处的。

命题4.8 设K是域并且char$K\neq 2,3$。如果$f(x)=x^3+bx^2+cx+d\in K[x]$在某个分裂域中有三个不同的根，则多项式$g(x)=$

$f(x-b/3)\in K[x]$有形式x^3+px+q，并且f的判别式为$-4p^3-27q^2$。

证明概要 设F是f在K上的分裂域。证明$u\in F$是f的根$\Longleftrightarrow u+b/3$是$g=f(x-b/3)$的根。由此推出$g$与$f$有同样的判别式。证明$g$有形式$x^3+px+q(p,q\in K)$。令$v_1$，$v_2$，$v_3$是$g$在$F$中的根，则由$(x-v_1)(x-v_2)(x-v_3)=g(x)=x^3+px+q$可得出

$$v_1+v_2+v_3=0;\ v_1v_2+v_1v_3+v_2v_3=p;\ -v_1v_2v_3=q.$$

由于每个v_i均是g的根，从而

$$v_i^3=-pv_i-q\ (i=1,\ 2,\ 3).$$

现在利用定义$\Delta^2=(v_1-v_2)^2(v_1-v_3)^2(v_2-v_3)^2$，上面诸方程以及$(v_i-v_j)^2=(v_i+v_j)^2-4v_iv_j$，通过一系列计算即知$g$的判别式$\Delta^2$是$-4p^3-27q^2$。 ∎

例 根据定理III.6.6和命题III.6.8，可知多项式$x^3-3x+1\in\mathbb{Q}[x]$是不可约的。由于$\mathrm{char}\mathbb{Q}=0$从而它也是可分的。其判别式$-4(-3)^3-27\cdot1^2=108-27=81$为$\mathbb{Q}$中平方数。从而由系4.7可知其伽罗华群为$A_3$。

例 如果$f(x)=x^3+3x^2-x-1\in\mathbb{Q}[x]$，则

$$g(x)=f(x-3/3)=f(x-1)=x^3-4x+2.$$

由Eisenstein判别法（定理III.6.15）知它是不可约的。根据命题4.8，f的判别式为$-4(-4)^3-27\cdot2^2=256-108=148$。它不是$\mathbb{Q}$中的平方数。因此$f$的伽罗华群是$S_3$。

现在转而讨论域K上的四次多项式。象上面一样，我们只谈在某个分裂域F中有四个不同根u_1，u_2，u_3，u_4的多项式$f\in k[x]$。这时F在K上是伽罗华的，并且f的伽罗华群可以看成是$\{u_1,\ u_2,\ u_3,\ u_4\}$上的置换群，从而可看成是$S_4$的子群。子集$V=\{(1),\ (12)(34),\ (13)(24),(14)(23)\}$是$S_4$的正规子群（习题I.6.7），

它在今后讨论中将起着重要的作用．注意 V 同构于 四 元群 $Z_2 \oplus Z_2$，而$V \cap G$是$G = \mathrm{Aut}_K F < S_4$的正规子群．

引理4.9 假设K，f，F，u_i，V和$G = \mathrm{Aut}_K F < S_4$如上一段所示．令$\alpha = u_1u_2 + u_3u_4$，$\beta = u_1u_3 + u_2u_4$，$\gamma = u_1u_4 + u_2u_3 \in F$，则在伽罗华对应之下（定理2.5），子域$K(\alpha, \beta, \gamma)$对应于正规子群$V \cap G$．于是$K(\alpha, \beta, \gamma)$在$K$上是伽罗华的，并且$\mathrm{Aut}_K K(\alpha, \beta, \gamma) \cong G/(G \cap V)$．

证明概要 $G \cap V$中每个元素都固定α，β，γ，从而固定$K(\alpha, \beta, \gamma)$．按照基本定理，为了完成证明只需验证$G - V$中每个元素至少移动 α，β和γ中的一个．例如若 $\sigma = (12) \in G$并且 $\sigma(\beta) = \beta$，则$u_2u_3 + u_1u_3 = u_1u_3 + u_2u_4$．从而$u_2(u_3 - u_4) = u_1(u_3 - u_4)$．于是或者$u_1 = u_2$，或者$u_3 = u_4$，而这均导致矛盾．因此$\sigma(\beta) \neq \beta$．类似地处理其余情形．〔提示：不必检查全部 20 个可能性，证明：从S_4中对于V的每个陪集里只需要考虑一个代表元素即可．〕∎

令K，f，F，u_i和α，β，γ如引理4.9 中所示．在决定任一四次多项式的伽罗华群的时候，元素 α，β，γ起着关键的作用．多项式$(x - \alpha)(x - \beta)(x - \gamma) \in K(\alpha, \beta, \gamma)[x]$叫作$f$的三次结式．三次结式实际上是$K$上的多项式：

引理4.10 如果K是域而$f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$，则$f$的三次结式是多项式 $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2 \in K[x]$．

证明概要 如果f在某个分裂域F中有根 u_1，u_2，u_3，u_4．由于$f = (x - u_1)(x - u_2)(x - u_3)(x - u_4)$，从而可以将$b$，$c$，$d$，$e$用$\{u_i\}$表达出来．将三次结式$(x - \alpha)(x - \beta)(x - \gamma)$ 展开并作适

当的代换，再利用α，β，γ的定义（引理4.9）及上面给出的b，c，d，e的表达式即可证明结果。 ∎

现在我们可以计算任何(不可约)可分四次多项式$f\in K[x]$的伽罗华群了。由于它的伽罗华群G是S_4的可迁子群，从而$|G|$可以被4整除（定理4.2），因此$|G|$的阶只能为24，12，8和4。验证S_4的24，12和4阶可迁子群只有24阶的S_4，12阶的A_4，4阶群V($\cong Z_2\oplus Z_2$)，以及由长为4的轮换所生成的各种4阶循环子群。参见习题I．4.5和定理I.6.8。由（1234）和（24）生成的正方形对称群D_4是S_4的一个8阶可迁子群。由于D_4不是S_4的正规子群，并且每个8阶子群都是Sylow2-子群，从而由Sylow第二和第三定理可知S_4恰有3个8阶子群，并且每个都同构于D_4。

命题4.11 令K是域而$f\in K[x]$是（不可约）可分四次多项式，其伽罗华群为G（看作是S_4的子群）。令α，β，γ为f的三次结式的根，又令$m=[K(\alpha,\ \beta,\ \gamma):K]$。则

(i) $m=6\Longleftrightarrow G=S_4$；

(ii) $m=3\Longleftrightarrow G=A_4$；

(iii) $m=1\Longleftrightarrow G=V$；

(iv) $m=2\Longleftrightarrow G\cong D_4$或者$G\cong Z_4$。并且$G\cong D_4$的充要条件是$f$在$K(\alpha,\ \beta,\ \gamma)$上不可约。

证明概要 由于$K(\alpha,\ \beta,\ \gamma)$是一个三次多项式在$K$上的分裂域，从而$m$只能等于1，2，3或者6。由此及定理前面的讨论，可知只需证明每个($\Longleftarrow$)即可。由引理4.9可知$m=[K(\alpha,\ \beta,\ \gamma):K]=|G/G\cap V|$，我们要利用这一事实。

如果$G=A_4$，则$G\cap V=V$，$m=|G/V|=|G|\ /\ |V|=3$。类似地，如果$G=S_4$，则$m=6$。如果$G=V$，则$G\cap V=G$而$m=|G/G|$

$=1$. 如果$G\cong D_4$，则$G\cap V=V$（因为V包含在S_4的每个Sylow 2-子群之中），从而$m=|G/V|=|G|/|V|=2$. 如果G是4阶循环群，则G由一个长为4的轮换生成，而此轮换的平方必属于V，从而$|G\cap V|=2$，而$m=|G/G\cap V|=|G|/|G\cap V|=2$.

由于f或者是可约的或者是不可约的，并且$D_4\ncong Z_4$，从而对于命题4.11的最后一个论断只需证明它的逆即可. 令u_1，u_2，u_3，u_4是f在某个分裂域F中的根. 假如$G\cong D_4$，则$G\cap V=V$. 由于V是可迁子群，而$G\cap V=\mathrm{Aut}_{K(\alpha,\beta,\gamma)}F$（引理4.9），从而对于每一对$i\neq j(1\leqslant i,\ j\leqslant 4)$，均有$\sigma\in G\cap V$，使$\sigma$可以诱导出同构$K(\alpha,\beta,\gamma)(u_i)\cong K(\alpha,\beta,\gamma)(u_j)$，$\sigma(u_i)=u_j$并且$\sigma|K(\alpha,\beta,\gamma)$是恒等映射. 从而由系1.9便知对于每对$i\neq j$，$u_i$和$u_j$是$K(\alpha,\ \beta,\ \gamma)$上同一不可约多项式的根. 因此$f$在$K(\alpha,\ \beta,\ \gamma)$上是不可约的. 另一方面，如果$G\cong Z_4$，则$G\cap V=\mathrm{Aut}_{K(\alpha,\beta,\gamma)}F$的阶数是2，从而不是可迁的. 因此存在$i\neq j$，使得没有$\sigma\in G\cap V$将$u_i$映到$u_j$. 但是$F$是$K(\alpha,\beta,\gamma)(u_i)$和$K(\alpha,\ \beta,\ \gamma)(u_j)$上的分裂域. 假如存在同构$K(\alpha,\beta,\gamma)(u_i)\cong K(\alpha,\beta,\gamma)(u_j)$将$u_i$映到$u_j$并且在$K(\alpha,\beta,\gamma)$上是恒等映射，根据定理3.8可知它必然是某个$\sigma\in\mathrm{Aut}_{K(\alpha,\beta,\gamma)}F=G\cap V$的限制. 由于不存在这样的自同构$\sigma$，从而$u_i$和$u_j$不能是$K(\alpha,\ \beta,\gamma)$上同一不可约多项式的根（系1.9）. 因此$f$必然在$K(\alpha,\ \beta,\ \gamma)$上可约. ∎

例 根据Eisenstein判别法（定理III.6.15）可知多项式$f=x^4+4x^2+2\in\mathbb{Q}[x]$是不可约的. 由于$\mathrm{char}\mathbb{Q}=0$，$f$是可分的. 利用引理4.10算出三次结式为$x^3-4x^2-8x+32=(x-4)(x^2-8)$，从而$\alpha=4$，$\beta=\sqrt{8}$，$\gamma=-\sqrt{8}$. 而$\mathbb{Q}(\alpha,\beta,\gamma)=\mathbb{Q}(\sqrt{8})=\mathbb{Q}(2\sqrt{2})=\mathbb{Q}(\sqrt{2})$在$\mathbb{Q}$上是2维的. 因此$f$的伽罗华群是（同构于）$D_4$或者$Z_4$. 作代换$z=x^2$可得$f$为$z^2+4z+2$，易知它的根为

$z=-2\pm\sqrt{2}$。于是f的根是$x=\pm\sqrt{z}=\pm\sqrt{-2\pm\sqrt{2}}$。从而

$$f=(x-\sqrt{-2+\sqrt{2}})(x+\sqrt{-2+\sqrt{2}})(x-\sqrt{-2-\sqrt{2}})(x+\sqrt{-2-\sqrt{2}})$$
$$=(x^2-(-2+\sqrt{2}))(x^2-(-2-\sqrt{2}))\in\mathbb{Q}(\sqrt{2})[x].$$

因此f在$\mathbb{Q}(\sqrt{2})$上是可约的，于是由命题4.11(iv)可知f的伽罗华群是4次循环群。

例 为求$f=x^4-10x^2+4\in\mathbb{Q}[x]$的伽罗华群，我们先证明$f$是不可约的（从而也是可分的）。现在$f$在$\mathbb{Q}$中没有根，从而由定理III.6.6和命题III.6.8可知f没有线性和三次因子。至于二次因子，由引理III.6.13可知只需证明f在$\mathbb{Z}[x]$中没有二次因子即可。不难证明，不存在整数a，b，c，d，使得$f=(x^2+ax+b)(x^2+cx+d)$。因此f在$\mathbb{Q}[x]$中不可约。f的三次结式是$x^3+10x^2-16x-160=(x+10)(x+4)(x-4)$，三个根均在$\mathbb{Q}$中，因此由命题4.11可得$m=[\mathbb{Q}(\alpha,\beta,\gamma):\mathbb{Q}]=1$，而$f$的伽罗华群是$V(\cong Z_2\oplus Z_2)$。

例 根据Eisenstein判别法，多项式$x^4-2\in\mathbb{Q}[x]$是不可约的（从而也是可分的）。三次结式为$x^3+8x=x(x+2\sqrt{2}i)(x-2\sqrt{2}i)$，而$\mathbb{Q}(\alpha,\beta,\gamma)=\mathbb{Q}(\sqrt{2}i)$在$\mathbb{Q}$上是2维的。证明$x^4-2$在$\mathbb{Q}(\sqrt{2}i)$上不可约（因为$\sqrt{2}$，$\sqrt[4]{2}\notin\mathbb{Q}(\sqrt{2}i)$）。从而由命题4.11可知$f$的伽罗华群是（同构于）$D_4$。

例 考虑$f=x^4-5x^2+6\in\mathbb{Q}[x]$。注意$f$在$\mathbb{Q}$上是可约的，即$f=(x^2-2)(x^2-3)$。从而不能利用命题4.11。显然$F=\mathbb{Q}(\sqrt{2},\sqrt{3})$是$f$在$\mathbb{Q}$上的分裂域。由于$x^2-3$在$\mathbb{Q}(\sqrt{2})$上不可约，从而$[F:\mathbb{Q}]=[F:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\cdot2=4$。因此$f$的伽罗华群$\mathrm{Aut}_{\mathbb{Q}}F$是4阶的（基本定理）。由定理4.2的证明以及系4.3可知$\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2})$共有两个元素：恒等映射1和映射$\sigma:\sqrt{2}\longmapsto-$

$\sqrt{2}$. 根据系1.9,1和σ均能够以两种不同的方式扩充成F的$\mathbf{Q}$-自同构(依赖于将$\sqrt{3}$映成$\sqrt{3}$还是$-\sqrt{3}$).这给出 $\mathrm{Aut}_{\mathbf{Q}}F$中4个不同的元素 (由 4 种可能的组合$\sqrt{2}\longmapsto\pm\sqrt{2}$, $\sqrt{3}\longmapsto\pm\sqrt{3}$ 所决定). 由于 $|\mathrm{Aut}_{\mathbf{Q}}F| = 4$, 而每个非恒等自同构的阶数均是2, 从而由习题I.4.5即知f的伽罗华群必定同构于四元群$Z_2\oplus Z_2$.

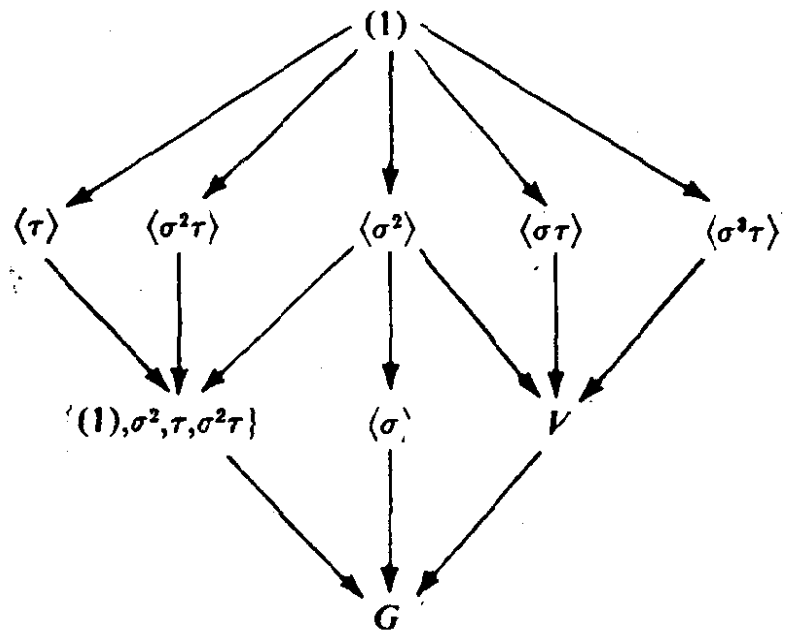
决定一个可分四次多项式的伽罗华群的子群和对应的中间域比三次多项式的情形还要复杂. 比如,甚至当$u_i\neq u_j$的时候,也可能有$K(u_i)=K(u_j)$(见上面最后一个例子).我们不能将关于四次多项式的这一问题的全部情形叙述成一个简单的命题, 所以, 要具体问题具体解决.

例 令$F\subset\mathbf{C}$是$f=x^4-2\in\mathbf{Q}[x]$在 $\mathbf{Q}$ 上的分裂域. 如果u是2的正实四次根, 则f的全部根为u, $-u$, ui, $-ui$. 为了将f的伽罗华群看成是S_4的子群, 我们必须将这些根安排成一定的次序. 假定$u_1=u$, $u_2=-u$, $u_3=ui$, $u_4=-ui$.从命题4.11后面的第三个例子知道,G是S_4中同构于D_4的三个8阶子群中的一个. 注意复共轭是$\mathbf{C}$的$\mathbf{R}$-自同构, 它显然为 $u\longmapsto u$, $-u\longmapsto -u$, $ui\longmapsto -ui$, $-ui\longmapsto ui$. 从而它诱导出$F=\mathbf{Q}(u, ui)$的一个$\mathbf{Q}$-自同构 τ. 作为S_4中的元素则 τ是 (34). 现在 S_4中每个8阶子群均与D_4共轭 (第二Sylow 定理). 通过不太复杂的计算可知, 包含(34)的8阶子群只有一个, 即是由$\sigma=(1324)$ 和 $\tau=(34)$生成的群D. 易知$F=\mathbf{Q}(u, ui)=\mathbf{Q}(u, i)$. 从而$F$的每个$\mathbf{Q}$-自同构都可由它在$u$和$i$上的作用所完全确定. 因此, D 中的元素或者用σ和τ来表达, 或者用它在u和i上的作用来表达. 它们可以归纳成如 417 面的表格.

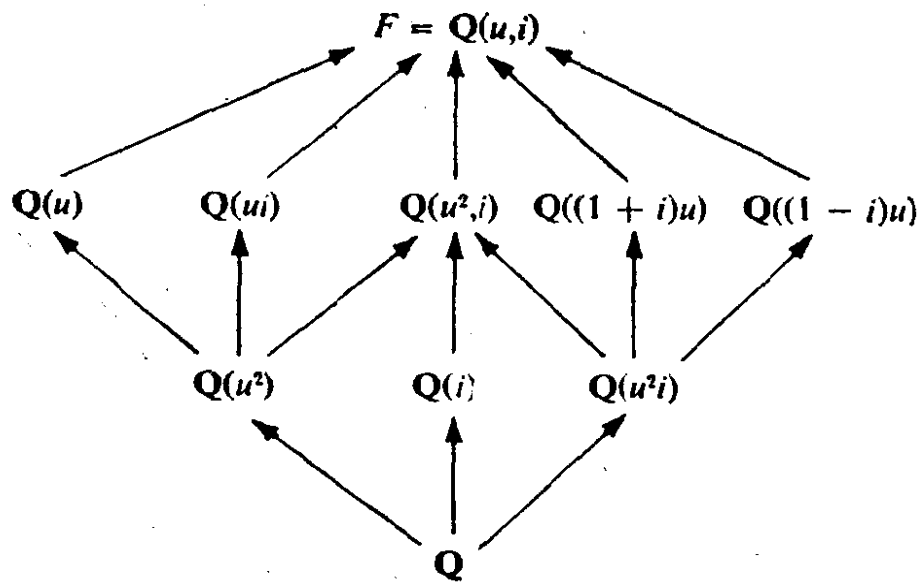
请读者验证: D 的子群格和子域格如 417 面图中 所 示. 其中在同样位置上的中间域和子群, 是彼此一一伽罗华对应的.

	(1)	(34)	(1324)	(12)(34)	(1423)	(13)(24)	(12)	(14)(23)
$u \mapsto$	u	u	ui	$-u$	$-ui$	ui	$-u$	$-ui$
$i \mapsto$	i	$-i$	i	i	i	$-i$	$-i$	$-i$

子群格（$H \longrightarrow K$表示$H < K$）：



中间域格（$M \longrightarrow N$表示$M \subset N$）：



至于如何计算任意域上次数大于4的多项式的伽罗华群，很缺乏有效的技术。下面是一个很特殊的情形。

定理4.12 如果 p是素数而f是有理数域上的p次不可约多项式，并且f在复数域中恰好有两个非实根，则f的伽罗华群是（同构于）S_p。

证明概要 令G是f的伽罗华群，并且看作是S_p的子群。因为$p \mid |G|$（定理4.2），由Cauchy定理II.5.2知G包含p阶元素σ，由系I.6.4知σ是长为p的轮换。现在复共轭$(a+bi \longmapsto a-bi)$是$\mathbb{C}$的$\mathbb{R}$自同构。它移动每个非实数。因此由定理2.2便知它将f的两个非实根对换，而固定所有其他的根。从而G中包含一个对换$c=(ab)$。由于σ可以写成$\sigma=(aj_2\cdots j_p)$，而σ的某个幂次有形式$\sigma^k=(abi_3\cdots i_p)\in G$。必要时改变符号，无妨设$\tau=(12)$而$\sigma^k=(123\cdots p)$。由练习题I.6.4知道这两个元素生成$S_p$，从而$G=S_p$。∎

例 观察 $f=x^5-4x+2\in\mathbb{Q}[x]$ 的图象，可知它只有三个实根。根据Eisenstein判别法（定理III.6.15）知道多项式f是不可约的，由定理4.12便知它的伽罗华群是S_5。

是否对于每个有限群G，均存在 $\mathbb{Q}$ 的伽罗华扩域使G是它的伽罗华群？这一问题仍未解决。但是如果 $G=S_n$，则答案是肯定的（习题14）。

习　题

注：若不作说明，则K为域，$f\in K[x]$，而F是f在K上的分裂域。

1. 假设$f\in K[x]$在F中分裂：$f=(x-u_1)^{n_1}\cdots(x-u_k)^{n_k}$ 诸u_i两两不同，$n_i\geqslant 1$）。令v_0，…v_k是多项式 $g=(x-u_1)(x-u_2)\cdots(x-u_k)$的系数，$E=K(v_0,\ \cdots,\ v_k)$。则

(a) F是g在E上的分裂域；

(b) F在E上是伽罗华的；

(c) $\mathrm{Aut}_E F = \mathrm{Aut}_K F$.

2. 假设K是$\mathbf{R}$的子域（从而F可以取作$\mathbf{C}$的子域），f是三次不可约多项式。令D为f的判别式.则

(a) $D>0 \Leftrightarrow f$有三个实根；

(b) $D<0 \Leftrightarrow f$恰好有一个实根.

3. 设f是可分的三次多项式，其伽罗华群为S_3而三个根为u_1，u_2，$u_3 \in F$。则扩张$K \subset F$的全部中间域为F，$K(\triangle)$，$K(u_1)$，$K(u_2)$，$K(u_3)$和K.对应的伽罗华群之子群分别为 1，A_3，T_1，T_2，T_3，S_3，其中$T_i = \{(1), (jk) \mid j \neq i \neq k\}$.

4. 如果$\mathrm{char} K \neq 2$，3，则$x^3 + bx^2 + cx + d$的判别式是$-4c^3 - 27d^2 + b^2(c^2 - 4bd) + 18bcd$.

5. 如果$\mathrm{char} K \neq 2$而$f \in K[x]$是三次多项式，它的判别式为K中的平方元素，则f在K中或者不可约或者完全分解.

6. 在任何基域K上，$x^3 - 3x + 1$或者不可约或者完全分解.

7. S_4不存在6阶可迁子群.

8. 设f是K上（不可约）四次可分多项式，u是f的根.则K和$K(u)$之间不存在真中间域$\Leftrightarrow f$的伽罗华群是A_4或者S_4.

9. 设$x^4 + ax^2 + b \in K[x]$ ($\mathrm{char} K \neq 2$) 是不可约的，并且其伽罗华群为G.

(a) 如果b是K中平方元素，则$G = V$.

(b) 如果b不是K中平方元素而$b(a^2 - 4b)$是K中平方元素，则$G \cong Z_4$.

(c) 如果b和$b(a^2 - 4b)$均不是K中平方元素，则$G \cong D_4$.

10. 在所指明的域上决定下列多项式的伽罗华群.

(a) $x^4 - 5$在$\mathbf{Q}$，$\mathbf{Q}(\sqrt{5})$以及$\mathbf{Q}(\sqrt{5}i)$上.

(b) $(x^3 - 2)(x^2 - 3)(x^2 - 5)(x^2 - 7)$在$\mathbf{Q}$上.

(c) $x^8 - x - 1$在$\mathbf{Q}$以及$\mathbf{Q}(\sqrt{23}i)$上.

(d) $x^8 - 10$在$\mathbf{Q}$以及$\mathbf{Q}(\sqrt{2})$上.

(e) $x^4 + 3x^3 + 3x - 2$在$\mathbf{Q}$上.

(*f*) x^5-6x+3在$\mathbf{Q}$上。

(*g*) x^8-2在$\mathbf{Q}$上。

(*h*) $(x^3-2)(x^2-5)$在$\mathbf{Q}$上。

(*i*) x^4-4x^2+5在$\mathbf{Q}$上。

(*j*) x^4+2x^2+x+3在$\mathbf{Q}$上。

11. 决定多项式$(x^3-2)(x^2-3)\in\mathbf{Q}[x]$(在$\mathbf{Q}$上) 的分裂域的全部中间域和其伽罗华群的全部子群。

12. 设K是实数域的子域，$f\in K[x]$为不可约四次多项式。如果f恰好有两个实根，则f的伽罗华群为S_4或者D_4。

13. 假设$f(x)\in K[x]$在分裂域F中有不同的根$u_1,u_2,\cdots,u_n$。令$G=\mathrm{Aut}_K F<S_n$是f的伽罗华群。又令$y_1,\cdots,y_n$为未定元。定义

$$g(x)=\prod_{\sigma\in S_n}(x-(u_{\sigma(1)}y_1+u_{\sigma(2)}y_2+\cdots+u_{\sigma(n)}y_n))$$

(*a*) 求证

$$g(x)=\prod_{\sigma\in S_n}(x-(u_1y_{\sigma(1)}+u_2y_{\sigma(2)}+\cdots+u_ny_{\sigma(n)}))$$

(*b*) 证明$g(x)\in K[y_1,\cdots,y_n,x]$

(*c*) 假设$g(x)$分解为$g_1(x)g_2(x)\cdots g_r(x)$，

$g_i(x)\in K(y_1,\cdots,y_n)[x]$是不可约首1多项式。

如果$x-\sum_i u_{\sigma(i)}y_i$是$g_1(x)$的因子，求证

$$g_1(x)=\prod_{\tau\in G}\left(x-\sum_i u_{\tau\sigma(i)}y_i\right)$$

求证由此推出$\deg g_i(x)=|G|$。

(*d*) 如果$K=\mathbf{Q}$，$f\in\mathbf{Z}[x]$是首1的，p是素数。以$\overline{f}\in Z_p[x]$表示将f之系数作mod p运算之后而得到的多项式。假如$\overline{f}$在Z_p的某个分裂域$\overline{F}$中有相异的根$\overline{u}_1,\cdots,\overline{u}_n$。求证

$$\overline{g}(x)=\prod_{\tau\in S_n}\left(x-\sum_i \overline{u}_i y_{\tau(i)}\right)\in\overline{F}[x,\ y_1,\cdots,y_n]。$$

如果$\overline{u_i}$安排成适当的次序，可以证明$\overline{f}$的伽罗华群$\overline{G}$是f之伽罗华群G的子群。

(*e*) 证明$x^6+22x^5-9x^4+12x^3-37x^2-29x-15\in\mathbf{Q}[x]$的伽罗华群是$S_6$[提示：对于$p=2$，3，5利用(*d*)]。

(*f*) $x^5-x-1\in\mathbf{Q}[x]$的伽罗华群是S_5。

14. 对于给定的$n\geqslant 3$，现在给出构作伽罗华群为S_n的多项式$f\in\mathbf{Q}[x]$的一种方法。它依赖于如下的事实，即在$Z_p[x]$中存在着任意次数的不可约多项式(p为素数，见后面的系5.9)。先选取f_1，f_2，$f_3\in\mathbf{Z}[x]$，使得

(i) $\deg f_1=n$，并且$\overline{f_1}\in Z_2[x]$不可约（记号见13(*d*)）。

(ii) $\deg f_2=n$并且$\overline{f_2}\in Z_3[x]$在$Z_3[x]$中分解成gh，其中g是$n-1$次不可约多项式而h是线性式。

(iii) $\deg f_3=n$并且$\overline{f_3}\in Z_5[x]$分解成gh或者gh_1h_2，其中g是$Z_5[x]$中不可约四次多项式，而h，h_1，h_2为$Z_5[x]$中奇次不可约多项式。

(*a*) 令$f=-15f_1+10f_2+6f_3$。则$f\equiv f_1\pmod 2$，$f\equiv f_2\pmod 3$和$f\equiv f_3\pmod 5$。

(*b*) f的伽罗华群G是可迁的(因为$\overline{f}$在$Z_2[x]$中不可约)。

(*c*) G包含有形如$S=(i_1i_2\cdots i_{n-1})$的轮换和元素$\sigma\lambda$，其中σ为对换而λ是阶为奇数的一些轮换的乘积。从而$\sigma\in G$，于是由习题I.6.3和可迁性可知存在某个$k(1\leqslant k\leqslant n-1)$，使得$(i_k i_n)\in G$。

(*d*) $G=S_n$（见(*c*)及习题I.6.4(*b*)）。

5. 有 限 域

在本节中我们用分裂域来刻划有限域（有时叫作伽罗华域），并且完全决定出它们的结构。有限域扩成或有限域时，证明了其伽罗华群是循环群，并且明显地给出此群的生成元。

开始先讲两个定理和一个引理，它们也可以用于无限域。当然在所有情形下，我们的兴趣主要在于应用到有限域上。

定理5.1 假设F是域而P是F的全部子域的交。则P是域并且P没有真子域。如果$\mathrm{char}F=p$(素数)，则$P\cong Z_p$。如果$\mathrm{char}F=0$，则$P\cong\mathbf{Q}$(有理数域)。域P叫作F的素子域。

证明概要 注意F的每个子域必然包含0和1_F。由此即知P是域并且它没有真子域。P显然包含全部形如$m1_F(m\in\mathbf{Z})$的元素。为了完成证明，我们只需再证：当$\mathrm{char}F=p$时，$P=\{m1_F\mid m\in\mathbf{Z}\}$；而当$\mathrm{char}F=0$时，$P=\{(m1_F)(n1_F)^{-1}\mid m,\ n\in\mathbf{Z},\ n\neq 0\}$。这可以直接证明，也可采用下述办法：根据定理III.1.9可知映射$\psi:\mathbf{Z}\longrightarrow P$，$m\longmapsto m1_F$是环同态，其核为$(n)$，其中$n=\mathrm{char}F$是0或者素数。如果$n=p$(素数)，则$Z_p\cong\mathbf{Z}/(p)=\mathbf{Z}/\ker\psi\cong\mathrm{Im}\psi\subset P$。如果$n=0$，则$\psi:\mathbf{Z}\longrightarrow P$是单同态，由系III.4.6可知有域的单同态$\bar{\psi}:\mathbf{Q}\longrightarrow P$。于是象前面一样，$\mathbf{Q}\cong\mathrm{Im}\,\bar{\psi}=P$。∎

系5.2 如果F是有限域，则$\mathrm{char}Fp=\neq 0$，其中p为素数，并且$|F|=p^n$(对于某个整数$n\geqslant 1$)。

证明 由定理III.1.9和定理5.1可知F的特征是素数$p\neq 0$。由于F是其素子域Z_p上的有限维向量空间，所以$F\cong Z_p\oplus Z_p\oplus\cdots\oplus Z_p$($n$个分量)(定理IV.2.4)。于是$|F|=p^n$。∎

在定理5.1的同构之下，今后我们永远将特征p有限域的素子域等同于Z_p。例如我们将写成$Z_p\subset F$。特别地，1_F与$1\in Z_p$一致。

定理5.3 如果F是域而G是F的非零元素乘法群的有限子群，则G是循环群，特别地，有限域全部非零元素形成的乘法群是循

环群.

证明 如果$G(\neq 1)$是有限Abel群，则由定理II.2.1可知 $G\cong Z_{m_1}\oplus Z_{m_2}\oplus\cdots\oplus Z_{m_k}$，其中 $m_1>1$ 并且 $m_1|m_2|\cdots|m_k$。由于 $m_k(\sum Z_{m_i})=0$，从而每个$u\in G$都是多项式$x^{m_k}-1_F\in F[x]$ 的根(注意G 是乘法群)。由于这个多项式在F中至多有m_k个不同的根(定理III.6.7)，从而$k=1$并且$G\cong Z_{m_k}$。∎

系5.4 如果F是有限域，则它是其素子域Z_p的单扩张。即存在$u\in F$使得$F=Z_p(u)$。

证明概要 取u为F之非零元素乘法群的生成元即可。∎

引理5.5 如果F是特征p域，$r\geqslant 1$为整数，则映射$\psi:F\longrightarrow F$，$u\longmapsto u^{p^r}$是域的Z_p—单同态。如果F是有限域，则ψ为F的Z_p-自同构。

证明概要 关键事实是：对于特征p的域F，$(u\pm v)^{p^r}=u^{p^r}\pm v^{p^r}$(对所有$u$，$v\in F$)(习题III.1.11)。由于$1_F\longmapsto 1_F$，可知$\psi$固定$F$的素子域$Z_p$中每个元素。∎

现在我们给出有限域的一种有益的刻划方式。

命题5.6 设p是素数而$n\geqslant 1$为整数。则F为 p^n 个元素的有限域$\Longleftrightarrow F$是$x^{p^n}-x$在Z_p上的分裂域。

证明 如果$|F|=p^n$，则F的非零元素乘法群的阶是p^n-1。从而每个非零元素$u\in F$均满足$u^{p^n-1}=1_F$即每个非零元素$u\in F$ 都是$x^{p^n-1}-1_F$的根，从而也是$x(x^{p^n-1}-1_F)=x^{p^n}-x\in Z_p[x]$的根。由于$0\in F$也是 $x^{p^n}-x$的根，而 $x^{p^n}-x$在F中恰好有p^n个不同的根(根据定理III.6.7它在F上分裂)，这些根恰好是F中全部元素。所

以F 是$x^{p^n}-x$在Z_p上的分裂域。

如果F是$f=x^{p^n}-x$在Z_p上的分裂域，由于$\mathrm{char}F=\mathrm{char}Z_p=p$，而$f'=-1$，从而$f$和$f'$互素。由定理III.6.10(ii)可知$f$有$p^n$ 个不同的根。如果ψ是引理5.5中的单同态($r=n$)，易知 $u\in F$是f的根$\Longleftrightarrow\psi(u)=u$。用此事实证明$f$在$F$中的全部根形成 F 的一个 p^n阶子域E，它必然包含F的素域Z_p。由于F是分裂域，它在Z_p上是由f的全部根(即E中全部元素)生成的。因此$F=Z_p(E)=E$。∎

系5.7 设p是素数而$n\geqslant 1$为整数，则存在p^n 元域。具有同样多个元素的任意两个有限域是彼此同构的。

证明 给定p和n，由定理3.2可知存在$x^{p^n}-x$ 在Z_p 上的分裂域，从命题5.6可知它的阶是p^n。由于每个p^n阶有限域都是$x^{p^n}-x$在Z_p上的分裂域(命题5.6)，从而由系3.9可知任意两个这样的域是彼此同构的。∎

系5.8 如果K是有限域而$n\geqslant 1$为整数，则存在K的单扩张$F=K(u)$，使得F是有限域并且$[F:K]=n$。K 上任意两个n维扩域都是K-同构的。

证明概要 给了p^r元域K。令F是$f=x^{p^{rn}}-x$在K上的分裂域。根据定理5.6，每个$u\in K$都满足$u^{p^r}=u$，由此可归纳证明出$u^{p^{rn}}=u$。所以F实际上是f在Z_p上的分裂域(习题3.3)。由命题5.6的证明可知F恰好由f的p^{rn} 个不同的根所组成。从而 $p^{rn}=|F|=|K|^{[F:k]}=(p^r)^{[F:k]}$，于是$[F:K]=n$。由系5.4可知$F$是$K$的单扩张。如果$F_1$是$K$的另一个扩域并且$[F_1:K]=n$，则 $[F_1:Z_p]=n[K:Z_p]=nr$，从而$|F_1|=p^{nr}$。由命题5.6推出F_1是 $x^{p^{rn}}-x$ 在Z_p 上的分

裂域，从而也是在K上的分裂域。从而由系3.9可知F和F_1是K-同构的。∎

系5.9 如果K是有限域而$n\geqslant 1$是整数，则$K[x]$中存在着n次不可约多项式。

证明 作为练习。利用系5.8和定理1.6 ∎

命题5.10 如果F是有限域K的有限维扩域，则F是有限域并且是K上的伽罗华扩张。其伽罗华群$\mathrm{Aut}_K F$是循环群。

证明概要 令Z_p是K的素子域。则F在Z_p上是有限维的（定理1.2），设维数是n，于是$|F|=p^n$。从命题5.6的证明和习题3.2可知F是$x^{p^n}-x$在Z_p上（从而也是在K上）的分裂域，其根是彼此不同的。由定理3.11即知F在K上是伽罗华的。而由引理5.5可知映射$\psi: F\longrightarrow F$，$u\longmapsto u^p$是Z_p-自同构。ψ^n显然是恒等映射，而ψ的k次幂（$k<n$）不是恒等映射（因为若不然，则$x^{p^k}-x$在F中有p^n（$n>k$）个不同的根，这就与定理 III.6.7 相矛盾）。根据基本定理，$|\mathrm{Aut}_{Z_p}F|=n$，$\mathrm{Aut}_{Z_p}F$ 必定是由ψ生成的循环群。由于$\mathrm{Aut}_K F$ 是$\mathrm{Aut}_{Z_p}F$的子群，根据定理I.3.5，可知$\mathrm{Aut}_K F$也是循环群。∎

习　题

注：F永远表示域K的扩域。

1. 如果K是特征p的有限域，描述K的加法群结构。
2. (Fermat)如果$p\in\mathbf{Z}$是素数，则对所有$a\in Z_p$，$a^p=a$。或者等价地说：对于每个$c\in\mathbf{Z}$，$c^p\equiv c(\mathrm{mod}\,p)$。
3. 如果$|K|=p^n$，则K中每个元素在K中都有唯一的p次根。
4. 如果首1多项式$f\in K[x]$（在某个分裂域中）的根是两两不同的并且它们

形成域，则$\mathrm{char}K = p$并且$f = x^{p^n} - x$（对于某个$n \geqslant 1$）。

5. (a) 构作9元域并给出它的加法表和乘法表。

(b) 对于25元域作同样的事情。

6. 如果$|K| = q$并且$(n, q) = 1$，而F是$x^n - 1$在K上的分裂域，则$[F : K]$是满足$n | (q^k - 1)$的最小正整数k。

7. 如果$|K| = q$而$f \in K[x]$是不可约的，则f整除$x^{q^n} - x$的充要条件是$\deg f$整除n。

8. 如果$|K| = p^r$而$|F| = p^n$，则$r | n$而$\mathrm{Aut}_K F$是由$\varphi: \ u \longmapsto u^{p^r}$所生成的循环群。

9. 如果$n \geqslant 3$，则$x^{2^n} + x + 1$在Z_2上可约。

10. 有限域中每个元素均可以表示成两个平方元素之和。

11. 令F是Z_p的代数闭包（p为素数）。则

(a) F是Z_p的伽罗华代数扩张。

(b) 映射$\varphi: \ F \to F$，$u \longmapsto u^p$是F的Z_p-自同构并且不是恒等自同构。

(c) 子群$H = \langle \varphi \rangle$是$\mathrm{Aut}_{Z_p} F$的真子群，它的固定域是$Z_p$，由(a)可知$Z_p$也是$\mathrm{Aut}_{Z_p} F$的固定域

12. 如果K是有限域而F是K的代数闭包，则$\mathrm{Aut}_K F$是Abel群。除了1_F之外，$\mathrm{Aut}_K F$中每个元素的阶都是无限的。

6. 可 分 性

现在我们同时讨论可分性和在某种意义上与它完全相反的一个概念——纯不可分，这种讲法为我们对于可分性的研究提供很大的方便。因此，本节开始先研究纯不可分扩张，定理6.4以几种不同的方式刻划这种扩张，然后用这些思想证明关于代数扩张可

分性的全部重要事实（主要是定理6.7）。我们详细讨论了代数扩张的可分次数和不可分次数（但是这方面的大多数内容在今后不需要）。最后证明本原元素定理（命题6.15），这个结果与本节中其他结果是无关的，可以在任何时候阅读。

定义6.1 设L是K的扩域。代数元素$u\in F$叫作在K上是纯不可分的，是指它在$K[x]$中的不可约多项式在$F[x]$中分解成$f=(x-u)^m$。假如F的每个元素在K上均是纯不可分的，我们称F是K的纯不可分扩张。

因此，u在K上是可分的$\Longleftrightarrow u$的n次极小多项式f（在某个分裂域中）有n个不同的根。而u在K上是纯不可分的$\Longleftrightarrow f$恰好有一个根。所以可能有的元素在K上既不是可分的，也不是纯不可分的。

定理6.2 设F是K的扩域。则$u\in F$在K上既是可分的又是纯不可分的，当且仅当$u\in K$。

证明 元素$u\in F$既是可分的又是纯不可分的$\Longleftrightarrow$它的极小多项式为$(x-u)^m$并且在某个分裂域中有m个不同的根。显然这只有$m=1$的时候，即$x-u\in K[x]$，从而$u\in K$。∎

如果$\mathrm{char}K=0$，则K上的每个代数元素在K上都是可分的。因此由定理6.2推出K中纯不可分元素只能是K中元素。从而当$\mathrm{char}K=0$时，K的纯不可分扩张只有K自身。所以通常我们只考虑特征不为零（即是素数）的情形。我们经常使用下列事实而不作明显的说明：如果$\mathrm{char}K=p\neq 0$，u，$v\in K$，则$(u\pm v)^{p^n}=u^{p^n}\pm v^{p^n}$（对于每个$n\geqslant 0$）（习题III.1.11）。为了刻划纯不可分扩张我们需要：

引理6.3 设F是K的扩域并且$\mathrm{char}K=p\neq 0$，如果$u\in F$在K上是代数的，则存在某个$n\geqslant 0$，使得u^{p^n}在K上是可分的。

证明概要 对于u在K上的次数作数学归纳法。如果$\deg u=1$或者u是可分的，则引理是对的。如果f是次数大于1的不可分元素u的极小多项式，则$f'=0$(定理III.6.10)，于是f是x^p的多项式(习题III.6.3)。因此u^p是K上的代数元素而次数小于$\deg u$，然后由归纳假设可知存在某个$m\geqslant 0$，使得$(u^p)^{p^m}$在K上是可分的。∎

定理6.4 如果F是域K的代数扩域，其特征$p\neq 0$，则下列一些命题是彼此等价的：

(i) F在K上纯不可分；

(ii) 每个元素$u\in F$的极小多项式均有形式$x^{p^n}-a\in K[x]$；

(iii) 如果$u\in F$，则存在某个$n\geqslant 0$，使得$u^{p^n}\in K$。

(iv) F中在K上可分的元素必然属于K；

(v) F是由全体纯不可分元素在K上生成的。

证明概要 (i)$\Longrightarrow$(ii)：令$(x-u)^m$是$u\in F$的极小多项式，令$m=np^r$，$(n,\ p)=1$。则$(x-u)^m=(x-u)^{p^r n}=(x^{p^r}-u^{p^r})^n$(习题III.1.11)。由于$(x-u)^m\in K[x]$，从而$x^{p^r(n-1)}$的系数$\pm nu^{p^r}$(定理III.1.6)必然属于$K$。但是从$(p,\ n)=1$可知$u^{p^r}\in K$(习题1)。由于$(x-u)^m=(x^{p^r}-u^{p^r})^n$在$K[x]$中是不可约的，必然$n=1$，而$(x-u)^m=x^{p^r}-a$，从而$a=u^{p^r}\in K$。

(ii)$\Longrightarrow$(iii)和(i)$\Longrightarrow$(v)是显然的。(iii)$\Longrightarrow$(i)由习题III.1.11。(i)$\Longrightarrow$(iv)由定理6.2。(iv)$\Longrightarrow$(iii)由引理6.3。

(v)$\Longrightarrow$(iii)：如果u在K上纯不可分，则由(i)$\Longrightarrow$(ii)的证明可知存在某个$n\geqslant 0$使得$u^{p^n}\in K$。对于任意的$u\in F$再使用定理

1.3和习题III.1.11. ∎

系6.5 如果F是K的有限维纯不可分扩张而$\mathrm{char}K=p\neq 0$，则存在某个$n\geqslant 0$使得$[F:K]=p^n$.

证明 根据定理1.11可知$F=K(u_1,\cdots,u_m)$. 从假设条件知每个u_i在K上都是纯不可分的，从而在$K(u_1,\cdots,u_{i-1})$上也是纯不可分的(习题2). 由定理1.6和6.4(ii)推出塔$K\subset K(u_1)\subset K(u_1,u_2)\subset\cdots\subset K(u_1,\cdots,u_m)=F$中的每一步的维数都是$p$的方幂，从而由定理1.2可知$[F:K]=p^n$. ∎

为证明关于可分性的主要定理我们还需要：

引理6.6 如果F是K的扩域，X是F的子集合，$F=K(X)$，并且X的每个元素在K上都是可分的，则F是K的可分扩张.

证明 如果$v\in F$，则存在$u_1,\cdots u_n\in X$，使得$v\in K(u_1,\cdots,u_n)$(定理1.3). 令$f_i\in K[x]$是u_i的极小多项式，从而也是可分多项式. E是$\{f_1,\cdots,f_n\}$在$K(u_1,\cdots,u_n)$上的分裂域. 则E也是$\{f_1,\cdots,f_n\}$在K上的分裂域(习题3.3). 由定理3.11可知E在K上是可分的(事实上也是伽罗华的). 这就导致$v\in K(u_1,\cdots,u_n)\subset E$在$K$上也是可分的. ∎

定理6.7 设F是K的代数扩域，S是F中全部在K上可分的元素所构成的集合，P是F中全部在K上纯不可分的元素所构成的集合. 则

(i) S是K的可分扩域.

(ii) F在S上纯不可分.

(iii) P为K的纯不可分扩域.

(iv) $P \cap S = K$。

(v) F在P上可分$\Longleftrightarrow F = SP$。

(vi) 如果F在K上正规，则S在K上是伽罗华的，F在P上是伽罗华的，并且$\mathrm{Aut}_K S \cong \mathrm{Aut}_P F = \mathrm{Aut}_K F$。

注记：S显然是K在F中的极大可分扩张，并且在K上可分的每个中间域都包含在S中。对于P和纯不可分中间域则有类似情形。如果$\mathrm{char}K = 0$，则$S = F$并且$P = K$(定理6.2)。

证明概要 (i) 如果$u, v \in S$并且$v \neq 0$，由引理6.6可知$K(u, v)$在K上可分，从而$u - v$，$uv^{-1} \in S$。从而S是子域，由引理6.3，定理6.4再利用习题III.1.11 (对于$\mathrm{char}K = p$) 或者 $P = K$ (对于$\mathrm{char}K = 0$)，这些事实即可按部就班地推导出(ii)和(iii)。由定理6.2可推出(iv)。

(v) 如果F在P上是可分的，则F在合成域SP上也是可分的(习题3.12)，同时在SP上又是纯不可分的((ii)和习题2)。从而由定理6.2可知$F = SP$。反之，如果$F = SP = P(S)$。由习题3.12和引理6.6可知F在P上是可分的。

(vi) 我们首先证明$\mathrm{Aut}_K F$的固定域K_0实际上是P。由此立刻推出F在P上是伽罗华的并且$\mathrm{Aut}_P F = \mathrm{Aut}_K F$。令$u \in F$在$K$上的极小多项式是$f$，$\sigma \in \mathrm{Aut}_K F$，则$\sigma(u)$是$f$的根 (定理2.2)。如果$u \in P$，则$f = (x-u)^m$，从而$\sigma(u) = u$。因此$P \subset K_0$。如果$u \in K_0$，并且$v \in F$是$f$的另一个根，则存在$K$-同构$\tau$：$K(u) \to K(v)$使得$\tau(u) = v$ (系1.9)。由定理3.8，3.14和习题3.2可知τ可以扩充为F的K-自同构。由于$u \in K_0$，从而$u = \tau(u) = v$。由正规性知f在$F[X]$中分裂，这就表明$f = (x-u)^m$ (对于某个m)。因此$u \in P$。从而$P \supset K_0$。于是$P = K_0$。

每个$\sigma \in \mathrm{Aut}_P F = \mathrm{Aut}_K F$必然将可分元素映成可分元素 (定理

2.2)。因此$\sigma \longmapsto \sigma|S$定义出一个同态$\theta$：$\mathrm{Aut}_P F \to \mathrm{Aut}_K S$。由于$F$在$S$上正规，从而$\theta$是满同态（定理3.8，3.14和习题3.2)。由于F在P上是伽罗华的，由(v)推出$F=SP$，这就导致θ是单同态。从而$\mathrm{Aut}_P F \cong \mathrm{Aut}_K S$。最后，假设$u \in S$是由全体$\sigma \in \mathrm{Aut}_K S$所固定。由于$\theta$是满同态，所以$u$属于$\mathrm{Aut}_P F$的固定域$P$，于是$u \in P \cap S = K$。从而$S$在$K$上是伽罗华的。∎

系6.8 如果F是E的可分扩域而E是K的可分扩域，则F在K上是可分的。

证明 如果S象定理6.7所示，则$E \subset S$而F在S上纯不可分。但是F在E上可分，从而在S上也可分(习题3.12)。于是由定理6.2便知$F=S$。∎

令F是特征$p \neq 0$的域。引理5.5表明，对于每个$n \geqslant 1$，集合$F^{p^n}=\{u^{p^n} \mid u \in F\}$是$F$的子域。根据定理6.4(iii)，$F$在$F^{p^n}$上是纯不可分的，从而在任意中间域上也是纯不可分的(习题2)。

系6.9 设F是K的代数扩域，$\mathrm{char}K=p \neq 0$。如果F在K上可分，则对于每个$n \geqslant 1$，均有等式$F=KF^{p^n}$。如果$[F:K]$有限，并且$F=KF^p$，则F在K上可分。特别地，$u \in F$在K上可分$\Longleftrightarrow K(u^p)=K(u)$。

证明概要 假设S如定理6.7中所示。如果$[F:K]$有限，则$F=K(u_1,\cdots,u_m)=S(u_1,\cdots,u_m)$（定理1.11)。由于$u_i$在$S$上都是纯不可分的（定理6.7)，从而存在$n \geqslant 1$，使得对于每个$i$，$u_i^{p^n} \in S$。由于$F=S(u_1,\cdots,u_m)$，从习题III.1.11和定理1.3推出$F^{p^n} \subset S$。$S$中每个元素在$F^{p^n}$上显然是纯不可分的，从而在$KF^{p^n}$上也是纯不可分的。而$S$在$K$上可分，从而在$KF^{p^n}$上也可分。因此由定

理6.2可知$S=KF^{p^n}$。利用$\mathrm{char}K=p$这一事实和定理1.3可证对每个$t\geqslant 1$均有$F^{p^t}=[K(u_1,\cdots,u_m)]^{p^t}=K^{p^t}(u_1^{p^t},\cdots,u_m^{p^t})$。注意这对于$F$在$K$上的任意生成元集合$\{u_1,\cdots,u_m\}$都是对的。现在如果$F=KF^p$，则$K(u_1,\cdots,u_m)=F=KF^p=K(u_1^p,\cdots,u_m^p)$。这样迭代下去，即可用生成元集合$\{u_i^{p^t}\}$代替$\{u_i\}[t=1,2,\cdots,n]$，从而$F=K(u_1,\cdots,u_m)=K(u_1^{p^n}\cdots,u_m^{p^n})=KF^{p^n}=S$，于是$F$在$K$上是可分的。反之，如果$F$在$K$上可分，则$F$在$KF^{p^n}$上既可分又纯不可分(对于每个$n\geqslant 1$)。从而由定理6.2即知$F=KF^{p^n}$。∎

下面我们从稍微不同的观点考虑可分性和不可分性。虽然命题6.12在第7节的某个地方要使用，但是为了理解后面的内容，最本质的事情实际上只是定义6.10和它后面的注记。

定义6.10 如果F是K的代数扩域而S是F的最大子域使得S在K上可分（象定理6.7中那样）。我们将维数$[S:K]$叫作F在K上的可分次数。并且表示成$[F:K]_s$。而维数$[F:S]$叫做是F在K上的不可分次数，表示成$[F:K]_i$。

注记：$[F:K]_s=[F:K]$并且$[F:K]_i=1$的充要条件是F在K上可分。而$[F:K]_i=[F:K]$并且$[F:K]_s=1$的充要条件是F在K上纯不可分。在任何情形下，由定理1.2可知必有$[F:K]=[F:K]_s[F:K]_i$，如果$[F:K]$有限并且$\mathrm{char}K=p\neq 0$，由系6.5和定理6.7(ii)知$[F:K]_i$是p的方幂。下面引理能使我们用另一种方法描述$[F:K]_s$，并且能够证明对于任一中间域E，$[F:E]_s[E:K]_s=[F:K]_s$。

引理6.11 假设F是E的扩域而E是K的扩域，N是K的正规扩域并且包含F。以r表示不同的E-单同态$F\to N$的个数，以t表示不

同的K-单同态$E\to N$的个数，则不同的K-单同态$F\to N$的个数为rt。

证明 为方便起见，我们假设r和t都是有限的。对于一般情形的证明是同样的，只不过稍微修改一下符号而已。令$\tau_1,\cdots,\tau_r$是全部E-单同态$F\to N$，而$\sigma_1,\cdots,\sigma_t$是全部K-单同态$E\to N$。每个σ_i都可以扩充成N的K-自同构（定理3.8和3.14以及习题3.2），它仍旧表示成σ_i。每个合成映射$\sigma_i\tau_j$都是K-单同态$F\to N$。如果$\sigma_i\tau_j=\sigma_a\tau_b$，则$\sigma_a^{-1}\sigma_i\tau_j=\tau_b$，从而$\sigma_a^{-1}\sigma_i|E=1_E$。于是$\sigma_i=\sigma_a$，即$i=a$。由于$\sigma_i$是单射，从而由$\sigma_i\tau_j=\sigma_i\tau_b$推出$\tau_j=\tau_b$，即$j=b$。因此，$rt$个$K$-单同态$\sigma_i\tau_j:F\to N$（$1\leqslant i\leqslant t$，$1\leqslant j\leqslant r$）是彼此不同的。令$\sigma$：$F\to N$是任意一个$K$-单同态。则$\sigma|E=\sigma_i$（对于某个$i$），而$\sigma_i^{-1}\sigma$是$K$-单同态$F\to N$，并且它在$E$上为恒等映射。因此$\sigma_i^{-1}\sigma=\tau_j$（对于某个$j$），于是$\sigma=\sigma_i\tau_j$。从而$rt$个映射$\sigma_i\tau_j$便是全部$K$-单同态$F\to N$。∎

命题6.12 设F是K的有限维扩域，N是K的正规扩域并且N包含F。则不同的K-单同态$F\to N$的个数恰好等于F在K上的可分次数$[F:K]_s$。

证明概要 令S是F的极大子域，使得S在K上可分（定理6.7(i)）。每个K-单同态$S\to N$都可以扩充成N的一个K-自同构（定理3.8，3.14和习题3.2）。从而（通过限制）也是K-单同态$F\to N$。我们断言：不同的K-单同态$F\to N$的个数恰好等于不同的K-单同态$S\to N$的个数。如果$\mathrm{char}K=0$，则$F=S$，所以这显然是对的。以下设$\mathrm{char}K=p\neq 0$。假设σ，τ是K-单同态$F\to N$，使得$\sigma|S=\tau|S$。如果$u\in F$，由定理6.4和6.7(ii)可知存在某个$n\geqslant 0$，使得$u^{p^n}\in S$。因此

$$\sigma(u)^{p^n}=\sigma(u^{p^n})=\tau(u^{p^n})=\tau(u)^{p^n},$$

于是$\sigma(u)=\tau(u)$. 所以从$\sigma|S=\tau|S$推出$\sigma=\tau$，这就证明了我们的断言. 所以我们不妨假定F在K上是可分的（即$F=S$），在这种情形下我们有$[F:K]=[F:K]_S$，$[F:E]=[F:E]_S$和$[E:K]=[E:K]_S$(对任意中间域E)(习题3.12).

现在对$n=[F:K]=[F:K]_S$采用数学归纳法. $n=1$时显然正确. 如果$n>1$，取$u\notin F-K$，则$[K(u):K]=r>1$. 如果$r<n$，用归纳假设和引理6.11（取$E=K(u)$)即可证明定理. 如果$r=n$，则$F=K(u)$，并且$[F:K]$是u的(可分)极小多项式$f\in K[x]$的次数. 每个K-单同态$\sigma:F\to N$由$v=f(u)$所完全决定. 由于v是f的根（象定理2.2中那样)，从而至多有$[F:K]=\deg f$个这样的K-单同态. 由正规性知f在N中分裂，并且f是可分的，从而由系1.9可知恰好有$[F:K]$个不同的K-单同态$F\to N$. ∎

系6.13 如果F是E的扩域而E是K的扩域，则

$$[F:E]_S[E:K]_S=[F:K]_S,\quad [F:E]_i[E:K]_i=[F:K]_i$$

证明作为练习. 利用引理6.11和命题6.12 ∎

系6.14 令$f\in K[x]$是域K上的不可约首1多项式，F是f在K上的分裂域，u_1是f在F中的一个根，则

(i) f的每个根的重数都是$[K(u_1):K]_i$，从而在$F[x]$中：

$$f=[(x-u_1)\cdots(x-u_n)]^{[K(u_1):K]_i},$$

其中$u_1,\cdots,u_n$是f的全部相异根，而$n=[K(u_1):K]_S$.

(ii) $u_1^{[K(u_1):K]_i}$在K上是可分的.

证明概要 由于$\mathrm{char}K=0$的情形显然正确，我们假定$\mathrm{char}K=p\neq 0$.

(i) 对于每个$i>1$，存在着K-同构$\sigma: K(u_1)\cong K(u_i)$，使得$\sigma(u_1)=u_i$，它可以扩充成$F$的$K$-自同构(系1.9，定理3.8和习题3.2)。因为$f\in K[x]$，由定理2.2可知

$$(x-u_1)^{r_1}\cdots(x-u_n)^{r_n}=f=\sigma f$$
$$=(x-\sigma(u_1))^{r_1}\cdots(x-\sigma(u_n))^{r_n}.$$

由于$u_1,\cdots,u_n$彼此不同，而σ为单射，再由$K[x]$是唯一因子分解整环，即知$(x-u_i)^{r_i}=(x-\sigma(u_1))^{r_1}$，从而$r_1=r_i$。这就表明$f$的每个根的重数都是$r=r_1$。从而$f=(x-u_1)^r\cdots(x-u_n)^r$，而$[K(u_1):K]=\deg f=nr$。现在由系1.9和定理2.2推出共存在$n$个不同的$K$-单同态 $K(u_1)\to F$，从而由命题6.12和定理3.14便知$[K(u_1):K]_S=n$。因此

$$[K(u_1):K]_i=[K(u_1):K]/[K(u_1):K]_S=nr/n=r.$$

(ii) 由于r是$p=\mathrm{char}K$的方幂，我们有$f=(x-u_1)^r\cdots(x-u_n)^r=(x^r-u_1^r)\cdots(x^r-u_n^r)$。因此$f$是$x^r$的多项式并且系数属于$K$。假定$f=\sum_{i=0}^{m}a_ix^{ri}$。从而$u_1^r$是$g(x)=\sum_{i=0}^{n}a_ix^i=(x-u_1^r)\cdots(x-u_n^r)\in K[x]$的根。由于$u_1,\cdots u_n$两两不同，从而$g(x)\in K[x]$是可分的，因此$u_1^{[K(u_1):K]_i}$在$K$上也是可分的。∎

下面一个结果与前面的内容无关，并且今后也不需要。

命题6.15 (本原元素定理) 设F是K的有限维扩域。

(i) 如果F在K上是可分的，则F是K的单扩张。

(ii) (Artin)更一般地，F是K的单扩张$\Longleftrightarrow$只有有限多中间域。

注记：满足$F=K(u)$条件的u叫作本原元素。

证明概要 引理3.17证明的第一段在K是有限域时也是正确

的，它表明一个可分扩张只有有限多个中间域．从而我们只需证明(ii)即可．当K为有限域时(ii)显然成立（系5.8），以下假定K是无限域．(ii)的$\Longleftarrow$部分已经在引理3.17证明的第二段中得到．反之，假定$F=K(u)$，其中u在K上是代数的（因为$[F:K]$有限）．令E是一个中间域，$g\in E[x]$是u在E上的极小多项式．如果$g=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，则$[F:E]=n$．证明$[F:K(a_0,\cdots,a_{n-1})]=n$，从而$E=K(a_0,\cdots,a_{n-1})$．因此每个中间域$E$均由$u$在$E$上的极小多项式$g$所唯一确定．如果$f$是$u$在$K$上的极小多项式，由定理1.6可知$g|f$．因为$f$在任意分裂域中的分解都是唯一的（系III.6.4），从而f只能具有有限个不同的首1因式．所以只有有限多个中间域．∎

习　题

注：若不作特别说明，F永远表示域K的扩域．

1．假设$\mathrm{char}K=p\neq0$，$n\geqslant1$是整数，并且$(p,n)=1$．如果$v\in F$并且$nv\in K$，则$v\in K$．

2．如果$u\in F$在K上是纯不可分的，则u在任何中间域E上也是纯不可分的．于是，如果F在K上是纯不可分的，则F在E上也是纯不可分的．

3．如果F在中间域E上纯不可分，而E在K上纯不可分，则F在K上也纯不可分．

4．如果$u\in F$在K上可分，$v\in F$在K上纯不可分，则$K(u,v)=K(u+v)$．又如果$u\neq0$，$v\neq0$，则$K(u,v)=K(uv)$．

5．如果$\mathrm{char}K=p\neq0$，$a\in K$但是$a\notin K^p$，则对于每个$n\geqslant1$，$x^{p^n}-a\in K[x]$均不可约．〔注〕

〔注〕 在本书中，“$f(x)\in K[x]$不可约”意思是$f(x)$在K上不可约．
——译者

6. 如果$f\in K[x]$是首1不可约多项式，$\deg f\geqslant 2$，并且f（在某个分裂域中）的所有根均相等，则$\mathrm{char}K=p\neq 0$并且$f=x^{p^n}-a$（$n\geqslant 1$，$a\in K$）。

7. 设F，K，S，P如定理6.7所示，又设E是中间域，则

   (*a*) F在E上纯不可分$\Longleftrightarrow S\subset E$。

   (*b*) 如果F在E上可分，则$P\subset E$。

   (*c*) 如果$E\cap S=K$，则$E\subset P$。

8. 如果$\mathrm{char}K=p\neq 0$，而$[F:K]$有限并且不被p整除，则F在K上可分。

9. 设$\mathrm{char}K=p\neq 0$。则代数元素$u\in F$在K上是可分的$\Longleftrightarrow$对于每个$n\geqslant 1$，$K(u)=K(u^{p^n})$。

10. 设$\mathrm{char}K=p\neq 0$。令$f\in K[x]$是n次不可约多项式。令m为最大非负整数，使得f是x^{p^m}的多项式但不是$x^{p^{m+1}}$的多项式，则$n=n_0p^m$。如果u是f的根，则$[K(u):K]_s=n_0$而$[K(u):K]_i=p^m$。

11. 如果$f\in K[x]$是$m>0$次不可约多项式，并且$\mathrm{char}K\nmid m$，则f是可分的。

12. F在K上是纯不可分的$\Longleftrightarrow F$在K上是代数的并且对于F的每个扩域E，均只有一个K-单同态$F\to E$（即包含映射）。

13. (*a*) 关于域K的下列诸条件是彼此等价的

   (i) $K[x]$中每个不可约多项式都是可分的。

   (ii) K的每个代数闭包在K上都是伽罗华的。

   (iii) K的每个代数扩域在K上都是可分的。

   (iv) 或者$\mathrm{char}K=0$，或者$\mathrm{char}K=p\neq 0$并且$K=K^p$。满足(i)—(iv)条件的域K叫作完全域。

   (*b*) 每个有限域都是完全域。

14. 如果$F=K(u,v)$，其中u和v在K上是代数的，并且u在K上是可分的，则F是K的单扩张。

15. 设$\mathrm{char}K=p\neq 0$，$F=K(u,v)$，其中$u^p\in K$，$[F:K]=p^2$。则F不是K的单扩张。展示该扩张具有无限多个中间域。

16. 设F是K的代数扩张，并且$K[x]$中每个多项式在F中都有根。则F是K的代数闭包。[提示：定理3.14，6.7和命题6.15可能是有帮助的.]

7. 循环扩张

第7—9节的基本议题是分析一些伽罗华扩张，其伽罗华群具有预先给定的结构（例如是循环群或者是可解群）。我们在本节中主要是刻划具有循环伽罗华群的有限维伽罗华扩张(命题7.7，7.8和定理7.11)。为了作到这一点，先讨论关于迹和范的一些知识。

定义7.1 假设F是K的有限维扩域，$\bar{K}$是K的代数闭包并且包含F。令$\sigma_1,\cdots,\sigma_r$是所有不同的K-单同态$F\to\bar{K}$。如果$u\in F$，则u的范是元素

$$N_K^F(u)=(\sigma_1(u)\sigma_2(u)\cdots\sigma_r(u))^{[F:K]_i}$$

而u的迹是元素

$$T_K^F(u)=[F:K]_i(\sigma_1(u)+\sigma_2(u)+\cdots+\sigma_r(u))。$$

注记：下面的定理7.3表明这一定义与$\bar{K}$的选取无关。利用K的任一包含F的正规扩域来代替$\bar{K}$，可以给出一个等价的定义(习题1)。$\bar{K}$在K上是正规的（定理3.4和3.14），从而由命题6.12可知$r=[F:K]_s$是有限的。在课文中明确无误的时候，有时将N_K^F和T_K^F简写作N和T。

还要注意，迹基本上是范的加性模拟。这意味着在许多例子中，关于迹或者范中一个命题的证明，可以直接转而用来证明关于另一个对象的类似命题。但是也有某些例外。例如若F在K上不可分。则$\mathrm{char}K=p\neq0$并且$[F:K]_i=p^t(t\geqslant1)$。从而对每个$u\in$

F, $T_K^F(u)=0$，但是N_K^F可以不是零。

例 令$F=\boldsymbol{C}$，$K=\boldsymbol{R}$。取$\bar{K}=\boldsymbol{C}$。不难看出，只有两个$\boldsymbol{R}$-单同态$\boldsymbol{C}\to\boldsymbol{C}$，即恒等映射和复共轭。从而$N(a+bi)=[(a+bi)(a-bi)]=a^2+b^2$。

这里主要是将范和迹应用于伽罗华扩张$K\subset F$。在这种情形下，伽罗华群是有限的，并且对于范和迹有更方便的刻划办法，这种刻划方式有时拿来作为定义。

定理7.2 如果F是K的有限维伽罗华扩域，并且

$$\mathrm{Aut}_K F=\{\sigma_1,\cdots,\sigma_n\},$$

则对于每个$u\in F$，

$$N_K^F(u)=\sigma_1(u)\sigma_2(u)\cdots\sigma_n(u),$$

$$T_K^F(u)=\sigma_1(u)+\sigma_2(u)+\cdots+\sigma_n(u).$$

证明 令$\bar{K}$是K的代数闭包并且包含F。由于F在K上是正规的（系3.15），从而K-单同态$F\to\bar{K}$恰好是$\mathrm{Aut}_K F$中的元素（定理3.14）。由于F在K上也是可分的（系3.15），从而$[F:K]_i=1$。现在由定义7.1直接得出定理的结论。∎

假设F在K上是伽罗华的，$\mathrm{Aut}_K F=\{\sigma_1,\cdots,\sigma_n\}$。由于$\mathrm{Aut}_K F$是群，（对于每一固定的$\sigma_i\in\mathrm{Aut}_K F$）元素$\sigma_i\sigma_1,\sigma_i\sigma_2\cdots,\sigma_i\sigma_n$仍旧是$\sigma_1,\sigma_2,\cdots,\sigma_n$（可能次序不同）。由此可知，对于每个$u\in F$，$N_K^F(u)$和$T_K^F(u)$被每个$\sigma_i\in\mathrm{Aut}_K F$所固定。因此$N_K^F(u)$和$T_K^F(u)$必然属于$K$。下面定理表明，即使$F$在$K$上不是伽罗华的，这一事实仍旧正确。此定理的前两条常常被使用，但是后两条今后是不需要的。

定理7.3 令F是K的有限维扩域，对于所有$u,v\in F$，

(i) $N_K^F(u)N_K^F(v)=N_K^F(uv)$,

$T_K^F(u)+T_K^F(v)=T_K^F(u+v)$

(ii) 如果$u\in K$，则 $N_K^F(u)=u^{[F:K]}$，$T_K^F(u)=[F:K]u$。

(iii) $N_K^F(u)$ 和$T_K^F(u)$ 是K中元素。更确切地说：

$$N_K^F(u)=((-1)^n a_0)^{[F:K(u)]}\in K,$$

$$T_K^F(u)=-[F:K(u)]a_{n-1}\in K$$

其中$f=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in K[x]$是$u$ 的极小多项式。

(iv) 如果E是中间域，则

$$N_K^E(N_E^F(u))=N_K^F(u),\qquad T_K^E(T_E^F(u))=T_K^F(u).$$

证明概要 (i) 和 (ii) 可以直接从定义 7.1 与$r=[F:K]_s$，$[F:K]_s[F:K]_i=[F:K]$这些事实得出。

(iii) 令$E=K(u)$。K的代数闭包$\bar{K}$ 若包含 F，则$\bar{K}$ 也是 E的代数闭包。从引理 6.11 的证明可知，所有不同的 K-单同态 $F\to\bar{K}$恰好是映射 $\sigma_k\tau_j$ $(1\leqslant k\leqslant t,\ 1\leqslant j\leqslant r)$ 全体，其中 $\{\sigma_k\}$ 是$\bar{K}$的全体K-自同构，它们在E上的限制两两不同，而$\{\tau_j\}$是全部不同的E-单同态$F\to\bar{K}$。因此由命题6.12可知$t=[E:K]_s$，从而$n=[E:K]=t[E:K]_i$（系6.13）。

利用(ii) 和系6.13证明$N_K^F(u)=\left(\prod_{k=1}^{t}\sigma_k(u)\right)^{[F:E][E:K]_i}$，

$T_K^F(u)=[F:E][E:K]_i\left(\sum_{k=1}^{t}\sigma_k(u)\right)$。由于$\sigma_i:K(u)\cong K(\sigma_i(u))$，从而由系1.9推出$\sigma_1(u),\cdots,\sigma_t(u)$是$f$的全部不同的根。由系6.4可知：

$$f=[x-\sigma_1(u))(x-\sigma_2(u))\cdots(x-\sigma_t(u))]^{[E:K]_i}$$

$$=\left[x^t-\left(\sum_{k=1}^{t}\sigma_k(u)\right)x^{t-1}+\cdots+(-1)^t\prod_{k=1}^{t}\sigma_k(u)\right]^{[E:K]_i}$$

如果$[E:K]_i=1$，则$n=t$，从而立刻得到结论。如果$[E:K]_i>1$，

则$[E:K]_i$是$p=\mathrm{char}K$的正幂次．计算a_0值是容易的，并且也容易看出$a_{n-1}=0=T_K^F(u)$．再使用习题III.1.11．

(iv) 利用证明（iii）过程中的记号，但这时E是任意中间域．再使用有关的定义和系6.13．∎

除了迹和范之外我们还需要

定义7.4 假设S是域F的一个自同构非空集合．如果对任意$a_1,\cdots,a_n\in F$，$\sigma_1,\cdots,\sigma_n\in S(n\geqslant 1)$，

$a_1\sigma_1(u)+\cdots+a_n\sigma_n(u)=0$（对所有$u\in F$）$\Longrightarrow a_i=0$（对每个$i$），这时我们便称$S$是线性无关的．

引理7.5 如果S是域F中一些彼此不同的自同构所组成的集合，则S是线性无关的．

证明 如果S不是线性无关的，则存在非零$a_i\in F$和不同的$\sigma_i\in S$，使得

$$a_1\sigma_1(u)+a_2\sigma_2(u)+\cdots+a_n\sigma_n(u)=0\ (\text{对所有}u\in F)\quad (1)$$

在所有这些“相关方程”之中选取一个使n为最小值的．显然$n>1$．因为σ_1和σ_2不同，从而存在$v\in F$，使得$\sigma_1(v)\neq\sigma_2(v)$．将(1)用于元素$uv$（对任意$u\in F$），便给出：

$$a_1\sigma_1(u)\sigma_1(v)+a_2\sigma_2(u)\sigma_2(v)+\cdots+a_n\sigma_n(u)\sigma_n(v)=0\quad (2)$$

将(1)式乘以$\sigma_1(v)$得到

$$a_1\sigma_1(u)\sigma_1(v)+a_2\sigma_2(u)\sigma_1(v)+\cdots+a_n\sigma_n(u)\sigma_1(v)=0\quad (3)$$

将(2)和(3)两式相减，便给出（对于每个$u\in F$）：$a_2[\sigma_2(v)-\sigma_1(v)]\sigma_2(u)+a_3[\sigma_3(v)-\sigma_1(v)]\sigma_3(u)+\cdots+a_n[\sigma_n(v)-\sigma_1(v)]\sigma_n(u)=0$．由于$a_2\neq 0$，$a_2(v)\neq\sigma_1(v)$，所以上式中系数不全为零，而这就与$n$的极小性相矛盾．∎

域K的扩域F叫作K的循环扩张或者Abel扩张，是指F为K的伽罗华代数扩张，并且$\mathrm{Aut}_K F$分别是循环群或者Abel群。在这种情形下，如果$\mathrm{Aut}_K F$是n阶有限循环群，则F叫作K的n次循环扩张（由基本定理可知这时$[F:K]=n$）。例如定理5.10是说：有限域的每个有限维扩张都是循环扩张。下一个定理给出循环扩张与范和迹之间的密切联系。

定理7.6 假设F是K的n次循环扩张，σ是$\mathrm{Aut}_K F$的生成元，$u\in F$，则

(i) $T_K^F(u)=0\Longleftrightarrow$存在某个$v\in F$，使得$u=v-\sigma(v)$，

(ii) (Hilbert定理90)〔注〕$N_K^F(u)=1_K\Longleftrightarrow$存在某个非零元素$v\in F$，使得$u=v\sigma(v)^{-1}$。

证明概要 为方便起见，记$\sigma(x)=\sigma x$。由于σ生成$\mathrm{Aut}_K F$，所以σ为n阶元素，而$\sigma,\sigma^2,\sigma^3,\cdots,\sigma^{n-1}$，$\sigma^n=1_F=\sigma^0$是$F$的$n$个不同的自同构。由定理7.2可知$T(u)=u+\sigma u+\sigma^2 u+\cdots+\sigma^{n-1}u$，$N(u)=u(\sigma u)(\sigma^2 u)\cdots(\sigma^{n-1}u)$。

(i) 如果$u=v-\sigma v$，则利用定义和下列事实

$$T(v-\sigma v)=T(v)-T(\sigma v),\quad \sigma^n(v)=v$$

即可证得$T(u)=0$。反之，假设$T(u)=0$。按下述方法选取$w\in F$使得$T(w)=1_K$：按照引理7.5（因为$1_K\neq 0$），存在$z\in F$使得

$$0\neq 1_F z+\sigma z+\sigma^2 z+\cdots+\sigma^{n-1}z=T(z)。$$

从定理7.2后面的注记知道$T(z)\in K$，因此$\sigma[T(z)^{-1}z]=T(z)^{-1}\sigma(z)$。所以若令$w=T(z)^{-1}z$，则

$$T(w)=T(z)^{-1}z+T(z)^{-1}\sigma z+\cdots+T(z)^{-1}\sigma^{n-1}z=$$

〔注〕 这一命题是Hilbert著名的〈数论报告〉(Zahlbericht)一书中的定理90，故后人多用此名称。 ——译者

$T(z)^{-1}T(z)=1_K$。现在令

$$v=uw+(u+\sigma u)(\sigma w)+(u+\sigma u+\sigma^2u)(\sigma^2w)+$$
$$(u+\sigma u+\sigma^2u+\sigma^3u)(\sigma^3w)+\cdots$$
$$+(u+\sigma u+\cdots+\sigma^{n-2}u)(\sigma^{n-2}w).$$

由于σ是自同构，并且从

$$0=T(u)=u+\sigma u+\sigma^2u+\cdots+\sigma^{n-1}u$$

推得 $u=-(\sigma u+\sigma^2u+\cdots+\sigma^{n-1}u)$，由此便可证得

$$v-\sigma v=uw+u(\sigma w)+u(\sigma^2w)+u(\sigma^3w)+\cdots+u(\sigma^{n-2}w)+$$
$$u(\sigma^{n-1}w)=uT(w)=u1_K=u.$$

(ii) 如果$u=v\sigma(v)^{-1}$，由于σ是n阶自同构，从而$\sigma^n(v^{-1})=v^{-1}$，$\sigma(v^{-1})=\sigma(v)^{-1}$。并且对每个$1\leqslant i\leqslant n-1$，$\sigma^i(v\sigma(v)^{-1})=\sigma^i(v)\sigma^{i+1}(v)^{-1}$。于是

$N(u)=(v\sigma(v)^{-1})(\sigma v\sigma^2(v)^{-1})(\sigma^2v\sigma^3(v)^{-1})\cdots(\sigma^{n-1}v\sigma^n(v)^{-1})$
$=1_K$。反之，假定$N(u)=1_K$，则 $u\neq0$。由引理7.5，存在 $y\in F$，使得由下式给出的元素

$$v=uy+(u\sigma u)\sigma y+(u\sigma u\sigma^2u)\sigma^2y+\cdots+(u\sigma u\cdots\sigma^{n-2}u)\sigma^{n-2}y$$
$$+(u\sigma u\cdots\sigma^{n-1}u)\sigma^{n-1}y$$

不为零。由于上式最后一项是$N(u)\sigma^{n-1}y=1_K\sigma^{n-1}y=\sigma^{n-1}y$，不难验证$u^{-1}v=\sigma v$，从而 $u=v\sigma(v)^{-1}(\sigma(v)\neq0$是因为$v\neq0$而$\sigma$为单射)。∎

现在我们已有足够的准备来分析循环扩张。开始我们先将问题化成简单的形式。

命题7.7 设 F 是K的n次循环扩域，并假设 $n=mp^t$，其中 $0\neq p=\mathrm{char}K$并且 $(m,p)=1$.则存在中间域链 $F\supset E_0\supset E_1\supset\cdots\supset E_{t-1}\supset E_t=K$，使得$F$是$E_0$的$m$次循环扩张，而对每个$\sigma\leqslant i\leqslant t$，

E_{i-1}是E_i的p次循环扩张。

证明概要 根据假设F在K上是伽罗华的，并且$\mathrm{Aut}_K F$是循环群（因此也是Abel群），从而每个子群都是正规的。由于循环群的每个子群和商群都是循环的(定理I.3.5)。由基本定理2.5(ii)可推出，对于每个中间域E，F在E上是循环的，E在K上是循环的。从而对每一对中间域$L\subset M$,M是L的循环扩张。特别地，M是L的伽罗华代数扩张。

令H是$\mathrm{Aut}_K F$的唯一的m阶(循环)子群（习题I.3.6)而E_0是它的固定域（于是$H=H''=E_0'=\mathrm{Aut}_{E_0}F$)。则$F$是$E_0$的$m$次循环扩张,$E_0$是$K$的$p^t$次循环扩张。由于$\mathrm{Aut}_K E_0$是$p^t$次循环群，从而有子群链

$$1=G_0<G_1<G_2<\cdots<G_{t-1}<G_t=\mathrm{Aut}_K E_0.$$

其中$|G_i|=p^i$，$[G_i:G_{i-1}]=p$，而G_i/G_{i-1}是p阶循环群（见定理I.3.4 (vii))。对于每个i，令E_i为G_i的固定域（对于E_0和$\mathrm{Aut}_K E_0$)。由基本定理2.5导致：

(i) $E_0\supset E_1\supset E_2\supset\cdots\supset E_{t-1}\supset E_t=K$;

(ii) $[E_{i-1}:E_i]=[G_i:G_{i-1}]=p$;

(iii) $\mathrm{Aut}_{E_i}E_{i-1}\cong G_i/G_{i-1}$.

因此E_{i-1}是E_i的p次循环扩张（$0\leqslant i\leqslant t-1$)。 ∎

令F为K的n次循环扩域。按照命题7.7，至少在原则上我们可以只需考虑两种情形：(i) $n=\mathrm{char}K=p\neq 0$；(ii) $\mathrm{char}K=0$或者$\mathrm{char}K=p\neq 0$但是$(p,n)=1$(即$\mathrm{char}K\nmid n$)。对于第一种情形我们有

命题7.8 假设K是特征为$p\neq 0$的域。则F是K的p次循环扩域$\Longleftrightarrow F$是形如$x^p-x-a\in K[x]$的不可约多项式在K上的分裂域。

并且在这种情形下，$F=K(u)$，其中u是x^p-x-a 的任意一根。

证明（$\Longrightarrow$）如果σ是循环群$\mathrm{Aut}_K F$ 的生成元，则由定理7.3(ii) 可知

$$T_K^F(1_K)=[F:K]\cdot 1_K=p1_K=0.$$

从而由定理7.6(i) 便知存在$v\in F$，使得$1_K=v-\sigma(v)$。如果$u=-v$，则$\sigma(u)=u+1_K\neq u$，从而$u\notin K$。由于$[F:K]=p$，因此没有中间域，所以必然$F=K(u)$。注意$\sigma(u^p)=(u+1_K)^p=u^p+1_K^p=u^p+1_K$，从而$\sigma(u^p-u)=(u^p+1_K)-(u+1_K)=u^p-u$。由于$F$在$K$上是伽罗华的并且$\mathrm{Aut}_K F=\langle\sigma\rangle$，所以$a=u^p-u\in K$。因此$u$是 $x^p-x-a\in K[x]$的根，因为u在K 上的次数是$[K(u):K]=[F:K]=p$，因此x^p-x-a是u在K上的不可约多项式。

K的素子域Z_p是由p个不同的元素0，$1=1_K$，$2=1_K+1_K$，$\cdots$，$p-1=1_K+\cdots+1_K$组成的（定理5.1）定理5.6之证明的第一段表明：对于每个$i\in Z_p$，$i^p=i$.由于u是x^p-x-a 的根,从而对于每个$\in Z_p$，$(u+i)^p-(u+i)-a=u^p+i^p-u-i-a=(u^p-u-a)+(i^p-i)=0+0=0$。因此$u+i\in K(u)=F$也是$x^p-x-a$ 的根（对于每个$i\in Z_p$)。从而F包含x^p-x-a的p个不同的根。所以$F=K(u)$ 是x^p-x-a在K上的分裂域。最后，如果$u+i(i\in Z_p\subset K)$ 是x^p-x-a的任一根，显然$K(u+i)=K(u)=F$。

（$\Longleftarrow$）假设F是$x^p-x-a\in K[x]$ 在K上的分裂域．我们不假定x^p-x-a是不可约的，从而我们要证明的内容比定理 的陈述稍微多一些。如果u 是 x^p-x-a 的根，则由上一段表明$K(u)$ 包含x^p-x-a的 p 个不同的根：$u,u+1,\cdots,u+(p-1)\in K(u)$。但是$x^p-x-a$在 F 中至多有p个根并且这些根在K 上生成 F。因此$F=K(u)$,x^p-x-a 的不可约因子是可分的，并且F在K上是伽罗华的(定理3.11和习题3.13)。每个$\tau\in\mathrm{Aut}_K F=\mathrm{Aut}_K K(u)$均由$\tau(u)$ 所

完全决定。由定理2.2推出$\tau(u)=u+i$（对于某个$i\in Z_p\subset K$）。验证$\tau\longmapsto i$定义出群的单同态θ：$\mathrm{Aut}_K F\to Z_p$。从而$\mathrm{Aut}_K F\cong \mathrm{Im}\theta$，它或者是1或者是$Z_p$。如果$\mathrm{Aut}_K F=1$，则由基本定理 2.5 可知$[F:K]=1$，从而$u\in K$而$x^p-x-a$在$K[x]$中分裂。因此若$x^p-x-a$在$K$上不可约，则必然$\mathrm{Aut}_K F\cong Z_p$所以在这个情况下，$F$是$K$的 p 次循环扩张。∎

系7.9 如果K是特征$p\neq 0$域，$x^p-x-a\in K[x]$，则x^p-x-a在$K[x]$中或者不可约，或者分裂。

证明 利用命题 7.8 中的记号。从上面命题证明的最后一段可知只需证明：如果$\mathrm{Aut}_K F\cong \mathrm{Im}\theta=Z_p$，则$x^p-x-a$是不可约的。如果$u$和$v=u+i(i\in Z_p\subset K)$ 是x^p-x-a的根，则存在$\tau\in \mathrm{Aut}_K F$，使得$\tau(u)=v$。从而 τ：$K(u)\cong K(v)$（取 τ使得$\theta(\tau)=i$）。因此u和v是$K[x]$中同一个不可约多项式的根（系1.9）。由于v是任意的，这就表明x^p-x-a是不可约的。∎

命题 7.8 完全描述了第 444 页所提到的第一种类型的循环扩张的结构。为了决定第二种类型的 n 次循环扩张的结构，需要对于基域K加上额外的条件。

设K是域而 n 为正整数。元素$\zeta\in K$叫作 n 次单位根，是指$\zeta^n=1_K$（即ζ是$x^n-1_K\in K[x]$的根）。不难看出，K 中全体 n 次单位根形成K之非零元素乘法群的一个子群。根据定理5.3，这个子群是循环的，并且从定理III.6.7可知它的阶至多是 n。$\zeta\in K$叫作 n 次本原单位根，如果 ζ 是 n 次单位根并且它在 n 次单位根乘法群中的阶为 n。特别地，每个 n 次本原单位根生成由全部 n 次单位根组成的循环群。

注记：如果$\mathrm{Char}K=p$并且 $p\mid n$，则$n=p^h m$，其中 $(p,m)=1$

并且$m<n$。因此$x^n-1_K=(x^m-1_K)^{p^h}$（习题III.1.11）。从而K中的n次单位根与K中的m次单位根是一致的。由于$m<n$，从而K中不存在n次本原单位根。反过来，如果$\mathrm{char}K\nmid n$（特别若$\mathrm{char}K=0$），则$nx^{n-1}\neq 0$，从而x^n-1_K与它的导函数互素。所以x^n-1_K在它的任何一个分裂域F中均有n个不同的根（定理III.6.10）。因此F中的n次单位根群的阶是n，并且F包含n次本原单位根（但是K不必如此）。注意如果K包含n次本原单位根，则K包含x^n-1_K的n个不同的根，从而$K=F$。

例 对于每个$n\geqslant 1$，1_K是域K中的n次单位根。如果$\mathrm{char}K=p\neq 0$并且$n=p^h$，则K中的n次单位根只有1_K。$\mathbf{C}$的子域$\mathbf{Q}(i)$包含4次本原单位根（$\pm i$），但是除了1之外，$\mathbf{Q}(i)$不包含3次单位根（因为另两个3次单位根是$-1/2\pm\sqrt{3}\,i/2$）。对于每个$n>0$，$e^{\frac{2\pi i}{n}}\in\mathbf{C}$是$n$次本原单位根。

为了完成对循环扩张的刻划，我们需要：

引理7.10 设n是正整数，域K包含n次本原单位根。

(i) 如果$d\mid n$，则$\zeta^{n/d}=\eta$是K中d次本原单位根。

(ii) 如果$d\mid n$，u是$x^d-a\in K[x]$的根并且$u\neq 0$，则x^d-a具有d个不同的根u，ηu，η^2u，…，$\eta^{d-1}u$，其中$\eta\in K$是一个d次本原单位根，此外，$K(u)$是x^d-a在K上的分裂域，并且在K上是伽罗华的。

证明 (i) 根据定义，ζ生成一个n阶循环乘法群。如果$d\mid n$，由定理I.3.4知$\eta=\zeta^{n/d}$的阶是d，从而η是d次本原单位根。

(ii) 如果u是x^d-a的根，则η^iu也是这样。元素$\eta^0=1_K$，η，…，η^{d-1}是两两不同的（定理I.3.4）。由于$\eta\in K$，从而$u,\eta u$，…，$\eta^{d-1}u$就是x^d-a在$K(u)$中的根，并且是两两不同的。因此$K(u)$是

x^d-a 在K上的分裂域。x^d-a 的不可约因子都是可分的，因为它的根是两两不同的。由定理3.11和习题3.13 即知 $K(u)$ 在K上是伽罗华的。∎

定理7.11 令n是正整数，域K包含n次本原单位根ζ。则关于K的扩域F的下列一些条件是彼此等价的。

(i) F是d 次循环扩域，其中$d \mid n$。

(ii) F是形如$x^n-a\in K[x]$的多项式在K上的分裂域（在这种情形下$F=K(u)$，其中u是x^n-a的任意一个根）。

(iii) F是形如$x^d-b\in K[x]$的不可约多项式在K上的分裂域，其中$d \mid n$。（在这种情形下，$F=K(v)$，其中v是x^d-b 的任意一个根。）

证明 (ii) $\Longrightarrow$(i)：引理7.10表明$F=K(u)$，并且F在K上是伽罗华的，其中 u 是 x^n-a 的任意一个根。如果 $\sigma\in \mathrm{Aut}_K F=\mathrm{Aut}_K K(u)$ 则σ由$\sigma(u)$ 所完全决定，由定理2.2知$\sigma(u)$ 是 x^n-a 的根，从而由引理 7.10可知有某个 i $(0\leqslant i\leqslant n-1)$ 使得 $\sigma(u)=\zeta^i u$。验证$\sigma\longmapsto\zeta^i$定义出从$\mathrm{Aut}_K F$到K的n次单位根（n 阶）乘法循环群之中的单同态。从而$\mathrm{Aut}_K F$是循环群，其阶 d 是 n 的因子(定理I.3.5和系I.4.6)。于是F是K上的 d 次循环扩张。

(i) $\Longrightarrow$ (iii) 根据假设，$\mathrm{Aut}_K F$是$d=[F:K]$阶循环群，令其生成元为σ。又设$\eta=\zeta^{n/d}\in K$是 d 次本原单位根。由于$N_K^F(\eta)=\eta^{[F:K]}=\eta^d=1_K$，从而由定理7.6 (ii) 推出$\eta=w\sigma(w)^{-1}$，$w\in F$。如果 $v=w^{-1}$，则$\sigma(v)=\eta v$，$\sigma(v^d)=(\eta v)^d=\eta^d v^d=v^d$。由于$F$在$K$上是伽罗华的，因此$v^d\in b$必然属于$K$，从而$v$是 $x^d-b\in K[x]$的根。根据引理7.10，$K(v)\subset F$，而$K(v)$ 是x^d-b在 K 上的分裂域 (x^d-b的不同的根是v，ηv，…，$\eta^{d-1}v$)。此外，对于每个 i

$(0\leqslant i\leqslant d-1)$，$\sigma^i(v)=\eta^i v$。从而$\sigma^i: K(v)\cong K(\eta^i v)$。由系1.9知$v$和$\eta^i v$是$K$上同一不可约多项式的根。从而$x^d-b$在$K[x]$中是不可约的。因此，$[K(v):K]=d=[F:K]$，于是$F=K(v)$。

(iii) $\Longrightarrow$(ii)：如果$v\in F$是$x^d-b\in K[x]$的根，由引理7.10可知$F=K(v)$。现在$(\zeta v)^n=\zeta^n v^n=1_K v^{d(n/d)}=b^{n/d}\in K$，从而$\zeta v$是$x^n-a\in K[x]$的根，其中$a=b^{n/d}$。又根据引理7.10可知$K(\zeta v)$是$x^n-a$在$K$上的分裂域。但是$\zeta\in K$，从而$F=K(v)=K(\zeta v)$。∎

在上述证明中，n次本原单位根显然起着重要的作用。在K不包含n次本原单位根的时候，刻划形如$x^n-a\in K[x]$的多项式的分裂域则要困难得多。在第8节中我们要考虑$a=1_K$的情形。

习　题

1. 如果在定义7.1中将$\overline{K}$改成K的任意一个包含F的正规扩张N，则这时给出的关于迹和范的新定义与原来的定义等价。特别地，新的定义不依赖于N的选取。见习题3.21。
2. 设F是有限域K的有限维扩域。则范N_K^F和迹T_K^F（看作是映射$F\to K$）都是满射。
3. 令$\overline{\mathbf{Q}}$为$\mathbf{Q}$的一个（固定的）代数闭包。$v\in\overline{\mathbf{Q}}$，$v\notin\mathbf{Q}$。令$E$是$\overline{\mathbf{Q}}$的一个子域，并且对于条件“$v\notin E$”是极大的。求证$E$的每个有限维扩张都是循环的。
4. 令K为域，$\overline{K}$是K的代数闭包，$\sigma\in\mathrm{Aut}_K\overline{K}$。又令
$$F=\{u\in\overline{K}\mid\sigma(u)=u\}\ .$$
则F是域，，并且F的每个有限维扩张都是循环的。
5. 如果F是K的p^n（p为素数）次循环扩张，而L是中间域，使得$F=L(u)$，并且L是K的p^{n-1}次循环扩张，则$F=K(u)$。
6. 如果$\mathrm{char}K=p\neq 0$。令$K_1=\{u^p-u\mid u\in K\}$。

(a) K存在p次循环扩张，$\Leftrightarrow$ $K \neq K_p$。

(b) 如果存在K的p次循环扩张，则对于每个$n \geqslant 1$均存在K的p^n次循环扩张。[提示：使用数学归纳法。如果E是K的p^{n-1}次循环扩张，并且$\mathrm{Aut}_K E$是由σ生成的，证明存在u，$v \in E$，使得$T_K^E(v) = 1_K$，并且$\sigma(u) - u = v^p - v$。从而$x^p - x - u \in K[x]$是不可约的。并且若w是它的一个根，则$K(w)$是K的p^n次循环扩张。]

7. 如果n是奇整数，域K包含n次本原单位根并且$\mathrm{char}K \neq 2$，则K也包含$2n$次本原单位根。

8. 如果F是$\mathbf{Q}$的有限维扩张，则F只包含有限多个单位根。

9. 下列域中都包含哪些单位根：$\mathbf{Q}(i)$，$\mathbf{Q}(\sqrt{2})$，$\mathbf{Q}(\sqrt{3})$，$\mathbf{Q}(\sqrt{5})$，$\mathbf{Q}(\sqrt{-2})$，$\mathbf{Q}(\sqrt{-3})$？

10. (a) 设p为素数，并且假定或者(i)$\mathrm{char}K = p$，或者(ii)$\mathrm{char}K \neq p$而K包含p次本原单位根。则$x^p - a \in K[x]$在$K[x]$中或者不可约或者分裂。

(b) 如果$\mathrm{char}K = p \neq 0$，则对于$x^p - a \in K[x]$的每个根$u$，$K(u) \neq K(u^p) \Leftrightarrow [K(u) : K] = p$。

8. 分圆扩张

除了定理8.1之外，本节在今后是不需要的。我们将考查多项式$x^n - 1_K$的分裂域，特别注意$K = \mathbf{Q}$的情形。这些分裂域是Abel扩张，并且它的伽罗华群是熟知的。

$x^n - 1_K \in K[x]$ $(n \geqslant 1)$在K上的分裂域F叫作n阶分圆扩张。如果$\mathrm{char}K = p \neq 0$，而$n = mp^t$其中$(p, m) = 1$，则$x^n - 1_K = (x^m - 1_K)^{p^t}$（习题III.1.11），从而$n$阶分圆扩张和$m$阶分圆扩张是一致的。于

是我们今后通常假定$\mathrm{char}K \nmid n$（即$\mathrm{char}K = 0$或者与n互素）。

n阶分圆扩张的维数与初等数论中的Euler函数φ有关系。这里$\varphi(n)$表示满足$1 \leqslant i \leqslant n$，$(i, n) = 1$的自然数$i$的个数。例如$\varphi(6) = 2$而$\varphi(p) = p - 1$（对于每个素数$p$）。以$\bar{i}$表示$i \in \boldsymbol{Z}$在正则射影$\boldsymbol{Z} \to Z_p$之下的象。不难验证$(i, n) = 1 \Longleftrightarrow \bar{i}$为环$Z_n$中的单位（习题1）。因此$Z_n$中单位组成的乘法群是$\varphi(n)$阶的。关于这个群的结构参见习题4。

定理8.1 令n为正整数，K为域，$\mathrm{char}k \nmid n$，而F是K的n阶分圆扩张。

(i) $F = K(\zeta)$，其中$\zeta \in F$是一个n次本原单位根。

(ii) F是d维Abel扩张，其中$d \mid \varphi(n)$（φ是Euler函数）。如果n是素数，则F事实上为循环扩张。

(iii) $\mathrm{Aut}_K F$同构于Z_n中单位乘法群的一个d阶子群。

注记：让我们回忆一下，Abel扩张是一个伽罗华代数扩张，并且其伽罗华群是Abel群。F在K上的维数可以小于$\varphi(n)$。例如若ζ是$\boldsymbol{C}$中五次本原单位根，则$\boldsymbol{R} \subset \boldsymbol{R}(\zeta) \subset \boldsymbol{C}$，从而$[\boldsymbol{R}(\zeta) : \boldsymbol{R}] = 2 < 4 = \varphi(5)$。如果$K = \boldsymbol{Q}$，则习题7完全决定了群$\mathrm{Aut}_{\boldsymbol{Q}} F$的结构。

证明概要 (i) 引理7.10前面的注记表明F包含n次本原单位根，根据定义，1_K，ζ，…，$\zeta^{n-1} \in K(\zeta)$是$x^n - 1_K$的n个不同的根，从而$F = K(\zeta)$。

(ii) 和(iii)：由于$x^n - 1_K$的不可约因子显然是可分的，从而由定理3.11和习题3.13可知F在K上是伽罗华的。如果$\sigma \in \mathrm{Aut}_K F$，则$\sigma$由$\sigma(\zeta)$所完全决定。从定理2.2可知$\sigma(\zeta) = \zeta^i (1 \leqslant i \leqslant n-1)$。类似地$\sigma^{-1}(\zeta) = \zeta^j$。从而$\zeta = \sigma^{-1}\sigma(\zeta) = \zeta^{ij}$。从定理I.3.4($v$)知

$ij=1(\mathrm{mod}n)$。于是$\bar{i}\in Z_n$是单位（这里$i\longmapsto\bar{i}$是正则射影$\boldsymbol{Z}\to Z_n$）。验证$\sigma\longmapsto\bar{i}$定义出从$\mathrm{Aut}_K F$到环Z_n的单位乘法(Abel)群之中的单同态（根据习题1后者的阶是$\varphi(n)$）。因此$\mathrm{Aut}_K F\cong\mathrm{Im}f$是$d$阶Abel群，其中$d\mid\varphi(n)$。于是由基本定理2.5，$[F:K]=d$。如果$n$为素数，则$Z_n$是域，从而由定理6.3可知$\mathrm{Aut}_K F\cong\mathrm{Im}f$是循环群。∎

设n为正整数，K为域，$\mathrm{char}K\nmid n$，F是K的n阶分圆扩张。K上的n阶分圆多项式指的是首1多项式$g_n(x)=(x-\zeta_1)(x-\zeta_2)\cdots(x-\zeta_r)$，其中$\zeta_1,\cdots\zeta_r$是$F$中全部$n$次本原单位根。

例 $g_1(x)=x-1_K$，$g_2(x)=(x-(-1_K))=x+1_K$。

如果$K=\boldsymbol{Q}$，则$g_3(x)=(x-(-1/2+\sqrt{3}i/2))(x-(-1/2-\sqrt{3}i/2))=x^2+x+1$，$g_4(x)=(x-i)(x+i)=x^2+1$。这些例子使人想到分圆多项式的某些特性。

命题8.2 设n是正整数，K为域，$\mathrm{char}K\nmid n$，$g_n(x)$是K上的n阶分圆多项式。则

(i) $x^n-1_K=\prod_{d\mid n}g_d(x)$。

(ii) $g_n(x)$的系数属于K的素子域P。如果$\mathrm{char}K=0$，而P等同于有理数域$\boldsymbol{Q}$，则这些系数实际上是整数。

(iii) $\deg g_n(x)=\varphi(n)$，其中φ为Euler函数。

证明 (i) 设F是K的n阶分圆扩张，$\zeta\in F$为n次本原单位根。引理7.10（用于F）表明，对于n的每个因子d，循环群$G=\langle\zeta\rangle$（即全体n次单位根所形成的群）包含全部d次单位根。显然（当$d\mid n$时）$\eta\in G$为d次本原单位根$\Longleftrightarrow|\eta|=d$。因此对于$n$的每个因子$d$，$g_d(x)=\prod_{\substack{\eta\in G\\|\eta|=d}}(x-\eta)$，并且$x^n-1_K=\prod_{\eta\in G}(x-\eta)=\prod_{d\mid n}\prod_{|\eta|=d}(x-\eta)$

$= \prod_{d \mid n} g_d(x)$。

(ii) 为证第一论断，我们对于n作数学归纳法．显然$g_1(x) = x - 1_K \in P[x]$．假设对于每个$k < n$，(ii) 均是对的．令$f(x) = \prod_{\substack{d \mid n \\ d < n}} g_d(x)$，由归纳假设可知$f \in P[x]$并且从(i)可知在$F[x]$中$x^n - 1_K = f(x)g_n(x)$．另一方面，$x^n - 1_K \in P[x]$并且$f$是首1的．从而用$P[x]$中的除法算式可知$x^n - 1_K = fh + r$，其中$h, r \in P[x] \subset F[x]$．由商式和余式的唯一性（对于$F[x]$中的除法算式），必然有$r = 0$和$g_n(x) = h \in P[x]$．这就完成了归纳证明．如果$\mathrm{char}K = 0$并且$P = \mathbf{Q}$，则利用$\mathbf{Z}[x]$和$\mathbf{Q}[x]$（分别代替$P[x]$和$F[x]$）中的除法算式，采用类似的归纳推理，即可证得$g_n(x) \in \mathbf{Z}[x]$．

(iii) 显然$\deg g_n$等于n次本原单位根的个数．令ζ是一个n次本原单位根，则其余（本原）单位根都是ζ的方幂．从而$\zeta^i (1 \leqslant i \leqslant n)$是$n$次本原单位根（即是$G$的生成元）$\Longleftrightarrow (i, n) = 1$（定理I.3.6）．但是由定义知这样的$i$恰有$\varphi(n)$个． ∎

注记：定理的第(i)部分给出决定$g_n(x)$的一个递推方法，因为

$$g_n(x) = (x^n - 1_K) / \prod_{\substack{d \mid n \\ d < n}} g_d(x)$$

例如，若p是素数，则$g_p(x) = (x^p - 1_K)/g_1(x) = (x^p - 1_K)/(x - 1_K) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1_K$．对于$K = \mathbf{Q}$，利用定理8.2前面的例子我们有：

$$\begin{aligned} g_6(x) &= (x^6 - 1)/g_1(x)g_2(x)g_3(x) \\ &= (x^6 - 1)/(x - 1)(x + 1)(x^2 + x + 1) \end{aligned}$$

$$= x^2 - x + 1$$

类似地，$g_{12}(x) = (x^{12}-1)/(x-1)(x+1)(x^2+x+1)$

$$(x^2+1)(x^2-x+1)$$

$$= x^4 - x^2 + 1.$$

如果基域为$\mathbb{Q}$，我们有比前面更强一些的结果.

命题8.3 如果F是有理数域$\mathbb{Q}$的n阶分圆扩张，$g_n(x)$是$\mathbb{Q}$上n阶分圆多项式. 则

(i) $g_n(x)$在$\mathbb{Q}[x]$中不可约.

(i) $[F:\mathbb{Q}] = \varphi(n)$，其中$\varphi$为Enler函数.

(iii) $\mathrm{Aut}_Q F$同构于环Z_n的单位乘法群.

证明概要 (i) 由引理III.6.13可知只需证明首1多项式$g_n(x)$在$\mathbb{Z}[x]$中不可约. 令h是g_n在$\mathbb{Z}[x]$中的不可约因子，$\deg h \geqslant 1$. 则$g_n(x) = f(x)h(x)$，其中$f, h \in \mathbb{Z}[x]$必然是首1的. 令ζ是h的根而p为任意素数，满足$(p, n) = 1$.

我们先证ζ^p也是h的根. 由于ζ是$g_n(x)$的根，从而ζ是n次本原单位根. 由命题8.2(iii) 的证明可知ζ^p也是n次本原单位根，从而它或者是f的根或者是h的根. 假设ζ^p不是h的根. 则ζ^p是$f(x) = \sum_{i=0}^{r} a_i x^i$的根. 从而$\zeta$是$f(x^p) = \sum_{i=0}^{r} a_i x^{ip}$的根. 由于$h$在$\mathbb{Q}[x]$中不可约 (引理III.6.13)，而$\zeta$是$h$的根，从而由定理1.6可知$h \mid f(x^p)$. 假设 $f(x^p) = h(x)k(x)$，其中$k \in \mathbb{Q}[x]$. 利用$\mathbb{Z}[x]$中除法算式：$f(x^p) = h(x)k_1(x) + r_1(x)$，其中$k_1, r_1 \in \mathbb{Z}[x]$. 从$\mathbb{Q}[x]$中除法算式的唯一性可知 $k(x) = k_1(x) \in \mathbb{Z}[x]$. 由正则射影 $\mathbb{Z} \to Z_p$ $(b \longmapsto \bar{b})$诱导出环的满同态$\mathbb{Z}[x] \to Z_p[x]$， $g = \sum_{i=0}^{t} b_i x^i \longmapsto$

$\overline{g}=\sum_{i=0}^{t}\overline{b}_i x^i$(习题III.5.1)。从而在$Z_p[x]$中$\overline{f}(x^p)=\overline{h}(x)\overline{k}(x)$。

但是在$Z_p[x]$中$\overline{f}(x^p)=\overline{f}(x)^p$（由于$\mathrm{char}Z_p=p$)。因此

$$\overline{f}(x)^p=\overline{h}(x)\overline{k}(x)\in Z_p[x]$$

所以在$Z_p[x]$中存在着$\overline{h}(x)$的某个正次数的不可约因子，它必然除尽$\overline{f}(x)^p$，从而也除尽$\overline{f}(x)$。另一方面，由于g_n是x^n-1的因子，从而$x^n-1=g_n(x)r(x)=f(x)h(x)r(x)$，其中$r(x)\in\boldsymbol{Z}[x]$。因此在$Z_p[x]$中，

$$x^n-\overline{1}=\overline{x^n-1}=\overline{f}(x)\overline{h}(x)\overline{r}(x)$$

由于$\overline{f}$和$\overline{h}$有公因子，$x^n-\overline{1}\in Z_p[x]$必然有重根。但是因为$(p,\ n)=1$，$x^n-\overline{1}$的全部根是两两不同的。（见引理7.10前面的注记)。这就得出矛盾。因此ζ^p是$h(x)$的根。

如果$r\in\boldsymbol{Z}$，$1\leqslant r\leqslant n$，$(r,\ n)=1$，则$r=p_1^{k_1}\cdots p_t^{k_t}$，其中$k_i>0$，并且每个$p_i$都是与$n$互素的素数。重复应用下述事实：若$\zeta$为$h$的根，则$\zeta^p$也为$h$的根。由此可证$\zeta^r$是$h(x)$的根。但是$\zeta^r(1\leqslant r\leqslant n,\ (r,\ n))$恰好是全部$n$次本原单位根（见命题8.2(iii)的证明)。因此$\prod_{\substack{1\leqslant r\leqslant n\\(r,\ n)=1}}(x-\zeta^r)=g_n(x)\mid h(x)$。从而$g_n(x)=h(x)$。即$g_n(x)$是不可约的。

(ii) 引理7.10表明$F=\boldsymbol{Q}(\zeta)$，从而由命题8.2和(i)即知$[F:\boldsymbol{Q}]=[\boldsymbol{Q}(\zeta):\boldsymbol{Q}]=\deg g_n=\varphi(n)$。

(iii) 它是(ii)，定理8.1和习题1的推论。∎

注记：Kronecker一个极不平凡的定理是说：$\boldsymbol{Q}$的每个Abel扩张均包含在某个分圆扩张之中。〔注〕

〔注〕 这个定理是Kronecker于1877年提出猜想而由Weber于1886年完全证明的。后人称之为Kronecker-Weber定理。

——译者

习　题

1. 如果$i\in\mathbf{Z}$，以$\overline{i}$表示在正则射影$\mathbf{Z}\to Z_n$之下i在Z_n中的象。证明$\overline{i}$是环Z_n中的单位$\Longleftrightarrow(i,\ n)=1$。从而$Z_n$中的单位乘法群是$\varphi(n)$阶群。

2. 证明Euler函数具有下列诸性质：

(a) 如果p是素数，$n>0$，则$\varphi(p^n)=p^n\left(1-\frac{1}{p}\right)=p^{n-1}(p-1)$。

(b) 如果$(m,\ n)=1$，则$\varphi(mn)=\varphi(m)\varphi(n)$。

(c) 如果$n=p_1^{k_1}\cdots p_r^{k_r}$（$p_i$两两不同，$k_i>0$），则$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$。

(d) $\sum\limits_{d\mid n}\varphi(d)=n$。

(e) $\varphi(n)=\sum\limits_{d\mid n}d\cdot\mu(n/d)$，其中$\mu$是如下定义的Möbius函数：

$$\mu(n)=\begin{cases}1, & \text{如果}n=1.\\ (-1)^t, & \text{如果}n\text{是}t\text{个不同素数之积.}\\ 0, & \text{如果存在素数}p,\ \text{使得}p^2\mid n.\end{cases}$$

3. 令φ是Euler函数。则

(a) 当$n>2$时$\varphi(n)$是偶数。

(b) 求满足$\varphi(n)=2$的全部$n>0$。

(c) 求满足$\varphi(n)=n/p$的全部数对$(n,\ p)$，（其中$n,\ p>0$，而p是素数[见习题2]。

4. (a) 如果p为奇素数而$n>0$，则环Z_{p^n}的单位乘法群是$p^{n-1}(p-1)$阶循环群。

(b) 如果$p=2$而$1\leqslant n\leqslant 2$，则(a) 也成立。

(c) 如果$n\geqslant 3$，则Z_{2^n}的单位乘法群同构于$Z_2\oplus Z_{2^{n-2}}$。

5. 对于$f(x)=\sum\limits_{i=0}^{t}a_ix^i$，令$f(x^s)$为多项式$\sum\limits_{i=0}^{t}a_ix^{is}$。求证$\mathbf{Q}$上分圆多项式

$g_n(x)$具有下列性质：

(a) 如果p是素数而$k \geqslant 1$，则$g_{p^k}(x) = g_p(x^{p^{k-1}})$。

(b) 如果 $n = p_1^{r_1} \cdots p_k^{r_k}$ (p_i是不同的素数，$r_i > 0$)，则

$$g_n(x) = g_{p_1 \cdots p_k}(x^{p_1^{r_1-1} \cdots p_k^{r_k-1}})$$

(c) 如果n是奇数，则$g_{2n}(x) = g_n(-x)$。

(d) 如果p是素数而$p \nmid n$，则$g_{pn}(x) = g_n(x^p)/g_n(x)$。

(e) $g_n(x) = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)}$，其中$\mu$是习题2(e)中的Möbius函数。

(f) 如果$n = p^k (k > 0)$，则$g_n(1) = p$；如果$n = 1$，则$g_n(1) = 0$；否则$g_n(1) = 1$。

6. 对于所有$n \leqslant 20$计算$\mathbf{Q}$上的n阶分圆多项式。

7. 设F_n是$\mathbf{Q}$的n阶分圆扩张。对于每个n决定$\mathrm{Aut}_{\mathbf{Q}} F_n$的结构[提示：如果$U_n^*$是$Z_n$中的单位乘法群，则当$n$的素因子分解式是$n = p_1^{n_1} \cdots p_r^{n_r}$的时候，$U_n^* = \prod_{i=1}^{r} U_{p_i^{n_i}}^*$。利用习题4]

8. 令F_n是$\mathbf{Q}$的n阶分圆扩张。

(a) 决定$\mathrm{Aut}_{\mathbf{Q}} F_5$和其全部中间域。

(b) 对于F_8作同样的事情。

(c) 对于F_7作同样的事情。如果ζ是7次本原单位根，$\zeta + \zeta^{-1}$在$\mathbf{Q}$上的极小多项式是什么？

9. 如果$n > 2$，ζ是$\mathbf{Q}$上n次本原单位根。则$[\mathbf{Q}(\zeta + \zeta^{-1}) : \mathbf{Q}] = \varphi(n)/2$。

10. (Wedderburn) 有限体D必为域。下面是一个证明轮廓 (其中E^*表示体E的非零元素组成的乘法群)：

(a) D的中心K是域，D是K上的向量空间，于是$|D| = q^n$，其中$q = |K| \geqslant 2$。

(b) 如果$0 \neq a \in D$，则$N(a) = \{d \in D \mid da = ad\}$是$D$的子体并且包含$K$。此外还有$|N(a)| = q^r$，其中$r \mid n$。

(c) 如果$0\neq a\in D-K$，则$N(a)^*$是a在群D^*中的中心化子，并且$|D^*:N(a)^*|=(q^n-1)/(q^r-1)$，其中$1\leqslant r<n$，$r|n$，

(d) $q^n-1=q-1+\sum_r (q^n-1)/(q^r-1)$，$r$过满足$1\leqslant r<n$，$r|n$的有限个数。[提示：利用$D^*$的类方程。见136页]。

(e) 对于每个n次本原单位根$\zeta\in\mathbf{C}$，我们有$|q-\zeta|>q-1$，其中对于$a+bi\in\mathbf{C}$，$|a+bi|=\sqrt{a^2+b^2}$。从而$|g_n(q)|>q-1$，其中g_n是$\mathbf{Q}$上的n阶分圆多项式。

(f) 如果$n>1$，则(d)中的方程是不可能成立的，于是$K=D$。[提示：利用命题8.2证明：对于n的每个正因子r，$r\neq n$，$f_r(x)=(x^n-1)/(x^r-1)\in\mathbf{Z}[x]$，并且$f_r(x)=g_n(x)h_r(x)$，其中$h_r(x)\in\mathbf{Z}[x]$。于是对每个这样的$r$，在$\mathbf{Z}$中$g_n(q)|f_r(q)$，从而由(d)可知$g_n(q)|(q-1)$。而这与(e)相矛盾。]

9. 根式扩张

在历史上，伽罗华理论起源于方程论中的一个古典问题，这个问题可以直觉地但是又相当确切地叙述如下：给了一个域K，是否存在着一个明显的“公式”(只包含域中运算和开n次方)使得它给出任意方程$f(x)=0$ ($f(x)\in K[x]$)的全部解？如果f的次数$\leqslant 4$，答案是肯定的（例如在$\deg f=2$和$\mathrm{char}K\neq 2$的时候，就是众所周知的“二次方程求解公式”，还见习题5)。但是我们要证明在一般情形下答案是否定的(命题9.8)。为此，我们需要刻划某种类型域的扩张，其伽罗华群是可解群（定理9.4和命题9.6)。

第一个任务是用域论的语言精确叙述上面的古典问题。在整

个讨论过程中，我们都在给定基域K的一个固定的代数闭包中工作。在直觉上，我们说存在着解某个特定方程$f(x)=0$的“公式”，这意味着通过有限步骤给出该方程的全部解，而每一步是域中运算（加减乘除）或者是开n次方。实行域中运算时可以不改变基域，但是在域E中开元素c的n次方时就要涉及到构作扩域$E(u)$，其中$u^n\in E$（即$u=\sqrt[n]{c}$）.从而若存在解$f(x)=0$的公式，则便存在有限的域塔

$$K=E_0\subset E_1\subset\cdots\subset E_n$$

其中E_n包含f在K上的分裂域，并且对于每个$i\geqslant 1$，$E_i=E_{i-1}(u_i)$，其中u_i的某个方幂属于E_{i-1}。

反之，假设存在着这样的域塔，并且E_n包含f的分裂域（即E_n包含$f(x)=0$的全部解），则

$$E_n=K(u_1,\ \cdots,\ u_n)。$$

并且由定理1.3可知每个解均具有形式

$$h(u_1,\ \cdots u_n)/g(u_1,\ \cdots,\ u_n)\ (h,\ g\in K[x_1,\ \cdots,\ x_n])。$$

所以每个解都可以用K中有限个元素，域中有限次运算和u_1，…，u_n表达出来（而u_1，…，u_n是由开方求得的）。但是这就等于说存在着这一特别给出的方程的求解“公式”。这些考虑使我们产生下面两个定义。

定义9.1 域K的扩域F叫作K的根式扩张，是指$F=K(u_1,\ \cdots,\ u_n)$，其中u_1的某个方幂属于K，并且对每个$i\geqslant 2$，u_i的某个方幂属于$K(u_1,\ \cdots,\ u_{i-1})$。

注记：如果$u_i^{m_i}\in K(u_1,\cdots,\ u_{i-1})$，则$u_i$是

$$x^{m_i}-u_i^{m_i}\in K(u_1,\cdots,\ u_{i-1})[x]$$

的根。从而由定理1.12可知$K(u_1,\cdots,\ u_i)$是$K(u_1,\cdots,\ u_{i-1})$的

有限维代数扩张。因此由定理1.2和1.11可知K的每个根式扩张F都是K的有限维代数扩张。

定义9.2 令K是域而$f \in K[x]$。方程$f(x)=0$叫作根式可解的，如果存在K的一个根式扩张F和f在K上的分裂域E，使得$F \supset E \supset K$。

上面提到的古典问题可以叙述成寻求方程$f(x)=0$的求解"公式"，使该公式对具有给定次数r的每一个多项式$f \in K[x]$都是对的(就象$r=2$时的二次方程求解公式那样)。不论这样一个求解"公式"可能会是什么样子，从定义9.1前面的讨论可以清楚地看出，这样一个"公式"的存在应该导致每个r次多项式方程都是根式可解的。

因此，欲证明这样一个公式是不存在的，只需要证明某个特定的多项式方程不是根式可解的即可。现在我们为此进行必要的准备工作(系9.5)，而把该古典问题的精确陈述放在附录中。

引理9.3 如果F是K的根式扩张而N是F在K上的正规闭包(定理3.16)，则N是K的根式扩张。

证明概要 将下述两个事实合在一起，便得到引理的证明。(i) 如果F是K的有限维扩张(不必是根式扩张)，而N是F在K上的正规闭包，则N是合成域$E_1E_2\cdots E_r$，其中每个E_i都是N的子域并且K-同构于F。(ii) 如果每个$E_1,\cdots,E_r$均是K的根式扩张，(这里的情形即是如此，因为F是根式扩张)，则合成域$E_1E_2\cdots E_r$也是K的根式扩张。这两个命题的证明如下：

(i) 令$\{w_1,\cdots,w_n\}$是F在K上的一组基，令f_i是w_i在K上的极小多项式。定理3.16的证明表明N是$\{f_1,\cdots,f_n\}$在K上的分

裂域. 设v是f_j在N中的任一根，由定理1.8可知存在 K- 同构 σ: $K(w_j)\cong K(v)$，使得 $6(w_j)=v$. 根据定理 3.8，σ 可以扩充成N的K-自同构τ.$\tau(F)$显然是N的子域，并且它 K-同构于F，而且包含 $\tau(w_j)=\sigma(w_j)=v$. 用这种方法，对于每个f_j的每个根 v，都可以找到N的一个子域E，使得$v\in E$，并且E与F是K- 同构的. 如果$E_1,\cdots,E_r$是如此得到的全部子域，则$E_1,E_2\cdots E_r$是N的子域，并且包含$f_1,\cdots,f_n$的全部根，从而$E_1E_2\cdots E_r=N$.

(ii) 假设 $r=2$，$E_1=K(u_1,\cdots,u_k)$，$E_2=K(v_1,\cdots,v_m)$ 如定义9.1所示，则$E_1E_2=K(u_1,\cdots,u_k,v_1,\cdots,v_m)$ 显然是K的根式扩张. 对于一般情形也可以类似地证明. ∎

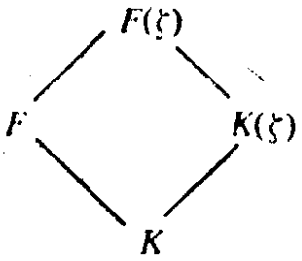
定理9.4 如果F是K的根式扩张，E是中间域，则$\mathrm{Aut}_K E$是可解群.

证明 如果K_0是E对于群$\mathrm{Aut}_K E$的固定域，则E在K_0上是伽罗华的，$\mathrm{Aut}_{K_0}E=\mathrm{Aut}_K E$，而$F$是$K_0$的根式扩张(习题1). 因此从一开始我们就可以假设E是K的伽罗华代数扩张. 令N是F在 K 上的正规闭包(定理3.16). 由引理9.3可知N是K的根式扩张，而由引理2.13可知E是稳定的中间域. 从而限制($\sigma\longmapsto\sigma|E$)诱导出同态$\mathrm{Aut}_K N\longrightarrow\mathrm{Aut}_K E$. 由于$N$是$K$上(从而也是$E$上)的分裂域，从定理3.8可知每个$\sigma\in\mathrm{Aut}_K E$均可扩充成$N$的一个$K$-自同构. 从而$\theta$是满同态. 由于可解群的同态象还是可解群(定理II.7.11)，所以只需证明$\mathrm{Aut}_K N$是可解群即可. 如果K_1是N对于$\mathrm{Aut}_K N$的固定域，则N是K_1的伽罗华根式扩张(习题1)，并且 $\mathrm{Aut}_{K_1}N=\mathrm{Aut}_K N$. 于是我们又可以回到原来的记号，从而不失普遍性假定$F=E$并且 F 是K的伽罗华根式扩张.

现在设$F=K(u_1,\cdots,u_n)$，其中$u_1^{m_1}\in K$，而当$i\geqslant 2$时 $u_i^{m_i}\in$

$K(u_1,\cdots,u_{i-1})$。我们可以假设$\mathrm{char}K\nmid m_i$。因为如果$\mathrm{char}K=0$，则这是显然的。如果$\mathrm{char}K=p\neq 0$并且$m_i=rp^t$，其中$(r,p)=1$，则$u_i^{p^t}\in K(u_1,\cdots,u_{i-1})$，从而$u_i^r$在$K(u_1,\cdots,u_{i-1})$上纯不可分。但是$F$在$K$上是伽罗华的，因此是可分的（定理3.11），从而$F$在$K(u_1,\cdots,u_{i-1})$上也是可分的(习题3.12)。于是由定理6.2可知$u_i^r\in K(u_1,\cdots,u_{i-1})$，因此我们可以假定$m_i=r$。

如果$m=m_1m_2\cdots m_n$，由上一段可知$\mathrm{char}K(=\mathrm{char}F)\nmid m$。考虑$F$的分圆扩张$F(\zeta)$，其中$\zeta$是$m$次本原单位根(定理8.1)。于是我们有如下的情形：



其中$F(\zeta)$在F上是伽罗华的（定理8.1），从而在K上也是伽罗华的(习题3.15(b))。基本定理2.5表明$\mathrm{Aut}_KF\cong\mathrm{Aut}_KF(\zeta)/\mathrm{Aut}_FF(\zeta)$。因此根据定理II.7.11可知只需证明$\mathrm{Aut}_KF(\zeta)$是可解群。注意$K(\zeta)$是$K$的伽罗华Abel扩张（定理8.1），从而由基本定理2.5可知$\mathrm{Aut}_KK(\zeta)\cong\mathrm{Aut}_KF(\zeta)/\mathrm{Aut}_{K(\zeta)}F(\zeta)$。如果我们知道$\mathrm{Aut}_{K(\zeta)}F(\zeta)$是可解的，那末由定理II.7.11就可以得出$\mathrm{Aut}_KF(\zeta)$是可解的(因为$\mathrm{Aut}_KK(\zeta)$是Abel群，当然是可解的)。于是，我们只需要证明$\mathrm{Aut}_{K(\zeta)}F(\zeta)$是可解群。

根据假设，$F(\zeta)$在K上是伽罗华的，从而在任一中间域上也是伽罗华的。令$E_0=K(\zeta)$并且

$$E_i=K(\zeta,u_1,\cdots,u_i)\qquad(1\leqslant i\leqslant n)$$

于是$E_n=K(\zeta,u_1,\cdots,u_n)=F(\zeta)$。令$H_i=\mathrm{Aut}_{E_i}F(\zeta)$是在伽罗华对应下对应的$\mathrm{Aut}_{K(\zeta)}F(\zeta)$的子群。我们有如下的图表：

$$
\begin{array}{ccc}
F(\zeta)=E_n & \longmapsto & H_n=1 \\
\vdots & & \vdots \\
E_i & \longmapsto & H_i=\mathrm{Aut}_{E_i}F(\zeta) \\
\cup & & \\
E_{i-1} & \longmapsto & H_{i-1}=\mathrm{Aut}_{E_{i-1}}F(\zeta) \\
\vdots & & \vdots \\
K(\zeta)=E_0 & \longmapsto & H_0=\mathrm{Aut}_{K(\zeta)}F(\zeta)
\end{array}
$$

根据引理7.10(i)可知对于每个i($1\leqslant i\leqslant n$)，$K(\zeta)$包含 m_i 次本原单位根。由于 $u_i^{m_i}\in E_{i-1}$，$E_i=E_{i-1}(u_i)$，从而由引理 7.10(ii)(取$d=m_i$)和定理7.11(ii)(取$u=m_i$)可知每个E_i都是E_{i-1}的循环扩张。特别地，E_i是 E_{i-1}的伽罗华扩张。由基本定理2.5导出$H_i\lhd H_{i-1}$($1\leqslant i\leqslant n$)并且 $H_{i-1}/H_i\cong\mathrm{Aut}_{E_{i-1}}E_i$，从而$H_{i-1}/H_i$ 是循环扩张。于是

$$1=H_n<H_{n-1}<\cdots<H_0=\mathrm{Aut}_{K(\zeta)}F(\zeta)$$

是可解列(定义II.8.3)。所以由定理II.8.5即知 $\mathrm{Aut}_{K(\zeta)}F(\zeta)$是可解群。∎

系9.5 设K是域而 $f\in K[x]$。如果方程$f(x)=0$是根式可解的，则f的伽罗华群是可解群。

证明从定理9.4和定义9.2直接推出。∎

例 多项式 $f=x^5-4x+2\in\mathbb{Q}[x]$ 的伽罗华群是 S_5(见定理4.12后面的例子)，而S_5不是可解群 (系II.7.12)所以 $x^5-4x+2=0$不是根式可解的，从而对于它没有(只包含域中运算和开方运算的) 求解“公式”。

注意在这里基域起着重要作用。多项式$x^5-4x+2=0$在$\mathbb{Q}$上

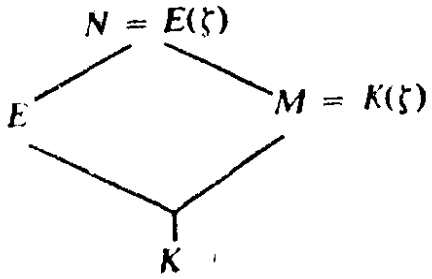
不是根式可解的，但是在实数域$\boldsymbol{R}$上它是根式可解的．事实上，$\boldsymbol{R}$上每个多项式都是根式可解的，因为所有解都在其代数闭包$\boldsymbol{C}=\boldsymbol{R}(i)$中，而$\boldsymbol{C}$是$\boldsymbol{R}$的根式扩张．

在本节的最后我们证明定理9.4一部分内容的逆．当K的特征为零时，这里没有任何困难．但是如果$\mathrm{char}K$大于零时，必须在其上加些限制(或者重新定义“根式扩张”，见习题2)．

命题9.6 设E是K的有限维伽罗华扩域，并且具有可解的伽罗华群$\mathrm{Aut}_K E$．假设$\mathrm{char}K\nmid[E:K]$．则存在K的某个根式扩张F．使得$F\supset E\supset K$．

注记：条件“E在K上伽罗华”是重要的(习题3)．

证明概要 由于$\mathrm{Aut}_K F$是有限可解群，从命题 II.8.6 可知它有素指数p的正规子群H．因为E在K上是伽罗华的，从而$|\mathrm{Aut}_K E|=[E:K]$(定理2.5)，从而$\mathrm{char}K\nmid p$．令$N=E(\zeta)$是E的分圆扩张，其中ζ是p次本原单位根(定理8.1)．令$M=K(\zeta)$．于是我们有



N是E的有限维伽罗华扩张（定理8.1)，从而也是K的有限维伽罗华扩张(练习题3.15(b))．现在M显然是K的根式扩张．从而（由习题4)只需证明存在M的根式扩张包含N即可．

首先注意，E是N和K的稳定中间域（引理 2.13)．从而限制$(\sigma\longmapsto\sigma|E)$诱导出同态$\theta$：$\mathrm{Aut}_M N\longrightarrow\mathrm{Aut}_K E$．如果$\sigma\in\mathrm{Aut}_M N$，则$\sigma(\zeta)=\zeta$．从而若$\sigma\in\mathrm{Ker}\theta$，则$\sigma=1_N$．于是$\theta$为单同态．

现在我们对于 $n=[E:K]$ 归纳证明定理。$n=1$的情形是显然的。假设定理对于维数$k<n$的所有扩张都成立，然后考虑两种可能性：

(i) 在θ之下$\mathrm{Aut}_M N$同构于$\mathrm{Aut}_K E$的一个真子群。

(ii) θ：$\mathrm{Aut}_M N \cong \mathrm{Aut}_K E$。

无论在哪种情形下，$\mathrm{Aut}_M N$都是可解的(定理 II.7.11)，而N是K的有限维伽罗华扩张。从而也是M的有限维伽罗华扩张。对于情形(i)，$[N:M]=|\mathrm{Aut}_M N|<|\mathrm{Aut}_K E|=[E:K]=n$，从而由归纳假设，可知存在$M$的一个根式扩张包含 N。正如本证明第一段所提到的，这就对于情形(i)证明了定理。

对于情形(ii)，令$J=\theta^{-1}(H)$。由于H是$\mathrm{Aut}_K E$的正规子群并且指数为p，从而J是$\mathrm{Aut}_M N$的正规子群并且指数为p。此外，由定理II.7.11可知J是可解的。如果P是J(对于$\mathrm{Aut}_M N$) 的固定域，我们有

$$\begin{array}{ccc} N & \longleftrightarrow & 1 \\ \cup & & \triangle \\ P & \longleftrightarrow & J=\mathrm{Aut}_P N \\ \cup & & \triangle \\ M & \longleftrightarrow & \mathrm{Aut}_M N \end{array}$$

基本定理2.5导致P在M上是伽罗华的，并且 $\mathrm{Aut}_M P \cong \mathrm{Aut}_M N/J$。但是由构作方式可知$[\mathrm{Aut}_M N:J]=p$。从而$\mathrm{Aut}_M P \cong Z_p$。因此$P$是$M$的循环扩张，并且 $P=M(u)$，其中u是某个（不可约）多项式$x^p-a\in M[x]$的根(定理7.11)。从而P是M的根式扩张并且$[N:P]<[N:M]=[F:K]=n$。由于$\mathrm{Aut}_P N=J$是可解的，而N在P上是伽罗华的(定理2.5)，由归纳假设可知存在P的某个根式扩张F包括

N。F显然是M的根式扩张(习题4)。这就完成了对于情形(ii)的证明。∎

系9.7 设K是域，$f\in K[x]$是$n(>0)$次多项式，$\mathrm{char}K\nmid n!$(当$\mathrm{char}K=0$时这永远成立)。则方程$f(x)=0$根式可解$\Longleftrightarrow f$的伽罗华群是可解的。

证明概要 ($\Longleftarrow$)令E是f在K上的分裂域。从命题9.6可知只需证明E在K上是伽罗华的并且$\mathrm{char}K\nmid[E:K]$即可。由于$\mathrm{char}K\nmid n!$，从定理III.6.10和习题III.6.3可知f的不可约因子是可分的，从而E在K上是伽罗华的(定理3.11和习题3.13)。由于每个素数若整除$[E:K]$必然整除$n!$(定理3.2)，从而$\mathrm{char}K\nmid[E:K]$。∎

附录：n次一般方程

为了看出我们的研究思想，最好考察一下在特征不为2的域上的二次多项式方程。不失普遍性，今后只考虑首1多项式。如果t_1和t_2是未定元，则在有理函数域$K(t_1,\ t_2)$上的方程

$$x^2-t_1x+t_2=0$$

叫做K上的二次一般方程。而K上的每个(首1)二次方程均可以由二次一般方程得到，这只需将t_1和t_2改成K中适当的元素即可，不难看出，2次一般方程(在$K(t_1,\ t_2)$的某个代数闭包中)的解可以写成

$$x=\frac{t_1\pm\sqrt{t_1^2-4t_2}}{2}$$

其中对于$n\in\mathbb{Z}$，$n=n1_K$。这就是熟知的二次方程求解公式.这表明二次一般方程的解属于根式扩域$K(t_1, t_2)(u)$，其中 $u^2=t_1^2-4t_2$。为了求出方程$x^2-bx+c=0(b, c\in K)$ 的解，只需将b,c分别代到t_1，t_2 中即可。这些解显然在根式扩张 $K(u)$中，其中$u^2=b^2-4c\in K$。现在我们将这个思想推广到任意次数的多项式方程上。

设K是域而n是正整数。考虑K上的有理函数域$K(t_1,\cdots,t_n)$，其中t_1，…，t_n是未定元。多项式

$$p_n(x)=x^n-t_1x^{n-1}+t_2x^{n-2}+\cdots+(-1)^{n-1}t_{n-1}x+(-1)^nt_n\in K(t_1,\cdots t_n)[x]$$

叫作K上的n次一般多项式，而方程 $p_n(x)=0$叫作K上的n次一般方程[3]。注意$K[x]$中的每个n次(首1)多项式 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$，都可以从一般多项式$p_n(x)$通过代换$t_i=(-1)^ia_i$而得到。

从上述讨论可以看出下面的定义是相当自然的。我们说对于n次一般方程存在着求解“公式”，是指这个方程在域$K(t_1,\cdots,t_n)$上是根式可解的。如果$p_n(x)$是根式可解的，则K上的每个n次(首1)多项式方程的解都可以在$p_n(x)=0$的解中采用适当的代换而得到。有了这种精确的陈述形式，现在我们可以解决本节一开始所介绍的那个古典问题。

命题9.8 (Abel) 设K是域，n为正整数。则仅当$n\leqslant 4$时 n次一般方程才是根式可解的。

注记：如果 charK = 0，则命题9.8中的“仅当”可以改成“当

3.为了简化某些计算工作，我们加进符号$(-1)^i$。

且仅当”。如果根式扩张定义成习题2的那个样子，则对于任何charK，都可以将“仅当”改成“当且仅当”。另一方面，当$n\geqslant 5$时n次一般方程根式不可解这一事实，并不排除域K上某些特殊的$n\geqslant 5$次多项式方程根式可解的可能性。

证明概要 假定记号同前。令$u_1,\cdots,u_n$是$p_n(x)$在某个分裂域$F=K(t_1,\cdots,t_n)(u_1,\cdots,u_n)$中的根。由于在$F$中$p_n(x)=(x-u_1)(x-u_2)\cdots(x-u_n)$，通过直接计算可知

$$t_1=\sum_{i=1}^{n}u_i,\quad t_2=\sum_{1\leqslant i<j\leqslant n}u_iu_j,\quad\cdots,\quad t_n=u_1u_2\cdots u_n.$$

即$t_i=f_i(u_1,\cdots,u_n)$，其中$f_1,\cdots,f_n$是n个未定元的初等对称函数(见第2节的附录)。于是$F=K(u_1,\cdots,u_n)$。现在考虑一组新的未定元$\{x_1,\cdots,x_n\}$和域$K(x_1,\cdots,x_n)$。令E是$K(x_1,\cdots,x_n)$中全部对称有理函数所构成的子域。证明的基本思想是构作一个域同构$F\cong K(x_1,\cdots,x_n)$，使得$K(t_1,\cdots t_n)$映到E之上。于是$p_n(x)$的伽罗华群$\mathrm{Aut}_{K(t_1,\cdots,t_n)}F$便同构于$\mathrm{Aut}_EK(x_1,\cdots,x_n)$。但是后者同构于$S_n$(第381页)。而$S_n$是可解群$\Longleftrightarrow n\leqslant 4$(系II.7.(2)和习题II.7.10)。从而由系9.5可知，如果$p_n(x)$是根式可解的，那末$n\leqslant 4$。[反之，如果$n\leqslant 4$并且$\mathrm{char}K=0$，由系9.7可知$p_n(x)$也是根式可解的。]

为了构作同构$F\cong K(x_1,\cdots,x_n)$，我们首先注意，从定理2.18知道$K(x_1,\cdots,x_n)$的子域E恰好是$K(f_1,\cdots,f_n)$，其中$f_1,\cdots,f_n$是初等对称函数。其次，我们按如下方法建立环同构$K[t_1,\cdots,t_n]\cong K[f_1,\cdots,f_n]$：根据定理III.5.5知道，$g(t_1,\cdots,t_n)\longmapsto g(f_1,\cdots,f_n)$(特别地有$t_i\longmapsto f_i$)定义了环的满同态$\theta:K[t_1,\cdots,t_n]\longrightarrow K[f_1,\cdots,f_n]$。假如$g(t_1,\cdots,t_n)\longmapsto 0$，则在$K[f_1,\cdots,f_n]\subset K(x_1,\cdots,x_n)$中$g(f_1,\cdots,f_n)=0$。根据定义

$$f_k = f_k(x_1, \cdots, x_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

从而$0 = g(f_1, \cdots, f_n) = g(f_1(x_1, \cdots, x_n), \cdots, f_n(x_1, \cdots, x_n))$. 由于$g(f_1, \cdots, f_n)$是域$K$上关于未定元$x_1, \cdots, x_n$的多项式，而$F = K(u_1, \cdots, u_n)$是包含$K$的一个域，作代换$x_i = u_i$即得出

$$\begin{aligned} 0 &= g(f_1(u_1, \cdots, u_n), \cdots, f_n(u_1, \cdots, u_n)) \\ &= g(t_1, \cdots, t_n). \end{aligned}$$

因此θ也是单同态，从而θ是同构. 进一步，θ可以扩充成商域的同构$\theta: K(t_1, \cdots, t_n) \cong K(f_1, \cdots, f_n) = E$(习题 III.4.7). 现在$F = K(u_1, \cdots, u_n)$是$p_n(x)$在$K(t_1, \cdots, t_n)$上的分裂域，并且由$\theta$所诱导的多项式之间的自然映射，$p_n(x) \longmapsto \overline{p_n}(x) = x^n - f_1 x^{n-1} + f_2 x^{n-2} + \cdots + (-1)^n f_n = (x - x_1) \cdots (x - x_n)$(见381页). 而$K(x_1, \cdots, x_n)$显然是$\overline{p_n}(x)$在$K(f_1, \cdots, f_n) = E$之上的分裂域. 由定理3.8知道同构$\theta$可以扩充成同构$F \cong K(x_1, \cdots, x_n)$，并由同构的构作方式知道它将$K(t_1, \cdots, t_n)$映到$E$上，而这正是我们所希望的.∎

习　题

1. 如果F是K的根式扩张而E是中间域，则F也是E的根式扩张.
2. 假设"根式扩张"按以下的方式定义：F是K的根式扩张，是指存在有限的域塔$K = E_0 \subset E_1 \subset \cdots \subset E_n = F$，使得对每个$1 \leqslant i \leqslant n$. $E_i = E_{i-1}(u_i)$，并且下面两个条件有一个是正确的：(i) $u_i^{m_i} \in E_{i-1}$(对于某个$m_i > 0$)；(ii) $\mathrm{char} K = p$并且$u_i^p - u_i \in E_{i-1}$. 叙述并证明与定理9.4，命题9.6，系9.7和命题9.8相类似的结果.
3. 设K是域，$f \in K[x]$是$n \geqslant 5$次不可约多项式，F是f在K上的分裂域. 假设$\mathrm{Aut}_K F \cong S_n$(见定理4.12下面的例子). 令$u$是$f$在$F$中的一个根，则
   (a) $K(u)$在K上不是伽罗华的，$[K(u): K] = n$，并且$\mathrm{Aut}_K K(u) = 1$

(从而是可解群).

(*b*) K上的正规闭包如果包含u，则也包含同构于F的一个子域.

(*c*) 不存在K的根式扩张E，使得$E\supset K(u)\supset K$.

4. 如果F是E的根式扩张，E是K的根式扩张，则F是K的根式扩张.

5. (Cardan)令K是域并且$\mathrm{char}K\neq 2$，3. 考虑三次方程 $x^3+a_1x^2+a_2x+a_3=0(a_i\in K)$.令

$$p=a_2-\frac{a_1^2}{3},\quad q=\frac{2a_1^3}{27}-\frac{a_1a_2}{3}+a_3,\quad P=\sqrt[3]{-q/2+\sqrt{p^3/27+q^2/4}},$$

$Q=\sqrt[3]{-q/2-\sqrt{p^3/27+q^2/4}}$ (适当选取立方根)，则上面所给出的方程的解是$P+Q-\frac{a_1}{3}$，$\omega P+\omega^2Q-\frac{a_1}{3}$，$\omega^2P+\omega Q-\frac{a_1}{3}$，其中$\omega$是一个3次本原单位根.

第VI章　域的结构

在这一章里，我们要分析一个给定域的任意扩域．由于在第V章中已经对于代数扩张作了比较详细的研究，所以这里着重于超越扩张．作为分析过程的第一步，我们要证明：每个域扩张$K\subset F$事实上均是两步的扩张$K\subset E\subset F$，其中F是E的代数扩张而E是K的纯超越扩张(第1节)．这里所使用的基本概念是超越基，它的势(叫作是超越次数)是扩张F/K的不变量(第1节)．在第2节我们将可分性推广到(可能)非代数的扩张中，并且用多种方式来刻划可分扩张．

1．超　越　基

这一节的第一部分是介绍代数无关概念，它是线性无关思想的推广．域F在子域K上的超越基是F在K上的向量空间基的模拟(即将线性无关改成代数无关)．我们要证明F在K上的超越基的势(即超越次数)是不变量，并且要研究它的性质．在本节中我们经常使用记号u/v来表示uv^{-1}，其中u、v均为某域中的元素并且$v\neq 0$．在本节中K永远表示域．

定义1.1 假设F是K的扩域，S是F的子集合。我们称S是在K上代数相关的，是指对于某个正整数n存在一个非零多项式$f\in K[x_1,\cdots,x_n]$，使得对S中n个不同元素$s_1,\cdots,s_n$满足$f(s_1,\cdots,s_n)=0$。如果S在K上不是代数相关的，我们便称S在K上是代数无关的。

注记：当课文很明确的时候，我们常常略去"在K上"一词。F的一个子集合S在K上是代数无关的，如果对于每个$n>0$，每个$f\in K[x_1,\cdots,x_n]$和每n个不同元素$s_1,\cdots,s_n\in S$，均有

$$f(s_1,\cdots,s_n)=0 \quad\Longrightarrow\quad f=0.$$

代数无关集合的每个子集合也是代数无关的。特别地，空集合是代数无关集合。K的每个非空子集合显然是代数相关的。一元集合$\{u\}$在K上代数相关的充要条件是u为K上的代数元素。代数无关集合中的每个元素显然都是K上的超越元素。因此，如果F为K的代数扩张，则只有空集合是F的代数无关子集。

代数相关和代数无关概念可以看成是线性相关和线性无关概念的推广。这是因为，集合S在K上是线性相关的，指的是存在某个正整数n和一次多项式$f\in K[x_1,\cdots,x_n]$，使得对S中n个不同元素$s_1,\cdots,s_n$，满足$f(s_1,\cdots,s_n)=0$。从而每个代数无关集合也是线性无关的，但反过来则不一定正确(见定义1.4后面的例子)。

例 设K是域。在有理函数域$K(x_1,\cdots,x_n)$中，未定元集合$\{x_1,\cdots,x_n\}$在K上是代数无关的。更一般地我们有：

定理1.2 假设F是K的扩域，F的子集合$\{s_1,\cdots,s_n\}$在K上代数无关，则存在K-同构$K(s_1,\cdots,s_n)\cong K(x_1,\cdots,x_n)$。

证明概要 由定理III.5.5和V.1.3可知映射θ：$K[x_1,\cdots,x_n]$

$\longrightarrow K[s_1,\cdots,s_n], x_i \longmapsto s_i$定义出环的$K$-满同态。从$\{s_1,\cdots,s_n\}$的代数无关性可推得$\theta$是单同态。根据系III.4.6可知$\theta$可以扩充成域的$K$-单同态$K(x_1,\cdots,x_n)\longrightarrow K(s_1,\cdots,s_n)$ （仍表示成θ），使得$\theta(f/g)=f(s_1\cdots,s_n)/g(s_1,\cdots,s_n)=f(s_1,\cdots,s_n)g(s_1,\cdots,s_n)^{-1}$。再由定理V.1.3(V)即知$\theta$是满同态。∎

系1.3 对于$i=1,2$，令F_i是K_i的扩域，$S_i\subset F_i$，并且S_i在K_i上是代数无关的。如果$\varphi: S_1\longrightarrow S_2$是集合的单射而$\sigma: K_1\longrightarrow K_2$是域的单同态，则$\sigma$可以扩充成域的单同态$\bar{\sigma}: K_1(S_1)\longrightarrow K_2(S_2)$，使得对每个$s\in S_1$，$\bar{\sigma}(s)=\varphi(s)$。此外，如果$\varphi$是一一对应而$\sigma$是同构，则$\bar{\sigma}$也是同构。

注记：特别地，从此系可以推出，域K上代数无关集合S的每个置换均可以扩充成$K(S)$的K-自同构。（只要取$K_1=K=K_2$，$\sigma=1_K$即可）。

系1.3的证明概要 对于每个$n\geqslant 1$，σ诱导出环的单同态$K_1[x_1,\cdots,x_n]\to K_2[x_1,\cdots,x_n]$（仍表示成$\sigma$）。由定理V.1.3可知，$K_1(S_1)$中每个元素均可表示成$f(s_1,\cdots,s_n)/g(s_1,\cdots,s_n)$ $(s_i\in S_1)$。为方便起见，我们将$\varphi(s)$记为φs，并且定义

$$\bar{\sigma}: K_1(S_1)\to K_2(S_2)$$

$$f(s_1,\cdots,s_n)/g(s_1,\cdots,s_n)\longmapsto \sigma f(\varphi s_1,\cdots,\varphi s_n)/\sigma g(\varphi s_1,\cdots,\varphi s_n)\in K_2(S_2).$$

对于S_1的每个有限子集合$\{s_1,\cdots,s_r\}$，$\bar{\sigma}$在$K_1(s_1,\cdots,s_r)$上的限制是合成映射

$$K_1(s_1,\cdots,s_r)\xrightarrow{\theta_1^{-1}}K_1(x_1,\cdots,x_r)\xrightarrow{\sigma}K_2(x_1,\cdots,x_r)\xrightarrow{\theta_2}K_2(\varphi s_1,\cdots,\varphi s_r),$$

其中θ_i是定理1.2中的K_i-同构，而σ是由$\sigma: K_1[x_1,\cdots,x_r]\longrightarrow$

$K_2[x_1,\cdots,x_r]$诱导出来的（唯一的）商域单同态，即$\hat{\sigma}(f/g)=(\sigma f)/(\sigma g)$(系III.4.6)。从而$\bar{\sigma}$定义出域的单同态。由$\bar{\sigma}$的构作方式可知$\bar{\sigma}$是$\sigma$的扩充，并且在$S_1$上与$\varphi$一致。如果$\sigma$是同构，则每个$\hat{\sigma}$从而每个$\theta_2\hat{\sigma}\theta_1^{-1}$均是同构。如果$\varphi$又是一一对应，则$\bar{\sigma}$必然是同构。∎

定义1.4 设F是K的扩域。F的子集合S叫作F在K上的一组超越基，是指S在K上代数无关，并且S在F的所有代数无关子集合中(对于集合论的包含关系)是极大的。

由Zorn引理不难推出超越基永远是存在的(习题2)。如果我们想到代数无关和线性无关的类似之处，那末超越基即是向量空间基的模拟（因为由引理IV.2.3可知向量空间基恰好是极大线性无关子集合).但是要注意,超越基不是向量空间基,虽然超越基是线性无关集合从而包含在某一组向量空间基之中(定理 IV.2.4)。

例 如果$f/g=f(x)/g(x)\in K(x)$，$f,g\neq 0$，则对于非零多项式$h(y_1,y_2)=g(y_1)y_2-f(y_1)\in K[y_1,y_2]$，我们有$h(x,f/g)=g(x)[f(x)/g(x)]-f(x)=0$。从而$\{x,f(x)/g(x)\}$在$K(x)$中是代数相关的。这就表明$\{x\}$是$K(x)$在$K$上的超越基。集合$\{x\}$不是向量空间基，因为$\{1_K,x,x^2,x^3,\cdots\}$在$K(x)$中是线性无关的。

为了得到刻划超越基的更有用的方式，我们需要

定理1.5 设F是K的扩域，S为F的子集合并且S在K上是代数无关的，而$u\in F-K(S)$。则$S\cup\{u\}$在K上是代数无关的$\Longleftrightarrow u$在$K(S)$上是超越的。

证明 ($\Leftarrow$) 如果存在两两相异的元素$s_1,\cdots,s_{n-1}\in S$和$f\in K[x_1,\cdots,x_n]$使得$f(s_1,\cdots,s_{n-1},u)=0$，则$u$是$f(s_1,\cdots,s_{n-1},x_n)\in$

$K(S)[x_n]$的根. 现在$f\in K[x_1,\cdots,x_n]=K[x_1,\cdots,x_{n-1}][x_n]$, 从而$f=h_rx_n^r+h_{r-1}x_n^{r-1}+\cdots+h_1x_n+h_0$, $h_i\in K[x_1,\cdots,x_{n-1}]$. 由于$u$在$K(S)$上是超越的, 从而$f(s_1,\cdots,s_{n-1},x_n)=0$. 于是对于每个$i$, $h_i(s_1,\cdots,s_{n-1})=0$. 由$S$的代数无关性可知对每个$i$, $h_i=0$, 从而$f=0$. 因此$S\cup\{u\}$是代数无关的.

($\Rightarrow$) 假设$f(u)=0$, 其中$f=\sum_{i=0}^{n}a_ix^i\in K(S)[x]$. 根据定理V.1.3可知存在$S$的有限子集合$\{s_1,\cdots,s_r\}$, 使得对于每个$i$, $a_i\in K(s_1,\cdots,s_r)$, 从而$a_i=f_i(s_1,\cdots,s_r)/g_i(s_1,\cdots,s_r)$, 其中$f_i$, $g_i\in K[x_1,\cdots,x_r]$. 令$g=g_1g_2\cdots g_n\in K[x_1,\cdots,x_n]$, 并且对每个$i$令$\bar{f}_i=f_ig_1\cdots g_{i-1}g_{i+1}\cdots g_n\in K[x_1,\cdots,x_r]$. 则$a_i=\bar{f}_i(s_1,\cdots,s_r)/g(s_1,\cdots,s_r)$并且

$$f(x)=\sum a_ix^i=\sum\frac{\bar{f}_i(s_1,\cdots,s_r)x^i}{g(s_1,\cdots,s_r)}$$

$$=g(s_1,\cdots,s_r)^{-1}[\sum\bar{f}_i(s_1,\cdots,s_r)x^i].$$

(上面所作的事情, 不过是提出f的诸系数的"公分母"). 令$h(x_1,\cdots,x_r,x)=\sum\bar{f}_i(x_1,\cdots,x_r)x^i\in K[x_1,\cdots,x_r,x]$. 由于$f(u)=0$而$g(s_1,\cdots,s_r)^{-1}\neq0$, 从而必然$h(s_1,\cdots,s_r,u)=0$. 由$S\cup\{u\}$的代数无关性推出$h=0$, 从而对每个$i$均有$\bar{f}_i=0$. 于是每个$a_i=0$, 即$f=0$. 从而$u$在$K(S)$上是超越的. ∎

系1.6 设F为K的扩域. F的子集合S在K上是代数无关的. 则S是F在K上的超越基$\Longleftrightarrow$$F$是$K(S)$的代数扩张.

证明作为练习. ∎

注记: 域F叫作域K的纯超越扩张, 是指$F=K(S)$, 其中$S\subset F$

并且S是K上的代数无关集合。 在这种情形下， 由系1.6可知S必然是F在 K 上的超越基. 如果 F/K 是任意域扩张，令S是 F在K上的一组超越基，令 $E=K(S)$. 则系1.6表明F是E的代数扩张而 E是K的纯超越扩张。 最后， 由系1.6和定义1.1后面的注记可知：F是K的代数扩张$\Longleftrightarrow$空集合是F在K上的超越基. 在这种情形下，空集合显然是F在K上唯一的超越基.

系1.7 如果F是K的扩域，$X\subset F$，并且F是$K(X)$的代数扩张(特别地，如果$F=K(X)$)，则X包含有F在K上的一组超越基.

证明 设 S 是 X 的一个极大代数无关子集合 (S 的存在性由Zorn引理所保证)。 由定理1.5可知每个元素 $u\in X-S$在$K(S)$上均是代数的， 从而由定理V.1.12可知$K(X)$是$K(S)$的代数扩张。于是由定理V.1.13可知F是$K(S)$的代数扩张. 因此由系1.6即知S是F在K上的超越基。 ∎

从与线性无关和向量空间基的类比中人们会猜想到，任意两组超越基有相同的势. 与向量空间的情形一样，我们将证明分成两部分.

定理1.8 设F是K的扩域。 如果S是F在K上一组有限的超越基，则F在K上的每组超越基均与S具有相同的势.

证明概要 设$S=\{s_1,\cdots,s_n\}$. 并且令T是任意一组超越基。我们断言：存在某个$t_1\in T$在$K(s_2,\cdots,s_n)$上是超越的. 因为不然的话，则T中每个元素在$K(s_2,\cdots,s_n)$上均是代数的，由定理V.1.12推出$K(s_2,\cdots,s_n)(T)$是$K(s_2,\cdots,s_n)$的代数扩张。 根据系1.6，F在$K(T)$上是代数的,从而F必然也是$K(T)(s_2,\cdots,s_n)=K(s_2,\cdots,s_n)(T)$的代数扩张。 于是由定理V.1.13可知$F$是$K(s_2,\cdots,s_n)$的代

数扩张，而这就导致矛盾（定理1.5）。从而存在某个 $t_1 \in T$， 在 $K(s_2,\cdots,s_n)$上是超越的。于是由定理1.5可知$\{t_1,s_2,\cdots,s_n\}$ 是代数无关的。

现在如果 s_1在$K(t_1,s_2,\cdots s_n)$上是超越的， 则由定理1.5可知 $\{t_1,s_1,s_2,\cdots s_n\}$就会是代数无关的。这显然是不可能的，因为$S$是超越基。因 此$s_1$在$K(t_1,s_2,\cdots,s_n)$上是代数的。 于是$K(S)(t_1)=K(t_1,s_2,\cdots,s_n)(s_1)$是$K(t_1,s_2,\cdots,s_n)$的代数扩张（定理V.1.12），从而$F$是$K(t_1,s_2,\cdots,s_n)$的代数扩张(定理V.1.13和系1.6)。于是由系1.6便知$\{t_1,s_2,\cdots,s_n)$是F在K上的一组超越基。

类似地可以推出，存在某个$t_2 \in T$在$K(t_1,s_3,\cdots,s_n)$上是超越的，从而$\{t_2,t_1,s_3,\cdots,s_n\}$也是一组超越基。归纳下去(每次都插进一个$t_i$而删去一个 s_i)我们就得到$t_1,\cdots,t_n \in T$， 使得 $\{t_1,\cdots,t_n\}$是F在K上的一组超越基。显然必定$T=\{t_1,\cdots,t_n\}$，从而$|S|=|T|$。 ∎

定理1.9 设F是K的扩域。 如果S是F在K上的一组无限的超越基，则F在K上的每组超越基均与S有同样的势。

证明 如果T是另一组超越基，由定理1.8可知T是无限集合。如果$s \in S$， 由系1.6可知 s在$K(T)$上是代数的。s 在$K(T)$上的不可约多项式f的系数均属于$K(T_s)$， 其中T_s是 T的某个有限子 集 合（定理V.1.3）。于是 $f \in K(T_s)[x]$， 而s在$K(T_s)$上是代数的。 对每个$s \in S$均取T的这样一个有限子集合T_s。

我们要证明$\bigcup_{s\in S} T_s$是F在K上的一组超越基。因为$\bigcup_S T_s \subset T$， 我们由此来证明$\bigcup_S T_s = T$。 由于$\bigcup_S T_s$是T的子集合， 从而它是代数无关的。进而， S中每个元素在$K(\bigcup_S T_s)$ 上都是代数的。 从而由

定理V.1.12可知$K(\bigcup_S T_s)(S)$在$K(\bigcup_S T_s)$上也是代数的。由于$K(S)\subset K(\bigcup_S T_s)(S)$，$K(S)$中每个元素在$K(\bigcup_S T_s)$上也是代数的。根据系1.6，$F$是$K(S)$的代数扩张，从而也是$K(\bigcup_S T_s)$的代数扩张(见定理V.1.13)。因此再由系1.6可知$\bigcup_S T_s$是超越基，于是$\bigcup_S T_s = T$。

最后我们再证明$|T|\leqslant|S|$。集合T_s不一定是彼此非交的，我们采用下述方式来补救这一点。将集合S赋以良序(引论的第7节)。用1表示S中第一个元素。令$T_1' = T_1$，然后对于每个$1<s\in S$，定义$T_s' = T_s - \bigcup_{i<s} T_i$。显然每个$T_s'$均是有限集合。验证$\bigcup_S T_s = \bigcup_S T_s'$并且$T_s'$是彼此非交的。对于每个$s\in S$，选取$T_s'$中元素的一个固定的次序：$t_1, t_2, \cdots, t_{k_s}$。于是我们有单射$T_s' \longrightarrow S\times \boldsymbol{N}^*$，$t_i \longmapsto (s,i)$。由定义8.3，8.4和引论中的定理8.11，便知

$$|T| = |\bigcup_S T_s| = |\bigcup_S T_s'| \leqslant |S\times \boldsymbol{N}^*| = |S|\,|\boldsymbol{N}^*| = S\aleph_0 = |S|.$$

在上述推理过程中交换S和T的作用，即可证明$|S|\leqslant|T|$，从而由引论中的Schroeder—Bernstein定理8.6即知$|S| = |T|$。 ∎

定义1.10 设F是K的扩域。则对于F在K上的任意一组超越基S，势$|S|$叫作F在K上的超越次数(表示成$tr.d.F/K$)。

由上述两个定理可知$tr.d.F/K$与S的选取无关。在代数无关与线性无关的类比中，$tr.d.F/K$相当于向量空间维数$[F:K]$。定义1.4后面的注记和例子表明$tr.d.F/K\leqslant[F:K]$，并且$tr.d.F/K = 0 \Longleftrightarrow F$是$K$的代数扩张。

定理1.11 如果F是E的扩域而E是K的扩域，则

$$tr.d.F/K = (tr.d.F/E) + (tr.d.E/K).$$

证明 设S是E在K上的超越基而T是F在E上的超越基。由于

$S\subset E$,从而S在E上是代数相关的，因此$S\cap T=\varnothing$，只需证明$S\cup T$是F在K上的超越基就可以了，因为在这种情形下从定义1.10和引论中的定义8.3可以推得

$$tr.d.F/K=|S\cup T|=|T|+|S|=(tr.d.F/E)+(tr.d.E/K)$$

首先，E中每个元素在$K(S)$上均是代数的(系1.6)，从而在$K(S\cup T)$上也是代数的。于是由定理V.1.12可知$K(S\cup T)(E)$在$K(S\cup T)$上也是代数的。由于

$$K(S\cup T)=K(S)(T)\subset E(T)\subset K(S\cup T)(E),$$

从而$E(T)$是$K(S\cup T)$的代数扩张。但是F在$E(T)$上是代数的（系1.6)，从而由定理V.1.13可知F在$K(S\cup T)$上也是代数的。于是由系1.6可知只需再证$S\cup T$在K上代数无关就可以了。

令f是K上$n+m$个变量的多项式(为方便起见，这$n+m$个变量记为$x_1,\cdots,x_n,y_1,\cdots,y_m$)，使得对某一组两两相异的元素$s_1,\cdots,s_n\in S,t_1,\cdots,t_m\in T$满足$f(s_1,\cdots,s_n,t_1,\cdots,t_m)=0$。令$g=g(y_1,\cdots,y_m)=f(s_1,\cdots,s_n,y_1,\cdots,y_m)\in K(S)[y_1,\cdots,y_m]\subset E[y_1,\cdots,y_m]$。由于$g(t_1,\cdots,t_m)=0$，而$T$在$E$上是代数无关的，从而$g=0$。现在

$$f=f(x_1,\cdots,x_n,y_1\cdots,y_m)=\sum_{i=1}^{r}h_i(x_1,\cdots,x_n)k_i(y_1,\cdots,y_m),$$

其中$h_i\in K[x_1,\cdots,x_n]$，$k_i\in K[y_1,\cdots,y_m]$。从而$0=g(y_1,\cdots,y_m)=f(s_1,\cdots,s_n,y_1,\cdots,y_m)$导致对每个$i$，$h_i(s_1,\cdots,s_n)=0$。但是$S$在$K$上是代数无关的，从而对每个$i$，$h_i=0$，于是$f(x_1,\cdots,x_n,y_1,\cdots,y_m)=0$。因此$S\cup T$在$K$上是代数无关的。 ∎

如果K_1和K_2是域，并且F_1和F_2分别是它们的代数闭包，则由定理V.3.8可知，每个同构$K_1\cong K_2$均可扩充成同构$F_1\cong F_2$。在适当的假设之下，这一结果现在可以推广到F_i是K_i的代数封闭域但不必是K_i的代数扩张的情形。

定理1.12 设F_1和F_2分别是K_1和K_2的扩域，并且F_1和F_2均是代数封闭的。如果$tr.d.F_1/K_1 = tr.d.F_2/K_2$，则每个域同构$K_1 \cong K_2$均可扩充成同构$F_1 \cong F_2$。

证明 令S_i是F_i在K_i上的一组超越基。由于$|S_1| = |S_2|$，由系1.3可知$\sigma: K_1 \cong K_2$能够扩充成同构$\bar{\sigma}: K_1(S_1) \cong K_2(S_2)$。但是$F_i$是代数封闭的，并且是$K_i(S_i)$的代数扩张(系1.6)，从而是$K_i(S_i)$的代数闭包。因此由定理V.3.4和V.3.8可知$\bar{\sigma}$可以扩充成同构$F_1 \cong F_2$。 ∎

习　题

注：F永远表示是K的扩域

1. (交换性质)。令S是F的子集合。如果$u \in F$在$K(S)$上是代数的，但是u在$K(S-\{v\})$上不是代数的，其中$v \in S$，则v在$K[(S-\{v\}) \cup \{u\}]$上是代数的。
2. (a) 利用Zorn引理证明每个域扩张均具有超越基。
   (b) F的每个代数无关子集合均包含在某一组超越基之中。
3. $\{x_1, \cdots, x_n\}$是$K(x_1, \cdots, x_n)$的一组超越基。
4. 如果E_1，E_2是中间域，则
   (i) $tr.d.E_1E_2/K \geqslant tr.d.E_i/K$ (对于$i=1, 2$)。
   (ii) $tr.d.E_1E_2/K \leqslant (tr.d.E_1/K) + (tr.d.E_2/K)$。
5. 如果$F = K(u_1, \cdots, u_n)$是K的有限生成扩张，E是中间域，则E也是K的有限生成扩张。[注：由定理V.1.11和V.1.12可知对于代数扩张的情形这显然是对的。]
6. (a) 如果S是复数域$\mathbf{C}$在有理数域$\mathbf{Q}$上的超越基，则S是无限的。[提示：如果S是有限的，证明

$|\mathbf{Q}(S)| = |\mathbf{Q}(x_1, \cdots x_n)| = |\mathbf{Q}[x_1, \cdots, x_n]| = |\mathbf{Q}| < |\mathbf{C}|$

(见引论中的习题8.3，8.9和定理1.2)。但是由引理V.3.5导致$|\mathbf{Q}(S)| = |\mathbf{C}|$。]

(*b*) 域$\mathbf{C}$有无限多个不同的自同构。

(*c*) $tr.d.\mathbf{C}/\mathbf{Q} = |\mathbf{C}|$

7. 如果F是代数封闭的，而E是中间域，并且$tr.d.E/K$是有限的，则每个K-单同态$E \to F$均可扩充成F的K-自同构。

8. 如果F是代数封闭的，并且$tr.d.F/K$是有限的，则每个K-单同态$F \to F$事实上均是自同构。

2. 线性无缘与可分性

本节的主要目的是将可分性概念推广到(可能)不是代数的域扩张中去。在代数扩张的情形，关于可分性的这个更为一般的概念与我们原先的定义是一致的(定理2.8)。我们首先引进线性无缘的思想，并且发展它的基本性质(定理2.2—2.7)。然后用线性无缘来定义可分性，并且用多种方式对可分性加以刻划(定理2.10)。在定理2.10的一些系中给出可分性的另一些性质。

在下面的讨论中，所有的域均假定是某个(固定)代数封闭域C的子域。

定义2.1 设C是代数封闭域，K，E，F均是C的子域，并且$K \subset E \cap F$。我们称E和F在K上是线性无缘的，是指E的每个子集合若在K上线性无关，则在F上也是线性无关的。

注记：另一种定义是采用张量积，由习题1给出。注意E的子

集合X在C的某个子域上是线性无关的$\Longleftrightarrow X$的每个有限子集合在此子域上均是线性无关的。从而为了证明线性无缘性，我们只要处理有限的线性无关集合即可。

例 如果$K\subset E$，则E和K在K上显然是线性无缘的。这一事实在许多证明中常常用到。另一些非平凡的例子见后面的定理和习题。

定义2.1的措辞方式会使我们想到线性无缘的定义关于E和F是对称的。现在我们证明这一事实。

定理2.2 设C是代数封闭域，K，E，F均是C的子域，并且$K\subset E\cap F$。则E和F在K上是线性无缘的$\Longleftrightarrow F$和E在K上是线性无缘的。

证明 只需假定E和F是线性无缘的来证明F和E是线性无缘的。假设$X\subset F$在K上是线性无关的但是在E上是线性相关的，则$r_1u_1+\cdots+r_nu_n=0$，其中$u_i\in X$而$r_i\in E$不全为零。取$\{r_1,\cdots,r_n\}$的一个子集合使对于“在K上线性无关”这一性质是极大的。必要时重新加以标号，可以假设这个子集合是$\{r_1,\ r_2,\ \cdots,\ r_t\}$ $(t\geqslant 1)$。于是对于每个$j>t$，$r_j=\sum_{i=1}^{t}a_{ij}r_i$，其中$a_{ij}\in K$（习题IV.2.1）。于是：

$$0=\sum_{j=1}^{n}r_ju_j=\sum_{j=1}^{t}r_ju_j+\sum_{j=t+1}^{n}\Big(\sum_{i=1}^{t}a_{ij}r_i\Big)u_j$$

$$=\sum_{k=1}^{t}\Big(u_k+\sum_{j=t+1}^{n}a_{kj}u_j\Big)r_k.$$

由于E和F是线性无缘的，从而$\{r_1,\ \cdots,\ r_t\}$在F上是线性无关的，从而对每个$k\leqslant t$，$u_k+\sum_{j=t+1}^{n}a_{kj}u_j=0$。这就与$X$在$K$上的线性无

关性相矛盾。因此X在E上是线性无关的。∎

下面的引理和定理对于两个域是否线性无缘提供一些有用的判别法。

引理2.3 设C是代数封闭域，K，E，F均是它的子域，并且$K\subset E\cap F$。令R是E的子环，并且$K(R)=E$，$K\subset R$（由此可知R是K上的向量空间）。则下面几个条件是彼此等价的：

(i) E和F在K上线性无缘；

(ii) R 的每个子集合若在K 上线性无关，则也在F上线性无关；

(iii) 存在着向量空间R在K上的一组基，使得它在F 上是线性无关的。

注记：此引理在稍微弱一些的假设之下也是正确的(习题2)，但是我们只需要引理2.3。

证明 (i)$\Longrightarrow$(ii)和(i)$\Longrightarrow$(iii)显然成立。

(ii)$\Longrightarrow$(i)：令 $X=\{u_1,\ \cdots,\ u_n\}$ 是E的有限子集合并且它在K上是线性无关的。我们必需证明X在F上也是线性无关的。由于$u_i\in E=K(R)$，每个u_i都有形式 $u_i=c_id_i^{-1}=c_i/d_i$，其中 $c_i=f_i(r_1,\ \cdots,r_{t_i})$，$0\neq d_i=g_i(r_1,\ \cdots,\ r_{t_i})$。而 $t_i\in R$，f_i，$g_i\in K[x_1,\ \cdots,x_{t_i}]$（定理V.1.3）。令$d=d_1d_2\cdots d_n$，并且对于每个$i$令$v_i=c_id_1\cdots d_{i-1}d_{i+1}\cdots d_n\in R$。则$u_i=v_id^{-1}$，并且$R$的子集合$X'=\{v_1,\ \cdots,\ v_n\}$在$C$的某个子域上是线性无关的$\Longleftrightarrow$$X$在此子域上是线性无关的。从假设知$X$在$K$ 上是线性无关的，所以 X'在K上也是线性无关的。于是由(ii)推出X'在F上是线性无关的，从而X在F上也是线性无关的。

(iii)$\Longrightarrow$(ii)：令U是R 在K上的一组基，并且在F上是线性

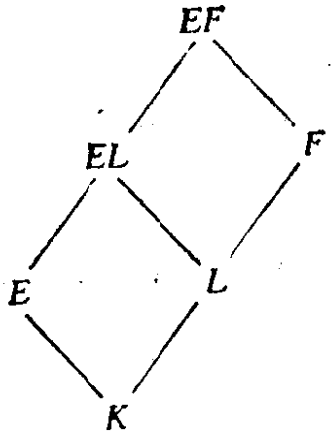
无关的。我们必须证明：R的每个有限子集合X如果在K上是线性无关的，那末它在F上也是线性无关的。由于X是有限的，于是存在U的一个有限子集合U_1，使得X包含在由U_1所张成的R的 K-子空间V之中（注意U_1是V在K上的一组基）。令V_1是由U_1 在F上所张成的向量空间。由(iii) 知U从而U_1在F上是线性无关的。因此U_1是V_1 在F上的一组基，并且$\dim_K V = \dim_F V_1$。现在X包含在V的某个有限K-基W之中（定理IV.2.4）。由于W必定张成 F-向量空间V_1，从而W包含V_1的一组F-基。因此 $|W_1| \leqslant |W| = \dim_K V = \dim_F V_1 = |W_1|$，于是 $W = W_1$。 从而W的子集合X必定在F上是线性无关的。∎

定理2.4 设C是代数封闭域，K，E，L，F均是C的子域，并且$K \subset E$，$K \subset L \subset F$。则E和F在K上线性无缘的充要条件是：

(i) E和L在K上是线性无缘的，并且

(ii)EL和F在L上是线性无缘的。

证明 形势如下图所示：



(⇐)：如果E的子集合X 在K上是线性无关的，由(i) 可知X在L上也是线性无关的。因此由(ii) 可知X在F上也是线性无关的（因为$X \subset E \subset EL$）。

(⇒)：如果E和F在K上是线性无缘的，则E和L在K上自然是线性无缘的。为证(ii)，注意$EL=L(R)$，其中R是由L和E生成的C的子环$L[E]$。根据定理 V.1.3，R的每个元素均有形式 $f(e_1, \cdots, e_n)$ $(e_i\in E,\ f\in L[x_1, \cdots, x_n])$。因此，$E$在 K上的任意一组基U均张成L-向量空间R。由于E和L在K上是线性无缘的，从而U在L上是线性无关的。于是U是R在L上的一组基。但是由于E和F是线性无缘的，从而U在F上也是线性无关的。于是由引理2.3可知EL和F在L上是线性无缘的。∎

下面我们要弄清在K的某些扩域上的线性无缘性，它在定义可分性的时候起着重要的作用。

定义2.5 设K是特征$p\neq 0$的域，C是代数封闭域，并且 $K\subset C$。对于每个整数$n\geqslant 0$，定义

$$K^{1/p^n}=\{u\in C \mid u^{p^n}\in K\}$$

$$K^{1/p^\infty}=\bigcup_{n\geqslant 0}K^{1/p^n}=\{u\in C \mid u^{p^n}\in K,\ \text{对于某个}n\geqslant 0\}.$$

注记：由于在特征为p的域中$(u\pm v)^{p^n}=u^{p^n}\pm v^{p^n}$，(习题III.1.11)，从而每个$K^{1/p^n}$事实上是域。由于当$0\leqslant n\leqslant m$时，$K=K^{1/p^0}\subset K^{1/p^n}\subset K^{1/p^m}\subset K^{1/p^\infty}$可知$K^{1/p^\infty}$也是域。事实上，由于$C$是代数封闭域，可知$K^{1/p^\infty}$是多项式集合$\{x^{p^n}-k \mid k\in K\}$在$K$上的分裂域(习题5)。特别地，每个$k\in K$有形式$v^{p^n}$，其中 $v\in K^{1/p^n}$.由于K^{1/p^n}是在K上的分裂域，它本质上与C是无关的(也就是说，如果选取另一个C'，则由定理V.3.8给出一个与K^{1/p^n}同构的域)。

引理2.6 如果F是K的扩域，$\mathrm{char}K=p\neq 0$。而C是包含F的代数封闭域，则对每个$n\geqslant 0$，F的子集合X在K^{1/p^n}上是线性无关

的$\Longleftrightarrow X^{p^n}=\{u^{p^n}\mid u\in X\}$在$K$上是线性无关的。进而，$X$在$K^{1/p^\infty}$上是线性无关的$\Longleftrightarrow$对于每个$n\geqslant 0$，$X$在$K^{1/p^n}$上都是线性无关的。

证明概要 每个$a\in K$都有形式$a=v^{p^n}$，其中$v\in K^{1/p^n}$（习题5）。第一个论断是由于：$\sum_i a_i u_i^{p^n}=0$ $(a_i\in K,\ u_i\in X)\Longleftrightarrow$ $\sum_i v_i^{p^n}u_i^{p^n}=0(v_i\in K^{1/p^n},\ v_i^{p^n}=a_i)\Longleftrightarrow(\sum_i v_iu_i)^{p^n}=0\Longleftrightarrow$ $\sum_i V_iu_i=0$。第二个论断是由于：如果$\sum_{i=1}^{t} w_iu_i=0$ $(w_i\in K^{1/p^\infty}$，$u_i\in X)$，则对于充分大的n有$w_1,\cdots,w_t\in K^{1/p^n}$。∎

定理2.7 设F是代数封闭域C的子域。如果F是域K的纯超越扩张，并且$\mathrm{char}K=p\neq 0$，则对于每个$n\geqslant 0$，F和K^{1/p^n}在K上是线性无缘的。并且F和K^{1/p^∞}在K上是线性无缘的。

证明 设$F=K(S)$，其中S是F在K上的一组超越基。如果$S=\varnothing$，则$F=K$，并且F在K上的每个线性无关子集均是由K中一个非零元素组成的。它显然在C的任一子域上都是线性无关的，从而$S=\varnothing$的时候定理是对的。如果S不空，令M是S上单项式集合（即S中有限个元素之积所构成的集合）。由于S在K上是代数无关的，从而M在K上是线性无关的。由定理V.1.3可知M张成子环$K[S]$（看作是K上向量空间）。因此M是$K[S]$的一组K-基。S的代数无关性导致对于每个$n\geqslant 0$，$M^{p^n}=\{m^{p^n}\mid m\in M\}$在$K$上是线性无关的。由引理2.6可知对于每个$n$，$M$在$K^{1/p^n}$上是线性无关的，从而在$K^{1/p^\infty}$上也是线性无关的。于是对于每个$0\leqslant n\leqslant\infty$，从引理2.3推出$F$和$K^{1/p^n}$在$K$上是线性无缘的（在引理2.3中分别取$R$，$E$，$F$为$K[S]$，$F$和$K^{1/p^n}$）。∎

下一个定理表明线性无缘与可分代数扩张之间的联系，由此产生出对于任意（可能非代数的）扩张的可分性定义。

定理2.8 设F是域K的代数扩张，$\mathrm{char}K=p\neq 0$。C是包含F的代数封闭域。则F在K上是可分的$\Longleftrightarrow F$和$K^{1/p}$在K上是线性无缘的。

证明 这里我们只证明由可分性导致F与$K^{1/p}$的线性无缘性。另一方向的证明很容易由后面一个结果推出来（见定理2.10后面的注记）。令$X=\{u_1, \cdots u_n\}$是F的有限子集合，并且X在K上是线性无关的。我们必须证明X在$K^{1/p}$上也是线性无关的。子域$E=K(u_1, \cdots, u_n)$在K上是有限维的（定理V.1.12），并且有一组基$\{u_1, \cdots, u_n, u_{n+1}, \cdots, u_r\}$包含$X$（定理IV.2.4）。如果$v\in E$而$k$是正整数，则$v^k=\sum_{i=1}^{r} a_i u_i (a_i\in K)$，从而$v^{kp}=(\sum_i a_i u_i)^p=\sum a_i^p u_i^p$。由于$v$在$K$上是可分的，从而$K(v)$在$K(v^p)$上既是代数可分扩张又是纯不可分扩张（定理V.6.4和引理V.6.6），从而$K(v)=K(v^p)=K[v^p]$（定理V.1.6和V.6.2）。因此v是诸v^{kp}的线性组合，从而也是诸u_i^p的线性组合。因此E是由$\{u_1^p, \cdots, u_r^p\}$张成的。由于$[E:K]=r$，由定理IV.2.5和IV.2.7可知$\{u_1^p, \cdots, u_r^p\}$一定是一组基。从而$\{u_1^p, \cdots, u_r^p\}$在K上是线性无关的，于是X^p在K上也是线性无关的。由引理2.6可知X在$K^{1/p}$上是线性无关的，于是F和$K^{1/p}$在K上是线性无缘的。 ∎

定义2.9 设F是K的扩域，F在K上的一组超越基S叫作F在K上的可分超越基，是指F在$K(S)$上是可分的。假如F在K上具有可

分超越基，则称F在K上可分生成的。

注记：让我们回忆(系1.6)：F是$K(S)$的代数扩张。如果F在K上是可分生成的，那么F在K上的超越基不一定均是可分超越基(习题8)。

例 如果F是K的可分代数扩张，则空集合是F在K上的可分超越基。每个纯超越扩张显然是可分生成的，因为这时$F=K(S)$。

为了使我们的主要定理在特征零的情形也是有意义的，我们规定（对任一特征零域K）$K^{1/0}=K^{1/0^n}=K^{1/0^\infty}=K$。

定理2.10 如果F是K的扩域，$\mathrm{char}K=p\geqslant 0$，而$C$是包含$F$的代数封闭域，则下列诸条件是彼此等价的。

(i) F和$K^{1/p}$在K上是线性无缘的；

(ii)对于某个$n\geqslant 1$，F和K^{1/p^n}在K上是线性无缘的；

(iii)F和K^{1/p^∞}在K上是线性无缘的；

(iv) 每个有限生成的中间域E在K上均是可分生成的；

(v) K_0和F在K上是线性无缘的，其中K_0是$\mathrm{Aut}_K F$（对于C和K）的固定域。

注记：定理的证明在下面。由(i)⇒(iv)可以证明定理2.8的第二部分：对于每个$u\in F$，$K(u)$是有限生成的中间域，从而在K上是可分生成的。但是已经假定F（从而$K(u)$）是K的代数扩张，而代数扩张的超越基只有空集合。因此$K(u)$在$K(\varnothing)=K$上是可分代数的。于是每个$u\in F$在K上都是可分代数的。

定理2.10的证明概要 除了证明(iii)⟺(v)之外，我们均假定$\mathrm{char}K=p\neq 0$。因为$\mathrm{char}K=0$的情形，是平凡的。另一方面，由于对于每个$n\geqslant 1$，$K^{1/p}\subset K^{1/p^n}\subset K^{1/p^\infty}$，从而立刻得出(iii)⇒(ii)⇒(i)。

(i)⇒(iv)：设$E=K(s_1, \cdots, s_n)$，$tr.d.E/K=r$。由系1.7可知$r\leqslant n$，并且$\{s_1, \cdots, s_n\}$的某个子集合（设是$\{s_1, \cdots, s_r\}$）为E在K上的一组超越基。如果$r=n$，则$\{s_1, \cdots, s_n\}$显然是可分超越基，从而(iv)成立。如果$r<n$，则s_{r+1}在$K(s_1, \cdots, s_r)$上是代数的（系1.6），因此s_{r+1}是一个不可约首1多项式$f(x)=\sum_{i=1}^{m} a_i x^i \in K(s_1, \cdots, s_r)[x]$的根。象证明定理 1.5时一样采用“最小公分母方法”，可以得出$f(x)=d^{-1}\left(\sum_{i=1}^{m} v_i x^i\right)$，其中$0\neq d\in K[s_1, \cdots, s_r]$，$v_i=h_i(s_1, \cdots, s_r)$，而$h_i(x_1, \cdots, x_r)\in K[x_1, \cdots, x_r]$。因此$f_1=\sum_{i=0}^{m} h_i(x_1, \cdots, x_r)x_{r+1}^i \in K[x_1, \cdots, x_{r+1}]$并且$f_1(s_1, \cdots, s_{r+1})=0$。从而存在一个具有最小正次数的多项式$g\in K[x_1, \cdots, x_{r+1}]$使得$g(s_1, \cdots, s_{r+1})=0$。$g$在$K[x_1, \cdots, x_{r+1}]$中显然是不可约的。我们称$x_i$出现在$g(x_1, \cdots, x_{r+1})$中，指得是$g$中有某个非零项包含一个因子$x_i^m$，$m\geqslant 1$。

我们断言：必定有某个x_i出现在g中，并且其指数不是p的倍数。因为不然的话，就会$g=c_0+c_1 m_1(x_1, \cdots, x_{r+1})^p+\cdots+c_k m_k(x_1, \cdots, x_{r+1})^p$，其中$c_j\in K$不全为零，而$m_j(x_1, \cdots, x_{r+1})$均是$x_1, \cdots, x_{r+1}$的单项式。令$m_0(x_1, \cdots, x_{r+1})=1_K$，并且对于每个$j\geqslant 0$，取$d_j\in K^{1/p}$，使得$d_j^p=c_j$。则$g=\left(\sum_{j=0}^{k} d_j m_j(x_1, \cdots, x_{r+1})\right)^p$，从而$g(s_1, \cdots, s_{r+1})=0$导致

$$\sum_{j=0}^{k} d_j m_j(s_1, \cdots, s_{r+1})=0$$

于是F的子集合$\{m_j(s_1, \cdots, s_{r+1}) | j \geqslant 0\}$在$K^{1/p}$上是线性相关的。但是这个子集合在$K$上必然是线性无关的（因为不然的话，将会存在$g_1 \in K[x_1, \cdots, x_{r+1}]$，使得$\deg g_1 < \deg g$，并且$g_1(s_1, \cdots, s_{r+1}) = 0$）。这就与$F$和$K^{1/p}$线性无缘这一事实相矛盾。因此必然有某个$x_i$（无妨设是$x_1$）出现在$g$中，并且其指数不是$p$的倍数。

多项式$g(x, s_2, \cdots, s_{r+1}) \in K(s_2, \cdots, s_{r+1})[x]$必定不为零。因为不然的话，由上一段知道$x_1$出现在$g(x_1, \cdots, x_{r+1})$中，从而将会得到一个多项式$g_2 \in K[x_1, \cdots, x_{r+1}]$，使得$0 < \deg g_2 < \deg g$并且$g_2(s_1, s_2, \cdots, s_{r+1}) = 0$。这就与$g$的取选方式相矛盾。因此$g(x, s_2, \cdots, s_{r+1}) \neq 0$。由于$g(s_1, s_2, \cdots, s_{r+1}) = 0$，从而$s_1$在$K(s_2, \cdots, s_{r+1})$上是代数的。但是$s_2, \cdots, s_{r+1}$在$K(s_2, \cdots, s_{r+1})$上显然是代数的，并且$E$也是$K(s_1, \cdots, s_{r+1})$的代数扩张，由定理V.1.12和V.1.13便知$E$是$K(s_2, \cdots, s_{r+1})$的代数扩张。由于$tr.d.E/K = r$，从而$\{s_2, \cdots, s_{r+1}\}$是$E$在$K$上的一组超越基（系1.7）。

从定理1.2的证明可知，$x_i \longmapsto s_i$决定一个K-同构ϕ：$K[x_2, \cdots, x_{r+1}] \cong K[s_2, \cdots, s_{r+1}]$。$\phi$显然可以扩充成$K$-同构$K[x_1, x_2, \cdots, x_{r+1}] = K[x_2, \cdots, x_{r+1}][x_1] \cong K[s_2, \cdots, s_{r+1}][x]$，使得$x_1 \longmapsto x$，$g(x_1, \cdots, x_{r+1}) \longmapsto g(x, s_2, \cdots, s_{r+1})$。由于$\phi$是同构，从而$g(x, s_2, \cdots, s_{r+1})$在$K[s_2, \cdots, s_{r+1}][x]$中必然是不可约的。从而$g(x, s_2, \cdots, s_{r+1})$在$K[s_2, \cdots, s_{r+1}][x]$中是本原的，于是由引理III.6.13和定理III.6.14可知它在$K(s_2, \cdots, s_{r+1})[x]$中也是不可约的。因为$\phi$是同构，$x$必然出现在$g(x, s_2, \cdots, s_{r+1})$之中，并且其指数不是$p$的倍数。因此$g(x, s_2, \cdots, s_{r+1})$的导函数不是零（习题III.6.3），从而由定理III.6.10可知$g(x, s_2, \cdots, s_{r+1})$是可分的。因此$s_1$是$K(s_2, \cdots, s_{r+1})$

上的可分代数元素，从而也是$K(s_2, \cdots, s_n)$上的可分代数元素．特别地，从引理V.6.6可知$E=K(s_1, \cdots, s_n)$是$K(s_2, \cdots, s_n)$的可分代数扩张．因此，如果$\{s_2, \cdots, s_n\}$是E在K上的一组超越基，则E在K上是可分生成的．如果不然，则$\{s_2, \cdots, s_n\}$包含一组超越基（系1.7），必要时重新加以标号，我们无妨假定这组超越基是$\{s_2, \cdots, s_{r+1}\}$．重复上面的推导过程（对于$1 \leqslant i \leqslant r+1$将$s_i$改成$s_{r+1}$并且可能再重新标号）可以证明$s_2$（从而$K(s_2, \cdots, s_n)$）在$K(s_3, \cdots, s_n)$上是可分代数的．于是由系V.6.8便知$E$在$K(s_3, \cdots, s_n)$上是可分代数的．继续这个过程我们就可求出$s_1, \cdots, s_t$，使得$E$是$K(s_{t+1}, \cdots, s_n)$的可分代数扩张，而$\{s_{t+1}, \cdots, s_n\}$是$E$在$K$上的一组超越基．从而$E$在$K$上是可分生成的．

(iv)⇒(iii)：设W是F的有限子集合，并且在K上是线性无关的．我们必须证明W在K^{1/p^∞}上也是线性无关的．令$E=K(W)$．我们只需证明E和K^{1/p^∞}在K上是线性无缘的，因为由这一事实立刻得出W在K^{1/p^∞}上是线性无关的．由于W是有限集合，由(iv)可知E在K上有可分超越基S．我们现在将定理2.4用于扩张$K \subset K^{1/p^\infty}$和$K \subset K(S) \subset E$，来证明E和K^{1/p^∞}的线性无缘性．方法如下：根据定理2.7，$K(S)$和K^{1/p^∞}是线性无缘的．设X是E的子集合，并且X在$K(S)$上是线性无关的．由于E是$K(S)$的可分代数扩张，由定理2.8中已经证过的一半可知X在$K(S)^{1/p}$上也是线性无关的．因此由引理2.6可知X^p在$K(S)$上是线性无关的．将以上三句话作归纳推理，即知对于每个$m \geqslant 0$，X^{p^m}在$K(S)$上都是线性无关的（注意$(X^{p^r})^p = X^{p^{r+1}}$）．于是再由引理2.6，可知对于每个$m \geqslant 0$，$X$在$K(S)^{1/p^m}$上都是线性无关的．从而$X$在$K(S)^{1/p^\infty}$上是线性无关的，从而$X$在其子域$K^{1/p^\infty}K(S)$上也是线性无关的．于是我们证明了$E$和$K^{1/p^\infty}K(S)$在$K(S)$上是线性无缘的．从而由定理2.4即知$E$和$K^{1/p^\infty}$在$K$上是线性无缘的．

(iii)$\Longleftrightarrow$(v)：只需证明$K_0=K^{1/p^\infty}$即可。令$u\in K_0$。如果u在K上是超越的，则存在$v\in C$，$v\neq u$，并且v在K上是超越的（例如取$v=u^2$）。由定理 V.1.5 给出的同构的合成 $K(u)\cong K(x)\cong K(v)$是K-同构σ，并且$\sigma(u)=v$。于是我们有$1=tr.d.K(x)/K=tr.d.K(u)/K=tr.d.K(v)/K$。定理1.11（如果$tr.d.C/K(u)$无限时利用引论中的引理8.9）导致$tr.d.C/K(u)=tr.d.C/K(v)$。从而由定理1.12可知$\sigma$可以扩充成$C$的$K$-自同构。但是$\sigma(u)=v\neq u$，这就与$u\in K_0$这一事实相矛盾。从而$u$必定在$K$上是代数的。假设$u$在$K$上的极小多项式为$f\in K[x]$。如果$v\in C$是$f$的另一个根，则存在$K$-同构$\tau$：$K(u)\longrightarrow K(v)$，并且$\tau(u)=v$（系 V.1.9）。与超越情形相类似的可以推导出，τ可以扩充成C的 K-自同构.由于$u\in K_0$，从而必然有$u=\tau(u)=v$，于是f在C中只有一个根。因此u在K上是纯不可分的。如果 $\mathrm{char}K=0$。则f必然可分，因此次数为1。于是 $u\in K=K^{1/0^\infty}$。如果$\mathrm{char}K=p\neq 0$，则由定理V.6.4 可知存在某个$n\geqslant 0$，使得$u^{p^n}\in K$。于是$u\in K^{1/p^n}\subset K^{1/p^\infty}$.于是我们证明了$K_0\subset K^{1/p^\infty}$。反之，假设$\mathrm{char}K=p\neq 0$，$u\in K^{1/p^n}\subset K^{1/p^\infty}$并且$\sigma\in \mathrm{Aut}_K C$。则 $\sigma(u)^{p^n}=\sigma(u^{p^n})=u^{p^n}$，从而$\sigma=\sigma(u)^{p^n}-u^{p^n}=(\sigma(u)-u)^{p^n}$，于是$\sigma(u)=u$。因此$K^{1/p^\infty}\subset K_0$。∎

定义2.11 域K的扩域F叫作在K上是可分的（或叫作K 的可分扩张），是指F满足定理2.10中彼此等价的那些条件。

注记：由定理 2.8 可知这个定义与代数扩张情形已经使用过的“可分性”定义（定义 V.3.10）是一致的。由于在 $\mathrm{char}K=0$ 时定理2.10的第一个条件显然成立，从而特征零域的每个扩域都是可分的。

在下面两个系理中我们给出可分性的一些基本性质。

系2.12 （MacLane判别法）如果F是域K的扩域，并且在K上是可分生成的，则F在K上是可分的。反之，如果F在K上是可分的并且是有限生成的，设$F=K(u_1, \cdots, u_n)$，则F在K上是可分生成的。事实上，存在$\{u_1, \cdots, u_n\}$的某个子集合是F在K上的一组可分超越基。

证明概要 在定理2.10的证明 (iv)$\Longrightarrow$(iii)$\Longrightarrow$(i) 中取$F=E$即可证明第一论断，因为只用到E是可分生成这一事实。而后面两个论断则是定理2.10中证明 (i)$\Longrightarrow$(iv) 的直接推论。∎

系2.13 假设F是域K的扩域而E为中间域。

(i) 如果F在K上是可分的，则E在K上也是可分的。

(ii) 如果F在E上是可分的，而E在K上是可分的，则F在K上也是可分的。

(iii) 如果F在K上是可分的，E在K上是代数的，则F在E上也是可分的。

注记：如果E在K上不是代数的，则 (iii) 可能不成立（见习题8）。

证明概要 (ii) 利用定理2.4和2.10。

(iii) 如果$\mathrm{char}K=p\neq 0$，令X是F的子集合，并且在E上是线性无关的。将X扩充成F在E上的一组基U，令V是E在K上的一组基。从定理IV.2.16的证明可知$UV=\{uv \mid u\in U, v\in V\}$是$F$在$K$上的一组基。由可分性即知$UV$在$K^{1/p}$上是线性无关的。由引理2.6导致$(UV)^p=\{u^pv^p \mid u\in U, v\in V\}$在$K$上是线性无关的。我们断言：$V^p$是$E$在$K$上的一组基。这是因为：从 (i) 知$E$在$K$上是可

分的，从而由E与$K^{1/p}$的线性无缘性可知V在$K^{1/p}$上是线性无关的，因此V^p在K上是线性无关的(引理2.6)。由系V.6.9知$E=KE^p$，从而V^p在K上张成E。因此V^p是E在K上的一组基。为了完成证明，我们还需要证明X在$E^{1/p}$上是线性无关的。如果$\sum_i a_i u_i = 0$($a_i \in E^{1/p}$，$u_i \in X \subset U$)，则$\sum_i a_i^p u_i^p = 0$。但是每个$a_i^p \in E$均有形式$\sum_j c_{ij} v_j^p (c_{ij} \in K,\ v_j \in V)$，从而我们有$0 = \sum_i \left(\sum_j c_{ij} v_j^p\right) u_i^p = \sum_{i,j} c_{ij} u_i^p v_j^p$。由$(UV)^p$的线性无关性推出对每个$i,j$均有$c_{ij}=0$。从而对每个$i$均有$a_i=0$。于是$X$在$E^{1/p}$上是线性无关的。∎

习　题

注：E和F永远是域K的扩域，而C是包含E和F的代数封闭域。

1. 由E和F生成的子环$E[F]$以显然的方式是K上的向量空间。张量积$E\otimes_K F$也是K-向量空间(见定理IV.5.5和系IV.5.12)。E和F在K上是线性无缘的$\Longleftrightarrow$$K$-线性变换$E\otimes_K F \to E[F]$(在$E\otimes_K F$的生成元上由$a\otimes b \longrightarrow ab$给出)是同构。

2. 假设E和F分别是整环R和S的商域。则C以显然的方式为R-模和S-模。

   (a) E和F在K上是线性无缘的$\Longleftrightarrow$$R$的每个子集合如果在$K$上是线性无关的，那末它在$S$上也是线性无关的。

   (b) 进一步假设R是K上的向量空间。则E和F在K上是线性无缘的$\Longleftrightarrow$$R$在$K$上的每一组基在$F$上均是线性无关的。

   (c) 又设R和S均是K上的向量空间。则E和F在K上是线性无缘的$\Longleftrightarrow$对于R在K上的每一组基X和S在K上的每一组基Y，集合$\{uv \mid u\in X, v\in Y\}$在$K$上是线性无关的。

3. 利用习题1证明定理2.2。

4. 利用习题1和张量积的结合律证明定理2.4。

5. 如果$\mathrm{char}K=p\neq 0$，则

(*a*) 对于每个$n\geqslant 0$，K^{1/p^n}均是域。见习题III.1.11。

(*b*) K^{1/p^∞} 是域。

(*c*) K^{1/p^n}是 $\{x^{p^n}-k\mid k\in K\}$ 在K上的分裂域。

6. 如果 $\{u_1, \cdots, u_n\}$ 在F上是代数无关的，则 F 和 $K(u_1, \cdots, u_n)$ 在K上是线性无缘的。

7. 如果E是K的纯超越扩张，F是K的代数扩张，则E和F在K上是线性无缘的。

8. 令$K=Z_p$，　　$F=Z_p(x)$，　　$E=Z_p(x^p)$。

(*a*) F在K上是可分的和可分生成的。

(*b*) $E\neq F$。

(*c*) F是E的纯不可分代数扩张。

(*d*) $\{x^p\}$ 是F在K上的一组超越基，但不是可分超越基。

9. 令$\mathrm{char}K=p\neq 0$，u是K上的超越元素。假设F在K上由 $\{u, v_1, v_2, \cdots\}$ 生成的，其中v_i是$x^{p^i}-u\in K(u)[x]$ 的根 $(i=1, 2, \cdots)$。则F在K上是可分的，但不是可分生成的。

10. (*a*) K为完全域$\Longleftrightarrow K$ 的每个扩域在K上均是可分的(见练习V.6.13)。

(*b*) (MacLane) 假设K 是完全域，F 不是完全域，并且 $tr.d.F/K=1$。则F在K上是可分生成的。

11. F是K的纯不可分扩张$\Longleftrightarrow$只有包含映射是K-单同态$F\to C$。

12. 我们称E和F在K上是自由的，是指E的每个子集合 X 如果在K上是代数无关的，便在F上也是代数无关的。求证

(*a*) 这个定义是对称的（即：E和F在K上是自由的$\Longleftrightarrow F$ 和 E在K上是自由的)。

(*b*) 如果E和 F 在K上是线性无缘的，则E和F在K上是自由的。以例表明反过来不一定成立。

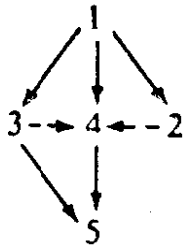
(c) 如果E在K上是可分的，并且E和F在K上是自由的，则EF在F上是可分的。

(d) 如果E和F在K上是自由的，并且E和F在K上均是可分的，则EF在K上是可分的。

第VII章　线性代数

线性代数是许多数学分支的重要工具，并且有广泛的应用。这一课题的大部分内容是研究（有限生成）自由模的同态（特别是研究有限维向量空间的线性变换）。这些同态与矩阵之间存在着重要的关系（第1节）。由于研究表达同一个同态（对于不同基）的两个矩阵之间的联系，产生出矩阵的等价和相似概念（第2节与第4节）。第5节研究矩阵的某些重要的相似不变量。在许多地方，矩阵的行列式（第3节）是很有益处的。

由于我们对于线性代数的应用也有相当大的兴趣，在本章中也放入不少计算性的材料。对于不少读者来说，这样一些材料对于他们可能是一种额外的负担。但是本章作了精心地安排，以便使只希望阅读这一理论的重要基本事实的那些读者可以花费比较少的时间。他只需要略去标成“命题”的全部结果，同时注意课文中的评论，在这些评论中指明哪些材料今后是需要的。本章各节之间的联系大致如下图所示：



与前面一样，其中虚线箭头$A\cdots\to B$表示第A节的各别结果在第B

节中用到，但是第B节与第A节本质上是独立的。

1. 矩阵和映射

首先简单复习一下矩阵的基本性质。然后阐明矩阵与自由模的同态之间的所有重要关系。除了定理1.1之外，所有的环均假定是含幺环，但是不再加别的限制。除了本节末尾对于对偶性所作的讨论之处，本节所有其余材料今后在本章中都是需要的。

设R是环。将一些元素作形如

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1m} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2m} \\ \vdots & & & & \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nm} \end{pmatrix}$$

的一个n行m列的排列(其中$a_{ij} \in R$)叫作R上一个 $n \times m$ 矩阵。$n \times n$矩阵也叫作方阵。为简洁起见，每个矩阵通常用大写字母A、B、C 或者 (a_{ij}) 来表示，其a_{ij}表示该矩阵的第i行第j列处的元素是 $a_{ij} \in R$。两个矩阵 (a_{ij}) 和 (b_{ij}) 相等，当且仅当对于每个i和j在R中均有$a_{ij} = b_{ij}$。元素 a_{11}，a_{22}，a_{33}，…，形成矩阵(a_{ij})的主对角线。一个$n \times n$方阵如果 $a_{ij} = 0$ (对于所有 $i \neq j$)，则称为对角方阵。如果 R 有幺元素，则单位方阵I_n是指 $n \times n$ 阶对角方阵，其中主对角线上的元素均是 1_R，即 $I_n = (\delta_{ij})$，其中δ_{ij}为Kronecker符号。一个$n \times m$ 矩阵若全部元素均为0，便称作零矩阵。以$\mathrm{Mat}_n R$表示R上全体$n \times n$方阵所组成的集合。$n \times m$矩阵$A = (a_{ij})$ 的转置是$m \times n$矩阵$A^t = (b_{ij})$，其中$b_{ij} = a_{ji}$(对于

每个i、j)。

如果$A=(a_{ij})$和$B=(b_{ij})$均是$n\times m$矩阵，则和$A+B$定义为$n\times m$矩阵(c_{ij})，其中$c_{ij}=a_{ij}+b_{ij}$。如果$A=(a_{ij})$是$m\times n$矩阵而$B=(b_{ij})$是$n\times p$矩阵，则乘积AB定义为$m\times p$矩阵(c_{ij})，其中$c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}$。乘法一般是不可交换的。如果$A=(a_{ij})$是$n\times m$矩阵而$r\in R$，则$rA$是$n\times m$矩阵$(ra_{ij})$，而$Ar$是$n\times m$矩阵$(a_{ij}r)$。而$rI_n$叫作是标量矩阵。如果矩阵乘积$AB$可以定义，则它们转置矩阵的乘积$B'A'$也可以定义。如果$R$是交换环，则$(AB)'=B'A'$。但是若$R$不是交换环，则此式可能不成立（习题1)。

定理1.1 如果R是环，则R上全体$n\times m$矩阵组成的集合对于加法形成R-R双重模，其中加法恒等元素是$n\times m$零矩阵。矩阵的乘法（在可定义的时候）与加法满足结合律与分配律。对于每个$n>0$，Mat_nR是环。如果R是含幺环，则Mat_nR也为含幺环，且幺元素是单位方阵I_n。

证明作为练习。∎

矩阵的一个重要应用是刻划自由模的同态。

定理1.2 设R是含幺环，E和F均是自由左R-模，并且分别具有由n个和m个元素组成的有限基。令M是由R上全体$n\times m$矩阵形成的左R-模。则有Abel群同构：

$$\mathrm{Hom}_R(E,\ F)\cong M.$$

如果R是交换环，则这是左R-模同构。

证明 令$\{u_1,\ \cdots,\ u_n\}$和$\{v_1,\ \cdots,\ v_m\}$分别为E和F的基，而$f\in\mathrm{Hom}_R(E,\ F)$。则有元素$r_{ij}\in R$，使得

$$f(u_1)=r_{11}v_1+r_{12}v_2+\cdots+r_{1m}v_m$$
$$f(u_2)=r_{21}v_1+r_{22}v_2+\cdots+r_{2m}v_m$$
$$\vdots$$
$$f(u_n)=r_{n1}v_1+r_{n2}v_2+\cdots+r_{nm}v_m$$

由于$\{v_1, \cdots, v_m\}$是F的基，从而r_{ij}是唯一确定的。定义映射β：$\mathrm{Hom}_R(E, F)\to M$，$f\to A$，其中$A$是$n\times m$矩阵$(r_{ij})$。不难验证$\beta$是加法同态。如果$\beta(f)=0$，则对于基中每个元素$u_i$均有$f(u_i)=0$，从而$f=0$。因此$\beta$是单同态。给了矩阵$(r_{ij})\in M$，定义$f: E\to F$，$f(u_i)=r_{i1}v_1+r_{i2}v_2+\cdots+r_{im}v_m(1\leqslant i\leqslant n)$。由于$E$是自由模，从定理IV.2.1可知$f$作为$\mathrm{Hom}_R(E, F)$中的元素是唯一确定的。由定义方式可知$\beta(f)=(r_{ij})$。于是$\beta$是满同态，从而是同构。如果$R$是交换环，则由定理IV.4.8后面的注记可知$\mathrm{Hom}_R(E, F)$是左$R$-模，其中$(rf)(x)=r(f(x))$。不难验证$\beta$是$R$-模同构。∎

设R, E, F和β如定理1.2所示。我们将定理1.2证明中的$n\times m$矩阵$(r_{ij})=\beta(f)$叫作是同态$f\in\mathrm{Hom}_R(E, F)$对于E和F的有序基$U=\{u_1, \cdots, u_n\}$和$V=\{v_1, \cdots, v_m\}$的矩阵。于是，f的矩阵的第i行即是$f(u_i)\in F$对于有序基$\{v_1, \cdots, v_m\}$的系数。特别当$E=F$并且$U=V$的时候，我们将(r_{ij})称作是自同态f对于有序基U的矩阵。

注记：令E，F，f，U，V如上一段所述。利用f的矩阵$A=(r_{ij})$，我们可以很方便的计算E中任意元素在f之下的象：如果$u=x_1u_1+x_2u_2+\cdots+x_nu_n\in E(x_i\in R)$，则

$$f(u)=f\Big(\sum_{i=1}^{n}x_iu_i\Big)=\sum_{i=1}^{n}x_if(u_i)=\sum_{i=1}^{n}x_i\Big(\sum_{j=1}^{m}r_{ij}v_j\Big)$$
$$=\sum_{j=1}^{m}\Big(\sum_{i=1}^{n}x_ir_{ij}\Big)v_j=\sum_{j=1}^{m}y_jv_j,$$

其中$y_j=\sum_{i=1}^{n}x_ir_{ij}$。因此，如果$X$是$1\times n$矩阵$(x_1x_2\cdots x_n)$而$Y$是$1\times m$矩阵$(y_1, \cdots, y_m)$，则$Y$恰好是矩阵乘积$XA$。$X$和$Y$有时叫作是行向量。

定理1.3 设R是含幺环。E，F和G分别是以$U=\{u_1, \cdots, u_n\}$，$V=\{v_1, \cdots, v_m\}$和$W=(w_1, \cdots w_q\}$为有限有序基的自由左R-模。如果$f\in \mathrm{Hom}_R(E, F)$的$n\times m$矩阵为$A$(对于基$U$和$V$)，$g\in \mathrm{Hom}_R(F, G)$的$m\times p$矩阵是$B$(对于基$V$和$W$)，则$gf\in \mathrm{Hom}_R(E, G)$的$n\times p$矩阵是$AB$(对于基$U$和$W$)。

证明 如果$A=(r_{ik})$，$B=(s_{kj})$，则对于每个$i=1, 2, \cdots, n$，

$$gf(u_i)=g\Big(\sum_{k=1}^{m}r_{ik}v_k\Big)=\sum_{k=1}^{m}r_{ik}g(v_k)$$

$$=\sum_{k=1}^{m}r_{ik}\Big(\sum_{j=1}^{p}s_{kj}w_j\Big)=\sum_{j=1}^{p}\Big(\sum_{k=1}^{m}r_{ik}s_{kj}\Big)w_j.$$

因此gf对于U和W的矩阵在(i, j)处为$\sum_{k=1}^{m}r_{ik}s_{kj}$。但这恰好为矩阵$AB$在$(i, j)$处的元素。∎

设R是含幺环，E是自由左R-模并且有n元有限基U。则$\mathrm{Hom}_R(E,E)$是环，其中映射f和g的乘积即为合成映射$fg: E\to E$(习题IV.1.7)。为今后作参考，我们这里谈谈环$\mathrm{Hom}_R(E,E)$与矩阵环Mat_nR之间的联系。如果S和T是任意环，函数$\theta: S\to T$叫作反同构，是指θ为加法群同构并且对每个s_1，$s_2\in S$，均有$\theta(s_1s_2)=\theta(s_2)\theta(s_1)$。由定理1.2和1.3可知，映射$\mathrm{Hom}_R(E, E)\to \mathrm{Mat}_nR$，$f\mapsto f$的矩阵(对于$U$)。是环的反同构。当然最好是希望$\mathrm{Hom}_R(E, E)$同构于某个矩阵环。为了证明这是可能的，我们需要新的概念。

环R的反环（表示成R^{op}）与R有同样的元素集合和同样的加法，但是R^{op}中乘法定义为

$$a\circ b=ba.$$

这里ba为R中乘法（见习题III.1.17）。映射 $r\to r$ 显然是反同构$R\to R^{op}$。如果 $A=(a_{ij})$和$B=(b_{ij})$均是R上$n\times n$方阵，则A和B也可看成是R^{op}上的方阵。在Mat_nR中$AB=(c_{ij})$，其中 $c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}$。但是在$\mathrm{Mat}_nR^{op}$中$AB=(d_{ij})$，其中

$$d_{ij}=\sum_{k=1}^{n}a_{ik}\circ b_{kj}=\sum_{k=1}^{n}b_{kj}a_{ik},$$

定理1.4 设R是含幺环，E是具有n元基的自由左 R-模。则有环同构

$$\mathrm{Hom}_R(E,\ E)\cong\mathrm{Mat}_n(R^{op}).$$

特别地，对于体R上每个 n 维向量空间，均存在这种同构（这时R^{op}也是体）。

注记：如果R为交换环，则$R=R^{op}$。这时可以将定理1.4的结论叙述得更漂亮些。

定理1.4的证明 设$\phi:\mathrm{Hom}_R(E,\ E)\to\mathrm{Mat}_n(R)$是反同构，即将每个$f$映成它对于给定基的矩阵。验证映射$\psi:\mathrm{Mat}_n(R)\to\mathrm{Mat}_n(R^{op})$，$\psi(A)=A^t$是环的反同构。于是合成映射$\psi\phi:\mathrm{Hom}_R(E,\ E)\leftarrow\mathrm{Mat}_nR^{op}$是环同构。定理的最后命题是定理 IV.2.4 和习题III.1.17的推论。∎

设R是含幺环，$A\in\mathrm{Mat}_n(R)$，我们称A是可逆的或者非异的，是指存在$B\in\mathrm{Mat}_n(R)$，使得$AB=I_n=BA$。不难看出，逆矩阵B如果存在则必唯一。通常将它记成A^{-1}。显然 $B=A^{-1}$也是可逆的，

并且 $(A^{-1})^{-1}=A$。两个可逆矩阵的乘积 AC 也是可逆的，并且 $(AC)^{-1}=C^{-1}A^{-1}$。如果A是交换环上的可逆矩阵，则 A^t也是可逆的，并且$(A^t)^{-1}=(A^{-1})^t$。(习题1)。

自由R-模同态的矩阵显然与定义域和值域中（有序）基的选取均有关系。所以我们需要知道表示同一映射对于两组不同的有序基的矩阵之间的关系。

引理1.5 设R是含幺环，E和F是分别以U和V为有序基的自由左R-模，其中 $|U|=n=|V|$。设 $A\in \mathrm{Mat}_n R$。则 A 是可逆的 $\Longleftrightarrow A$是某个同构$f:E\to F$对于U和V的矩阵。并且在这种情形下，f^{-1}对于V和U的矩阵是A^{-1}。

证明概要 R-模同态$f:E\to F$是同构$\Longleftrightarrow$存在R-模同态 $f^{-1}:F\to E$，使得$f^{-1}f=1_E, ff^{-1}=1_F$。(见定理I.2.3)。假设f是同构，它对于U和V的矩阵为A，令B是f^{-1}对于V和U 的矩阵。于是我们可绘成

$$\begin{array}{ll} \text{映射：} & f \quad f^{-1} \\ \text{模：} & E\to F\to E \\ \text{基：} & U \quad V \quad U \\ \text{矩阵：} & A \quad B \end{array}$$

根据定理1.3，AB是$f^{-1}f=1_E$对于U的矩阵。但是I_n 显然是 1_E对于U的矩阵。从而由定理1.2的证明可知$AB=I_n$。类似的$BA=I_n$，从而A是可逆的并且$B=A^{-1}$。反方向的推导留给读者作为练习。∎

定理1.6 设R为含幺环。E和F是自由左R-模，并且U 和V分别是它们的有限有序基，$|U|=n$，$|V|=m$。令$f\in \mathrm{Hom}_R(E,F)$对于U和V的$n\times m$矩阵为A。则f对于E 和F 的另两组有序基的矩

阵为B⟺存在可逆矩阵P和Q，使得$B=PAQ$.

证明（⟹）：如果B是f对于E的基U'和F的基V'的$n\times m$矩阵，则$|U'|=n$，$|V'|=m$。令P是恒等映射1_E对于有序基U'和U的$n\times n$矩阵。由引理1.5可知P是可逆的。类似地，令Q是1_F对于V和V'(注意次序!)的$m\times m$矩阵。我们可以绘成

$$\begin{array}{ll} \text{映射：} & \quad 1_E \quad\quad f \quad\quad 1_F \\ \text{模：} & E\longrightarrow E\longrightarrow F\longrightarrow F \\ \text{基：} & U' \quad U \quad\quad V \quad\quad V' \\ \text{矩阵：} & \quad\quad P \quad A \quad\quad Q \end{array}$$

根据定理1.3，$f=1_Ff1_E$对于U'和V'的矩阵恰好是PAQ。从而由定理1.2的证明可知$B=PAQ$.

（⟸）：如上给定U,V,f,A和$B=PAQ$，其中P和Q是可逆的。令$g:E\to E$，$h:F\to F$均是同构，使得g对于U的矩阵是P，h对于V的矩阵是Q^{-1}。(引理1.5)。如果$U=\{u_1,\cdots,u_n\}$，则$g(U)=\{g(u_1),\cdots,g(u_n)\}$也是$E$的一组有序基，并且$P$是$1_E$对于有序基$g(U)$和$U$的矩阵。类似地，$Q^{-1}$是$1_E$对于有序基$h(V)$和$V$的矩阵，于是$Q=(Q^{-1})^{-1}$是$1_F$对于$V$和$h(V)$的矩阵(引理1.5)。我们可以绘成：

$$\begin{array}{ll} \text{映射：} & \quad 1_E \quad\quad f \quad\quad 1_F \\ \text{模：} & E\longrightarrow E\longrightarrow F\longrightarrow F \\ \text{基：} & g(U)\ U \quad\quad V \quad h(V) \\ \text{矩阵：} & \quad\quad P \quad A \quad\quad Q \end{array}$$

根据定理1.3，$f=1_Ff1_E$对于有序基$g(U)$和$h(V)$的矩阵为$PAQ=B$. ∎

系1.7 设R是含幺环。E是具有有序基U的自由左R-模，其中$|U|=n$(有限)。令A是$f\in \mathrm{Hom}_R(E,E)$对于U的$n\times n$矩阵。则f对于E的另一组有序基的$n\times n$矩阵为B⟺存在某个可逆矩阵P使

得$B=PAP^{-1}$。

证明概要 在定理1.6中如果$E=F$，$U=V$，$U'=V'$，则由引理1.5可知$Q=P^{-1}$。∎

定义1.8 设R为含幺环。两个方阵$A,B\in \mathrm{Mat}_n R$叫做相似的，是指存在可逆方阵P，使得$B=PAP^{-1}$。两个$n\times m$矩阵C，D叫做等价的，如果存在可逆方阵P和Q，使得$D=PCQ$。

于是可以用等价和相似的术语将定理1.6和系1.7重新加以叙述。等价和相似均是等价关系(习题7)，我们将在第2节和第4节对它们作更详细的研究。

在本节的最后我们讨论右模和对偶性问题。

如果R是交换环，则上述诸结果对于右R-模也同样是对的。但是在一些重要情形下R不是交换的（例如体上的向量空间)。为了对非交换环上的右模证明定理1.3的类比，有必要以某种少许不同的方式定义同态的矩阵。

设R是含幺环。E和F为自由右R-模，并且分别以$U=\{u_1,\cdots,u_n\}$和$V=\{v_1,\cdots,v_m\}$为有限有序基。我们将同态$f\in \mathrm{Hom}_R(E,F)$对于U和V的矩阵定义为$m\times n$矩阵(注意行与列的数目)：

$$\begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ s_{m1} & s_{m2} & \cdots & s_{mn} \end{pmatrix}$$

其中$s_{ij}\in R$由下列方程组唯一确定：

$$\begin{aligned} f(u_1) &= v_1 s_{11} + v_2 s_{21} + \cdots + v_m s_{m1} \\ &\vdots \\ f(u_n) &= v_1 s_{1n} + v_2 s_{2n} + \cdots + v_m s_{mn}。 \end{aligned}$$

因此$f(u_j)$对于有序基V的系数是f的$m\times n$矩阵(s_{ij})的第j列(与定

理1.2的证明比较)。

f的作用可以用矩阵来刻划：设 $u=u_1x_1+u_2x_2+\cdots+u_nx_n$ ($x_i\in R$)是E中任意元素，X是$n\times 1$矩阵（或叫作列向量）$\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$。令$A$是$f$对于基$U$和$V$的矩阵。则$f(u)=v_1y_1+v_2y_2+\cdots+v_my_m$，其中 $y_i\in R$并且$\begin{pmatrix}y_1\\ \vdots\\ y_m\end{pmatrix}$是$m\times 1$矩阵(列向量)$AX$。

现在不难证明定理1.2—1.5的类比。特别地：

定理1.9 设R是含幺环。E和F是自由右 R-模，并且分别具有n元和m元的有限基U 和V。令N是由R上全体$m\times n$ 矩阵组成的右R-模。则

(i) 存在Abel群同构$\mathrm{Hom}_R(E,F)\cong N$。并且当$R$是交换环时，它也是右$R$-模同构。

(ii) 设 G 为自由右 R-模，并且有 p元有限基W。如果$f\in\mathrm{Hom}_R(E,F)$(对于U和V)的$m\times n$矩阵是A，$g\in\mathrm{Hom}_R(F,G)$(对于V和W)的$p\times m$矩阵是B，则$gf\in\mathrm{Hom}_R(E,G)$(对于U和W)的$p\times n$矩阵是BA。

(iii) 存在环同构$\mathrm{Hom}_R(E,E)\cong\mathrm{Mat}_nR$。

证明 作为练习。见定理1.2—1.4。注意对于右模，(iii)是同构而不是反同构。∎

命题1.10 设R是含幺环，$f:E\to F$是有限生成自由左R-模的同态。如果A是f对于(有序)基U和V的矩阵，则A也是自由右 R-模对于对偶基V^* 和U^* 的同态 $\bar{f}:F^*\to E^*$的矩阵。

注记：对偶映射与对偶基的定义见定理IV.4.10和 IV.4.11.

如果R是交换环（例如是域）习惯上将左R-模M的对偶M^*也看成是左R-模(即$rm^*=m^*r$，对于$r\in R$，$m^*\in M^*$)。这时，对偶映射$\bar{f}$的矩阵是转置矩阵A^t(习题8)。

命题1.10的证明 回忆：$F^*=\mathrm{Hom}_R(F,R)$的对偶基$V^*=\{v_1^*,\cdots,v_m^*\}$由

$$v_i^*(v_j)=\delta_{ij}\quad(\text{Kronecker 符号，}1\leqslant i,\ j\leqslant m)$$

所确定。对于E^*的对偶基$U^*=\{u_1^*,\cdots,u_n^*\}$则是类似的（定理IV.4.11)。根据右模同态的矩阵的定义，我们需要证明：对于每个$j=1,2,\cdots,m$，$\bar{f}(v_j^*)=\sum_{i=1}^{n}u_i^*r_{ij}$，其中$A=(r_{ij})$是$f:E\to F$对于$U$和$V$的$n\times m$矩阵。由于上述方程两边均是映射$E\to R$，只需检查它们在每个$u_k\in U$上的作用即可。根据定理IV.4.10我们有：

$$\bar{f}(v_j^*)(u_k)=v_j^*(f(u_k))=v_j^*\Big(\sum_{i=1}^{m}r_{ki}v_i\Big)=\sum_{i=1}^{m}r_{ki}v_j^*(v_i)$$

$$=r_{kj}.$$

另一方面，

$$\Big(\sum_{i=1}^{n}u_i^*r_{ij}\Big)(u_k)=\sum_{i=1}^{n}u_i^*(u_k)r_{ij}=r_{kj}.\ \blacksquare$$

习　题

注：所有矩阵均是含幺环R上的矩阵。

1. 设R是交换环。

(*a*) 如果乘积AB可以定义，则乘积B^tA^t也可以定义，并且$(AB)^t=B^tA^t$。

(*b*) 如果A可逆，则A^t也可逆，并且$(A^t)^{-1}=(A^{-1})^t$。

(*c*) 如果R不是交换环，则(*a*)和(*b*)可能不成立。

2. 矩阵$(a_{ij})\in \mathrm{Mat}_n R$叫作（上）三角矩阵，是指$a_{ij}=0$（当$j<i$时）。叫作严格三角矩阵，是指$a_{ij}=0$(当$j\leqslant i$时)。

证明对角矩阵集合是$\mathrm{Mat}_n R$的子环，并且(环)同构于$R\times\cdots\times R$(n个)。证明三角矩阵集合T是$\mathrm{Mat}_n R$的子环，而严格三角矩阵集合I是T的理想。试决定商环T/I。

3. (*a*) 环$\mathrm{Mat}_n R$的中心为 $\{rI_n \mid r$属于R的中心$\}$。[提示：$\mathrm{Mat}_n R$的中心中的每个矩阵必然与每个矩阵$B_{r,s}$可换，其中$B_{r,s}$在(r,s)处为1_R，而其余地方均是0。]

(*b*) $\mathrm{Mat}_n(R)$的中心同构于R的中心。

4. R上全体$m\times n$矩阵组成的集合是具有mn个元素的基的自由R-模。

5. 矩阵$A\in \mathrm{Mat}_n R$叫作对称的，是指$A=A^t$。叫作斜对称的，是指$A=-A^t$。

(*a*) 如果A和B是对称的(或者斜对称的)，则$A+B$也是对称的（或者是斜对称的)。

(*b*) 设R为交换环。如果A和B是对称的，则AB是对称的$\Longleftrightarrow AB=BA$。再证：对于任意矩阵$B\in \mathrm{Mat}_n R$，$BB^t$和$B+B^t$是对称的，而$B-B^t$是斜对称的。

6. 如果R是体，$A,B\in \mathrm{Mat}_n R$，并且$BA=I_n$，则$AB=I_n$，从而$B=A^{-1}$。[提示：利用线性变换]。

7. 矩阵相似是$\mathrm{Mat}_n R$上的等价关系。在R上全体$m\times n$矩阵所组成的集合中，矩阵等价是等价关系。

8. 设E和F是域上有限维(左)向量空间，并且象通常那样将对偶空间看成是左向量空间。如果A是线性变换$f:E\to F$的矩阵，则对偶映射$\overline{f}:F^*\to E^*$的矩阵为A^t。

2. 秩和等价

本节的主要目的是研究体上或者主理想整环上矩阵等价的充要条件. 其中一个充要条件与秩的概念有关. 此外，我们还给出等价矩阵的标准型（定理2.6和命题2.11）. 最后，叙述求这些标准型的实际方法以及计算体上可逆矩阵的逆的方法. 附录中考虑了这个方法在有限生成 Abel 群上的应用，这一附录今后不需要.

定义2.1 设$f:E\to F$是体D上(左) 向量空间的线性变换. 我们将$\mathrm{Im}f$的维数叫做f的秩 (rank). 而 $\mathrm{Ker}\,f$的维数叫做f的脐 (nullity).

注记：如果$f:E\to F$如定义2.1所示，由系 IV.2.14可知 (f的秩) + (f的脐) = $\dim_D E$.

如果R是含幺环，n是正整数，则R^n表示自由R-模 $R\oplus\cdots\oplus R$ (n个). R^n的标准 (有序) 基是指 $\{\varepsilon_1=(1_R,0,\cdots,0),\ \varepsilon_2=(0,1_R,0,\cdots,0),\cdots,\varepsilon_n=(0,\cdots,0,1_R)\}$.

定义2.2 含幺环R上一个$n\times m$矩阵 A的行空间(或列空间)是由A的诸行 (或者诸列，分别看作是R^m和R^n中的元素) 所生成的自由左 (或者右) 模R^m(或者R^n)的子模. 如果R是体，则 A的行空间 (或者列空间) 的维数叫作是A 的行秩 (列秩).

定理2.3 如果 $f:E\to F$是体D 上有限维左 (或者右) 向量空

间，A是f对于某两组基的矩阵，则f的秩等于A 的行秩（或者列秩）。

注记：从右向量空间映射的矩阵的定义方式可知，对于右向量空间，则“行秩”要改成“列秩”。

定理2.3的证明 设A是f对于E的基$U=\{u_1,\cdots,u_n\}$和 F的基$V=\{v_1,\cdots,v_m\}$的$n\times m$(或者$m\times n$) 矩阵。这时，在通常的同构$F\cong D^m$，$\sum_i r_i v_i \longmapsto (r_1,\cdots,r_m)$之下，元素$f(u_1),\cdots,f(u_n)$ 映到A的诸行（或者诸列）之上（看成是D^m中的向量)。由于$\mathrm{Im}f$ 是由$f(u_1,\cdots,u_n)$所张成的，$\mathrm{Im}f$同构于A的行空间（或者列空间)，从而f的秩等于A的行秩（或者列秩)。∎

现在我们要证明体上矩阵的行秩等于列秩。我们在系 2.5 中证明这一事实，但是这对于理解后面的内容不是重要的，因为此后我们实际上只用“行秩”。

命题2.4 体D 上有限维左向量空间的每个线性变换 $f:E\to F$均与它的对偶映射 $\bar{f}:F^*\to E^*$ 有相同的秩。

对偶映射定义于定理IV.4.10.

证明 设$\mathrm{rank}f=r$.由系IV.2.14可知存在基$X=\{u_1,\cdots,u_n\}$，使得$\{u_{r+1},\cdots,u_n\}$是$\mathrm{Ker}\,f$的基而$Y_1=\{f(u_1),\cdots f(u_r)\}$是 $\mathrm{Im}\,f$的基。将Y_1扩充成F的基$r=\{t_1=f(u_1),\cdots,t_r=f(u_r),\ t_{r+1},\cdots,t_m\}$。考虑$E^*$和$F^*$的对偶基$X^*$和$Y^*$(定理IV.4.11)。对于每个$i=1,2,\cdots,m$,验证

$$f(t_i^*)(u_j)=t_i^*(f(u_j))=\begin{cases}t_i^*(t_j)=\delta_{ij}, & \text{如果}1\leqslant j\leqslant r.\\ t_i^*(0)=0, & \text{如果}r+1\leqslant j\leqslant n.\end{cases}$$

其中δ_{ij}是Kronecker 符号。于是对于$1\leqslant j\leqslant n$均有

$$\bar{f}(t_i^*)(u_j)=\begin{cases}\delta_{ij}=u_i^*(u_j), & \text{如果}1\leqslant i\leqslant r.\\ 0, & \text{如果}r+1\leqslant i\leqslant m.\end{cases}$$

从而当 $1\leqslant i\leqslant r$ 时 $\bar{f}(t_i^*)=u_i^*$，而当 $r+1\leqslant i\leqslant m$ 时 $\bar{f}(t_i^*)=0$.但是$\mathrm{Im}\bar{f}$ 是由 $\bar{f}(r^*)$张成的，从而也是由$\{u_1^*,\cdots,u_r^*\}$ 张成的。由于$\{u_1^*,\cdots,u_r^*\}$是X^*的子集。它在E^*中是线性无关的.因此$\{u_1^*,\cdots,u_r^*\}$是 $\mathrm{Im}\bar{f}$ 的一组基，从而$\mathrm{rank}\bar{f}=r=\mathrm{rank}f$。 ∎

系2.5 如果A是体D上$n\times m$矩阵,则A的行秩等于A 的列铁。

证明 设$f:D^n\to D^m$是左向量空间的线性变换，它对于标准基的矩阵是A。则右向量空间之间的对偶映射 $\bar{f}$ 的矩阵也是A （命题1.10） 由定理2.3和命题2.4即知 A 的行秩 $=\mathrm{rank}f=\mathrm{rank}\bar{f}=$ A的列秩。 ∎

注记：由系2.5立刻推出：对于域上任意矩阵A，A的行秩 $=$ A'的行秩。

根据系2.5,我们今后将略去“行”或者“列”字，而简述为体上矩阵的秩。

在下面定理2.6中，体 D 上矩阵的等价用秩和如下一些矩阵来刻划。如果m，n为正整数，则$E_0^{n,m}$定义为 $n\times m$ 零矩阵。对于每个$r(1\leqslant r\leqslant\min(n,m))$，$E_r^{n,m}$定义为如下的$n\times m$矩阵：它的前$r$行为$D^m$中的标准基向量$\varepsilon_1,\cdots,\varepsilon_r$，而其余行均是零。即

$$E_r^{n,m}=\begin{pmatrix}1_R & 0 & 0 & \cdots & & \cdots & 0\\ 0 & 1_R & 0 & \cdots & & \cdots & 0\\ \vdots & & & & & & \vdots\\ 0 & \cdots & & 0 & 1_R & 0 & \cdots & 0\\ 0 & \cdots & & 0 & 0 & 0 & \cdots & 0\\ \vdots & & & & & & & \vdots\\ 0 & \cdots & \cdots & & & & & 0\end{pmatrix}=\begin{pmatrix}I_r & 0\\ 0 & 0\end{pmatrix}$$

显然$\operatorname{rank} E_r^{n,m}=r$。此外，如果$E_r^{n,m}$是自由$R$-模$E$，$F$对于$E$的基$\{u_1,\cdots,u_n\}$和$F$的基$\{v_1,\cdots,v_m\}$的$R$-模同态$f:E\to F$的矩阵，则

$$f(u_i)=\begin{cases}v_i, & \text{如果}1\leqslant i\leqslant r\\ 0, & \text{如果}r+1\leqslant i\leqslant n.\end{cases}$$

由定理1.6和下面定理2.6直接推出：有限维向量空间的每个线性变换对于适当的两组基具有上述简单形式（习题6）。

所谓集合X上等价关系R的一个标准型集合是指X的一个子集合C，使得每个R-等价类在C中恰包含一个元素。换句话说，对于每个$x\in X$，存在唯一的$c\in C$，使得x和c是R等价的。我们现在证明：矩阵集合$\{E_r^{n,m}\}$形成体上全部$n\times m$矩阵对于矩阵等价的标准型集合。

定理2.6 设M是体D上全部$n\times m$矩阵所组成的集合。令A，$B\in M$。

(i) A等价于$E_r^{n,m}\Longleftrightarrow\operatorname{rank}A=r$。

(ii) A等价于$B\Longleftrightarrow\operatorname{rank}A=\operatorname{rank}B$。

(iii) 矩阵集合$\{E_r^{n,m}\mid 1\leqslant r\leqslant\min(n,m)\}$[注]是$M$对于矩阵等价的标准型集合。

证明概要 (i) 根据定理1.2，A是某个线性变换$f:D^n\to D^m$对于某两组基的矩阵。如果$\operatorname{rank}A=r$，则系IV.2.14推出存在D^n的基$U=\{u_1,\cdots,u_n\}$和D^m的基$V=\{v_1,\cdots,v_m\}$，使得$f(u_i)=v_i$ $(1\leqslant i\leqslant r)$，而$f(u_i)=0$ $(r+1\leqslant i\leqslant n)$。$f$对于$U$和$V$的矩阵显然是$E_r^{n,m}$，因此由定理1.6便知$A$与$E_r^{n,m}$等价。反之，假设$A$等价于$E_r^{n,m}$，由定理1.6可知存在线性变换$g:D^n\to D^m$，使得$A$是$g$对于两组基的矩阵，而$E_r^{n,m}$是$g$对于另两组基的矩阵。从而由定理2.3可知$\operatorname{rank}A$

[注]：应为$0\leqslant r\leqslant\min(n,m)$。证明也要作微小的修改。——译者

$= \mathrm{rank}g = \mathrm{rank}E_r^{n,m} = r$。由(i)即可推出(ii)和(iii)。∎

下面一些定义，定理和系具有一系列有益的推论，其中还给出实际方法来构作：

(i) 主理想整环上矩阵的等价标准型（命题2.11）；

(ii) 体上矩阵的等价标准型$E_r^{n,m}$；

(iii) 体上可逆矩阵的逆（命题2.12）。

命题2.11只是在下面证明命题4.9时使用.其他内容均与命题2.11无关并且今后是不需要的。

我们常常将环R上一给定$n\times m$矩阵的诸行（或者诸列）看作是R^m(或者是R^n)中元素。因此我们可以谈：将一行（或者一列）乘以某标量再加到另一行上（或者列上）。例如

$$r(a_1,a_2,\cdots,a_m)+(b_1,b_2,\cdots,b_m)$$
$$=(ra_1+b_1,\cdots,ra_m+b_m)。$$

定义2.7 设A是含幺环R上的矩阵。下列诸项均叫作A上的初等行变换：

(i) 交换A的两行；

(ii) 将A的一行左乘以单位$c\in R$；

(iii) 对于$r\in R$，$i\neq j$，将第j行左乘以r加到第i行之上。

类似地定义A上的初等列变换((ii)和(iii)中的左乘均改成右乘)。将单位矩阵I_n恰好进行一次初等行（或列）变换所得的矩阵叫作$n\times m$的初等（变换）矩阵。

定理2.8 设A是含幺环R上的$n\times m$矩阵。E_n(或者E_m)是I_n(或者I_m)上进行初等行（或者列）变换T而得到的初等矩阵。则E_nA(或者AE_m)是A上作用T而得到的矩阵。

证明作为练习. ∎

系2.9 含幺环R上每个$n\times n$初等矩阵E都是可逆的，并且其逆也是初等矩阵.

证明概要 验证可以从E经一个初等行变换T得到I_n. 如果F是T作用于I_n上而得到的初等矩阵，由定理2.8可知$FE=I_n$，直接验证$EF=I_n$. ∎

系2.10 如果B是含幺环R上一个$n\times m$矩阵A经过有限次初等行变换或者初等列变换而得到的矩阵，则B与A等价.

证明 由于从A得到B的每个行（或者列）运算均是左乘(或者右乘）一个适当的初等矩阵（定理2.8)，从而$B=(E_p\cdots E_1)\cdot A(F_1\cdots F_q)=PAQ$,其中每个$E_i$和$F_j$均是初等矩阵,而$P=E_p\cdots E_1$，$Q=F_1\cdots F_q$. P和Q是可逆矩阵之乘积（系2.9)，从而均是可逆的. ∎

现在我们考虑主理想整环R上矩阵等价的标准型. 根据系IV.2.12，R上自由模的秩是一个可定义的不变量. 由于自由R-模的每个子模也是自由的（定理IV.6.1),我们可以将自由R-模同态$f: E\to F$的秩定义为$I_m f$的秩. 而类似地将R上矩阵A的行秩定义为行空间A的秩（见定义2.2). 不难看出，定理2.3的证明在这里仍然有效.从而有限生成自由R-模之间的映射f的秩是f对于任意两组基的矩阵的行秩. 于是，如果A等价于矩阵B，则A的行秩等于B的行秩. 这是根据定理1.6,A和B分别是同一同态$f: R^n\to R^m$对于不同的两组基的矩阵，从而A的行秩$=B$的行秩. 下面是定理2.6对于主理想整环上矩阵的类似结果.

命题2.11 如果A是主理想整环R上的 $n\times m$ 矩阵并且秩 $r>0$，则 A等价于形如$\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$的矩阵，其中$L_r$是$r\times r$ 的对角方阵，并且具有非零对角元素$d_1,\cdots,d_r$，而且$d_1|d_2|\cdots|d_r$。R中理想(d_1)，$\cdots,(d_r)$是由A的等价类所唯一确定的。

注记：这个命题对于主理想整环上 $n\times m$ 矩阵的等价给出一个标准型集合（习题5)。如果R是欧氏整环，则由下面的证明，习题5与定理2.8，可知矩阵$\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$可以由$A$通过有限次初等行变换或者初等列变换而得到。

命题2.11的证明概要 (i)回忆：$a,b\in R$ 是相伴的，是指$a|b$并且$b|a$。根据定理III.3.2，a和b相伴$\Longleftrightarrow a=bu$，其中u 是单位。我们称$c\in R$是$a\in R$的真因子，是指$c|a$，并且c与a不相伴（即$a\nmid c$)。元素 a 的两个因子c_1和c_2叫作是不同的，是指的c_1和c_2不相伴（这在语言上有少许混乱)。现在根据定理 III.3.7 可知R是唯一因子分解整区。如果$a=p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$(其中$p_i$是不同的不可约元素，而$n_i>0$)，则$a$的每个因子均相伴于形如$p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$的元素，其中$0\leqslant k_i\leqslant n_i(1\leqslant i\leqslant t)$。于是，$R$ 的非零元素只有限多个不同的真因子。

(ii) 如果a和b是R中非零元素，令c是它们的最大公因子。根据定义III.3.10和定理III.3.11可知存在$r,s\in R$，使得$ar+bs=c$；$ca_1=a$，$cb_1=b$，从而$a_1r+b_1s=1_R$而 $ba_1-ab_1=0$。于是$m\times m$方阵

$$T=\begin{pmatrix} r & -b_1 & 0 \\ s & a_1 & \\ 0 & 0 & I_{m-2} \end{pmatrix}$$

是可逆的，并且其逆是

$$T^{-1}=\begin{pmatrix} a_1 & b_1 & \\ -s & r & 0 \\ 0 & 0 & I_{m-2} \end{pmatrix}$$

如果A的第1行是$(a,b,a_{13},\cdots a_{1m})$，则$A$等价于$AT=I_nAT$，其中第1行是$(c,0,a_{13},\cdots,a_{1m})$。如果$A$的第1列是$(a,d,a_{31},\cdots,a_{n1})^t$，[注]类似的过程得到一个可逆方阵$S$，使得$A$等价于$SA$，而$AS$的第1列为$(e,0,a_{31},\cdots,a_{n1})^t$，其中$e$是$a$和$d$的最大公因子。这种方阵$S$或者$T$叫作是辅助方阵。

(iii) 由于$A\neq 0$，适当交换一些行或者列，以及用辅助矩阵去右乘A，就可将A变为A_1，而A_1的第1行为$(a_1,0,\cdots,0)$，其中$a_1\neq 0$。由(ii)和系2.10可知A等价于A_1。

(iv) 如果a_1可除尽A_1的第1列中全部元素，则有限次初等行运算即可将A_1变为矩阵

$$B=\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2m} \\ \vdots & & & \\ 0 & b_{n2} & \cdots & b_{nm} \end{pmatrix},$$

由系2.10可知B等价于A_1，从而也等价于A。

(V) 如果a_1不能除尽A_1的第1列中某元素b，则经过一系列交换行或者列的运算以及左乘辅助矩阵，可将A_1变成A_2，其中A_2的第1列是$(a_2,0,\cdots,0)^t$，而a_2是a_1和b的最大公因子(见(ii))。注意A_2的第1行可能有许多非零元素。但是由于$a_2\mid a_1,a_2\mid b$并且$a_1\nmid b$，从而由(i)知a_2是a_1的真因子。A_2等价于A_1，于是由(ii)

[注] 为了印刷方便，我们常常将$n\times 1$列向量写成$1\times n$行向量的转置。

例如$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}=(a_1,a_2)^t$。

和系2.10可知也等价于A。

(vi) 如果a_2除尽A_2的第1行中每个元素，则通过一系列初等列运算可得到一个与A等价的矩阵，它有形如B的一般形式。

(vii) 如果a_2不能除尽A_2的第1行中某个元素k，重复(iii)可得到一个等价于A的矩阵A_3，A_3的第1行为$(a_3,0,\cdots,0)$，而a_3是a_2和k的公因子。A_3在第1列可能有非零元素。但是由于$a_3 \mid a_2$，$a_3 \mid k$并且$a_2 \nmid k$，从而由(i)知a_3是a_2的真因子。此外，由(v)知a_2和a_3是a_1的不同的真因子。A_3等价于A_2，从而由(ii)和系2.10可知也等价于A。

(viii) 由于a_1只有有限多个不同的真因子，重复有限多次(iii)－(vii)，必定得到一个等价于A的矩阵C，它有如下的形式：

$$C=\begin{pmatrix} s_1 & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & & \vdots \\ 0 & c_{n2} & \cdots & c_{nm} \end{pmatrix}$$

其中$s_1 \neq 0$。

(ix) 如果s_1不能除尽某个c_{ij}，将第i行加到第1行上然后重复(iii)—(viii)。结果得到一个等价于A的矩阵D，D与C有同样的形式，只是它在(1，1)处的元素s_2是s_1和c_{ij}的公因子，所以是s_1的真因子。

(x) 如果s_2不能除尽D中全部元素，重复(ix)即给出一个等价于A的矩阵，它与C有同样的形式，但是在(1,1)处的元素s_3又是s_2的真因子。从而s_2和s_3是s_1的不同真因子。由于s_1只有有限多个不同的真因子，从而重复有限次这个过程之后，必然得到一个矩阵，它等价于A，与C有同样的形式，并且在(1.1)处的元素除尽此矩阵中全部其他元素。

(xi) 采用归纳法和(x)可证A等价于对角矩阵$F=\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$，并且满足定理中所述的条件。由于$F$的秩显然是$r$，由定理2.6即知$A$的秩是$r$。

(xii) **（唯一性）** 设A和F如(xi)中所示，其中L_r的对角元素为$d_1,\cdots,d_r$。假设M是等价于A的矩阵（从而rank $M=r$），而N是形如$\begin{pmatrix} L_r' & 0 \\ 0 & 0 \end{pmatrix}$的等价于$M$的矩阵，其中$L_r'$是$r\times r$的对角方阵，并且对角元素$k_i$均不为0，而且$k_1\mid k_2\mid\cdots\mid k_r$。由定理1.2知$F$是同态$f:R^n\to R^m$对于$R^n$中基$\{u_1,\cdots,u_n\}$和$R^m$中基$\{v_1,\cdots,v_m\}$的矩阵。因此$f(u_i)=d_iv_i(1\leqslant i\leqslant r)$，$f(u_i)=0\,(r+1\leqslant i\leqslant n)$，从而$\mathrm{Im}f=Rd_1v_1\oplus\cdots\oplus Rd_rv_r$。根据系I.8.11对于模的类似结果可知

$$R^m/\mathrm{Im}f=R_{v_1}/Rd_1v_1\oplus\cdots\oplus R_{v_r}/Rd_rv_r\oplus R\oplus\cdots\oplus R$$

$$\cong R/(d_1)\oplus\cdots\oplus R/(d_r)\oplus R\oplus\cdots\oplus R$$

（m个直和分量，$d_1\mid d_2\mid\cdots\mid d_r$）。

根据假设，F等价于N。由定理1.6知N是f对应于另两组基的矩阵。重复上述推理可证$R^m/\mathrm{Im}f\cong R/(k_1)\oplus\cdots\oplus R/(k_r)\oplus R\oplus\cdots\oplus R$（$m$个直和分量，$k_1\mid k_2\mid\cdots\mid k_r$）。根据主理想整环上模的结构定理IV.6.12即知$(d_i)=(k_i)(1\leqslant i\leqslant r)$。∎

将命题2.11的证明技术加以简化，即可用来得到体D上$n\times m$矩阵A的标准型$E_r^{n,m}$。如果$A=0=E_0^{n,m}$，则没什么可作的。如果a_{ij}是A中非零元素，将第i行和第1行交换，再将第j列和第1列交换，就将a_{ij}移到(1,1)位置上。将第1行乘以a_{ij}^{-1}使第1行变成$(1_R,c_2,\cdots,c_m)$。将其余诸行减去第1行的适当倍数，再对列作类似事情，即得到如下形式的矩阵：

$$\begin{pmatrix} 1_R & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & c_{2m} \\ \vdots & & & \\ 0 & c_{n2} & \cdots & c_{nm} \end{pmatrix}$$

如果c_{ij}均为0，则事毕。如果某个$c_{ij} \neq 0$，则在$(n-1)\times(m-1)$子阵(c_{ij})上重复上述过程。由于在第2—n行和列上的运算对于第1行和第1列没有影响，我们得到

$$\begin{pmatrix} 1_R & 0 & 0 & \cdots & 0 \\ 0 & 1_R & 0 & \cdots & 0 \\ 0 & 0 & d_{33} & \cdots & d_{3m} \\ \vdots & & & & \\ 0 & 0 & d_{n3} & \cdots & d_{nm} \end{pmatrix}$$

继续下去便得到矩阵 $\mathrm{E}_r^{n,m}$（对于某个r）。根据系2.10，A等价于$E_r^{n,m}$，从而$\mathrm{rank}A = r$，而由定理2．6即知$E_r^{n,m}$是A的等价标准型。

将上面技巧稍加修改，即可用来求可逆矩阵的逆，这从下一命题的证明中即可明白。

命题2.12 关于体D上$n\times n$方阵A的以下诸条件是彼此等价的。

(i) $\mathrm{rank}A = n$;

(ii) A等价于单位矩阵I_n;

(iii) A是可逆的;

(iv) A是一些初等变换矩阵的乘积。

证明概要 (i)$\Longleftrightarrow$(ii)：根据定理2.6(因为$E_n^{n,n} = I_n$)。

(i)$\Rightarrow$(iii)：由于A的秩为n，因此A的n行必然线性无关（见定理Ⅳ.2.5和定义2.2)。于是$A = (a_{ij})$的第1行不是零向量，即

对于某个j，$a_{1j}\neq 0$。交换第j列和第1列，然后将新的第1列乘以a_{1j}^{-1}。从其余诸列减去第1列的适当倍数则给出矩阵

$$B=\begin{pmatrix} 1_D & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & & & \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

由系2.10知B等价于D。归纳下去，我们可以假设有一系列初等列变换将A变成（从而等价于）矩阵

$$C=\begin{pmatrix} I_{k-1} & & 0 & \\ c_{k} & \cdots & c_{kk} & \cdots & c_{kn} \\ \vdots & & & \\ c_{n1} & \cdots & c_{nk} & \cdots & c_{nn} \end{pmatrix}$$

必有某个$j\geq k$，使得$c_{kj}\neq 0$，因不然则第k行便是前$k-1$行的线性组合，这就与$\mathrm{rank}C=\mathrm{rank}A=n$相矛盾（定理2.6）。交换第$j$列和第$k$列，并将新的第$k$列乘以$c_{kk}^{-1}$，然后将其余诸列中减去第$k$列的适当倍数。结果给出等价于$A$的矩阵$D$（系2.10）：

$$D=\begin{pmatrix} & I_k & & 0 & \\ d_{k+1} & \cdots & d_{k+1\,k+1} & \cdots & d_{k+1\,n} \\ \vdots & & & & \\ d_{n1} & \cdots & d_{nk+1} & \cdots & d_{nn} \end{pmatrix}$$

这就完成了归纳推理，从而证明了$k=n$时也成立，即A通过有限次初等列变换即可变成I_n。于是由定理2.8可知$A(F_1F_2\cdots F_t)=I_n$，其中每个F_i都是初等矩阵。根据习题1.7即知矩阵$F_1F_2\cdots F_t$是A的双侧逆元素，所以A是可逆的。

(i)⇒(iv)：利用系2.9和$A=F_t^{-1}\cdots F_2^{-1}F_1^{-1}$即得证。

(iii)⇒(i)：由引理1.5和定理2.3。

(iv)⇒(iii)：由系2.9。∎

注记：由(i)⇒(iii)的证明可知$A^{-1}=F_1F_2\cdots F_t$可以用将A变I_n的同样一系列初等列变换得到.通常用这种方法计算逆矩阵要比行列式方法（第3节）方便.

附录：用生成元集合和关系集合所定义的Abel群

Abel群G叫作由生成元$a_1,\cdots,a_m(a_i\in G)$和关系

$$\begin{aligned}
&r_{11}a_1+r_{12}a_2+\cdots+r_{1m}a_m=0\\
&r_{21}a_1+r_{22}a_2+\cdots+r_{2m}a_m=0\\
&\vdots\\
&r_{n1}a_1+r_{n2}a_2+\cdots+r_{nm}a_m=0
\end{aligned}$$

所定义的，指的是$G\cong F/K$，其中F是集合$\{a_1,\cdots,a_m\}$上的自由Abel群，K是由$b_i=r_{i1}a_1+\cdots+r_{im}a_m(1\leqslant i\leqslant n)$所生成的子群.注意同一记号$a_i$既表示$G$中元素又表示自由Abel群$F$的基元素（见定理II.1.1).这个定义与第I.9节中讨论的生成元和定义关系的概念是一致的（见习题10).

基本问题是决定由给定有限个生成元和关系所定义的Abel群G的结构.由于G是有限生成的，从而G必然是循环群的直和（定理II.2.1).现在我们决定这些循环直和成份的阶.

设G是由生成元$a_1,\cdots,a_m$和关系$\sum_j r_{ij}a_j=0\ (1\leqslant i\leqslant n)$所定义的群.我们把这件事情表示成$n\times m$矩阵$A=(r_{ij})$.$A$的诸行代表子群$K$的生成元$b_1,\cdots,b_n$(对于$F$的有序基$\{a_1,\cdots,a_m\}$).我们断言，在$A$上作初等行变换和列变换时，其效果为：

(i) 如果$B=(s_{ij})$是从A通过初等行变换而得到的，则F中元素$c_i=s_{i1}a_1+\cdots+s_{im}a_m(1\leqslant i\leqslant n)$（即$B$的诸行）生成子群$K$(习题11(a))。

(ii) 如果$B=(s_{ij})$是从A通过初等列变换而得到的，则容易决定F的一组基$\{a'_1,\cdots,a'_m\}$，使得$b_i=s_{i1}a'_1+s_{i2}a'_2+\cdots+s_{im}a'_m(1\leqslant i\leqslant n)$（习题11(b)、(c)）。

如果$K\neq 0$，由命题2.11和习题7可知，通过有限次初等行变换和列变换，可以将A变成对角矩阵

$$\begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & dr & \\ & & & 0 \\ 0 & & & 0 \\ & & & & \ddots \end{pmatrix}$$

其中$d_i\neq 0(1\leqslant i\leqslant r)$并且$d_1|d_2|\cdots|d_r$。换句话说，通过有限次初等变换，产生出$F$的一组基$\{u_1,\cdots,u_m\}$，使得$\{d_1u_1,d_2u_2,\cdots,d_ru_r\}$生成$K$。于是由系I.8.11便有

$$\begin{aligned} G\cong F/K&\cong(\boldsymbol{Z}u_1\oplus\cdots\oplus\boldsymbol{Z}u_m)/(\boldsymbol{Z}d_1u_1\oplus\cdots\oplus\boldsymbol{Z}d_ru_r\oplus 0\oplus\\ &\qquad\cdots\oplus 0)\\ &\cong\boldsymbol{Z}/d_1\boldsymbol{Z}\oplus\cdots\oplus\boldsymbol{Z}/d_r\boldsymbol{Z}\oplus\boldsymbol{Z}/0\oplus\cdots\oplus\boldsymbol{Z}/0\\ &\cong Z_{d_1}\oplus\cdots\oplus Z_{d_i}\oplus\boldsymbol{Z}\oplus\cdots\oplus\boldsymbol{Z}。\end{aligned}$$

其中$(\boldsymbol{Z}\oplus\cdots\oplus\boldsymbol{Z})$的秩是$m-r$，而$d_1|d_2|\cdots|d_r$(见定理II.2.6)。

例 决定由生成元a,b,c和关系$3a+9b+9c=0$，$9a-3b+9c=0$所决定的Abel群G的结构，令F是自由Abel群$\boldsymbol{Z}a+\boldsymbol{Z}b+\boldsymbol{Z}c$，$k$是由$b_1=3a+9b+9c$和$b_2=9a-3b+9c$所生成的子群。则$G$同构于$F/K$，并且

$$A=\begin{pmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \end{pmatrix}$$

下面我们指明矩阵A用初等变换作对角化的各步骤（有时将几个变换归并成一步）。在每一步都指明F的基和用所给矩阵表示的K的生成元（求法很简单，见习题11）。

矩阵	F的有序基	K的生成元(表示成这组基的线性组合)
$\begin{pmatrix}3&9&9\\9&-3&9\end{pmatrix}$	a,b,c。	$b_1=3a+9b+9c$ $b_2=9a-3b+9c$
$\begin{pmatrix}3&0&3\\9&-30&9\end{pmatrix}$	$a+3b,b,c$	$b_1=3(a+3b)+9c$ $b_2=9(a+3b)-30b+9c$
$\begin{pmatrix}3&0&0\\9&-30&-18\end{pmatrix}$	$a+3b+3c$, b,c	$b_1=3(a+3b+3c)$ $b_2=9(a+3b+3c)-30b-18c$
$\begin{pmatrix}3&0&0\\0&-30&-18\end{pmatrix}$	$a+3b+3c$ b,c	$b_1=3(a+3b+3c)$ $b_2-3b_1=-30b-18c$
$\begin{pmatrix}3&0&0\\0&18&30\end{pmatrix}$	$a+3b+3c$ c,b	$b_1=3(a+3b+3c)$ $-(b_2-3b_1)=30b+18c$
$\begin{pmatrix}3&0&0\\0&18&12\end{pmatrix}$	$a+3b+3c$ $c+b,b$	$b_1=3(a+3b+3c)$ $-b_2+3b_1=18(c+b)+12b$
$\begin{pmatrix}3&0&0\\0&6&12\end{pmatrix}$	$a+3b+3c$ $c+b,b+(c+b)$	$b_1=3(a+3b+3c)$ $-b_2+3b_1=6(c+b)+12(2b+c)$
$\begin{pmatrix}3&0&0\\0&6&0\end{pmatrix}$	$a+3b+3c$, $5b+3c$, $2b+c$	$b_1=3(a+3b+3c)$ $-b_2+3b_1=6(5b+3c)$

于是$G\cong F/K\cong\boldsymbol{Z}/3\boldsymbol{Z}\oplus\boldsymbol{Z}/6\boldsymbol{Z}\oplus\boldsymbol{Z}/0\boldsymbol{Z}\cong Z_3\oplus Z_6\oplus\boldsymbol{Z}$。如果$\overline{v}\in G$是$v+K\in F/K$在同构$F/K\cong G$之下的象，则$G$是生成元为$\overline{a+3b+3c}$的3阶循环子群，生成元为$\overline{5b+3c}$的6阶循环子群和生生成元为$\overline{2b+c}$的无限循环子群的内直和。

习　题

1. 设f，$g:E\to E$，$h:E\to F$，$k:F\to G$是体D上左向量空间的线性变换，并

且$\dim_D E = n$, $\dim_D F = m$, $\dim_D G = P$.则

(a) $\text{rank}(f+g) \leqslant \text{rank}f + \text{rank}g$.

(b) $\text{rank}((kh) \leqslant \min\{\text{rank}k, \text{rank}h\}$

(c) kh的胞数$\leqslant h$的胞数$+k$的胞数.

(d) $\text{rank}f + \text{rank}g - n \leqslant \text{rank}fg \leqslant \min\{\text{rank}f, \text{rank}g\}$.

(e) $\text{Max}\{g$的胞数, h的胞数$\} \leqslant hg$的胞数.

(f) 如果$m \neq n$, 则(e)对于h和k不成立.

2. 体D上$n \times m$矩阵A有$m \times n$左逆B (即$BA = I_m$) $\Longleftrightarrow \text{rank}A = m$.而$A$有$m \times n$右逆$C$(即$AC = I_n$) $\Longleftrightarrow \text{rank}A = n$.

3. 如果$(c_{i1}, c_{i2}, \cdots, c_{jm})$是矩阵$(c_{ij})$的非零行，它的首项$c_{it}$指的是$t$为第一个整数使$c_{ij} \neq 0$者.体$D$上矩阵$C = (c_{ij})$叫作对于行是梯形的，是指：(i) 存在某个$r \geqslant 0$，使$c$的前$r$行是非零行向量而其余诸行均是零. (ii) 每个非零行的首项均是1_D. (iii) 如果$c_{ij} = 1_D$为第i行的首项，则对于所有$k \neq i$, $c_{kj} = 0$. (iv) 如果$c_{1j_1}, c_{2j_2}, \cdots, c_{rj_r}$是第$1, 2, \cdots, r$行的首项，则$j_1 < j_2 < \cdots < j_r$.

(a) 如果C对于行是梯形的，则C的秩等于非零行数.

(b) 如果A是D上矩阵，则经过有限步初等行变换可将A变成对于行的梯形矩阵.

4. (a) 域K上n个方程的m元线性方程组

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m = b_1 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m = b_n \end{cases}$$

有(公共)解$\Longleftrightarrow$矩阵方程$AX = B$有解X，其中A是$n \times m$矩阵(a_{ij})，X是$m \times 1$列向量$(x_1, x_2, \cdots, x_m)^t$，而$B$是$n \times 1$列向量$(b_1, b_2, \cdots, b_n)^t$.

(b) 如果A_1和B_1分别是由A和B经过同样一些初等行变换所得到的矩阵，则$AX = B$有解$\Longleftrightarrow A_1X = B_1$有解.

(c) 令C是$n \times (m+1)$矩阵

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} & b_1 \\ \vdots & & & \\ a_{n1} & \cdots & a_{nm} & b_n \end{pmatrix}$$

则$AX=B$有解$\Longleftrightarrow$rank$A$=rank$C$.并且在这种情形下,解是唯一的$\Longleftrightarrow$rank$A=m$.[提示：利用(b)和习题3.]

(d) 方程组$AX=B$叫作是齐次的,如果B是零列向量.齐次方程组$AX=B$有非平凡(即x_i不全为0)的解$\Longleftrightarrow$rank$A<m$.

5. 设R是主理想整环.对于每个正整数r和非零理想序列$I_1\supset I_2\supset\cdots\supset I_r$,取元素序列$d_1,\cdots,d_r\in R$,使得$(d_i)=I_i$并且$d_1\mid d_2\mid\cdots\mid d_r$.对于给定的正整数对$(n,m)$令

$$S=\left\{n\times m\text{矩阵}\ \begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}\ \middle|\ 1\leqslant r\leqslant\min(n,m),\ L_r=\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}\right\}.$$

求证S是R上全体$n\times m$矩阵的等价标准型集合.

6. (a) 如果$f:E\to F$是体上有限维向量空间的线性变换,则存在E的一组基$\{u_1,\cdots,u_n\}$和F的一组基$\{v_1,\cdots,v_m\}$以及整数$r(r\leqslant\min(n,m))$,使得$f(u_i)=v_i(1\leqslant i\leqslant r)$而$f(u_i)=0(r+1\leqslant i\leqslant n)$.

(b) 叙述并证明主理想整区上有限秩自由模的类似结果(见命题2.11).

7. 设R是具有函数$\phi:R-\{0\}\to\mathbf{N}$的欧氏整区(定义III.3.8).(例如令$R=\mathbf{Z}$).

(a) 如果$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$是$R$上$2\times2$方阵,则经过有限次初等行变换和列变换可将$A$化成对角方阵.[提示：如果$a\neq0$,$b\neq0$,则$b=ag+r$,其中$r=0$或者$r\neq0$而$\phi(r)<\phi(a)$.作适当的初等列变换则得出：

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\to\begin{pmatrix} a & b-aq \\ c & d-cq \end{pmatrix}=\begin{pmatrix} a & r \\ c & * \end{pmatrix}\to\begin{pmatrix} r & a \\ * & c \end{pmatrix}.$$

由于$\phi(r)<\phi(a)$,重复这一过程即将A变成$B=\begin{pmatrix} s & 0 \\ u & * \end{pmatrix}$,其中$s\neq0$时则

$\phi(s)<\phi(a)$. 如果$u\neq 0$，对于行作类似变化即可将B变成$C=\begin{pmatrix} t & w \\ 0 & * \end{pmatrix}$，其中$t\neq 0$时则$\phi(t)<\phi(s)<\phi(a)$(并且可能$w\neq 0$). 由于在(1,1)处的元素的$\phi$值严格下降，重复若干(有限)次之后必得到对角方阵$D=\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$.]

(*b*) 如果A是可逆的，则A是初等矩阵的乘积.[提示：由(*a*)和系2.10的证明可知$D=PAQ$,其中P和Q是可逆的,从而D也是可逆的并且d_1和d_2是R中单位. 于是$A=P^{-1}\begin{pmatrix} d_1 & 0 \\ 0 & 1_R \end{pmatrix}\begin{pmatrix} 1_R & 0 \\ 0 & d_2 \end{pmatrix}Q^{-1}$. 再利用系2.9.]

(*c*) 欧氏整环上的每个$n\times m$辅助矩阵（见命题2.11的证明）都是一些初等矩阵的乘积.

8. (*a*) 主理想整环上的可逆矩阵是一些初等矩阵和辅助矩阵的乘积.

(*b*) 欧氏整环上的可逆矩阵是一些初等矩阵的乘积[见习题7].

9. 设n_1, n_2, …, n_t, n是正整数，并且$n_1+n_2+\cdots+n_t=n$. 对于每个i，令M_i是$n_i\times n_i$方阵. 又令M是$n\times n$方阵

$$\begin{pmatrix} M_1 & & 0 \\ & M_2 & \\ & & \ddots \\ 0 & & M_t \end{pmatrix}.$$

其中每个M_i的主对角线均在M的主对角线之上. 求证：对于$\{1,2,\cdots,t\}$的每个置换σ，M相似于矩阵

$$\sigma M=\begin{pmatrix} M_{\sigma(1)} & & & 0 \\ & M_{(\sigma 2)} & & \\ & & \ddots & \\ 0 & & & M_{\sigma(t)} \end{pmatrix}.$$

[提示：如果$t=3$，$\sigma=(13)$，$P=\begin{pmatrix} 0 & & I_{n3} \\ & I_{n2} & \\ I_{n1} & & 0 \end{pmatrix}$，则$P^{-1}=\begin{pmatrix} 0 & & I_{n1} \\ & I_{n2} & \\ I_{n3} & & 0 \end{pmatrix}$

并且$PMP^{-1}=\sigma M$. 对于一般情形，要将结果2.8—2.10的证明作一些修改.]

10. 给了集合$\{a_1,\cdots,a_n\}$和由a_i组成的字$w_1,w_2,\cdots,w_r$，以F^*表示集合$\{a_1,\cdots,a_n\}$上的自由(非Abel乘法)群，M是由字w_1, w_2, …, w_r生成

的正规子群（见第1.9节）.令N是由$\{a_ia_ja_i^{-1}\ a_j^{-1}|1\leqslant i,\ j\leqslant n\}$生成的正规子群.求证

(a) F^*/M是由生成元素$\{a_1, \cdots, a_n\}$和关系$\{w_1=w_2=\cdots=w_r=e\}$所定义的群（定义I.9.4）.

(b) F^*/N是集合$\{a_1, \cdots, a_n\}$上的自由Abel群（见练习II.1.12）.

(c) $F^*/(M\vee N)$是由生成元素$\{a_1, \cdots, a_n\}$和关系$\{w_1=w_2=\cdots=w_r=e\}$定义的Abel群（用乘法记号）.

(d) 有群的满同态$F^*\to F^*/N\to F^*/(M\vee N)$.

11. 设F是以$\{a_1, \cdots, a_m\}$为基的自由Abel群.令K是由$b_i=r_{i1}a_1+\cdots+r_{im}a_m(1\leqslant i\leqslant n,\ r_{ij}\in\mathbf{Z})$生成的$F$的子群.

(a) 对于每个i，$\{b_1, \cdots, b_{i-1}, -b_i, b_{i+1}, \cdots, b_n\}$和$\{b_1, \cdots, b_{i-1}, b_i+rb_j, b_{i+1}, \cdots, b_n\}$ $(r\in\mathbf{Z},\ i\neq j)$均生成$K$.[见引理II.1.5]

(b) 对于每个i，$\{a_1, \cdots, a_{i-1}, -a_i, a_{i+1}, \cdots, a_n\}$是$F$的一组基，并且对于这组基，$b_j=r_{j1}a_1+\cdots+r_{j,i-1}a_{i-1}-r_{ji}(-a_i)+r_{j,i+1}a_{i+1}+\cdots+r_{jm}a_m$.

(c) 对于每个i和$j\neq i$，$\{a_1, \cdots, a_{j-1}, a_j-ra_i, a_{j+1}, \cdots, a_m\}$ $(r\in\mathbf{Z})$是F的一组基，并且对于这组基，$b_k=r_{k1}a_1+\cdots+r_{k,i-1}a_{i-1}+(r_{ki}+rr_{kj})a_i+r_{k,i+1}a_{i+1}+\cdots+r_{k,j-1}a_{j-1}+r_{kj}(a_j-ra_i)+r_{k,j+1}a_{j+1}+\cdots+r_{km}a_m$.

12. 决定由生成元$\{a,b\}$和关系$2a+4b=0$，$3b=0$定义的Abel群的结构.决定由生成元$\{a,b,c,d\}$和关系$2a+3b=4a=5c+11d=0$定义的Abel群的结构.决定由生成元$\{a,b,c,d,e\}$和关系$\{a-7b+14d-21c=0,\ 5a-7b-2c+10d-15e=0,\ 3a-3b-2c+6d-9e=0,\ a-b+2d-3e=0\}$所定义的Abel群结构.

3. 行 列 式

我们将行列式函数 $\mathrm{Mat}_n R \to R$ 定义成是特殊的 R-多线性函数，然后讲述它的基本性质（定理3.5）。本节其余部分是谈计算行列式的技巧以及行列式和方阵可逆性的联系。除了少数例外，这些材料今后是不需要的。在本节中所有的环均是含幺交换环，所有的模都是幺作用模。

如果B是R-模，$n \geqslant 1$是整数，B^n表示R-模$B \oplus B \oplus \cdots \oplus B$($n$个)。模$B^n$的凭借集合显然是积集合$B \times \cdots \times B$。

定义3.1 设B_1，…，B_n和C均是含幺交换环R上的模。函数$f: B_1 \times \cdots \times B_n \to C$叫作$R$-多线性的，是指对每个$i = 1, 2, \cdots, n$和$r, s \in R, b_j \in B_j, b, b' \in B_i$均有：

$$f(b_1, \cdots, b_{i-1}, rb + sb', b_{i+1}, \cdots, b_n) = rf(b_1, \cdots, b_{i-1}, b, b_{i+1}, \cdots, b_n) + sf(b_1, \cdots, b_{i-1}, b', b_{i+1}, \cdots, b_n).$$

如果$C = R$，称f是n-线性型或者R-多线性型。如果$C = R$而$B_1 = B_2 = \cdots = B_n = B$，则$f$叫作$B$上的$R$-多线性型。

2-线性函数通常叫作是双线性的（见定理IV.5.6）。设B和C是R-模，$f: B^n \to C$是R-多线性函数。则f叫作对称函数，是指对于每个$\sigma \in S_n$，均有

$$f(b_{\sigma(1)}, \cdots b_{\sigma(n)}) = f(b_1, \cdots, b_n).$$

f叫作反对称的，是指对于每个$\sigma \in B_n$，均有

$$f(b_{\sigma(1)}, \cdots, b_{\sigma(n)}) = (\mathrm{sgn}\sigma) f(b_1, \cdots, b_n).$$

f叫作交错的，如果对于i和$j(i\neq j)$，当$b_i=b_j$时，就有

$$f(b_1,\cdots,b_n)=0.$$

例 设B是自由R-模$R\oplus R$，令$d:B\times B\to R$定义为$((a_{11},a_{12}),(a_{21},a_{22}))\longmapsto a_{11}a_{22}-a_{12}a_{21}$.则$d$是$B$上的斜对称交错双线性型。如果将$B$中元素想象为是$R$上$2\times 2$方阵，则$d$不过是通常的行列式函数。

定理3.2 如果B和C是含幺交换环R上的模，则每个交错R-多线性函数$f:B^n\to C$是斜对称的。

证明概要 如果$n=2$而$\sigma=(12)$，则

$$\begin{aligned}0&=f(b_1+b_2,\ b_1+b_2)\\&=f(b_1,b_1)+f(b_1,b_2)+f(b_2,b_1)++f(b_2,b_2)\\&=0+f(b_1,b_2)+f(b_2,b_1)+0,\end{aligned}$$

从而$f(b_2,b_1)=-f(b_1,b_2)=(\mathrm{sgn}\sigma)f(b_1,b_2)$。对于一般情形，只需对于$\sigma$是对换的情形证明即可。而这时不难将$n=2$的情形推广，从而得到证明。∎

我们的主要兴趣是自由R-模R^n上的交错n-线性型。这样的型是从$(R^n)^n=R^n\oplus\cdots\oplus R^n$($n$个)到$R$的函数。

定理3.3 如果R是含幺交换环，$r\in R$。则存在唯一的交错R-多线性型$f:(R^n)^n\to R$，使得$f(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)=r$，其中$\{\varepsilon_1,\cdots,\varepsilon_n\}$是$R^n$的标准基。

注记：标准基的定义见定义2.1的后面所述。下面一些事实对于理解后面的证明或许是有益的。由于R^n中元素可以等同于$1\times n$行向量，显然存在着R-模同构$(R^n)^n\cong \mathrm{Mat}_n R$，$(X_1,X_2,\cdots,X_n)\longmapsto A$，其中$A$是以$X_1$，$X_2$，…，$X_n$为行向量的矩阵。如果

$\{\varepsilon_1,\cdots,\varepsilon_n\}$是$R^n$的标准基，则在这个同构之下$(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)\longmapsto I_n$。所以定理3.3中的多线性型可以想象成是以$n\times n$方阵的$n$行为$n$个自变量的函数。

定理3.3的证明 （**唯一性**） 如果存在着这样的交错n-线性型f，并且$(\mathbf{X}_1,\cdots,\mathbf{X}_n)\in(R^n)^n$，对于每个$i$均存在$a_{ij}\in R$，使得$\mathbf{X}_i=(a_{i1},\ a_{i2},\ \cdots,\ a_{in})=\sum_{j=1}^{n}a_{ij}\varepsilon_j$。（换句话说，在同构$(R^n)^n\cong\mathrm{Mat}_nR$之下，$(\mathbf{X}_1,\cdots,\mathbf{X}_n)\longmapsto(a_{ij})$。）因此由多线性可知

$$f(\mathbf{X}_1,\cdots,\mathbf{X}_n)=f\Big(\sum_{j_1}a_{1j_1}\varepsilon_{j_1},\ \sum_{j_2}a_{2j_2}\varepsilon_{j_2},\cdots,\ \sum_{j_n}a_{nj_n}\varepsilon_{j_n}\Big)$$

$$=\sum_{j_1}\sum_{j_2}\cdots\sum_{j_n}a_{1j_1}a_{2j_2}\cdots a_{nj_n}f(\varepsilon_{j_1},\varepsilon_{j_2},\cdots,\varepsilon_{j_n}).$$

由于f是交错的，所以最后的和式只有当$j_1,\ j_2,\ \cdots,\ j_n$彼此不同时才可能有非零项。而当$j_1,\ j_2,\ \cdots,\ j_n$彼此不同时，则存在某个置换$\sigma\in S_n$，使得$(j_1,\ \cdots,\ j_n)=(\sigma 1,\ \cdots,\ \sigma n)$。于是由定理3.2，

$$f(\mathbf{X}_1,\ \cdots,\ \mathbf{X}_n)=\sum_{\sigma\in S_n}a_{1\sigma 1}a_{2\sigma 2}\cdots a_{n\sigma n}f(\varepsilon_{\sigma 1},\ \varepsilon_{\sigma 2},\ \cdots,\varepsilon_{\sigma n})$$

$$=\sum_{\sigma\in S_n}(\mathrm{sgn}\sigma)a_{1\sigma 1}\cdots a_{n\sigma n}f(\varepsilon_1,\varepsilon_2,\ \cdots,\varepsilon_n).$$

由于$f(\varepsilon_1,\cdots,\varepsilon_n)=r$，我们有

$$f(\mathbf{X}_1,\cdots,\mathbf{X}_n)=\sum_{\sigma\in S_n}(\mathrm{sgn}\sigma)ra_{1\sigma 1}a_{2\sigma 2}\cdots a_{n\sigma n}. \qquad (1)$$

(1)式表明$f(\mathbf{X}_1,\cdots,\mathbf{X}_n)$由$\mathbf{X}_1,\ \cdots,\ \mathbf{X}_n$和$r$所唯一决定。

（**存在性**） 我们用(1)式定义函数$f:(R^n)^n\to R$（其中$\mathbf{X}_i=(a_{i1},\cdots,a_{in})$），只需验证$f$是交错$n$-线性型并且$f(\varepsilon_1,\cdots,\varepsilon_n)=r$即

可。对于每个固定的k，$\sum_{\sigma\in S_n}(\mathrm{sgn}\sigma)ra_{1\sigma 1}\cdots a_{n\sigma n}$ 中每一项恰好包含一个因子a_{ij}使得$i=k$，从而不难看出f是R-多线性的。由于$\varepsilon_i=\sum_{j=1}^{n}\delta_{ij}\varepsilon_j$（$\delta_{ij}$为Kronecker符号），从而$f(\varepsilon_1,\cdots,\varepsilon_n)=r$。最后，我们还要证明当$i\neq j$而$X_i=X_j$时$f(X_1,\cdots,X_n)=0$。为记号上方便起见不妨假设$i=1$，$j=2$。如果 $\rho=(12)$，则映射$A_n\to S_n,\sigma\longmapsto\sigma\rho$是单射，它的象是全体奇置换所组成的集合（这是因为$\sigma$是偶置换，所以$\sigma\rho$是奇置换，并且 $|A_n|=|S_n|/2$）。从而 S_n是彼此非交的一些二元集合$\{\sigma,\sigma\rho\}(\sigma\in A_n)$的并。如果$\sigma$是偶置换，则$f(X_1,X_2,X_3,\cdots,X_n)$中对应于$\sigma$的项是

$$+ra_{1\sigma 1}a_{2\sigma 2}b_{3\sigma 3}\cdots a_{n\sigma n}$$

由于$X_1=X_2$，$a_{1\sigma 1}=a_{2\sigma 1}$，$a_{2\sigma 2}=a_{1\sigma 2}$，从而对应于奇置换 $\sigma\rho$ 的项是

$$\begin{aligned}-ra_{1\sigma\rho 1}a_{2\sigma\rho 2}a_{3\sigma\rho 3}\cdots a_{n\sigma\rho n}&=-ra_{1\sigma 2}a_{2\sigma 1}a_{3\sigma 3}\cdots a_{n\sigma n}\\&=-ra_{1\sigma 1}a_{2\sigma 2}a_{3\sigma 3}\cdots a_{n\sigma n}.\end{aligned}$$

因此$f(X_1,X_2\cdots,X_n)$中诸项两两抵消，于是

$$f(X_1,X_2\cdots,X_n)=0.$$

所以f是交错型。∎

现在我们可以利用定理 3.3 和它后面的注记来定义行列式。特别地，我们常常将Mat_nR和$(R^n)^n$ 在（注记中所给的）同构之下等同起来（该同构将$(\varepsilon_1,\cdots,\varepsilon_n)$映成$I_n$）。于是，$\mathrm{Mat}_nR$上的一个多线性型也是$(R^n)^n$上的 R-多线性型，而后者的自变量为$n\times n$方阵的诸行，看作是R^n中的元素。

定义3.4 设R是含幺交换环。我们把满足$d(I_n)=1_R$的唯一的交错R-多线性型$d:\mathrm{Mat}_nR\to R$叫作是Mat_nR上的行列式函数。而元数$d(A)\in R$叫作是方阵$A\in\mathrm{Mat}_nR$的行列式，并且表示成$|A|$。

定理3.5 设R是含幺交换环，$A,B\in\mathrm{Mat}_nR$。

(i) Mat_nR上的每个交错R-多线性型f均是行列式函数d的常数倍。并且这个常数是唯一的。

(ii) 如果$A=(a_{ij})$，则$|A|=\sum_{\sigma\in S_n}(\mathrm{sgn}\sigma)a_{1\sigma 1}a_{2\sigma 2}\cdots a_{n\sigma n}$。

(iii) $|AB|=|A||B|$。

(iv) 如果A是Mat_nR中可逆方阵，则$|A|$是R中单位。

(v) 如果A和B相似，则$|A|=|B|$。

(vi) $|A^t|=|A|$。

(vii) 如果$A=(a_{ij})$是三角方阵，则$|A|=a_{11}a_{22}\cdots a_{nn}$。

(viii) 如果B是由A交换两行(或者两列)而得到的，则$|B|=-|A|$。如果B是将A的一行(或者一列)乘以$r\in R$而得到的，则$|B|=r|A|$。如果B是将第i行(或者第i列)的某个倍数加到第j行(或者第j列)之上而得到的$(i\neq j)$，则$|B|=|A|$。

证明概要 (i) 令$f(I_n)=r\in R$。而d为行列式函数。验证函数$rd:\mathrm{Mat}_nR\to R,A\longmapsto r|A|=rd(A)$也是$\mathrm{Mat}_nR$上的交错$R$-多线性型，并且$rd(I_n)=r$。由定理3.3的唯一性论断可知$f=rd$。由此即刻得出$r$的唯一性。

(ii) 是定理3.3的证明中方程(1)的重新叙述。

(iii) 固定B，并且以Y_1，Y_2，…，Y_n表示B的诸列。如果C是任意$n\times m$矩阵，其诸行为X_1，…，X_n，则CB在(i,j)处的元素恰

好是(1×1方阵)元素X_iY_j。从而CB的第i行是$(X_iY_1, X_iY_2, \cdots, X_iY_n)$。利用这一事实来验证映射 $\mathrm{Mat}_nR \to R, C \longmapsto |CB|$ 是Mat_nR上的交错R-多线性型f。由 (i) 即知 $f = rd$, $r \in R$。从而 $|CB| = f(C) = rd(C) = r|C|$。特别地，$|B| = |I_nB| = r|I_n| = r$，从而 $|AB| = r|A| = |A||B|$。

(iv) $AA^{-1} = I_n$和(iii)导致$|A||A^{-1}| = |AA^{-1}| = |I_n| = 1$。从而$|A|$是$R$中单位，并且$|A|^{-1} = |A^{-1}|$。

(v) 类似地，$B = PAP^{-1}$ 导致$|B| = |P||A||P^{-1}| = |A|$，因为$R$是交换环。

(vi) 令$A = (a_{ij})$。如果$\{i_1, \cdots, i_n\} = \{1, \cdots, n\}$，由于 R 是交换环，所以每个乘积$a_{i_1 1}a_{i_2 2}\cdots a_{i_n n}$均可写成$a_{1 j_1}a_{2 j_2}\cdots a_{n j_n}$。如果$\sigma$是置换$\sigma(k) = i_k$，则$\sigma^{-1}$是置换$\sigma^{-1}(k) = j_k$。此外，不难看出，对于每个$\sigma \in S_n$，$\mathrm{sgn}\sigma = \mathrm{sgn}\sigma^{-1}$。令$A^t = (b_{ij})$，由于 S_n是群，从而

$$|A^t| = \sum_{\sigma \in S_n} (\mathrm{sgn}\sigma) b_{1\sigma 1}\cdots b_{n\sigma n} = \sum_{\sigma \in S_n} (\mathrm{sgn}\sigma) a_{\sigma 1, 1}\cdots a_{\sigma n, n}$$

$$= \sum_{\sigma^{-1} \in S_n} (\mathrm{sgn}\sigma^{-1}) a_{1, \sigma^{-1}1}\cdots a_{n, \sigma^{-1}n} = |A|.$$

(vii) 根据假设，或者对所有$j < i$均有 $a_{ij} = 0$，或者对所有$j > i$均有$a_{ij} = 0$。无论是哪一种情形均可证明当$\sigma \in S_n, \sigma \neq (1)$时，$a_{1,\sigma 1}\cdots a_{n,\sigma n} = 0$，从而

$$|A| = \sum_{\sigma \in S_n} (\mathrm{sgn}\sigma) a_{1,\sigma 1}\cdots a_{n,\sigma n} = a_{11}a_{22}\cdots a_{nn}.$$

(viii) 令$X_1, \cdots, X_i, \cdots, X_j, \cdots, X_n$是$A$的诸行。如果 B的诸行是$X_1, \cdots, X_j, \cdots, X_i, \cdots, X_n$，由于$d$是斜对称的 (定理3.2)，从而

$$|B| = d(X_1,\cdots,X_j,\cdots,X_i,\cdots,X_n) = -d(X_1,\cdots,X_i,\cdots,X_j,\cdots,X_n) = -|A|.$$

类似地，如果B的诸行为$X_1,\cdots,X_i,\cdots,rX_i+X_j,\cdots,X_n$，由于$d$是多线性并且是交错的，从而

$$\begin{aligned}|B| &= d(X_1,\cdots,X_i,\cdots,rX_i+X_j,\cdots,X_n)\\ &= rd(X_1,\cdots,X_i,\cdots,X_i,\cdots,X_n)\\ &\quad + d(X_1,\cdots,X_i,\cdots,X_j,\cdots x_n) = r0+|A| = |A|.\end{aligned}$$

另一论断也可类似证明。最后利用(v)即可证明关于列的相应命题。∎

如果R是域，定理3.5的后部分给出计算$|A|$的一种方法。使用初等行变换和列变换可将A变成对角方阵$B=(b_{ij})$。通过(viii)可以得知每一步骤之下$|A|$发生什么变化。最后给出$|B|=r|A|$，其中$0\neq r\in R$。然后由(vii)知$r|A| = b_{11}b_{22}\cdots b_{nn}$，从而

$$|A| = r^{-1}b_{11}b_{22}\cdots b_{nn}.$$

更一般地，在任意含幺交换环R上的$n\times n$方阵A的行列式可用下法计算：对于每个数对(i,j)，以A_{ij}表示将A去掉第i行和第j列所得到的$(n-1)\times(n-1)$方阵。我们将$|A_{ij}|\in R$叫作是$A=(a_{ij})$在(i,j)处的余子式，而将$(-1)^{i+j}|A_{ij}|\in R$叫作是a_{ij}的代数余子式。

命题3.6 如果A是含幺交换环R上的$n\times n$方阵，则

$$|A| = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}|A_{ij}|.\quad(1\leqslant i\leqslant n).$$

$$= \sum_{i=1}^{n}(-1)^{i+j}a_{ij}|A_{ij}|.\quad(1\leqslant j\leqslant n).$$

它们分别称作是$|A|$按第i行展开和按第j列展开。

证明 让我们固定j而来证明第二个论断。由定理3.3和定义3.4可知只需证明映射

$$\phi:\mathrm{Mat}_nR\to R,\quad A=(a_{ij})\longmapsto\sum_{i=1}^{n}(-1)^{i+j}a_{ij}|A_{ij}|$$

是交错R-多线性型并且$\phi(I_n)=1_R$。令$X_1,\cdots,X_n$是A的诸行。如果$X_k=X_t$，$1\leqslant k<t\leqslant n$，则当$i\neq k$，$t$时，$|A_{ij}|=0$(因为它是有两个同样行的矩阵之行列式)。由于从$A_{tj}$依次将第$t$行与第$t-1$，$\cdots,k-1$行相交换即得到$A_{kj}$，由定理3.5可知$|A_{kj}|=(-1)^{t-k-1}\cdot|A_{tj}|$.因此$\phi(A)=(-1)^{k+j}|A_{tj}|+(-1)^{t+j}|A_{tj}|=(-)^{k+j+t-k-1}|A_{tj}|+(-1)^{t+j}|A_{tj}|=0$。所以$\phi$是交错型。如果对于某个$k$，$X_k=rY_k+sW_k$,令$B=(b_{ij})$和$C=(c_{ij})$是诸行分别为$X_1,\cdots,X_{k-1},Y_k,X_{k+1},\cdots,X_n$和$X_1,\cdots,X_{k-1},W_k,X_{k+1},\cdots,X_n$的两个方阵。为证$\phi$是$R$-多线性的，我们只需证明$\phi(A)=r\phi(B)+s\phi(C)$。当$i=k$时，$|A_{kj}|=|B_{kj}|=|C_{kj}|$，从而$a_{kj}|A_{kj}|=(rb_{kj}+sc_{kj})|A_{kj}|=rb_{kj}|B_{kj}|+Sc_{kj}|C_{kj}|$。如果$i\neq k$，由于每个$|A_{ij}|$都是$A_{ij}$的诸行的多线性函数，并且当$i\neq k$时$a_{ij}=b_{ij}=C_{ij}$，因此我们有$a_{ij}|A_{ij}|=a_{ij}(r|B_{ij}|+s|C_{ij}|)=rb_{ij}|B_{ij}|+sc_{ij}|C_{ij}|$。从而$\phi(A)=r\phi(B)+s\phi(C)$，即$\phi$是$R$-多线性函数。显然$\phi(I_n)=1_R$。从而$\phi$是行列式函数。利用转置即可得到定理的第一论断。∎

命题3.7 如果$A=(a_{ij})$是含幺交换环R上$n\times n$方阵，$A^a=(b_{ij})$是$n\times n$方阵，其中$b_{ij}=(-1)^{i+j}|A_{ij}|$，则$AA^a=|A|I_n=A^aA$。此外，$A$在$\mathrm{Mat}_RR$中可逆$\Longleftrightarrow|A|$是$R$中单位。并且在这种情形下，$A^{-1}=|A|^{-1}A^a$。

矩阵A^a叫作是A的伴随方阵。注意若R是域，则$|A|$为单位$\Longleftrightarrow|A|\neq0$。

证明 AA^a在(i,j)处元素是$c_{ij}=\sum_{k=1}^{n}(-1)^{i+k}a_{ik}|A_{jk}|$。如果$i=j$,由命题3.6可知$c_{ii}=|A|$。如果$i\neq j$(无妨设$i<j$),令$A$的诸行为$X_1,\cdots,X_n$,又令$B=(b_{ij})$是以$X_1,\cdots,X_i,\cdots,X_{j-1},X_i,X_{j+1},\cdots,X_n$为其$n$行的方阵。则对每个$k$均有$b_{ik}=a_{ik}=b_{jk}$。由于行列式是交错型,从而$|B|=0$。于是

$$c_{ij}=\sum_{k=1}^{n}(-1)^{j+k}a_{ik}|A_{jk}|=\sum_{k=1}^{n}(-1)^{j+k}b_{jk}|B_{jk}|=|B|=0.$$

因此$c_{ij}=\delta_{ij}|A|$(δ_{ij}为Kronecker符号),并且$AA^a=|A|I_n$。特别地,将A改成A^t又有:$A^t(A^t)^a=|A^t|I_n$。由于$(A^a)^t=(A^t)^a$,从而$|A|I_n=|A^t|I_n=A^t(A^t)^a=A^t(A^a)^t=(A^aA)^t$,于是$A^aA=(|A|I_n)^t=|A|I_n$。所以若$|A|$为$R$中单位,则$|A|^{-1}A^a\in \mathrm{Mat}_nR$并且显然有$(|A|^{-1}A^a)A=I=A(|A|^{-1}A^a)$从而$A$是可逆的,并且(唯一的)逆是$A^{-1}=|A|^{-1}A^a$。反之,如果$A$可逆,由定理3.5即知$|A|$是单位。∎

系3.8 (Cramer法则) 设$A=(a_{ij})$是域K上n元n个方程的方程组

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=b_1 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{nn}x_n=b_n \end{cases}$$

的系数方阵。如果$|A|\neq 0$,则此方程组有唯一解,并且此解为

$$x_j=|A^{-1}|\left(\sum_{i=1}^{n}(-1)^{i+j}b_i|A_{ij}|\right)\quad(1\leqslant j\leqslant n).$$

证明 显然,给定方程组有解$\Longleftrightarrow$矩阵方程$AX=B$有解,其中X和B分别是列向量$X=(x_1,\cdots,x_n)^t$和$B=(b_1,\cdots,b_n)^t$。由于

$|A| \neq 0$，从命题3.7可知A是可逆的，从而$X = A^{-1}B$即是一组解。而这也是唯一的一组解(因为$AY = B$导致$Y = A^{-1}B$)。经过简单计算并且利用

$$X = A^{-1}B = (|A|^{-1}A^a)B = |A|^{-1}(A^aB).$$

即给出x_j的公式。∎

习　题

注：若非特别声明，所有矩阵均是含么交换环R上的矩阵。

1. 如果$r + r \neq 0$(对于R中每个非零元素r)，证明：n-线性型$B^n \to R$是交错的$\Leftrightarrow$它是斜对称的。如果char$R = 2$呢？

2. (a) 如果$m > n$，则$(R^n)^m$上每个交错R-多线性型均为零。

   (b) 如果$m < n$，则在$(R^n)^m$上存在着非零的交错R-多线性型。

3. 利用习题2直接证明：如果有R-模同构$R^m \cong R^n$，则$m = n$。

4. 如果$A \in \mathrm{Mat}_n R$，则$|A^a| = |A|^{n-1}$，$(A^a)^a = |A|^{n-2}A$。

5. 如果R是域，A，B均是$\mathrm{Mat}_n R$中可逆方阵。则除了有限个$r \in R$之外，$A + rB$均是可逆方阵。

6. 设A是域上$n \times n$方阵。不用命题3.7来证明：A是可逆的$\Leftrightarrow |A| \neq 0$。[提示：定理2.6和3.5(viii)，命题2.12。]

7. 设F是以$U = \{u_1, \cdots, u_n\}$为基的自由R-模。如果R-模自同态$\phi: F \to F$对于U的方阵是A，我们定义$|A| \in R$为自同态ϕ的行列式，并且记成$|\phi|$。

   (a) $|\phi|$与U的选择方式无关。

   (b) $|\phi|$是R中唯一的元素，使得对于F^n上每个交错R-多线性型f和每个$b_i \in F$，均有

   $$f(\phi(b_1), \phi(b_2), \cdots, \phi(b_n)) = |\phi| f(b_1, \cdots, b_n).$$

8. 假设$(b_1, \cdots, b_n)$是齐次线性方程组

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n &= 0 \end{aligned}$$

的一组解，而 $A=(a_{ij})$是它的系数矩阵，则对于每个i均有$|A|b_i=0$。〔提示：如果B_i是$n\times n$对角方阵，其对角元素为$1_K,\cdots,1_K,b_i,1_K,\cdots,1_K$，则$|AB_i|=|A|b_i$。为了证明$|AB_i|=0$，对于每个$j\neq i$，将$AB_i$第$j$列的$b_j$倍加到第$i$列之上，所得矩阵的行列式为$|AB_i|$，但是对每个$k=1,2,\cdots,n$，它在$(k,i)$处的元素是$a_{k1}b_1+a_{k2}b_2+\cdots+a_{kn}b_n=0$。〕

4. 一个线性变换的分解和相似性

本节研究域K上有限维向量空间E对于线性变换$E\to E$的结构。该线性变换将E分解成一些子空间的直和，并且E的每个这样的分解结合一个$K[x]$中多项式不变量集合（定理4.2）。这些多项式不变量集合可以使我们选取E的一组基，使得给定的线性变换对于这组基的矩阵是某种特定类型的（定理4.6）。由此给出$\mathrm{Mat}_n K$中几种不同类型的相似标准型（系4.7）。

注：本节的结果在很大程度上依赖于主理想整环上有限生成模的结构定理（第IV.6节）。

设K是域，$\phi:E\to E$是n维K-向量空间E的线性变换。我们首先回忆一下关于$\mathrm{Hom}_K(E,E)$和$\mathrm{Mat}_n K$的结构的某些事实。$\mathrm{Hom}_K(E,E)$不仅是含幺环（习题IV.1.7），而且又是K上向量空间，其中$(k\psi)(u)=k\psi(u)(k\in K,u\in E,\psi\in\mathrm{Hom}_K(E,E))$。（见定理IV.4.8后面的注记）。因此，如果$f=\sum k_i x^i$是$K[x]$中的多项式，则$f(\phi)=\sum k_i\phi^i$定义出$\mathrm{Hom}_K(E,E)$中一个元素（通常令$\phi^0$

$=1_E$)。类似地，环$\mathrm{Mat}_n K$也是K上的向量空间。如果$A\in \mathrm{Mat}_n K$，则$f(A)=\sum k_i A^i$定义出K上一个$n\times n$方阵(其中$A^0=I_n$)。

定理4.1 设E是域K上的n维向量空间，$\phi: E\to E$是线性变换，A是K上$n\times n$方阵。

(i) 存在着唯一的正次数首1多项式$q_\phi\in K[x]$，使得$q_\phi(\phi)=0$，并且如果$f\in K[x]$，$f(\phi)=0$，则$q_\phi\mid f$。

(ii) 存在唯一的正次数首1多项式$q_A\in K[x]$，使得$q_A(A)=0$，并且若$f\in K[x]$，$f(A)=0$，则$q_A\mid f$。

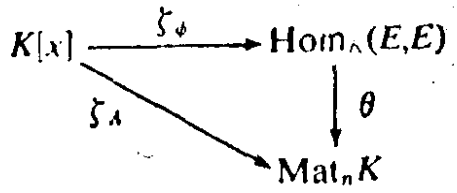
(iii) 如果A是ϕ对于E中某一组基的矩阵，则$q_A=q_\phi$。

证明 (i) 根据定理III.5.5，存在着唯一的(非零)环同态$\zeta=\zeta_\phi: K[x]\to \mathrm{Hom}_K(E,E)$，使得$x\longmapsto\phi$，并且$k\longmapsto k1_E$(对每个$k\in K$)。所以若$f\in K[x]$，则$\zeta(f)=f(\phi)$。易知$\zeta$是$K$-向量空间的线性变换。由于$\dim_K E$是有限的，由定理IV.2.1，IV.2.4，IV.4.7和IV.4.9可知$\mathrm{Hom}_K(E,E)$是K上有限维向量空间。从而$\mathrm{Im}\zeta$在K上也必定是有限维的。但是$K[x]$在K上是无限维的，由系IV.2.14可知$\mathrm{Ker}\zeta\neq 0$。因为$K[x]$是主理想整环，它的单位正好是K的非零元素(系III.6.4)，从而有首1多项式$q\in K[x]$，使得$\mathrm{Ker}\zeta=(q)$。由于ζ不是零映射，从而$(q)\neq K[x]$，因此$\deg q\geqslant 1$。如果$\mathrm{Ker}\zeta=(q_1)$，而$q_1\in K[x]$是首1多项式，由定理III.3.2即知$q\mid q_1$，$q_1\mid q$，但两者均是首1的，从而$q=q_1$。所以$q_\phi=q$具有所述性质。

(ii) 证明与(i)相同，只是将ϕ改成A，而将$\mathrm{Hom}_K(E,E)$改成$\mathrm{Mat}_n K$。$q_A\in K[x]$是满足$(q_A)=\mathrm{Ker}\zeta_A$的唯一的首1多项式，其中$\zeta_A: K[x]\to \mathrm{Mat}_n K$是由$f\longmapsto f(A)$所给出的唯一的环同态。

(iii) 设A是ϕ对于E的基U的矩阵，令$\theta: \mathrm{Hom}_K(E,E)\cong \mathrm{Mat}_n R$

是定理1.2中的同构，并且$\theta(\phi)=A$。于是由定理 III.5.5 可知图表



是交换的，这是由于$\theta\xi_\phi(x)=\theta(\phi)=A=\xi_A(x)$，而$\theta\xi_\phi(k)=\theta(k1_E)=kI_n=\xi_A(k)$(对每个$k\in K$)。由于$\theta$是同构，从而$(q_\phi)=\mathrm{Ker}\xi_\phi=\mathrm{Ker}\theta\xi_\phi=\mathrm{Ker}\xi_A=(q_A)$。因此$q_\phi\mid q_A$，$q_A\mid q_\phi$，因为两者均是首1的，从而$q_\phi=q_A$。 ∎

如果K，E和ϕ如定理4.1中所示，我们将q_ϕ和q_A分别叫做线性变换ϕ和矩阵A的极小多项式，一般来说，q_ϕ不一定是不可约的。由系1.7和定理4.1(iii) 立刻推出相似矩阵有同样的极小多项式。

设K，E和ϕ如上所示。则由ϕ给出E的如下（左）$K[x]$-模结构：如果$f\in K[x]$，$u\in E$，则 $f(\phi)\in\mathrm{Hom}_K(E,E)$，其中$fu$定义为$fu=f(\phi)(u)$。$E$的$K$-子空间$F$叫作对于$\phi$的不变子空间（或者叫$\phi$-不变子空间），是指$\phi(F)\subset F$。显然$F$是$\phi$-不变$K$-子空间$\Longleftrightarrow$$F$是$E$的$K[x]$-子模，特别地，对于任意$v\in E$，由集合$\{\phi^i(v)\mid i\geqslant 0\}$张成的子空间$E(\phi,v)$是$\phi$-不变的。不难看出，$E(\phi,v)$恰好是由$v$生成的循环$K[x]$-子模$K[x]v$.我们将$E(\phi,v)$叫做一个$\phi$-循环(子)空间。

定理4.2 设$\phi:E\to E$是域K上n维向量空间E的线性变换。则

(i) 存在着正次数首1多项式q_1，q_2，…，$q_t\in K[x]$和E的ϕ-循环子空间E_1，…，E_t，使得$E=E_1\oplus E_2\oplus\cdots\oplus E_t$，而$q_1\mid q_2\mid\cdots\mid q_t$。并且$q_i$是$\phi\mid E_i:E_i\to E_i$的极小多项式。$(q_1,\cdots,q_t)$由$E$和$\phi$所唯一确定。最后，$q_t$是$\phi$的极小多项式。

(ii) 存在着不可约首 1 多项式p_1，…，$p_s\in K[x]$和E的ϕ-循环子空间E_{11}，…，E_{1k_1}，E_{21}，…，E_{2k_2}，E_{31}，…，E_{sk_s}，使得

$E=\sum_{i=1}^{s}\sum_{j=1}^{k_i}E_{ij}$，并且对于每个 i，均存在整数序列 $m_{i1}\geqslant m_{i2}\geqslant$

$\cdots\geqslant m_{ik_i}\geqslant 0$，使得 $p_i^{m_{ij}}$是$\phi|E_{ij}:E_{ij}\to E_{ij}$的极小多项式。多项式集合$\{p_i^{m_{ij}}\mid 1\leqslant i\leqslant s,\ 1\leqslant j\leqslant k_i\}$由$E$和 ϕ 所唯一确定。最后，$p_1^{m_{11}}p_2^{m_{21}}\cdots p_s^{m_{s1}}$是$\phi$的极小多项式。

定理第(i)部分中的多项式$q_1,\cdots,\ q_t$叫做线性变换ϕ 的不变因子。第(ii)部分的$\{p_i^{m_{ij}}\}$叫做ϕ的初等因子。

定理4.2的证明概要 (i) 前面已经指明，E 是主理想整环$K[x]$上的左模，其中$f(u)=f(\phi)u$ $(f\in K[x],\ u\in E)$。由于E是K上有限维向量空间，并且$K\subset K[x]$，从而E必然是有限生成的非零 $K[x]$-模。如果q_ϕ是ϕ的极小多项式，则$q_\phi\neq 0$，并且$q_\phi E=0$，从而 E是扭 $K[x]$-模。根据定理 IV.6.12(i)，E是内直和$E=E_1\oplus\cdots\oplus E_t$，其中$E_i$是$q_i$阶非零循环$K[x]$-模 $(q_i\in K[x])$。并且 $q_1\mid q_2\mid\cdots\mid q_t$。由本定理前面的注记可知每个 E_i 均是ϕ-循环子空间。因为E_i的阶是 q_i，由定理 IV.6.4和其后的例子可知有 $K[x]$ -模同构$E_i\cong K[x]/(q_i)$。由于$E_i\neq 0$，并且$K[x]$ 中非零理想均有唯一的首 1 多项式生成元素 (定理III.3.2和系III.6.4)，我们可以假定每个q_i都是正次数的首 1 多项式。从定理IV.6.12(i) 的唯一性结果和$q_1\mid q_2\mid\cdots\mid q_t$即知$q_1$，…，$q_t$是由$K[x]$一模$E$ (即由E和ϕ) 所唯一确定的。利用E_i的$K[x]$-模结构和 E_i是q_i 阶循环模这一事实，可以证明$\phi|E_i$的极小多项式为q_i。最后，$q_tE=q_t(\phi)E_1\oplus\cdots\oplus q_t(\phi)E_t=0$，从而$(q_t)\subset(q_\phi)$。由于$q_\phi E=0$，又有$q_\phi E_t=0$，从

而$(q_\phi)\subset(q_t)$。由$(q_t)=(q_\phi)$和两者均是首1多项式，便推出$q_t=q_\phi$.将E分解成素幂阶循环$K[x]$-模的直和(定理 IV.6.12(ii))，即可类似地证明定理第二部分。∎

注记：如果$\phi=0$，由定理4.2的证明可知ϕ的极小多项式是x，而它的不变因子和初等因子均是$q_1=x$，$q_2=x$，…，$q_n=x$。(习题2)。

从定理4.2的证明可知，线性变换$\phi:E\to E$的不变因子和初等因子不过就是$K[x]$-模E的不变因子和初等因子.所以我们可以象在定理IV.6.12的证明中所作的那样，从不变因子可得到初等因子,或者反过来从初等因子可得到不变因子(还见第122—123页)。我们将在下面的命题4.9中讨论计算一给定线性变换的不变因子的方法。

例 令$K=\mathbb{Q}$，$\dim_K E=15$。并假设ϕ的不变因子是$q_1=x^4-x^2-2$，$q_2=x^5-x^3-2x$和$q_3=x^6-x^4-2x^2$。则$q_1=(x^2-2)(x^2+1)$，$q_2=xq_1$，$q_3=xq_2$，从而ϕ的初等因子为：x^2-2，x^2+1，$x,x^2-2,x^2+1,x^2,x^2-2,x^2+1$.见定理 IV.6.12的证明(或者见第122—123页).反之,如果线性变换ψ的初等因子是$x-1$，$x-1$，$x-2$，$x-3$，$(x-2)^2$，x^2+1，x^2+1，x^2+1和$(x-1)^3$，则不变因子是$q_1=(x-1)(x^2+1)$，$q_2=(x-1)(x-2)(x^2+1)$，$q_3=(x-3)(x-2)^2(x^2+1)(x-1)^3$。

从定理4.2可以看出，下一步我们应当研究ϕ-循环空间。

定理4.3 设$\phi:E\to E$是域K上有限维向量空间的线性变换。则：E是ϕ-循环空间并且ϕ的极小多项式是$q=x^r+a_{r-1}x^{r-1}+\cdots+a_0\in K[x]$的充要条件是$\dim_K E=r$并且$E$存在有序基$V$，使得$\phi$对于$V$的矩阵为

$$A=\begin{pmatrix} 0 & 1_k & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1_k & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1_k & 0 & \cdots & 0 & 0 \\ \vdots & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1_k \\ -a_0 & -a_1 & -a_2 & -a_3 & -a_4 & \cdots & -a_{r-2} & -a_{r-1} \end{pmatrix}.$$

此外，在这种情形下，存在某个 $v\in E$，使得 $V=\{v, \phi(v), \phi^2(v), \cdots, \phi^{r-1}(v)\}$。

矩阵A叫作首1多项式$q\in K[x]$〔注〕的伴随矩阵。注意若$q=x+a_0$，则$A=(-a_0)$。

定理4.3的证明 ($\Longrightarrow$)：如果E是ϕ-循环空间，从定理4.2前面的注记可知存在$v\in E$，使E是循环$K[x]$-模$K[x]v$，其中E的$K[x]$-模结构是由 ϕ 诱导出来的。如果 $k_0v+k_1\phi(v)+\cdots+k_{r-1}\phi^{r-1}(v)=0(k_i\in K)$，则对于多项式 $f=k_0+k_1x+\cdots+k_{r-1}x^{r-1}$ 我们有$f(\phi)(v)=0$，于是在$E=K[x]v$上有$f(\phi)=0$。由于$\deg f\leqslant r-1<\deg q$，并且从定理4.1(i) 知道$q\mid f$，从而$k_i$均为0。所以$\{v, \phi(v), \cdots, \phi^{r-1}(v)\}$ 是线性无关的。如果 $fv=f(\phi)(v)$ $(f\in K[x])$是$E=K[x]v$中任意元素，我们有除法算式$f=qh+s$，其中 $s=\sum_{i=1}^{t}k_ix^i$的次数 $t<\deg q$。从而 $f(\phi)=q(\phi)h(\phi)+s(\phi)=0+s(\phi)=s(\phi)$，而$fv=f(\phi)(v)=s(\phi)(v)=k_0+k_1\phi(v)+\cdots+k_t\phi^t(v)$，$t\leqslant r-1$。因此

$$\{v, \phi(v), \cdots, \phi^{r-1}(v)\}$$

张成E，所以是E的一组基。由于 $q(\phi)=0$，我们有 $\phi(\phi^{r-1}(v))$

〔注〕 如果E看作是右K—向量空间，并且相应地构作映射的矩阵(见第505页)，则为了使此定理仍旧正确，q的伴随矩阵必须定义成A^t。

$=\phi^r(v)=-a_0v-a_1\phi(v)-\cdots-a_{r-1}\phi^{r-1}(v)$。由此立刻得到$\phi$对于$\{v,\ \phi(v),\ \cdots,\ \phi^{r-1}(v)\}$的矩阵是$q$的伴随矩阵。

($\Longleftarrow$)：如果A是ϕ对于基$\{v=v_1,\ v_2,\ \cdots,\ v_r\}$的矩阵，经过简单的计算就可知道$v_i=\phi^{i-1}(v)(2\leqslant i\leqslant r)$，并且$\phi^r(v)=\phi(v_r)=-a_0v-a_1\phi(v)-\cdots-a_{r-1}\phi^{r-1}(v)$。从而$E$是由$v$生成的$\phi$-循环空间，而$E=K[x]v$。由于$q(\phi)v=0$，从而在$E$上$q(\phi)=0$。因为

$$\{v,\ \phi(v),\ \cdots,\ \phi^{r-1}(v)\}$$

线性无关，所以不存在非零的次数小于 r 的$f\in K[x]$，使得$f(\phi)=0$。再用除法算式即知q是ϕ的极小多项式。 ∎

系4.4 设ψ：$E\to E$是域K上有限维向量空间E上的线性变换。则：E是ψ-循环空间并且ψ的极小多项式是 $q=(x-b)^r(b\in K)$ 的充要条件是 $\dim_K E=r$并且E存在有序基，使得ψ对于此基的方阵是

$$B=\begin{pmatrix} b & 1_k & 0 & 0 & \cdots & 0 & 0 \\ 0 & b & 1_k & 0 & \cdots & 0 & 0 \\ 0 & 0 & b & 1_k & \cdots & 0 & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & b & 1_k \\ 0 & 0 & 0 & 0 & \cdots & 0 & b \end{pmatrix}$$

$r\times r$方阵B叫做与$(x-b)^r\in K[x]$相结合的初等Jordan方阵。注意当$r=1$时，$B=(b)$。

系4.4的证明概要 设$\phi=\psi-b1_E\in \mathrm{Hom}_K(E,E)$。则：$q=(x-b)^r$是$\psi$的极小多项式$\Longleftrightarrow x^r$是 ϕ 的极小多项式（例如$\phi^r=(\psi-b1_E)^r=q(\psi)=0$）。$E$具有分别由$\phi$和$\psi$诱导出来的两个 $K[x]$-模结构。对于每个$f\in K[x]$和$v\in E$，则ϕ-结构中的$f(x)v$ 等于ψ-结构

中的$f(x-b)v$。因此，E 是ϕ-循环的$\Longleftrightarrow E$ 是ψ-循环的。由于$\psi=\phi+b1_E$，定理1.2表明，对于E的某个给定的（有序）基，ϕ的矩阵是x^r的伴随方阵$\Longleftrightarrow\psi$对于同一组基的矩阵是结合于$(x-b)^r$的初等Jordan方阵$B=A+bI_n$。然后将定理4.3用于ϕ，使用上述一些事实再将结果转化成关于ψ的命题，即可完成证明。 ∎

为了用上述结果得到 $\mathrm{Mat}_n K$ 上的相似标准型集合，我们需要

引理4.5 设$\phi:E\to E$是域K上n维向量空间E 上的线性变换。对于$1\leqslant i\leqslant n$，令M_i是K上的$n_i\times n_i$方阵，$n_1+n_2+\cdots+n_t=n$。则：$E=E_1\oplus E_2\oplus\cdots\oplus E_t$，其中每个$E_i$都是$E$的$\phi$-不变子空间，并且$M_i$是$\phi|E_i$对于$E_i$的某个有序基的矩阵$\Longleftrightarrow\phi$对于 E 的某个有序基的矩阵为

$$M=\begin{pmatrix} M_1 & & & 0 \\ & M_2 & & \\ & & \ddots & \\ 0 & & & M_t \end{pmatrix}$$

其中M_i的主对角线均在M的主对角线上。

引理4.5中的方阵M叫作是方阵$M_1,\cdots,M_t$(按这种次序)的直和。

引理4.5的证明概要 （$\Longrightarrow$）：对于每个i，设V_i是E_i的一组有序基，使得$\phi|E_i$对于V_i的矩阵是M_i。由于$E=E_1\oplus\cdots\oplus E_t$，易知 $V=\sum_{i=1}^{t}V_i$是E的一组基。验证M是ϕ对于V的矩阵（其中V中基元素的次序以显然的方式给出）。

($\Longleftarrow$)：反之，假设$U=\{u_1, \cdots, u_n\}$是E的一组基而M是ϕ对于U的矩阵，令E_1是E的子空间，并且以$\{u_1, \cdots, u_n\}$为基，而对于$i>1$，令E_i是E的子空间并且以$\{u_{r+1}, \cdots, u_{r+n_i}\}$为基，其中$r=n_1+\cdots+n_{i-1}$。则$E=E_1\oplus E_2\oplus\cdots\oplus E_t$，其中每个$E_i$均是$\phi$-不变的，并且$M_i$是$\phi|E_i$对于$\{u_{r+1}, \cdots, u_{r+n_i}\}$的矩阵。 ∎

定理4.6 设$\phi: E\to E$是域K上n维向量空间E的线性变换。则

(i) E存在一组基，使得ϕ对于这组基的矩阵是ϕ的不变因子$q_1, \cdots, q_t\in K[x]$的伴随方阵的直和。

(ii) E存在一组基，使得ϕ对于这组基的矩阵是ϕ的初等因子$p_1^{m_{11}}, \cdots, p_s^{m_{sk_s}}\in K[x]$的伴随方阵的直和。

(iii) 如果ϕ的极小多项式q有因式分解$q=(x-b_1)^{r_1}(x-b_2)^{r_2}\cdots(x-b_d)^{r_d}(b_i\in K)$（例如在$K$为代数封闭域时总可以这样作），则$\phi$的每个初等因子都具有形式$(x-b_i)^j(j\leqslant r_i)$。并且$E$有一组基，使得$\phi$对于这组基的矩阵是结合于$\phi$的初等因子的初等Jordan方阵的直和。

证明 是4.2—4.5诸结果的直接推论（对于(iii)还要用到$K[x]$的唯一因式分解性质），留给读者去作。从下面的系立刻得到$\mathrm{Mat}_n K$上两种（当K代数封闭时则是三种）相似标准型集合。

系4.7 设A是域K上的$n\times n$方阵。

(i) A相似于方阵D，其中D是唯一一组多项式$q_1, \cdots, q_t\in K[x]$的伴随方阵的直和，其中$q_1|q_2|\cdots|q_t$。方阵D是唯一确定的。

(ii) A相似于方阵M，其中M是唯一一组多项式$p_1^{m_{11}}, \cdots, p_s^{m_{sk_s}}\in K[x]$（$q_i$为$K[x]$中不可约多项式）的伴随方阵的直和。

如果不计$p_i^{m_{ij}}$的伴随方阵在M的主对角线上的次序，则M是唯一确定的。

(iii) 如果K是代数封闭域，则A相似于方阵J，其中J是结合于唯一一组多项式$\{(x-b)^m\}$ $(b\in K)$ 的初等 Jordan 方阵的直和。如果不计初等 Jordan 方阵在J的主对角线上的次序，则M是唯一确定的。

系4.7的证明见下面。第(i) 部分中的方阵D叫做方阵A的有理标准型。第 (ii)部分中的方阵M叫做方阵A的素有理标准型，而第 (iii) 部分中的方阵J叫做方阵A的 Jordan 标准型[注] "有理"一词是指的这样一个事实，即强调这里的矩阵相似是在给定的域K中而不是在K的扩域中 (见习题7)。在第 (i) 部分中所唯一决定的多项式q_1，…，q_t 叫作是方阵 A 的不变因子。类似地，在第 (ii) 部分中所唯一决定的多项式$q_i^{m_{ij}}$叫作是方阵 A 的初等因子。

系4.7的证明概要 (ii) 设$\phi: K^n\to K^n$是线性变换，它对于标准基的矩阵为 A(定理1.2)。系1.7和定理4.6 表明 A 相似于D，其中D为ϕ的初等因子$p_i^{m_{ij}}$的伴随方阵按某种次序的直和。如果A也相似于D_1，其中D_1是f_1，…，$f_b\in K[x]$的伴随方阵的直和，而f_1，…，f_b均是不可约多项式的幂，则D_1也是ϕ对于K^n的某一组基的矩阵 (系1.7)。根据定理4.3和引理4.5，$K^n=E_1\oplus E_2\oplus\cdots\oplus E_b$，其中每个$E_i$均是$\phi$-循环子空间，而$f_i$是$\phi|E_i$ 的极小多项式。由定理4.2的唯一性结果即知$\{f_i\}$恰好是ϕ的初等因子$\{p_i^{m_{ij}}\}$，从而D和D_1的区别只在于这些$p_i^{m_{ij}}$的伴随方阵沿主对角线的安排次序可能不同。类似地可以证明 (i) 和(ii)，并且由于不变因子(与

〔注〕 注意：某些作者用稍微不同的方式定义有理标准型和Jordan标准型。

初等因子不同）可以由整除性安排成唯一的次序，所以（i）中的唯一性可以叙述得更强些。 ∎

系4.8 设$\phi: E \to E$是域K上n维向量空间E上的线性变换。

(i) 如果ϕ对于某一组基的矩阵为 $A \in \mathrm{Mat}_n K$，则ϕ的不变因子和初等因子就是A的不变因子和初等因子。

(ii) $\mathrm{Mat}_n K$中两个方阵相似的充要条件是它们具有同样的不变因子(或者初等因子)。

证明作为练习。 ∎

注记：如果k是域K中的元素，则方阵kI_n是不可约多项式$x-k$，…，$x-k$的1×1伴随方阵的直和。于是由系 4.7 可知$x-k$，…，$x-k$是kI_n的初等因子。所以若$k_1 \neq k_2$，则由系4.8可知$k_1 I_n$和$k_2 I_n$不相似。因此当K是无限域的时候，$\mathrm{Mat}_n K$有无限多个相似等价类。另一方面，由定理2.6可知$\mathrm{Mat}_n K$只有$n+1$个不同的矩阵等价的等价类。

例 设E为有限维实向量空间，$\phi: E \to E$是线性变换，它的不变因子是$q_1 = x^4 - 4x^3 + 5x^2 - 4x + 4 = (x-2)^2(x^2+1) \in \boldsymbol{R}[x]$和$q_2 = x^7 + 6x^6 + 14x^5 - 20x^4 + 25x^3 - 22x^2 + 12x - 8 = (x-2)^3(x^2+1)^2 \in \boldsymbol{R}[x]$。由定理4.6(i)可知$\dim_{\boldsymbol{R}} E = 11$，而$\phi$的极小多项式是$q_2$。根据定理4.2后面的注记可知$\phi$在$\boldsymbol{R}[x]$中的初等因子是$(x-2)^3 = x^3 - 6x^2 + 12x - 8$，$(x-2)^2 = x^2 - 4x + 4$，$(x^2+1)^2 = x^4 + 2x^2 + 1$和$x^2+1$。根据定理4.6可知$E$存在两组基，使得$\phi$对于这两组基的矩阵分别是

$$D=\begin{pmatrix}
0 & 1 & 0 & 0 & & & & & & & \\
0 & 0 & 1 & 0 & & & & 0 & & & \\
0 & 0 & 0 & 1 & & & & & & & \\
-4 & 4 & -5 & 4 & & & & & & & \\
 & & & & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
 & & & & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
 & & & & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
 & & & & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 & 0 & & & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
 & & & & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
 & & & & 8 & -12 & 22 & -35 & 20 & -14 & -6
\end{pmatrix}$$

$$M=\begin{pmatrix}
0 & 1 & 0 & & & & & & & & \\
0 & 0 & 1 & & & & & & & & \\
8 & -12 & 6 & & & & & & & & \\
 & & & 0 & 1 & & & & & 0 & \\
 & & & -4 & 4 & & & & & & \\
 & & & & & 0 & 1 & 0 & 0 & & \\
 & & & & & 0 & 0 & 1 & 0 & & \\
 & & & & & 0 & 0 & 0 & 1 & & \\
 & & & & & -1 & 0 & -2 & 0 & & \\
 & 0 & & & & & & & & 0 & 1 \\
 & & & & & & & & & -1 & 0
\end{pmatrix}$$

方阵D是有理标准型，而M是素有理标准型．如果E是复向量空间，而$\psi: E\to E$是线性变换，并且具有同样的不变因子$q_1=(x-2)^2(x^2+1)\in \mathbf{C}[x]$和$q_2=(x-2)^3(x^2+1)^2\in \mathbf{C}[x]$，由于在$\mathbf{C}[x]$中$x^2+1=(x+i)(x-i)$，从而$\psi$在$\mathbf{C}[x]$中的初等因子为$(x-2)^3$，$(x-2)^2$，$(x+i)^2$，$(x+i)$，$(x-i)^2$和$(x-i)$．所以$\psi$对于$E$的某一组基的矩阵具有如下的 Jordan 标准型

$$J=\begin{pmatrix}
2 & 1 & 0 & & & & & & & \\
0 & 2 & 1 & & & & & 0 & & \\
0 & 0 & 2 & & & & & & & \\
 & & & 2 & 1 & & & & & \\
 & & & 0 & 2 & & & & & \\
 & & & & & -i & 1 & & & \\
 & & & & & 0 & -i & & & \\
 & & & & & & & -i & & \\
 & & & & & & & & i & 1 \\
 & 0 & & & & & & & 0 & i \\
 & & & & & & & & & & i
\end{pmatrix}$$

注记：矩阵$A\in \mathrm{Mat}_n K$在$K[x]$中的不变因子与A在$F[x]$中的不变因子是一样的，其中F为K的扩域(习题6)。但是，正如上例所展示的，A在K上的初等因子和A在F上的初等因子可能会不同。

在本节的最后我们给出计算一给定方阵A的不变因子的方法。按照系4.8可知，如果某个线性变换对于某一组基的矩阵是A，那末也就给出了计算此线性变换的不变因子的方法。该方法是下面命题的推论。

命题4.9 设A是域K上的$n\times n$方阵。则多项式方阵$xI_n-A\in \mathrm{Mat}_n K[x]$（在$K[x]$上）等价于对角方阵$D$，其中$D$具有非零对角元素$f_1$，…，$f_n\in K[x]$，每个$f_i$都是首1多项式，并且$f_1|f_2|\cdots|f_n$。那些不为常数的多项式组成$A$的不变因子。

注记：如果K是域，则$K[x]$为欧氏整环（系II.6.4)。从而由下面的证明和命题2.11后面的注记可知：方阵D可以从xI_n-A通过有限次初等行变换和列变换而得到。所以命题4.9事实上提供出求不变因子的一种构造性的方法。在证明的后面我们将给出例子。

命题4.9的证明概要 令$\phi: K^n \to K^n$是线性变换，并且它对于K^n的标准基$\{\varepsilon_i\}$的方阵是$A=(a_{ij})$。象通常一样，将K^n看成是由ϕ所诱导的$K[x]$-模。令F是以$U=\{u_1, \cdots, u_n\}$为基的自由$K[x]$-模。令$\pi: F \to K^n$是唯一的$K[x]$-模同态，使得$\pi(u_i)=\varepsilon_i (1 \leqslant i \leqslant n)$（定理IV.2.1）。令$\psi: F \to F$是唯一的$K[x]$-模同态，使得$\psi(u_i)=xu_i-\sum_{j=1}^{m} a_{ij}u_j$。则$\psi$对于基$U$的方阵是$xI_n-A$。

我们断言：$K[x]$-模序列$F \xrightarrow{\psi} F \xrightarrow{\pi} K^n \longrightarrow 0$是正合的。$\pi$显然是$K[x]$-模满同态。由于$A$是$\phi$的方阵并且$K^n$的$K[x]$-模结构是由$\phi$诱导的，从而

$$\pi(xu_i)=x\pi(u_i)=x\varepsilon_i=\phi(\varepsilon_i)=\sum_{j=1}^{n} a_{ij}\varepsilon_j.$$

于是对于每个i均有

$$\pi\psi(u_i)=\pi(xu_i-\sum_{j=1}^{n} a_{ij}u_j)$$

$$=\pi(xu_i)-\sum_{j} a_{ij}\pi(u_j)$$

$$=\sum_{j} a_{ij}\varepsilon_j-\sum_{j} a_{ij}\varepsilon_j=0,$$

从而$\mathrm{Im}\psi \subset \mathrm{Ker}\pi$。为证$\mathrm{Ker}\pi \subset \mathrm{Im}\psi$，只需验证$F$中元素$w$均有形式$w=\psi(v)+\sum_{j=1}^{n} k_j u_j (v \in F, k_j \in K)$即可。因为在这种情形下，如果$w \in \mathrm{Ker}\pi$，则

$$0=\pi(w)=\pi\psi(v)+\pi(\sum_{j} k_j u_j)=0+\sum_{j} k_j \varepsilon_j.$$

由于$\{\varepsilon_i\}$是K^n的一组基，从而k_j均为0。因此$w=\psi(v)$，即$\mathrm{Ker}\pi \subset \mathrm{Im}\psi$。因为$F$中元素均可表示成一些$fu_i$ ($f\in K[x]$) 之和，我们只需证明：对于每个i和t，均存在$v_{it}\in F$和$k_j\in K$，使得 $x^t u_i=\psi(v_{it})+\sum_{j=1}^{n} k_j u_j$。对于$t=1$和任意$i$，我们有$xu_i=\psi(u_i)+\sum_j a_{ij}u_j$ ($a_{ij}\in K$)。现在归纳地假设对于每个j均有$v_{j,t-1}\in F$和$k_{jr}\in K$，使得 $x^{t-1}u_j=\psi(v_{j,t-1})+\sum_{r=1}^{n} k_{jr}u_r$。则对于每个$i$均有

$$x^t u_i = x^{t-1}(xu_i) = x^{t-1}(\psi(u_i)+\sum_j a_{ij}u_j)$$

$$=\psi(x^{t-1}u_i)+\sum_j a_{ij}x^{t-1}u_j$$

$$=\psi(x^{t-1}u_i)+\sum_j a_{ij}(\psi(v_{j,t-1})+\sum_r k_{jr}u_r)$$

$$=\psi(x^{t-1}u_i+\sum_j a_{ij}v_{j,t-1})+\sum_r(\sum_j a_{ij}k_{jr})u_r.$$

因此$x^t u_i=\psi(v_{it})+\sum_r c_r u_r$，其中 $v_{it}=x^{t-1}u_i+\sum_j a_{ij}v_{j,t-1}\in F$ 而 $c_r=\sum_j a_{ij}k_{jr}\in K$。这就完成了归纳证明。所以$F\xrightarrow{\psi} F\xrightarrow{\pi} K^n\to 0$是正合的，于是$K^n\cong F/\mathrm{Ker}\pi=F/\mathrm{Im}\psi$。

由于$K[x]$是主理想整环，从命题2.11可知 xI_n-A 等价于对角方阵 $D=\begin{pmatrix} L_r & 0 \\ 0 & 0 \end{pmatrix}$，其中$r$是$xI_n-A$的秩而$L_r$是r×r 对角方阵并且有非零对角元素$f_1$，…，$f_r\in K[x]$，其中 $f_1|f_2|\cdots|f_r$。我们可以假设f_i均是首1多项式(不然的话，将 D 作适当的初等行变

换)。行列式$|xI_n-A|$显然是$K[x]$中的n次首1多项式。特别地，$|xI_n-A|\neq 0$。从定义1.8和定理3.5(iii)，(iv)可知$|D|$是$|xI_n-A|$乘以$K[x]$中单位，从而$|D|\neq 0$。因此D中每个对角元素均不为0。所以$L_r=D$并且$r=n$。由于D等价于xI_n-A，D是ψ对于F的某一对有序基$V=\{v_1,\cdots,v_n\}$和$W=\{w_1,\cdots,w_n\}$的方阵（定理1.6)。这就意味着对每个i均有$\psi(v_i)=f_iw_i$，并且$I_m\psi=K[x]f_1w_1\oplus\cdots\oplus K[x]f_nw_n$。

从而

$$K^n\cong F/\mathrm{Ker}\pi=F/\mathrm{Im}\psi=\frac{K[x]w_1\oplus\cdots\oplus K[x]w_n}{K[x]f_1w_1\oplus\cdots\oplus K[x]f_nw_n}$$

$$\cong K[x]w_1/K[x]f_1w_1\oplus\cdots\oplus K[x]w_n/K[x]f_nw_n$$

$$\cong K[x]/(f_1)\oplus\cdots\oplus K[x]/(f_n),$$

其中$f_1|f_2|\cdots|f_n$，并且f_i均是首1多项式。对于某个$t(0\leqslant t\leqslant n)$我们有$f_1=f_2=\cdots=f_t=1_k$，而$f_{t+1},\cdots,f_n$不为常数。于是当$i\leqslant t$时，$K[x]/(f_i)=K[x]/(1_k)=0$，而当$i>t$时，$K[x]/(f_i)$是阶为$f_i$的循环$K[x]$-模。从而$K^n$是非零扭循环$K[x]$-子模（即$\phi$-循环子空间）$E_{t+1},\cdots,E_n$的内直和，其中$E_{t+1},\cdots,E_n$的阶分别是$f_{t+1},f_n$，并且$f_{t+1}|f_{t+2}|\cdots|f_n$。由于$K^n$的$K[x]$-模结构是由$\phi$诱导的，从而$0=f_iE_i=f_i(\phi)E_i$。由此即知$f_i$是$\phi|E_i$的极小多项式。从而由定理4.2可知$f_{t+1},\cdots,f_n$是$\phi$（从而$A$）的不变因子。∎

例 如果$\phi:\mathbb{Q}^3\to\mathbb{Q}^3$是线性变换，并且它对于某一组基的方阵是$A=\begin{pmatrix}0&4&2\\-1&-4&-1\\0&0&-2\end{pmatrix}$，则$xI_3-A=\begin{pmatrix}x&-4&-2\\1&x+4&1\\0&0&x+2\end{pmatrix}$。通过适当的初等行变换和列变换，则有

$$\begin{pmatrix} x & -4 & -2 \\ 1 & x+4 & 1 \\ 0 & 0 & x+2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & x+4 & 1 \\ x & -4 & -2 \\ 0 & 0 & x+2 \end{pmatrix} \longrightarrow$$

$$\begin{pmatrix} 1 & x+4 & 1 \\ 0 & -4-x(x+4) & -2-x \\ 0 & 0 & x+2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -(x+2)^2 & -(x+2) \\ 0 & 0 & x+2 \end{pmatrix} \longrightarrow$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -(x+2)^2 & 0 \\ 0 & 0 & x+2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+2 & 0 \\ 0 & 0 & (x+2)^2 \end{pmatrix}.$$

从而由系4.8和命题4.9即知A和ϕ的不变因子是$x+2$，和$(x+2)^2$，而它们的极小多项式是$(x+2)^2$。

习　题

注：若不特别声明，E均指是域K上n维向量空间。

1. 如果A和B是K上$n\times n$方阵，它们的极小多项式分别是q_1和q_2，则A与B的直和（为$2n\times 2n$方阵）的极小多项式是q_1和q_2的最小公倍式。
2. 0线性变换$E\to E$的不变因子和初等因子均是$q_1=x$，$q_2=x$，…，$q_n=x$。
3. (*a*) 设a，b，c是域K中彼此不同的三个元素，$D\in \mathrm{Mat}_6K$是对角方阵，其主对角元素依次为a，a，a，b，b，c。则D的不变因子是$q_1=x-a$，$q_2=(x-a)(x-b)$ 和$q_3=(x-a)(x-b)(x-c)$。

   (*b*) 描述Mat_nK中任一对角方阵的不变因子。
4. 如果q是线性变换ϕ：$E\to E$ 的极小多项式，并且 $\dim_K E=n$，则 $\deg q\leqslant n$。
5. 首1多项式$f\in K[x]$的伴随方阵的极小多项式恰好是f。
6. 设F是K的扩域。则矩阵$A\in \mathrm{Mat}_nK$ 在$K[x]$中的不变因子等于A看作是F上方阵时在$F[x]$中的不变因子。[提示：K^n的一组K-基即是F^n的

F-基。然后利用线性变换。]

7. 设F是K的扩域。则：A，$B\in \mathrm{Mat}_n K\subset \mathrm{Mat}_n F$在$F$上相似$\Longleftrightarrow$它们在$K$上相似[见习题6]。

8. $A\in \mathrm{Mat}_n K$ 相似于一个对角方阵$\Longleftrightarrow$ A 的全部初等因子都是一次多项式。

9. 如果$A\in \mathrm{Mat}_n K$是幂零方阵（即对于某个$r>0$，$A^r=0$），则A相似于下面形式的方阵：除了次对角线（即主对角线之上相邻的那条对角线）上某些元素为1_K之外，其余元素均是零。

10. 对于下述各方阵$A\in \mathrm{Mat}_n \mathbf{Q}$，求它的所有可能的有理标准型和素有理标准型：(i) A是6×6方阵，其极小多项式为$(x-2)^2(x+3)$；(ii) A是7×7方阵，其极小多项式为$(x^2+1)(x-7)$。如果A看作是$\mathbf{C}$上方阵，求这些A的Jordan标准型。

11. 如果A是首1多项式 $f\in K[x]$的伴随方阵，$\deg f=n$。直接证明$A-xI_n$相似于一个对角方阵，其主对角元素为1_K，1_K，…，1_K，f。

12. $A\in \mathrm{Mat}_n K$ 叫作是幂等方阵，指的是$A^2=A$。求证 $\mathrm{Mat}_n K$中两个幂等方阵相似的充要条件是它们等价。

13. 每个$n\times n$方阵A均相似于它的转置A^t。

5. 特征多项式，特征向量和特征值

我们在本节中要研究域上有限维向量空间上一个线性变换的另一些不变量。因为其中某些结果在更一般的情形下也是对的，所以如果可能的话，我们将处理含幺交换环上有限秩的自由模。

如果A是含幺交换环K上的$n\times n$方阵，则xI_n-A是$K[x]$上的$n\times n$方阵，从而行列式$|xI_n-A|$为$K[x]$中元素。多项式$p_A=|xI_n$

$-A|\in K[x]$叫做方阵A的特征多项式。显然p_A是n次首1多项式。如果$B\in \mathrm{Mat}_n K$与A相似，令$B=PAP^{-1}$，由于xI_n属于环$\mathrm{Mat}_n K[x]$的中心，从而

$$p_B=|xI_n-B|=|xI_n-PAP^{-1}|=|P(xI_n-A)P^{-1}|$$
$$=|P||xI_n-A||P|^{-1}=|xI_n-A|=p_A.$$

也就是说，相似方阵有同样的特征多项式。

设ϕ：$E\to E$是秩n（有限）的自由K-模E上的自同态（见定义IV.2.8和系IV.2.12）。如果A是ϕ对于某一组有序基的方阵，则定义p_A为自同态ϕ的特征多项式，并且表示成p_ϕ。因为表示ϕ的两个方阵是相似的(系1.7)，所以p_ϕ与A的选取方式无关。

引理5.1 (i) 如果A_1，A_2，…，A_r是含幺交换环K上的一些方阵（体积大小不必相同），$P_i\in K[x]$是A_i的特征多项式，则$P_1P_2\cdots P_r\in K[x]$是A_1，A_2，…，A_r的直和方阵的特征多项式。

(ii) 首1多项式$f\in K[x]$的伴随方阵C的特征多项式就是f。

证明概要 (i) 如果$A\in \mathrm{Mat}_n K$，$B\in \mathrm{Mat}_m K$，则

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}=\begin{pmatrix} A & 0 \\ 0 & I_m \end{pmatrix}\begin{pmatrix} I_n & 0 \\ 0 & B \end{pmatrix},$$

从而$\begin{vmatrix} A & 0 \\ 0 & B \end{vmatrix}=\begin{vmatrix} A & 0 \\ 0 & I_m \end{vmatrix}\begin{vmatrix} I_n & 0 \\ 0 & B \end{vmatrix}=|A||B|.$

然后即可归纳证明方阵B_1，…，B_k的直和方阵的行列式是$|B_1||B_2|\cdots|B_k|$。

(ii) 将$|xI_n-C|$按最后一行展开即知f是C的特征多项式。∎

定理5.2 设ϕ：$E\to E$为域K上n维向量空间上的线性变换，并且它的特征多项式，极小多项式和不变因子分别是p_ϕ，q_ϕ和

q_1，…，$q_t \in K[x]$。

(i) 特征多项式是不变因子的乘积，即：$p_\phi = q_1 q_2 \cdots q_t = q_1 q_2 \cdots q_{t-1} q_\phi$。

(ii) (Cayley-Hamiltom) ϕ 是它的特征多项式的根，即 $p_\phi(\phi) = 0$。

(iii) $K[x]$中一个不可约多项式可以整除p_ϕ的充要条件是它可以整除q_ϕ。

以上(i)—(iii) 诸条结论作必要的改动，则对于任意方阵$A \in \mathrm{Mat}_n(K)$也是对的。

证明 根据定理4.6，ϕ对于某一组基的方阵是q_1，…，q_t的伴随方阵的直和方阵D。因此$p_\phi = p_D = q_1 q_2 \cdots q_t$(引理5.1)。又由定理4.2有$q_\phi = q_t$，从而由$q_\phi(\phi) = 0$推出$p_\phi(\phi) = 0$。(iii) 是(i)和事实$q_1 | q_2 | \cdots | q_t$的直接推论。利用系4.7和4.8可以同样地证明对于$A \in \mathrm{Mat}_n K$的类似结论。∎

注记：Cayley-Hamilton 定理 (定理5.2(ii))在任意含幺交换环上均是对的(习题2)。

定义5.3 设ϕ：$E \to E$是域 K上向量空间E上的线性变换。非零向量$u \in E$叫做ϕ的特征向量，是指$\phi(u) = ku$ 其中k是K中某个元素。元素$k \in K$叫做ϕ的特征值，是指存在某个非零向量$u \in E$，使得$\phi(u) = ku$。

两个不同的（甚至是线性无关的）特征向量可能有同样的特征值。另一方面，对应于不同特征值的一些特征向量必定是线性无关的（习题8)。

定理5.4 设ϕ：$E \to E$是域K上有限维向量空间E上的线性变

换，则ϕ的全部特征值即是ϕ的特征多项式p_ϕ在K中的全部根。

注记：特征多项式$p_\phi \in K[x]$在K中可能无根。在这种情况下，ϕ(在K上)没有特征值和特征向量。

定理5.4的证明概要 设A是ϕ对于某一组有序基的方阵。如果$k\in K$,则$kI_n - A$是$k1_E - \phi$对于同一组基的方阵。如果存在某个非零向量$u\in E$，使得$\phi(u) = ku$，则$(k1_E - \phi)(u) = 0$,从而$k1_E - \phi$不是单同态。于是$kI_n - A$不可逆(引理1.5)，所以由命题3.7和习题3.6可知$|kI_n - A| = 0$。即k是$p_\phi = |xI_n - A|$的根。反之，如果k是p_ϕ的根，则$|kI_n - A| = 0$。从而由引理1.5和命题3.7(或者习题3.6)可知$kI_n - A$不是同构。由于E是有限维的，从而$kI_n - A$不是单同态(习题IV.2.14)。因此有非零向量$u\in E$，使得$(k1_E - \phi)(u) = 0$，于是$\phi(u) = ku$，即k是ϕ的特征值。∎

如果$k\in K$是K-向量空间E上自同态ϕ的特征值，不难看出$C(\phi, k) = \{v\in E | \phi(v) = kv\}$是$E$的非零子空间。我们将$C(\phi,k)$称为$k$的特征空间。

定理5.5 设$\phi: E\to E$是域K上有限维向量空间E上的线性变换。则：ϕ对于E的某一组有序基的方阵是对角方阵$D \Longleftrightarrow \phi$的全部特征向量张成$E$。此外，在这种情形下，$D$的全部对角元素即是$\phi$的全部特征值，并且每个特征值$k\in K$在对角线上出现$\dim_K C(\phi, k)$次。

证明 根据定理IV.2.5可知，ϕ的全部特征向量张成$E \Longleftrightarrow E$具有由特征向量所构成的基。显然，$U = \{u_1, \cdots, u_n\}$是一组特征向量所构成的基并且其特征值分别是$k_1, \cdots, k_n \in K \Longleftrightarrow \phi$对于$U$的方阵是对角方阵$D$,它的主对角线元素为$k_1, k_2, \cdots, k_n$。在这种

情形下，假设$v=\sum_{i=1}^{n} r_i u_i$是ϕ的特征向量并且$\phi(v)=kv$。由于U是线性无关的，而$\sum_{i=1}^{n} kr_i u_i = kv = \phi(v) = \sum_{i=1}^{n} r_i \phi(u_i) = \sum_{i=1}^{n} r_i k_i u_i$，我们有$kr_i = r_i k_i (1 \leqslant i \leqslant n)$。从而当$r_i \neq 0$时便有$k = k_i$。但是由于$v \neq 0$，从而至少有一个$r_i \neq 0$。因此$\phi$的特征值只能是$k_1, \cdots, k_n$。此外，如果$k$是$\phi$的特征值并且它在$D$的对角线上出现$t$次，令$u_{i_1}, \cdots, u_{i_t}$是以$k$为特征值的$U$中元素，根据上面的推理可知$\{u_{i_1}, \cdots, u_{i_t}\}$张成$C(\phi, k)$。由于$\{u_{i_1}, \cdots, u_{i_t}\}$是线性无关的，因此它是$C(\phi, k)$的一组基。从而$\dim_K C(\phi, k) = t$。 ∎

域K上的$n \times n$方阵A的特征值和特征向量分别定义成是线性变换$\phi: K^n \to K^n$的特征值和特征向量，其中ϕ对于标准基的方阵为A。从定理5.4可知，A的特征值是K上n维向量空间上任意自同态的特征值，只要这个自同态对于某一组基的方阵是A。

最后我们简单讨论一下方阵的另一些相似不变量。

命题5.6 设K是含幺交换环。ϕ是秩n自由K-模上的自同态，$A=(a_{ij}) \in \mathrm{Mat}_n K$是$\phi$相对于某一组有序基的方阵。如果$\phi$和$A$的特征多项式是$p_\phi = p_A = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in K[x]$，则

$$(-1)^n c_0 = |A|, \quad -c_{n-1} = a_{11} + a_{22} + \cdots + a_{nn}.$$

证明 从定理3.5 (viii) 可知$c_0 = p_\phi(0) = |0I_n - A| = |-A| = (-1)^n |A|$。将$p_\phi = |xI_n - A|$按第一行展开，展开式的第一项是$(x-a_{11})(x-a_{22})\cdots(x-a_{nn}) = x^n - (a_{11}+a_{22}+\cdots+a_{nn})x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$，$b_i \in K$。而展开式其余各项均不包含$x^{n-1}$项，从而$-c_{n-1} = a_{11} + \cdots + a_{nn}$。 ∎

设K是含幺交换环。K上$n\times n$方阵$A=(a_{ij})$的迹是$a_{11}+a_{22}+\cdots+a_{nn}\in K$，并且表示成$TrA$。秩为$n$的自由$K$-模的自同态$\phi$的迹是$TrA$(表示成$Tr\phi$)，其中$A$是$\phi$对于某一组有序基的方阵。由于$p_\phi=p_A$与方阵$A$的选取无关，从而由命题5.6可知$Tr\phi$也与$A$的选取无关。由系1.7可知(或者利用下面的(iii)直接推出)，相似方阵有同样的迹。对于$A,B\in Mat_nK$，$k\in K$，不难看出有：

(i) $Tr(A+B)=Tr(A)+Tr(B)$;

(ii) $Tr(kA)=kTrA$;

(iii) $Tr(AB)=Tr(BA)$。

习题9揭示出这里定义的迹与伽罗华理论中定义的迹函数（定义V.7.1)之间的联系。

习　题

注：除非特别声明，K永远是含幺交换环。

1. 直接证明K上一个方阵和它的转置具有同样的特征多项式。

2. (Cayley-Hamiltom) 如果ϕ是有限秩的自由K-模E上的自同态，则$p_\phi(\phi)=0$.[提示：如果A是ϕ的方阵而$B=xI_n-A$,则在$\mathrm{Mat}_nK[x]$中$B^aB=|B|I_n=p_\phi I_n$。如果E是由ϕ诱导的$K[x]$-模，而ψ是以B为矩阵的$K[x]$-模同态$E\to E$，则对于每个$u\in E$均有$\psi(u)=xu-\phi(u)=\phi(u)-\phi(u)=0$.]

3. 如果A是K上的$n\times m$矩阵，B是K上的$m\times n$方阵，则$x^mp_{AB}=x^np_{BA}$。此外，如果$n=m$,则$p_{AB}=p_{BA}$。[提示：设$C=\begin{pmatrix}xI_n & A\\ B & I_m\end{pmatrix}$，$D=\begin{pmatrix}I_n & 0\\ -B & xI_m\end{pmatrix}$，它们均是$K[x]$上的$(m+n)\times(m+n)$方阵，注意$|CD|=|DC|$.]

4. (a) 给出$\mathbf{Q}$上三个3×3方阵，使它们彼此互不相似，并且每个方阵均只

有 -2 是它的特征值.

(*b*) 给出$\mathbf{R}$上一个4×4方阵，使得它在$\mathbf{R}$上的特征值为±1，而在$\mathbf{C}$上的特征值为±1和$\pm i$.

5. 设K是域而$A\in \mathrm{Mat}_n K$.

(*a*) 0是A的特征值$\Longleftrightarrow A$不可逆.

(*b*) 如果$k_1, \cdots, k_r\in K$是A的全部特征值（不必不同），$f\in k[x]$，则$f(A)\in \mathrm{Mat}_n K$的全部特征值是$f(k_1), \cdots, f(k_r)$.

6. 如果ϕ和ψ都是代数封闭域K上有限维向量空间的自同态，并且$\phi\psi=\psi\phi$，则ϕ和ψ具有一个公共特征向量.

7. (*a*) 设ϕ和ψ是有限维向量空间E的自同态，并且$\phi\psi=\psi\phi$. 如果E具有由ϕ的特征向量构成的一组基，也具有由ψ的特征向量构成的一组基，则E必具有由ϕ和ψ的公共特征向量所构成的一组基.

(*b*) 将(*a*)叙述成关于与对角方阵相似的方阵的一个命题.

8. 设$\phi: E\to E$是域K上向量空间E的线性变换. 如果U是一个由ϕ的一些特征向量所组成的集合，并且这些特征向量所对应的特征值是两两不同的，则U是线性无关集合.[提示：如果U是线性相关的，则有关系$r_1u_1+\cdots+r_tu_t=0$ $(u_i\in U,\ 0\neq r_i\in K)$，并且$t$是有此性质的最小正整数. 利用变换$k_1\mathbf{1}_E-\phi$(其中$\varphi(u_1)=k_1u_1$)即导致矛盾.]

9. 设F是域K的扩域，$u\in F$. 令$\phi_u: F\to F$是由$v\longmapsto uv$给出的向量空间F的自同态. 则

(*a*) $Tr\phi$是定义V.7.1中给出的元素u的迹$T_K^F(u)$. [提示：先考虑$F=K(u)$的情形.]

(*b*) ϕ的行列式是元素u的范$N_K^F(u)$.

10. 设K是域而$A\in \mathrm{Mat}_n K$.

(*a*) 如果A是幂零的（即存在某个m使得$A^m=0$），则对于每个$r\geq1$均有$TrA^r=0$.[提示：A^r的极小多项式为x^t，并且A^r相似于它的有理标准型或者Jordan标准型.]

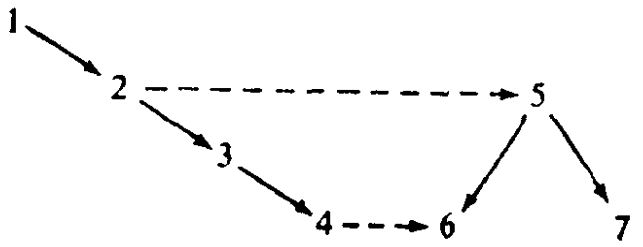
(*b*) 如果$\mathrm{char}k=0$. 并且$TrA^r=0$（对于每个$r\geq1$），则A是幂零方阵.

第VIII章　交换环和交换模

本章大部分内容是对通常称作交换代数的学科作一个简略的介绍。我们从链条件(第1节)和素理想(第2节)开始，它们在研究交换代数的时候均起着中心的作用。事实上，在第1节中可以不必加上交换性的限制，因为这些内容在研究任意环的时候都是重要的(第IX章)。

我们按照一个相当熟悉的模式来叙述交换环的理论，即试图对于某些环得到一个结构理论，这些环具有某些性质，而这些性质在各种熟知的环中已被证明是很有用处的。因此，我们在第2节和第3节考虑理想的准素分解（类似于整环中元素的因子分解）。然后研究具有象整数环那样性质的一些环，如Dedekind 环（第6节)和Noether 环（第4节)。分析 Dedekind 整环的时候需要关于环的扩张的一些知识(第5节)，这些知识也用来证明Hilbert 零点定理(第7节)，这是一个关于多项式环$K[x_1,\cdots x_n]$中理想的一个著名的经典结果。

除了在第 1 节中之外，所有的环都是交换环。本章各节之间的依赖关系大致如下图所示



其中虚线$A\dashrightarrow B$表示在第B节中使用第A节中的个别结果，但是第B节本质上不依赖于第A节。第5节不需要第1节，但是第4节需要第1节。第4节中只有一个重要结果依赖于第2节和第3节。但正如习题中所显示的，如果采用另一种证明方法，那么这个依赖关系也可以消除。

1. 链 条 件

在本节中我们简要介绍一下关于模和环的升链和降链条件的基本事实。这些事实在本章其余各节和第IX章中将会用到。在本节中环不必是交换环，也不必有幺元素。

定义1.1 模A称作满足子模升链条件（ACC）（或者叫作Noether模），是指对于A的每个子模链$A_1\subset A_2\subset A_3\subset\cdots$，均有整数$n$，使得当$i\geqslant n$时均有$A_i=A_n$。

模B称作是满足子模降链条件（DCC）（或者叫作是Artin模），是指对于A的每个子模链$A_1\supset A_2\supset A_3\supset\cdots$，均有整数$n$，使得当$i\geqslant n$时均有$A_i=A_n$。

例 $\boldsymbol{Z}$-模（即Abel群）$\boldsymbol{Z}$满足子模升链条件，但是不满足降链条件（习题II.3.5）。$\boldsymbol{Z}$-模$Z(p^\infty)$满足降链条件，但是不满足升链条件（习题II.3.13）。

如果环R看成是它本身上的左（右）模，那末不难看出，R的子模恰好是R的左（右）理想。所以在这个时候，通常不是讲子模的链条件，而是讲左理想或者右理想的链条件。

定义1.2 环 R叫作是左(右)Noether 环，是指R满足左(右)理想的升链条件. 假如R同时是左 Noether环和右Noether环，便称它为Noether环.

环 R叫作是左(右)Artin环，是指 R满足左 (右) 理想的降链条件. 假如R同时是左Artin环和右Artin环，便称它为Artin环.

换句话说，环 R 是左 (右)Noether 的，如果它是左(右) Noether R-模的话. 对于Artin 环则有类似的论断. 于是，下面的所有定义和关于具有子模升链或降链条件的模上的结果，经过必要的修改，均可用到(左或右)Noether环和Artin环上来.

例 体D同时是Noether环和Artin环，这是因为只有D和O是它的左理想或右理想 (习题IV.2.7). 每个交换主理想环都是Noether环(引理IV.3.6). 而 $\boldsymbol{Z}$, Z_n, $F[x]$(F为域)均是它的特殊情形.

例 体D上$n\times n$方阵全体构成环 $\mathrm{Mat}_n D$，它既是 Noether 环也是Artin环(见后面的系1.1.2).

注记：右Noether环 (或 Artin 环)不必为左 Noether 环 (或 Artin环)(习题1). 习题II.3.5表明Noether 环不必为Artin 环. 但是，每个具有幺元素的左(右)Artin环均是左(右)Noether环(见后面的习题IX.3.13).

在引论的第7节中，我们定义了半序集合$(C,\leqslant)$中的极大元. 类似地可以定义极小元：$b\in C$ 是极小元，是指对于每个元素$c\in C$，只要c和b可以比较，就必然 $b\leqslant c$. 注意：不必对于每个$c\in C$均有$b\leqslant c$. 另一方面，C 可以具有许多个极小元，也可能没有极小元.

定义1.3 模A叫作是满足子模极大条件（极小条件），是指A的每个子模非空集合均有极大(极小)元素（对于集合论的包含关系）。

定理1.4 模A满足子模升链(降链)条件的充要条件是A满足子模极大(极小)条件。

证明 假设A满足子模极小条件，并且$A_1 \supset A_2 \supset \cdots$是子模链。则集合$\{A_i \mid i \geqslant 1\}$有极小元素，假定极小元素为$A_n$，于是当$i \geqslant n$时，由假设条件我们有$A_n \supset A_i$，而由极小性又有$A_n \subset A_i$，从而对于每个$i \geqslant n$均有$A_i = A_n$。即$A$满足降链条件。

反之，假设A满足降链条件，而S是A的子模非空集合。则存在$B_0 \in S$。如果S没有极小元，那末对于S中每个子模B，均至少还存在一个子模$B' \in S$，使得$B \supsetneq B'$。对于S中每个B均取这样的一个B'（选择公理）。这就定义出一个函数$f: S \to S$，$B \mapsto B'$。从引论中的定理6.2(其中对于每个n均取$f_n = f$)，可知存在函数φ：$\boldsymbol{N} \to S$，使得

$$\varphi(0) = B_0, \quad \varphi(n+1) = f(\varphi(n)) = \varphi(n)'.$$

如果用$B_n \in S$表示$\varphi(n)$，则有序列$B_0 \supsetneq B_1 \supsetneq B_2 \supsetneq \cdots$，这就与降链条件相矛盾。所以$S$必有极小元，即$A$满足极小条件。

类似地可证升链条件和极大条件的等价性。∎

定理1.5 假设$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$是模的短正合序列。则：$B$满足子模的升(降)链条件$\Longleftrightarrow A$和$C$均满足子模的升(降)链条件。

证明概要 如果B满足升链条件，则它的子模$f(A)$也是如此。由正合性知A同构于$f(A)$，从而A满足升链条件。如果$C_1 \subset C_2 \subset \cdots$是$C$的子模链，则$g^{-1}(C_1) \subset g^{-1}(C_2) \subset \cdots$是$B$的子模链。因此存在$n$，使得当$i \geqslant n$时均有$g^{-1}(C_i) = g^{-1}(C_n)$。由正合性可知$g$为

满同态，因此对每个$i \geqslant n$均有$C_i = C_n$。即C也满足升链条件。

假设A和C均满足升链条件，而 $B_1 \subset B_2 \subset \cdots$ 是B的一个子模链。对于每个 i，令

$$A_i = f^{-1}(f(A) \cap B_i),\quad C_i = g(B_i).$$

再令$f_i = f|A_i$，$g_i = g|B_i$。对于每个$i \geqslant n$，证明下面序列

$$0 \to A_i \xrightarrow{f_i} B_i \xrightarrow{g_i} C_i \to 0.$$

是正合的。再证明 $A_1 \subset A_2 \subset \cdots$，$C_1 \subset C_2 \subset \cdots$。根据假设可知存在整数$n$，使得对于每个$i \geqslant n$均有$A_i = A_n$和$C_i = C_n$。对于每个$i \geqslant n$，图表

$$\begin{array}{ccccccc} 0 \to & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n & \to 0 \\ & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta_i} & & \downarrow{\scriptstyle \gamma} & \\ 0 \to & A_i & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_i & \to 0, \end{array}$$

是交换的，并且两个行均是正合的，其中α和γ均是恒等映射，而β是包含映射。由引理IV.1.17推出β_i也为恒等映射，从而B也满足升链条件。降链条件的情形可以类似地证明。∎

系1.6 如果A是模B的子模。则B满足升(降)链条件$\Longleftrightarrow A$和B/A均满足升(降)链条件。

证明 将定理1.5用于序列$0 \to A \xrightarrow{\subseteq} B \to B/A \to 0$。∎

系1.7 如果$A_1, \cdots, A_n$是模，则直和$A_1 \oplus A_2 \oplus \cdots \oplus A_n$满足升(降)链条件$\Longleftrightarrow$每个$A_i$均满足升(降)链条件。

证明概要 对n作数学归纳法。当$n = 2$时，将定理1.5用于序列$0 \to A_1 \xrightarrow{l_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$即可。∎

定理1.8 如果R是含幺左 Noether(Artin) 环，则每个有限生成幺作用R-模A均满足子模升链(降链)条件。

将"左"均改成"右"之后，类似的命题也是对的。

证明 如果A是有限生成的，由系IV.2.2可知，存在有限生成自由R-模F和满同态π：$F\to A$。根据定理 IV.2.1，F 是有限多个R的直和，再由系1.7即知F是左Noether(Artin)模。从而由系1.6可知$A\cong F/\mathrm{Ker}\pi$也是左 Noether(Artin)模。∎

下面一个刻划升链条件的方式，对于降链条件则没有类似的命题。

定理1.9 模A满足子模升链条件$\Longleftrightarrow A$的每个子模均是有限生成的。特别地，交换环R是Noether环$\Longleftrightarrow R$的每个理想均是有限生成的。

证明 ($\Longrightarrow$)：如果B是A的一个子模，以S表示B的全部有限生成子模所构成的集合。S是非空的($0\in S$)。根据定理1.4，S有极大元C。假设C是由$c_1,c_2,\cdots c_n$ 有限生成的。对于每个 $b\in B$，以D_b表示由$b,c_1,c_2,\cdots c_n$生成的B的子模，则$D_b\in S$，而 $C\subset D_b$。由于C是极大元，从而对于每个$b\in B$均有$D_b=C$，于是$b\in D_b=C$，从而 $B\subset C$。但是由构作方式可知 $C\subset B$。从而$B=C$，即B是有限生成的。

($\Longleftarrow$)：给了子模链$A_1\subset A_2\subset A_3\subset\cdots$，容易证明$\bigcup\limits_{i\geqslant 1}A_i$ 也是A的子模，从而是有限生成的，设它是由$a_1,\cdots,a_k$ 有限生成的。由于每个a_i都是某个A_j中的元素，令n是一个下 标，使得对于每个$i=1,2,\cdots,k$ 均有$a_i\in A_n$，这时$\bigcup A_i\subset A_n$，所以对于每个 $i\geqslant n$

均有 $A_i = A_n$。 ∎

在本节的最后，我们把第II.8节关于群上子正规列的主要结果推广到模上来。我们介绍这些内容是为了证明系1.12。而系1.12在第IX章中是有用的。开始我们先给出一大堆定义，其中大多数与第II.8节中对于群所给出的那些定义是完全一致的。

模 A 的一个正规列是一个子模链：$A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n$。此序列的因子是商模

$$A_i/A_{i+1} \quad (0 \leqslant i \leqslant n-1).$$

序列中真包含关系的个数(=非平凡的因子个数)叫作是该序列的长度。正规列 $A_0 \supset A_1 \supset \cdots \supset A_n$ 之内插入有限个另外的子模之后，所得到的正规列叫作是原序列的细化。如果新序列的长度大于原序列的长度，便称新序列是原序列的真细化。两个序列叫作是等价的，是指在它们的非平凡因子之间存在着一一对应，并且对应的因子都是同构的模。于是，等价的序列必然有相同的长度。A 的一个组成列是指一个正规列 $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n = 0$，使得每个因子 A_k/A_{k+1} $(0 \leqslant k \leqslant n-1)$ 均不为0并且均没有非零真子模。[注]

第II.8节中的各种结果均可转移到模上来。例如：组成列没有真细化，从而它等价于它的任意一个细化（见定理IV.1.10，定理II.8.4和引理II.8.8）。Schreier，Zassenhaus和Jordan—Hölder定理对于模也是对的：

定理1.10 模 A 的任意两个正规列均有等价的细化。A 的任

[注] 如果 R 具有1，我们把不具有真子模的非零幺作用模叫作是单模。于是，一个组成列即是所有因子均为单模的正规序列 $A = A_0 \supset A_1 \supset \cdots \supset A_n = 0$。如果 R 不具有1，则要采用某种不同的方式来定义单性，见定义IX.1.1和其后的注记。

意两个组成列都是等价的.

证明 请参见关于群的对应结果（引理II.8.9，定理II.8.10和II.8.11）. ∎

定理1.11 非零模 A 具有组序列$\Longleftrightarrow A$ 同时满足子模的升链和降链条件.

证明 （$\Longrightarrow$）：假设 A有长度为n的组成列S. 如果A不满足升链条件或者不满足降链条件，我们均可以找到A的一个长为$n+1$的正规列T：

$$A = A_0 \supsetneqq A_1 \supsetneqq A_2 \supsetneqq \cdots \supsetneqq A_n \supsetneqq A_{n+1}$$

根据定理1.10，S 和T具有等价的细化. 组成列S的细化应当与S有相同长度n，而T的每个细化的长度至少为$n+1$. 但是等价序列应当有相同的长度，这就导致矛盾. 所以 A同时满足升链条件和降链条件.

（$\Longleftarrow$）：如果B是A的非零子模，令

$$S(B) = \{C \mid C\text{为}B\text{的子模，并且}C \neq B\}.$$

如果B没有真子模，则 $S(B) = \{0\}$. 此外我们也定义$S(0) = \{0\}$. 对于每个B，由定理1.4可知$S(B)$存在极大元 B'. 以S表示A的全部子模所构成的集合. 定义映射 f：$S \to S$，$f(B) = B'$（为了能够同时选取这些B'，这里需要选择公理）. 由引论中的归纳定理6.2（对每个n令$f = f_n$），可知存在一个函数φ：$\boldsymbol{N} \to S$，使得

$$\varphi(0) = A,\ \varphi(n+1) = f(\varphi(n)) = \varphi(n)'.$$

如果令$A_i = \varphi(i)$，由构作方式可知$A \supset A_1 \supset A_2 \supset \cdots$为降链. 于是存在$n$，使得对于每个$i \geqslant n$均有$A_i = A_n$. 由于$A_{n+1} = A_n' = f(A_n)$，从$f$的定义可知$A_{n+1} = A_n \Longrightarrow A_n = 0 = A_{n+1}$. 以$m$表示使$A_m = 0$的最小整数. 则$m \leqslant n$，并且对于每个$k < m$均有$A_k \neq 0$. 进而，对于

每个$k<m$，A_{k+1}是A_k的极大子模并且$A_k \supsetneq A_{k+1}$。从而每个A_k/A_{k+1}均不为0，并且由定理IV.1.10可知它们均没有非零真子模。于是$A \supset A_1 \supset \cdots \supset A_n = 0$是$A$的组成列。∎

系1.12 如果D是体，则D上$n \times n$方阵形成的环$\mathrm{Mat}_n D$既是Noether环也是Artin环。

证明概要 由定义1.2和定理1.11可知只需证明$R = \mathrm{Mat}_n D$具有左R-模和右R-模的组成列。对于每个i，以$e_i \in R$表示在(i,i)位置上为1_D而其余元素均是0的方阵。证明$\mathrm{Re}_i = \{\mathrm{Ae}_i \mid A \in R\}$是$R$的左理想(子模)，并且它是由$R$中第$i$列之外的诸列均为零的全部这种方阵所构成的。证明$\mathrm{Re}_i$是极小非零左理想(即没有非零真子模)，一种证法是利用初等变换方阵（定义VII.2.7和定理VII.2.8)。令$M_0 = 0$，对于每个$i \geqslant 1$，令$M_i = R(e_1 + e_2 + \cdots + e_i)$。证明每个$M_i$均是$R$的左理想，并且$M_i/M_{i-1} \cong \mathrm{Re}_i$，从而$R = M_n \supset M_{n-1} \supset \cdots \supset M_1 \supset M_0 = 0$是左$R$-模组成列。改用右理想$e_i R = \{e_i A \mid A \in R\}$，用类似的推理可证$R$有右$R$-模组成列。∎

习　题

1. (a) 环$\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a \in \mathbf{Z}, b, c \in \mathbf{Q}\right\}$是右Noether环，但不是左Noether环。

   (b) 环$\left\{\begin{pmatrix} d & r \\ 0 & s \end{pmatrix} \mid d \in \mathbf{Q}, r, s \in \mathbf{R}\right\}$是右Artin环，但不是左Artin环。

2. 如果I是主理想整环R中的非零理想，则I/R同时是Noether环和Artin环。

3. 设S是含幺交换Noether环R的一个乘法子集合，则$S^{-1}R$是Noether环。

4. 设R是含幺交换环。如果R的理想I不是有限生成的，则存在一个无限的

理想真升链$J_1 \subsetneq J_2 \subsetneq \cdots$，使得对于每个$k$均有$J_k \subset I$。但是这些$J_k$的并不一定等于$I$。

5. 左Noether(Artin)环的同态象也是左Noether(Artin)环。

6. 环R为左Noether(Artin)环$\Leftrightarrow$对于每个$n \geqslant 1$，$\mathrm{Mat}_n R$均为左Noether(Artin)环。

7. Artin整环必是域。〔提示：为了求$a \neq 0$的逆元素，考虑$(a) \supset (a^2) \supset (a^3) \supset \cdots$.〕

2. 素理想和准素理想

我们的主要目的是研究某些交换环中的理想结构。首先发展素理想的基本性质，然后引进理想的根并且定义准素理想。最后讨论理想的准素分解。除了定理2.2以外，所有的环均是交换环。

开始我们先谈一些背景性材料，它们是我们即将要引进的概念的动机，也是一些所熟悉的例子的源泉。本节中有很多内容都是由于研究主理想整环而产生的。我们知道，这样一个整环D是唯一因子分解整环(定理III.3.7)。

D的唯一因子分解性质可以用理想的语言叙述成如下的方式：D中每个真理想均是一些极大理想(从而为素理想)之乘积，并且不计次序这些极大理想是唯一确定的(习题III.3.5)。D中每个非零素理想都可以写成(p)，根据定理III.3.4可知p是素元(=不可解元)，并且$(p)^n = (p^n)$。从而D中每个真理想(a)均可（不计次序)唯一写成如下形式：

$$(a)=(p_1^{n_1})(p_2^{n_2})\cdots(p_r^{n_r})=(p_1^{n_1})\cap(p_2^{n_2})\cap\cdots\cap(p_r^{n_r}),$$

其中$n_i>0$，而p_i是彼此不同的素元(习题III.3.5)。现在理想$Q=(p^n)$(p为素元)有如下的性质：$ab\in Q$，$a\notin Q\Longrightarrow$有k使得$b^k\in Q$(习题III.3.5)。这样一个理想称作是准素理想。上面的讨论表明，主理想整环中的每个理想均以唯一的方式表示成为有限个准素理想之交。进而，D中这些准素理想与素理想有明显的联系。事实上，每个准素理想$(p^n)=(p)^n$均是一个素理想的幂。

按照上面所勾划的考虑方式，我们的观点从考虑D中元素唯一表达成素元之乘积，转向去考虑主理想整环D中理想的“准素分解”。我们现在将要对于更广泛的一些环(例如，理想不必为主理想，而准素理想也不必为素理想的幂)研究理想的“准素分解”。首先从关于素理想的某些事实开始。

定理2.1 交换环R中理想$P(\neq R)$是素理想的充要条件是$R-P$为乘法集合。

证明 这不过是定理III.2.15的另一种叙述方式，见定义III.4.1. ∎

注记：环R中全部素理想所构成的集合叫作是R的谱。

定理2.2 如果S是环R的乘法子集合，并且S与R的理想I非交，则存在一个理想P，它在R的理想集合中对于性质“与S非交并且包含理想I”是极大的。此外，每个这样的理想P必是素理想。

注：定理常常用于$I=0$的情形。

证明概要 集合$\mathscr{S}=\{R$的理想$A\mid A\cap S=\varnothing, A\supset I\}$是非空的，这是因为$I\in\mathscr{S}$。由于$S\neq\varnothing$(定义III.4.1)，从而$\mathscr{S}$中每个理想均真包含在$R$之中，将$R$赋以包含序，根据Zorn引理，存在一个理想

P在$\mathscr{S}$中极大．设A和B都是R中理想，并且$AB\subset P$．如果$A\not\subset P$并且$B\not\subset P$，则理想$P+A$和$P+B$均真包含P，因此均与S相交．于是存在$p_i\in P$，$a\in A$，$b\in B$，使得

$$p_1+a=s_1\in S,\quad p_2+b=s_2\in S.$$

因此$s_1s_2=p_1p_2+p_1b+ap_2+ab\in P+AB\subset P$．这就与 $s_1s_2\in S$和$S\cap P=\varnothing$相矛盾．因此$A\subset P$或者$B\subset P$，即P是素理想．∎

定理2.3 设K是交换环R的子环．如果$P_1,\cdots,P_n$为R的素理想，并且$K\subset P_1\cup P_1\cup\cdots\cup P_n$，则存在某个$i$使得$K\subset P_i$．

注记：当$n\leqslant 2$的时候，从下面的证明可知不需要假定每个 P_i都是素理想．但是当$n>2$时则需要这个假定．

证明 假如对于每个i均有$K\not\subset P$．不妨假设$n>1$，并且n是使$K\subset P_1\cup\cdots\cup P_n$ 成立的最小值．也就是说，对于每个 i 均有$K\not\subset\bigcup_{j\neq i}P_j$．这时，对于每个 i 均存在 $a_i\in K-\bigcup_{j\neq i}P_j$．由于 $K\subset\bigcup_i P_i$，从而 $a_i\in P_i$．元素 $a_1+a_2a_3\cdots a_n$ 属于 K，从而也属于$\bigcup_i P_i$．因此$a_1+a_2a_3\cdots a_n=b_j$，$b_j\in P_i$．如果$j>1$，则$a_1\in P_j$，这就导致矛盾．如果$j=1$，则$a_2a_3\cdots a_n\in P_1$，由定理 III.2.15 可知存在某个$i>1$使得$a_i\in P_1$，这也导致矛盾．∎

定理2.4 如果R是含幺交换环，P是R的理想，并且P在所有非有限生成的理想集合中是极大的，则P是素理想．

证明 假设$ab\in P$，但是$a\notin P$，$b\notin P$．则理想 $P+(a)$和$P+(b)$均真包含P，由极大性可知它们均是有限生成的，即$P+(a)=$

$(p_1+r_1a,\ \cdots,\ p_n+r_na)$，$P+(b)=(p_1'+r_1'b,\cdots,p_m'+r_m'b)$，其中$p_i,\ p_i'\in P,\ r_i,\ r_i'\in R$(见定理III.2.5和III.2.6)．如果$J=\{r\in R\mid ra\in P\}$，则$J$是$R$的理想．由于$ab\in P$，从而对于每个$i$均有$(p_i'+r_i'b)a=p_i'a+r_i'ba\in P$．于是$P\subsetneqq P+(b)\subset J$．由极大性可知$J$是有限生成的．设$J=\{j_1,\ \cdots,\ j_k\}$．如果$x\in P$，则 $x\in P+(a)$，从而有$s_i\in R$，使得$\sum_i s_ir_i\in J$．因此有$t_i\in R$，使得$\sum_{i=1}^{n}s_ir_i=\sum_{i=1}^{k}t_ij_i$，而$x=\sum_{i=1}^{n}s_ip_i+\sum_{i=1}^{k}t_ij_ia$．所以 P 由 $p_1,\ \cdots p_n,\ j_1a,\ \cdots,\ j_ka$ 生成．这就导致矛盾．因此$a\in P$或者$b\in P$．由定理III.2.15可知P 是素理想．∎

定义2.5 设I是交换环R的理想．I的根(或者叫作是幂零根，表示成Red$I$)指的是理想$\bigcap_{P\supset I}P$，即是包含I的所有素理想之交．如果不存在包含I的素理想，则Rad$I$定义为R．

注记：如果R有1，根据定理III.2.18，每个理想$I(\neq R)$均包含在一个极大理想M之中．由于$M\neq R$，并且从定理III.2.19知道M必然是素理想，因此Rad$I\neq R$．零理想的根有时也叫作是环 R的幂零根，或者叫作是环 R的素根，虽然这些术语不太一致．

例 在整环中，零理想为素理想．从而 Rad0 = 0．在整数环$\mathbb{Z}$中，Rad(12) = (2) ∩ (3) = (6)，而Rad(4) = (2) = Rad(32)．

定理2.6 如果I是交换环R的理想，则Rad$I=\{r\in R\mid$存在$n>0$，使得$r^n\in I\}$．

证明 如果Rad$I=R$，则$\{r\in R\mid r^n\in I\}\subset$Rad$I$．如果 Rad$I\neq$

R，而$r^n \in I$，设P是包含I的任一个素理想，则$r^n \in P$。由定理III.2.15可知$r \in P$。因此也有$\{r \in R \mid r^n \in I\} \subset \mathrm{Rad}I$。

反之，如果$t \in R$，并且对于每个$n>0$均有$t^n \notin I$，则$S=\{t^n+x \mid n \in \boldsymbol{N}^*, x \in I\}$是乘法集合，并且$S \cap I=\varnothing$。由定理2.2可知存在一个素理想$P$与$S$非交并且$P \supset I$。由构作方式可知$t \notin P$，于是$t \notin \mathrm{Rad}I$。这就证明了：$t \notin \{r \in R \mid r^n \in I\} \Longrightarrow t \notin \mathrm{Rad}I$。从而$\mathrm{Rad}I \subset \{r \in R \mid r^n \in I\}$。∎

定理2.7 如果I，I_1，I_2，…，I_n是交换环R中的理想，则

(i) $\mathrm{Rad}(\mathrm{Rad}I)=\mathrm{Rad}I$；

(ii) $\mathrm{Rad}(I_1 I_2 \cdots I_n)=\mathrm{Rad}\left(\bigcap_{j=1}^{n} I_j\right)=\bigcap_{j=1}^{n} \mathrm{Rad}I_j$。

(iii) $\mathrm{Rad}(I^m)=\mathrm{Rad}I$。

证明概要 对于每种情形，我们都只证两个包含关系当中的一个。

(i) 如果$r \in \mathrm{Rad}(\mathrm{Rad}I)$，则$r^n \in \mathrm{Rad}I$，于是有$n$，$m>0$，使得$r^{nm}=(r^n)^m \in I$。因此$r \in \mathrm{Rad}I$，从而$\mathrm{Rad}(\mathrm{Rad}I) \subset \mathrm{Rad}I$。

(ii) 如果$r \in \bigcap_j \mathrm{Rad}I_j$，则有$m_1$，$m_2$，…，$m_n>0$，使得$r^{m_j} \in I_j (1 \leqslant j \leqslant n)$。令$m=m_1+m_2+\cdots+m_n$，则$r^m=r^{m_1} r^{m_2} \cdots r^{m_n} \in I_1 I_2 \cdots I_n$，从而$\bigcap_j \mathrm{Rad}I_j \subset \mathrm{Rad}(I_1 \cdots I_n)$。最后，由于$I_1 \cdots I_n \subset \bigcap_j I_j$，我们有$\mathrm{Rad}(I_1 \cdots I_n) \subset \mathrm{Rad}\left(\bigcap_j I_j\right)$。

(iii)为(ii)之特殊情形。∎

定义2.8 交换环R中的理想$Q(\neq R)$叫作准素理想，是指对

于任意a，$b\in R$：

$$ab\in Q,\ a\notin Q\Longrightarrow \text{有}n>0,\text{使得}b^n\in Q.$$

例 素理想显然是准素理想. 如果p是素数，$n>1$为正整数，则$(p)^n=(p^n)$为$\mathbb{Z}$中准素理想但不是素理想(习题17). 一般来说，素理想P的幂P^n不一定是准素理想.

例 如果F为域，则(x,y)是$F[x,y]$中的极大理想（习题12），因此是素理想(定理III.2.19). 并且$(x,\ y)^2=(x^2,xy,y^2)\subsetneq(x^2,\ y)\subsetneq(x,\ y)$. 理想$(x^2,y)$为准素理想，而$(x,\ y)$是包含$(x^2,y)$的唯一的(真)素理想(习题12). 所以，在$F[x,y]$中准素理想$(x^2,y)$不是素理想的幂.

本节以下假设环R均有幺元素1_R.

定理2.9 如果Q是交换环R的准素理想，则$\mathrm{Rad}Q$为素理想.

证明 假设$ab\in\mathrm{Rad}Q$，$a\notin\mathrm{Rad}Q$，则有n使得$a^nb^n=(ab)^n\in Q$. 由于$a\notin\mathrm{Rad}Q$，从而$a^n\notin Q$. 由Q的准素性可知有$m>0$，使得$(b^n)^m\notin Q$，因此$b\in\mathrm{Rad}Q$，于是从定理III.2.15便知$\mathrm{Rad}Q$是素理想. ∎

根据定理2.9，我们将采用下列一些术语. 如果Q是交换环R中的准素理想，则Q的根P叫作Q所结合的素理想. 或者称之为Q是属于素理想P的准素理想；Q是对于P的准素理想；Q是P-准素理想等等. 对于一个给定的准素理想Q，它所结合的素理想$\mathrm{Rad}Q$显然是唯一的. 但是对于一个给定的素理想P，它可以是许多个不同的准素理想所结合的素理想.

例 如果p为$\mathbb{Z}$中素数，那么准素理想(p^2)，(p^3)，…，均属于素理想(p). 在环$\mathbb{Z}[x,\ y]$中，理想$(x^2,\ y)$，$(x^2,\ y^2)$，$(x^2,\ y^3)$等均是属于素理想$(x,\ y)$的准素理想(习题13).

定理2.10 设Q和P是交换环R中的理想，则Q为对于P的准素理想当且仅当下列二条件同时成立的时候：

(i) $Q\subset P\subset \mathrm{Rad}Q$;

(ii) 如果$ab\in Q$, $a\notin Q$, 则$b\in P$.

证明概要 假设(i)和(ii)成立. 如果$ab\in Q$, $a\notin Q$, 则$b\in P\subset \mathrm{Rad}Q$, 因此有$n>0$,使得$b^n\in Q$. 即$Q$为准素理想. 为证$Q$是对于$P$的准素理想，我们只需证明$P=\mathrm{Rad}Q$. 由(i)知$P\subset \mathrm{Rad}Q$. 如果$b\in \mathrm{Rad}Q$, 令$n$是使$b^n\in Q$的最小正整数. 如果$n=1$, 则$b\in Q\subset P$. 如果$n>1$, 则$b^{n-1}b=b^n\in Q$, 而由$n$的极小性可知 $b^{n-1}\notin Q$. 再由(ii)即知$b\in P$. 因此: $b\in \mathrm{Rad}Q\Longrightarrow b\in P$. 从而 $\mathrm{Rad}Q\subset P$. 反方向的推导是显然的. ∎

定理2.11 如果Q_1, …, Q_n是交换环R中的准素理想，并且全是对于P 的准素理想，则$\bigcap_{i=1}^{n} Q_i$也是对于P的准素理想.

证明 设 $Q=\bigcap_{i=1}^{n} Q_i$. 由定理2.7(ii) 可知$\mathrm{Rad}Q=\bigcap_{i=1}^{n}\mathrm{Rad}Q_i$

$=\bigcap_{i=1}^{n} P=P$. 特别地, $Q\subset P\subset \mathrm{Rad}Q$. 如果$ab\in Q$, $a\notin Q$, 则对于某个i有$ab\in Q_i$并且$a\notin Q_i$. 由于Q_i是P-准素理想,由定理2.10(ii)可知$b\in P$. 再由定理2.10即知Q是P-准素理想. ∎

定义2.12 交换环R中的理想I称作具有准素分解，是指$I=Q_1\cap Q_2\cap\cdots\cap Q_n$, 其中$Q_i$均是准素理想. 如果每个 Q_i均不包含$Q_1\cap\cdots\cap Q_{i-1}\cap Q_{i+1}\cap\cdots\cap Q_n$, 并且$Q_i$的根是彼此不同的，则

这样的准素分解叫作既约的(或者叫作不可删的)。

定理2.13 假设I是交换环R的理想。如果I有准素分解，则必有既约的准素分解。

证明 如果$I=Q_1\cap\cdots\cap Q_n$(Q_i准素)，并且Q_i包含$Q_1\cap\cdots\cap Q_{i-1}\cap Q_{i+1}\cap\cdots\cap Q_n$，则$I=Q_1\cap\cdots\cap Q_{i-1}\cap Q_{i+1}\cap\cdots\cap Q_n$也是一个准素分解。于是，在去掉这种多余的$Q_i$(并且重新加以标记)之后，我们有$I=Q_1\cap\cdots\cap Q_k$，其中每个$Q_i$均不包含其余$Q_j$的交。以$P_1$，…，$P_r$表示集合$\{\mathrm{Rad}Q_1,\ \cdots,\ \mathrm{Rad}Q_k\}$中彼此不同的素理想。令$Q_i'$为属于$P_i$的所有那些$Q$之交($1\leqslant i\leqslant r$)。根据定理2.11，$Q_i'$是$P_i$-准素的。每个$Q_i'$显然不包含其余$Q_j'$之交。因此$I=\bigcap_{i=1}^{k}Q_i=\bigcap_{i=1}^{r}Q_i'$，这是既约的准素分解。∎

这里显然会提出两个问题：什么样的理想有既约的准素分解？既约的准素分解是否在某种意义下是唯一的？下一节我们将在更一般的情形下给出这两个问题的答案(定理3.5和3.6)。

习　题

注：R均为交换环

1. 设R是含幺的Artin交换环。

   (*a*) R的每个素理想均是极大理想〔提示：定理III.2.16和III.2.20，习题1.5和1.7〕

   (*b*) R只有有限多个不同的素理想。

2. 如果R有1，R的素理想非空集合$\{P_i\mid i\in I\}$对于包含序是链，则$\bigcup_{i\in I}P_i$

和 $\bigcap_{i\in I} P_i$ 也是素理想.

3. 设 P_1, P_2, …, P_n 为 R 的素理想, I 为 R 的理想并且 $I\not\subset P_i$(对每个 i), 则存在 $r\in I$ 使得 $r\notin P_i$(对每个 i).

4. 设 R 有1, M_1, …, M_r 为 R 的彼此不同的极大理想, 求证 $M_1\cap M_2\cap\cdots\cap M_r = M_1M_2\cdots M_r$. 如果"极大"改成"素"结论是否还对?

5. 设 R 有1. 求证 R 的全体零因子构成的集合是一些素理想的并.

6. 设 R 有1. R 的素理想 P 叫作理想 I 的极小素理想, 是指 $I\subset P$, 并且不存在素理想 P' 使得 $I\subset P'\subsetneq P$.

   (a) R 的理想 I 如果包含在 R 的素理想 P 之中, 则 P 包含 I 的某个极小素理想.〔提示: 对于集合{素理想 $P'\mid I\subset P'\subset P$}用Zorn引理〕

   (b) 每个真理想均至少具有一个极小素理想.

7. 含幺环 R 中理想 I 的根是 I 的全部极小素理想之交〔见习题6〕.

8. 设 R 有1, I 是理想, J 是有限生成理想并且 $J\subset \mathrm{Rad}I$, 则存在正整数 n 使得 $J^n\subset I$.

9. Z_n 中零理想的根是什么?

10. 如果 S 是交换环 R 的乘法子集合, I 为 R 的理想, 则 $S^{-1}(\mathrm{Rad}I) = \mathrm{Rad}(S^{-1}I)$ (在环 $S^{-1}R$ 中).

11. 设 $Q(\neq R)$ 为 R 的理想. 则: Q 为准素理想 $\Longleftrightarrow$ R/Q 的每个零因子均是幂零元素(见习题III.1.12).

12. 设 F 为域, 则

   (a) (x, y) 为 $F[x, y]$ 中的极大理想.

   (b) $(x, y)^2 = (x^2, xy, y^2)\subsetneq(x^2, y)\subsetneq(x, y)$.

   (c) (x^2, y) 为准素理想, 并且只有 (x, y) 是包含它的素理想.

13. 在环 $\mathbf{Z}[x, y]$ 中, (x^2, y), (x^2, y^2), (x^2, y^3), …, (x^i, y^j), … 均是属于素理想 (x, y) 的准素理想.

14. 如果 $\bigcap_{i=1}^{n}$ 改成无限交, 则定理2.11的结论不再成立. [提示: 考虑 $\mathbf{Z}$]

15. 设$f: R \to S$是含幺交换环的满同态. J是S的理想, $I = f^{-1}(J)$. 则

(a) I为R的准素理想$\Longleftrightarrow J$为S的准素理想.

(b) 如果J是P-准素理想, 则I是$f^{-1}(P)$-准素理想.

16. 求$\mathbf{Z}[x, y]$中理想$I = (x^2, xy, 2)$的一个既约准素分解, 并决定此分解式中每个准素理想相结合的素理想.

17. (a) 如果p为素数而$n>1$, 则(p^n)是$\mathbf{Z}$的准素理想但不是素理想.

(b) 求$\mathbf{Z}$中理想(12600)的一个既约准素分解.

18. 设F是域, I是$F[x, y]$中的理想(x^2, xy). 则I 至少有如下三个既约准素分解:

(i) $I = (x) \cap (x^2, y)$;

(ii) $I = (x) \cap (x^2, x+y)$;

(iii) $I = (x) \cap (x^2, xy, y^2)$.

19. (a) 下面是环$\mathbf{Z}[x]$中的准素分解:

$$(4, 2x, x^2) = (4, x) \cap (2, x^2);$$

$$(9, 3x+3) = (3) \cap (9, x+1).$$

(b) (a) 中准素分解是否既约?

3. 准素分解

我们要把第2节的结果推广到模上去. 要证明(子模或者理想)既约准素分解的唯一性命题, 还要证明Noether模(Noether环)的每个子模(理想)均具有准素分解, 在本节中所有环均是含幺交换环, 而所有的模均是幺作用模.

定义3.1 设R是含幺交换环, B为R-模. 称子模$A(\neq B)$是准素的, 是指

$r\in R$，$b\notin A$，$rb\in A\Longrightarrow$存在正整数n使得$r^nB\subset A$。

例 将环R看成是R-模，设Q为R的准素理想（从而是子模）。如果$rb\in Q$，$r\in R$，$b\notin Q$，则有n使得$r^n\in Q$。由于Q为理想，从而$r^nR\subset Q$。因此Q是模R的准素子模。反之，R的每个准素子模也是准素理想（习题1）。因此，关于准素子模的所有结果均可用于准素理想。

定理3.2 设R是含幺交换环，A是R-模B的准素子模。则$Q_A=\{r\in R\mid rB\subset A\}$是$R$的准素理想

证明 由$A\neq B$可知$1_R\notin Q_A$，从而$Q_A\neq R$。如果$rs\in Q_A$并且$s\notin Q_A$，则$sB\not\subset A$。于是存在$b\in B$使得$sb\notin A$但是$r(sb)\in A$。由于A是准素的，从而存在n使得$r^nB\subset A$，即$r^n\in Q_A$。这就表明Q_A是准素的。∎

设R，A，B，Q_A如定理3.2所示。根据定理2.9可知$\mathrm{Rad}Q_A=P$是素理想。不难看出，$P=\{r\in R\mid$存在$n>0$使得$r^nB\subset A\}$。我们把A叫作属于素理想P的准素子模，或者叫作P-准素子模，这个术语与理想的情形是一致的。特别若J是准素理想，则$Q_J=J$。

定义3.3 设R是含幺交换环，B是R-模。B的子模C叫作具有准素分解，是指$C=A_1\cap A_2\cap\cdots\cap A_n$，其中$A_i$是$B$的$P_i$-准素子模（$P_i$为$R$的素理想）。如果每个$A_i$均不包含在$A_1\cap\cdots\cap A_{i-1}\cap A_{i+1}\cap\cdots\cap A_n$之中，并且素理想$P_1$，…，$P_n$彼此不同，则称上述准素分解是既约的。

这个定义也与理想的情形是一致的。如果C，A_i和P_i如定义所述，并且对每个$j\neq i$，$P_i\not\subset P_j$，则称P_i是C的孤立素理想。换句话说，P_i为孤立素理想$\Longleftrightarrow P_i$是集合$\{P_1,\cdots,P_n\}$中的极小元。

如果P_i不是孤立素理想，则P_i叫作嵌入素理想。

定理3.4 设R是含幺交换环，B是R-模。如果B的子模C有准素分解，则C必有既约的准素分解。

证明概要 证明与定理 2.13 相仿。注意若 $Q_A=\{r\in R\mid rB\subset A\}$，则$\bigcap_{i=1}^{n}Q_{A_i}=Q_{\cap A_i}$。因此若$A_1$，…，$A_r$是属于同一素理想$P$的准素子模，则由定理2.11可知$\bigcap_{i=1}^{r}A_i$也是如此。∎

定理3.5 设R是含幺交换环，B是 R-模。如果B的子模$C(\neq B)$有两个既约准素分解

$$A_1\cap A_2\cap\cdots\cap A_k=C=A_1'\cap A_2'\cap\cdots\cap A_s',$$

其中A_i是P_i-准素子模，A_j'是P_j'-准素子模。则$r=s$，并且(在重新标记之后) $P_i=P_i'(1\leqslant i\leqslant k)$。此外，如果 A_i和 A_i'均是P_i-准素子模并且P_i是孤立素理想，则$A_i=A_i'$。

证明 必要时改变一下记号，我们总可认为 P_1 是集合$\{P_1,\cdots,P_k,P_1',\cdots,P_s'\}$中的极大元。先证存在某个$j$使得$P_1=P_j'$。如果不然，即如果$P_1\neq P_j'(1\leqslant j\leqslant s)$，由于$P_1$是极大元，从而$P_1\not\subset P_j'(1\leqslant j\leqslant s)$。因为第1个分解是既约的，从而$P_1$，…，$P_k$两两不同，因此 $P_1\not\subset P_i(2\leqslant i\leqslant k)$。根据定理2.3 可知 $P_1\not\subset P_2\cup\cdots\cup P_k\cup P_1'\cup\cdots\cup P_s'$。于是有 $r\in P_1$，使得$r\notin P_i(i\geqslant 2)$，$r\notin P_j'(1\leqslant j\leqslant s)$。由于$A_1$是$P_1$-准素的，从而$r^nB\subset A_1$ (对某个正整数n)。令C^*为子模$\{x\in B\mid r^nx\in C\}$。如果$k=1$，则$C=A_1$，从而 $C^*=B$。我们证明当$k\geqslant 1$时$C^*=C$，而当 $k>1$时 $C^*=A_2\cap\cdots\cap A_k$。首先容易看出，当$k>1$时，$A_2\cap\cdots\cap A_k\subset C^*$并且$A_1'\cap\cdots\cap A_s'=C\subset$

C^*。另一方面，如果$x\notin A_i(i\geqslant 2)$，则$r^n x\notin A_i$（不然的话，由于$A_i$是$P_i$-准素的，可知$r^n\in P_i$。再由$P_i$为素理想就得出$r\in P_i$)。因此$r^n x\notin C$，于是$x\notin C^*$。所以当$k>1$时$C^*\subset A_2\cap\cdots\cap A_k$。类似地推理可知$C^*\subset A_1'\cap A_2'\cap\cdots\cap A_s'=C$，从而当$k\geqslant 1$时$C^*=C$，而当$k>1$时$C^*=A_2\cap\cdots\cap A_k$。如果$k=1$，则由上述可知$C^*=B$从而$C=C^*=B$，这与假定事实$C\neq B$相矛盾。如果$k>1$，则

$$A_2\cap\cdots\cap A_k=C^*=C=A_1\cap A_2\cap\cdots\cap A_k,$$

从而$A_2\cap\cdots\cap A_k\subset A_1$，这与第1准素分解的既约性相矛盾。因此不可能$P_1\neq P_j'$（对每个$j$)，于是存在$j$使得$P_1=P_j'$，不妨设$j=1$。

现在对k归纳证明定理。如果$k=1$，则必然$s=1$。这是因为若$s>1$，则上面已证$P_1=P_1'$。交换A_i和A_i'的地位即知$B=C^*=A_2'\cap\cdots\cap A_s'$从而存在某个$j\geqslant 2$使得$A_j'=B$。于是第2准素分解式不是既约的，这就导致矛盾。因此$s=1=k$并且$A_1=C=A_1'$。现在设$k>1$并且定理对于有小于k项既约准素分解的所有子模都是对的。上一段的推理（对于$P_1=P_1'$）表明，当$k>1$时子模C^*有两个既约准素分解：

$$A_2\cap A_3\cap\cdots\cap A_k=C^*=A_2'\cap\cdots\cap A_s'.$$

由归纳假设可知$h=s$，并且（在重新标记之后）$P_i=P_i'$（对于每个i)。这就证明了定理的第一部份。

假设A_i和A_i'均是P_i-准素子模，而P_i为孤立素理想。为符号方便起见令$i=1$。由于P_1是孤立的，对每个$j\geqslant 2$均有$r_j\in P_j-P_1$。于是当$j>1$时，$t=r_2r_3\cdots r_k\in P_j$但是$t\notin P_1$。因为$A_j$是$P_j$-准素的，对每个$j\geqslant 2$均有整数$n_j$使得$t^{n_j}B\subset A$。类似地，对每个$j\geqslant 2$均有$m_j$使得$t^{m_j}B\subset A_j'$。令$n=\max\{n_2,\ \cdots,\ n_k,\ m_2,\ \cdots,\ m_k\}$，则对每个$j\geqslant 2$，$t^nB\subset A_j$，$t^nB\subset A_j'$。令$D$为子模$\{x\in B\mid t^nx\in C\}$。为了完成唯一性的证明，我们只需证明$A_1=D=A_1'$即可。如果$x$

$\in A_1$则$t^n x \in A_1 \cap A_2 \cap \cdots \cap A_k = C$，于是$x \in D$，从而$A_1 \subset D$.如果$x \in D$，则$t^n x \in C \subset A_1$。由于$A_1$是$P_1$-准素的并且$t \notin P_1$，从而$t^m B \not\subset A_1$（对所有$m>0$）。因为$A_1$是准素的，我们必然$x \in A_1$(不然的话，$t^n x \in A_1$并且$x \notin A_1$，由定义2.1即知存在某个正整数$q$使得$t^{nq} B \subset A_1$)。于是$D = A_1$。同样可证$A_1' = D$。因此$A_1 = A_1'$。∎

至今我们均假定模有准素分解，现在我们对下列问题给出部份答案：什么样的模[理想]具有准素分解？

定理3.6 设R为含幺交换环，B为R-模并且满足子模升链条件。则每个子模$A(\neq B)$均有既约准素分解。特别地，交换Noether环R上有限生成模B的每个子模$A(\neq B)$和R的每个理想$(\neq R)$均具有准素分解。

证明 设$\mathcal{S} = \{B$的子模$M \mid M$不具有准素分解$\}$。准素子模显然均不属于$\mathcal{S}$。我们需要证明$\mathcal{S}$是空集.如果$\mathcal{S}$非空，由定理1.4可知$\mathcal{S}$具有极大元C。由于C不是准素的，从而存在$r \in R$和$b \in B - C$，使得$rb \in C$但是$r^n B \not\subset C$（对所有$n>0$）。令$B_n = \{x \in B \mid r^n x \in C\}$。则$B_n$为$B$的子模并且$B_1 \subset B_2 \subset B_3 \subset \cdots$。由假设可知，存在$k>0$，使得$B_i = B_k$（对每个$i \geqslant k$）。令$D$是子模$\{x \in B \mid$存在$y \in B$和$c \in C$使得$x = r^k y + c\}$，显然$C \subset B_k \cap D$。反之，如果$x \in B_k \cap D$，则$x = r^k y + c$，$r^k x \in C$，从而$r^{2k} y = r^k (r^k y) = r^k (x - c) = r^k x - r^k c \in C$。因此$y \in B_{2k} = B_k$。于是$r^k y \in C$，从而$x = r^k y + c \in C$。这就表明$B_k \cap D \subset C$，从而$B_k \cap D = C$。现在$C \neq B_k \neq B$并且$C \neq D \neq B$（因为$b \in B_k - C$而$r^k B \not\subset C$)，由$C$在$\mathcal{S}$中的极大性可知$B_k$和$D$均有准素分解。于是$C$也有准素分解，这就导致矛盾。从而$\mathcal{S}$为空集，即每个子模均有准素分解。再由定理3.4即知每个子模均有既约准素分解。定理的最后论断现在由定理1.8和1.9立刻推出。∎

习　题

注：若非特别声明，R永远指的是含幺交换环。

1. 环R看成是R-模，如果Q是R的准素子模，则Q是准素理想。

2. (a) 设f：$B\to D$为R-模满同态，$C(\neq D)$ 是D的子模.则：C为D 的准素子模$\Longleftrightarrow f^{-1}(C)$ 为B的准素子模。

   (b) 如果C和$f^{-1}(C)$ 均准素，则它们属于同一个素理想P。

3. 如果$A(\neq B)$ 是R-模B的子模，P为R的理想，并且

   (i) $rx\in A$，$x\notin A$ $(r\in R,\ x\in B)\Rightarrow r\in P$；

   (ii) $r\in P\Rightarrow$存在正整数n使得$r^nB\subseteq A$，

   则P为素理想并且A是B的P-准素子模。

4. 如果A是R-模B的P-准素子模，$rx\in A(r\in R,\ x\in B)$，则或者$r\in P$或者$x\in A$。

5. 如果A是R-模B的P-准素子模，C为B 的子模，并且$C\not\subset A$，则$\{r\in R\mid rC\subseteq A\}$是$P$-准素理想。[提示：习题3可能有帮助.]

6. 设A是R-模B的P-准素子模，C为B的子模，并且$C\not\subset A$。则$A\cap C$是C的P-准素子模。[提示：习题3可能有帮助.]

7. 如果B为R-模，$x\in B$，x 的零化理想为记 $\mathrm{ann}x=\{r\in R\mid rx=0\}$。求证$\mathrm{ann}x$是$R$的理想。

8. 如果$B\neq 0$是R-模，P是理想集合$\{\mathrm{ann}x\mid 0\neq x\in B\}$的极大元（见习题7），则$P$是素理想。

9. 设R是Noether环，B为R-模。如果P是R的素理想并且$P=\mathrm{ann}x$（对某个$0\neq x\in B$）（见习题7），则P叫作B的结合素理想。

   (a) 如果$B\neq 0$，则B存在结合素理想。[提示：利用习题8.]

   (b) 如果$B\neq 0$并且B满足子模升链条件，则存在素理想 P_1，…，P_{r-1}和子模列$B=B_1\supseteq B_2\supseteq\cdots\supseteq B_r=0$，使得对每个$i<r$，$B_i/B_{i+1}\cong R/P_i$。

10. 设R和B如习题9 (b) 中所述，则关于$r\in R$的下列条件是等价的：

(i) 对每个$x\in B$均存在正整数$n(x)$使得$r^{n(x)}x=0$。

(ii) r在B的每个结合素理想之中（见习题9和15）。

11. 设R为Noether环，$r\in R$，B为R-模。则："由$rx=0$ $(x\in B)$推出$x=0$" $\Longleftrightarrow$ r不在B的任何一个结合素理想之中（见习题8和9）。

12. 设R为Noether环，B为R-模并且满足子模升链条件，则下列两条件等价：

(i) B恰好有一个结合素理想（见习题9）；

(ii) $B\neq 0$，并且对每个$r\in R$，或者"$rx=0$，$x\in B\Rightarrow x=0$"，或者"$x\in B\Rightarrow$有正整数$n(x)$，使得$r^{n(x)}x=0$"。[见习题10和11.]

13. 设R和B如习题12所示，则：B的子模A是准素的 $\Longleftrightarrow$ B/A恰好有一个结合素理想P.并且在上述条件成立的时候，A为P-准素子模（见习题9和12）。

14. 设R和B如习题12所示.如果$A(\neq B)$是B的子模，则A的每个结合素理想均是B的结合素理想.而B的结合素理想必是A或者B/A的结合素理想（见习题9）。

15. 设R和B如习题12所示，$0=A_1\cap\cdots\cap A_n$为0的既约准素分解，其中A_i为P_i-准素子模，则B的全部结合素理想为P_1，…，P_n.特别地，B只有有限个结合素理想.[提示：见习题9，13和14]

16. 设S为R的乘法子集，A为R-模B的P-准素子模，如果$P\cap S=\phi$，则$S^{-1}A$为$S^{-1}R$-模$S^{-1}B$的$S^{-1}P$-准素子模。

4. Noether环和Noether模

这节内容包括彼此独立的两部份。第一部份谈Noether模(即满足升链条件的模)的准素特性。证明Krull相交定理的一个相当强的形式。给出中山引理和它的一些有趣的推论。本节第二部份

不依赖于第一部份。我们要证明：若R是含幺Noether交换环，则多项式环$R[x_1, \cdots, x_n]$和幂级数环$R[[x]]$也是如此。除了个别例外，本节中所有环均是含幺交换环。

让我们回忆：交换环R是Noether环$\Longleftrightarrow R$满足（双侧）理想的极大条件（定义1.2和定理1.4）$\Longleftrightarrow R$的每个理想均是有限生成的（定理1.9）。事实上，对于后一条件我们只需要考虑R的素理想：

命题4.1 （I.S.Cohen） 含幺交换环R是Noether环$\Longleftrightarrow R$的每个素理想均是有限生成的。

证明概要 （$\Longleftarrow$）设$\mathscr{S}=\{R$的理想$I \mid I$不是有限生成的$\}$，如果$\mathscr{S}$非空，由Zorn引理可求得$\mathscr{S}$的极大元P，由命题2.4可知P是素理想。由假设即知P是有限生成的，这就与$P\in\mathscr{S}$相矛盾。于是$\mathscr{S}=\phi$。由定理1.9即知R是Noether环。∎

为了证明Krull相交定理我们需要一些预备知识。设B是交换环R上的模，不难看出$I=\{r\in R \mid$对每个$b\in B, rb=0\}$是R的理想。I叫作B在R中的零化理想。

引理4.2 设B是含幺交换环R上的有限生成模，I是B在R中的零化理想。则：B满足子模升（降）链条件$\Longleftrightarrow R/I$是Noether（Artin）环。

证明概要 设B由$b_1, \cdots, b_n$生成，并且B满足升链条件，则由定理IV.1.5可知$B=Rb_1+\cdots+Rb_n$。从而$I=I_1\cap I_2\cap\cdots\cap I_n$，其中$I_j$是子模$Rb_j$的零化理想。由系III.2.27可知存在环的单同态θ：$R/I\to R/I_1\times\cdots\times R/I_n$。易知$\theta$也是$R$-模单同态。对每个$j$，验证映射$R/I_j\to Rb_j$，$r+I_j\mapsto rb_j$是$R$-模同构。因为$B$的子模$Rb_j$

满足升链条件，从而 R/I_i 也是如此。由系1.7即知$R/I_1\oplus\cdots\oplus R/I_n$满足$R$-子模升链条件，于是它的子模 $\mathrm{Im}\theta\cong R/I$ 也满足 R-子模升链条件。但是环R/I的每个理想均是R/I的R-子模，从而R/I是Noether环。

反之，设R/I是Noether环。验证B是R/I-模（其中$(r+I)b=rb$），并且B的 R/I-子模也就是 R-子模，于是由定理1.8即知B满足升链条件。∎

回忆：设I是含幺环R的理想，B为R-模，则$IB=\left\{\sum_{i=1}^{n} r_i b_i \mid r_i \in I, b_i\in B,\ n\in \mathbb{N}^*\right\}$是$B$的子模（习题IV.13）。

引理4.3 设P是含幺交换环R的素理想。如果C是Noether$R$-模A的P-准素子模，则存在正整数m使得$P^mA\subset C$。

证明 设I是A在R中的零化理想。考虑环 $\bar{R}=R/I$，以 $\bar{r}$ 表示陪集$r+I\in\bar{R}$，显然$I\subset\{r\in R\mid rA\subset C\}\subset P$，从而 $\bar{P}=P/I$是$\bar{R}$ 的理想。A和C均是 $\bar{R}$-模（ $\bar{r}a=ra$，对于$r\in R$，$a\in A$）。我们断言：C是A的准素$\bar{R}$-子模。如果 $\bar{r}a\in C(r\in R,\ a\in A-C)$，则$ra\in C$，由于$C$是准素$R$-子模，从而$r^nA\subset C$（对某个$n$），于是$\bar{r}^nA\subset C$，即$C$是$\bar{R}$-准素的。由于$\{\bar{r}\in\bar{R}\mid \bar{r}^kA\subset C$（对某个$k>0$）$\}=\{\bar{r}\in\bar{R}\mid r^kA\subset C\}=\{\bar{r}\in\bar{R}\mid r\in P\}=\bar{P}$，从而$\bar{P}$是 $\bar{R}$的素理想并且C是A的$\bar{P}$-准素的$\bar{R}$-子模（见定理2.9和3.2）。

由引理4.2可知$\bar{R}$是Noether环，再由定理1.9可知 $\bar{P}$ 是有限生成的。设$\bar{p}_1$，…，$\bar{p}_s$ ($p_i\in P$) 是$\bar{P}$的生成元。对每个i均存在n_i使得 $\bar{p}_i^{n_i}A\subset C$。令$m=n_1+\cdots+n_s$，则由定理III.1.2(V) 和III.2.5(vi) 可知 $\bar{P}^mA\subset C$。现在由$\bar{P}=P/I$和$IA=0$即知$P^mA\subset C$。∎

定理4.4 （Krull相交定理）设R是含幺交换环，I为R的理想，A为Noether R-模，如果$B=\bigcap_{n=1}^{\infty} I^nA$，则$IB=B$。

定理4.4首先是对于Noether局部环R和它的唯一极大理想I证明的。我们这里给出的证明（象原始证明一样）依赖于准素分解特性。然而若假设R是Noether环，则有许多不使用准素分解特性的证明（习题2）。

定理4.4的证明 如果$IB=A$，则$A=IB\subset B$，于是$B=A=IB$。如果$IB\neq A$，由定理3.6知IB有准素分解：

$$IB=A_1\cap A_2\cap\cdots\cap A_s,$$

其中A_i是A的P_i-准素子模，P_i为R的素理想。由于总有$IB\subset B$，为了再证$B\subset IB$（从而$B=IB$），只需证明$B\subset A_i$（对每个i）即可。

固定i（$1\leqslant i\leqslant s$），先设$I\subset P_i$，由引理4.3可知存在整数m使得$P_i^mA\subset A_i$，于是$B=\bigcap_n I^nA\subset I^mA\subset P_i^mA\subset A_i$。再设$I\not\subset P_i$，则存在$r\in I-P_i$。如果$B\not\subset A_i$，则存在$b\in B-A_i$。由于$rb\in IB\subset A_i$，$b\notin A_i$而$A_i$是准素的，从而$r^nA\subset A_i$（对某个$n>0$）。于是$r\in P_i$（这是因为$A_i$是$P_i$-准素子模），而这与$r\in I-P_i$相矛盾，因此$B\subset A_i$。∎

引理4.5 （**中山引理**） 设J是含幺交换环R的理想，则下列诸条件彼此等价：

(i) J包含在R的每个极大理想之中；

(ii) 对每个$j\in J$，1_R-j是单位；

(iii)如果A是有限生成R-模并且$JA=A$，则$A=0$；

(iv) 如果B是有限生成R-模A的子模，并且 $A=JA+B$，则 $A=B$。

注记　如果将(i)改成“J包含在R的Jacobson根中”，那末上述引理对于非交换环R也是对的(习题IX.2.17)。

证明　(i)⇒(ii)　如果$j\in J$而1_R-j不是单位，则理想 $(1_R-j)\neq R$ (定理III.3.2)，从而(1_R-j)包含在某个极大理想$M(\neq R)$之中(定理III.2.18)。但是由$1_R-j\in M$和$j\in J\subset M$得出$1_R\in M$，这与$M\neq R$相矛盾。因此1_R-j是单位。

(ii)⇒(iii)　由于A是有限生成的，从而必然存在 A 的极小生成集合 $X=\{a_1,\cdots,a_n\}$ (也就是说，X的真子集均不生成A)。如果$A\neq 0$，由极小性可知$a_1\neq 0$，由$JA=A$,$a_1=j_1a_1+j_2a_2+\cdots+j_na_n$　$(j_i\in J)$。又因$1_Ra_1=a_1$，于是当$n=1$时 $(1_R-j_1)a_1=0$，而当$n>1$时

$$(1_R-j_1)a_1=j_2a_2+\cdots+j_na_n.$$

因为1_R-j_1是R中单位，$a_1=(1_R-j_1)^{-1}(1_R-j_1)a_1$。因此当$n=1$时$a_1=0$ (这导出矛盾)，而当$n>1$时a_1是$a_2,\cdots,a_n$的线性组合，从而$\{a_2,\cdots,a_n\}$生成A，而这又与X的极小性相矛盾。

(iii)⇒(iv)　对于商域 A/B 验证 $J(A/B)=A/B$，从而由(iii)即知$A/B=0$，于是$A=B$。

(iv)⇒(i)　设M是任一极大理想，则理想$JR+M$包含M。但是 $JR+M\neq R$ (否则便由 (iv) 推出$R=M$)，由M 的极大性即知 $JR+M=M$，因此$J=JR\subset M$。∎

现在我们给出中山引理的一些应用，开始先谈完备化理论中的一个结果。

命题4.6　设J是含幺交换环R的理想。则：J 包含在R的每个

极大理想之中$\Longleftrightarrow$对于每个满足子模升链条件的R-模A，$\bigcap_{n=1}^{\infty} J^nA = 0$。

证明 ($\Rightarrow$) 如果$B = \bigcap_{n=1}^{\infty} J^nA$，由定理4.4知$JB = B$。由于定理1.9知$B$是有限生成的，再由中山引理4.5即知$B = 0$。

($\Leftarrow$) 假设$R \neq 0$，而M是R的极大理想。于是$M \neq R$，而$A = R/M$为非零R-模并且没有真子模（定理IV.1.10）。所以A满足升链条件，由假设得出$\bigcap_{n} J^nA = 0$。由于JA是A的子模，从而$JA = A$或者$JA = 0$。如果$JA = A$，则$J^nA = A$(对每个n)，从而$\bigcap_{n} J^nA = A \neq 0$，这就导致矛盾。因此$JA = 0$。但是$0 = JA = J(R/M)$,于是$J \subset JR \subset M$。∎

系4.7 设R为 Noether 局部环而M是R 的唯一极大理想，则$\bigcap_{n=1}^{\infty} M^n = 0$。

证明 设$J = M$，$A = R$，则$J^nA = M^n$。然后利用命题4.6。∎

命题4.8 设R是局部环，则有限生成投射R-模必是自由模。

事实上，I.Kaplansky〔63〕给出如下强得多的结果：（不必交换的）局部环上每个投射模均是自由的。

命题4.8的证明 设P是有限生成投射 R-模。由系 IV.2.2可知存在秩有限的自由R-模F和满同态 $\pi: F \to P$。设F是所有这种自由R-模之中秩最小者。令$\{x_1, \cdots, x_n\}$为R-模 F 的一组基。由于π是满同态，$\{\pi(x_1), \cdots, \pi(x_n)\}$必然生成$P$。我们先证 $K = \mathrm{Ker}\,\pi$包

含在MF之中，其中M是R的唯一极大理想。如果$K\subsetneq MF$，则存在$k\in K$，$k\notin MF$。现在$k=r_1x_1+r_2x_2+\cdots+r_nx_n$，其中$r_i\in R$是唯一确定的。由于$k\notin MF$，从而有$r_i$(不妨设为$r_1$)$\notin M$。由定理III.4.13可知$r_1$是单位，从而$x_1-r_1^{-1}k=-r_1^{-1}r_2x_2-\cdots-r_1^{-1}r_nx_n$。

由于$k\in Ker\pi$，$\pi(x_1)=\pi(x_1-r_1^{-1}k)=\pi(\sum_{i=2}^{n}-r_1^{-1}r_ix_i)=\sum_{i=2}^{n}(-r_1^{-1}r_i)\pi(x_i)$。于是$\{\pi(x_2),\cdots,\pi(x_n)\}$生成$P$。如果令$F'$为以$\{x_2,\cdots,x_n\}$为基的$F$的子模，$\pi'$：$F'\to P$是$\pi$在$F'$上的限制，则$\pi'$也是满同态。而这与$F$的选取方式（具有极小势的基）相矛盾，于是$K\subset MF$。

由于$0\to K\xrightarrow{\subset}F\xrightarrow{\pi}P\to 0$是正合的并且$P$是投射模，由定理IV.3.4可知$K\oplus P\cong F$。在这个同构之下，对每个$k\in K$,$(k,0)\longmapsto k$（见定理IV.1.18的证明），于是$F$是内直和$F=K\oplus P'$，其中$P'\cong P$。于是$F=K+P'\subset MF+P'$。如果$u\in F$，则$u=\sum_i m_iv_i+p_i$，$m_i\in M$，$v_i\in F$，$p_i\in P'$。从而在$R$-模$F/P'$中：

$$u+P'=\sum_i m_iv_i+P'=\sum_i m_i(v_i+P')\in M(F/P'),$$

因此$M(F/P')=F/P'$。由于F是有限生成的，从而F/P'也是有限生成的。于是由中山引理4.5，$K\cong F/P'=0$，即$P\cong P'=F$，从而P是自由模。∎

我们以两个著名的定理结束本节。其证明与本章前面内容无关。

定理4.9 （Hilbert基定理） 设R为含幺Noether交换环，则$R[x_1,x_2,\cdots,x_n]$也是如此。

证明 显然只需证明$R[x]$是Noether环。根据定理1.9我们只需证明$R[x]$的每个理想J均是有限生成的。

对于每个$n\geqslant 0$，令$I_n=\{r\in R\mid r=0$或者r是J中某个n次多项式f的首项系数$\}$。验证I_n是R的理想。如果r是I_n中非零元素，$f\in J$是以r为首项系数的n次多项式，则r也是多项式$xf\in J$的首项系数并且xf的次数是$n+1$。于是$I_0\subset I_1\subset I_2\subset\cdots$。由于$R$是Noether环，存在整数$t$使得当$n\geqslant t$时，$I_n=I_t$。进而，由定理1.9可知每个$I_n$ $(n\geqslant 0)$均是有限生成的，设$I_n=(r_{n1},r_{n2},\cdots,r_{ni_n})$。对于每个$r_{nj}(0\leqslant n\leqslant t,\ 1\leqslant j\leqslant i_n)$，令$f_{nj}\in J$是以$r_{nj}$为首项系数的$n$次多项式。注意$f_{0j}=r_{0j}\in R\subset R[x]$。我们现在来证明$R[x]$的理想$J$是由多项式有限集合$X=\{f_{nj}\mid 0\leqslant n\leqslant t,\ 1\leqslant j\leqslant i_n\}$生成的。

显然$(X)\subset J$。反之，J中0次多项式恰好是I_0中的元素，从而它们均属于(X)。现在归纳假设(X)包含J中次数$<k$的全部多项式，令$g\in J$的次数是k并且首项系数是$r\neq 0$。

如果$k\leqslant t$，则$r\in I_k$，于是$r=s_1r_{k1}+s_2r_{k2}+\cdots+s_{i_k}r_{ki_k}(s_j\in R)$。因此$\sum_{j=1}^{i_k}s_jf_{kj}\in(X)$是首项系数为$r$的$k$次多项式。从而$g-\sum_j s_jf_{kj}$的次数$\leqslant k-1$。由归纳假设可知$g-\sum_j s_jf_{kj}\in(X)$，从而$g\in(X)$。

如果$k\geqslant t$，则$r\in I_k=I_t$，于是$r=\sum_{j=1}^{i_t}s_jr_{tj}\quad(s_j\in R)$。由于$\sum_{j=1}^{i_t}s_jx^{k-t}f_{tj}\in(X)$是首项系数为$r$的$k$次多项式，因此$g-\sum_j s_j\cdot x^{k-t}f_{tj}$的次数$\leqslant k-1$，由归纳假设它属于$(X)$。从而$g\in(X)$。这

就完成了归纳推理。因此$J=(X)$。∎

命题4.10 如果R是含幺 Noether 交换环，则$R[[x]]$也是如此。

注记：我们的证明利用了命题4.1。但是也可采用命题4.9的证明方法，只是在推理中将首项（最高次项）系数改成用最低次项的非零系数，并且在证明过程中还要考虑得仔细一些，以保证归纳构作的某些幂级数事实上是能够定义的。此外，还需要选择公理和归纳公理的某种形式（在公开发表的许多证明中，这部份常常叙述的不清楚）。

命题4.10的证明 根据命题4.1只需证明$R[[x]]$中每个素理想P均是有限生成的。定义环的满同态$R[[x]]\to R$，方法是把每个幂级数 $f=\sum_{i=0}^{\infty}a_ix^i$映成它的常数项$a_0$。以$P^*$表示$P$在这个同态之下的象。则$P^*$是 R 的有限生成理想（习题III.2.13和定理1.9）。设$P^*=(r_1,\cdots,r_n)$。对于每个r_i取$f_i\in P$使得f_i的常数项为r_i。

如果$x\in P$，我们来证P是由r_1，…，r_n，x生成的。首先注意：如果 $f_k=r_k+\sum_{i=1}^{\infty}a_ix^i$，则 $r_k=f_k-x\left(\sum_{j=0}^{\infty}a_{j+1}x^j\right)\in P$。如果 $g=\sum_{i=0}^{\infty}b_ix^i\in P$，则 $b_0=s_1r_1+\cdots+s_nr_n$ $(s_i\in R)$从而 $g-\sum_{i=0}^{n}s_ir_i$的常数项为零。即 $g-\sum_{i=0}^{n}s_ir_i=xg_1(g_1\in R[[x]])$。因此 $g=\sum_i s_ir_i+xg_1$，而P是由r_1，…，r_n，x生成的。

如果$x\notin P$，我们来证P是由$f_1,\cdots,f_n\in P$生成的。对于$h=\sum_{i=0}^{\infty}$

$c_i x^l \in P$，则$c_0 = t_1 r_1 + \cdots + t_n r_n (t_i \in R)$。从而$h - \sum_{i=1}^{n} t_i f_i = xh^*$ $(h^* \in R[[x]])$。由于$x \notin P$ 和 $xh^* = h - \sum_i t_i f_i \in P$ 而 P 是素理想，从而$h^* \in P$。对每个$h \in P$，取$t_i \in R$和$h_i^* \in P$使得$h = \sum_{i=1}^{n} t_i f_i + xh^*$（选择公理）。令$\lambda$：$P \to P$是由$h \longmapsto h^*$定义的映射。对于每个$g \in P$，根据引论中归纳定理6.2（对所有$n$取$\lambda = f_n$）可知存在函数$\phi$：$\boldsymbol{N} \to P$使得

$$\phi(0) = g,\ \phi(k+1) = \lambda(\phi(k)) = \phi(k)^*。$$

令$\phi(k) = h_k \in R[[x]]$，以t_{ki}表示上面所选取的R中元素，使得

$$h_k = \sum_{i=1}^{n} t_{ki} f_i + xh_k^* = \sum_{i=1}^{n} t_{ki} f_i + xh_{k+1}。$$

对于每个$i(1 \leqslant i \leqslant n)$，令$g_i = \sum_{k=0}^{\infty} t_{ki} x^k \in R[[x]]$。于是

$$\begin{aligned} g_1 f_1 + \cdots + g_n f_n &= \sum_{i=1}^{n} \Big(\sum_{k=0}^{\infty} t_{ki} x^k \Big) f_i \\ &= \sum_{k=0}^{\infty} \Big(\sum_{i=1}^{n} t_{ki} f_i \Big) x^k \\ &= \sum_{k=0}^{\infty} (h_k - xh_{k+1}) x^k。 \end{aligned}$$

于是对每个 $m \geqslant 0$，$g_1 f_1 + \cdots + g_n f_n$ 中 x^m 的系数等于$\sum_{k=0}^{m} (h_k - xh_{k+1})x^k$中$x^m$的系数。但是

$$\sum_{k=0}^{m} (h_k - xh_{k+1}) x^k = h_0 - x^{m+1} h_{m+1} = g - x^{m+1} h_{m+1},$$

从而$g_1 f_1 + \cdots + g_n f_n$中$x^m$的系数恰好是$g$中 x^m 的系数，因此 $g = g_1 f_1 + \cdots + g_n f_n$。即$f_1, \cdots, f_n$生成$P$。∎

习　题

1. 设R是含幺交换环，I是R的有限生成理想．C是 R- 模A的子模．如果对每个$r\in I$均存在正整数m（依赖于r）使得$r^mA\subset C$.求证存在某个n使得 $I^nA\subset C$.〔提示：见定理III.1.2(v)和III.2.5(vi)〕.

2. 不用准素分解证明Krull相交定理的如下等价形式：设R是含幺Noether交换环，I是R的理想，A是有限生成R-模，$B=\bigcap_{n=1}^{\infty} I^nA$，则$IB=B$.〔提示：设$C$是集合 $\mathscr{S}=\{A$的子模$S\mid B\cap S=IB\}$ 中的极大元．只需证明$I^mA\subset C$(对某个m).又由习题1可知只需证明对每个$r\in I$均有n（依赖于r）使得$r^nA\subset C$.对每个k，令$D_k=\{a\in A\mid r^ka\in C\}$．则$D_0\subset D_1\subset D_2\subset\cdots$是$R$-子模升链.于是存在$n$使得$k\geqslant n$时$D_k=D_n$．证明 $(r^nA+C)\cap B=IB$．由C的极大性可知$r^nA+C=C$，即$r^nA\subset C$．〕

3. 设R是Noether局部环，M是 R 的唯一极大理想．如果 R/M^2 中理想 M/M^2由 $\{a_1+M^2,\cdots,a_n+M^2\}$ 生成，则R中理想 M由 $\{a_1,\cdots,a_n\}$ 生成．

4. （中山引理的另一形式）设R是含幺Noether交换环，理想J包含在 R 的每个极大理想之中，A是有限生成R-模．如果$R/J\otimes_R A=0$，则$A=0$．〔提示：使用正合序列$0\to J\to R\to R/J\to 0$ 和自然同构 $R\otimes_R A\cong A$ 证明 $JA=A$．〕

5. 设R和J如习题4所示．A为有限生成R-模，f：$C\to A$是R- 模同态．则按通常方式f 诱导出同态$\overline{f}$：$C/JC\to A/JA$（系IV.1.8)．求证若$\overline{f}$是满同态，则f也是满同态．

6. (a) 设R是含幺交换环．如果R 的每个理想均可由一个有限或可数无限子集生成，则$R[x]$也是如此．

   (b) 叙述并证明关于$R[[x]]$类似于 (a) 的结果(答案与 (a) 不完全一样)．

7. 设R是含幺交换环，$f, g \in R[[x]]$。令 $I_n f$ 为f的初始项次数（即 $f=\sum_{i=0}^{\infty} a_i x^i$中最小$n$使得$a_n \neq 0$）.求证

(a) $I_n(f+g) \geqslant \min\ (I_n f,\ I_n g)$.

(b) $I_n(fg) \geqslant I_n f + I_n g$.

(c) 如果R是整环，则 $I_n(fg) = I_n f + I_n g$.

8. 设R是含幺Noether交换环，$Q_1 \cap \cdots \cap Q_n = 0$是$R$中零理想的既约准素分解，$Q_i$为$P_i$-准素理想。则$R$ 的全体零因子组成的集合即是 $P_1 \cup P_2 \cup \cdots \cup P_n$.

9. 设R是含幺交换环。如果R的每个极大理想均有形式(c)，其中 $c^2 = c \in R$，则R是 Noether环。〔提示：证明每个准素理想均是极大理想，然后利用命题4.1〕

5. 环 的 扩 张

本节第一部分定义环的扩张并证明整性扩张的基本性质，后一部份是研究环R和扩环S的素理想之间的关系，本节中的环均指含幺交换环。

定义5.1 设S是含幺交换环，R是S的子环并且$1_s \in R$，则S称作R的扩环.

例 域K的每个扩域F显然是K的扩环。如果R是含幺交换环，则$R[[x]]$和$R[x_1, \cdots, x_n]$均是R的扩环。环$\mathbb{Z}$不是偶整数子环E的扩环，因为$1 \notin E$.

定义5.2 设S是R的扩环，$s\in S$. 如果存在首1多项式$f(x)\in R[x]$使得s是f的根(即$f(s)=0$)，则s叫作在R上整. 如果S中每个元素均在R上整，则S叫作R的整性扩张[注]

定义5.2的关键是要求f为首1多项式.

例 域K的每个代数扩域F均是整性扩环(见定义V.1.4后面的注记). 环R在R上整，因为$r\in R$是$x-r\in R[x]$的根. 在$\boldsymbol{Z}$的扩环$\boldsymbol{R}$(实数域)中，元素$1/\sqrt{3}$在$\boldsymbol{Z}$上是代数的，因为它是$3x^2-1$的根，但是$1/\sqrt{3}$不在$\boldsymbol{Z}$上整. 另一方面，$1/\sqrt{3}$在有理数域$\boldsymbol{Q}$上整，因为它是$x^2-1/3$的根.

设S是R的扩环，X为S的子集，X在R上生成的子环指的是S的包含$X\cup R$的所有子环的交，并且表示成$R[X]$，定理V.1.3的前半部份对于环也是对的，从而$R[X]=\{f(s_1,\cdots,s_t)\mid t\in\boldsymbol{N}^*,\ f(x_1,\cdots,x_t)\in R[x_1,\cdots,x_t],\ s_i\in X\}$. 特别地，对于$s_1,\cdots,s_t\in S$，由$\{s_1,\cdots,s_t\}$在$R$上生成的子环为

$$R[s_1,\cdots,s_t]=\{f(s_1,\cdots,s_t)\mid f\in R[x_1,\cdots,x_t]\}$$

$R[s_1,\cdots,s_t]$中元素有时也叫作关于$s_1,\cdots,s_t$的多项式，虽然$R[s_1,\cdots,s_t]$不一定同构于多项式环$R[x_1,\cdots,x_t]$(例如当f为非零多项式时，$f(s_1,\cdots,s_t)$可能为0). 不难看出，对于每个i($1\leqslant i\leqslant t$)，$R[s_1,\cdots,s_{i-1}][s_i]=R[s_1,\cdots,s_i]$，由于环$R[s_1,\cdots,s_t]$包含$R$，从而以显然方式$R[s_1,\cdots,s_t]$是$R$-模，同样地，$R[s_1,\cdots,s_t]$上的每个模也显然是$R$-模.

定理5.3 设S是R的扩环，$s\in S$. 则下列条件是彼此等价的

(i) s在R上整；

[注] 注意S在R上整(integral)和S为整环(domain)是两个不同的概念，不要因中译名相近而混淆. ——译者

(ii) $R[s]$是有限生成R-模；

(iii) 存在S的子环T，$1_S \in T$，$R[s] \subset T$，并且T是有限生成R-模；

(iv) 存在S的$R[s]$-子模B，使得B是有限生成R-模并且它在$R[s]$中的零化理想为0。

证明概要 (i)⇒(ii)设s是n次首1多项式$f \in R[x]$的根。我们证明$1_R = s^0, s, s^2, \cdots, s^{n-1}$生成$R$-模$R[s]$.如上所述，$R[s]$中元素均有形式$g(s)$，$g \in R[x]$。利用除法算式得到$g(x) = f(x)q(x) + r(x)$，$\deg r < \deg f$因此在$S$中，$g(s) = f(s)q(s) + r(s) = 0 + r(s) = r(s)$。于是$g(s)$是$1_R, s, s^2, \cdots, s^m$的$R$-线性组合，其中$m = \deg r < \deg f = n$。

(ii) ⇒(iii)取$T = R[s]$

(iii)⇒(iv)设B为子环T。由于$R \subset R[s] \subset T$，B是$R[s]$-模，并且由(iii)知B作为R-模是有限生成的由于$1_S \in B$,可知$uB = 0$(对$u \in S$)⇒$u = u1_S = 0$即B在$R[s]$中的零化理想是0。

(iv)⇒(i)设B在R上是由$b_1, \cdots, b_n$生成的。由于B是$R[s]$-模，$sb_i \in B$(对每个i)。于是有$r_{ij} \in R$使得

$$\begin{aligned}
sb_1 &= r_{11}b_1 + r_{12}b_2 + \cdots + r_{1n}b_n \\
sb_2 &= r_{21}b_1 + r_{22}b_2 + \cdots + r_{2n}b_n \\
&\vdots \qquad\qquad\qquad\qquad \vdots \\
sb_n &= r_{n1}b_1 + r_{n2}b_2 + \cdots + r_{nn}b_n
\end{aligned}$$

从而

$$\begin{aligned}
(r_{11} - s)b_1 + r_{12}b_2 + \cdots + r_{1n}b_n &= 0 \\
r_{n}b_1 + (r_{22} - s)b_2 + \cdots + r_{2n}b_n &= 0 \\
&\vdots \qquad\qquad\qquad\qquad \vdots \\
r_{n1}b_1 + r_{n2}b_2 + \cdots + (r_{nn} - s)b_n &= 0。
\end{aligned}$$

令M为n阶方阵(r_{ij})，$d\in R[s]$是矩阵$M-sI_n$的行列式。则由习题VII.3.8可知$db_i=0$(对每个i)。由于B是由$b_1,\cdots,b_n$生成的，从而$dB=0$根据(iv)知B在$R[s]$中的化零理想是0，从而$d=0$。令$f\in R[x]$是多项式$|M-xI_n|$，则f和$-f$至少有一个是首1的，并且

$$\pm f(s)=\pm|M-sI_n|=\pm d=0$$

因此s在R上整。∎

系5.4 设S是R的扩环，S为有限生成R-模。则S是R的整性扩张。

证明 对于每个$s\in S$，可取S为定理5.3(iii)中的T。然后由定理5.3(i)即知s在R上整。∎

下一个定理的证明依赖于以下的事实：如果$R\subset S\subset T$是环的扩张($1_T\in R$)，T为有限生成S-模而S为有限生成R-模，则T为有限生成R-模，这一事实的证明可参见定理IV.2.16证明的第二段。

定理5.5 设S是R的扩环，$s_1,\cdots,s_i\in S$均在R上整，则$R[s_1,\cdots,s_i]$是有限生成R-模并且为R的整性扩张。

证明 考虑环的扩张

$$R\subset R[s_1]\subset R[s_1,s_2]\subset\cdots\subset R[s_1,\cdots,s_i]$$

对于每个i，s_i在R上整，从而也在$R[s_1,\cdots,s_{i-1}]$上整。由于$R[s_1,\cdots,s_i]=R[s_1,\cdots,s_{i-1}][s_i]$，根据定理5.3(i)和(ii)可知$R[s_1,\cdots,s_i]$是有限生成$R[s_1,\cdots,s_{i-1}]$-模。重复应用定理前面的注记可知$R[s_1,\cdots,s_n]$是有限生成$R$-模，于是由系5.4即知$R[s_1,\cdots,s_n]$是$R$的整性扩张。∎

定理5.6 如果T是S的整性扩环，S是R的整性扩环，则T是R

的整性扩环。

证明 T显然是R的扩环。设$t\in T$，则t在S上整。于是t是某个首1多项式$f=\sum_{i=0}^{n}s_ix^i\in S[x]$的根。由于$f$也是$R[s_0,s_1,\cdots,s_{n-1}]$上的多项式，从而$t$在$R[s_0,\cdots,s_{n-1}]$上整，根据定理5.5，$R[s_0,\cdots,s_{n-1}][t]$是有限生成$R[s_0,\cdots,s_{n-1}]$-模，而$S$在$R$上整，由定理5.5可知$R[s_0,\cdots,s_{n-1}]$是有限生成$R$-模。由定理5.5前面的注记可知 $R[s_0,\cdots,s_{n-1}][t]=R[s_0,\cdots,s_{n-1},t]$ 是有限生成R-模。由于$R[t]\subset R[s_0,\cdots,s_{n-1},t]$，从定理5.3(iii)即知$t$在$R$上整。∎

定理5.7 设S是R的扩环，$\hat{R}=\{s\in S\mid s在R上整\}$。则$\hat{R}$为$R$的整性扩环，并且$S$的每个在$R$上整的子环均包含在$\hat{R}$之中。

证明 设$s,t\in\hat{R}$，则 $s,t\in R[s,t]$，从而$r-s$，$rs\in R[s,t]$。由于s和t在R上整，从而环$R[s,t]$在R上整(定理5.5)。因此$r-s$，$rs\in\hat{R}$。于是$\hat{R}$是S的子环(见定理I.2.5)。$\hat{R}$包含R(因为R中元素显然在R上整)。而由$\hat{R}$的定义即知$\hat{R}$在R上整并且包含S的每个在R上整的子环。∎

设S为R的扩环，定理5.7中的环$\hat{R}$叫作R在S中的整闭包。如果$\hat{R}=R$，则称R在S中整闭。

注记：(i)由于 $1_R\in R\subset\hat{R}$，可知S是$\hat{R}$的扩环由定理5.6和5.7即知$\hat{R}$在S中整闭。

(iii) 整闭和整闭包都是相对性概念，涉及到一个给定的环R和它的特定的扩环S。所以，如果不指明扩环S，那末“R是整闭的”一词便含混不清，但是有一种情形可以不用明显提到环S：整环R叫作整闭的，是指R在其商域中整闭。

例 整环$\boldsymbol{Z}$(在有理数域$\boldsymbol{Q}$中)是整闭的(习题8).但是$\boldsymbol{Z}$在复数域$\boldsymbol{C}$中不是整闭的，因为$i\in\boldsymbol{C}$在$\boldsymbol{Z}$上整(但是$i\notin\boldsymbol{Z}$)。

例 更一般地，每个唯一因子分解整环均是整闭的(习题8)。特别地,多项式环$F[x_1,\cdots,x_n]$(在它的商域$F(x_1,\cdots,x_n)$中)是整闭的，其中F是域。

下面定理只在证明定理6.10时用到

定理5.8 设T是整环R的乘法子集，$0\notin T$，如果R整闭，则$T^{-1}R$也是整闭整环。

证明概要 $T^{-1}R$是整环(定理III.4.3(ii))并且可以将R看成是$T^{-1}R$的子环(定理III.4.4(ii))。于是R的商域$Q(R)$可看成是$T^{-1}R$的商域$Q(T^{-1}R)$的子域请读者证明$Q(R)=Q(T^{-1}R)$。

设$u\in Q(T^{-1}R)$在$T^{-1}R$上整，则

$$u^n+(r_{n-1}/s_{n-1})u^{n-1}+\cdots+(r_1/s_1)u+(r_0/s_0)=0,$$

其中$r_i\in R$，$s\in T$。将此等式乘以s^n，其中$s=s_0s_1\cdots s_{n-1}\in T$，可知$su$在$R$上整。由于$su\in Q(T^{-1}R)=Q(R)$而$R$整闭，从而$su\in R$。因此$u=su/s\in T^{-1}R$，即$T^{-1}R$整闭.∎

本节其余部份阐述环R和S的(素)理想之间的关系，其中S是R的扩环。这部份内容只有一个地方在证明引理7.3的时候使用。

如果S是R的扩环而$I(\neq S)$是S的理想，不难看出$I\cap R\neq R$并且$I\cap R$是R的理想(习题10)。理想$J=I\cap R$叫作I在R的限制理想，并且称I位于J上。

如果Q是S的素理想,则Q在R的限制$Q\cap R$也是R的素理想(习题10)。反问题是：给了R中一个素理想P，是否S中存在素理想Q位于P上(即$P=Q\cap R$)？有许多例子说明答案是否定的(比如$R=\boldsymbol{Z}$而$S=\boldsymbol{Q}$)。下一定理给出此问题的部份解答。

定理5.9 （提升定理） 设S是R的整性扩环，P为R的素理想。则存在S的素理想Q位于P上（即$Q \cap R = P$）。

证明 由于P是素理想，$R-P$是R的乘法子集合（定理2.1），从而也是S的乘法子集合。显然$0 \notin R-P$。根据定理2.2存在S的理想它在集合{S的理想$I \mid I \cap (R-P) = \phi$}中是极大的。进而，这样的$Q$必为S中的素理想。显然$Q \cap R \subset P$.如果$Q \cap R \neq P$，取$u \in P$使得$u \notin Q$，则S中的理想$Q + (u)$真包含$Q$。由极大性可知存在$c \in (Q + (u)) \cap (R - P)$。设$c = q + su (q \in Q, s \in S)$。由于$s$在$R$上整，因此存在$r_i \in R$，使得

$$s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0.$$

将此式乘以u^n，给出

$$(su)^n + r_{n-1}u(su)^{n-1} + \cdots + r_1 u^{n-1}(su) + r_0 u^n = 0.$$

由于$su = c - q$，由二项式定理III.1.6给出

$$v = c^n + r_{n-1}uc^{n-1} + \cdots + r_1 u^{n-1}c + r_0 u^n \in Q.$$

但是$v \in R$，于是$v \in R \cap Q \subset P$。但是$u \in P$和$v \in P$导致$c^n \in P$。由于P为素理想，从而$c \in P$，这就导出矛盾。∎

系5.10 设S为R的整扩环。P_1和P均为R中的素理想，并且$P_1 \subset P$。如果Q_1是S中的素理想，并且Q_1位于P_1上，则存在S的素理想Q，使得$Q_1 \subset Q$并且Q位于P上。

证明概要 象定理5.9的证明那样，$R-P$为S中的乘法子集合。由于$Q_1 \cap R = P_1 \subset P$，我们有$Q_1 \cap (R-P) = \phi$.根据定理2.2，存在$S$的素理想$Q$包含$Q_1$并且是集合{$S$的理想$I \mid Q_1 \subset I, I \cap (R-P) = \phi$}中的极大元素。现在将定理5.9的证明逐字逐句搬过来，即可证明$Q \cap R = P$。∎

定理5.11 设S为R的整扩环，P为R中的素理想．如果Q和Q'是S中的素理想，$Q\subset Q'$并且Q和Q'均位于P上，则$Q=Q'$．

证明 只需证明如下的命题：如果Q为S中的素理想，并且$Q\cap R=P$，则Q是集合$\mathscr{S}=\{S$中理想$I\mid I\cap(R-P)=\varnothing\}$中的极大元．

如果Q不是$\mathscr{S}$中的极大元，则存在S中的理想I，使得

$$Q\subsetneq I，\text{并且}I\cap(R-P)=\varnothing．$$

于是$I\cap R=P$．取$u\in I-Q$，由于u在R上整，从而集合$\{$首1多项式$f\in R[x]\mid \deg f\geqslant 1，f(u)\in Q\}$是非空的．取具有最小次数的这样一个$f=\sum_{i=0}^{n}r_ix^i$，则

$$u^n+r_{n-1}u^{n-1}+\cdots+r_1u+r_0\in Q\subset I,$$

因此$r_0\in I\cap R\subset P=Q\cap R\subset Q$．因此

$$u(u^{n-1}+r_{n-1}u^{n-2}+\cdots+r_2u+r_1)\in Q．$$

由$\deg f$的极小性可知$(u^{n-1}+r_{n-1}u^{n-1}+\cdots+r_1)\notin Q$．由于我们所选的$u$也不属于$Q$，这就与$Q$是素理想(定理III2.15)相矛盾．因此$Q$为$S$中极大元．∎

定理5.12 设S为R的整扩环，Q为S中的素理想，并且Q位于R的素理想P之上．则Q为S中极大理想$\Longleftrightarrow P$为R中极大理想．

证明 设Q为S中极大理想，根据定理 III 2.18，可知R存在极大理想M包含P．由定理III.2.19知M也是素理想．根据系5.10，S中存在素理想Q'使得$Q\subset Q'$，并且Q'位于M上．由于Q'为素理想，从而$Q'\neq S$（定义III.2.14）．而Q之极大性导致 $Q=Q'$．从而$P=Q\cap R=Q'\cap R=M$．因此P为R中极大理想．

反之，假定P为R中极大理想．由于Q为 S 中素理想，从而$Q \neq S$，并且S中存在极大理想N包含Q(定理III.2.18)．由定理 III.2.19知N为素理想，从而$1_R = 1_S \notin N$．因为$P = R \cap Q \subset R \cap N \subsetneq R$．由极大性可知必然$P = R \cap N$．因此$Q$和$N$均位于$P$上，并且$Q \subset N$．从而由定理5.11可知$Q = N$．∎

习　题

注：如不特别声明，S永远为R的扩环．

1．设S为R的整扩环，并且R和S均为整环.则 S 为域$\Longleftrightarrow R$为域.[提示：系III2.21]．

2．设R为整环，如果R的商域F在R上整，则R为域．

3．设R为整环，F为R的商域.如果$0 \neq a \in R$并且 $1_R/a \in F$在R上整，则a为R中单位．

4．(a) 设R为整环，F为 R 的商域．$0 \neq a \in R$．则下列诸条件彼此等价：

(i) R的每个非零素理想均包含a；

(ii) R的每个非零理想均包含a的某个方幂；

(iii) $F = R[1_R/a]$ (环扩张)．

一个包含 $a \neq 0$ 的整环R如果满足条件（i）—（iii），就叫作是一个 Goldmann 环

(b) 主理想整环是Goldmann环的充要条件是该整环只有有限多个素理想．

(c) Goldmann环的同态象是否也为Goldmann环？

5．如果S为R的整扩环，而f；$S \to S$ 为环同态，并且 $f(1_S) = 1_S$，则$f(S)$是$f(R)$ 的整扩环．

6．如果S为R的整扩环，则$S[x_1, \cdots, x_n]$是$R[x_1, \cdots, x_n]$的整扩环．

7．如果S是R的整扩环，而T为R的乘法子集合 $(0 \notin T)$，则$T^{-1}S$为$T^{-1}R$

的整扩环［提示：如果$s/t\in T^{-1}S$，则$s/t=\phi_T(s)\ (1_R/t)$，其中ϕ_T：$S\to T^{-1}S$是正则映射（定理III.4.4）。求证$\phi_T(s)$和$1_R/t$在$T^{-1}R$上整，从而由定理5.5可知s/t在$T^{-1}R$上整。］

8. 每个唯一因子分解整环均整闭。［提示：命题III.6.8］。

9. 设T为含幺交换环，$\{S_i\mid i\in I\}$，$\{R_i\mid i\in I\}$为子环族，使得对于每个i，T为S_i的扩环，而S_i为R_i的扩环。如果每个R_i均在S_i中整闭，则$\bigcap_i R_i$在$\bigcap_i S_i$中整闭。

10. (a) 如果$I(\neq S)$为S的理想，则$I\cap R\neq R$并且$I\cap R$为R的理想。

(b) 如果Q为S的素理想，则$Q\cap R$为R的素理想。

6. Dedekind 整环

我们在本节中考查 Dedekind 整环。它界于主理想整环和 Noether 整环之间。Dedekind 整环在代数数论和曲线的代数理论中是很重要的，主要结果是定理 6.10，此定理以多种方式对 Dedekind 整环加以刻划。

下面的Dedekind整环的定义是基于如下的事实：每个主理想整环D均是Noether环（引理III.3.6）。因此每个理想($\neq$D)均有准素分解（定理3.6）。从第二节的引言可知，主理想整环的准素分解具有特别强的形式，即每个真理想均（唯一地）表为素理想之积。

定义6.1 整环R叫作是Dedekind整环，是指每个理想($\neq R$)均是有限个素理想之积。

例 上面的讨论表明，每个主理想整环都是 Dedekind整环。

但是反过来不成立。在定理6.10后面有例子表明 Dedekind 整环不必为主理想整环。

从定义不能明显地看出每个Dedekind整环都是Noether环。为了证明这个事实以及为了发展Dedekind整环的其他性质，我们必须引进分式理想概念。

定义6.2 设 R 为整环，K是它的商域。R的一个分式理想是 K 的非零R-子模 I，并且存在非零元素$a\in R$，使得 $aI\subset R$。

例 整环R中每个通常的非零理想均是R的 R-子模，从而为R的分式理想。反之，R的每个分式理想如果包含在R之中，必然是R 的通常的理想。

例 K的每个有限生成 R-子模I 是R的分式理想。因为如果I是由b_1，…，$b_k\in K$生成的，则 $I=Rb_1+\cdots+Rb_n$，并且对于每个 i，$b_i=c_i/a_i$，其中 $0\neq a_i$，$c_i\in R$。令 $a=a_1a_2\cdots a_n$。则 $a\neq 0$ 而 $aI=Ra_2\cdots a_nc_1+\cdots+Ra_1\cdots a_{n-1}c_n\subset R$。

注记：如果I为整环R的分式理想，$aI\subset R$ $(0\neq a\in R)$，则 aI 是R中通常理想，并且映射$I\to aI$，$x\to ax$是 R-模同构。

定理6.3 如果R是整环，K是R的商域，则R 的全部分式理想集合形成一个含幺交换半群，其幺元素为 R，而乘法是

$$IJ=\left\{\sum_{i=1}^{n}a_ib_i \mid a_i\in I,\ b_i\in J \quad n\in \boldsymbol{N}^*\right\}$$

证明 作为练习。注意如果I和J是R的理想，则IJ 正好是通常的理想之积。▌

整环R的分式理想I叫作可逆的，是指存在R 的某个分式理想

J，使得 $IJ=R$。因此，可逆分式理想[注]恰好为分式理想含幺半群中的可逆元。

注记：(i) 可逆分式理想I的逆是唯一的。并且$I^{-1}=\{a\in K\mid aI\subset R\}$。事实上，对于任意分式理想 I，不难看出，集合 $I^{-1}=\{a\in K\mid aI\subset R\}$也是分式理想，并且$I^{-1}I=II^{-1}\subset R$。如果$I$是可逆的，并且$IJ=JI=R$，显然有$J\subset I^{-1}$。反之，因为$I^{-1}$和$J$均为$K$的$R$-子模，从而 $I^{-1}=RI^{-1}=(JI)I^{-1}=J(II^{-1})\subset JR=RJ\subset J$，于是 $J=I^{-1}$。

(ii) 如果I，A，B 均是R的分式理想，并且$IA=IB$，而 I是可逆的，则 $A=RA=(I^{-1}I)A=J^{-1}(IB)=RB=B$。

(iii) 如果I为R中的通常理想，则$R\subset I^{-1}$。

例 整环R中每个非零主理想都是可逆的。如果K是 R 的商域，而$I=(b)$，其中$b\neq 0$，令$J=Rc\subset K$，其中$c=1_R/b$。则J 为R的分式理想，并且$IJ=R$。

可逆分式理想在刻划Dedekind 整环时起着关键的作用。下面五个结果展示了关于可逆分式理想的一些事实。

引理6.4 设I，I_1，$I_2\cdots$，I_n是整环R的理想。

(i) 理想$I_1I_2\cdots I_n$可逆$\Longleftrightarrow$每个I_j均是可逆的。

(ii) 如果$P_1\cdots P_m=I=Q_1\cdots Q_n$，其中$P_i$，$Q_j$ 均是R中的素理想，并且每个P_i均可逆，则 $m=n$，并且（在重新加以标号之后）$P_i=Q_i$ $(1\leqslant i\leqslant m)$。

证明 (i) 如果J为分式理想，使得$J(I_1\cdots I_n)=R$，则对每个 $j=1$，2，$\cdots$，n，我们有$I_j(JI_1\cdots I_{j-1}I_{j+1}\cdots I_n)=R$，从而$I_j$ 是可

〔注〕 在文献中，可逆分式理想有时也简称作可逆理想。

逆的。反之，如果每个I_j是可逆的，则 $(I_1\cdots I_n)(I_1^{-1}\cdots I_n^{-1})=R$，因此$I_1\cdots I_n$是可逆的。

(ii) 对于m作数学归纳法。如果$m=1$，读者可自行证明.如果$m>1$，取一个P_i（不妨设为P_1），使得当 $2\leqslant i\leqslant m$时，P_1均不真包含P_i。由于$Q_1\cdots Q_n=P_1\cdots P_m\subset P_1$，而$P_1$ 为素理想，从而有某个Q_j（不妨设为Q_1）包含在P_1之中（定义III.2.14)。类似地，由于$P_1\cdots P_m=Q_1\cdots Q_n\subset Q_1$，从而有某个 i，使得 $P_i\subset Q_1$。于是$P_i\subset Q_1\subset P_1$。由$P_1$的极小性，我们必须有$P_i=Q_1=P_1$。因为$P_1=Q_1$是可逆的，从定理6.3后面的注记 (ii) 可推出

$$P_2P_3\cdots P_m=Q_2Q_3\cdots Q_n。$$

因此由归纳假设可知$m=n$，并且（在重新加以标号之后）$P_i=Q_i$ $(1\leqslant i\leqslant m)$。∎

在引理6.4和定理 III.3.4前面的例子表明，主理想整环中每个非零素理想都是可逆的极大理想。更一般的我们有

定理6.5 如果R是 Dedekind 整环，则R的每个非零素理想均是可逆的极大理想。

证明 我们首先证明，每个可逆素理想P 都是极大理想。如果$a\in R-P$，我们要证明由P 和a 生成的理想 $P+Ra$是 R。假如$P+Ra\neq R$，因为R是 Dedekind整环，从而有素理想P_i和 Q_j，使得$P+Ra=P_1P_2\cdots P_m$，$P+Ra^2=Q_1Q_2\cdots Q_n$。令 π：$R\to R/P$是正则满同态，考虑由 $\pi(a)$ 和$\pi(a^2)$ 生成的 R/P之两个主理想，显然

$$(\pi(a))=\pi(P_1)\cdots\pi(P_m),\quad (\pi(a^2))=\pi(Q_1)\cdots\pi(Q_n).$$

由于 $\mathrm{Ker}\pi=P\subset P_i$，而对于每个$i$均有 $P\subset Q_i$，从而$\pi(P_i)$和$\pi(Q_i)$均为R/P中素理想（习题III.2.17(a)）。因为R/P 是整环（定理

III.2.16)，从而R/P中每个主理想均可逆（见引理6.4前面的例子）。于是由引理6.4(i)，可知$\pi(P_i)$和$\pi(Q_j)$是可逆的。因为

$\pi(Q_1)\cdots\pi(Q_n)=(\pi(a^2))=(\pi(a))^2=\pi(P_1)^2\cdots\pi(P_m)^2$。引理6.4 (ii) 导致$n=2m$，并且（在重新加以标号之后）$\pi(P_i)=\pi(Q_{2i})=\pi(Q_{2i-1})$ $(1\leqslant i\leqslant m)$。因为对于每个$i$和$j$均有$\mathrm{Ker}\pi=P\subset P_i$和$P\subset Q_j$，从而

$P_i=\pi^{-1}(\pi(P_i))=\pi^{-1}(\pi(Q_{2i}))=Q_{2i}$。 类似地，$P_i=Q_{2i-1}$ $(1\leqslant i\leqslant m)$。从而$P+Ra^2=(P+Ra)^2$，而$P\subset P+Pa^2\subset(P+Ra)^2\subset P^2+Ra$。如果$b=c+ra\in P(c\in P^2, r\in R)$，则$ra\in P$。因此$r\in P$（因为$a\notin P$而$P$为素理想）。从而$P\subset P^2+Pa\subset P$，这又导致$P=P^2+Pa=P(P+Ra)$。由于$P$可逆，从而$R=P^{-1}P=P^{-1}P(P+Ra)=R(P+Ra)=P+Ra$。这就导致矛盾。从而每个可逆素理想均是极大理想。

现在假设P为R中任意非零素理想，而c为P中非零元素。则$(c)=P_1P_2\cdots P_n$，其中P_i均为素理想。由于$P_1P_2\cdots P_n=(c)\subset P$，从而有某个$k$，使$P_k\subset P$（定义III.2.14)。主理想$(c)$是可逆理想，从而$P_k$也可逆（引理6.4 (i)）。由证明的第一部分可知P_k为极大理想，从而$P_k=P$，即P为可逆极大理想。∎

例 如果F为域，则多项式整环$F[x_1, x_2]$中主理想(x_1)和(x_2)均为素理想，但均不是极大理想（因为$(x_i)\subsetneq(x_1, x_2)\subsetneq F[x_1, x_2]$)。因此$F[x_1, x_2]$不是Dedekind整环（定理6.5)。但是$F[x_1, x_2]$为Noetker整环（定理4.9)。从而存在着不是Dedekind整环的Noether整环。

引理6.6 如果I是整环R的分式理想，$f\in\mathrm{Hom}_R(I, R)$，则对每个$a, b\in I$，均有$af(b)=bf(a)$。

证明 令$a=r/s$, $b=v/t$ (r, s, v, $t\in R$, s, $t\neq 0$), 则$sa=r$, $tb=v$, 于是$sab=rb\in I$, $tab=va\in I$. 因此在R中有$sf(tab)=f(stab)=tf(sab)$. 从而$af(b)=saf(b)/s=f(sab)/s=f(tab)/t=tbf(a)/t=bf(a)$. ∎

引理6.7 设R为整环而K是它的商域, 则R 中每个可逆分式理想均是有限生成的R-模.

证明 由于 $I^{-1}I=R$, 从而有 $a_i\in I^{-1}$, $b_i\in I$, 使得$1_R=\sum_{i=1}^{m}a_ib_i$. 如果$c\in I$, 则$c=\sum_{i=1}^{n}(ca_i)b_i$. 进而, 由于 $a_i\in I^{-1}=\{a\in K\mid aI\subset R\}$, 从而$ca_i\in R$. 因此$I$作为$R$-模是由$b_1$, $\cdots b_n$ 生成的 (定理IV.1.5(iii)). ∎

我们已经看到,主理想整环D 中每个非零理想I均是可逆的. 进而,作为D-模,I同构于 D(见定理IV.1.5(i)). 因此I是自由模, 从而为投射 D-模. 这个结果在任意整环中都成立.

定理6.8 假设R是整环而I是R 的分式理想. 则 I 是可逆的$\Longleftrightarrow$$I$为投射$R$-模.

证明 ($\Longrightarrow$): 由引理6.7和定理IV.1.5可知 $I=Rb_1+\cdots+Rb_n$, 其中$b_i\in I$并且 $1_R=\sum_{i=1}^{n}a_ib_i(a_i\in I^{-1})$. 令$F$为自由 R-模, 并且n个元素 e_1, $\cdots$, e_n 形成它的一组基. 则映射 π: $F\to I$, $e_i\longmapsto b_i$是R-模满同态 (见定理IV2.1),从而有短正合序列 $0\to\mathrm{Ker}\,\pi\to F\xrightarrow{\pi}I\to 0$. 定义 ζ: $I\to F$, $c\longmapsto ca_1e_1+\cdots+ca_ne_n(c\in I)$, 证明$\zeta$为$R$-模同态, 并且$\pi\zeta=1_I$. (注意$a_i\in I^{-1}$, 从而对于每个$i$, $ca_i\in R$). 于是正合序列是分裂的, 从而I 为自由 R-模的直和成

分（定理IV.1.18）。于是由定理N.3.14可知I为投射R-模。

（$\Longleftarrow$）：令$X=\{b_j \mid j\in J\}$是投射R-模I的一个非零生成元集合（可能是无限集合）。设b_0为X中一个固定元素。令F是以$\{e_j \mid j\in J\}$为基的自由R-模。而φ：$F\to I$，$e_i\longmapsto b_i$是R-模满同态（定理IV.2.1）。由于I为投射模，从而存在R-模同态ψ：$I\to F$，使得$\varphi\psi=1_I$。对于每个$j\in J$，设π_j：$F\to Re_j\cong R$为正则射影：$F\ni\sum_i r_ie_i\longmapsto r_j\in R$（见定理IV.2.1）。于是对于每个$j$，映射$\theta_j=\pi_j\psi$：$I\to R$是$R$-模同态。令$c_j=\theta_j(b_0)$。对于每个$c\in I$，由引理6.6知$cc_j=c\theta_j(b_0)=b_0\theta_j(c)$，从而在$R$的商域K中，$c(c_j/b_0)=cc_j/b_0=b_0\theta_j(c)/b_0=\theta_j(c)\in R$。因此

$$c_j/b_0\in I^{-1}=\{a\in K\mid aI\subset R\}.$$

从而对于每个$c\in I$均有

$$\psi(c)=\sum_{j\in J_1}\theta_j(c)e_j=\sum_{j\in J_1}c(c_j/b_0)e_j,$$

其中J_1为有限子集合$\{j\in J\mid\theta_j(c)\neq 0\}$。因此对于每个$0\neq c\in I$，

$$c=\phi\psi(c)=\phi\left(\sum_{j\in J_1}c(c_j/b_0)e_j\right)=\sum_{j\in J_1}c(c_j/b_0)b_j$$

$$=c\left(\sum_{j\in J_1}(c_j/b_0)b_j\right).$$

从而$1_R=\sum_{j\in J_1}(c_j/b_0)b_j$，其中$c_j/b_0\in I^{-1}$。由此得出$R\subset I^{-1}I$。由于$I^{-1}I\subset R$永远成立，从而$R=I^{-1}I$，即$I$是可逆的。∎

为了刻划Dedekind整环，我们还需要引进另一个概念。一个离散赋值环是恰好有一个非零素理想的主理想整环（注意零理想在每个整环中均是素理想）。

引理6.9 如果R为Noether 整闭整环，并且 R有唯一的非零素理想P，则R是离散赋值环。

证明 我们只需要证明R 中每个真理想均是主理想。这需要下列一些事实：

(i) 设K是R的商域。对于R的每个分式理想I，集合$\bar{I} = \{a \in K \mid aI \subset I\}$恰好是$R$；

(ii) $R \subsetneq P^{-1}$；

(iii) P可逆；

(iv) $\bigcap_{n \in N^*} P^n = 0$；

(v) P为主理想。

先假设 (i)—(v) 成立。设I为R中任意理想。则I包含在R的一个非零极大理想 M 之中 (定理 III.2.18)，而 M为素理想 (定理III.2.19)。由唯一性可知$M = P$，从而$I \subset P$。由(iv) 可知 $\bigcap_{n \in N^*} P^n = 0$，从而有一个最大整数m，使得$I \subset P^m$但是$I \not\subset P^{m+1}$。取 $b \in \mathrm{I} - P^{m+1}$。由 (v) 知$P = (a)$，$a \in R$。从而 $P^m = (a)^m = (a^m)$。因为 $b \in P^m$，从而 $b = ua^m$，此外 $u \notin P = (a)$ (否则 $b \in P^{m+1} = (a^{m+1})$)。因此$u$为$R$中单位(否则由定理III.3.2，$(u)$将为真理想，从而由上面的推导，$(u)$ 包含在P之中)。于是由定理III.3.2，$P^m = (a^m) = (ua^m) = (b) \subset I$，从而$I$为主理想$P^m = (a^m)$。

下面验证命题(i)—(v)的正确性。

(i) 显然$R \subset \bar{I}$。不难看出，$\bar{I}$是K的子环，并且是R的分式理想。从而 (作为R-模) $\bar{I}$同构于R的某个理想 (见定理6.3前面的注记)。由于R是Noether 环，从而$\bar{I}$是有限生成的 (定理1.9)。定理5.3 (取$T = \bar{I}$) 导致$\bar{\mathrm{I}}$的每个元素在R上均整，而R是整闭的，从

而$\bar{I}\subset R$。于是$I=R$。

(ii) 注意对R中每个理想J均有$R\subset J^{-1}$。令$\mathscr{F}=\{R$中理想$J\mid R\subsetneq J^{-1}\}$。由于$P$是真理想（定义III.2.14），根据定理III.3.2可知P中每个非零元素均不是单位。如果$J=(a)$ $(0\neq a\in P)$，则$1_R/a\in J^{-1}$，但是$1_R/a\notin R$，从而$R\subsetneq J^{-1}$。因此$\mathscr{F}$是非空集合。由于R是Noether环，$\mathscr{F}$具有极大元M（定理1.4）。我们现在证M为R的素理想：如果$ab\in M$，其中a，$b\in R$而$a\notin M$。取$c\in M^{-1}-R$，则$c(ab)\in R$。因此$bc(aR+M)\subset R$，从而$bc\in(aR+M)^{-1}$。于是$bc\in R$（否则$aR+M\in\mathscr{F}$，这就与M的极大性相矛盾）。从而$c(bR+M)\subset R$，于是$c\in(bR+M)^{-1}$。但是$c\notin R$。由M的极大性可知$bR+M=M$，于是$b\in M$因此由定理III.2.15可知M为素理想。由于$M\neq 0$，从而由唯一性知$P=M$。因此$R\subsetneq M^{-1}=P^{-1}$。

(iii) 显然$P\subset PP^{-1}\subset R$。采用本证明第一段(注)中的推理，可以证明$P$是$R$中的唯一极大理想，从而$P=PP^{-1}$或者$PP^{-1}=R$。但是如果$P=PP^{-1}$，则$P^{-1}\subset\bar{P}$，而由(i)和(ii)可知$R\subsetneq P^{-1}\subset\bar{P}=R$，这就导致矛盾。因此$PP^{-1}=R$。即$P$是可逆的。

(iv) 如果$\bigcap_{n\in N^*}P^n\neq 0$，则$\bigcap_{n\in N^*}P^n$是$R$的分式理想。验证$P^{-1}\subset\overline{\bigcap_{n\in N^*}P^n}$。因此由(i)和(ii)可知$R\subsetneq P^{-1}\subset\overline{\bigcap_{n\in N^*}P^n}=R$。这就导致矛盾。

(v) 存在$a\in P$使得$a\notin P^2$（否则便有$P=P^2$，从而$\bigcap_{n\in N^*}P^n=P\neq 0$。这就与(iv)相矛盾）。因此$aP^{-1}$是$R$中非零理想，并且$aP^{-1}\not\subset P$（否则便有$a\in aR=aP^{-1}P\subset P^2$）。本证明的第一段指出，

(注) 即指“先假定(i)—(v)成立…从而$I\subset P$.”那一段，下同.——译者注。

R中每个真理想均包含在P之中，从而$aP^{-1}=R$。于是由 (iii) 可知 $(a)=(a)R=(a)P^{-1}P=(aP^{-1})P=RP=P$。 ∎

定理6.10 关于整环R的下列诸条件是彼此等价的：

(i) R为Dedekind整环；

(ii) R中每个真理想均可唯一地表示成有限多个素理想的乘积；

(iii) R中每个非零理想均可逆；

(iv) R的每个分式理想均可逆；

(v) R的所有分式理想构成的集合对于乘法形成群；

(vi) R中每个理想均是投射R—模。

(vii) R的每个分式理想均是投射R—模。

(viii) R为 Noether 整闭整环，并且每个非零素理想均是极大理想；

(ix) R是Noether环，并且对于R的每个非零素理想 P，R在P处的局部化R_P是离散赋值环。

证明 等价(iv)$\Longleftrightarrow$(v)是显然的(见定理6.3)。(i)$\Longrightarrow$(ii)和 (ii)$\Longrightarrow$(iii) 从引理 6.4 和定理 6.5 得到。(iii)$\Longleftrightarrow$(vi) 和 (vii)$\Longleftrightarrow$(iv) 是定理6.8的直接推论。(vi)$\Longrightarrow$(vii) 可由定理6.3前面的注记得出。于是，为了完成整个证明，我们只需再验证(iv)$\Longrightarrow$(viii)，(viii)$\Longrightarrow$(ix)和(ix)$\Longrightarrow$(i)即可。

(iv)$\Longrightarrow$(viii)：由 (iv) 知R中每个理想均可逆，从而根据引理6.7，它们均是有限生成的。因此由定理1.9可知R是Noether环。令K为R的商域。如果$u\in K$在R上整，由定理5.3可知$R[u]$为K的有限生成R-子模。由定义6.2后面第二个例子，可知$R[u]$是R的分式理想。由(iv)知$R[u]$是可逆的。由于$R[u]R[u]=R[u]$，

从而$R[u]=RR[u]=(R[u]^{-1}R[u])R[u]=R[u]^{-1}R[u]=R$，即$u\in R$。从而$R$是整闭整环。最后，若$P$是$R$中非零素理想，则存在$R$的一个极大理想$M$包含$P$（定理III.2.18)。由(iv)知$M$是可逆的，因此$M^{-1}P$为$R$的分式理想，并且$M^{-1}P\subset M^{-1}M=R$。从而$M^{-1}P$为$R$中理想。由于$M(M^{-1}P)=RP=P$而$P$为素理想，从而$M\subset P$或者$M^{-1}P\subset P$。但是如果$M^{-1}P\subset P$，则$R\subset M^{-1}=M^{-1}R=M^{-1}PP^{-1}\subset PP^{-1}\subset R$，从而$M^{-1}=R$。因此$R=MM^{-1}=MR=M$。这就与$M$为极大理想相矛盾。从而$M\subset P$，即$M=P$。所以$P$为极大理想。

(viii)$\Longrightarrow$(ix)：从定理5.8可知R_P为整闭整环。由引理III.4.9知R_P中每个理想均有形式$I_P=\{i/s\mid i\in I,\ s\notin P\}$，其中$I$是$R$的理想。由(viii)和定理1.9知$R$的每个理想均是有限生成的，从而$R_P$的每个理想均是有限生成的。由定理1.9便知$R_P$为Noether环。由定理IV.4.11可知$R_P$的每个非零素理想均有形式$I_P$，其中$I$为$R$的非零素理想，并且包含在$P$中，但是由(viii)，$R$的每个非零素理想均是极大理想，从而$P_P$是$R_P$中唯一的非零素理想。由引理6.9便知$R_P$是离散赋值环，

(ix)$\Longrightarrow$(i)：我们先证每个理想$I(\neq 0)$均可逆。由于II^{-1}为R的分式理想，并且包含在R中（定理6.3后面的注记(i)），从而II^{-1}为R中的理想。如果$II^{-1}\neq R$，则存在极大理想M包含II^{-1}(定理III.2.18)。但是M为素理想(定理III.2.19)。由(ix)知I_M为R_M中主理想，设$I_M=(a/s)$，其中$a\in I$，$s\in R-M$。因为R是Noether环，由定理1.9可知I是有限生成的，设$I=(b_1,\cdots,b_n)$。对于每个i，$b_i/1_R\in I_M$，从而在R_M中$b_i/1_R=(r_i/s_i)(a/s)$，其中$r_i\in R$，$s_i\in R-M$。因此，$s_isb_i=r_ia\in I$。设$t=ss_1s_2\cdots s_n$。因为$R-M$是乘法子集，$t\in R-M$。在R的商域中，对于每个i均有$(t/a)b_i=$

$tb_i/a = s_1\cdots s_{i-1}s_{i+1}\cdots s_n r_i a \in I \subset R$，于是$t/a \in I^{-1}$。从而$t = (t/a)a \in I^{-1}I \subset M$，这就与$t \in R - M$这一事实相矛盾。因此$II^{-1} = R$，即$I$是可逆的。

对于R的每个理想$I(\neq R)$，取R的一个极大理想M_I，使得$I \subset M_I \subsetneq R$（定理 III.2.18 和选择公理）。如果 $I = R$，令 $M_R = R$。则IM_I^{-1}是R的分式理想，并且$IM_I^{-1} \subset M_I M_I^{-1} \subset R$。因此$IM_I^{-1}$是$R$的理想，并且显然包含$I$。另一方面，如果$I$为真理想，则$I \subsetneq IM_I^{-1}$（否则的话，由于$I$和$M_I$均是可逆的，便有$R = RR = (I^{-1}I)(M_I^{-1}M_I) = I^{-1}(IM_I^{-1})M_I = I^{-1}IM_I = RM_I = M_I$，这就与$M_I$的选取方法相矛盾）。令 S 是 R 的全部理想构成的集合，定义函数 f：$S \longrightarrow S$，$I \longmapsto IM_I^{-1}$。给了一个真理想J，由引论中的归纳定理（其中对于每个n均取$f_n = f$），可知存在一个函数ϕ：$\boldsymbol{N} \longrightarrow S$，使得$\phi(0) = J$，$\phi(n+1) = f(\phi(n))$。如果令 $J_n = \phi(n)$，而$M_n = MJ_n$，则有理想的升链：$J = J_0 \subset J_1 \subset \cdots$，使得 $J = J_0$ 并且 $J_{n+1} = f(J_n) = J_n M_n^{-1}$。因为$R$是 Noether 环而$J$是它的真理想，从而有一个最小整数 k，使得

$$J = J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_{k-1} \subsetneq J_k = J_{k+1}.$$

因此 $J_k = J_{k+1} = f(J_k) = J_k M_k^{-1}$。上面的注记表明这只在$J_k = R$的时候才有可能。从而$R = J_k = f(J_{k-1}) = J_{k-1}M_{k-1}^{-1}$。

于是

$$J_{k-1} = J_{k-1}R = J_{k-1}M_{k-1}^{-1}M_{k-1} = RM_{k-1} = M_{k-1}.$$

由于 $M_{k-1} = J_{k-1} \subsetneq J_k = R$，从而$M_{k-1}$是极大理想。而$k$的极小性保证$M_0$，…，$M_{k-2}$也均是极大理想（否则便有 $M_j = R$，从而 $J_{j+1} = J_j M_j^{-1} = J_j R^{-1} = J_j R = J_j$）。不难证明

$$M_{k-1} = J_{k-1} = J_{k-2}M_{k-2}^{-1} = J_{k-3}M_{k-3}^{-1}M_{k-2}^{-1} = \cdots$$
$$= JM_0^{-1}M_1^{-1}\cdots M_{k-2}^{-1}.$$

由于M_i均是可逆的，因此

$$M_{k-1}(M_0\cdots M_{k-2})=JM_0^{-1}\cdots M_{k-2}^{-1}(M_0\cdots M_{k-2})=J.$$

于是J为真极大理想（从而为素理想）的积。因此R为Dedekind整环。 ∎

最后我们给出一个例子，表明存在着不是主理想整环的Dedekind整环。

例 整环$\mathbf{Z}[\sqrt{10}]=\{a+b\sqrt{10}\mid a,b\in\mathbf{Z}\}$的商域为$\mathbf{Q}(\sqrt{10})=\{r+s\sqrt{10}\mid r,\ s\in\mathbf{Q}\}$。利用初等数论经过一些乏味的计算，可知$\mathbf{Z}[\sqrt{10}]$是整闭的（习题14）。因为赋值映射 $\mathbf{Z}[x]\longrightarrow\mathbf{Z}[\sqrt{10}]$，$f(x)\longmapsto f(\sqrt{10})$是满同态，而$\mathbf{Z}[x]$为Noether环（定理4.9），从而$\mathbf{Z}[\sqrt{10}]$也是Noether环（习题1.5）。最后，不难证明$\mathbf{Z}[\sqrt{10}]$的每个真素理想必是极大理想（习题15）。因此由定理6.10 (viii) 可知$\mathbf{Z}[\sqrt{10}]$是Dedekind 整环。但是$\mathbf{Z}[\sqrt{10}]$不是主理想整环（定理III.3.7和习题III.3.4）。

习　题

1. $\mathbf{C}$的子整环$\mathbf{Z}[\sqrt{5}i]$中由3和$1+\sqrt{5}i$生成的理想是可逆的。
2. 一个整环如果是局部环，则此整环中的可逆理想必为主理想。
3. 如果I为整环R中的可逆理想，而S为R中的乘法集合，并且$0\notin S$，则$S^{-1}I$为$S^{-1}R$中的可逆理想。
4. 设R为含幺环而P为R-模。则P为投射模$\Leftrightarrow$存在着集合$\{a_i\mid i\in I\}\subset P$和$\{f_i\mid i\in I\}\subset \mathrm{Hom}_R(P,R)$，使得对于每个$a\in P$均有$a=\sum_{i\in I}f_i(a)a_i$[见

定理6.8的证明].

5. (引理6.9的逆).离散赋值环R是Noether整闭整环.[提示:习题5.8].

6. (a) 如果整环R中每个素理想均可逆，则R为Dedekind整环.

(b) 如果R是Noether整环，并且它的每个极大理想均是可逆的，则R为Dedekind整环.

7. 如果S为Dedekind整环R的乘法子集合（并且$1_R \in S$，$0 \notin S$），则$S^{-1}R$为Dedehind整环.

8. 如果R为整环而P为$R[x]$中素理想，并且$P \cap R = 0$，则$R[x]_P$为离散赋值环.

9. 如果Dedekind整环R只有有限个非零素理想 P_1，…，P_n，则R为主理想整环.[提示：存在$a_i \in P_i - P_i^2$,然后由中国剩余定理III.2.25可知存在$b_i \in P_i$，使得$b_i = a_i \pmod{P_i}$.并且$b_i \equiv 1_R \pmod{P_j}$（对每个$j \neq i$).证明$P_i = (b_i)$，由此得出每个理想均为主理想.]

10. 如果I为Dedekind整环R中的非零理想，则R/I为Artin环.

11. Dedekind整环中每个真理想均可由至多两个元素生成.

12. 一个R-模叫作是可除模，是指对于每个非零$r \in R$，$rA = A$.如果R是Dedehind整环则每个可除R-模均是内射模.[注意：逆命题也是对的，但是证明比较难.]

13. 如果R是Dedekind整环，K是它的商域，F是K的有限维扩域，而S是R在F中的整闭包（即$S = \{a \in F \mid a$在R上整$\}$.则S为Dedekind整环.

14. (a) 证明整环$\mathbf{Z}[\sqrt{10}]$是$\mathbf{Z}$的整扩环，并且它的商域为$\mathbf{Q}(\sqrt{10})$.

(b) 设$u \in \mathbf{Q}(\sqrt{10})$在$\mathbf{Z}[\sqrt{10}]$上整，则$u$在$\mathbf{Z}$上整（定理 5.6).此外，又如果$u \in \mathbf{Q}$，则$u \in \mathbf{Z}$（习题5.8).证明如果$u \in \mathbf{Q}(\sqrt{10}) - \mathbf{Q}$，则$u$是$\mathbf{Z}[x]$中一个二次不可约首1多项式的根.[提示：系III.6.13 和定理V.1.6].

(c) 求证：如果$u = r + s\sqrt{10} \in \mathbf{Q}(\sqrt{10})$,而$u$为 $x^2 + ax + b \in \mathbf{Z}[x]$的根，则$a = -2r$并且$b = r^2 - 10s^2$.[提示：注意$u^2 - 2ru + (r^2 - 10s^2)$

$=0$. 如果$u\notin\mathbf{Q}$则利用定理V.1.6]

(*d*) 求证$\mathbf{Z}[\sqrt{10}]$整闭.[提示：如果$u=r+s\sqrt{10}\in\mathbf{Q}(\sqrt{10})$是$x^2+ax+b\in\mathbf{Z}[x]$的根，并且若$a$为偶数，则由(*c*)$\Rightarrow s\in\mathbf{Z}$从而$s\in\mathbf{Z}$. 如果$a$为奇数则导出矛盾.]

15. (*a*) 如果P为环$Z[\sqrt{10}]$的非零素理想，则$P\cap\mathbf{Z}$为$\mathbf{Z}$的非零素理想.[提示：如果$0\neq u\in P$，则由习题14，u为$x^2+ax+b\in\mathbf{Z}[x]$的根. 证明a和b必有一个不为零，并且属于P.]

(*b*) $\mathbf{Z}[\sqrt{10}]$的每个非零素理想都是极大理想.[利用(*a*)，定理III.3.4，然后或者直接推导，或者用定理5.12]

16. 所谓赋值整环是满足下面性质的整环：a，$b\in R\Rightarrow a|b$或$b|a$.(离散赋值环显然是赋值整环.) 所谓Prüfer整环是一个整环并且它的每个有限生成理想均是可逆的.

(*a*) 下列三个命题是彼此等价的：

(i) R为Prüfer整环；

(ii) 对于R中每个素理想P，R_P均是赋值整环；

(iii) 对于R中每个极大理想M，R_M均是赋值整环.

(*b*) 一个Prüfer整环为Dedekind整环的充要条件是它为Noether环.

(*c*) 如果R为Prüfer整环，其商域为K，则满足$R\subset S\subset K$的任一整环S必是Prüfer整环.

7. Hilbert 零点定理

第VI.1节和本章第5节的结果可以用来证明经典代数几何中一个著名的结果：Hilbert零点定理. 其中我们也要证明Noether正则化引理. 开始我们先非常简略地勾划一下它的几何背景.

(在本节末尾还要继续进行这一讨论)。

经典代数几何是研究多项式方程组。

$$f(x_1, x_2, \cdots x_n) = 0 \quad (f \in S).$$

的公共解。其中K为域而$S \subset K[x_1, \cdots, x_n]$。这种方程组的每个解是一个$n$元组 $(a_1, \cdots, a_n) \in F^n = F \times \cdots \times F$($n$个)，其中$F$是$K$的代数封闭的扩域，并且对于每个$f \in S$均有$f(a_1, \cdots, a_n) = 0$。这样一个解也叫作$S$在$F^n$中的零点。而$S$的全部零点所成的集合叫作$F^n$中由$S$定义的一个仿射$K$-簇（或者叫作$K$-代数集合)。并且表示成$V(S)$。因此

$V(S) = \{(a_1, \cdots, a_n) \in F^n \mid f(a_1, \cdots, a_n) = 0$ (对于每个$f \in S)\}$注意如果I是S在$K[x_1, \cdots, x_n]$中生成的理想，则 $V(I) = V(S)$。

映射$S \longrightarrow V(S)$是从 $K[x_1, \cdots, x_n]$ 的子集族到F^n的子集族的函数。反之，我们如下定义一个从F^n的子集族到$K[x_1 \cdots, x_n]$的子集族的函数：$Y \longrightarrow J(Y)$，其中$Y \subset F^n$，而

$$J(Y) = \{f \in K[x_1, \cdots, x_n] \mid f(a_1, \cdots, a_n) = 0 \quad (\text{对每个}(a_1, \cdots, a_n) \in Y)\}$$

注意$J(Y)$事实上为$K[x_1, \cdots, x_n]$ 的理想。由V和J给出的对应具有一些性质，其形式与域的伽罗华扩张中间域和伽罗华群的子群之间的伽罗华对应很相象。换句话说，我们有引理 $V.2.6$的如下模拟：

引理7.1 设F为K的代数封闭的扩域，令S，T为$K[x_1, \cdots, x_n]$的子集合，X，Y为F^n的子集合。则：

(i) $V(K[x_1, \cdots, x_n]) = \phi$，$J(F^n) = \phi$，$J(\phi) = K[x_1, \cdots, x_n]$；

(ii) $S \subset T \Rightarrow V(T) \subset V(S)$；$X \subset Y \Rightarrow J(Y) \subset J(X)$；

(iii) $S\subset J(V(S))$, $Y\subset V(J(Y))$;

(iv) $V(S)=V(J(V(S)))$, $J(Y)=J(V(J(Y)))$。

证明作为练习。∎

人们自然要问：哪些对象在这个对应之下是闭的，即哪些S和Y满足$J(V(S))=S$, $V(J(Y))=Y$？$K[x_1,\cdots,x_n]$的闭子集合容易刻划（习题2）。但是为了刻划F^n的闭子集，需要Hilbert零点定理。这个定理是说：对于$K[x_1,\cdots,x_n]$的每个真理想I，均有$J(V(I))=RadI$，为了证明Hilbert零点定理，我们需要两个预备性结果，其中第一个结果也有它自身的重要性。

定理7.2 （Noether正则化引理）设R为整环，并且为域K上的有限生成扩环。设r为R的商域F对于K的超越次数。则存在R中代数无关子集合$\{t_1,t_2,\cdots,t_r\}$，使得R在$K[t_1,\cdots,t_r]$上整。

证明 设$R=K[u_1,\cdots,u_n]$，则$F=K(u_1,\cdots,u_n)$。如果$\{u_1,\cdots,u_n\}$在K上是代数无关的，由系vi.1.6可知$\{u_1,\cdots,u_n\}$是F在K上的超越基，于是$r=n$，而定理显然是对的。如果$\{u_1,\cdots,u_n\}$在K上代数相关，则$r\leqslant n-1$（系v1.1.7），而

$$\sum_{(i_1,\cdots,i_n)\in I} k_{i_1\cdots i_n}u_1^{i_1}u_2^{i_2}\cdots u_n^{i_n}=0。$$

其中I是非负整数的n数组形成的有限集合，并且对于每个$(i_1,\cdots,i_n)\in I$, $k_{i_1},\cdots,i_n$为K中非零元素。以C表示一个正整数，它大于每个数组$(i_1,\cdots,i_n)\in I$中的每个分量i_s。如果$(i_1,\cdots,i_n)$, $(j_1,\cdots,j_n)\in I$并且

$$i_1+ci_2+c^2i_3+\cdots+c^{n-1}i_n=j_1+cj_2+c^2j_3+\cdots+c^{n-1}j_n,$$

则$c\mid(i_1-j_1)$，这必然导致$i_1=j_1$（因为$c>i_1\geqslant 0$, $c>j_1\geqslant 0\Rightarrow c>|i_1-j_1|$），从而$i_2+ci_3+\cdots+c^{n-2}i_n=j_2+cj_3+\cdots+c^{n-2}j_n$。

如前一样，我们有 $c \mid i_2 - j_2$，于是 $i_2 = j_2$。重复使用这个推理，可知 $(i_1,\cdots,i_n) = (j_1,\cdots,j_n)$。因此集合

$$\{i_1 + ci_2 + c^2 i_3 + \cdots + c^{n-1} i_n \mid (i_1,\cdots,i_n) \in I\}$$

是 $|I|$ 个不同的非负整数。特别地，它有唯一的极大值 $j_1 + cj_2 + \cdots + c^{n-1} j_n$（对于某个 $(j_1,\cdots,j_n) \in I$）。令

$$v_2 = u_2 - u_1^c,\ v_3 = u_3 - u_1^{c^2},\cdots,v_n = u_n - u_1^{c^{n-1}}.$$

如果将上面关于代数相关的关系式展开，通过变量代换 $u_i = v_i + u_1^{c^{i-1}}$ $(2 \leqslant i \leqslant n)$，我们得到

$$k_{j_1\cdots j_n} u_1^{j_1 + cj_2 + c^2 j_3 + \cdots + c^{n-1} j_n} + f(u_1, v_2, v_3, \cdots, v_n) = 0,$$

其中 $f \in K[x_1,\cdots,x_n]$ 对于 x_1 的次数严格小于 $j_1 + cj_2 + \cdots + c^{n-1} j_n$。因此 u_1 为首 1 多项式

$$x^{j_1 + cj_2 + \cdots + c^{n-1} j_n} + k^{-1}_{j_1\cdots j_n} f(x, v_2, \cdots, v_n) \in K[v_2,\cdots,v_n][x]$$

的根，从而 u_1 在 $K[v_2,\cdots,v_n]$ 上整。根据定理5.5，$K[u_1, v_2, \cdots, v_n] = K[v_2,\cdots,v_n][u_1]$ 在 $K[v_2,\cdots,v_n]$ 上整。由于每个 u_i $(2 \leqslant i \leqslant n)$ 显然在 $K[u_1, v_2, \cdots, v_n]$ 上整，从而由定理5.5和5.6 导致

$$R = K[u_1,\cdots,u_n]$$

在 $K[v_2,\cdots,v_n]$ 上整（从而 F 在 $K(v_2,\cdots,v_n)$ 上代数）。如果 $\{v_2,\cdots,v_n\}$ 是代数无关的，由系vi.1.6可知 $r = n-1$，从而证毕。如果不然，在上面推理过程中用 $K[v_2,\cdots,v_n]$ 代替 R，可知对于某些 $w_3,\cdots,w_n \in R$，$K(v_2,\cdots,v_n)$ 在 $K[w_3,\cdots,w_n]$ 上整。根据定理5.6知 R 在 $K[w_3,\cdots,w_n]$ 上整（从而 F 在 $K[w_3,\cdots,w_n]$ 上代数，于是 $r \leqslant n-2$）。如果 $\{w_3,\cdots,w_n\}$ 是代数无关的，我们又完成了证明。否则再重复上面的推导过程。因此，用数学归纳法即给出 R 的 r 元代数无关子集 $\{z_{n-r+1},\cdots,z_n\}$，使得 R 在 $K[z_{n-r+1},\cdots,z_n]$

上整。∎

现在令K为域，F为K的代数封闭扩域。如果$K[x_1,\cdots,x_n]$的一个真理想I是有限生成的，设$I=(g_1,\cdots,g_k)$，则仿射簇$V(I)$显然是由$g_1,\cdots,g_k$的全部公共根$(a_1,\cdots,a_n)\in F^n$所构成的（见习题4）。如果$n=1$，$K[x_1]$为主理想整环，从而$V(I)$显然是非空的。更一般地（并且也有些令人吃惊地，）我们有：

引理7.3 如果F是域K的代数封闭扩域，而I为$K[x_1,\cdots,x_n]$的真理想，则I在F^n中定义的仿射簇非空。

证明 从定理III.2.18和III.2.19可知I包含在某个真素理想P之中，从而$V(P)\subset V(I)$。因此只需对于$K[x_1,\cdots,x_n]$的每个真素理想P证明$V(P)$非空即可。注意$P\cap K=0$（不然的话，令$0\neq a\in P\cap K$，则$1K=a^{-1}a\in P$，这就与P为真理想相矛盾。）

设R为整环$K[x_1,\cdots,x_n]/P$（见定理III.2.16），而$\pi:K[x_1,\cdots,x_n]\to R$为正则满同态。如果用$u_i$代表$\pi(x_i)\in R$，则$R=\pi(K)[u_1,\cdots,u_n]$。此外，由于$K\cap P=0$，可将$K$同构地映到$\pi(K)$之上。特别地，$\pi(K)$为域。根据Noether正则化引理，$R$中存在子集合$\{t_1,\cdots,t_r\}$，使得$\{t_1,\cdots,t_r\}$在$\pi(K)$上代数无关，并且$R$在$S=\pi(K)[t_1,\cdots,t_r]$上整。如果$M$是由$t_1,\cdots,t_r$生成的$S$的理想，则映射$\pi(K)\to S/M,\pi(a)\longmapsto\pi(a)+M$是同构（见定理Vi.1.2）。从而由定理III.2.20可知M为S的极大理想。因此R中存在极大理想N，使得$N\cap S=M$（定理5.9和5.12）。以$\tau:R\to R/N$表示正则满同态。由定理III.2.20可知$\tau(R)=R/N$为域。第二同构定理III.2.12连同上面定义的映射一起给出同构

$$K\cong\pi(K)\cong S/M=S/(N\cap S)\cong(S+N)/N=\tau(S)。$$

$$a\longmapsto\pi(a)\longmapsto\pi(a)+M\longmapsto\pi(a)+N=\tau(\pi(a))。$$

以$\overline{\tau(R)}$表示$\tau(R)$的一个代数闭包。由于R在S上整，从而$\tau(R)$为$\tau(S)$的代数扩域。因此$\overline{\tau(R)}$也是$\tau(S)$的代数闭包(定理V.3.4)。现在F包含K的一个代数闭包$\bar{K}$（练习V.3.7)。由定理V.3.8知道同构$K\cong\tau(S)$可以扩充为同构$\bar{K}\cong\overline{\tau(R)}$。这个同构的逆的限制给出单同构$\sigma$：$\tau(R)\to\bar{K}\subset F$。以$\phi$表示映射$K[x_1,\cdots,x_n]\xrightarrow{\pi}R\xrightarrow{\tau}\tau(R)\xrightarrow{\sigma}F$的合成映射，不难证明$\phi|K=1_K$并且$\phi|P=0$。从而对于每个$f(x_1,\cdots,x_n)\in P\subset K[x_1,\cdots,x_n]$，$f(\phi(x_1),\cdots,\phi(x_n))=\phi(f(x_1,\cdots,x_n))=0$，从而$(\phi(x_1),\cdots,\phi(x_n))$是$P$在$F^n$中的一个零点。因此$V(P)$是非空的。 ∎

命题7.4 （Hilbert零点定理）设F为域K的代数封闭扩域。I为$K[x_1,\cdots,x_n]$的真理想。令$V(I)=\{(a_1,\cdots,a_n)\in F^n\mid g(a_1,\cdots,a_n)=0$（对于每个$g\in I$)}。则

$\mathrm{Rad}I=J(V(I))=\{f\in K[x_1,\cdots,x_n]\mid f(a_1,\cdots,a_n)=0$（对于每个$(a_1,\cdots,a_n)\in V(I)$}

换句话说，$f(a_1,\cdots,a_n)=0$(对于I在F^n中的每个零点$(a_1,\cdots,a_n)$)$\Longleftrightarrow$存在某个$m\geqslant 1$，使得$f^m\in I$。

注记：我们用引理7.3证明此定理。但是由此定理也可推出引理7.3（习题6)，从而两者事实上是等价的。

命题7.4的证明 如果$f\in\mathrm{Rad}I$，则有$m\geqslant 1$，使得$f^m\in I$（定理2.6)。如果$(a_1,\cdots,a_n)$是I在F^n中的零点，则$0=f^m(a_1,\cdots,a_n)=(f(a_1,\cdots,a_n))^m$。但是$F$为域，从而$f(a_1,\cdots,a_n)=0$，即$\mathrm{Rad}_I\subset JV(I)$。

反之，设$f\in JV(I)$。由于$0\in\mathrm{Rad}I$，从而可以假定$f\neq 0$。将$K[x_1,\cdots,x_n]$看作是环$K[x_1,\cdots,x_n,y]$的子环，其中$x_1,\cdots,x_n,y$是$n+1$个

未定元。令L为$K[x_1,\cdots,x_n,y]$中由I和$yf-1_F$生成的非零理想。如果$(a_1,\cdots,a_n,b)$是L在F^{n+1}中的零点，则$(a_1,\cdots,a_n)$必为I在F^n中的零点，但是对于I在F^n中的每个零点$(a_1,\cdots,a_n)$，均有$(yf-1_F)(a_1,\cdots,a_n,b)=bf(a_1,\cdots,a_n)-1_F=-1_F$。因此$L$在$F^{n+1}$中没有零点，即$V(L)$为空集合。根据引理7.3可知$L=K[x_1,\cdots,x_n,y]$。因此

$$1_F=\sum_{i=1}^{t-1}g_if_i+g_t(yf-1_F),$$

其中$f_i\in I(1\leqslant i\leqslant t-1)$并且$g_i\in K[x_1,\cdots,x_n,y]$。定义赋值同态$K[x_1,\cdots,x_n,y]\to K(x_1,\cdots,x_n)$，$x_i\longmapsto x_i(1\leqslant i\leqslant n)$，$y\to f^{-1}=1_K/f(x_1,\cdots,x_n)$（系III5.6），则在域$K(x_1,\cdots,x_n)$中有

$$1_F=\sum_{i=1}^{t-1}g_i(x_1,\cdots,x_n,f^{-1})f_i(x_1,\cdots,x_n).$$

以m表示一个正整数，它大于每个g_i对于y的次数$(1\leqslant i\leqslant t-1)$。则对于每个$i$，均有$f^m(x_1,\cdots,x_n)g_i(x_1,\cdots,x_n,f^{-1})\in K[x_1,\cdots,x_n]$。从而$f^m=f^m1_F=\sum_{i=1}^{t-1}f^m(x_1,\cdots,x_n)g_i(x_1,\cdots,x_n,f^{-1})$，$f_i(x_1,\cdots,x_n)\in I$。即$f\in \mathrm{Rad}I$。于是$JV(I)\subset \mathrm{Rad}_I$。∎

正如本节一开始所提到的，现在可以很容易决定闭的对象（习题1—3）。

在本节的最后，我们试图非正式地建立几何与代数之间的联系，也即是谈一下用代数刻划代数几何的经典方式。设K为域。则每个多项式$f\in K[x_1,\cdots,x_n]$决定一个函数$F^n\to F$，$(a_1,\cdots,a_n)\longmapsto f(a_1,\cdots,a_n)$。如果$V=V(I)$是包含在$F^n$中的仿射簇，则上述函数到$V$的限制叫作是$V$上的正则函数。正则函数$V\longrightarrow F$的全

体形成一个环$\Gamma(V)$，它同构于

$$K[x_1,\cdots,x_n]/J(V(I))$$

（习题10）．这个环叫作是V的坐标环．由于 $I\subset J(V(I))=\mathrm{Rad}I$，从而环$\Gamma(V)$ 没有非零的幂零元素．此外，$\Gamma(V)$ 是K上有限生成代数（因为$K[x_1,\cdots,x_n]$和理想$J(V(I))$ 均是K上有限生成代数，见第IV.7节）．反过来，可以证明：有限生成 K-代数如果没有非零的幂零元素，则必是某个仿射簇的坐标环．因此，在仿射簇和一类特殊的交换环之间存在着一一对应关系．适当定义态射之后，仿射簇形成一个范畴，而上述那一类特殊的交换环也形成一个范畴，并且上面所显示的一一对应事实上是范畴的“等价”．因此，关于仿射簇的命题均等价于交换代数的某个命题．进一步可参见W. Fulton[53]和I. G. MacDonald[55]．

习　题

注：F永远是域K的代数封闭域，而J，V和F^n如前所示

1．F^n的子集合Y是闭集（即$V(J(Y))=Y$）$\Longleftrightarrow Y$为由$K[x_1,\cdots,x_n]$中某个子集合S所决定的仿射K-簇．

2．$K[x_1,\cdots,x_n]$的子集合S是闭的（即$J(V(S))=S$）$\Longleftrightarrow S$为根式理想（即S为理想并且$S=\mathrm{Rad}S$）．

3．在F^n中仿射K-簇集合与$K[x_1,\cdots,x_n]$的根式理想集合之间存在着反序（对于包含序）的一一对应[见习题1和2]．

4．F^n中每个仿射K-簇均有形式$V(S)$，其中S为$K[x_1,\cdots,x_n]$的有限集合．[提示：定理1.9，4.9和习题3]．

5．如果$V_1\supset V_2\supset\cdots$是$F^n$中仿射$K$-簇的降链，则有某个$m$，使得$V_m=V_{m+1}=\cdots$[提示：定理4.9和习题3.]

6. 求证Hilbert零点定理可以推出引理7.3.

7. 如果$I_1,\cdots,I_k$为$K[x_1,\cdots,x_n]$中理想，则$V(I_1\cap I_2\cap\cdots\cap I_k)=V(I_1)\cup V(I_2)\cup\cdots\cup V(I_k)$，$V(I_1I_2\cdots I_k)=V(I_1)\cap V(I_2)\cap\cdots\cap V(I_k)$.

8. F^n中一个K-簇V叫作不可约的，是指$V=W_1\cup W_2$，其中W_1和W_2均为F^n中的K-仿射簇，则必然$V=W_1$或者$V=W_2$.

(a) 求证V不可约$\Longleftrightarrow J(V)$为$K[x_1,\cdots,x_n]$中的素理想.

(b) 令$F=\mathbf{C}$而$S=\{x_1^2-2x_2^2\}$.则$V(S)$为不可约$\mathbf{Q}$-簇，但是作为$\mathbf{R}$-簇则不是不可约的.

9. F^n中每个非空K-簇均可以唯一地写成F^n中不可约K-仿射簇之有限并$V_1\cup V_2\cup\cdots\cup V_k$，使得当$i\neq j$时$V_j\not\subset V_i$.（习题8）.

10. K-仿射簇$V(I)$的坐标环同构于$K[x_1,\cdots,x_n]/J(V(I))$.

第IX章　环的结构

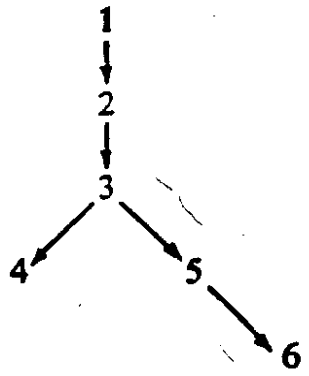
本章的第一部分讲环的一般结构理论。尽管这里引进的概念和技巧已经有了非常广泛的应用，但是完整的结构定理只适用于一定类型的环。决定这样一类环的基本方法可以形象地描述如下：我们挑选出一个“令人讨厌”的性质 P，使得该性质满足某些条件。比如说，每个环均有一个理想对于这个性质是极大的，这个理想称作该环的 P-根。然后我们试图去发现 P- 根为零的这类环的结构定理.为了得到实际上较强的结构定理,往往还需要再加一些假定（例如适当的链条件等）。这些思想在第 1 节和第 2 节的引言中作了详细的讨论。在开始仔细学习本章之前，读者应当很好地阅读这两部分讨论。

我们要研究两个不同的根：Jacobson 根（第 2 节）和素根（第 4 节）。在第 3 节中,我们对于左Artin 半单环（即Jacobson根为零的左 Artin 环）得到十分深刻而有用的结构定理。第 4 节讨论Goldie 定理，它刻划了左 Noether 半素环（即素根为零的左Noether环）。所有这些结构定理的基本构件是体上向量空间的自同态环和它的某些“稠”子环（第 1 节）。

本章的后两节处理含幺交换环上的代数，将Jacobson 根及其有关的概念和结果移植到代数上（第 5 节）。在第6节中研究除法代数。

本章中经常不断出现的一个主题是环的结构与此环上模的结构之间的密切联系。利用模来研究环，使我们具有了新的眼力和深刻的定理。

本章各节之间的依赖关系如下图所示。其中有许多讨论依赖于第VIII.1节（链条件）。



1. 单环和本原环

在这一节我们要研究一些环，它们是环的结构理论中的基本构件。

首先让我们回忆某些事实。这些事实是本章大部分内容的诱发因素

(i) 如果V是体D上的向量空间，则$\mathrm{Hom}_D(V,V)$是环（习题IV.1.7)。称作V的自同态环。

(ii) 体上有限维向量空间的自同态环同构于一个（可能与前不同的）体上的$n\times n$阶方阵组成的全阵环（定理VII.1.4)。

(iii) 如果D是体，则$\mathrm{Mat}_n D$是单环（即没有非平凡的真理想。习题III.2.9)，并且它同时是左和右Artin环(系VIII.1.12)。

从而由(ii)可知，体上有限维向量空间的自同态环是Artin单环。

(iv) 体上无限维向量空间的自同态环既不是单环也不是Artin环，但是这种环在后面的意义下是本原环。

矩阵环和体上向量空间的自同态环是极为有用的数学概念，它们自然地出现在许多完全不同的数学课题中。所以，似乎理应采用这样的环，或者至少是与它们很相象的环作为结构理论的基石，然后试图用这些基本的环去描述任意环。

基于此，我们挑选出向量空间V的自同态环的两个基本性质：单性（定义1.1）和本原性(定义1.5)作为瞄准对象。如前所述，这两个概念大致上分别对应着V的维数是有限的和无限的这两种情形。在本节中我们分析单环和本原环，证明在一些重要情形下它们与自同态环一致。而在另一些情形下，它们在某种意义下很接近于自同态环。

更确切地说，可以证明，每个本原环R均同构于某个体D上一个向量空间V的自同态环的一个特别类型的子环（叫作稠子环）(定理1.12)。而R为左Artin环的充要条件是$\dim_D V$有限（定理1.9)。在后面这个经典情形下，单环和本原环是一致的，并且事实上同构于V的整个自同态环（定理1.14)。进而，在这种情形下，$\dim_D V$是唯一确定的，而V也决定到同构（命题1.17)。这些结果注定了单性和本原性成为基本概念。

正如本章引言中所提到的，模在环论中起着关键性作用。所以我们从一开始就同时对于环和模定义单性并且同时阐述它们的基本性质。

定义1.1 环R上的（左）模A叫作单的（或者叫作不可约的)，是指$RA\neq 0$，并且A没有非零真子模。环R叫作单的，是指

$R^2 \neq 0$并且R没有非零真(双侧)理想。

注记：(i) 每个单模（单环）均不为零。

(ii) 含幺环上的每个单模都是幺作用模（习题Iv.1.17)。对于含幺环R上的幺作用模A，$RA \neq 0$。因此A为单模的充要条件是A没有非零真子模。

(iii) 每个单模A均是循环模。事实上，对于每个非零元素$a \in A$，$A = Ra$。〔证明：$Ra(a \in A)$和$B = \{c \in A \mid Rc = 0\}$均是$A$的子模，由于单性可知它们或者为0或者为$A$。但是$RA \neq 0$，从而$B \neq A$。于是$B = 0$。于是对于每个非零元素$a \in A$，$Ra = A$。〕另一方面，循环模不一定是单模（例如循环$Z$-模$Z_6$)。

(iv) 关于群，模和环的“单性”定义可以放到一个更一般的定义方式中，它可以粗糙地叙述为：假设一个代数对象C在某种合理的意义下是非平凡的（例如$RA \neq 0$或者$R^2 \neq 0$)，则称C是单的，是指值域为C的每个同态的核均是0或者C。这里关键在于，不存在不平凡的核这件事，等价于不存在群的非零真正规子群，模的非零真子模，或者是环的非零真理想。

例 每个体D都是单环或者单D-模（见定理III.2.2之前的注记)。

例 设D为体而$R = \mathrm{Mat}_n D (n > 1)$。对于每个$k (1 \leqslant k \leqslant n)$，$I_k = \{(a_{ij}) \in R \mid a_{ij} = 0$当$j \neq k$时$\}$是单左$R$-模（见系VIII.1.12的证明。)

例 上例表明，当$n > 1$时，$\mathrm{Mat}_n D$（D为体）不是它自身上的单左模。但是由习题III.2.9可知$\mathrm{Mat}_n D$ $(n \geqslant 1)$是单环。所以由定理VII.1.4可知，体上有限维向量空间的自同态环均是单环。

例 环R的左理想I叫作极小左理想，是指$I \neq 0$并且对于每个

左理想J，若$0 \subset J \subset I$，则必然$J=0$或者$J=I$。设I是R的左理想并且$RI \neq 0$，则I为单左R-模的充要条件是I为极小左理想。

例 如果F是特征零域而R是多项式集合$F[x,y]$的加法群。定义$xy=yx+1$，$ax=xa$，$ay=ya$ $(a \in F)$，然后由分配律给出R中乘法。则R由此而成为环，并且是单环。它没有零因子，但它也不是体(习题1)。

设$A=Ra$是循环R-模，由$r \longmapsto ra$定义的映射θ：$R \to A$是R-模满同态，其核I是R的左理想（子模）(定理IV.1.5)。根据第一同构定理IV.17，R/I同构于A。又根据定理IV.1.10，R/I的每个子模都有形式J/I，其中J为R中包含I的左理想。因此R/I（从而A）没有非零真子模的充要条件是I为R的极大左理想。根据上面的注记 (iii)，每个单R-模都是循环的，从而每个单R-模均同构于R/I，其中I是某个极大左理想。反之，如果I是R的极大左理想，只要$R(R/I) \neq 0$，则R/I为单R-模。为了保证$R(R/I) \neq 0$我们引入下面的定义：

定义1.2 环R中的左理想I叫作正规的，是指存在$e \in R$，使得对于每个$r \in R$，$r-re \in I$。类似的，一个右理想J叫作正规的，是指存在$e \in R$，使得对于每个$r \in R$，$r-er \in J$。

注记：含幺环R中每个左理想均是正规的(令$e=1_R$)。

定理1.3 环R上左模A是单模的充要条件是A同构于R/I，其中I是某个正规极大左理想。

注记：如果R有1，则此定理是上面讨论的直接推论。如果将所有“左”均改为“右”，则定理1.3仍然正确。

定理1.3的证明 从定义1.2前面的讨论可知，假如A是单模，

则 $A=Ra\cong R/I$，其中极大理想I为θ之核。由于 $A=Ra$，从而存在$e\in R$，使得$a=ea$，于是对每个$r\in R$，$ra=rea$，即$(r-re)a=0$，于是$r-re\in \mathrm{Ker}\theta=I$。因此$I$是正规的。

反之，设I是 R的正规极大左理想，并且 $A\cong R/I$。按照定义1.2前面的讨论，只需证明$R(R/I)\neq 0$即可。如果$R(R/I)=0$，则对于每个$r\in R$，$r(e+I)=I$，从而$re\in I$。由于$r-re\in I$，因此$r\in I$，即$R=I$，而这与I的极大性相矛盾。∎

我们已经给出关于单性的所需事实。现在转而讨论本原性。为了定义本原性我们需要：

定理1.4 设 B 为环 R 上左模A的子集合。则$\mathscr{A}(B)=\{r\in R \mid rb=0,\ \forall b\in B\}$ 是R的左理想。又如果B是A的子模，则$\mathscr{A}(B)$是 R的理想。

$\mathscr{A}(B)$叫作B 的（左）零化子。可以类似地定义右模的右零化子。

定理1.4证明概要 容易验证$\mathscr{A}(B)$是左理想。设 B 为子模。如果$r\in R$并且$\in \mathscr{A}s(B)$，则对于每个$b\in B$，$(sr)b=s(rb)=0$（因为$rb\in B$）。从而$sr\in \mathscr{A}(B)$，于是$\mathscr{A}(B)$也是右理想。∎

定义1.5 （左）模 A叫作忠实的，是指它的（左）零化子$\mathscr{A}(A)$是 0。环 R叫作（左）本原的，是指存在着忠实的单左R-模。

类似地可以定义右本原环。存在着不是左本原环的右本原环（见 G. Bergman〔58〕）。以后“本原”将永远指“左本原”。但是所证明的关于左本原环的全部结果，对于右本原环也是正确的。

例 设V是体 D上（可能无限维的）向量空间，R是V的自同

态环$\mathrm{Hom}_D(V,V)$。注意V是左R-模，其中$\theta v=\theta(v)$（对于$v\in V$，$\theta\in R$）（习题IV.1.7）。如果u为V中非零向量，则V有包含u的一组基（定理IV.2.4）。如果$v\in V$，则存在$\theta_v\in R$，使得$\theta_v u=v$（只要定义$\theta_v(u)=v$，而对其余基元素w定义$\theta_v(w)=0$即可。因为由定理IV.2.1和IV.2.4可知$\theta_v\in R$）。所以，对于每个非零元素$u\in V$，$Ru=V$，即V没有非零真R-子模。由于R有1，从而$RV\neq 0$。从而V为单R-模。如果$\theta V=0$（$\theta\in R$），则$\theta=0$，从而$\mathscr{A}(V)=0$，即V为忠实R-模。因此R是本原的。如果V是D上的有限维向量空间，由习题III.2.9和定理VII.1.4可知R是单环。但是当V在D上是无限维的时候R不是单环，因为集合$\{\theta\in R\mid \mathrm{Im}\theta$为$V$的有限维子空间$\}$是$R$的真理想(习题3)。

下面两个结果提供出本原环的又一些例子。

命题1.6 含幺单环R是本原的。

证明 按照定理III.2.18，R包括极大左理想I。由于R有1_R，从而I是正规的，因此从定理1.3可知R/I是单R-模。因为$\mathscr{A}(R/I)$是R的理想并且不包含1_R，由单性可知$\mathscr{A}(R/I)=0$。因此R/I是忠实的。∎

命题1.7 交换环R是本原的当且仅当R是域。

证明 从命题1.6可知域是本原的。反之，设A是一个忠实单左R-模。则$A\cong R/I$，其中I是R的某个正规极大左理想。由于R是交换环，I事实上是一个理想，并且$I\subset\mathscr{A}(R/I)=\mathscr{A}(A)=0$。因为$I=0$是正规的，因此存在$e\in R$，使得对每个$r\in R$，$r=re(=er)$。因此$R$是含幺交换环。由于$I=0$是极大理想，根据系III.2.21可知$R$是域。∎

为了刻划非交换的本原环，我们需要“稠”的概念。

定义1.8 设V是体D上的（左）向量空间。自同态环$\mathrm{Hom}_D(V,V)$的子环R叫作V的自同态稠环（或者叫作$\mathrm{Hom}_D(V,V)$的稠子环），是指对于每个正整数n，V的每个线性无关子集合$\{u_1,\cdots,u_n\}$和V的任意子集合$\{v_1,\cdots,v_n\}$，均存在$\theta\in R$，使得$\theta(u_i)=v_i(1\leqslant i\leqslant n)$。

例 $\mathrm{Hom}_D(V,V)$是它自身的稠子环。因为如果$\{u_1,\cdots,u_n\}$是V的线性无关子集合，则根据定理IV.2.4.存在V的一组基$U\supset\{u_1,\cdots,u_n\}$。如果$v_1,\cdots,v_n\in V$，根据定理IV.2.1和IV.2.4，由$\theta(u_i)=v_i$和$\theta(u)=0$（对于$u\in U-\{u_1,\cdots,u_n\}$）定义的映射$\theta$：$V\to V$是$\mathrm{Hom}_D(V,V)$中的元素。在有限维的情形下，$\mathrm{Hom}_D(V,V)$的稠子环只有它自身，这从下面的定理可以看出。

定理1.9 设R是体D上向量空间V的自同态稠环。则R为左（右）Artin环的充要条件是$\dim_D V$有限。并且在这种情形下$R=\mathrm{Hom}_D(V,V)$。

证明 如果R是左Artin环并且$\dim_D V$无限，则V中存在一个无限的线性无关子集合$\{u_1,u_2,\cdots\}$，从习题IV.1.7可知V是左$\mathrm{Hom}_D(V,V)$-模，因此是左R-模。对于每个n。以I_n表示集合$\{u_1,\cdots,u_n\}$在R中的左零化子。从定理1.4可知$I_1\supset I_2\supset\cdots$是$R$的左理想下降链。设$w$是$V$中任一非零元素。由于对于每个$n$，$\{u_1,\cdots,u_{n+1}\}$是线性无关的，并且$R$是稠子环，从而存在$\theta\in R$使得

$$\theta u_i=0\ (1\leqslant i\leqslant n)\ \text{而}\theta u_{n+1}=w\neq 0.$$

于是$\theta\in I_n$但是$\theta\notin I_{n+1}$。因此$I_1\supsetneq I_2\supsetneq\cdots$是真下降链，这就导致矛盾。于是$\dim_D V$有限。

反之，如果$\dim_D V$有限，则V有有限基$\{v_1,\cdots,v_m\}$。如果f是$\mathrm{Hom}_D(V,V)$中任一元素，由定理IV.2.1和IV.2.4，f由它在v_1，…，v_m上的作用所完全决定。因为R是稠子环，因此存在$\theta\in R$使得

$$\theta(v_i)=f(v_i)\quad(1\leqslant i\leqslant m)$$

于是$f=\theta\in R$。因此$\mathrm{Hom}_D(V,V)=R$。而由定理VII.1.4和系VIII.1.12可知$\mathrm{Hom}_D(V,V)$是Artin环。∎

为了证明每个本原环均同构于适当向量空间的一个自同态稠环，我们需要两个引理。

引理1.10 (Schur) 设A为环R上的单模而B为任一R-模。

(i) 每个非零R-模同态f：$A\to B$都是单同态。

(ii) 每个非零R-模同态g：$B\to A$都是满同态。

(iii) 自同态环$D=\mathrm{Hom}_R(A,A)$是体。

证明 (i) $\mathrm{Ker}f$为A的子模。由于$f\neq 0$从而$\mathrm{Ker}f\neq A$。由单性便知$\mathrm{Ker}f=0$。

(ii) 由于$g\neq 0$，$\mathrm{Im}g$是A的非零子模，由单性即知$\mathrm{Im}g=A$。

(iii) 如果$f\in D$并且$f\neq 0$，由(i)和(ii)可知f是同构。因此f有双侧逆$f^{-1}\in\mathrm{Hom}_R(A,A)=D$（见定义IV.1.2后面的一段）。从而$D$中每个非零元素都是单位，即$D$是体。∎

注记：如果A是单R-模，则A是体$\mathrm{Hom}_R(A,A)$上的向量空间，其中$fa=f(a)$（习题IV.1.7和引理1.10）。

引理1.11 设A是环R上的单模。将A看作体$D=\mathrm{Hom}_R(A,A)$上的向量空间。如果V是D-向量空间A的有限维D-子空间，并且$a\in A-V$，则存在$r\in R$，使得$ra\neq 0$并且$rV=0$。

证明 对于$n=\dim_D V$归纳. 如果$n=0$, 则$V=0$而$a\neq 0$. 因为A是单模, 由定义1.1后面的注记(iii) 可知$A=Ra$. 从而存在$r\in R$使得$ra=a\neq 0$,而 $rV=r0=0$. 假设$\dim_D V=n>0$而定理对于维数小于n的情形都是对的. 设$\{u_1,\cdots,u_{n-1},u\}$是V的一组D-基, 而令W是由$\{u_1,\cdots,u_{n-1}\}$张成的$(n-1)$维D-子空间 (当$n=1$时取$W=0$). 则 $V=W\oplus Du$ (向量空间直和). 现在W可能不是A 的R-子模. 但是无论如何, 由定理1.4知W在 R 中的左零化子 $I=\mathscr{A}(W)$是R的左理想.因此Iu是A的R-子模 (习题IV.1.3). 由于$u\in A-W$, 由归纳假设导致存在$r\in R$, 使得$ru\neq 0$而 $rW=0$ (即$r\in I=\mathscr{A}(W)$). 从而 $0\neq ru\in Iu$. 因此 $Iu\neq 0$. 由单性可 知 $A=Iu$.

〔注记: 将上面的归纳推理反过来, 便可证明: 若 $v\in A$, 并且对于每个$r\in I$均有$rv=0$, 则$v\in W$.〕

我们必须寻求$r\in R$使得$ra\neq 0$同时$rV=0$. 如果没有这样的r存在, 则我们可如下定义一个映射θ: $A\to A$: 对于 $ru\in Iu=A$, 令$(ru)=ra\in A$. 我们断言 θ 是可定义的. 这是因为: 如果 $r_1u=r_2u$ $(r_i\in I=\mathscr{A}(W))$, 则$(r_1-r_2)u=0$, 从而 $(r_1-r_2)V=(r_1-r_2)(W\oplus Du)=0$. 从而由假设可知$(r_1-r_2)a=0$. 因此 $\theta(r_1u)=r_1a=r_2a=\theta(r_2u)$. 不难证明 $\theta\in \mathrm{Hom}_R(A,A)=D$. 于是对于每个$r\in I$,

$$0=\theta(ru)-ra=r\theta(u)-ra=r(\theta(u)-a).$$

因此, 从上面方括号中的注记可知$\theta(u)-a\in W$. 从而

$$a=\theta(u)-(\theta(u)-a)\in Du+W=V.$$

而这与$a\notin V$这一事实相矛盾. 因此存在$r\in R$, 使得$ra\neq 0$同时 $rV=0$. ∎

定理1.12 (Jacobson密度定理) 设R是本原环而A是忠实单R-模。将A看作是体$D=\mathrm{Hom}_R(A,A)$上的向量空间。则R同构于D-向量空间A的一个自同态稠环。

注记：定理1.12的逆也是对的，事实上还可以具有强得多的形式(习题4)。

定理1.12的证明 对于每个$r\in R$，由$a_r(a)=ra$给出映射a_r：$A\to A$。易知α_r是A的一个D-自同态，即$\alpha_r\in\mathrm{Hom}_D(A,A)$。进而，对于所有$r$，$s\in R$，我们有

$$\alpha_{(r+s)}=\alpha_r+\alpha_s,\quad \alpha_{rs}=\alpha_r\alpha_s.$$

从而由$\alpha(r)=\alpha_r$定义的映射α：$R\to\mathrm{Hom}_D(A,A)$是环同态。由于A为忠实R-模，从而$\alpha_r=0\Longleftrightarrow r\in(A)=0$。因此$\alpha$是单射，于是$R$同构于$\mathrm{Hom}_D(A,A)$的子环$\mathrm{Im}\alpha$。

为了完成证明，我们还要证$\mathrm{Im}\alpha$是$\mathrm{Hom}_D(A,A)$的稠子环。给了A的一个D-线性无关子集合$U=\{u_1,\cdots,u_n\}$和A的任意子集合$\{v_1,\cdots,v_n\}$。我们要寻求$\alpha_r\in\mathrm{Im}\alpha$，使得$\alpha_r(u_i)=v_i$ $(1\leqslant i\leqslant n)$。对于每个$i$，以$V_i$表示由$\{u_1,\cdots,u_{i-1},u_{i+1},\cdots,u_n\}$张成的$A$之$D$-子空间。由于$U$是$D$-线性无关的，$u_i\notin V_i$。因此由引理1.11可知存在$r_i\in R$，使得$r_iu_i\neq 0$，并且$r_iV_i=0$。再将引理1.11用于零子空间和非零元素$r_iu_i$：于是存在$s_i\in R$，使得$s_ir_iu_i\neq 0$而$s_i0=0$。由于$s_ir_iu_i\neq 0$，可知$A$的$R$-子模$Rr_iu_i\neq 0$，由单性便知$Rr_iu_i=A$。因此存在$t_i\in R$，使得$t_ir_iu_i=v_i$。令

$$r=t_1r_1+t_2r_2+\cdots+t_nr_n\in R.$$

注意当$i\neq j$时$u_i\in V_j$，因此$t_ir_ju_i\in t_j(r_jV_j)=t_j0=0$。从而对于每个$1\leqslant i\leqslant n$，

$$\alpha_r(u_i)=(t_1r_1+\cdots+t_nr_n)u_i=t_ir_iu_i=v_i.$$

因此$\mathrm{Im}\alpha$是D-向量空间A的一个自同态稠环。∎

注记：在证明定理 1.12 的时候，只有证α是单射的时候用到了A的忠实性。因此从这个证明可知，每个环如果有单模A，则它必有一个同态象，使这个同态象是D-向量空间A的自同态稠环。

系1.13 如果R是本原环，则存在某个体D，使得或者R同构于有限维D-向量空间的自同态环，或者对每个正整数m，均存在R的一个子环R_m和环的满同态 $R_m \to \mathrm{Hom}_D(V_m, V_m)$，其中$V_m$是一个$m$维$D$-向量空间。

注记：通过定理 VII.1.4 可以将这个系用体上矩阵环的语言表达出来。

系1.13的证明概要 采用定理1.12中的符号，

$$\alpha: R \to \mathrm{Hom}_D(A, A)$$

是单同态，使得$R \cong \mathrm{Im}\alpha$并且$\mathrm{Im}\alpha$为$\mathrm{Hom}D(A, A)$中的稠子环。如果$\dim_D A = n$有限，由定理1.9可知$\mathrm{Im}\alpha = \mathrm{Hom}_D(A, A)$。如果$\dim_D A$无限，而$\{u_1, u_2 \cdots\}$是无限线性无关集合，令$V_m$是由$\{u_1, \cdots, u_m\}$张成的$A$之$m$维$D$-子空间。易知$R_m = \{r \in R \mid rV_m \subset V_m\}$是$R$的子环。利用$R \cong \mathrm{Im}\alpha$在$\mathrm{Hom}_D(A, A)$中的稠性可以证明，由$r \longmapsto \alpha_r | V_m$定义的映射$R_m \longrightarrow \mathrm{Hom}_D(V_m, V_m)$是环的满同态。∎

定理1.14 (Wedderburn-Artin) 左Artin 环R的下列四个条件彼此等价：

(i) R为单环；

(ii) R为本原环；

(iii) R同构于体D上的一个非零有限维向量空间的自同态环；

(iv) 存在某个正整数n，使得R同构于体上的$n\times n$全阵环。

证明 (i)$\Longrightarrow$(ii)：首先注意，$I=\{r\in R\mid Rr=0\}$是R的理想，从而$I=R$或者$I=0$。由于$R^2\neq 0$，因此必然$I=0$。由于R是左Artin环，R的非零左理想集合包含有极小左理想J。J没有非零真R-子模(因为J的R-子模是R的左理想)。我们断言：J在R中的左零化子$\mathscr{A}(J)$为零。因为若不然，由单性便有$\mathscr{A}(J)=R$。并且对于每个非零元素$u\in J$，$Ru=0$。从而每个这种非零元素u均包含在$I=0$中，这就导致矛盾。因此$\mathscr{A}(J)=0$而$RJ\neq 0$。从而J为忠实单R-模，即R是本原的。

(ii)$\Longrightarrow$(iii)：根据定理1.12，R同构于体D上向量空间V的自同态稠环T。由于R是左Artin环，从定理1.9便知$R\cong T=\mathrm{Hom}_D(V,V)$

(iii)$\Longrightarrow$(iv)：定理vii.1.4。

(iv)$\Longrightarrow$(i)：习题III.2.9。∎

在本节的最后，我们来证明：对于单左Artin环R，定理1.14中的整数$\dim_D V$和n都是唯一确定的，并且定理1.14(iii)和(iv)中的体不计同构也是唯一确定的。为此我们需要两个引理。

引理1.15 设V是体D上有限维向量空间。如果A和B都是自同态环$R=\mathrm{Hom}_D(V,V)$上的忠实单模，则A和B是同构的R-模。

证明 由定理VII.1.4，VIII.1.4和系VIII.1.12可知，环R包含(非零)极小左理想I。因为A是忠实的，存在$a\in A$，使得$Ia\neq 0$。因此Ia为A的非零子模(习题IV.1.3)，从而由单性即知$Ia=A$。由$i\longmapsto ia$给出的映射θ：$I\longrightarrow Ia=A$是非零R-模满同态。由引理1.10可知θ是同构。类似地有$I\cong B$。∎

引理1.16 设V为体 D 上非零向量空间，而 R 是自同态环 $\mathrm{Hom}_D(V,V)$。如果g：$V\to V$是加法群同态，使得对于每个 $r\in R$ 均有$gr=rg$，则存在$d\in D$，使得对于每个$v\in V$均有$g(v)=dv$。

证明 设u是V的非零元素。我们断言：u和$g(u)$ 在D上线性相关。如果$\dim_D V=1$，则这是显然的。如果 $\dim_D V\geqslant 2$ 而 $\{u, g(u)\}$是线性无关的，由于R在R中稠(定义1.8后面的例子)，从而存在$r\in R$，使得$r(u)=0$而$r(g(u))\neq 0$。但是由假设我们有

$$r(g(u))=rg(u)=gr(u)=g(r(u))=g(0)=0,$$

这就导致矛盾。因此存在$d\in D$，使得 $g(u)=du$。如果$v\in V$，由稠性可知存在$s\in R$，使得$s(u)=v$。由于 $s\in R=\mathrm{Hom}_D(V, V)$，从而$g(v)=g(s(u))=sg(u)=s(du)=ds(u)=dv$。∎

命题1.17 对于 $i=1$，2，以V_i表示体D_i上有限维（维数为 n_i）向量空间。

(i) 如果存在环同构$\mathrm{Hom}_{D_1}(V_1, V_1)\cong\mathrm{Hom}_{D_2}(V_2, V_2)$，则$\dim_{D_1}V_1=\dim_{D_2}V_2$并且$D_1$同构于$D_2$，

(ii) 如果有环同构$\mathrm{Mat}_{n_1}D_1\cong\mathrm{Mat}_{n_2}D_2$，则$n_1=n_2$ 并且D_1同构于D_2。

证明概要 (i) 定义1.5后面的例子表明，对于 $i=1$，2，v_i是忠实单$\mathrm{Hom}_{D_i}(V_i, V_i)$ 一模。令$R=\mathrm{Hom}_{D_1}(V_1, V_1)$，而

$$\sigma: R\to\mathrm{Hom}_{D_1}(V_2, V_2)$$

是同构，通过σ拉回到R，可使V_2 为忠实单R-模（即$rv=\sigma(r)V$，对于$r\in R$，$v\in V_2$)。由引理1.15可知存在R-模同构ϕ：$V_1\to V_2$。对于$v\in V_1$和$f\in R$我们有

$$\phi[f(v)]=f\phi(v)=(\sigma f)[\phi(v)],$$

从而作为加法群同态$V_2\to V_2$，我们有

$\phi f\phi^{-1}=\sigma(f)$。

对于每个 $d\in D_i$，令α_d：$V_i\to V_i$是由$x\longmapsto dx$定义的加法群同态。显然$\alpha_d=0\Longleftrightarrow d=0$。对于每个 $f\in R=\mathrm{Hom}_{D_1}(V_1, V_1)$ 和每个 $d\in D_1$，均有$f\alpha_d=\alpha_d f$。从而

$$[\phi\alpha_d\phi^{-1}](\sigma f)=\phi\alpha_d\phi^{-1}\phi f\phi^{-1}=\phi\alpha_d f\phi^{-1}$$
$$=\phi f\alpha_d\phi^{-1}=\phi f\phi^{-1}\phi\alpha_d\phi^{-1}=(\sigma f)[\phi\alpha_d\phi^{-1}]。$$

由于σ为满射，从引理1.16（取$V=V_2$，$g=\phi\alpha_d\phi^{-1}$）导致存在$d^*\in D_2$，使得$\phi\alpha_d\phi^{-1}=\alpha d^*$。令$\tau$：$D_1\to D_2$是由$\tau(d)=d^*$给出的映射，则对于每个$d\in D$，

$$\phi\alpha_d\phi^{-1}=\alpha_{\tau(d)}$$

易知τ是环的单同态。将上面推理中D_1和D_2的位置倒转过来（同时分别以ϕ^{-1}，σ^{-1}代替ϕ，σ），可知对于每个$k\in D_2$，给出元素$d\in D$，使得

$$\phi^{-1}\alpha_k\phi=\alpha_d:\ V_1\to V_1。$$

于是$\alpha_k=\phi\alpha_d\phi^{-1}=\alpha_{\tau(d)}$。从而$k=\tau(d)$，即$\tau$是满同态。因此$\tau$为同构。进而，对于每个$d\in D_1$和$v\in V_1$，我们有

$$\phi(dv)=\phi\alpha_d(v)=\alpha_{\tau(d)}\phi(v)=\tau(d)\phi(v)。$$

利用这一事实可以证明：$\{u_1, \cdots, u_k\}$在V_1中是D_1-线性无关的$\Longleftrightarrow\{\phi(u_1), \cdots, \phi(u_k)\}$在$V_2$中是$D_2$-线性无关的。由此得出$\dim_{D_1}V_1=\dim_{D_2}V_2$。

(ii) 利用(i)，习题III.1.17(e)和定理VII.1.4。

习　题

1. 设F是特征零域，$R=F[x, y]$是二个未定元的多项式加法群。由$ax=xa$，$ay=ya(a\in F)$，x与y之积$=xy$，y与x之积$=xy+1$，以及分配律

定义出R上乘法.则

(a) R是环.

(b) $yx^k = x^k y + kx^{k-1}$, $y^k x = xy^k + ky^{k-1}$.

(c) R是单环.[提示：设f为R的理想I 中的非零元素. 则或者f中没有包含y的项，或者 $g = xf - fx$为I中非零元素， 并且g对于y的次数比f对于y的次数要低. 对于后一种情形，再考虑$xg - gx$，从而总可以求出一个非零元素$h \in I$，使得h不包含y. 如果h不为常数，再考虑 $hy - yh$.从而经过有限步之后，便得到I中一个非零的常数元素. 于是$I = R$.]

(d) R没有零因子.

(e) R不是体.

2. (a) 如果 A 为R-模，则通过 $(r + \mathscr{A}(A))a = ra (a \in A)$ 可使 A 为$R/\mathscr{A}(A)$-模.

(b) 如果A为单左R-模，则$R/\mathscr{A}(A)$为本原环.

3. 设V为体D上无限维向量空间.

(a) 如果$F = \{\theta \in \mathrm{Hom}_D(V, V) \mid \mathrm{Im}\theta$为有限维$\}$，则$F$是$\mathrm{Hom}_D(V, V)$的非零真理想，从而$\mathrm{Hom}_D(V, V)$不单.

(b) F自己是单环.

(c) F包含在$\mathrm{Hom}_D(V, V)$的每个非零理想中.

(d) $\mathrm{Hom}_D(V, V)$不是(左)Artin环.

4. 设V是体D上的向量空间. $\mathrm{Hom}_D(V, V)$ 的子环R叫做n重可迁的，是指对于每个$k (1 \leqslant k \leqslant n)$，$V$的每个线性无关子集合$\{u_1, \cdots, u_k\}$以及$V$的任一子集合 $\{v_1, \cdots, v_k\}$，均存在 $\theta \in R$，使得 $\theta(u_i) = v_i$ $(1 \leqslant i \leqslant k)$.

(a) 如果R是1重可迁的，则R为本原环.[提示：考查定义1.5后面的例子.]

(b) 如果R是2重可迁的，则R在$\mathrm{Hom}_D(V, V)$ 中稠.[提示：利用(a)证明R是$\mathrm{Hom}_\Delta(V, V)$的稠子环，其中$\Delta = \mathrm{Hom}_R(V, V)$. 利用双可迁性证明$\Delta = \{\beta_d \mid d \in D\}$,其中$\beta_d$: $V \to V$ 由$x \longmapsto dx$定义.

于是$\mathrm{Hom}_{\Delta}(V, V) = \mathrm{Hom}_{D}(V, V)$.]

5. 如果R为本原环，并且$a(ab-ba)=(ab-ba)a$($\forall a, b\in R$)，则R为体.
[提示：证明R同构于某个体D上一个向量空间V的自同态稠环，并且$\dim_{D}V=1$，从而$R\cong D$.]

6. 如果R为含幺本原环，而$e\in R$，使得$e^2=e\neq 0$，则
(a) eRe为R的子环，并且e是eRe的幺元素.
(b) eRe为本原环.[提示：如果R同构于体D上向量空间的一个自同态稠环，则Ve为D-向量空间，并且eRe同构于Ve的一个自同态稠环.]

7. 如果R是向量空间V的一个自同态稠环，而K为R的非零理想，则K也是V的一个自同态稠环.

2. Jacobson根

在本节中我们定义Jacobson根（定理2.3）同时讨论它的基本性质（定理 2.12—2.16）.考查单环，本原环和半单环之间的关系（定理2.10），并且给出许多例子.

在对于环的结构作进一步研究之前，我们综述一下我们要使用的一般技巧.目前，很少有希望对所有的环作同构分类.所以我们试图发现某些类型的环,对于它们可以得到满意的结构定理.决定这样类型的环的经典方法是：挑选出环的某种“令人讨厌”的性质，或者某种“不希望有”的性质，然后只研究不具有这种性质的那些环.为了使这种方法实际上可以执行，我们还需要再加上某些假定.

假设P是环的某种性质.我们称理想（或者环）I是一个P-理想（或者P-环），是指I有性质P.假设

(i) P-环的同态还是P-环；

(ii) 每个环R（或者至少某个指定类$\mathscr{C}$中的每个环）都包含一个P-理想$P(R)$，使得$P(R)$包含R的所有其他P-理想（$P(R)$叫作是R的P-根）；

(iii) 商环$R/P(R)$的P-根为零；

(iv) 环$P(R)$的P-根为$P(R)$。

满足(i)—(iv)的性质P称作根性质。

可以把P-根看作是衡量一个给定的环具备那个所“不希望有”的性质P的程度。如果我们选定了一个根性质P，然后我们试图寻求那些“好”环，即P-根为零的那些环的结构定理。这样的环叫作无P-根环或者叫作P-半单环。事实上，我们更多地关心P-根自身，而不是产生它的根性质P。按照条件(iii)，一个环若有P-根，则必有一个P-半单的商环。所以P-根愈大，则在研究P-半单环时，抛掉（或除去）的成份就愈多。所以基本问题是要发现某些类型的根，使我们抛掉的东西尽可能地少，同时还能得到相当深刻的结构定理。

Wedderburn在研究有限维代数时第一个引进根的概念。他的结果后来被推广到(左)Artin环上。但是Wedderburn根（即极大幂零理想）和由此得到的相当强的结构定理只适用于(左) Artin环。随后又出现了许多其他的根。一般说来，在左Artin环中，这些根中的每个均与Wedderburn根是一致的，但是它们也可以定义在非Artin环上。

本节的主要目的是研究一个这样的根，即Jacobson根。另一种根即素根在第4节中讨论，并参见习题4.11。还可见N.J.Divinshy〔22〕或者M.Gray〔23〕，那里对于根进行了广泛的讨论。在使用Jacobson根的过程中得到许多漂亮的定理，这充分表明对于Jacobson根值得作详细的研究。事实上，在讲述第1节的过程中

就是以Jacobson根作为背景的. Jacobson半单环（即 Jacobson根为零的环）可以用单环和本原环的语言来刻划（第3节）.

在定义Jacobson根之前，需要两点预备知识.

定义2.1 环R 的理想P叫作左(右)本原的，是指商环R/P是左(右)本原环.

注记：由于零环没有单模，因此零环不是本原的，从而R 自身不是左(右)本原理想.

定义2.2 环R 中元素a叫作左拟正规的，是指存在$r\in R$，使得 $r+a+ra=0$. 元素r叫作a的左拟逆元素. R的一个（右，左，双侧）理想 I叫作左拟正规的，是指I中每个元素都是左拟正规的. 类似地，$a\in R$ 叫作右拟正规的，是指存在$r\in R$，使得$r+a+ar=0$. 类似地定义右拟逆元素和右拟正规理想.

注记：为方便起见，有时将$r+a+ra$记为roa. 如果R有幺元素1_R，则a为左(右)拟正规元素$\Leftrightarrow 1_R+a$是左(右)可逆的（习题1).

为了简化一些结果的叙述，我们今后作以下的约定（它实际上是公理集合论中的一个定理). 如果环R中满足一给定性质的子集合所构成的集族$\mathscr{C}$是空的，则定义$\bigcap_{I\in\mathscr{C}} I=R$.

定理2.3 如果R是环，则R有一个理想$J(R)$使得：

(i) $J(R)$是所有单左 R-模的左零化子之交；

(ii) $J(R)$是R的所有正规极大左理想之交；

(iii)$J(R)$是R 的所有左本原理想之交；

(iv) $J(R)$ 是R的一个左拟正规左理想，并且包含R 的每个左拟正规左理想；

(v) 如果(i)—(iv)中的“左” 均改为“右”，则命题仍然正确。

定理 2.3 的证明见（引理2.8）后。理想 $J(R)$ 叫作环 R 的Jacobson根。在历史上，它首先是用拟正规性（定理2.3(iv)）的语言定义的。而拟正规性是引言中所定义的根性质。随着模在研究环中起着愈来愈重要的作用，人们给出了$J(R)$的其它一些刻划方式（定理2.3(i)—(iii)）。

注记：根据定理2.3(i) 和上面所作的约定可知，如果R没有单左R-模（从而没有单左R-模的零化子），则 $J(R)=R$. 如果R有幺元素，则每个理想都是正规的，并且永远存在极大左理想(定理III.2.18)，因此由定理2.3(ii)可知$J(R)\neq R$. 由定理2.3(iv)不能推出$J(R)$包含R的全部左拟正规元素，见习题4.

为证定理2.3我们需要五个预备性引理。这些引理是对左理想进行叙述和证明的。但是当把“左”全改成“右”之后，引理2.4—2.8仍然正确。在证明定理2.3之后我们给出一些例子。

引理2.4 如果$I(\neq R)$ 是环R的正规左理想，则I包含在一个正规的极大左理想中。

证明概要 由于I正规，存在$e\in R$，使得$r-re\in I$ (对于每个$r\in R$)。因此，包含I的每个左理想J都是正规的(采用同一个元素$e\in R$)。如果$I\subset J$并且$e\in J$，则$r-re\in I\subset J$导致对于每个$r\in R$ 均有$r\in J$，从而$R=J$。由这一事实便知道：Zorn 引理可以用到集合$\mathcal{S}=\{$左理想 $L\mid I\subset L\subsetneq R\}$上，其中$\mathcal{S}$ 的半序为包含关系。$\mathcal{S}$中的极大元即为包含I的正规极大左理想。∎

引理2.5 设R为环而K为R的所有正规极大左理想之交，则K为R的左拟正规左理想。

证明 K显然是左理想。如果$a\in K$。令$T=\{r+ra\mid r\in R\}$。若$T=R$，则存在$r\in R$使得$r+ra=-a$，于是$r+a+ra=0$。即a是左拟正规元素。因此只需证明$T=R$即可。

证明T为R的正规左理想（取$e=-a$）。如果$T\neq R$，由引理2.4可知T包含在某个正规极大左理想I_0之中（于是当R没有正规极大左理想时，则必然$T=R$）。由于$a\in K\subset I_0$，从而对所有$r\in R$，$ra\in I_0$。于是从$r+ra\in T\subset I_0$可知$r\in I_0$（对于每个$r\in R$）。从而$R=I_0$。这与I_0的极大性相矛盾。因此$T=R$。∎

引理2.6 设环R具有单左R-模。如果I是R的一个左拟正规左理想，则I包含在所有单左R-模之左零化子的交中。

证明 如果$I\subsetneq\cap\mathscr{A}(A)$，其中是对所有的单左$R$-模$A$求交，则对于某个单左$R$-模$B$，有$IB\neq 0$，从而存在某个非零元素$b\in B$，使得$Ib\neq 0$。由于$I$是左理想，从而$Ib$是$B$的非零子模。由单性可知$B=Ib$，于是有$a\in I$，使得$ab=-b$。因为$I$是左拟正规的，所以存在$r\in R$，使得$r+a+ra=0$。因此$0=ob=(r+a+ra)b=rb+ab+rab=rb-b-rb=-b$。这与$b\neq 0$相矛盾，从而必然有$I\subset\cap\mathscr{A}(A)$。∎

引理2.7 环R中的理想P是左本原的$\Leftrightarrow P$是某个单左R-模的左零化子。

证明 如果P是左本原理想，令A为忠实单R/P-模。证明A是R-模，其中$ra(r\in R,\ a\in A)$定义为$(r+P)a$。则$RA=(R/P)A$

$\neq 0$，并且A的每个R-子模也是 A 的R/P-子模，从而 A 是单 R-模。如果$r \in R$，则$rA = 0 \Longleftrightarrow (r+P)A = 0$。但是$(r+P)A = 0 \Longleftrightarrow r \in P$，因为$A$是忠实$R/P$-模。因此$P$是单$R$-模$A$的左零化子。

反之，假设P是单R-模B的左零化子。证明B是单R/P-模，其中$(r+P)b = rb (r \in R,\ b \in B)$。进而，若$(r+P)B = 0$，则$rB = 0$，从而$r \in \mathscr{A}(B) = P$并且在$R/P$中 $r+P = 0$。因此B 为忠实R/P-模。于是R/P是左本原环，即P是R的左本原理想。∎

引理2.8 设I是环R的左理想。如果I为左拟正规的，则 I 也是右拟正规的。

证明 如果I左拟正规而$a \in I$，则存在$r \in R$，使得$r \circ a = r + a + ra = 0$。因为$r = -a - ra \in I$，从而有$s \in R$，使得 $s \circ r = s + r + sr = 0$，因此$s$是右拟正规元素。易知运算$\circ$满足结合律，从而

$$a = o \circ a = (s \circ r) \circ a = s \circ (r \circ a) = s \circ o = s.$$

从而 a 是右拟正规元素。即I为右拟正规理想。∎

定理2.3的证明 设 $J(R)$ 是所有单左 R-模的左零化子之交。如果R没有单左R-模，由上面的约定我们有 $J(R) = R$。根据定理1.4知$J(R)$是理想。我们现在证明命题 (ii)—(iv) 对于所有左理想都是正确的。

首先我们注意：R本身不能是一个单左R-模A 的零化子（因为否则便有$RA = 0$）。这一事实加上定理1.3和引理2.7，便可推得下列一些条件是彼此等价的：

(a) $J(R) = R$；

(b) R没有单左R-模；

(c) R没有正规极大左理想；

(d) R没有左本原理想。

因此按照上面的约定，便知当$J(R)=R$时，(ii)，(iii)和(iv)均正确。

(ii) 假设$J(R)\neq R$而令K是R的所有正规极大左理想之交。于是由引理2.5和2.6可知$K\subset J(R)$。反之，设$c\in J(R)$。根据定理1.3，$J(R)$是全部商环R/I的左零化子之交，其中I遍历R的所有正规极大左理想。对于每个正规极大理想I，均存在$e\in R$，使得$c-ce\in I$。由于$c\in\mathscr{A}(R/I)$，从而$cr\in I(\forall r\in R)$。特别有$ce\in I$。因此，对于每个正规极大理想I，$c\in I$。从而$J(R)\subset\cap I=K$，即$J(R)=K$。

(iii) 为引理2.7的直接推论。

(iv) 由(ii)和引理2.5可知$J(R)$是左拟正规左理想。根据引理2.6可知$J(R)$包含每个左拟正规左理想。

为了完成证明，我们还需要证明用“右”代替“左”之后(i)—(iv)仍旧正确。设$J_1(R)$为所有单右R-模之右零化子之交。则上面的证明将“左”改成“右”之后仍旧成立。因此(i)—(iv)对于理想$J_1(R)$是成立的。但是根据(iv)和引理(2.8)可知$J(R)$是右拟正规的。因此由(iv)知$J(R)\subset J_1(R)$。类似地，$J_1(R)$也是左拟正规的，从而$J_1(R)\subset J(R)$。于是$J(R)=J_1(R)$。∎

例 设R是局部环，M是它的唯一极大理想（即由R中全部非单位元素所构成的，见定理3.4(3)）。我们要证明$J(R)=M$。由于R有1_R，从而$J(R)\neq R$。根据定理III.3.2，每个真理想只包含非单位元素，从而$J(R)\subset M$。另一方面，如果$r\in M$，则$1_R+r\notin M$（否则便有$1_R\in M$）。从而1_R+r为单位，于是r为左拟正规元素（习题1）。从而由定理2.3(iv)可知$M\subset J(R)$，即$M=J(R)$。这里有两个特殊情形。

例 域F上的幂级数环$F[[x]]$是局部环，并且极大理想为主理想(x)（系III.5.10）。因此$J(F[[x]])=(x)$。

例 如果p为素数，则$Z_{p^n}(n\geqslant 2)$是局部环，而极大理想为主理想(p)。作为Abel群，(p)同构于$Z_{p^{n-1}}$。因此$J(Z_{p^n})=(p)$。习题10中考虑Z_m的根(其中m为任意整数)。

定义2.9 环R叫作(Jacobson)半单的，是指它的Jacobson根$J(R)$是零。R叫作根环，是指$J(R)=R$。

注记：本书中的“根”永远指“Jacobson根”，而“半单”永远指“Jacobson半单”。读者在阅读环论方面的文献时，必须决定每个特别的定理中使用的根和半单性是在哪种意义下的。许多根(和半单性)的定义需要环是(左)Artin环。对于Jacobson根则不然，它可以定义在任意环上。

例 根据定理2.3(ii)，每个体都是半单的，因为只有零理想为正规极大左理想。

例 根据定理III.3.4。$\boldsymbol{Z}$中极大理想有形式(p)，其中p为素数。于是$J(Z)=\bigcap_p(p)=0$，即$\boldsymbol{Z}$是Jacobson半单环。关于它的推广见习题9。

例 如果D是体，则多项式环$R=D[x_1,\cdots,x_n]$是半单的。因为若$f\in J(R)$，则由定理2.3(iv)可知f同时为左和右拟正规元素。于是由习题1可知$1_R+f=1_D+f$是R中单位。由于只有D中非零元素是R中单位（见定理III.6.1），因此$f\in D$。于是$J(R)$为D的理想。由D的单性可知$J(R)=0$或者$J(R)=D$。但是-1_D不是左拟正规元素(证明!)，从而$-1_D\notin J(R)$。因此$J(R)=0$，即R是半单的。

定理2.10 设R为环.

(i) 如果R是本原的，则R为半单的.

(ii) 如果R是单和半单的，则R本原.

(iii)如果R是单的，则R或者是本原半单环，或者为根环.

证明 (i) R有忠实单左R-模A，于是$J(R)\subset\mathscr{A}(A)=0$.

(ii) 由单性$R\neq 0$. 从而必然存在单左 R- 模A (否则由定理2.3(i)可知 $J(R)=R\neq 0$，而这与半单性相矛盾). 根据定理1.4，左零化子$\mathscr{A}(A)$为R的理想，并且 $\mathscr{A}(A)\neq R$ (因为 $RA\neq 0$). 由单性可知$\mathscr{A}(A)=0$，于是A为忠实单R-模. 因此R是本原的.

(iii) 如果R 是单的，则理想 $J(R)$ 为R或者为零. 对于前一情形R是根环，对于后一情形R是半单的，再由 (ii) 可知是本原的. ∎

例 根据定理2.10(i)和定义1.5后面的例子，可知体上(左)向量空间的自同态环是半单的. 于是再由定理 VII.1.4 便知体上$n\times n$全阵环是半单的.

例 E.Sasiada 和 P. M. Cohn〔66〕给出单的根环的一个例子.

(在左Artin环中) 古典的 Wedderburn 根是极大幂零理想. 我们现在阐明这个根与 Jacobson根之间的联系.

定义2.11 环R 的元素a叫作幂零的，是指存在某个正整数n，使得$a^n=0$. R的一个 (左，右或者双侧) 理想I叫作是诣零理想，是指I中每个元素都是幂零元素. I叫作幂零理想，是指存在正整数n，使得$I^n=0$.

每个幂零理想都是诣零理想，因为$I^n=0$导致对于每个$a\in I$均

有$a^n=0$。但是诣零理想可能不是幂零理想(习题11)。

定理2.12 设R是环，则每个诣零左或右理想都包含在根$J(R)$之中。

注记：由定理立刻推出，每个诣零环都是根环。

证明 如果$a^n=0$，令$r=-a+a^2-a^3+\cdots+(-1)^{n-1}a^{n-1}$。则可证$r+a+ra=0=a+r+ar$，从而$a$同时是左和右拟正规的。因此每个诣零左(右)理想都是左(右)拟正规的。从而由定理2.3(iv)即知它包含在$J(R)$之中。∎

命题2.13 设R为左(右)Artin环，则根$J(R)$为幂零理想。从而R的每个诣零左或右理想都是幂零理想，并且$J(R)$为R的唯一极大幂零左(或右)理想。

注记：如果R为左(右) Noether环，则每个诣零左或右理想都是幂零理想(习题16)。

证明 设$J=J(R)$，考虑(左)理想链$J\supset J^2\supset J^3\supset\cdots$。由假设可知存在$k$，使得当$i\geqslant k$时，$J^i=J^k$。我们断言$J^k=0$。如果$J^k\neq 0$，则集合$S=\{$左理想$I\mid J^kI\neq 0\}$是非空的（因为$J^kJ^k=J^{2k}=J^k\neq 0$)。由定理VIII.1.4可知$S$有极小元素$I_0$。因为$J^kI_0\neq 0$，从而有非零元素$a\in I_0$，使得$J^ka\neq 0$。显然$J^ka$是$R$的左理想，它包含在$I_0$中。进而$J^ka\subset S$，因为$J^k(J^ka)=J^{2k}a=J^ka\neq 0$。于是由极小性可知$J^ka=I_0$。因此有非零元素$r\in J^k$，使得$ra=a$。由于$-r\in J^k\subset J(R)$，$-r$是左拟正规的，从而有$s\in R$，使得$s-r-sr=0$。于是

$$\begin{aligned}a=ra&=-(-ra)=-(-ra+0)=-(-ra+sa-sa)\\&=-(-ra+sa-s(ra))\\&=-(-r+s-sr)a=-0a=0.\end{aligned}$$

这就与$a \neq 0$ 相矛盾。因此 $J^h = 0$。本定理的最后一个论断现在是定理2.12的直接推论。∎

最后我们打算证明左拟正规性是本节引言中所定义的根性质。根据定理2.3(iv)，它所结合的根显然是 Jacobson 根，并且左拟正规环恰好是根环（定义2.9）。由于一个环同态必然将左拟正规元素映成左拟正规元素，所以根环的同态象也是根环。为了完成我们的讨论。我们必须证明$R/J(R)$是半单的，并且 $J(R)$ 是根环。

定理2.14 如果R为环，则商环$R/J(R)$是半单的。

证明 设$\pi: R \to R/J(R)$为正则满同态，并且以 $\bar{r}$ $(r \in R)$表示$\pi(r)$。令$\mathscr{C}$ 为R的全部正规极大左理想所构成的集合。如果$I \in \mathscr{C}$，则由定理2.3(ii)可知$J(R) \subset I$，又由定理IV.1.10 可知 $\pi(I) = I/J(R)$为$R/J(R)$的极大左理想。如果$e \in R$，使得对每个 $r \in R$ 均有 $r - re \in I$，则对于每个 $\bar{r} \in R/J(R)$均有$\bar{r} - \bar{r}\,\bar{e} \in \pi(I)$。因此对于每个 $I \in \mathscr{C}$，$\pi(I)$是正规的。由于 $J(R) = \bigcap_{I \in \mathscr{C}} I$，不难证明：如果 $\bar{r} \in \bigcap_{I \in \mathscr{C}} \pi(I) = \bigcap_{I \in \mathscr{C}} I/J(R)$，则$r \in J(R)$。于是由定理2.3(ii)(用于$R/J(R)$)可知

$$J(R/J(R)) \subset \bigcap_{I \in \mathscr{C}} \pi(I) \subset \pi(J(R)) = 0$$

从而$R/J(R)$是半单的。∎

引理2.15 设R为环而$a \in R$。

(i) 如果$-a^2$是左拟正规的，则a亦然。

(ii) $a\in J(R)\Longleftrightarrow Ra$为左拟正规左理想.

证明 (i) 如果 $r+(-a^2)+r(-a^2)=0$，令 $s=r-a-ra$，易证$s+a+sa=0$，于是a为左拟正规元素.

(ii) 如果$a\in J(R)$，则$Ra\subset J(R)$. 因为$J(R)$是左拟正规的，从而Ra亦是如此. 反之，设Ra是左拟正规的，证明$K=\{ra+na\mid r\in R,\ n\in\mathbb{Z}\}$是$R$的左理想并且包含$a$和$Ra$. 如果 $s=ra+na$，则 $-s^2\in Ra$. 由假设知 $-s^2$ 为左拟正规的，从而由(i)即知s亦是如此. 因此K为左拟正规左理想. 由定理2.3(iv)便知$a\in K\subset J(R)$. ∎

定理2.16 (i) 将环R的理想 I 自身看成环，则 $J(I)=I\cap J(R)$.

(ii) 如果R是半单的，则R的每个理想也是半单环.

(iii) $J(R)$为根环.

证明 (i) $I\cap J(R)$ 显然是I的理想. 如果$a\in I\cap J(R)$，则 a 为R 中左拟正规元素，从而有 $r\in R$使得 $r+a+ra=0$. 但是 $r=-a-ra\in I$，因此$I\cap J(R)$ 中每个元素均为I中的左正规元素，从而由定理2.3(iv)(用于I)便知$I\cap J(R)\subset J(I)$.

假设$a\in J(I)$. 对于$r\in R$, $-(ra)^2=-(rar)a\in IJ(I)\subset J(I)$，从而由定理2.3(iv) 可知 $-(ra)^2$ 为I中左拟正规元素. 再由引理2.15(i)便知ra为I中左拟正规元素. 因此Ra为 R 的左拟正规左理想，从而由引理2.15(ii) 便知 $a\in J(R)$. 因此 $a\in J(I)\cap J(R)\subset I\cap J(R)$. 于是$J(I)\subset I\cap J(R)$，这就证明了$J(I)=I\cap J(R)$. 命题(ii)和(iii)是(i)的直接推论. ∎

定理2.17 如果$\{R_i\mid i\in I\}$是一族环，则

$$J\Big(\prod_{i\in I} R_i\Big) = \prod_{i\in I} J(R_i).$$

证明概要 证明：元素$\{a_i\}\in\prod R_i$在$\prod R_i$中是左拟正规的$\Longleftrightarrow$对于每个i，a_i在R_i中是左拟正规的。从而$\prod J(R_i)$是$\prod R_i$的左拟正规理想。于是由定理2.3(iv)可知$\prod J(R_i)\subset J(\prod R_i)$。

对于每个$k\in I$，令π_k：$\prod R_i\to R_k$为正则射影。证明$I_k=\pi k(J(\prod R_i))$是R_k的左拟正规理想，于是$I_k\subset J(R_k)$，从而$J(\prod R_i)\subset\prod J(R_i)$.∎

习　题

注：R永远为环。

1. 对于a、$b\in R$，令$a\circ b=a+b+ab$。

   (a) $\circ$是满足结合律的二元运算，并且其幺元素为$0\in R$。

   (b) R中同时左和右拟正规的元素所组成的集合G对于运算$\circ$形成群。

   (c) 如果R中有1_R，则$a\in R$为左(右)拟正规元素$\Longleftrightarrow$ 1_R+a是左(右)可逆的。〔提示：$(1_R+r)(1_R+a)=1_R+r\circ a$，$r(1_R+a)-1_R=(r-1_R)\circ a$〕

2. (Kaplansky) R为体$\Longleftrightarrow$ R中除了一个元素之外的每个元素都是左拟正规的。〔注意：在体D中只有-1_D不是左拟正规元素，参见习题1.〕

3. 设I为R中左理想，而令$(I:R)=\{r\in R\mid rR\subset I\}$。

   (a) $(I:R)$是R的理想。如果I是正规的，则$(I:R)$是包含在I中的R之最大理想。

   (b) 如果I是R的正规极大左理想，并且$A\cong R/I$，则$\mathscr{A}(A)=(I:R)$。因此$J(R)=\cap(I:R)$，其中I跑过R的全部正规极大左理想。

4. 根$J(R)$中不包含非零的幂等元素。但是非零幂等元素可以是左拟正规元素。〔提示：习题1和2.〕

5. 如果R有1_R，则

(a) $J(R)=\{r\in R \mid 1_R+sr$是左可逆的（对于每个$s\in R$）$\}$

(b) $J(R)$ 是满足下面性质的最大理想 K：对于每个 $r\in K$，1_R+r均是单位。

6. (a) 半单环的同态象不必是半单的。

(b) 如果$f:R\to S$是环的满同态，则 $f(J(R))\subset J(S)$。

7. 如果R是所有分母为奇数的有理数构成的环，则 $J(R)$ 是由所有奇分母和偶分子的有理数所构成的。

8. 设R为体 D上$n\times n$ 的全部上三角方阵所构成的环（见习题VII.1.2)。求 $J(R)$，并且证明$R/J(R)$同构于直积$D\times D\times\cdots\times D$($n$个)。〔提示：证明严格三角方阵是幂零的。〕〔注〕

9. 主理想整环 R是半单的$\Longleftrightarrow R$为域或者R包含无穷多个彼此不相伴的不可约元素。

10. 设 D为主理想整环，d是 D 中非零元素并且 d 不是单位。令 R 为商环 $D/(d)$。

(a) R半单$\Longleftrightarrow d$为D中一些彼此不相伴的不可约元素的乘积。〔提示：习题VIII.1.2.〕

(b) $J(R)=?$

11. 如果p是素数，令R 为 $\prod_{n\geq 1} Z_{p^n}$的子环 $\sum_{n\geq 1} Z_{p^n}$。I_n是 Z_{p^n} 中由 $p\in Z_{p^n}$ 生成的理想。则理想 $I=\sum_{n\geq 1} I_n$是R的诣零理想，但不是幂零理想。

12. 设R是不含幺元素的环。象定理III.1.10中那样将R嵌到含幺并且特征为零的环S之中，求证 $J(R)=J(S)$。从而每个半单环都可以嵌到含幺半单环中。

13. $J(\mathrm{Mat}_n R)=\mathrm{Mat}_n(J(R))$。下面是证明的轮廓。

(a) 如果A是左R-模，将$A^n=A\oplus A\oplus\cdots\oplus A$($n$个) 中元素看成是列向

〔注〕 方阵(a_{ij})叫作是严格(上)三角方阵，是指当$i\leqslant j$时，$a_{ij}=0$。

——译者

量，则A^n是左$(\mathrm{Mat}_n R)$-模(在通常矩阵乘法之下)。

(*b*) 如果A是单R-模，则A^n是单$(\mathrm{Mat}_n R)$-模。

(*c*) $J(\mathrm{Mat}_n R)\subset \mathrm{Mat}_n J(R)$。

(*d*) $\mathrm{Mat}_n J(R)\subset J(\mathrm{Mat}_n R)$。[提示：如下证明$\mathrm{Mat}_n J(R)$是$\mathrm{Mat}_n R$的左拟正规理想：对于每个$k=1,2,\cdots,n$，令$K_k=\{(a_{ij})\mid a_{ij}\in J(R),\ a_{ij}=0$ (当$j\neq k$时)$\}$。证明K_k是$\mathrm{Mat}_n R$的左拟正规左理想。并且注意$K_1+K_2+\cdots+K_n=\mathrm{Mat}_n J(R)$。]

14. (*a*) 设I为$R[X]$的非零理想，$p(x)$是I中首项系数为a并且具有最小次数的非零多项式。如果$f(x)\in R[x]$并且$a^m f(x)=0$，则$a^{m-1}p(x)f(x)=0$。

(*b*) 如果环R没有非零的诣零理想 (特别若R是半单的)，则$R[x]$是半单的。[提示：设M是$J(R[x])$中最小次数的非零多项式构成的集合。以N表示M中多项式的首项系数和零所构成的集合。用(*a*)来证明N是R的诣零理想，从而$J(R[x])=0$。]

(*c*) 存在环R，使得$R[x]$半单但是R不半单。[提示：考虑$R=F[[t]]$，其中F为域。]

15. 设L是R的左理想而K是R的右理想。$M(R)$是由R的全部幂零理想所生成的理想。

(*a*) $L+LR$是理想，并且对于每个$n\geqslant 1$，$(L+LR)^n\subset L^n+L^nR$。

(*b*) $K+RK$是理想，并且对于每个$n\geqslant 1$，$(K+RK)^n\subset K^n+RK^n$。

(*c*) 如果L[或者K]为幂零的，则理想$L+LR$[或者$K+RK$]也是幂零的，从而$L\subset M(R)$[或者$K\subset M(R)$]。

(*d*) 如果N是R的极大幂零理想，则R/N没有非零的幂零左或右理想。[提示：先证R/N没有非零的幂零理想，然后将(*c*)用于环R/N。]

(*e*) 如果K[或者L]是诣零理想，但不是幂零理想，而$\pi: R\to R/N$是正则满同态，则$\pi(K)$[或者$\pi(L)$]是R/N的诣零右[或者左]理想，但不是幂零理想。

16. (Levitzky)左Noether环R中的每个诣零左理想或者诣零右理想I都是幂

零理想.

[证明概要：由习题15可以假设R没有非零的幂零左或右理想．假设I是左或者右理想，并且不是幂零理想．又令$0\neq a\in I$．证明aI是诣零右理想(即使I为左理想时也是如此)，从而对于每个 $u\in aR$，左理想$\mathscr{A}(u)\neq 0$．于是存在非零元素 $u_0\in aR$，使得$\mathscr{A}(u_0)$极大．从而对于每个$x\in R$，如果$u_0x\neq 0$，则$\mathscr{A}(u_0)=\mathscr{A}(u_0x)$．证明对于每个$y\in R$均有$(u_0y)u_0=0$，于是$(Ru_0)^2=0$．因此$Ru_0=0$．这导致$\{r\in R\mid Rr=0\}$ 是R的非零的幂零右理想．矛盾．]

17．求证中山引理VIII.4.5中条件(i)如果改成条件

(i′) J包含在R的Jacobson根之中，

则此引理对于任意环R也是对的．[提示：利用定理2.3(iv)和习题1(c)来证(i′)⇒(ii)．]

3．半 单 环

按照第 2 节一开始所描绘的根的理论，我们现在把研究限制在 Jacobson 半单环的情形．任何半单环均可刻划为：它是本原环的直积的一些特殊类型的子环 (命题3.2)．对于半单 (左) Artin 环，则可以证明更强的结果．这样的环事实上是有限个单环的直积 (定理3.3)．还可以用模的语言以多种方式刻划它们 (定理3.7)．在这个过程中我们定义了任意环上的半单模，并且发展了它们的基本性质(定理3.6)．

定义3.1 环R叫作一族环$\{R_i\mid i\in I\}$的子直积，是指R是直积$\prod_{i\in I}R_i$的子环，并且对于每个 $k\in I$均有 $\pi_k(R)=R_k$， 其中 π_k：

$\prod_{i\in I} R_i \to R_k$是正则满同态。

注记：环S同构于一族环$\{R_i \mid i\in I\}$的子直积$\Longleftrightarrow$存在环的单同态$\phi: S\to \prod_{i\in I} R_i$，使得对于每个$k\in I$，$\pi_k\phi(S)=R_k$。

例 设P为素数集合。对于每个$k\in \mathbb{Z}$，$p\in P$，以$k_p\in Z_p$表示k在正则满同态$\mathbb{Z}\to Z_p$之下的象。则由$k\longmapsto \{k_p\}_{p\in P}$给出的映射$\phi$：$\mathbb{Z}\to \prod_{p\in P} Z_p$是环的单同态，并且对于每个$p\in P$，$\pi_p\phi(\mathbb{Z})=Z_p$。因此$\mathbb{Z}$同构于一族域$\{Z_p \mid p\in P\}$的子直积。更一般地我们有

命题3.2 非零环R是半单的$\Longleftrightarrow R$同构于一些本原环的子直积。

注记：由命题1.7和3.2可知非零交换半单环是域的子直积。

证明概要 假设R是非零半单环，以$\mathscr{P}$表示R的全部左本原理想所构成的集合。则对于每个$P\in\mathscr{P}$，R/P均是本原环(定义2.1)。由定理2.3(iii)可知$0=J(R)=\bigcap_{P\in\mathscr{P}} P$。对于每个$P$，令$\lambda_P$：$R\to R/P$和$\pi_P$：$\prod_{Q\in\mathscr{P}} R/Q\to R/P$为相应的正则满同态。由$r\longmapsto\{\lambda_P(r)\}_{P\in\mathscr{P}}$给出的映射$\phi$：$R\to\prod_{P\in\mathscr{P}} R/P$是环的单同态，并且对于每个$P\in\mathscr{P}$，$\pi_P\phi(R)=R/P$。

反之，设有一族本原环$\{R_i \mid i\in I\}$和环的单同态$\phi: R\to\prod_{i\in I} R_i$，使得对于每个$k\in I$，$\pi_k\phi(R)=Rk$。令$\psi k$为满同态$\pi_k\phi$，则$R/\ker\psi_k$同构于本原环$R_k$(系III.2.10)。于是$\ker\psi_k$为$R$的左本原理想(定义2.1)。因此由定理2.3(iii)可知$J(R)\subset\bigcap_{k\in I}\ker\psi_k$。但是若

$r\in R$和$\psi_k(r)=0$，则$\phi(r)$在$\prod R_i$中的第k个分量为0。因此若$r\in\bigcap_{k\in I}ker\psi_k$，我们必需有$\phi(r)=0$。由于$\phi$是单同态，从而$r=0$。因此$J(R)\subset\bigcap_{k\in I}ker\psi_k=0$，即$R$是半单的。∎

按照第1节关于本原环的结果，我们现在可以把半单环刻划为：它同构于一族环的子直积，而该族环中每个环都是某个体上向量空间的自同态稠环。遗憾的是，子直积（和自同态稠子环）往往不是容易处理的对象。可是如果不作进一步的限制，这或许是我们能够得到的最好结果了。但是对于(左)Artin环，这些结果可以大大地加强。

定理3.3 （Wedderburn-Artin） 关于环R的以下几个条件彼此等价。

(i) R是非零半单左Artin环；

(ii) R是有限个单理想的直积，而每个单理想均同构于一个体上有限维向量空间的自同态环；

(iii) 存在着体$D_1,\cdots,D_t$和正整数$n_1,\cdots,n_t$，使得R同构于环$\mathrm{Mat}_{n_1}D_1\times\mathrm{Mat}_{n_2}D_2\times\cdots\times\mathrm{Mat}_{n_t}D_t$。

注记：R的单理想是指理想本身是单环。

证明 (ii)$\Longleftrightarrow$(iii)：由习题III.2.9和定理VII.1.4.

(ii)$\Rightarrow$(i)：由假设有$R\cong\prod_{i=1}^{t}R_i$，其中每个R_i都是向量空间的自同态环。定义1.5后面的例子表明，每个R_i都是本原的，从而由定理2.10(i)可知$J(R_i)=0$。于是由定理2.17便有

$$J(R)\cong\prod_{i=1}^{t}J(R_i)=0.$$

因此R是半单的。由定理VII.1.4，系 VIII.1.7和 VIII.1.12可知R是左Artin环。

(i)⇒(ii)：由于$R\neq 0$并且$J(R)=0$，根据定理2.3(iii)可知R有左本原理想。假设R只有有限多不同的左本原理想：$P_1, P_2, \cdots, P_t$。则每个R/P_i都是本原环(定义2.1)，故为左Artin环(系VIII.1.6)。因而由定理1.14可知R/P_i均是单环，从而同构于体上有限维左向量空间的自同态环。由于R/P_i是单环，每个P_i都是R的极大理想(定理III.2.13)。进而$R^2 \not\subset P_i$(否则$(R/P_i)^2=0$)，由极大性便知$R^2+P_i=R$。同样地，若$i\neq j$，则由极大性有$P_i+P_j=R$。由系III.2.27(中国剩余定理)和定理2.3(iii)可知存在环同构：

$$R=R/0=R/J(R)=R/\bigcap_{i=1}^{t}P_i\cong R/P_1\times\cdots\times R/P_t,$$

如果$i_k: R/P_k\to\prod_{i=1}^{t}R/P_i$是正则嵌入(定理 III.2.22)，则每个$i_k(R/P_k)$都是$\prod_{i=1}^{t}R/P_i$的单理想。在同构$\prod_{i=1}^{t}R/P_i\cong R$之下，$i_k(R/P_k)$的象是$R$的单理想。显然$R$是这些理想的(内)直积。

为了完成证明，我们只需证明R不能有无限多个不同的左本原理想。假设不然，令$P_1, P_2, P_3, \cdots$是R的不同的左本原理想序列。由于

$$P_1\supset P_1\cap P_2\supset P_1\cap P_2\cap P_3\supset\cdots$$

是(左)理想下降链，因此存在整数n，使得$P_1\cap\cdots\cap P_n=P_1\cap P_2\cap\cdots\cap P_n\cap P_{n+1}$，即$P_1\cap\cdots\cap P_n\subset P_{n+1}$。上一段已经证明了$R^2+P_i=R$和$P_i+P_j=R(1\leqslant i\neq j\leqslant n+1)$。由定理III2.25的证明可知$P_{n+1}+(P_1\cap\cdots\cap P_n)=R$。从而$P_{n+1}=R$。而这与$P_{n+1}$为左本原理想(见定义2.1后面的注记)这一事实相矛盾。所以R只有有限多个不同

的本原理想．从而完成了证明．∎

系3.4 (i)半单左 Artin 环必有幺元素．

(ii) 半单环是左Artin环$\Longleftrightarrow$它是右Artin环．

(iii) 半单左Artin环同时为左和右Noether环．

注记：实际上可以证明得更多些：每个含幺左Artin环都是左Noether环(习题13)．

证明概要 (i)为定理3.3．

(ii) 定理3.3 中将所有"左"均改成"右"之后，命题仍然正确．从而由定理3.3中的等价条件(i)和(iii)导致：R为左Artin环$\Longleftrightarrow R$为右Artin环．

(iii) 系VIII.1.7，VIII.1.12和定理3.3(iii)．∎

下面一个系今后是不需要的．注意环R的元素e叫作是幂等元素，是指$e^2=e$．

系3.5 如果I是半单左Artin环R中的理想，则$I=Re$，其中e为R的中心之中的幂等元素．

证明概要 由定理3.3可知R是单理想的(环) 直积，即$R=I_1\times\cdots\times I_n$．对于每个$j$，由单性知$I\cap I_j$为0或者$I_j$．必要时重新排列下标之后，我们可以假设$I\cap I_j=I_j(1\leqslant j\leqslant t)$，$I\cap I_j=0(t+1\leqslant j\leqslant n)$．根据系3.4 可知$R$有$1_R$，于是存在$e_j\in I_j$，使得$1_R=e_1+e_2+\cdots+e_n$．由于$j\neq k$时$I_j\cap I_k=0$，我们有

$$e_1+e_2+\cdots+e_n=1_R=(1_R)^2=e_1^2+e_2^2+\cdots+e^2{}_n$$

于是$e_j^2=e_j$(对于每个j)．易证每个e_i都在R的中心之中，$e=e_1+\cdots+e_t$是I中的幂等元素，并且它在R的中心之中．由于I为理想，$Re\subset I$．反之，若$u\in I$，则$u=u1_R=ue_1+\cdots+ue_n$．但是当$j>t$时

$ue_j \in I \cap I_j = 0$. 因此$u = ue_1 + \cdots + ue_t = ue$. 从而$I \subset Re$. ∎

定理3.3是用环论语言来刻划半单左 Artin 环.从环与模的密切关系读者可能猜想到这样的环也可用模的语言来严格地刻划. 为此我们需要一个定理，这个定理对于任意环上的模都是对的.

定理3.6 关于环R上非零模A的下列诸条件彼此等价.

(i) A为一族单子模的和;

(ii) A为一族单子模的(内)直和;

(iii) 对于A中每个非零元素a, $Ra \neq 0$. 同时，A的每个子模B均是直和成份（即有某个子模C使得$A = B \oplus C$.）

满足定理 3.6 中等价条件的模叫作半单模或者叫作完全可约模.“半单”一语起因于定理3.3(ii) 和下面要证的事实:(左)Artin 半单环上的模都是半单的.

定理3.6的证明概要 (i)⇒(ii):设A是单子模族$\{B_i \mid i \in I\}$之和（即A是由$\bigcup_{i \in I} B_i$生成的）. 用Zorn 引理可证I有非空子集J，它对于下面的性质是极大的：由$\{B_j \mid j \in J\}$生成的子模事实上为直和$\sum_{j \in J} B_j$. 我们断言 $A = \sum_{j \in J} B_j$. 为证此我们只需要证明：对于每个$i \in I$均有 $B_i \subset \sum_{j \in J} B_j$. 由于$B_i$是单子模，而 $B_i \cap (\sum B_j)$ 是B_i的子模. 从而或者$B_i \cap (\sum B_j) = B_i$，这导致$B_i \subset \sum B_j$；或者$B_i \cap (\sum B_j) = 0$. 但是后一情形是不可能出现的. 因为在这种情况下，$K = \{i\} \cup J$也是一个集合，使得由$\{B_k \mid k \in K\}$生成的子模是直和(定理IV.1.1S)，而这与J的极大性相矛盾.

(ii)⇒(iii)： 假设A是直和$\sum_{i \in I} B_i$,其中B_i均为单子模. 如果

a是A中非零元素，则$a=b_{i_1}+\cdots+b_{i_k}$，其中$0\neq b_{i_k}\in B_{i_k}$($i_1,\cdots,i_k\in I$)。显然$Ra=0\Longleftrightarrow$对于每个i_k均有$Rb_{i_k}=0$。但是由定义1.1后面的注记(iii)表明$Rb_{i_k}=B_{i_k}\neq 0$，因此$Ra\neq 0$。

设B是A的非零子模。由单性可知$B\cap B_i$为0或者B_i。如果对于所有i均有$B\cap B_i=B_i$，则$A=B$，从而B显然为直和成份：$A=B\oplus 0$。否则便有i使得$B\cap B_i=0$。利用Zorn引理可以发现I的一个子集合J对于性质$B\cap(\sum_{j\in J}B_j)=0$是极大的。我们证明$A=B\oplus(\sum_{j\in J}B_j)$。根据定理IV.1.15，只需证明对于每个$i$均有$B_i\subset B\oplus(\sum_{j\in J}B_j)$。如果$i\in j$则$B_i\subset\sum_{j\in J}B_j$从而证毕。如果$i\notin J$而$B_i\not\subset B\oplus\sum_{j\in J}B_j$，则由$B_i$的单性可知$B_i\cap(B\oplus\sum_{j\in J}B_j)=0$。从而集合$J\cup\{i\}$与$J$之极大性相矛盾。因此$B_j\subset B\oplus\sum_{j\in J}B_j$。

(iii)⇒(i)：首先，如果N是A的任一子模，则N的每个子模K均是N的直和成份。因为由假设知K是A的直和成份，设$A=K\oplus L$。则$N=N\cap A=(N\cap K)\oplus(N\cap L)=K\oplus(N\cap L)$。

其次我们证明A有单子模。由于$A\neq 0$，A中存在非零元素a。利用Zorn引理可以发现A的一个子模B对于性质$a\notin B$是极大的。由假设知$A=B\oplus C$，其中C是非零子模，并且$RC\neq 0$。我们证明C是单模：因为不然的话，C有真子模D，由上一段可知D是C的直和成份。从而$C=D\oplus E$，$E\neq 0$，于是$A=B\oplus C=B\oplus D\oplus E$，其中$D\neq 0$，$E\neq 0$。现在$B\oplus D$和$B\oplus E$都真包含$B$。由$B$的极大性必然$a\in B\oplus D$和$a\in B\oplus E$。于是$b+d=a=b'+e$($b$，$b'\in B$，$d\in D$，

$e \in E$). 现在$0 = a - a = (b - b') + d - e \in B \oplus D \oplus E$, 从而 $d = 0$, $e = 0$, $b - b' = 0$. 于是$a = b \in B$, 这就导致矛盾. 因此C是单模.

令A_0是由A的全部单子模所生成的A的子模. 则$A = A_0 \oplus N$, 其中N为某个子模. 由上一段最后所述, 可知N满足与A相同的假设条件. 如果$N \neq 0$, 则由上一段的推理可知N包含有一个非零单子模T. 由于T为A的单子模, $T \subset A_0$. 因此$T \subset A_0 \cap N = 0$. 这就导致矛盾. 从而$N = 0$, 即$A = A_0$是一族单子模的和. ∎

现在我们可以用模的语言给出半单左 Artin 环的许多刻划方法. 由于环R(看作左R-模)的子模恰是R 的左理想, 从而其中一些刻划方法可以用左理想的语言来叙述. R的子集合$\{e_1, \cdots, e_m\}$叫作是正交幂等元素集合, 是指对于每个i均有$e_i^2 = e_i$并且当$i \neq j$时$e_i e_j = 0$.

定理3.7 含幺非零环R的下列诸条件彼此等价.

(i) R为半单左Artin环;

(ii) 每个幺作用左R-模都是投射模;

(iii) 每个幺作用左R-模都是内射模;

(iv) 每个幺作用左 R- 模的短正合序列都是分裂的正合序列;

(v) 每个非零的幺作用左R-模都是半单的;

(vi) R自己是幺作用半单左R-模;

(vii) R的每个左理想均有形式Re, 其中e为幂等元素;

(viii) R是极小左理想$K_1, \cdots, K_m$(作为左R-模)的内直和, 并且$K_i = Re_i (e_i \in R) (1 \leqslant i \leqslant m)$, 而 $(e_1, \cdots, e_m)$. 是正交幂等元素集合, 并且$e_1 + e_2 + \cdots + e_m = 1R$.

注记: 由于对于半单环, 它是左 Artin 环$\Longleftrightarrow$它是右 Artin

环(系3.4)。因此定理3.7中每个条件均等价于它对于右模和右理想的类似的论断。此外，不失普遍性可以假设R有1_R，因为由系3.4知道，每个半单左Artin环均有1。如果略去“幺作用”一词，则定理不再成立(习题10)。

定理3.7的证明概要 (ii)$\Leftrightarrow$(iii)$\Leftrightarrow$(iv)是习题IV.3.1。为了完成证明，我们只需再证明(iv)$\Leftrightarrow$(v)和(v)$\Rightarrow$(vii)$\Rightarrow$(vi)$\Rightarrow$(i)$\Rightarrow$(viii)$\Rightarrow$(v)。

(iv)$\Rightarrow$(v)：如果B是非零幺作用R-模A的子模，则

$$0\to B\subseteq A\to A/B\to 0$$

是短正合序列，由假设它是分裂的。从定理IV.1.18的证明可知$A=B\oplus C$，其中$C\cong A/B$。由于A为幺作用模，对于每个非零元素$a\in A$都有$Ra\neq 0$。因此由定理3.6可知A是半单的。

(v)$\Rightarrow$(iv)：设$0\to A\xrightarrow{f} B\xrightarrow{g} C\to 0$为幺作用$R$-模短正合序列。则$f$：$A\to f(A)$为同构。从(V)知$B$半单。根据定理3.6可知$f(A)$为$B$的直和成份。如果$\pi$：$B\to f(A)$为正则满同态，则$\pi f=f$，并且$f^{-1}\pi$：$B\to A$是$R$-模同态，使得$(f^{-1}\pi)f=1_A$。由定理IV.1.18可知序列是分裂的。

(v)$\Rightarrow$(vii)：R的左理想恰好为它的子模。如果L为左理想，则由(v)和定理3.6可知存在另一左理想I，使得$R=L\oplus I$，从而有$e_1\in L$，$e_2\in I$，使得$1_R=e_1+e_2$。由于$e_1\in L$，$Re_1\subset L$。如果$r\in L$，则$r=re_1+re_2$，于是$re_2=r-re_1\in L\cap I=0$。因此对于每个$r\in L$均有$r=re_1$。特别地，$e_1e_1=e_1$和$L\subset Re_1$。因此$L=Re_1$并且e_1是幂等元素。

(vii)$\Rightarrow$(vi)：R的子模L是左理想，从而$L=Re$，其中e为幂等元素。证明$R(1_R-e)$也是R的左理想，并且$R=Re\oplus R(1_R-e)$。

因此由定理3.6即知R是半单的。

(Vi)⇒(i)：由假设R是直和$\sum_{i\in I}B_i$，其中B_i均是R的单子模(左理想)。从而I有一个有限子集合I_0(为方便起见，令$I_0=\{1,2,\cdots,k\}$)，使得$1_R=e_1+\cdots+e_k(e_i\in B_i)$。因此对于每个$r\in R$均有$r=re_1+re_2+\cdots+re_k\in\sum_{i=1}^{k}B_i$，于是$R=\sum_{i=1}^{k}B_i$。如果$r\in J(k)$，则由定理2.3(i)可知$rB_i=0(1\leqslant i\leqslant k)$。于是

$$r=r1_R=re_1+re_2+\cdots+re_k=0.$$

从而$J(R)=0$，即R是半单的。由于B_i是单的并且

$$(B_1\oplus\cdots\oplus B_i)/(B_1\oplus\cdots\oplus B_{i-1})\cong B_i,$$

从而序列

$$R=B_1\oplus\cdots\oplus B_k\supset B_1\oplus\cdots\oplus B_{k-1}\supset\cdots\supset B_1\oplus B_2\supset B_1\supset 0$$

是R的组成列。从而由定理VIII.1.11便知R是左Artin环。

(i)⇒(viii)：按照定理3.3，我们可以假设$R=\prod_{i=1}^{t}\mathrm{Mat}_{n_i}D_i$，其中$n_i>0$，$D_i$均为体。对于每个固定的$i$和每个$j=1,2,\cdots,n_i$，以$e_{ij}$表示$\mathrm{Mat}_{n_i}D_i$中方阵，它在$(j,j)$位置为元素$1_{D_i}$，而在其余地方均为0。则$\{e_{i1},\cdots,e_{in_i}\}$是$\mathrm{Mat}_{n_i}D_i=R_i$中的正交幂等元素集合，它们的和是单位方阵。从系 viii.1.12的证明可知，每个R_ie_{ij}均是R_i的极小左理想，而$R_i=R_ie_{i1},\oplus\cdots\oplus R_ie_{in_i}$。由于$R$是环直积$R_1\times\cdots\times R_t$，从而$R_iR_j=0$(当$i\neq j$时)；$Re_{ij}=R_ie_{ij}$；$Re_{ij}$为$R$的极小左理想；最后，$\{e_{ij}\mid 1\leqslant i\leqslant t,1\leqslant j\leqslant n_i\}$是$R$中正交幂等元素集合，并且其和为$\sum_{i=1}^{t}\left(\sum_j e_{ij}\right)=\sum_{i=1}^{t}1_{R_i}=1_R$。显然

$$R=\sum_{i=1}^{t}\sum_{j=1}^{n_i}Re_{ij}.$$

(viii)⇒(v)：设A是任意幺作用R-模。对于每个$a\in A$，和每个i，K_ia为A的子模(习题IV.1.3)，而$a=1_Ra=e_1a+\cdots+e_ma\in K_1a+\cdots+K_ma$。从而子模$K_ia(a\in A,1\leqslant i\leqslant m)$生成$A$。对于每个$a\in A$和每个$i$，由$k\longmapsto ka$给出的映射$f$：$K_i\to K_ia$是$R$-模满同态。由于$K_i$是含幺环的极小左理想，从而$K_i$是单$R$-模。于是由Schur引理1.10可知，在$K_ia=0$时$f$为同构。从而$\{K_ia\mid 1\leqslant i\leqslant m,a\in A,K_ia\neq 0\}$是一族单子模，其和为$A$。于是由定理3.6可知$A$是半单的。∎

定理3.3和3.7表明，半单左Artin环可以分解为单理想的直积或者极小左理想的直和。我们现在讨论这两种分解的唯一性问题。

命题3.8 设R为半单左Artin环。

(i) $R=I_1\times\cdots\times I_n$，其中每个$I_i$均是$R$的单理想。

(ii) 如果J为R的任意单理想，则对于某个k，$J=I_k$。

(iii) 如果$R=J_1\times\cdots\times J_m$，其中$J_k$都是$R$的单理想，则$n=m$并且(在重新标记之后)$I_k=J_k(1\leqslant k\leqslant n)$。

注记：结论$J=I_k$和$J_k=I_k$分别比命题$J\cong I_k$和$J_k\cong I_k$要强得多。在命题3.8中所唯一决定的单理想$I_1,\cdots,I_n$叫作R的单分支。

证明 (i) 是由于定理3.3。

(ii) 如果J为R的单理想，则$RJ\neq 0$，于是有某个k使得$I_kJ\neq 0$。由于I_kJ是非零理想，并且同时在I_k和J之中。由I_k和J的单性即知$I_k=I_kJ=J$。

(iii) 由假设可知$I_1,\cdots,I_n$均是非零理想并且彼此没有非零公共元素，$J_1,\cdots,J_m$也是如此。当$J_k=I_k$时，令$J_k\to I_k$。由此定义出m元集合$\{J_1,\cdots,J_m\}$到n元集合$\{I_1,\cdots,I_n\}$的映射θ。由(ii)知θ是

可定义的，并且为单射，因此$m \leqslant n$. 将J_k和I_k的作用颠倒过来，同样推出$n \leqslant m$. 从而$n = m$. 并且θ是一一对应. ∎

根据定理3.7(viii)，半单左Artin环R是极小左理想的直和. 这个分解的唯一性(不计同构)是下面命题的直接推论，因为R是半单R-模(定理3.7(vi))，而R的极小左理想恰是它的单模.

命题3.9 设A为环R上的半单模. 如果有直和分解

$$A = B_1 \oplus \cdots \oplus B_m \text{和} A = C_1 \oplus \cdots \oplus C_n,$$

其中B_i，C_j均是A的单子模，则$m = n$并且(在重新标记之后)$B_i \cong C_i (1 \leqslant i \leqslant m)$.

注记：这里的唯一性命题比命题3.8中的要弱. 如果将"$B_i \cong C_i$"改成"$B_i = C_i$"，则命题3.9不再成立(习题11).

证明 序列

$$A = B_1 \oplus \cdots \oplus B_m \supset B_2 \oplus \cdots \oplus B_m \supset \cdots \supset B_m \supset 0$$

是A的组成序列，其单因子为$B_1, B_2, \cdots, B_m$. 类似地，$A = C_1 \oplus \cdots \oplus C_n \supset C_2 \oplus \cdots \oplus C_n \supset \cdots \supset C_n \supset 0$也是$A$的组成序列，其单因子为$C_1, C_2, \cdots, C_n$. 由Jordan-Hölder定理viii.1.10即推出$m = n$并且(在重新标记之后)$B_i \cong C_i (1 \leqslant i \leqslant m)$. ∎

下列定理只用于定理6.7的证明中.

定理3.10 设R是半单左Artin环.

(i) 每个半单左(右)R-模均同构于R的一个极小左(右)理想.

(ii) 不同构的单左(右)R-模的个数等于R的单分支个数.

证明 由系3.4知R也是右Artin环. 从前面关于左右对称的一些结果，我们只需对左模证明即可.

(i) 根据定理3.7，$R=K_1\oplus\cdots\oplus K_m$，其中每个$K_i$都是$R$的非极小左理想(单子模)。$R$有幺元素(系3.4)。由定义1.1后面的注记(ii)，可知每个单R-模A均为幺作用模。又从定理3.7的(viii)⇒(v)证明中可知有某个$i(1\leqslant i\leqslant m)$和$a\in A$，使得$A$包含一个非零子模$K_ia$，并且$K_ia\cong K_i$。再由$A$的单性导致$A=K_ia\cong K_i$。

(ii) R的单分支是$R=I_1\times\cdots\times I_n$中的单理想$I_j$(命题3.8)。从(i)可知我们只需证明：

(a) 每个K_i均在某个I_t中；

(b) 每个I_t均包含某个K_i；

(c) $K_i\cong K_j$(作为R-模)⇒K_i和K_j包含在同一个单分支I_t中。

现在对这三个论断证明如下。

(a) 由于R有幺元素，从而$K_i=RK_i=I_1K_i\times\cdots\times I_nK_i$。但是每个$I_jK_i$都是$R$的左理想并且包含在$K_i$中，从而必然有$t$，使得$I_tK_i=K_i$，而由极小性即知当$j\neq t$时$I_jK_i=0$。因此$K_i=I_tK_i\subset I_t$。

(b) 如果I_t不包含K_i，根据(a)即知$R=\sum K_i$包含在

$$I_1\times\cdots\times I_{t-1}\times I_{t+1}\times\cdots\times I_n$$

之中，由单性知$I_t\neq 0$而$R=\prod I_j$，从而

$$0\neq I_t=I_t\cap R=I_t\cap(I_1\times\cdots\times I_{t-1}\times I_{t+1}\times\cdots\times I_n)=0.$$

这就导致矛盾。

(c) 如果$K_i\subset I_{t_1}$而$K_i\subset I_{t_2}$，其中$t_1\neq t_2$，则由(a)可知$0\neq K_i=I_{t_1}K_i$而$0\neq K_i=I_{t_2}K_j$。由于$R=\prod I_j$，$I_{t_1}I_{t_2}=0=I_{t_2}I_{t_1}$。于是不可能有$R$-模同构$K_i\cong K_j$。反之，设$K_i\subset I_t$和$K_j\subset I_t$。则$K_i$和$K_j$为$I_t$-模。因为$I_t$单，而由(a)有$0\neq K_i=I_tK_i$，从而$K_i$在$I_t$中之左零化子必然是零。从而$K_jK_i\neq 0$(因为$0\neq K_j\subset I_t$)。因此有$a\in K_i$，使得$K_ja\neq 0$。由于$K_i$和$K_j$为$R$的左理想，$K_ja$为$R$的非零左理想而$K_ja\subset K_i$。由极小性可知$K_ja=K$。从定理3.7对于(viii)⇒(v)的证明

中可以看出$K_j a \cong K_j$，从而$K_i \cong K_j$。 ∎

习　题

1. 环R同构于一族环$\{R_i | i \in I\}$的子直积$\Longleftrightarrow$对于每个$i \in I$均存在R的一个理想K_i，使得$R/K_i \cong R_i$而$\bigcap_{i \in I} K_i = 0$。

2. 环R叫作亚不可约的（或者叫作：对于子直积是不可约的），是指R的所有非零理想之交不为零。

   (*a*) R是亚不可约的$\Longleftrightarrow$如果R同构于$\{R_i | i \in I\}$的子直积，则必然有某个$i \in I$，使得$R \cong R_i$[见习题1]。

   (*b*) (Birkhoff)每个环均同构于一族亚不可约环的子直和。

   (*c*) 亚不可约的交换环中的零因子与0一起形成一个理想。

3. 半单Artin交换环是域的直积。

4. 将所有1008阶半单环作同构分类。其中有多少是交换环？[提示：习题V.8.10]。

5. 环R中元素a叫作（在Von Neumann意义下）正规的，是指存在$x \in R$，使得$axa = a$。如果R中每个元素均是正规的，则称R为正规环。

   (*a*) 每个体均是正规环。

   (*b*) 正规环的有限直积是正规环。

   (*c*) 每个正规环都是半单的[反过来不成立，例如$\mathbf{Z}$]。

   (*d*) 体上(不必有限维)向量空间上全部线性变换所成的环是正规的。

   (*e*) 半单左Artin环是正规的。

   (*f*) R正规$\Longleftrightarrow$$R$的每个主左(右)理想都是由幂等元素生成的。

   (*g*) 含幺非零正规环R为体$\Longleftrightarrow$只有0和1_R是R中幂等元素。

6. (*a*) 半单模的非零同态象和非零子模均是半单的。

   (*b*) 两个半单子模的交或者是0或者仍旧半单。

7. 关于半单模A的下列诸条件彼此等价。

(a) A是有限生成的；

(b) A是有限个单子模的直和；

(c) A有组成序列；

(d) A同时满足子模升链条件和降链条件（见定理viii.1.11）。

8. 设A是左Artin环R上的模，并且对于每个非零元素$a\in A$均有$Ra\neq 0$。令$J=J(R)$。则$JA=0\Longleftrightarrow A$半单。〔提示：如果$JA=0$，则$A$为$R/J$—模，而$R/J$是半单左Artin环。见习题IV.1.17.〕

9. 设R为环，并且作为左R-模它是其极小左理想的直和。假设$\{r\in R|Rr=0\}=0$。如果A为R-模，并且$RA=A$，则A是半单的。〔提示：如果I是一个极小左理想而$a\in A$，求证Ia或者为0，或者为A的单子模.〕

10. 求证一个非零R-模A如果$RA=0$，则A不能为半单模，但是可能为投射模。从而定理3.7若去掉“幺作用”一词则不再成立。〔见习题IV.2.2，定理IV.3.2和命题IV.3.5.〕

11. 设R是一个无限域上的2×2方阵环。

(a) R有无限多个不同的真左理想，并且其中任意两个真左理想作为左R-模均是同构的。

(b) R中存在无限多个不同的极小左理想对(B,C)，使得$R=B\oplus C$。

12. 左Artin环R的不同构单左R-模的个数等于不同构的单右R-模的个数。〔提示：证明A为单R-模$\Longleftrightarrow A$为单$R/J(R)$-模。利用定理2.14和3.10.〕

13. (a) (Hopkins)如果R是含幺左Artin环，则R为左Noether环。〔提示：设n为最小正整数使得$J^n=0$(命题2.13)。令$J^0=R$。由于$J(J^i/J^{i+1})=0$，而R为左Artin环，从而每个$J^i/J^{i+1}$$(0\leqslant i\leqslant n+1)$均有组成列（习题7和8）。利用这些和定理IV.1.10来构作R的组成列，再利用定理VIII.1.11.〕

注记：如果将假设“R有1_R”改成弱很多的“$\{r\in R|rR=0=Rr\}=0$”，则Hopkins定理仍旧成立。见L.Fuchs〔13；第283—283页.〕

(b) Hopkins定理的逆不成立。

4. 素根，素环和半素环

现在我们引进环的素根。一个环叫作半素的，是指它的素根为零(定义4.1)。然后我们给出类似于第2和3节中对于Jacobson根与半单环所证明的那些结果(命题4.2—4.4)。在素根，素理想，半素环，素环和Jacobson根，左本原理想，半单环，本原环之间有很强的类比。

本节的其余部分讨论Goldie定理4.8，这是关于满足某种类型左理想降链条件的半素环的结构定理。在这里，Goldie定理所起的作用与Wedder-burn-Artin定理1.14和3.3对于满足左理想降链条件的环所起的作用是一样的。事实上，可以把Goldie定理看作是Wedderburn-Artin定理到很广一类环上的推广。在命题4.4之后，定理4.8之前以及系4.9之后所作的讨论中，我们对此再作更加充分的解释。

本节在今后是不需要的。

定义4.1 环R的素根$P(R)$是所有素理想的交。如果R没有素理想，则规定$P(R)=R$。如果$P(R)=0$，称R为半素环。

注记：素根(也称作Bear下根或者McCoy根)具有第2节引言中所定义的根性质，详见习题1和习题2。半素环是对于素根来说是半单的环(见第2节引言)。我们用“半素”一词，是为了避免与Jacobson半单性相混淆，同时也免得用语上造成混乱。习题3讨论了素根和Jacobson根之间的关系。

与Jacobson根的情形一样，环R的素根和幂零理想有密切联

系。为了证明这样的结果，我们需要复习一些术语。

设S是环R的子集合。由定理1.4知集合$\{r\in R\mid rS=0\}$为R的左理想。如果S是左理想，则该集合事实上是R的理想。集合$\{r\in R\mid rS=0\}$叫作S的左零化子，并且记成$\mathscr{A}_r(S)$。类似地，集合

$$\mathscr{A}_r(S)=\{r\in R\mid Sr=0\}$$

是R的右理想，并且当S是右理想时，它为R的理想，称$\mathscr{A}_r(S)$为S之右零化子。R的左(右)理想I叫作是一个左(右)零化子，是指有R的某个子集合S，使得$I=\mathscr{A}(S)(I=\mathscr{A}_r(S))$。

注记：两个左(右)零化子的交仍是左(右)零化子，因为$\mathscr{A}(S)\cap\mathscr{A}(T)=\mathscr{A}(S\cup T)$。如果$S$和$T$均是左理想，则$\mathscr{A}(S)\cap\mathscr{A}(T)=\mathscr{A}(S\cup T)=\mathscr{A}(S+T)$。

命题4.2 环R是半素环$\Longleftrightarrow R$没有非零的幂零理想。

证明概要 ($\Rightarrow$)：如果I为幂零理想而K为任一素理想，则有某个n使得$I^n=0\in K$。从而$I\subset K$。因此$I\subset P(R)$。若R半素，则$P(R)=0$。从而只有零理想是幂零理想。

($\Leftarrow$) 反之，设R没有非零的幂零理想。我们要证$P(R)=0$。这只需证明对于每个$0\neq a\in R$均有素理想K使得$a\notin K$，从而$a\notin P(R)$。首先我们注意$\mathscr{A}(R)\cap R$是R的幂零理想。这是因为：

$$(\mathscr{A}(R)\cap R)(\mathscr{A}(R)\cap R)\subset\mathscr{A}(R)R=0.$$

从而$\mathscr{A}(R)=\mathscr{A}(R)\cap R=0$。类似有$\mathscr{A}_r(R)=0$。如果$b$为$R$中任一非零元素，我们证明$RbR\neq 0$。因为若不然，则$Rb\subset\mathscr{A}(R)=0$，从而$Rb=0$。因此$b\in\mathscr{A}_r(R)=0$，这就导致矛盾。因此$RbR$是$R$的非零理想，从而不是幂零理想。于是$bRb\neq 0$(否则便有$(RbR)^2\subset RbRbR=0$)。对于每个$0\neq b\in R$，取$f(b)\in bRb$使得$f(b)\neq 0$。由引论中的递归定理6.2可知存在函数$\varphi$：$\mathbf{N}\to R$使得

$$\varphi(0)=a,\ \varphi(n+1)=f(\varphi(n)).$$

令$a_n=\varphi(n)$，则$a_{n+1}=f(a_n)\neq 0$。令$S=\{a_i\mid i\geqslant 0\}$，由Zorn引理可求出一个理想$K$对于性质$K\cap S=\phi$是极大的(因为$0\notin S$，从而至少有一个理想与$S$非交)。

因为$a=a_0\in S$，$a\notin K$，从而$K\neq R$。为了完成证明，我们只需证K是素理想即可。如果A和B是R的理想，并且$A\not\subset K$，$B\not\subset K$。则由极大性可知$(A+K)\cap S\neq\phi$，$(B+K)\cap S\neq\phi$。从而有i，j使得$a_i\in A+K$，$a_j\in B+K$。取$m>max(i,j)$，由于对于每个n均有$a_{n+1}=f(a_n)\in a_nRa_n$，从而$a_m\in(a_iRa_i)\cap(a_jRa_j)\subset(A+K)\cap(B+K)$。因此

$$a_{m+1}=f(a_m)\in a_mRa_m\subset(A+K)(B+K)\subset AB+K.$$

但是$a_{m+1}\notin K$，从而$AB\not\subset K$，于是K为素理想。∎

环R叫做素环，是指零理想是素理想（即若I和J为理想，$IJ=0$，则$I=0$或者$J=0$)。素理想，素环和半素环之间的关系类似于左本原理想，本原环和半单环之间的关系，特别地，我们指出如下事实：

(i) 素根(Jacobson根)是所有素理想(本原理想)之交，(见定理2.3(iii))。

(ii) 每个素环都是半素的，因为0是素理想。这对应于如下的事实：每个本原环都是半单的(定理2.10(i))。

命题4.3 K是环R的素理想$\Longleftrightarrow R/K$为素环。

注记：这是定义2.1(左本原理想)之模拟。

证明概要 如果R/K为素环，令π：$R\to R/K$为正则满同态。设I和J是R中的理想，$IJ\subset K$。则$\pi(I)$和$\pi(J)$为R/K中的理想（习题III.2.13(b))，并且$\pi(I)\pi(J)=\pi(IJ)=0$。由于R/K是素环，

从而$\pi(I)=0$或者$\pi(J)=0$。 即$I\subset K$或者$J\subset K$。 因此K为素理想(定义III.2.14)。反过来则是定理III.2.13和定义III.2.14的直接推论。∎

下面是半素——半单类比的最后一部分。

命题4.4 环R是半素的$\Longleftrightarrow R$同构于素环的子直积。

证明概要 如果将"半单"和"本原"分别改成"半素"和"素"，则命题3.2正好是命题4.4。经过这样的改变，并用命题4.3代替定义2.1，即可将命题3.2的证明移植过来。∎

我们已经看到，本原环是半单环的基本构件。命题4.4表明素环是半素环的基本构件。在这里，本原环和素环有不相象的地方：本原环可以用很熟悉的矩阵环和向量空间上的自同态环来刻划(第1节)，而对于素环则没有相应的结果。但是形势也不是完全无希望的。对于本原环和半单左 Artin 环我们已经得到很丰硕的结果(第1节和第3节)、而对于满足某些链条件的素环和半素环，似乎应当得到一些有益的刻划。现在我们就来具体地作这件事。

首先我们注意，在左 Artin环中素根和Jacobson 根是一致的(习题3(c))。从而左 Artin 半素环也是半单环，因此它的结构由Wedderburn—Artin定理3.3所决定。由系3.4，每个半素(半单)左Artin环也是左Noether环，所以下一个明显的目标是考虑半素左Noether环类(即满足左理想升链条件的半素环)。注意这种环可能不是左Artin环(例如$\mathbb{Z}$)。从而任何一个对半素左Noether环的刻划方式都是我们上述结果的不平凡的推广。

我们事实上要刻划更广泛一类环，它真包含全部半素左Noether环。这广泛的一类环叫作半素左Goldie 环，我们现在来定义它。

R的一族左理想$\{I_j \mid j \in J\}$叫作无关的，是指对于每个$k \in J$均有$I_k \cap I_k^* = 0$，其中I_k^*是由$\{I_j \mid j \neq k\}$生成的左理想。换句话说，$\{I_j \mid j \in J\}$是无关的$\Longleftrightarrow$由$\{I_j \mid j \in J\}$生成的左理想I实际上是内直和$I = \sum_{j \in J} I_j$(见定理IV.1.15)。

定义4.5 环R叫作(左)Goldie环，是指

(i) R满足左零化子升链条件；并且

(ii) R的左理想无关集合必为有限集合。

注记：(i) 定义4.5的条件(i)的意思是：给了任意一个左零化子链$\mathscr{A}(S_1) \subset \mathscr{A}(S_2) \subset \cdots$，必存在$n$，使得当$i \geqslant n$时均有$\mathscr{A}(S_i) = \mathscr{A}(S_n)$。这个条件也等价于：

(i′) R满足左零化子极大条件（即由左零化子构成的每个非零集合按集合包含关系均具有极大元素。）。

为了看出(i)与(i′)等价，只需注意：定理viii.1.4的证明完全可以搬到现在的情形上来，而且反过来也对。

(ii) 也可以用显然的方式定义右Goldie环。一个右Goldie环不必为左Goldie环，见A.W.Goldie[62]。

例 每个左Noether环R也是左Goldie 环。这是因为条件(i)显然满足。另一方面，如果$\{I_j \mid j \in J\}$是无限的左理想无关集合，则存在I_1，I_2，…，使得$I \subsetneqq I_1 \times I_2 \subsetneqq I_1 \times I_2 \times I_3 \subsetneqq \cdots$。这与升链条件相矛盾。因此条件(ii)也成立。从而R为Goldie环。存在着不是左Noether环的左Goldie环。

上面例子表明，半素左Goldie环类包括半素左Noether环类。我们下面要用半素左Goldie环的左商环(其意义见下面的定义)来刻划半素左Goldie环。

定义4.6 环R中的非零元素a叫作正规的，是指a不是左零因子也不是右零因子。

定义4.7 含幺环$Q(R)$叫作环R的左商环，是指

(i) $R\subset Q(R)$；

(ii) R中正规元素均为$Q(R)$中单位；

(iii) $Q(R)$中每个元素c均有形式$c=a^{-1}b$，其中$a,b\in R$，并且a为正规元素。

注记：(i)环R不一定有左商环。但是如果它有左商环，那末由定义4.7不难看出，$Q(R)$不计同构是唯一确定的。

(ii) 用同样的方法可以定义R的右商环，只是在条件(iii)中的"$c=a^{-1}b$"改成"$c=ba^{-1}$"。一个右商环可以不是左商环（见N. J. Divinsky[22，第71页]）。

(iii) 如果R是环，并且有左商环$Q(R)=T$，则称R为T中的左order。

例 设R是交换环，并且至少有一个正规元素。以S表示R的正规元素全体。则全商环$S^{-1}R$是含幺环（定理III.4.3），并且它包含一个子环$\varphi_S(R)$与R同构(定理III.4.4(ii))。如果象通常那样将R和$\varphi_S(R)$等同，则$R\subset S^{-1}R$，R中正规元素均是$S^{-1}R$中的单位(定理III.4.4(i))，并且$S^{-1}R$中元素均有形式$s^{-1}r(r\in R,\ s\in S\subset R)$。因此$S^{-1}R$为$R$的左商环。特别地，有理数域$\mathbb{Q}$是左 Noether 环$\mathbb{Z}$的左商环。

例 每个半单左 Artin 环是它自己的左商环(习题6)。

由定义4.7易知，左商环$Q(R)$的结构和环R的结构有密切的联系。所以，如果我们不能用熟知的环来明显地刻划环R，我们

退一步便是希望R有左商环，并且左商环可以用熟知的环来明显地刻划。这正是Goldie定理所要作的事情。

定理4.8 (Goldie) R是半素左 Goldie 环 $\Longleftrightarrow$ R有左商环$Q(R)$并且$Q(R)$是半单左Artin环；R是素的左Goldie环$\Longleftrightarrow$ R有左商环$Q(R)$并且$Q(R)$是单的左Artin环。

为了节省篇幅起见，我们在这里不证明定理 4.8。一个最好的证明是C.Procesi与L.Small[65]。在I.Herstein [24]中有一个稍微推广了的形式。证明虽然很长，但是并不比本章前面给出的许多证明困难。它要用到Ore定理。Ore定理的证明在I.N.Herstein[24，第170页]中给出了一个摘要，而在N.J.Divinsky[22，第66页]中则给出了详细证明。

由于半单左Artin环的结构已经完全决定，定理4.8对于半素左Goldie环给出了我们能作到的最好的刻划(半素左Noether环为其特殊情形)。由于降链条件改成了升链条件，我们付出的代价则是产生了环R和$Q(R)$之间的“差距”。正如我们在命题4.4后面的讨论和习题3.13中所观察到的，升链条件比降链条件要弱得多。

系4.9 R为半素(或者素)左Goldie环$\Longleftrightarrow$$R$ 有左商环$Q(R)$，并且$Q(R)\cong Mat_{n_1}D_1\times\cdots\times Mat_{n_k}D_k$(或者$Q(R)\cong Mat_{n_1}D_1$)，其中$n_1$，…，$n_k$为正整数，而$D_1$，…，$D_k$为体。

证明 定理1.14，3.3，和4.8。∎

系4.9是 Goldie 定理的另一种形式，它可以看作是Wedderburn—Artin 定理1.14和3.3到很大一类环上的推广。定理3.3是说，半单左Artin环是体上方阵环的直积。而Goldie定理是说，每个半素左Goldie环均有左商环，并且这个左商环是体上方阵环的

直积．但是，每个半单左Artin环都是半素左Goldie环(系3.4，习题3(*a*)和定义4.5后面的例子)．进而，每个半单左 Artin 环是它自己的左商环(习题6)．因此在这种情况下 Goldie 定理就归结为Wedderburn—Artin定理．对于单左Artin环和定理1.4也可作类似地推理．

习　　题

注：R永远是环．

1．R的子集合T叫作一个m-系(广义乘法系)，是指

$c,d\in T\Rightarrow$存在$x\in R$，使得$cxd\in T$．求证：

(*a*) P是R的素理想$\Longleftrightarrow R-P$为m-系〔提示：习题III.2.14〕．

(*b*) 设I为R的理想，并且 I 与m-系T不相交．求证I包含在某个理想Q中，而Q对于性质$Q\cap T=\phi$是极大的．然后证明Q是素理想．〔提示：适当修改定理VIII.2.2的证明．〕

(*c*) R中元素r 叫作有零性质，是指：一个 m-系如果包含r则必包含0．求证：素根$P(R)$为集合$M=\{r\in R\mid r$有零性质$\}$．〔提示：利用 (*a*)证明$M\subset P(R)$，然后用(*b*)证明$P(R)\subset M$．〕

(*d*) $P(R)$中每个元素c均是幂零元素．〔提示：$\{c^i\mid i\geqslant 0\}$ 为m-系．〕如果R为交换环，则$P(R)$即是由R中全部幂零元素所构成的．

2．(*a*) 如果I为R的理想，则$P(I)=I\cap P(R)$．特别有$P(P(R))=P(R)$．〔提示：习题1(*c*)．〕

(*b*) $P(R)$是P中满足$P(R/K)=0$的最小理想K．特别地，$P(R/P(R))=0$，从而$R/P(R)$是半素环．〔提示：习题III.2.17(*d*)．〕

(*c*) 理想I叫作有零性质，是指I中每个元素均有零性质．(习题1(*c*))．求证零性质是根性质(定义见第2节引言)，并且它的根恰好是$P(R)$．

3．(*a*) 半单环必为半素环．

(*b*) $P(R)\subset J(R)$.[提示：习题1(*d*)或者由(*a*)和习题2(*b*).]

(*c*) 如果R为左Artin环，则$P(R)=J(R)$.[提示：命题2.13.]

4. R为半素环$\Longleftrightarrow$对于所有的理想A和B，若$AB=0$则$A\cap B=0$.

5. (*a*) 设R为含幺环，则方阵环$\mathrm{Mat}_n R$为素环$\Longleftrightarrow R$为素环.

(*b*) 如果R为任意环，则$P(\mathrm{Mat}_n R)=\mathrm{Mat}_n P(R)$[提示：当$R$有$\mathbf{1}_R$时利用习题2和上面(*a*)部分.在一般情况下用定理III.1.10将R嵌到含幺环S中，然后由习题2可知$P(R)=R\cap P(S)$.]

6. 如果R是半单左Artin环，则R是它自己的左商环.[提示：由定理3.3可知R有$\mathbf{1}_R$，从而只需证明R中每个正规元素均为单位即可，由定理3.3和一个直接的推导，可以假定$R=\mathrm{Mat}_n D$，其中D为体.然后再用定理VII.2.6和命题VII.2.12]

7. 下列诸命题彼此等价：

(*a*) R为素环；

(*b*) $a,b\in R$，$aRb=0\Rightarrow a=0$或者$b=0$；

(*c*) R的每个非零右理想的右零化子均为0.

(*d*) R的每个非零左理想的左零化子均为0.

8. 每个本原环都是素环[见习题7].

9. 含幺素环的中心是整环.[见习题7.其逆见习题10.]

10. 设J为整环而F为J的商域.以R表示形如

$$\begin{pmatrix} A_n & & & & \mathbf{0} \\ & d & & & \\ & & d & & \\ & & & d & \\ \mathbf{0} & & & & \ddots \end{pmatrix}$$

的所有无限矩阵（行和列均以$\mathbf{Z}^*$为下标集合）所构成的集合，其中$A_n\in \mathrm{Mat}_n(F)$，而$d\in J\subset F$.

(*a*) R为环.

(*b*) R的中心是由全部形如

$$\begin{pmatrix} d & & 0 \\ & d & \\ & & d \\ 0 & & \ddots \end{pmatrix}, \quad d \in J$$

的矩阵所构成的集合，因此它同构于J.

(c) R是本原环(由习题8即知它为素环)。

11. R中由全部诣零理想所生成的理想叫作是R的诣零根(Nil radical)，表示成$N(R)$.

(a) $N(R)$是诣零理想.

(b) $N(N(R)) = N(R)$

(c) $N(R/N(R)) = 0$.

(d) $P(R) \subset N(R) \subset J(R)$

(e) 如果R为左Artin环，则$P(R) = N(R) = J(R)$.

(f) 如果R是交换环，则$P(R) = N(R)$.

5. 代　　数

在本节中，我们将第1—3节的概念和结果转移到K-代数上来(K是含幺交换环).特别地,对于K-代数证明了Wedderburn-Artin定理(定理5.4)。本章的后一部分处理域上代数，其中包括代数性代数和有限群上的群代数.在本节中K 永远指的是含幺交换环.

为了把第1—3节的结果转移到K-代数上来，首先要复习一下K-代数，K-代数同态，子代数和代数理想的定义(第IV.7节).我们知道，如果一个K-代数A有1_A，则(左，右，双侧)代数理想和环A的(左,右,双侧)理想是一致的(见定义IV.7.3后面的注记)。这一事实今后将常常用到而不加解释。

一个左Artin$K$-代数是满足左代数理想降链条件的K-代数。一个左Artin$K$-代数可以不必是左Artin环(习题1)。

例 如果D为K上除法代数，则$\mathrm{Mat}_n D$是K-代数。由系VIII.1.12可知它是左Artin$K$-代数。

定义5.1 设A为含幺交换环K上的代数。

(i) 一个左(代数)A-模指的是一个幺作用左K-模M，并且M还是环A上的左模，同时有$k(rc)=(kr)c=r(kc)$(对于每个$k\in K$，$r\in A$，$c\in M$)。

(ii) A-模M的一个A-子模指的是M的一个子集合，并且该子集合自身(对于M中的运算)是一个代数A-模。

(iii) 一个代数A-模M叫作单的(或者叫作不可约的)，是指$AM\neq 0$并且M没有真A-子模。

(iv) 代数A-模同态f：$M\to N$是一个映射，它同时是K-模同态和A-模同态。

注记：如果A是K-代数，那末术语"A-模"永远指的是一个代数A-模。否则我们便写成环A上的模。类似地定义右A-模N，即是要满足$k(cr)=(kc)r=c(kr)$(对于每个$k\in K$，$r\in A$，$c\in N$)。

现在，对应于环上的各种概念，我们可以用同样方法定义单K-代数，本原K-代数，K-代数的Jacobson根，半单K-代数等等。这只需把环理想，环上的模和环同态改成代数理想，代数上的模和代数同态。为了把第1—3节的结果(特别是Wedderburn-Artin定理)，移植到K-代数上来，下面两个定理是有用的。

定理5.2 设A是K-代数。则

(i) A的子集合I是正规极大左代数理想$\Longleftrightarrow I$是环A的正规

极大左理想.

(ii) 环A的Jacobson根等于代数A的Jacobson根. 特别地, A为半单环$\Longleftrightarrow A$为半单代数.

注记: 如果A有1_A, 则定理5.2显然成立.因为在这种情形下. 代数理想和环理想是一致的.

证明 (i)如果I为环A的正规极大左理想, 只需证明对于每个$k\in K$均有$kI\subset I$. 假设对于某个$k\in K$, $kI\not\subset I$. 由于$r(kI)=k(rI)$(定义5.1(i)), 从而$I+kI$为A的左理想并且真包含I. 由极大性可知$A=I+kI$. 由假设可知存在$e\in A$, 使得对于每个$r\in A$, $r-re\in I$. 令$e=a+kb(a,b\in I)$, 则

$$e^2=e(a+kb)=ea+e(kb)=ea+(ke)b\in I.$$

由于$e-e^2\in I$并且$e^2\in I$, 从而$e\in I$. 即事实"$r-re\in I$(对于一切$r\in A$)"导致$A=I$. 这就与I之极大性相矛盾, 因此对于每个$k\in K$均有$kI\subset I$.

反之, 设I是正规极大左代数理想, 于是它也是环A的正规左理想. 根据引理2.4, I包含在环A的某个正规极大左理想I_1中. 上一段表明I_1事实上为正规左代数理想, 从而由极大性可知$I=I_1$.

(ii) 由(i)和定理2.3(ii)推得. ∎

定理5.3 设A为K-代数. 则每个单的代数A-模也是环A上的单模. 环A上每个单模M均可唯一地赋以K-模结构, 使得M为单的代数A-模.

证明 设N是单的代数A-模, 则$AN\neq 0$. 如果N_1为N的子模. 则AN_1为N的代数子模, 因此$AN_1=N$或者$AN_1=0$. 如果$AN_1=N$, 则$N_1=N$. 如果$AN_1=0$, 则$N_1\subset D=\{c\in N\mid Ac=0\}$. 但是$D$为$N$的一个代数子模, 并且$D\neq N$(因为$AN\neq 0$). 因此由单性可知$D$

$=0$，即$N_1=0$。从而N没有真子模，即它是环A上的单模。

如果M为环A上的单模，根据定义1.1后面的注记(iii)，M为循环模。设$M=Ac(c\in M)$。在$M=Ac$上如下定义一个K-模结构

$$k(rc)=(kr)c\quad(k\in K,\ r\in A)。$$

由于$kr\in A$，从而$(kr)c\in Ac=M$。为证K在M上的作用可以由此定义，我们必须证明

$$rc=r_1c\Rightarrow(kr)c=(kr_1)c\quad(k\in K,\ r,r_1\in A)。$$

显然这只需证明

$$rc=0\Rightarrow(kr)c=0\quad(k\in K,\ r\in A)。$$

现在根据定理1.3的证明，可知$M\cong A/I$，其中正规极大左理想I是由$x\longmapsto xc$给出的映射$A\to Ac=M$的核。从而$rc=0\Rightarrow r\in I$。但是由定理5.4，I为代数理想，因此$kr\in I$。从而$(kr)c=0$。即上面方法定义了K在M上的作用。容易证明M是K-模，并且是代数A-模。而M的K-模结构是唯一决定的，因为M上每个K-模结构如果使$M=Ac$成为A-模，必然满足$k(rc)=(kr)c\ (k\in K,\ r\in A)$。∎

定理5.4 A为半单左 Artin K-代数$\Longleftrightarrow$存在着 K-代数同构

$$A\cong \mathrm{Mat}_{n_1}D_1\times \mathrm{Mat}_{n_2}D_2\times\cdots\times \mathrm{Mat}_{n_t}D_t,$$

其中n_i为正整数，D_i均为K上除法代数。

注记：定理5.4对于域K上任意半单有限维代数A都是有效的，因为这种A必为左Artin 代数（习题2）。

证明概要 利用定理5.2和5.3以及习题3和4就可以把 Wedderburn-Artin 定理3.3的证明移植到K-代数上来。∎

本节其余部分处理关于域上代数的一些问题。首先，对于 K 为代数封闭域的情形，我们得到定理5.4的一个加强形成。最后考虑域上的群代数。

假设A是域K上含幺非零代数。容易看出，由$k\longmapsto k1_A$ 定义

的映射α：$K\longrightarrow A$是K-代数同态。由于$\alpha(1_K)=1_A\neq 0$，从而Ker $\alpha\neq K$。但是域没有真理想，所以Ker$\alpha=0$。即α是单同态。进而，α的象位于A的中心中，因为对于$k\in K$，$r\in A$ 我们有

$$\alpha(k)r=(k1_A)r=k(1_Ar)1_A=(1_Ar)(k1_A)=r\alpha(k).$$

于是我们得到以下的约定：

如果A是域K上含幺非零代数，则K可等于 Imα并且可看成是A的中心的子代数。

在这种等同之下，K在A上的K-模运算与在A 中乘以子代数K的元素是一致的，因为$ka=(k1_A)a=a(k)a$。

定义5.5 域K上代数A中元素a叫作在K 上是代数的，是指它是$K[x]$中某个多项式的根。A 叫作是K上的代数性代数，是指A中每个元素在K上都是代数的。

例 如果A为有限维，则A必为代数性代数。因为若$\dim_K A=n$，$a\in A$，则$n+1$个元素a，a^2，a^3，$\cdots$，a^{n+1}必然线性相关。因此有不全为 0 的 $k_i\in K$，使得 $k_1a+k_2a^2+\cdots+k_{n+1}a^{n+1}=0$。从而$f(a)=0$，其中$f$为非零多项式$k_1x+k_2x^2+\cdots+k_{n+1}x^{n+1}\in K[x]$。

例 K 上只有有限多非零元素的可数无限阶方阵全体所形成的代数是无限维单的代数性代数（习题5）。

注记：代数性代数的根是诣零根（习题6）。

引理5.6 如果D是代数封闭域K上代数性除法代数，则 $D=K$。

证明 由上述的约定可知K包含在D 的中心中。如果$a\in D$，则有$f(x)\in K[x]$，使得 $f(a)=0$。由于K 是代数封闭域，$f(x)=k(x-k_1)(x-k_2)\cdots(x-k_n)(k,\ k_i\in K,\ k\neq 0)$。于是

$$0 = f(a) = k(a-k_1)(a-k_2)\cdots(a-k_n).$$

由于D是体，从而有i使得$a-k_i=0$，即$a=k_i\in K$从而$D\subset K$。∎

定理5.7 设A是代数封闭域K上有限维代数性代数。则存在正整数$n_1,\cdots,n_t$，使得有代数同构

$$A\cong \mathrm{Mat}_{n_1}K\times\cdots\times\mathrm{Mat}_{n_t}K.$$

证明 由定理5.4（和其后的注记）可知$A\cong\mathrm{Mat}_{n_1}D_1\times\mathrm{Mat}_{n_2}D_2\times\cdots\times\mathrm{Mat}_{n_t}D_t$，其中$D_i$均为$K$上除法代数。每个$D_i$在$K$上都是有限维的（不然的话，$\mathrm{Mat}_{n_i}D_i$从而$A$将会是无限维的）。因此由引理5.6可知对于每个$i$都有$D_i=K$。∎

对于域上的群代数已进行了多年的研究。它们的用处是：利用群代数结构可以采用环论上的技巧来研究群。

命题5.8 (Maschke) 设$K(G)$为域K上有限群G的群代数。如果K的特征为0，则$K(G)$是半单代数。如果K的特征为素数p，则$K(G)$是半单的$\Longleftrightarrow p\nmid|G|$。

证明概要 假设$\mathrm{char}K=0$或者p，其中$p\nmid|G|$。如果B是含幺的K-代数（例如$K(G)$），如下定义映射α：$B\longrightarrow\mathrm{Hom}_K(B,B)$，其中$\alpha(b)$定义为映射$\alpha_b$：$B\to B$，$\alpha_b(x)=bx$。不难证明如此可以定义出$\alpha$并且它是$K$-代数单同态。

对于$g\in G$，我们把$K(G)$中元素1_Kg简记成g。由定义可知$K(G)$是K-向量空间，$X=\{g\mid g\in G\}$是一组基并且维数为$n=|G|$。对于每个$u\in K(G)$，以M_u表示α_u对于基X的方阵。设$e\neq g\in G$，则对于每个$g_1\in G$均有$\alpha_g(g_1)=gg_1\neq g_1$（因为$G$是群）。因此$\alpha_g$置换基$X$的诸元素并且$X$中没有基元被$\alpha_g$所固定。于是，$\alpha_g$对于基$X$的方阵$M_g$可以从单位方阵$I_n$经过适当的行置换（没有行保持不动）

而得到（见定理VII.1.2)。由于M_u的迹TrM_u是M_u中主对角元素之和，从而不难看出

(i) 当$g\in G$，$g\neq e$时，$TrM_g=0$；

(ii) $M_e=I_n$，从而$TrM_e=n1_K$；

(iii) 如果$u=k_1g_1+\cdots+k_ng_n\in K(G)$，则

$$\alpha_u=\sum_{i=1}^{n}k_i\alpha g_i,\quad TrM_u=\sum_{i=1}^{n}k_iTrM_{gi}.$$

如果$K(G)$的根J不为0，则有非零元素$v\in J$，$v=k_1g_1+\cdots+k_ng_n$。我们可以假设$g_1=e$和$k_1=1_K$（否则设$k_i\neq 0$，我们将v换成$k_i^{-1}g_i^{-1}v$然后重新赋以下标)。因为$K(G)$在K上是有限维的，$K(G)$是左Artin 代数（习题2)。从而由命题2.13 (对于代数而言)。可知J是幂零根。从而$v\in J$为幂零元素，于是α_v是幂零的。由定理VII.1.3知M_v为幂零方阵。因此$TrM_v=0$(习题 VII.5.10) 另一方面，上面的(i)—(iii)导致

$$TrM_v=\sum_{i=1}^{n}k_iTrMg_i=1_KTrM_e+\sum_{i=2}^{n}k_iTrMg_i=TrM_e+0=n1_K.$$

但是$n1_K\neq 0$，这是因为$\mathrm{char}K=0$或者$\mathrm{char}K=p$ 而 $p\nmid|G|=n$。这就导出矛盾。因此$J=0$，即$K(G)$是半单的。

反之，设$\mathrm{char}K=p$，而$p|n$。以w表示$K(G)$ 中基X的所有元素之和，即 $w=g_1+g_2+\cdots+g_n\in K(G)$。显然 $w\neq 0$。易知对于每个$g\in G$均有 $wg=gw$，从而W在$K(G)$的中心之中。证明 $w^2=nw=(n1_K)w$，从而 $w^2=0$(因为$p|n$)。因此 $(K(G)w)(K(G)w)=0$。从而非零左理想$K(G)w$是幂零理想。由定理2.12知 $K(G)w\subset J$。于是$J\neq 0$。即$K(G)$不是半单的。∎

下面一个系（取K 为复数域）在研究有限群的表示和特征时

是很有用处的.

系5.9 设$K(G)$为代数封闭域K上有限群G的群代数. 如果$\mathrm{char}K=0$或者$\mathrm{char}K=p$并且$p\nmid|G|$,则存在正整数$n_1,\cdots,n_t$和K-代数同构

$$K(G)\cong \mathrm{Mat}_{n_1}K\times\cdots\times \mathrm{Mat}_{n_t}K.$$

证明 由于G为有限群, $K(G)$是有限维K-代数, 从而为左Artin代数 (习题2), 然后利用定理5.7和命题5.8即可. ∎

习 题

注: K永远为含幺交换环而A为K-代数.

1. 习题IV.7.4中的$\mathbf{Q}$-代数A是左Artin $\mathbf{Q}$-代数, 但不是左Artin环.
2. 域K上有限维代数同时满足左和右代数理想的升链条件和降链条件.
3. (*a*) 如果M为左代数A-模, 则$\mathscr{A}(M)=\{r\in A\mid rc=0,$对于每个$c\in M\}$是$A$的代数理想.

   (*b*) A中的代数理想P叫作本原的,是指商代数R/P是本原的 (即它有忠实单的代数R/P-模). 求证每个本原代数理想都是环A的本原理想, 并且反之亦然.
4. 设M是单的代数A-模.则

   (*a*) $D=\mathrm{Hom}_A(M,M)$是K上的除法代数, 其中$\mathrm{Hom}_A(M,M)$表示代数A-模M的全部自同态.

   (*b*) M为左代数D-模.

   (*c*) M的D-代数自同态环$\mathrm{Hom}_D(M,M)$是一个K-代数.

   (*d*) 由$r\mapsto a_r$(其中$a_r(x)=rx$)给出的映射$A\to\mathrm{Hom}_D(M,M)$是K-代数同态.
5. 设A为域K上的可数无限阶方阵 (每个方阵均只有有限个元素不为0)所构成的集合 (方阵的行和列均以$\mathbf{N}^*$为下标集合).

求证

(*a*) A为单K-代数.

(*b*) A为无限维代数性K-代数.

6. 域K上代数性代数A的根J是诣零根.

[提示：如果$r\in J$并且$k_nr^n+k_{n-1}r^{n-1}+\cdots+k_1r^t=0(k_t\neq 0)$，则$r^t=r^tu$，其中$u=-k_t^{-1}k_nr^{n-t}-\cdots-k_t^{-1}k_{t+1}r$，从而$-u$为右拟正规元素．设$-u+v-uv=0$，求证$0=r^t(-u+v-uv)=-r^t$.]

7. 设A为K-代数而C为环A的中心.求证

(*a*) C为A的K-子代数.

(*b*) 如果K是代数封闭域而A是有限维半单代数，则A的单分支的个数t(见定理5.7)恰好等于$\dim_K C$.

6. 除法代数

我们首先研究域上一些单代数，然后转入特殊情形，即域上除法代数．我们要证明，除法代数的极大子域对于该除法代数的结构有很大的影响．最后证明Noether-Skolem定理(6.7)．而起源于Frobenius和Wedderburn的两个著名定理均是Noether-Skolem定理的系(系6.8和6.9)．在本节中，我们大量地使用了代数的张量积(第IV.7节)．

定义6.1 域K上含幺代数A叫作中心单代数，是指A为单K-代数并且A的中心恰好为K.

例 设D为除法代数而K是D的中心．不难证明，如果$d\in K$，$d\neq 0$，则$d^{-1}\in K$．从而K为域．显然D是K上的代数(K的作用即是D中原来的乘法)．进而，由于D为含幺单环，它也是单代数.

因此D是K上的中心单代数。

我们知道，如果A 和B均是含幺 K-代数，则它们的张量积 $A\otimes_K B$也是如此(定理IV.7.4)。$a\otimes b$和$a_1\otimes b_1$的乘积为 $aa_1\otimes bb_1$。此后，我们将集合$\{1_A\otimes b\mid b\in B\}$ 和$\{a\otimes 1_B\mid a\in A\}$ 分别表示为$1_A\otimes_K B$和$A\otimes_K 1_B$。注意$A\otimes_K B=(A\otimes_K 1_B)(1_A\otimes_K B)$。

定理6.2 如果A 是域 K上的中心单代数而 B 为含幺单 K-代数，则$A\otimes_K B$为单K-代数。

证明 由于B为K上向量空间，它有一组基Y,并且从定理IV.5.11可知$A\otimes_K B$中元素u均可写成$\sum_{i=1}^{n} a_i\otimes y_i$，其中$y_i\in Y$而$a_i$是唯一确定的。如果$U$为$A\otimes_K B$ 中非零理想，取$0\neq u\in U$使得$u=\sum_{i=1}^{n} a_i\otimes y_i$，其中$a_i$ 均不为0并且n达到极小值。由于A 为含幺单代数而Aa_1A为A的非零理想，从而$Aa_1A=A$。于是有元素$r_1,\cdots,r_t$，$s_1,\cdots,s_t\in A$，使得$1_A=\sum_{j=1}^{t} r_j a_1 s_j$。由于$U$ 是理想，从而 $v=\sum_{j=1}^{t}(r_j\otimes 1_B)u(s_j\otimes 1_B)$属于$U$。现在

$$
\begin{aligned}
v &= \sum_j (r_j\otimes 1_B)\Big(\sum_i a_i\otimes y_i\Big)(s_j\otimes 1_B)\\
&= \sum_i \Big(\sum_j r_j a_i s_j\Big)\otimes y_i\\
&= \sum_j r_j a_1 s_j\otimes y_1+\sum_{i=2}^{n}\Big(\sum_j r_j a_i s_j\Big)\otimes y_i\\
&= 1_A\otimes y_1+\sum_{i=2}^{n}\bar{a}_i\otimes y_i,
\end{aligned}
$$

其中 $\bar{a}_i = \sum_{j=1}^{t} r_j a_i s_j$。由$n$的极小性可知 $i \geqslant 2$时 $\bar{a}_i \neq 0$。如果$a \in A$，

则元素$w = (a \otimes 1_B)v - v(a \otimes 1_B) \in U$，并且

$$w = \left(a \otimes y_1 + \sum_{i=2}^{n} a\bar{a}_i \otimes y_i\right) - \left(a \otimes y_1 + \sum_{i=2}^{n} \bar{a}_i a \otimes y_i\right)$$

$$= \sum_{i=2}^{n} \left(a\bar{a}_i - \bar{a}_i a\right) \otimes y_i.$$

由n的极小性可知$w = 0$，并且$i \geqslant 2$时$a\bar{a}_i - \bar{a}_i a = 0$。因此对于每个$a \in A$均有$a\bar{a}_i = \bar{a}_i a$，即$\bar{a}_i$均属于$A$的中心。由假定$A$的中心为$K$，从而$\bar{a}_i$均属于$K$，于是

$$v = 1_A \otimes y_1 + \sum_{i=2}^{n} \bar{a}_i \otimes y_i = 1_A \otimes y_1 + \sum_{i=2}^{n} 1_A \otimes \bar{a}_i y_i = 1_A \otimes b.$$

其中$b = y_1 + \bar{a}_2 y_2 + \cdots + \bar{a}_n y_n \in B$。

由于每个$\bar{a}_i$均不为0，而y_i在K上线性无关，从而$b \neq 0$。由于B有1_B，再由B的单性即知$BbB = B$。因此

$$1_A \otimes_K B = 1_A \otimes_K BbB = (1_A \otimes_K B)(1_A \otimes_K b)(1_A \otimes_K B)$$
$$= (1_A \otimes_K B)v(1_A \otimes_K B) \subset U.$$

从而

$$A \otimes_K B = (A \otimes_K 1_B)(1_A \otimes_K B) \subset (A \otimes_K 1_B)U \subset U.$$

因此$U = A \otimes_K B$，即$A \otimes_K B$只有一个非零理想。由于$A \otimes_K B$有幺元素$1_A \otimes 1_B$，从而$(A \otimes_K B)^2 \neq 0$，于是$A \otimes_K B$是单代数。∎

现在我们考虑体。假设D是体，F是D的子环。如果$1_D \in F$并且F为域，我们称F是D的子域。显然D是任一子域F上的向量空间。D的子域F叫作极大子域，是指它不真包含在D的任一其他子域之中。极大子域永远是存在的（习题4）。D的每个极大子域必

然包含D的中心K（不然的话，F和K将要生成D的一个比F大的子域，见习题3）。不难看出，F事实上是单K-代数。正如下面定理所指出的，体的极大子域对于体本身的结构有很大影响。

定理6.3 设D为体，K和F分别是它的中心和极大子域。则作为K-代数，$D\otimes_K F$同构于$\mathrm{Hom}_F(D,D)$的一个稠子代数，这里D看成F上向量空间。

证明 $\mathrm{Hom}_F(D,D)$是F-代数（定义IV.7.1后面第三个例子），从而也是K-代数。对于每个$a\in D$，令α_a：$D\to D$，$\alpha_a(x)=xa$。对于每个$c\in F$令β_C：$D\to D$，$\beta_c(x)=cx$。验证$\alpha_a,\beta_c\in\mathrm{Hom}_F(D,D)$，并且对于每个$a\in D,c\in F$均有$\alpha_a\beta_c=\beta_c\alpha_a$。验证映射$D\times F\to\mathrm{Hom}_F(D,D)$，$(a,c)\longmapsto\alpha_a\beta_c$是$K$-双线性映射。由定理IV.5.6知这个映射诱导出一个K-模同态θ：$D\otimes_K F\to\mathrm{Hom}_F(D,D)$，使得

$$\theta\Big(\sum_{i=1}^{n}a_i\otimes c_i\Big)=\sum_{i=1}^{n}\alpha_{c_i}\beta_{c_i}\quad(a_i\in D,\ c_i\in F)$$

验证θ为K-代数同态，并且θ不为零（因为$\theta(1_D\times 1_F)$是D上的恒等映射）。由于D是中心单代数而F为单K-代数，由定理6.2可知$D\otimes_K F$为单代数。因为$\theta\neq 1$而$\mathrm{Ker}\,\theta$为代数理想，从而$\mathrm{Ker}\,\theta=0$。于是θ为单同态。因此$D\otimes_K F$同构于$\mathrm{Hom}_F(D,D)$的K-子代数$\mathrm{Im}\,\theta$。我们还需证明$A=\mathrm{Im}\theta$在$\mathrm{Hom}_F(D,D)$中稠。

显然D为$\mathrm{Hom}_F(D,D)$上的左模，其中$fd=f(d)$（$f\in\mathrm{Hom}_F(D,D)$，$d\in D$）。从而D为$A=\mathrm{Im}\theta$上的左模。如果d为D的非零元素，则由于D是体，我们有

$$\begin{aligned}Ad&=\{\theta(u)(d)\mid u\in D\otimes_K F\}\\&=\Big\{\sum_i c_i d a_i\mid i\in N^*,\ c_i\in F,\ a_i\in D\Big\}=D.\end{aligned}$$

从而D没有非平凡A-子模，即D为单A-模．进而，D为忠实A-模（因为若$f\in \mathrm{Hom}_F(D,D)$并且$fD=0$，则f必为零映射）．于是由稠性定理1.12可知 A 同构于 $\mathrm{Hom}_\Delta(D,D)$ 的稠子环，其中 Δ 为体 $\mathrm{Hom}_A(D,D)$而D为左Δ-向量空间．在单同态$A\to \mathrm{Hom}_\Delta(D,D)$ 之下，$f\in A$的象作为$\mathrm{Hom}_\Delta(D,D)$中元素仍然是f．

我们现在构作环同构$F\cong\Delta$．设β：$F\to\Delta=\mathrm{Hom}_A(D,D)$ 是由$c\longmapsto\beta_c$（记号同前）所给出的映射．验证$\beta_c\in\Delta$，并且β是环的单同态．如果$f\in\Delta$而$x\in D$，则$\alpha_x=\theta(x\otimes 1_D)\in A$，并且

$$f(x)=f(1_Dx)=f[\alpha_x(1_D)]=\alpha_x(f(1_D))=f(1_D)x=\beta_c(x),$$

其中$c=f(1_D)$．为证β是满同态，只需证$c\in F$．因为在这种情形下，对于每个$x\in D$均有$f(x)=cx=\beta_c(x)$，从而$f=\beta_c=\beta(c)$．如果$y\in F$，则$\beta_y=\theta(1_D\otimes y)\in A$，而$\alpha_y=\theta(y\otimes 1_D)\in A$，同时

$$\begin{aligned}cy&=f(1_D)y=\alpha_y(f(1_D))=f(\alpha_y(1_D))=f(1_Dy)=f(y1_D)\\&=f(\beta_y(1_D))=\beta_yf(1_D)=\beta_y(c)=yc.\end{aligned}$$

因此C与F中每个元均可交换．如果$c\notin F$，则c和F 生成D 的一个子域，它真包含极大子域F（习题3），这就导致矛盾．从而 $c\in F$．因此β：$F\cong\Delta$．

为了完成证明，令$v_1,\cdots,v_n\in D$而$\{u_1,\cdots,u_n\}$是D 的F-线性无关子集合．我们证明 $\{u_1,\cdots,u_n\}$ 也是 Δ- 线性无关的：如果

$\sum_{i=1}^{n}g_iu_i=0$ $(g_i\in\Delta)$，则

$$0=\sum g_iu_i=\sum\beta c_i(u_i)=\sum c_iu_i,$$

其中$c_i\in F$，而$g_i=\beta(c_i)=\beta_{c_i}$，由$\{u_1,\cdots,u_n\}$ 的F-线性无关性导致c_i均为0，从而$g_i=\beta(0)=0$（对于每个i）．因此 $\{u_1,\cdots,u_n\}$ 是Δ-线性无关的．由于A在$\mathrm{Hom}_\Delta(D,D)$ 中稠（定义1.7），存在

$h \in A$，使得对于每个i均有$h(u_i) = v_i$。因此A在$\mathrm{Hom}_F(D, D)$中稠。∎

定理6.3有一个很有趣的推论。但是这需要两个预备性引理。

引理6.4 设A为域K上含幺代数，而域$F \supset K$，则$A \otimes_K F$是F-代数并且$\dim_K A = \dim_F(A \otimes_K F)$。

证明概要 由于F是域，从而K-F双重模$A \otimes_K F$是F上向量空间，其中$b(a \otimes b_1) = (a \otimes b_1)b = a \otimes b_1 b (a \in A, b, b_1 \in F$，见定理IV.5.5和随后的注记)。根据定理IV.7.4，$A \otimes_K F$是K-代数，易知它也是F-代数。如果X为A的一组K-基，由定理IV.5.11(的一个显然的模拟)，$A \otimes_K F$中每个元素均可写成

$\sum_i x_i \otimes c_i = \sum_i (x_i \otimes 1_F)c_i = \sum_i c_i(x_i \otimes 1_F)$ $(x_i \in X, c_i \in F)$。其中元素x_i和c_i是唯一确定的。由此可知

$$X \otimes_K 1_F = \{x \otimes 1_F \mid x \in X\}$$

是$A \otimes_K F$的一组F-基。显然$\dim_K A = |X| = |X \otimes_K 1_F| = \dim_F(A \otimes_K F)$。∎

引理6.5 设D是域K上的除法代数，A为含幺的有限维K-代数，则$D \otimes_K A$是左Artin$K$-代数。

证明概要 $D \otimes_K A$为D上向量空间，其中$d \in D$在$D \otimes_K A$的生成元$d_1 \otimes a$上的作用为$d(d_1 \otimes a) = dd_1 \otimes a = (d \otimes 1_A)(d_1 \otimes a)$(定理IV.5.5)。因此$D \otimes_K A$的每个左理想也是$D \otimes_K A$的$D$-子空间。引理6.4的证明在这里仍然有效，从而$\dim_D(D \otimes_K A) = \dim_K A$。由于右边是有限的，对于维数作通常的归纳推理可知$D \otimes_K A$是左Artin代数。∎

定理6.6 设D是体，K和F分别是它的中心和极大子域。则$\dim_K D$有限$\Leftrightarrow\dim_K F$有限。并且在这种情形下，$\dim_F D=\dim_K F$，$\dim_K D=(\dim_K F)^2$。

证明 如果$\dim_K F$是无限的，则$\dim_K D$亦然。如果$\dim_K F$是有限的，由引理6.5可知$D\otimes_K F$为左Artink-代数。从而由定理6.3即知$D\otimes_K F$同构于$\mathrm{Hom}_F(D,D)$的一个左Artin稠子代数。由定理6.3的证明可知这个同构实际上是F-代数同构。于是存在F-代数同构$D\otimes_K F\cong\mathrm{Hom}_F(D,D)$，而根据定理1.9可知$n=\dim_F D$有限。因此由定理VII.1.4（及其随后的注记）可知$D\otimes_K F\cong\mathrm{Hom}_F(D,D)\cong\mathrm{Mat}_n F$。现在由引理6.4推出

$\dim_K D=\dim_F(D\otimes_K F)=\dim_F(\mathrm{Mat}_n F)=n^2=(\dim_F D)^2$。另一方面，由定理IV.2.16可知$\dim_K D=(\dim_F D)(\dim_K F)$。因此$\dim_K F=\dim_F D$。∎

我们知道，如果u为含幺环R中的单位，则由$r\longmapsto uru^{-1}$给出的映射$R\to R$是环的自同构。这叫作由u诱导出的内自同构。

定理6.7 (Noether—Skolem) 设R为左Artin单环，K是R的中心（从而R为K-代数）。令A和B是R的有限维单K-子代数，并且均包含K。如果$\alpha:A\to B$是K-代数同构，并且使K的元素不动，则α可扩充成R的一个内自同构。

证明 由Wedderburn—Artin定理1.14，我们无妨设$R=\mathrm{Hom}_D(V,V)$，其中V为体D上的n维向量空间。定理VII.1.3后面的注记表明，存在着环上的反自同构$R=\mathrm{Hom}_D(V,V)\to\mathrm{Mat}_n D$。在这个映射之下，$R$的中心必然同构地映到$\mathrm{Mat}_n D$的中心之上。但是$\mathrm{Mat}_n D$的中心同构于$D$的中心（习题VII.1.3），从而我们可以把$K$等同于$D$的中心，即$D$是中心单$K$-代数。

注意V是左R-模，其中 $rv=r(v)$ $(v\in V,\ r\in R=\mathrm{Hom}_D(V,V))$。由于$V$为左$D$-向量空间，从而$V$为$K$-代数$D\otimes_K R$上的左（代数）模，其中$D\otimes_K R$的生成元$d\otimes r$在$v\in V$上的作用由下式给出

$$(d\otimes r)v=d(rv)=d(r(v))=r(dv) \tag{i}$$

如果$\bar{A}$是$D\otimes_K R$的子代数$D\otimes_K A$，则V显然为左$\bar{A}$-模。类似地，如果$\bar{B}=D\otimes_K B$，则V是左$\bar{B}$-模。现在映射$\bar{\alpha}=1_D\otimes\alpha:\bar{A}\to\bar{B}$是$K$-代数同构。从而沿着$\bar{\alpha}$拉回之后，又给出$V$的第二个$\bar{A}$-模结构（即对于$v\in V$和$\bar{a}\in\bar{A}$，定义$\bar{a}v=\bar{\alpha}(\bar{a})v$）。在这第二个$\bar{A}$-模结构之下，$\bar{A}=D\otimes_K A$的生成元$d\otimes r$在$v\in V$上的作用由下式给出

$$\begin{aligned}(d\otimes r)v&=\bar{\alpha}(d\otimes r)v=(d\otimes\alpha(r))v=d(\alpha(r)(v))\\&=\alpha(r)(dv).\end{aligned} \tag{ii}$$

由定理6.2和引理6.5可知$\bar{A}$为单左Artin K-代数。从而由定理3.10可知，不计同构则只有一个单$\bar{A}$-模。现在由定理3.7，V对于$\bar{A}$-模结构(i)或者(ii)都是半单模，从而有$\bar{A}$-模同构。

$$V=\sum_{i\in I}U_i\ \text{（对应于结构 (i)），以及}\tag{iii}$$

$$V=\sum_{j\in J}W_j\ \text{（对应于结构 (ii)）}\tag{iv}$$

其中U_i，W_j均为单$\bar{A}$-模，而$U_i\cong W_j$（对于所有i，j）。由于$dv=(d\otimes 1_R)v$ $(d\in D,\ v\in V)$，从而V的每个$\bar{A}$-子模均是V的D-子空间，而每个$\bar{A}$-模同构都是D-向量空间同构。由于$\dim_D V=n$是有限的，从而U_i，W_j在D上都是有限维的，维数为t，而下标集合I和J也均是有限集合。设

$$I=\{1,\ 2,\ \cdots,\ m\},\ J=\{1,\ 2,\ \cdots,\ s\}.$$

于是

$$\dim_D V = \dim_D\Big(\sum_{i=1}^{m} U_i\Big) = \sum_{i=1}^{m} \dim_D U_i = mt,$$

$$\dim_D V = \dim_D\Big(\sum_{j=1}^{s} W_j\Big) = \sum_{j=1}^{s} \dim_D W_j = st.$$

从而$m = s$. 由于对于所有i, j均有$U_i \cong W_j$, 从而$\sum_{i=1}^{m} U_i \cong \sum_{j=1}^{m} W_j$.

将此同构与上面的同构 (iii) 和 (iv) 合在一起，便给出具有$\bar{A}$-模结构(i)的V 和具有$\bar{A}$-模结构 (ii) 的V之间的$\bar{A}$-模同构β. 从而对于每个$\bar{a} \in \bar{A}$和 $v \in V$均有

$$\beta(\bar{a}\, v) = \bar{\alpha}(\bar{a})(\beta(v)).$$

特别地，对于$d \in D$和$\bar{d} = d \otimes 1_A \in \bar{A}$，我们有

$$\beta(dv) = \beta(\bar{d}v) = \bar{\alpha}(\bar{d})(\beta(v)) = (d \otimes 1_B)\beta(v) = d\beta(v).$$

于是$\beta \in \mathrm{Hom}_D(V, V) = R$. 由于$\beta$为同构，从而$\beta$为$R$ 中单位. 进而，对于$r \in A$和$\bar{r} = 1_D \otimes r \in \bar{A}$，我们有

$$\begin{aligned}\beta r(v) = \beta[r(v)] = \beta[\bar{r}\, v] &= \bar{\alpha}(\bar{r})\beta(v)\\ &= (1_D \otimes \alpha(r))\beta(v) = \alpha(r)[\beta(v)]\\ &= [\alpha(r)\beta](v).\end{aligned}$$

于是在$R = \mathrm{Hom}_D(V, V)$中我们有$\beta r = \alpha(r)\beta$. 换句话说，

$$\beta r \beta^{-1} = \alpha(r) \quad (\text{对于每个} r \in A).$$

因此，R中由β诱导出来的内自同构为映射α: $A \to B$的扩充. ∎

下面系中提到的实四元数除法代数，其定义参见定义III.1.5后的例5和定义III.7.1后的例5.

系6.8 (Frobenius) 设D 为实数域$\boldsymbol{R}$上的代数性除法代数. 则D同构于$\boldsymbol{R}$，复数域$\boldsymbol{C}$，或者是实四元数除法代数$\boldsymbol{T}$.

证明概要 设K为D的中心而F是D的极大子域. 我们有 $\boldsymbol{R}\subset K\subset F\subset D$. 其中$F$是$\boldsymbol{R}$的代数扩域. 由系$V.3.20$知$\dim_K F\leqslant\dim_{\boldsymbol{R}}F\leqslant 2$. 又由定理 6.6知 $\dim_F D=\dim_K F$, $\dim_K D=(\dim_K F)^2$. 从而只能有$\dim_K D=1$和$\dim_K D=4$两种情形. 如果$\dim_K D=1$, 则 $D=F$并且由系$V.3.20$可知D同构于$\boldsymbol{R}$或者$\boldsymbol{C}$.

如果$\dim_K D=4$, 则$\dim_K F=2=\dim_F D$, 从而$K=\boldsymbol{R}$, 而由系$V.3.20$可知F同构于$\boldsymbol{C}$. 进而, D是非交换的, 否则D便为代数封闭域$\boldsymbol{C}$的真代数扩域. 由于F同构于$\boldsymbol{C}$, 从而有$i\in F$使得$i^2=-1$, 并且$F=\boldsymbol{R}(i)$. 由$a+bi\longmapsto a-bi$给出的映射$F\to F$是F 的非平凡自同构, 并且固定$\boldsymbol{R}$中每个元素. 根据定理 6.7, 它可扩充成D的一个内自同构β, 即$\beta(x)=dxd^{-1}$, 其中d为D 中某个非零元素.

由于$-i=\beta(i)=did^{-1}$, 所以$-id=di$, 从而$id^2=d^2i$. 于是$d^2\in D$与$F=\boldsymbol{R}(i)$中每个元素均可交换. 因此$d^2\in F$ (否则d^2 和F将会生成D的一个子域, 并且这个子域真包含极大子域F). 由于F中被β固定的元素均属于$\boldsymbol{R}$, 而$\beta(d^2)=dd^2d^{-1}=d^2$, 从而$d^2\in\boldsymbol{R}$. 如果$d^2>0$, 则$d\in\boldsymbol{R}$, 而这又不可能, 因为$d\in\boldsymbol{R}$导致$\beta$ 为恒等映射. 于是存在某个非零元素$r\in\boldsymbol{R}$使得$d^2=-r^2$, 从而 $(d/r)^2=-1$. 令$j=d/r$而$k=ij$. 验证$\{1, i, j, k\}$是D的一组$\boldsymbol{R}$-基, 从而有$\boldsymbol{R}$-代数同构$D\cong\boldsymbol{T}$. ∎

系6.9 (Wedderburn) 有限体D必为域.

注记: 习题$V.8.10$给出这一事实的初等证明 (利用分圆多项式).

证明 设K为D的中心而F是任一极大子域. 由定理 6.6 我们有$\dim_K D=n^2$, 其中 $n=\dim_K F$. 从而每个极大子域均是有限域, 其阶为q^n, 而$q=|K|$. 因此, 任意两个极大子域F和F' 均是同构

的，并且可选取同构β：$F\to F'$固定K中每个元素（系V.5.8）。根据定理6.7，β由D中一个内自同构给出。于是有某个非零元素$a\in D$，使得$F'=aFa^{-1}$。

如果$u\in D$，则$K(u)$为D的子域（习题3）。从而$K(u)$包含在某个极大子域之中，即存在某个$a\in D$使得$K(u)\subset aFa^{-1}$。因此$D=\bigcup_{0\neq a\in D} aFa^{-1}$，而$D^*=\bigcup_{a\in D^*} aF^*a^{-1}$。（其中$D^*$和$F^*$分别为$D$和$F$中非零元素组成的乘法群）。根据下面的引理6.10可知这只可能有$F=D$。∎

引理6.10 如果G为有限（乘法）群而H是它的真子群，则$\bigcup_{x\in G} xHx^{-1}\subsetneq G$。

证明 H有$[G:N]$个共轭子群，其中N为H在G中的正规化子（系II.4.4）。由于$H<N<G$而$H\neq G$，从而$[G:N]\leqslant[G:H]$并且$[G:H]>1$。设r为$\bigcup_{x\in G} xHx^{-1}$中不同元素个数，则由于$[G:H]>1$所以

$$r\leqslant 1+(|H|-1)[G:N]\leqslant 1+(|H|-1)[G:H]$$
$$=1+|H|[G:H]-[G:H]=1+|G|-[G:H]<|G|.$$ ∎

习　题

1. 如果A是域K上有限维中心单代数，则$A\otimes_K A^{op}\cong \mathrm{Mat}_n K$，其中$n=\dim_K A$而$A^{op}$的定义见习题III.1.17。
2. 如果A和B是域K上的中心单代数，则$A\otimes_K B$亦然。
3. 设D为体而F是D的子域。如果$d\in D$与F中每个元素均可交换，则由F和d生成的子体$F(d)$（它是D中包含F与d的全部子体之交）是一个子域

(见定义V.1.3).

4. 如果D是体，则D必存在极大子域.

5. 如果A为域K上有限维中心单代数.则$\dim_K A$是完全平方数.

6. 如果A和B是域K上的左 Artin 代数，则$A\otimes_K B$不必为左 Artin 代数.
[提示：设A为除法代数，中心为K，极大子域为B，使$\dim_B A$无限.]

7. 如果D为它的中心K上的有限维除法代数，而F是D的极大子域，则存在K-代数同构$D\otimes_K F\cong \mathrm{Mat}_n F$，其中$n=\dim_F D$.

8. 设A是它的中心K上的有限维单代数如果A的一个自同构保持其中心元素不动，那末它必为内自同构.

9. (Dickson) 设D为除法代数，中心为K.如果a，$b\in D$ 在K上是代数的并且有相同的极小多项式，则存在$d\in D$使得$b=dad^{-1}$.

第X章　范畴理论

我们在第I.7 节就已经介绍过范畴理论，本章将要完成这 件工作。范畴与函子最早出现在Eilenberg—Maclane于四十年代的代数拓扑著作中。不久，人们就看出这些概念有极为广泛的应用。许多不同的数学课题都可以用范畴的语言加以解释，从而范畴理论中的技巧和定理能够用到这些课题中。比如，在完全不同领域中的两个证明常常使用“类似”的方法。范畴代数提供了确切表达这些相似性的手段。这样一来，往往可以给出一个范畴方式的证明，使得原先两个不同领域中的已知结果均是它的特殊情形。这个统一化过程提供了一种手段，使我们能够加深理解数学宽广的领域和新的课题，只要这些领域和课题的基础部分可以用范畴语言表达出来。

在本书中，我们主要按上述方式来使用范畴理论，即是说作为一种方便的统一化语言。但是近年来，范畴理论本身作为一种数学原则开始出现。现在，促使范畴理论发展的源泉，在很大程度上来自这一理论本身。范畴理论这种广阔的发展在本章中只简略地提到。

第 1 节充分讨论函子和自然变换这些基本概念。可表函子（第 1 节）和函子的伴随对（第 2 节）是两种特别重要类型的函子。第 3 节是将已知范畴（如环上模的范畴）中的一些概念尽

可能多地移植到任意范畴中。

本章依赖于第I.7 节，但是除了某些例子之外，它与本书其余部分是无关的。第 1 节和第 3 节本质上是彼此独立的。第 1 节是为第 2 节作准备。

1. 函子和自然变换

正如我们在前几章中所经常看到的，任何数学对象的研究均需要考虑这些对象之间的“映射”。现在我们的数学对象是“范畴”（第I.7节）。而函子可以粗略地描绘成从一个范畴到另一范畴的“映射”并保持适当的结构。而自然变换又是从一个函子到另一函子的“映射”。

开始我们先定义协变函子和反变函子，并给出大量例子。然后引进自然变换以及更多的例子。本节的最后部分谈范畴理论中一类最重要的函子，即可表函子。

读者应当复习一下范畴的基本性质（第I.7节），特别是泛对象这一概念（它在研究可表函子时是需要的）。我们常常同时处理许多范畴。因而，如果A和B是范畴$\mathscr{C}$中的对象，则$\mathscr{C}$中从A到B的全部态射(morphism) 所成的集合有时表示成$\hom_{\mathscr{C}}(A, B)$，而不是象过去那样只写成$\hom(A, B)$。

定义1.1 设$\mathscr{C}$和$\mathscr{D}$均是范畴。从$\mathscr{C}$到$\mathscr{D}$的一个协变函子T（表示成$T:\mathscr{C}\to\mathscr{D}$）是指一对函数（均表示成$T$）：一个是对象函数，即将$\mathscr{C}$中每个对象$C$对应于$\mathscr{D}$中一个对象$T(C)$，另一个是态射函数，即将$\mathscr{C}$中每个态射$f:C\to C'$对应于$\mathscr{D}$中一个态射$T(f)$：$T(C)$

$\to T(C')$，使得：

(i) 对于$\mathscr{C}$中每个恒等态射1_C，均有$T(1_C)=1_{T(C)}$；

(ii) 对于$\mathscr{C}$中任意两个态射f和g，均有$T(g\circ f)=T(g)\circ T(f)$，只要合成运算$g\circ f$是可定义的。

例 (协变)恒等函子$I_{\mathscr{C}}:\mathscr{C}\to\mathscr{C}$，即将范畴$\mathscr{C}$的每个对象和态射均映成自身。

例 设R是环而A是一个固定的左R-模。对于每个R-模C，令$T(C)=\mathrm{Hom}_R(A,C)$。对于每个R-模同态$f:C\to C'$，以$T(f)$表示通常的诱导映射$\bar{f}:\mathrm{Hom}_R(A,C)\to\mathrm{Hom}_R(A,C')$(见定理IV.4.1后面的注记)。则$T$是从左$R$-模范畴到Abel群范畴的协变函子。

例 更一般地，设A为范畴$\mathscr{C}$中一个固定的对象。如下定义从$\mathscr{C}$到集合范畴&的协变函子h_A：对于$\mathscr{C}$中对象C，令$h_A(C)=\mathrm{hom}(A,C)$(即$\mathscr{C}$中从A到C的全部态射)；如果$f:C\to C'$是$\mathscr{C}$中的态射，令$h_A(f):\mathrm{hom}(A,C)\to\mathrm{hom}(A,C')$是由$g\longmapsto fog$ $(g\in\mathrm{hom}(A,C))$给出的函数。函子h_A叫作协变hom函子。后面还要对这个函子作进一步讨论。

例 可以用下述方式定义一个从集合范畴到含幺环R上左模范畴的协变函子F：对于每个集合X，$F(X)$是X上的自由R-模(见定理IV.2.1后面的注记)。如果$f:X\to X'$是一个函数，以$F(f):F(X)\to F(X')$表示由$\bar{f}\,i=f$唯一决定的模同态$\bar{f}:F(X)\to F(X')$，其中i是嵌入映射$X\to F(X)$(定理IV.2.1)。

例 设$\mathscr{C}$是一个具体范畴(定义I.7.6)，例如左R-模范畴，群范畴或者是环范畴。如下定义从$\mathscr{C}$到集合范畴$\mathscr{S}$的(协变)忘却函子：将每个对象A对应于它的凭借集合(仍表示成A)，而将每个态射$f:A\to A'$对应于函数$f:A\to A'$(见定义I.7.6)。

定义1.2 设$\mathscr{C}$和$\mathscr{D}$均是范畴. 从$\mathscr{C}$到$\mathscr{D}$的一个反变函子S(表示成S: $\mathscr{C}\longrightarrow\mathscr{D}$)是指一对函数. (均表示成 S): 一个是对象函数, 即将$\mathscr{C}$中每个对象C对应于$\mathscr{D}$中一个对象$S(C)$;另一个是态射函数, 即将$\mathscr{C}$中每个态射$f:C\longrightarrow C'$对应于 $\mathscr{D}$ 中一个态射$S(f):S(C')\longrightarrow S(C)$. 使得

(i) 对于$\mathscr{C}$中每个恒等态射1_C, 均有$S(1_C)=1_{S(C)}$;

(ii) 对于$\mathscr{C}$中任意两个态射f和g,均有 $S(g\circ f)=S(f)\circ S(g)$, 只要合成运算$g\circ f$是可定义的.

由此可知,反变函子S: $\mathscr{C}\longrightarrow\mathscr{D}$的态射函数将态射的方向反转.

例 设R为环而B是一个固定的左R-模. 如下定义从左R-模范畴到Abel群范畴的反变函子S: 对于每个R-模 C, 定义$S(C)=\mathrm{Hom}_R(C, B)$. 如果$f$: $C\longrightarrow C'$是R-模同态, 则$S(f)$是诱导映射 $\bar{f}\,\mathrm{Hom}_R(C', B)\longrightarrow\mathrm{Hom}_R(c, B)$(见定理IV.4.1后面的注记).

例 更一般地, 设B是范畴$\mathscr{C}$中一个固定对象. 如下定义从$\mathscr{C}$到集合范畴$\mathscr{S}$的反变函子 h^B: 对于$\mathscr{C}$ 中对象 C, 令 $h^B(C)=\mathrm{hom}(C,B)$(即$\mathscr{C}$中从 C到B的全部态射); 如果 f: $C\longrightarrow C'$是$\mathscr{C}$中的态射, 令$h^B(f)$: $\mathrm{hom}(C', B)\longrightarrow\mathrm{hom}(C, B)$ 是由 $g\longmapsto g\circ f(g\in\mathrm{hom}(C', B))$给出的函数. 函子$h^B$叫作反变hom函子.

下面方法可以用来将反变函子的研究归结为对协变函子的研究. 如果$\mathscr{C}$是一个范畴, 我们如下定义 $\mathscr{C}$的一个反向(或者对偶)范畴,表示成$\mathscr{C}^{OP}$: $\mathscr{C}^{OP}$的对象与$\mathscr{C}$的对象相同. $\mathscr{C}^{OP}$中从A到B的态射集合$\mathrm{hom}_{\mathscr{C}^{OP}}(A, B)$ 定义为$\mathscr{C}$中从B到A的态射集合$\mathrm{hom}_{\mathscr{C}}(B, A)$. 如果将态射$f\in\mathrm{hom}_{\mathscr{C}}(B, A)$ 考虑成是$\mathrm{hom}_{\mathscr{C}^{OP}}(A, B)$中态射的时候, 我们将它表示成$f^{OP}$. $\mathscr{C}^{OP}$中态射的合成定义为

$$g^{OP}\circ f^{OP}=(f\circ g)^{OP}.$$

如果S：$\mathscr{C}\longrightarrow\mathscr{D}$是反变函子，则由

$$\bar{S}(A)=S(A),\ \bar{S}(f^{OP})=S(f)$$

（对于$\mathscr{C}$中每个对象A和态射f）唯一决定了一个协变函子$\bar{S}$：$\mathscr{C}^{OP}\longrightarrow\mathscr{D}$。反之，不难看出，$\mathscr{C}^{OP}$上每个协变函子均可以从$\mathscr{C}$上的反变函子用这种办法得到。

我们知道，关于范畴中对象和态射的每个命题通过将态射反转方向都可得到一个对偶命题。由此可知：范畴$\mathscr{C}$中一个命题是对的，当且仅当它在$\mathscr{C}^{OP}$中的对偶命题是对的。所以，关于$\mathscr{C}$上对象、态射以及反变函子S的一个命题是对的，只要关于$\mathscr{C}^{OP}$上的协变函子$\bar{S}$的对应对偶命题是对的。基于此，以后我们对于许多结果只对协变函子证明，然后通过对偶化容易得出其反变情形。

为了定义多变量的函子，最方便的是引入乘积范畴的概念。如果$\mathscr{C}$和$\mathscr{D}$是范畴，它们的乘积$\mathscr{C}\times\mathscr{D}$是如下定义的范畴：对象为$(C,\ D)$，其中$C$和$D$分别是$\mathscr{C}$和$\mathscr{D}$中的对象；$\mathscr{C}\times\mathscr{D}$的态射$(C,D)\longrightarrow(C',\ D')$是$(f,\ g)$，其中$f$：$C\longrightarrow C'$，和$g$：$D\longrightarrow D'$分别是$\mathscr{C}$和$\mathscr{D}$中的态射。合成运算由$(f',\ g')\circ(f,\ g)=(f'\circ f,g'\circ g)$给出。容易证明它们满足范畴的全部公理。类似地可定义多于两个范畴的乘积。

在适当的乘积范畴上可以定义多变量的函子。这样一个函子可以对某些变量是协变的，而对另一些变量则是反变的。例如，若$\mathscr{C}$，$\mathscr{D}$，$\mathscr{E}$是范畴，那末从$\mathscr{C}\times\mathscr{D}$到$\mathscr{E}$的二变量函子$T$（对第一变量反变而对第二变量协变）定义为：其对象函数是将$\mathscr{C}\times\mathscr{D}$中每个对象$(C,\ D)$对应于$\mathscr{E}$中一个对象$T(C,\ D)$，而态射函数是将$\mathscr{C}\times\mathscr{D}$中每个态射$(f,\ g)$（其中$f$：$C\longrightarrow C'$，$g$：$D\longrightarrow D'$）对应于$\mathscr{E}$中一个态射$T(f,\ g)$：$T(C',\ D)\longrightarrow T(C,\ D')$，使得满足如下

二条件：

(i) 对于$\mathscr{C}\times\mathscr{D}$中每个对象$(C, D)$，均有$T(1_C, 1_D)=1_{T(C, D)}$；

(ii) $T(f'\circ f, g'\circ g)=T(f, g')\circ T(f', g)$，只要合成运算$f'\circ f$和$g'\circ g$分别在$\mathscr{C}$和$\mathscr{D}$中是可以定义的。

从第(ii)条件即知，如果固定$\mathscr{C}$中一个对象C，则对象函数$T(C, -)$和态射函数$T(1_C, -)$构成一个协变函子$\mathscr{D}\longrightarrow\mathscr{E}$。类似地，对于$\mathscr{D}$中一个固定的对象$D$，$T(-, D)$和$T(-, 1_D)$构成一个反变函子$\mathscr{C}\longrightarrow\mathscr{E}$。

例 $\mathrm{Hom}_R(-, -)$是从左R-模(注)范畴$\mathscr{M}$到Abel群范畴的二变量函子，它对于第一变量是反变的而对于第二变量是协变的。

例 更一般地，设$\mathscr{C}$是任一范畴。考虑如下定义的从$\mathscr{C}$到集合范畴$\mathscr{S}$的二变量函子$\hom_{\mathscr{C}}(-, -)$：$\mathscr{C}$中每一对对象(A, B)对应于集合$h_{\mathscr{C}}(A, B)$；而每一对$f: A\longrightarrow A'$和$g: B\longrightarrow B'$对应于由$h\longmapsto g\circ h\circ f$给出的函数$\hom(f, g): \hom_{\mathscr{C}}(A', B)\longrightarrow\hom_{\mathscr{C}}(A, B')$。$\hom_{\mathscr{C}}(-, -)$对于第一变量是反变的而对于第二变量是协变的。注意对于固定的对象A，$\hom_{\mathscr{C}}(A, -)$恰好是协变hom函子h_A，并且$h_A(g)=\hom(1_A, g)$。类似地，对于固定对象B，$\hom_{\mathscr{C}}(-, B)$是反变函子h^B，并且$h^B(f)=\hom(f, 1_B)$。

例 设K为含幺交换环，则由

$$T(A_1, \cdots, A_n)=A_1\otimes_K\cdots\otimes_K A_n$$

$$T(f_1, \cdots, f_n)=f_1\otimes\cdots\otimes f_n$$

给出的函子是由K-模范畴到自身的n个协变变量的函子。

如果$T_1: \mathscr{C}\longrightarrow\mathscr{D}$和$T_2: \mathscr{D}\longrightarrow\mathscr{C}$是两个函子，可以定义它

注：严格说来，$Hom_R(-, -)$应当是$\mathscr{M}\times\mathscr{M}$上的函子，但是现在通常大都说成是$\mathscr{M}$上的函子，因为这不会引起混淆。

们的合成（表示为T_2T_1），即是一个从$\mathscr{C}$到$\mathscr{B}$的函子，其对象函数和态射函数分别为

$$C\longrightarrow T_2(T_1(C)),\quad f\longrightarrow T_2(T_1(f)).$$

如果T_1和T_2同时是协变或反变的，则T_2T_1是协变的。否则T_2T_1便是反变的。

定义1.3 设$\mathscr{C}$和$\mathscr{D}$是范畴，而S：$\mathscr{C}\longrightarrow\mathscr{D}$和$T$：$\mathscr{C}\to\mathscr{D}$是两个协变函子。一个自然变换$\alpha$：$S\to T$是指一个函数，它将$\mathscr{C}$中每个对象$C$对应于$\mathscr{D}$中一个态射$\alpha_C$：$S(C)\to T(C)$，使得对于$\mathscr{C}$中每个态射$f$：$C\to C'$，下面一个$\mathscr{D}$中的图表是交换的：

$$\begin{array}{ccc} S(C) & \xrightarrow{\alpha_C} & T(C) \\ \downarrow{\scriptstyle S(f)} & & \downarrow{\scriptstyle T(f)} \\ S(C') & \xrightarrow[\alpha_{C'}]{} & T(C') \end{array}$$

如果对于$\mathscr{C}$中每个C，α_C均是等价，则称α为函子S和T的自然同构（或者自然等价）。

同样可以定义两个反变函子S，T：$\mathscr{C}\to\mathscr{D}$的自然变换或者自然同构$\beta$：$S\to T$，只是对于$\mathscr{C}$中每个态射$f$：$C\to C'$，其交换图表改成

$$\begin{array}{ccc} S(C) & \xrightarrow{\beta_C} & T(C) \\ \uparrow{\scriptstyle S(f)} & & \uparrow{\scriptstyle T(f)} \\ S(C') & \xrightarrow[\beta_{C'}]{} & T(C'), \end{array}$$

注记：两个自然变换的合成显然仍是自然变换。类似地可以定义多变量函子的自然变换。

例 如果T：$\mathscr{C}\to\mathscr{C}$为任一函子，由$C\to 1_{T(C)}$定义出一个自然同构$I_T$：$T\to T$，叫作是恒等自然同构。

例 设$\mathscr{M}$为环R上的左模范畴，T：$\mathscr{M}\to\mathscr{M}$是双重对偶函子，即是将每个模$A$对应于它的双重对偶模 $A^{**}=\mathrm{Hom}_R(\mathrm{Hom}_R(A, R), R)$。对于每个模$A$，以$\theta_A$：$A\to A^{**}$表示定理IV.4.12中的同态。则$A\mapsto\theta_A$定义出从恒等函子$\mathrm{I}_{\mathscr{M}}$到函子$T$的一个自然变换（习题IV.4.9）。如果范畴$\mathscr{M}$改成是体上有限维左向量空间范畴$\mathscr{V}$，而$T$看成是函子$\mathscr{V}\to\mathscr{V}$，则由定理IV.4.12(iii)可知$A\mapsto\theta_A(A\in\mathscr{V})$定义出从$\mathrm{I}_{\mathscr{V}}$到$T$的自然同构。还参见习题5。

自然变换往往以另一种面貌出现在某些特定的范畴中。例如在R-模范畴中（类似地在群范畴和环范畴中等等），它可以叙述成如下形式的命题：某个同态是自然的，而其中没有提到任何函子。这类被简缩了的命题的确切意义为：那里有两个（能够被明显指出的）函子，而这两个函子之间存在着自然变换。

例 如果B是含幺环R上的幺作用左模，则有模的自然同构α_B：$R\otimes_R B\cong B$（定理IV.5.7）。不难证明，对于每个模同态f：$B\to C$，图表

$$\begin{array}{ccc} R\otimes_R B & \xrightarrow{\alpha_B} & B \\ {\scriptstyle 1_R\otimes f}\downarrow & & \downarrow{\scriptstyle f} \\ R\otimes_R C & \xrightarrow[\alpha_C]{} & C \end{array}$$

是交换的。因此“自然同构”一词意味着$B\mapsto\alpha_B$定义出一个自然同构α：$T\to\mathrm{I}_{\mathscr{M}}$，其中$\mathscr{M}$为幺作用左$R$-模范畴，而$T$：$\mathscr{M}\to\mathscr{M}$是由$B\mapsto R\otimes_R B$和$f\mapsto 1_R\otimes f$给出的函子。

例 如果A，B，C是环R上的左模，则定理IV.4.7中的Abel群同构

$$\phi:\ \mathrm{Hom}_R(A\oplus B,\ C)\cong\mathrm{Hom}_R(A,\ C)\oplus\mathrm{Hom}_R(B,\ C)$$

是自然的。这里我们可以按下述方式解释“自然”一词：固定

任何两个变量，例如A和C，而对每个模同态f：$B\to B'$，图表

$$\begin{array}{ccc} \mathrm{Hom}_R(A\oplus B',C) & \xrightarrow{\phi} & \mathrm{Hom}_R(A,C)\oplus\mathrm{Hom}_R(B',C) \\ \downarrow{\scriptstyle \mathrm{Hom}(1_A\oplus f,\ 1_C)} & & \downarrow{\scriptstyle \mathrm{Hom}(1_A,1_C)\oplus \mathrm{Hom}(f,1_C)} \\ \mathrm{Hom}_R(A\oplus B,\ C) & \xrightarrow{\phi} & \mathrm{Hom}_R(A,C)\oplus\mathrm{Hom}_R(B,\ C) \end{array}$$

是交换的，其中$1_A\oplus f$：$A\oplus B\to A\oplus B'$由$(a,\ b)\mapsto(a,f(b))$所定义。于是ϕ定义了反变函子S和T的一个自然同构，其中

$S(B)=\mathrm{Hom}_R(A\oplus BC)T(B)=\mathrm{Hom}_R(A,\ C)\oplus\mathrm{Hom}_R(B,\ C)$。

我们说成同构中对于B是自然的.类似地可以证明ϕ对于A和C也是自然的。

习题4给出另一些例子。

定义1.4 设T是从范畴$\mathscr{C}$到集合范畴$\mathscr{S}$的协变函子。则T叫作可表函子，是指存在$\mathscr{C}$中一个对象A和从协变hom函子$h_A=\mathrm{hom}_{\mathscr{C}}(A,\ -)$到函子$T$的一个自然同构$\alpha$。这时将$(A,\ \alpha)$叫作$T$的一个表示，并且说成：$T$可以用对象$A$来表示。

类似地，一个反变函子S：$\mathscr{C}\to\mathscr{S}$叫作可表函子，是指存在$\mathscr{C}$中一个对象$B$和一个自然同构$\beta$：$h^B\to S$，其中$h^B=\mathrm{hom}_{\mathscr{C}}(-,\ B)$。并且将$(B,\ \beta)$叫作$S$的一个表示。

例 设A和B是含幺交换环K上的幺作用模.对于每个K-模C，以$T(C)$表示全部K-双线性映射$A\times B\to C$所组成的集合。如果f：$C\to C'$是K-模同态，令$T(f)$：$T(C)\to T(C')$是一个函数，它将双线性映射g：$A\times B\to C$映成双线性映射fg：$A\times B\to C'$。于是T是从K-模范畴$\mathscr{M}$到集合范畴$\mathscr{S}$的协变函子。我们断言：T可以用K-模$A\oplus_K B$来表示。为了看出这一点，对于每个K-模C定义函数

$$\alpha_C:\ \mathrm{Hom}_K(A\oplus_K B,\ C)\to T(C),$$

其中$\alpha_C(f)=fi$，而i：$A\times B\to A\oplus_k B$是正则双线性映射：现在，对于每个 $f\in \mathrm{Hom}_K(A\oplus_K B,\ C)$，$\alpha_C(f)$：$A\times B\to C$ 显然是双线性的。根据定理 IV.5.6可知每个双线性映射g：$A\times B\to C$均有形式$\bar{g}i$，其中 $\bar{g}$：$A\otimes_K B\to C$是唯一决定的K-模同态。因此α_C是集合上的一一映射(即是范畴 $\mathscr{S}$中的等价)，不难验证 $C\mapsto\alpha_C$ 决定了从$h_{A\otimes_K B}$到 T的一个自然同构，于是$(A\otimes_K B,\ \alpha)$ 是T的一个表示。$A\otimes_k B$恰好是适当范畴中的泛对象（定理IV.5.6)，这件事并不是偶然的，我们现在要证明：对于任意可表函子，类似的事实也是对的。

设$(A,\ \alpha)$ 是协变函子T：$\mathscr{C}\to\mathscr{S}$ 的一个表示。令$\mathscr{C}_T$为范畴 $\{(C,\ s)\mid C$为 $\mathscr{C}$中对象，$s\in T(C)\}$。$\mathscr{C}_T$中从 $(C,\ s)$ 到 $(D,\ t)$ 的态射定义为$\mathscr{C}$中的态射f：$C\to D$并且满足$T(f)(s)=t\in T(D)$。注意f为$\mathscr{C}_T$中的等价$\Longleftrightarrow f$为$\mathscr{C}$ 中的等价。范畴$\mathscr{C}_T$中的泛对象(见定义I.7.9) 叫作函子T的泛元素。

例 定义1.4后面的例子表明，$(A\otimes_K B,\alpha)$是函子T：$\mathscr{M}\to\mathscr{S}$的一个表示。由此显然推出：对于每个$K$-模$C$ 和双线性映射f：$A\times B\to C$ (即对于每个 $(C,\ f)$，其中$f\in T(C)$)，均存在唯一的 K- 模同态 $\bar{f}$：$A\otimes_k B\to C$，使得 $\bar{f}i=f$ (即$T(\bar{f})(i)=f$，其中 $i=\alpha_{A\otimes_K B}(1_{A\otimes_K B})\in T(A\otimes_k B)$)。因此 $(A\otimes_K B,i)=(A\otimes_K B,\ \alpha_{A\otimes_K B}(1_{A\otimes_K B}))$是范畴$\mathscr{M}_T$中的泛对象，即是$T$的泛元素。

以上面的例子作为起点，我们现在来证明，函子T：$\mathscr{C}\to\mathscr{S}$的表示本质上等价于$T$的泛元素。我们首先需要

引理1.5 设T：$\mathscr{C}\to\mathscr{S}$是从范畴 $\mathscr{C}$ 到集合范畴 $\mathscr{S}$ 的协变函子，而A为$\mathscr{C}$中一个对象。

(i) 如果 α：$h_A\to T$是从协变 hom 函子 h_A到T的一个自然变

换，而$u=\alpha_A(1_A)\in T(A)$，则对$\mathscr{C}$中任一个对象C和$g\in \hom_{\mathscr{C}}(A, C)$，均有

$$\alpha_C(g)=T(g)(u).$$

(ii) 如果$u\in T(A)$，并且对于$\mathscr{C}$中每个对象C，$\beta_C: \hom_{\mathscr{C}}(A, C)\to T(C)$由$g\mapsto T(g)(u)$所定义，则$\beta: h_A\to T$是自然变换，并且$\beta_A(1_A)=u$。

证明 (i) 设C为$\mathscr{C}$中对象，$g\in \hom_{\mathscr{C}}(A, C)$。由假设可知图表

$$\begin{array}{ccc} h_A(A)=\hom_{\mathscr{C}}(A, A) & \xrightarrow{\alpha_A} & T(A) \\ {\scriptstyle h_A(g)}\downarrow & & \downarrow{\scriptstyle T(g)} \\ h_A(C)=\hom_{\mathscr{C}}(A, C) & \xrightarrow{\alpha_C} & T(C) \end{array}$$

是交换的，从而

$$\begin{aligned}\alpha_C(g)&=\alpha_C(g\circ 1_A)=\alpha_C[h_A(g)(1_A)]\\&=[\alpha_C h_A(g)](1_A)=(T(g)\alpha_A)(1_A)=T(g)[\alpha_A(1_A)]\\&=T(g)(u).\end{aligned}$$

(ii) 我们必须证明，对于$\mathscr{C}$的每个态射$k: B\to C$，图表

$$\begin{array}{ccc} h_A(B)=\hom_{\mathscr{C}}(A, B) & \xrightarrow{\beta_B} & T(B) \\ {\scriptstyle h_A(k)}\downarrow & & \downarrow{\scriptstyle T(k)} \\ h_A(C)=\hom_{\mathscr{C}}(A, C) & \xrightarrow{\beta_C} & T(C) \end{array}$$

是交换的。这一事实不难得到，因为对于任意$f\in \hom_{\mathscr{C}}(A, B)$，

$$\begin{aligned}[\beta_C h_A(k)](f)&=\beta_C(k\circ f)=T(k\circ f)(u)=[T(k)T(f)](u)\\&=T(k)[T(f)(u)]=T(k)[\beta_B(f)]\\&=[T(k)\beta_B](f).\end{aligned}$$

因此β是自然变换。最后有

$$\beta_A(1_A)=T(1_A)(u)=1_{T(A)}(u)=u \quad \blacksquare$$

定理1.6 设T：$\mathscr{C}\to\mathscr{S}$是从范畴$\mathscr{C}$到集合范畴$\mathscr{S}$的协变函子。从而在$T$的全部表示组成的类$X$和$T$的全部泛元素组成的类$Y$之间存在着一一对应，其对应由$(A,\ \alpha)\mapsto(A,\ \alpha_A(1_A))$给出。

注记：由于α_A：$\hom_{\mathscr{C}}(A,A)\to T(A)$，从而$\alpha_A(1_A)$是$T(A)$中元素。

证明 设$(A,\ \alpha)$是T的一个表示，令$\alpha_A(1_A)=u\in T(A)$。又设$(B,\ s)$是$\mathscr{C}_T$中一个对象。由假设可知α_B：$h_A(B)=\hom_{\mathscr{C}}(A,B)\to T(B)$是一一对应，从而有唯一的态射$f$：$A\to B$，使得$s=\alpha_B(f)$。由引理1.5可知$T(f)(u)=\alpha_B(f)=s$。因此$f$是$\mathscr{C}_T$中从$(A,\ u)$到$(B,\ s)$的态射。如果$g$是$\mathscr{C}_T$中另一个从$(A,\ u)$到$(B,\ s)$的态射，则$g\in\hom_{\mathscr{C}}(A,B)$而$T(g)(u)=s$。于是由引理1.5可知$\alpha_B(g)=T(g)(u)=s=\alpha_B(f)$。由于$\alpha_B$是一一对应，从而$f=g$。因此$f$是$\mathscr{C}_T$中唯一确定的从$(A,\ u)$到$(B,\ s)$的态射。从而$(A,u)$是$\mathscr{C}_T$中泛对象，即$(A,\ u)$是$T$的泛元素。

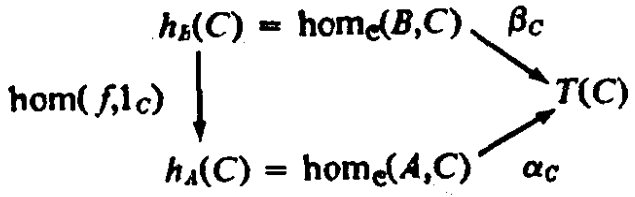
反之，设$(A,\ u)$为T的泛元素。令β：$h_A\to T$是引理1.5(ii)中的自然交换，使得对于$\mathscr{C}$中每个对象C，β_C：$\hom_{\mathscr{C}}(A,C)\to T(c)$均是由$\beta_C(f)=T(f)(u)$所给出的。如果$s\in T(C)$，则$(C,\ s)$属于$\mathscr{C}_T$。由于$(A,\ u)$是$\mathscr{C}_T$中的泛对象，从而存在$f\in\hom_{\mathscr{C}}(A,C)$使得$s=T(f)(u)=\beta_C(f)$。因此$\beta_C$是满射。如果$\beta_C(f_1)=\beta_C(f_2)$，则$T(f_1)(u)=\beta_C(f_1)=\beta_C(f_2)=T(f_2)(u)$，于是$f_1$和$f_2$同时为$\mathscr{C}_T$中从$(A,\ u)$到$(C,\ T(f_1)(u))=(C,\ T(f_2)(u))$的态射。从泛性质可知$f_1=f_2$。因此每个$\beta_C$都是单射，从而是一一对应(即为$\mathscr{S}$中的等价)。因此$\beta$是自然同构，于是$(A,\ \beta)$为$T$的一个表示。

为了完成证明，利用引理1.5可以验证$\phi\psi=1_Y$和$\psi\phi=1_X$，其

中ϕ：$X\to Y$由 $(A,\ \alpha)\mapsto(A,\ \alpha_A(1_A))$给出，而$\psi$：$Y\to X$由$(A,\ u)\mapsto(A,\ \beta)$给出($\beta$的意义如前一段所述)。因此$\phi$是一一对应。

∎

系1.7 设T：$\mathscr{C}\to\mathscr{S}$是从范畴$\mathscr{C}$到集合范畴$\mathscr{S}$的协变函子。如果 $(A,\ \alpha)$ 和 $(B,\ \beta)$ 均是T的表示，则存在唯一的等价f：$A\to B$，使得对于$\mathscr{C}$中每个对象C，下面的图表都是交换的：



证明 设$u=\alpha_A(1_A)$，$v=\beta_B(1_B)$。由定理1.6可知$(A,\ u)$和$(B,\ v)$均是T的泛元素，从而由定理1.7.10可知在$\mathscr{C}$中存在唯一的等价f：$A\to B$，使得$T(f)(u)=v$。由引理1.5 (i) 可知，对于$\mathscr{C}$中每个对象C和$g\in\hom_{\mathscr{C}}(B,\ C)$均有

$$[\alpha_C\hom(f,\ 1_C)](g)=\alpha_C(g\circ f)=T(g\circ f)(u)$$
$$=[T(g)T(f)](u)=T(g)[T(f)(u)]=T(g)(v)$$
$$=\beta_C(g),$$

从而上面的图表是交换的。进而，如果f_1：$A\to B$也使上面的图表交换，则对于$C=B$和$g=1_B$便有

$$T(f_1)(u)=\alpha_B(f_1)=\alpha_B(1_B\circ f_1)=\alpha_B[\hom(f_1,\ 1_B)(1_B)]$$
$$=\beta_B(1_B)=v.$$

由唯一性可知$f_1=f$。∎

系1.8 (Yoneda) 设T：$\mathscr{C}\to\mathscr{S}$是从范畴$\mathscr{C}$到集合范畴$\mathscr{S}$的协变函子。而$A$是$\mathscr{C}$的一个对象。则在集合$T(A)$和集合 $\mathrm{Nat}(h_A,\ T)$ 之间存在着一一对应，其中$\mathrm{Nat}(h_A,\ T)$是从协变 hom 函子

h_A到函子T 的全部自然变换所构成的集合。此外，这个一一对应对于A和T都是自然的。

证明概要 由$\alpha \longmapsto \alpha_A(1_A) \in T(A)$定义函数 $\psi = \psi_A$: $\mathrm{Nat}(h_A, T) \to T(A)$。而由$u \longmapsto \beta$定义函数$\phi$: $T(A) \to \mathrm{Nat}(h_A, T)$，其中$\beta$由引理1.5(ii) 给出。验证$\phi\psi$和$\psi\phi$均是相应集合中的恒等映射。因此$\psi_A$为一一对应。

系中关于自然性的那个推断意味着图表

$$\begin{array}{ccc} \mathrm{Nat}(h_A,T) & \xrightarrow{\psi_A} & T(A) \\ {\scriptstyle N^*(f)}\downarrow & & \downarrow{\scriptstyle T(f)} \\ \mathrm{Nat}(h_B,T) & \xrightarrow[\psi_B]{} & T(B) \end{array}$$

$$\begin{array}{ccc} \mathrm{Nat}(h_A,T) & \xrightarrow{\psi_A} & T(A) \\ {\scriptstyle N_*(\alpha)}\downarrow & & \downarrow{\scriptstyle \alpha_A} \\ \mathrm{Nat}(h_A,S) & \xrightarrow[\psi_A]{} & S(A) \end{array}$$

都是交换的，其中 $f: A \to B$是$\mathscr{C}$中任一态射，α: $T \to S$ 是函子之间的任一自然变换，$N^*(f)$和$N_*(\alpha)$的定义为：对于$\mathscr{C}$中每个对象C和$\beta \in \mathrm{Nat}(h_A, T)$，映射

$$N^*(f)(\beta)_C: h_B(C) = \mathrm{hom}_{\mathscr{C}}(B, C) \to T(C)$$

由$g \longmapsto \beta_C(g \circ f)$给出。而映射$N_*(\alpha)$: $\mathrm{Nat}(h_A, T) \to \mathrm{Nat}(h_A, S)$由$\beta \longmapsto \alpha\beta$给出。∎

可表函子是自然同构于协变（或反变）hom函子的单变量函子。但是对于一个给定的范畴 $\mathscr{D}$，hom $\mathscr{D}(-, -)$ 是二变量函子。我们现在研究何时一个二变量函子T自然同构于$\mathrm{hom}\mathscr{D}(-, -)$。

我们将处理下面稍微一般的情形。设$\mathscr{C}$和$\mathscr{D}$均是范畴，而 T:

$\mathscr{C}\times\mathscr{D}\to\mathscr{S}$是一个函子，它对于第一变量是反变的，而对于第二变量是协变的。如果S：$\mathscr{C}\to\mathscr{D}$是一个协变函子，不难验证$(C, D)\longmapsto \hom_{\mathscr{D}}(S(C), D)$和$(f, g)\longmapsto \hom_{\mathscr{D}}(S(f), g)$定义了一个函子$\mathscr{C}\times\mathscr{D}\to\mathscr{S}$，并且此函子对于第一变量是反变的，而对于第二变量是协变的。

定理1.9 设$\mathscr{C}$和$\mathscr{D}$均是范畴，T是从乘积范畴$\mathscr{C}\times\mathscr{D}$到集合范畴$\mathscr{S}$的函子，此函子的第一变量是反变的而第二变量是协变的。并且对于$\mathscr{C}$的每个对象C，协变函子$T(C, -)$：$\mathscr{D}\to\mathscr{S}$有表示$(A_C, \alpha^C)$。则存在唯一的协变函子$S$：$\mathscr{C}\to\mathscr{D}$，使得$S(C)=A_C$，并且

$$\alpha_D^C: \hom_{\mathscr{D}}(S(C), D)\to T(C, D)$$

给出了从$\hom_{\mathscr{D}}(S(-), -)$到$T$的一个自然同构。

关于符号的注记：对于$\mathscr{C}$中每个对象C，A_C是$\mathscr{D}$中的对象，而α^C是从$\hom_{\mathscr{D}}(A_C, -)$到$T(C, -)$的自然同构。因此对于$\mathscr{D}$中每个$D$，存在着等价

$$\alpha_D^C: \hom_{\mathscr{D}}(A_C, D)\to T(C, D).$$

定理1.9的证明 函子S的对象函数定义为$S(C)=A_C$（对于$\mathscr{C}$中每个对象C）。而S的态射函数定义为：对于$\mathscr{C}$中每个对象C，我们有$\alpha^C A_C$：$\hom_{\mathscr{D}}(A_C, A_C)\to T(C, A_C)$和$u_C=\alpha_{A_C}^C(1_{A_C})\in T(C, A_C)$。根据定理1.6可知$(A_C, u_C)$是函子$T(C, -)$的泛元素。如果$f$：$C\to C'$是$\mathscr{C}$的态射，令$v=T(f, 1_{A_{C'}})(u_{C'})\in T(C', A_{C'})$。由$(A_C, u_C)$在$\mathscr{D}_T(C, -)$中的泛性质可知在$\mathscr{D}$中存在唯一态射$\bar{f}: A_C\to A_{C'}$，使得

$$T(1_C, \bar{f})(u_C)=v=T(f, 1_{A_{C'}})(u_{C'}).$$

定义$S(f)$为这个态射$\bar{f}$。

显然 $S(1_C)=1_{AC}=1_{S(C)}$。如果 $C\xrightarrow{f}C'\xrightarrow{g}C''$是$\mathscr{C}$中的态射，由定义可知$S(g)$是唯一的态射$\bar{g}$：$A_C{}'\to A_C{}''$使得

$$T(1_C{}',\ \bar{g})(u_C{}')=T(g,\ 1_{AC}{}'')(u_C{}'').$$

类似地，$S(g\circ f)$是唯一的态射：$\bar{h}$：$A_C\to A_C{}''$，使得

$$T(1_C,\ \bar{h})(u_C)=T(g\circ f,\ 1_{A_C}{}'')(u_C{}'').$$

于是$S(g)\circ S(f)=\bar{g}\circ\bar{f}$是一个态射$A_C\to A_C{}''$使得

$$\begin{aligned}T(1_C,\ \bar{g}\circ\bar{f})(u_C)&=T(1_C,\ \bar{g})T(1_C,\ \bar{f})(u_C)\\&=T(1_C,\ \bar{g})T(f,1_{A_C}{}')(u_C{}')\\&=T(f,\ \bar{g})(u_C{}')\\&=T(f,\ 1_{AC''})T(1_C{}',\ \bar{g})(u_C{}')\\&=T(f,\ 1_{AC''})T(g,\ 1_{AC''})(u_C{}'')\\&=T(g\circ f,\ 1_{AC''})(u_C{}'')\\&=T(1_C,\ \bar{h})(u_C).\end{aligned}$$

从而由$\mathscr{D}_T(C,-)$中泛对象的唯一性，我们有

$$S(g)\circ S(f)=\bar{g}\circ\bar{f}=\bar{h}=S(g\circ f).$$

因此S：$\mathscr{C}\to\mathscr{D}$是协变函子。

为证α：$\hom_{\mathscr{D}}(S(-),-)\to T$是自然变换，我们只需证明：对于$\mathscr{C}$中每个态射$f$：$C\to C'$和$\mathscr{D}$中态射$g$：$\mathscr{D}\to\mathscr{D}'$，图表

$$\begin{array}{ccc}\hom_{\mathscr{D}}(A_{C'},D) & \xrightarrow{\alpha^{C'}{}_D} & T(C',D)\\ \Big\downarrow{\scriptstyle \hom(S(f),1_D)} & & \Big\downarrow{\scriptstyle T(f,1_D)}\\ \hom_{\mathscr{D}}(A_C,D) & \xrightarrow{\alpha^{C}{}_D} & T(C,D)\\ \Big\downarrow{\scriptstyle \hom(1_{A_C},g)} & & \Big\downarrow{\scriptstyle T(1_C,g)}\\ \hom_{\mathscr{D}}(A_C,D') & \xrightarrow[\alpha^{C}{}_{D'}]{} & T(C,D')\end{array}$$

是交换的。首先知道下面正方形是交换的，这是因为根据假设对于固定的C，

$$\alpha^C: \hom_{\mathscr{A}}(A_C, -)\to T(C, -)$$

是自然同构。至于上面的正方形，令 $k\in\hom_{\mathscr{A}}(A_{C'}, D)$，于是由引理1.5(i)可知

$$\begin{aligned}T(f, 1_D)\alpha_D^{C'}(k) &= T(f, 1_D)T(1_{C'}, k)(u_{C'})\\ &= T(f, k)(u_{C'})\\ &= T(1_C, k)T(f, 1_{A_{C'}})(u_{C'})\\ &= T(1_C, k)T(1_C, \bar{f})(u_C)\\ &= T(1_C, k\circ\bar{f})(u_C)\\ &= T(1_C, k\circ S(f))(u_C)\\ &= \alpha_{D,}^{C}(k\circ S(f))\\ &= \alpha_{D,}^{C}\hom(S(f), 1_D)(k).\ \blacksquare\end{aligned}$$

习　题

注：在这些习题当中，$\mathscr{S}$为集合与函数所组成的范畴，$\mathscr{R}$是环和环同态范畴，R为环，$\mathscr{S}$为左R-模和R-模同态范畴，$\mathscr{G}$为群和群同态范畴。

1. 按以下方式构作函子：

(a) 协变函子$\mathscr{G}\to\mathscr{S}$，每个群对应于它的全部子群所构成的集合。

(b) 协变函子$\mathscr{R}\to\mathscr{R}$，每个环$N$对应于多项式环$N[x]$.

(c) 对于两个变量均为协变的函子$\mathscr{A}\times\mathscr{A}\to\mathscr{A}$，使得

$$(A, B)\longmapsto A\oplus B.$$

(d) 协变函子$\mathscr{G}\to\mathscr{G}$，每个群$G$对应于它的换位子群$G'$(定义II.7.7)。

2. (a) 如果T：$\mathscr{C}\to\mathscr{D}$是协变函子，令$\mathrm{Im}T$为如下的系统：它的对象集合是$\{T(C)\mid C\in\mathscr{C}\}$，而态射集合为$\{T(f)$：$T(C)\to T(C')\mid f: C\to C'$为$\mathscr{C}$中的态射$\}$.证明$\mathrm{Im}T$不一定是范畴。

(b) 如果T的对象函数是单射，求证ImT是范畴。

3. (a) 如果S：$\mathscr{C}\to\mathscr{D}$是函子，当$S$为协变时令$\sigma(S)=1$；而当$S$为反变时令$\sigma(S)=-1$.又若$T$：$\mathscr{D}\to\mathscr{E}$是另一个函子.求证$TS$是从$\mathscr{C}$到$\mathscr{E}$的函子，并且$\sigma(TS)=\sigma(T)\sigma(S)$。

(b) 将(a)推广到有限个函子的情形：S_1：$\mathscr{C}_1\to\mathscr{C}_2$，$S_2$：$\mathscr{C}_2\to\mathscr{C}_3$，$\cdots S_n$：$\mathscr{C}_n\to\mathscr{C}_{n+1}$。

4. (a) 如果A，B，C是集合，则有自然的一一对应：$A\times B=B\times A$和$(A\times B)\times C\to A\times(B\times C)$。

(b) 求证定理IV.4.9；IV.5.8；IV.5.9；和IV.5.10中的同构都是自然的。

5. 设$\mathscr{V}$为如下的范畴：对象集合是域F（特征$\neq 2$，3）上的有限维向量空间全体.态射集合是全部向量空间同构.将左向量空间V的对偶空间仍看作是左向量空间（见命题VII.1.10后面的注记）。

(a) 如果ϕ：$V\to V_1$是向量空间同构（$\mathscr{V}$中的态射），则对偶映射$\overline{\phi}$：$V_1^*\to V^*$也是向量空间同构（见定理IV.4.10).从而ϕ^{-1}：$V^*\to V_1^*$也是$\mathscr{V}$的态射.

(b) D：$\mathscr{V}\to\mathscr{V}$是协变函子，其中$D(V)=V^*$，$D(\phi)=\overline{\phi^{-1}}$.

(c) 对于$\mathscr{V}$中每个V，取它的一组基$\{x_1,\cdots,x_n\}$令，$\{f_{x1},\cdots,f_{xn}\}$是V^*中的对偶基(定理IV.4.11).则由$x_i\longmapsto f_{xi}$定义的映射α_V：$V\to V^*$是同构.从而α_V：$V\cong D(V)$。

(d) 同构α_V不是自然的.即$V\longmapsto\alpha_V$不是从恒等函子I.到D的自然同构.〔提示：考虑基为$\{x\}$的一维空间，令$\phi(x)=cx$，其中$c\neq 0$，$\pm 1_F$.〕

6. (a) 设S：$\mathscr{C}\to\mathscr{D}$和$T$：$\mathscr{C}\to\mathscr{D}$是协变函子，而$\alpha$：$S\to T$是自然同构.则存在自然同构$\beta$：$T\to S$使得$\beta\alpha=I_S$，$\alpha\beta=1_T$，其中$I_S$：$S\to S$和$I_T$：$T\to T$分别是恒等自然同构.〔提示：对于每个$C\in\mathscr{C}$，$\alpha_C$：$S(C)\to T(C)$是等价，从而有逆态射$\beta_C$：$T(C)\to S(C)$.〕

(b) 将(a)推广到多变量函子的情形。

7. 从$\mathscr{S}$到$\mathscr{S}$的协变可表函子将满映射变成满映射。

8. (a) 忘却函子$\mathscr{M}\to\mathscr{S}$（见定义1.2前面的例子）是可表的。

(b) 忘却函子$\mathscr{G}\to\mathscr{S}$是可表的。

9. (a) 设P：$\mathscr{S}\to\mathscr{S}$是函子，它将每个集合$X$对应于幂集合$P(X)$（即$X$的全部子集构成的集合），并将每个函数$f$：$A\to B$对应于映射$P(f)$：$P(B)\to P(A)$，后者将$B$的子集$X$映到$f^{-1}(X)\subset A$。求证$P$是可表反变函子。

(b) 设Q：$\mathscr{S}\to\mathscr{S}$的对象函数定义为$Q(A)=P(A)$。如果$f$：$A\to B$，令$Q(f)$：$Q(A)\to Q(B)$定义为$X\longmapsto f(X)$（对于$X\subset A$）。求证$Q$是协变函子。$Q$是否为可表函子？

10. 设(A,α)和(B,β)分别为协变函子S：$\mathscr{C}\to\mathscr{S}$和$T$：$\mathscr{C}\to\mathscr{S}$的表示。如果$\tau$：$S\to T$是自然变换，则$\mathscr{C}$中存在唯一的态射$f$：$A\to B$，使得对于$\mathscr{C}$中每个对象$C$，下面的图表是交换的：

$$\begin{array}{ccc} \hom_{\mathscr{C}}(A,C) & \xrightarrow{\alpha_C} & S(C) \\ \Big\downarrow{\scriptstyle \hom(f,1_C)} & & \Big\downarrow{\scriptstyle \tau_C} \\ \hom_{\mathscr{C}}(B,C) & \xrightarrow[\beta_C]{} & T(C) \end{array}$$

2. 伴随函子

本节定义和讨论函子伴随对。虽然它们早已出现在许多数学分支之中，但只在近年来才对它作出形式化的描述。

设S：$\mathscr{C}\to\mathscr{D}$和$T$：$\mathscr{D}\to\mathscr{C}$是协变函子。正如我们在定理1.9前面的讨论中所注意到的，$(C,D)\longmapsto\hom_{\mathscr{D}}(S(C),D)$和$(f,g)\longmapsto\hom_{\mathscr{D}}(S(f),g)$定义出一个函子$\mathscr{C}\times\mathscr{D}\to\mathscr{S}$，它对于第一变量是反变的而对于第二变量是协变的。我们把这个函子表示成

$\hom_{\mathscr{D}}(S(-),\ -)$。类似地有函子$\hom_{\mathscr{C}}(-,\ T(-))$：$\mathscr{C}\times\mathscr{D}\to\mathscr{S}$，它定义为

$$(C,\ D)\longmapsto \hom_{\mathscr{C}}(C,\ T(D)),$$

$$(f,\ g)\longmapsto \hom_{\mathscr{C}}(f,\ T(g)).$$

定义2.1 设S：$\mathscr{C}\to\mathscr{D}$和$T$：$\mathscr{D}\to\mathscr{C}$为协变函子。称$S$为$T$的左伴随函子（或者称$T$为$S$的右伴随函子，或者称$(S,\ T)$为伴随对），是指存在从函子$\hom_{\mathscr{D}}(S(-),\ -)$到函子$\hom_{\mathscr{C}}(-,T(-))$的自然同构。

因此，如果S是T的左伴随函子，则对于$\mathscr{C}$中每个C和$\mathscr{D}$中每个D均存在一一对应

$a_{C,D}$：$\hom_{\mathscr{D}}(S(C),D)\to\hom_{\mathscr{C}}(C,T(D))$，并且它对于$C$和$D$是自然的。伴随函子理论首先受到下面例子的启发。

例 设R和S是环，A_R和C_S为模，${}_RB_S$为双重模（系数环分别如下标所示）。按照定理IV.5.10，存在着Abel群同构：

$\mathrm{Hom}_S(A\otimes_R B,C)\cong\mathrm{Hom}_R(A,\mathrm{Hom}_S(B,C))$。不难证明它对于$A$和$C$（以及对于B）都是自然的。由定理IV.5.5(iii)可知$A\otimes_R B$是右S-模，而由习题IV.4.4(c)可知$\mathrm{Hom}_S(B,C)$是右R-模。令B是一个固定的R-S模，$\mathscr{C}$是右R-模范畴，$\mathscr{D}$是右S-模范畴，于是$\hom_{\mathscr{C}}(X,Y)=\mathrm{Hom}_R(X,Y)$，$\hom_{\mathscr{D}}(U,V)=\mathrm{Hom}_S(U,V)$。则上面的同构可以简单地叙述成：从$\mathscr{C}$到$\mathscr{D}$的函子$-\otimes_R B$是从$\mathscr{D}$到$\mathscr{C}$的函子$\hom_S(B,-)$的左伴随函子。

例 设R是含幺环，$\mathscr{M}$为幺作用左R-模范畴。令T：$\mathscr{M}\to\mathscr{S}$为忘却函子，即将每个模对应于它的凭藉集合。于是，对于每个集合X和模A，$\hom_{\mathscr{S}}(X,T(A))$恰好是函数$X\to A$的全体。令$F$：$\mathscr{S}\to\mathscr{M}$是一个函子，它将每个集合$X$对应成集合$X$上的自由$R$-模

$F(X)$。令i_X：$X\to F(X)$是正则映射。对于每个集合X和模A，映射

$\alpha_{X,A}$：$\mathrm{Hom}_R(F(X),A)\to \mathrm{hom}_{\mathscr{D}}(X,T(A))$定义为$g\longmapsto gi_X$。不难看出，它对于$X$和$A$是自然的。由于$F(X)$是$X$上的自由$R$-模，可知$\alpha_{X,A}$是单射（定理IV.2.1 (iV)）。进而，每个函数f：$X\to T(A)$均有形式 $f=\bar{f}i_X$，其中同构 $\bar{f}$：$F(X)\to A$ 是唯一确定的（定理IV.2.1(iV)）。从而$\alpha_{X,A}$是满射，即$\alpha_{X,A}$是一一对应。因此F为 T 的左伴随。

习题中还将给出另一些例子。

在函子伴随对与可表函子之间有密切的联系。

命题2.2 协变函子T：$\mathscr{D}\to\mathscr{C}$有左伴随函子$\Longleftrightarrow$对于$\mathscr{C}$ 中每个对象C，函子$\mathrm{hom}_{\mathscr{C}}(C,T(-))$：$\mathscr{D}\to\mathscr{S}$是可表的。

证明 如果S：$\mathscr{C}\to\mathscr{D}$是$T$的左伴随，则对于$\mathscr{C}$中的对象 C 和$\mathscr{D}$中的对象D，均存在一一对应

$\alpha_{C,D}$：$\mathrm{hom}_{\mathscr{D}}(S(C),\ D)\to\mathrm{hom}_{\mathscr{C}}(C,T(D))$，

并且它对于C和D是自然的。因此对于固定的C，$(S(C),\alpha_C,\_)$ 是函子$\mathrm{hom}_{\mathscr{C}}(C,T(-))$的一个表示。

反之，对于每个C，设A_C 是D 中的对象，它表示 $\mathrm{hom}_{\mathscr{C}}(C,T(-))$。由定理1.9可知存在协变函子$S$：$\mathscr{C}\to\mathscr{D}$，使得$S(C)=A_C$，并且存在函子自然同构

$$\mathrm{hom}_{\mathscr{D}}(S(-),-)\to\mathrm{hom}_{\mathscr{C}}(-,T(-)).$$

因此S为T的左伴随函子。∎

系2.3 协变函子T：$\mathscr{D}\to\mathscr{C}$有左伴随函子$\Longleftrightarrow$对于$\mathscr{C}$ 中每个对象C，均存在$\mathscr{D}$中的对象$S(C)$和态射u_C：$C\to T(S(C))$，使得$(S(C),\ u_C)$是函子$\mathrm{hom}_{\mathscr{C}}(C,T(-))$：$\mathscr{D}\to\mathscr{S}$的泛元素。

证明作为练习，见定理1.6. ∎

系2.4 协变函子T：$\mathscr{D}\to\mathscr{C}$的任意两个左伴随函子都是自然同构的.

证明 如果S_1：$\mathscr{C}\to\mathscr{D}$和$S_2$：$\mathscr{C}\to\mathscr{D}$是$T$的两个左伴随函子，则有自然同构

$$\alpha:\ \hom_{\mathscr{D}}(S_1(-),\ -)\to\hom_{\mathscr{C}}(-,\ T(-)),$$

$$\beta:\ \hom_{\mathscr{D}}(S_2(-),\ -)\to\hom_{\mathscr{C}}(-,\ T(-)).$$

根据命题 2.2 证明的第一部分，可知对于$\mathscr{C}$的每个对象 C，对象$S_1(C)$和$S_2(C)$均可以表示函子 $\hom_{\mathscr{D}}(C,T(-))$.从而由系 1.7 可知，对于$\mathscr{C}$的每个对象$C$，均有等价 f_C：$S_1(C)\to S_2(C)$. 我们只需再证明f_C对于C是自然的. 即给了$\mathscr{C}$中的一个态射g：$C\to C'$，我们必须证明

$$\begin{array}{ccc} S_1(C) & \xrightarrow{f_C} & S_2(C) \\ {\scriptstyle S_1(g)}\downarrow & & \downarrow{\scriptstyle S_2(g)} \\ S_1(C') & \xrightarrow[f_{C'}]{} & S_2(C') \end{array}$$

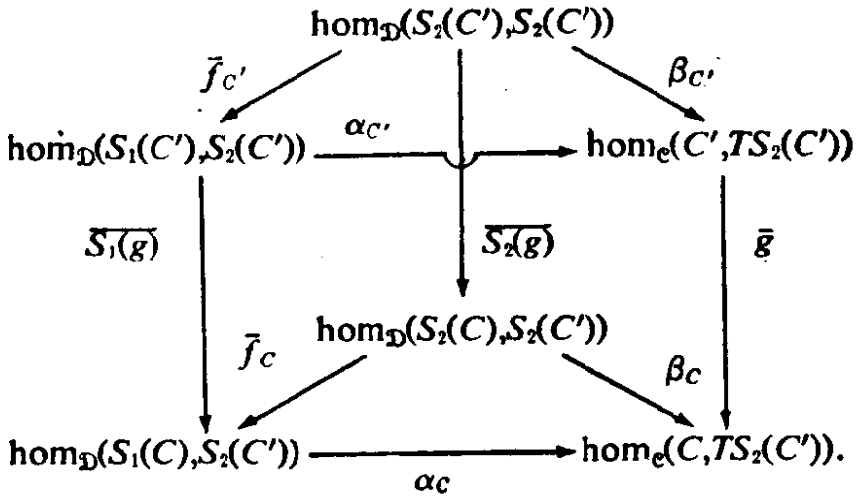
是交换图表. 事实上，我们只需证明

$$\begin{array}{ccc} \hom_{\mathscr{D}}(S_1(C'),S_2(C')) & \xleftarrow{\hom(f_{C'},1)} & \hom_{\mathscr{D}}(S_2(C'),S_2(C')) \\ {\scriptstyle \hom(S_1(g),1)}\downarrow & & \downarrow{\scriptstyle \hom(S_2(g),1)} \\ \hom_{\mathscr{D}}(S_1(C),S_2(C')) & \xleftarrow[\hom(f_C,1)]{} & \hom_{\mathscr{D}}(S_2(C),S_2(C')) \end{array}$$

是交换图表即可（其中$\mathbf{1}=\mathbf{1}_{S_1(C')}$），因为 $\mathbf{1}S_2(C')$的象在一个方向为$S_2(g)\circ f_C$，而在另一方向则为$f_{C'}\circ S_1(g)$.

考虑下面的三维图表(其中$\mathbf{1}=\mathbf{1}_{S_1(C')}$，$\alpha_X=\alpha_{X,S_1(C')}$，并且为

简单起见，诱导映射hom(k, 1)表示成$\bar{k}$)：



我们必须证明左后面的矩形是交换的。由系1.7可知上下三角形都是交换的。此外，因为α和β分别是自然的，从而前面的矩形和右后面的矩形都是交换的。从而

$$\alpha_C\overline{S_1(g)}\bar{f}_{C'}=\bar{g}\alpha_{C'}\bar{f}_{C'}=\bar{g}\beta_{C'}=\beta_C\overline{S_2(g)}=\alpha_C\bar{f}_C\overline{S_2(g)}.$$

由假设知$\alpha_C=\alpha_{C,S_1(C')}$是单射，从而必然有$\overline{S_1(g)}\bar{f}_{C'}=\bar{f}_C\overline{S_2(g)}$。因此左后面的矩形是交换的。∎

习　题

注：$\mathscr{S}$代表集合范畴。

1. 如果T：$\mathscr{C}\to\mathscr{S}$是协变函子，并且有左伴随函子，则$T$是可表函子。

2. 设$\mathscr{C}$为具体范畴，T：$\mathscr{C}\to\mathscr{S}$为忘却函子。如果$T$有左伴随$F$：$\mathscr{S}\to\mathscr{C}$，我们称$F$为自由对象函子，而 $F(X)(X\in\mathscr{S})$ 叫作X上的自由F－对象。求证：

(a) 群范畴有自由对象函子。

(b) 含幺交换环和把1映到1的同态所构成的范畴有自由对象函子。[如

果X是有限集合，用习题III.5.11定义$F(X)$]。

3. 设X是一个固定集合，由$Y \mapsto X \times Y$定义出一个函子$S: \mathscr{S} \to \mathscr{S}$。则$S$是协变hom函子$h_X = \hom_{\mathscr{S}}(X, -)$的左伴随。

4. 设$\mathscr{G}$是群范畴，$\mathscr{A}$是Abel群范畴，$\mathscr{F}$是域范畴，$\mathscr{D}$是整环范畴，$\mathscr{M}$为幺作用左K—模范畴，$\mathscr{B}$为幺作用K—R模范畴（K，R均为含幺环）。对于下列每种情形，T均是相应的忘却函子（例如$T: \mathscr{F} \to \mathscr{D}$是将每个域$F$映成$F$自己，但是后一个$F$看成是整环），在下列诸情况下，求证$(S, T)$是伴随对。

(a) $T: \mathscr{A} \to \mathscr{G}$，$S: \mathscr{G} \to \mathscr{A}$。其中$S(G) = G/G'$，而$G'$为$G$的换位子群（定义II.7.7）。

(b) $T: \mathscr{F} \to \mathscr{D}$，$S: \mathscr{D} \to \mathscr{F}$。其中$S(D)$是$D$的商域（第III.4节）。

(c) $T: \mathscr{M} \to \mathscr{A}$，$S: \mathscr{A} \to \mathscr{M}$。其中$S(A) = K \otimes_Z A$（见定理IV.5.5）。

(d) $T: \mathscr{B} \to \mathscr{M}$，$S: \mathscr{M} \to \mathscr{B}$，其中$S(M) = M \otimes_Z R$。

3. 态　　射

作为函子初等理论的一个重要部分，是试图将一些熟知的范畴（例如集合范畴或者模范畴）中的概念尽可能多地推广到任意范畴中去。我们在本节中把单同态，满同态，同态的核和余核等概念以各种不同程度推广到任意范畴中去。

记号：以后我们把范畴中两个态射的合成记为gf，而不是象以前那样写成$g \circ f$。

首先让我们回忆一下：范畴中的态射$f: C \to D$是等价的充要条件是存在态射$g: D \to C$，使得$gf = 1_C$，$fg = 1_D$。这个定义不过反映了如下的事实：群范畴（或者环范畴，模范畴等等）中的同态是同构的充要条件是它有双侧逆（见定理I.2.3）。采用类似的方

一，我们可以将单同态和满同态概念按下面方法推广到任意范畴上去。

定义3.1 范畴$\mathscr{C}$中的态射$f: C\to D$叫作单的，是指对于每个对象B和态射$g, h\in\hom(B, C)$，均有

$$fh=fg\Longrightarrow h=g.$$

态射f叫作满的，是指对于每个对象E和态射$k,t\in\hom(D,E)$，均有

$$kf=tf\Longrightarrow k=t.$$

例 集合范畴中的态射是单的（满的）$\Longleftrightarrow$它是单射（满射）（习题1）。

例 设$\mathscr{C}$为群范畴，环范畴或者是环上的左模范畴。如果$f: C\to D$和$g, h: B\to C$均是同态（即是$\mathscr{C}$中的态射），由习题IV.1.2(a)可知$fh=fg\Rightarrow h=g$的充要条件是f为单同态(注)。所以单同态的范畴定义与过去在这些范畴中给出的定义是一致的。

例 习题IV.1.2(b)表明，在环R上左模范畴中的态射f是满的$\Longleftrightarrow f$是满同态。这一事实对于群的范畴也是对的，但是证明更困难（习题2）。因此在这两个范畴中，满同态的范畴定义与早先的定义是一致的。

例 在环范畴中，不难看出，每个满同态是满的态射。但是如果$f, g: \boldsymbol{Q}\to R$是环的同态，使得$f|\boldsymbol{Z}=g|\boldsymbol{Z}$，由习题III.1.18可知$f=g$。因此，嵌入映射$\boldsymbol{Z}\to\boldsymbol{Q}$是环范畴中满的态射，但是它显然不是满射。

例 在可除Abel群和群同态范畴中，正则映射$\pi: \boldsymbol{Q}\to\boldsymbol{Q}/\boldsymbol{Z}$

注：在习题中只处理模的情形，但是对于群和环的情形，同样的推理也是对的。

是单的态射，但显然不是单射。为了证明前一论断，设 g, h: $A\to\mathbb{Q}$是同态，其中A为可除群并且$\pi g=\pi h$。如果 $g\neq h$，则存在 $a\in A$, $r,s\in\mathbb{Z}(s\neq\pm1)$，使得 $g(a)-h(a)=r/s\neq0$。由假设有 $b\in A$，使得$rb=a$。从而 $r(g(b)-h(b))=g(a)-h(a)=r(1/s)$，于是$g(b)-h(b)=1/s$.因此$0=\pi g(b)-\pi h(b)=\pi(g(b)-h(b))=\pi(1/s)$。从而$1/s\in\mathrm{Ker}\pi=\mathbb{Z}$，而这与 $s\neq\pm1$相矛盾。因此$g=h$，即π为单的态射。

命题3.2 设$f:B\to C$和$g:C\to D$是范畴$\mathscr{C}$的态射。

(i) f和g为单态射$\Rightarrow gf$为单态射。

(ii) gf为单态射$\Rightarrow f$为单态射。

(iii) f和g为满态射$\Rightarrow gf$为满态射。

(iv) gf为满态射。$\Rightarrow g$为满态射。

(v) f为等价$\Rightarrow f$为满态射和单态射。证明作为练习。∎

注记：命题3.2前面的两个例子表明(v)的逆不成立。

范畴$\mathscr{C}$中的对象0叫作一个零对象，如果0在$\mathscr{C}$中同时是泛对象和余泛对象（见定义I.7.9)。因此，对于$\mathscr{C}$的每个对象C，存在着唯一的态射$0\to C$和唯一的态射$C\to0$。

例 零模是环上左模范畴中的零对象。对于群和环有类似的结论。集合范畴则没有零对象。

命题3.3 设C是范畴$\mathscr{C}$中的对象。

(i) $\mathscr{C}$中任意两个零对象是等价的。

(ii) 如果0是零对象，则（唯一的）态射$0\to C$是单的，而(唯一的）态射$C\to0$是满的。

证明概要 (i) 定理I.7.10。

(ii) 如果 $0_C \circ f = 0_C \circ g$，其中 $0_C: 0 \to C$。由 0 的余泛性可知 $f = g$。从而0_C是单态射。∎

命题3.4 设范畴$\mathscr{C}$有零对象 0，则对于$\mathscr{C}$中任意两个对象C，D均存在唯一的态射 $0_{C,D}: C \to D$，使得对于每个态射$f \in \hom(D, E)$和$g \in \hom(B, C)$均有

$$f \circ 0_{C,D} = 0_{C,E}, \quad 0_{C,D} \circ g = 0_{B,D}$$

注记：$0_{C,D}$称作零态射.

证明（唯一性） 如果$\{0'_{C,D}\}$ 和$\{0_{C,D}\}$ 是具有所述性质的两个态射族，则对于C和D我们有

$$0_{C,D} = 0'_{D,D} \quad 0_{C,D} = 0'_{C,D}.$$

（存在性） 对于$\mathscr{C}$中每个对象A，令 $l_A: 0 \to A$和$\pi_A: A \to 0$ 是上述唯一的态射. 由泛性可知，对于每个 $f: \hom(D, E)$ 均有 $f\iota_D = \iota_E: 0 \to E$。由余泛性可知，对于每个$g \in \hom(B, C)$ 均有 $\pi_C g = \pi_B: B \to 0$。定义$0_{C,D}$为合成$C \xrightarrow{\pi_C} 0 \xrightarrow{\iota_D} D$。于是对于$f \in \hom(D,E)$有 $f \circ 0_{C,D} = f\iota_D\pi_C = \iota_E\pi_C = 0_{C,E}$。对于另一种情形则有类似结果。∎

最后我们在任意范畴中研究态射的核与余核概念。我们从稍微一般的情况下开始。

定义3.5 设$f: C \to D$和$g: C \to D$是范畴$\mathscr{C}$中的态射。态射组(f, g)的差核（或者叫作等子）是指满足下述诸条件的一个态射 $i: B \to C$.

(i) $fi = gi$;

(ii) 如果$h: A \to C$ 是态射并且 $fh = gh$，则存在唯一的态射

$\bar{h}$：$A\to B$，使得$i\bar{h}=h$。

(f, g)的差余核（或者叫作余等子）是指满足下述诸条件的一个态射j：$D\to E$。

(iii) $jf=jg$；

(iv) 如果k：$D\to F$是态射，并且$kf=kg$，则存在唯一的态射$\bar{k}$：$E\to F$，使得$\bar{k}j=k$。

例 在集合范畴$\mathcal{S}$中，f：$C\to D$和g：$C\to D$的差核是包含映射$B\to C$，其中$B=\{C\in C\mid f(c)=g(c)\}$同样的结构表明，在群、环和模范畴中，每一对态射也都有差核。

例 设f：$G\to H$和g：$G\to H$是群同态。令N为H中包含$\{f(a)g(a)^{-1}\mid a\in G\}$的最小正规子群。根据定理I.5.6可知正规满同态$H\to H/N$是$(f, g)$的差余核。

命题3.6 设f：$C\to D$和g：$C\to D$是范畴$\mathcal{C}$中的态射。

(i) 如果i：$B\to C$是(f, g)的差核，则i是单态射。

(ii) 如果i：$B\to C$和j：$A\to C$均是(f, g)的差核，则有唯一的等价h：$A\to B$，使得$ih=j$。

证明 (i) 设h, k：$F\to B$是态射，使得$ih=ik$。则$f(ih)=(fi)h=(gi)h=g(ih)$。由于i是(f, g)的差核，从而有唯一的态射t：$F\to B$，使得$it=ih$。但是$t=h$和$t=k$均满足这个条件，由唯一性知$h=k$。因此i是单态射。

(ii) 由假设可知存在唯一的态射h：$A\to B$和k：$B\to A$，使得分别得$ih=j$和$jk=i$。于是$ihk=jk=i=i\circ 1_B$，$jkh=ih=j=j\circ 1_A$。由(i)可知i和j均是单态射，从而$hk=1_B$，$kh=1_A$。因此h为等价。∎

注记：差余核是满态射，并且命题3.6(ii)的对偶对于差余

核也成立。

现在设范畴$\mathscr{C}$具有零对象0，从而也有零态射（命题3.4）。态射$f: C\to D$的核（如果存在的话）定义为$(f, 0_{C,D})$的任意一个差核，有时将它记作 Ker$f$.由定义 3.5，命题3.4和 3.6 可知$k: K\to C$是$f: C\to D$的核的充要条件是：

(i) k是单态射，$fk=0_{k,D}$；并且

(ii) 如果$h: B\to C$是态射，使得$fh=0_{B,D}$,则存在唯一的态射$\bar{h}: B\to K$，使得$k\bar{h}=h$。

根据命题3.6可知K不计等价是唯一决定的。

态射$f: C\to D$的余核$t: D\to E$对偶地定义为$(f, 0_{C,D})$的差余核。有时将它记作Coker$f$。与上面相仿，t可以刻划成：

(iii) t是满态射，$tf=0_{C,E}$；并且

(iv) 如果$g: D\to F$是态射,使得$gf=0_{C,F}$,则存在唯一的态射$\bar{g}: E\to F$，使得$\bar{g}t=g$。

例 在群、环和模范畴中，态射 $f: C\to D$ 的核是包含映射$K\to C$，其中K为通常的核，即$K=\{c\in C\mid f(c)=0\}$。在模范畴中，正则满同态$D\to D/\mathrm{Im}f$是f的余核。

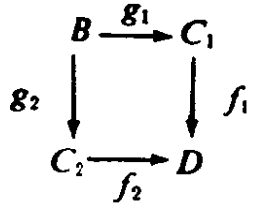
习　题

1. 集合范畴中的一个态射是单（满）态射的充要条件是它为单（满）射.

2. 群范畴中的态射$f: G\to H$是满态射$\Longleftrightarrow$它是通常意义下的满同态.[提示:如果f为满态射，$K=\mathrm{Im}f$，而$j: K\to H$是对应的包含映射，由命题3.2可知j是满态射.如下证明f是满射（即$K=H$）：令S是K在H中的左陪集全体而成的集族.令$T=S\cup\{u\}$，$u\notin S$.以A表示T的全部置换而成的群.$t: H\to A$由$t(h)(h'K)=hh'K$和$t(h)(u)=u$给出.令 $s: H\to A$

是由$\sigma t(h)$所决定的，其中$\sigma \in A$是u和F作对换，求证s和t是同态并且$sj = tj$.于是$s = t$.证明对于每个$h \in H$均有$lK = K$.因此$K = H$.]

3. 范畴$\mathscr{C}$中的态射交换图表



叫作对于f_1和f_2的一个回拉，是指对于每一对态射h_1：$B' \to C_1$和h_2：$B' \to C_2$，如果$f_1h_1 = f_2h_2$，那未必存在唯一的态射t：$B' \to B$，使得$h_1 = g_1t, h_2 = g_2t$.求证：

(a) 如果对于f_1和f_2有另一个回拉，使B_1在交换图表的左上角，则B和B_1等价.

(b)在上面的回拉图表中，如果f_2为单态射，则g_1亦然.

(c) 集合范畴中每对函数f_1：$C_1 \to D$和f_2：$C_2 \to D$均有回拉.

4. 求证在集合范畴中每对函数f，g：$C \to D$均有差余核.

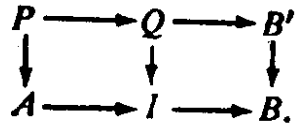
5. 设f，g：$C \to D$是范畴$\mathscr{C}$中的态射.对于$\mathscr{C}$中每个对象X，令

$$E_q(X, f, g) = \{h \in \hom(X, C) \mid fh = gh\}$$

(a) $E_q(-, f, g)$是从$\mathscr{C}$到集合范畴的反变函子.

(b) 态射i：$K \to C$是(f, g)的差核$\Longleftrightarrow E_q(-, f, g)$是可表函子并且以$K$为表示对象（即存在自然同构$\tau$：$\hom\mathscr{C}(-, K) \to E_q(-, f, g)$）.[提示：证明对于$h$：$X \to K$有$\tau_X(h) = ih$，其中$i = \tau_K(1_K)$.]

6. 下面的图表中，如果正方形都是回拉，并且$B' \to B$是单态射，则大矩形也是一个回拉.[提示：见习题3.]



7. 在具有零对象的范畴中，单态射的核是零态射.

文 献 目 录

下面列出课文中实际引用的全部书籍和文章。此外还列出另一些可能会有益处的参考书。这里不打算给出一个完备的参考文献目录，而只是一些适当选择的代数以及有关领域的英文书籍，任何人如果能读本书的话，他就几乎可以看懂所列的全部书籍。在某些情况下，本书的某些部分为阅读这些著作提供了预备知识。

为了方便读者，我们将这些书按照内容加以分类。但是这种分类不是绝对的。例如，分到“一般读物”中的某些书籍可能对于群论或者域论和伽罗华理论作了相当完整的论述。象【26】和【39】等书籍便分放到几个不同的类中。

书 籍

一般读物

【1】 Chevalley, C, Fundamental Conceprs of Algebra. New York, Academic Press, Inc. 1956.

【2】 Faith, C., Algebra: Rings, Modules and Categories I. Berlin,Springer-verlag, 1973.

【3】 Goldhaber, J. and G. Ehrlich, Algebra. New York, The Macmillan Company, 1970.

【4】 Herstein, I., Topics in Algebra. Waltham, Mass. Blaisdell Publishing Company, 1964.

【5】 Lang, S., Algebra. Reading, Mass.: Addison-Wesley, Publishing Company, Inc., 1965.

【6】 Maclane, S. and G. Birkhoff, Algebra. New York, The Macmillan Company, 1967.

【7】 Van der Waerden, B. L., Algebra. (7th ed., 2 vols); New York, Frederick Ungar Publishing Co., 1970.

集 合 论

【8】 Eisenberg, M., Axiomatic Theory of Sets and Classes. New York, Holt, Rinehart and Winston, Inc., 1971.

【9】 Halmos, P., Naive Set Theory, Princeton, N. J. D. Van Nostrand Company Inc., 1960.

【10】 Suppes, P., Axiomatic Set Theory. Princeton, N. J. D. Van Nostrand Company, Inc., 1960.

群 论

【11】 Curtis, C. W. and I. Reiner, Representation Theory of Finite Groups and Associative Algebras. New York, Interscience Publishers, 1962.

【12】 Dixon, J., Problems in Group Theory. Waltham, Mass.: Blaisdell Publishing Company, 1967.

【13】 Fuchs, L. , Infinite Abelian Groups. New York, Academic Press, Inc. , 1970.

【14】 Gorenstein, D. , Finite Groups. New York, Harper and Row, Publishers, 1968.

【15】 Hall, M. , The Theory of Groups. New York, The Macmillan Company, 1959.

【16】 Hall, M. and J. K. Senior, The Groups of Order 2^n ($n \leqslant 6$). New York, The Macmillan Company, 1964.

【17】 Kaplansky, I. , Infinite Abelian Groups (2d ed), Ann Arbor, Mich,, University of Michigan Press, 1969.

【18】 Kurosh, A. G, The Theory of Groups (2vols.), New York, Chelsea Publishing Company, 1960.

【19】 Rotman, J. , The Theory of Groups (2d ed.). Boston, Allyn and Bacon, Inc. , 1973.

【20】 Scott, W. R. , Group Theory. Englewood Cliffs, N. J. , Prentice-Hall, Inc. , 1964.

【21】 Zassenhaus, H. , The Theory of Groups. New York, Chelsea Publishing Company, 1958.

环论和模论

【22】 Divinsky, N. J. , Rings and Radicals. Toronto, University of Toronto Press, 1965.

【23】 Gray, M. , A Radical Approach to Algebra. Reading, Mass, Addison-Wesley Publishing Company, Inc, 1970.

【24】 Herstein, I. N. , Noncommutative Rings. Math. Assoc of America, distributed by J. Wiley, 1968.

【25】 Jacobson N. , Structure of Rings. Amer. Math. Soc. Colloq. Publ. , vol. 37, 1964.

【26】 Jans, J. , Rings and Homology. New York, Holt, Rinehart and Winston, Inc. , 1964.

【27】 Lambek, J. , Lectures on Rings and Modules. Waltham Mass, Blaisdell Publishing Company, 1966.

【28】 McCoy, N. , Theory of Rings. New York, The Macmillan Company, 1964.

【29】 Northcott, D, G. , Lessons on Rings, Modules and Multiplicity. New York, Cambridge University Press, 1968.

交 換 代 数

【30】 Atiyah, M. F. and I. G. MacDonald, Introduction to Commutative Algebra. Reading, Mass. , Addison-Wesley Publishing Company, Inc, 1969.

【31】 Kaplansky, I, Commutative Rings. Boston, Allyn and Bacon, Inc. , 1970.

【32】 Larsen, M. and P. J. McCarthy, Multiplicative Theory of Ideals. New York, Academic Press, Inc. , 1971.

【33】 Zariski, O. and P. Samuel, Commutative Algebra (vols. I and II). Princeton N. J. , D Van Nostrand Company, Inc. , 1958, 1960

同调代数

【34】 Hilton, P. J. and U. Stammbach, A Course in Homological Algebra. Berlin: Springer-Verlag, 1971.

【35】 S. MacLane, Homology. Berlin: Springer-Verlag, 1963.

域　论

【36】 Artin, E., Galois Theory. Notre Dame, Ind.: Notre Dame Mathematical Lectures No. 2 (2d ed.), 1944.

【37】 Gaal, L., Classical Galois Theory with Examples. Chicago: Markham, 1971.

【38】 Jacobson, N., Lectures in Abstract Algebra(vol. III). Princeton, N. J.: D. Van Nostrand Company,. Inc., 1964.

【39】 Kaplansky, I., Fields and Rings (2d ed). Chicago. University of Chicago Press, 1972.

【40】 McCarthy, P. J., Algebraic Extensions of Fields. Waltham, Mass,; Blaisdell Publishing Company, 1966.

线性与多线性代数

【41】 Greub, W., Linear Algebra (3rd ed). Berlin: Sprin-

ger-Verlag, 1967.

【42】 Greub, W., Multilinear Algebra. Berlin, Springer-Verlag, 1967.

【43】 Halmos, P. R., Finite Dimensional Vector Spaces (2d ed.). Princeton, N. J., D. Van Nostrand Company, Inc. 1958.

【44】 Jacobson,N., Lectures in Abstract Algebra (vol. II). Princeton, N. J., D. Van Nostrand Company, Inc, 1953.

范畴理论

【45】 MacLane, S, Categories for the Working Mathematician. Berlin, Springer-verlag, 1972.

【46】 Mitchell, B, Theory of Categories. New York, Academic Press, Inc., 1965.

【47】 Pareigis, B., Categories and Functors. New York: Academic Press, Inc., 1970.

数　论

【48】 Artin E., Algebraic Numbers and Algebraic Functions. New York: Gordon and Breach, 1967.

【49】 Lang, S., Algebraic Number Theory. Reading Mass.: Addison-Wesley Publishing Company. Inc., 1970.

【50】 O'Meara, O. T., Introduction to Quadratic Forms.

Berlin: Springer-Verlag, 1963.

[51] Shockley, J. E., Introduction to Number Theory. New York, Holt, Rinehart and Winston, Inc., 1967.

[52] Weiss E., Algebraic Number Theory. New York; McG-rawHill Inc., 1963.

代数几何

[53] Fulton, W., An Introduction to Algebraic Geometry. New York, W. A. Benjamin Inc., 1969.

[54] Lang, S., Introduction to Algebraic Geometry. New York, Interscience Publishers, 1959.

[55] MacDonald, I. G., Algebraic Geometry, Introduction to Schemes. New York, W. A. Benjamin Inc., 1968.

分　析

[56] Burrill, C., W, Foundations of Real Numbers. New York, McGraw-Hill, Inc, 1967.

[57] Hewitt, E. and K. Stromberg, Real and Abstract Analysis. Berlin, Springer-Verlag, 1969.

文　献

[58] Bergman, G., "A Ring Primitive on the Right but Not on the Left," Proc. Amer. Math. Soc., 15 (1964),

pp. 473—475; correction, pg. 1000.

[59] Cohen, P. J., Set Theory and the Continuum Hypothesis, New York, W. A. Benjamin Inc., 1966.

[60] Corner, A. L. S., "On a Conjecture of Pierce Concerning Direct Decomposition of Abelian Groups," Proc. Colloq. on Abelian Groups, Budapest, 1964, PP. 43—48.

[61] Feit, W. and J. Thompson, "Solvability of Groups of Odd Order," Pac. Jour. Math., 13 (1963), pp. 775—1029.

[62] Goldie, A. W., "Semiprime rings with maximum condition," Proc. Lond. Math. Soc., 10 (1960), pp. 201—220.

[63] Kaplansky, I, "Projective Modules," Math. Ann., 68 (1958), pp. 372—377.

[64] Krull, W., "Galoissche Theorie der unendlichen algebraischen Erweiterungen," Math. Ann., 100 (1928), pp. 687—698.

[65] Procesi, C. and L. Small, "On a theorem of Goldie," Jour. of Algebra, 2 (1965), pp. 80—84.

[66] Sasiada, E. and P. M. Cohn, "An Example of a Simple Radical Ring," Jour. of Algebra, 5 (1967), pp. 373—377.