《近世代数》习题解答和补充材料

李尚应

2021 年 12 月 17 日

目录

符号索引

符号	含义	本书中初次出现处
$\exists$	存在	1.1.1
$\forall$	对任意的	1.1.1
$\in$	属于	1.1.1
$\cap$	左右两边的交集	1.1.1
$\cup$	左右两边的并集	1.1.1
i	虚数单位或者某个指定的下标序列中的元素	1.1.1
$\bigcap_{i\in I}$	一群基于下标 i 指定的集合的交集（下标也可写在符号正下方，下同）	1.1.1
$\bigcup_{i\in I}$	一群基于下标 i 指定的集合的并集	1.1.1
A^c	A 的补集	1.1.1
$\Leftrightarrow$	等价于	1.1.1
id_M	集合 M 上的恒等映射，当上下文清楚时可省去集合标识（如果群中的元素是集合上的置换，该群的单位元素为恒等映射，本书在这种情况也惯用 id 而不是 1）	1.1.2
$\to$	集合间的映射	1.1.2
$\mapsto$	元素被映射到	1.1.2
s.t.	such that 使得	1.1.2
$\circ$	有时被用来表示映射的复合	1.1.2
$\Leftarrow$	右边推出左边，右边为左边的充分条件	1.1.2
$\Rightarrow$	左边推出右边，右边为左边的必要条件	1.1.2
f^{-1}	当 f 是映射时，指它的逆映射	1.1.2
$\lvert A\rvert$	当 A 是集合时，指 A 的元素个数	1.1.4
$X-Y$	当 X,Y 是集合时，指 $\{x\in X \mid x\notin Y\}$	1.1.5
$\mathbb{N}$	自然数集合（警告：在国际上 0 是不是自然数并无统一的说法，本书用 $\mathbb{N}$ 表示非负整数，以 $\mathbb{Z}_+$ 表示 1 以上的整数，而在国际上（荷兰除外）有些文献用 $\mathbb{N}$ 表示正整数）	1.1.5
$\sim$	可表示某种关系	1.1.6
$[a]$	可表示 a 的等价类	1.1.7

$\varnothing$	空集	1.1.7
$\sum_{i=n_1}^{n_2}$	按下标 i 从 n_1 到 n_2 求和（$i=n_1$ 也可写在符号正下方，n_2 也可写在符号正上方，下文 $\prod$ 同）	1.1.9
1_G	群 G 的单位元（或域 F 的乘法单位元），在上下文清楚时可省去群标识	1.2.1
$f(a)_G^{-1}$	$f(a)$ 在群 G 的逆元，在上下文清楚时可省去群标识	1.2.1
$\lvert\alpha-\beta\rvert$	当 α,β 是点时，表示它们的距离	1.2.3
x_G^{-1}	当 x 为群 G 中元素且群的运算表示为乘法时，表示 x 在 G 中的逆元. 当上下文清楚时常省去 G	1.2.4
$\mathbb{Z}$	整数集合	1.2.5
ζ_n	n 次单位根，经常规定为其中辐角主值最小的非实数 $\cos(2\pi i/n)+i\sin(2\pi i/n)$	1.2.6
$A\leqslant B$	当 A,B 为群时，指 A 是 B 的子群	1.2.7
$A\times B$	当 A,B 为集合（或群）时，指 A 和 B 作为集合（或群）的直积	1.2.7
$(G,\cdot)$	群 G，其中运算用 $\cdot$ 表示	1.2.8
$\subseteq$	左边集合包含于右边	1.2.11
$\mathrm{GL}_n(F)$	域 F 上的 n 阶一般线性群	1.2.13
$\mathrm{SL}_n(F)$	域 F 上的 n 阶特殊线性群	1.2.13
$T_n(F)$	域 F 上对角线元全为 1_F 的 n 阶上三角阵集合	1.2.13
$\mathrm{Diag}_n(F)$	域 F 上 n 阶可逆对角阵集合	1.2.13
$B_n(F)$	域 F 上 n 阶可逆上三角阵集合	1.2.13
$\mathbb{R}$	实数集合	1.2.13
$\mathrm{O}_n(F)$	域 F 上 n 阶正交群	1.2.13
$\mathrm{O}_{p,q}(F)$	域 F 上 $p+q$ 阶广义正交群，p,q 分别为双线性型标准形式中正负单位个数	1.2.13
$\mathrm{Sp}_{2n}(F)$	域 F 上 $2n$ 阶辛群	1.2.13
$\mathrm{U}(n)$	n 阶酉群	1.2.13
$\mathbb{C}$	复数集合	1.2.13
$\gcd(a,b)$	a,b 的最大公约数	1.2.18
$\overline{n}$	n 的等价类，常用于循环群 $\mathbb{Z}/m\mathbb{Z}$	1.2.18
$\cong$	同构	1.2.20
$\mathbb{F}_p$	p 元有限域，其中 p 是素数，其加法和乘法即整数加法乘法同余 p 的结果	1.2.21
$F^\times$	当 F 是域时，常指 F 中可逆元构成的乘法群. $\mathbb{Q}^\times,\mathbb{R}^\times,\mathbb{C}^\times$ 即非零实数/复数构成的乘法群	1.2.21
$\langle x,y,\cdots\rangle$	$x,y,\cdots$ 生成的群/子群	1.3.7
$\mathrm{Aut}(G)$	群 G 的自同构群	1.3.15

第一部分

补充材料

第二部分

习题提示

第三部分

习题答案

第一章　群论基础

1.1 集合论预备知识

1.1.1 设 B，$A_i(i \in I)$ 是集合 Ω 的子集，试证：

(1) $B \cap (\bigcup_{i\in I} A_i) = \bigcup_{i\in I}(B \cap A_i)$;

证明. $x \in B \cap (\bigcup_{i\in I} A_i) \Leftrightarrow x \in B$ 且 $x \in \bigcup_{i\in I} A_i$
$\Leftrightarrow x \in B$ 且 $(\exists i \in I \text{ s.t. } x \in A_i)$
$\Leftrightarrow \exists i \in I \text{ s.t. } (x \in B$ 且 $x \in A_i)$
$\Leftrightarrow \exists i \in I \text{ s.t. } x \in (B \cap A_i)$
$\Leftrightarrow x \in \bigcup_{i\in I}(B \cap A_i)$ □

(2) $B \cup (\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(B \cup A_i)$;

证明. $x \in B \cup (\bigcap_{i\in I} A_i) \Leftrightarrow x \in B$ 或 $x \in \bigcap_{i\in I} A_i$
$\Leftrightarrow x \in B$ 或 $(\forall i \in I,\ x \in A_i)$
$\Leftrightarrow$(这一步只需论证 $x \notin B$ 时的情形) $\forall i \in I,\ (x \in B$ 或 $x \in A_i)$
$\Leftrightarrow \forall i \in I,\ x \in (B \cup A_i)$
$\Leftrightarrow x \in \bigcap_{i\in I}(B \cup A_i)$ □

(3) $(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} A_i^c$;

证明. $x \in (\bigcap_{i\in I} A_i)^c$
$\Leftrightarrow x \notin (\bigcap_{i\in I} A_i)$
$\Leftrightarrow x$ 不满足 $\forall i \in I,\ x \in A_i$
$\Leftrightarrow \exists i \in I \text{ s.t. } x \notin A_i$
$\Leftrightarrow \exists i \in I \text{ s.t. } x \in A_i^c$
$\Leftrightarrow x \in \bigcup_{i\in I} A_i^c$ □

1.1.2 对任意集合 X，令 id_X 为 $X \to X : x \mapsto x$(对 $\forall x \in X$ 成立)，(这样的映射叫做**恒等映射**，记为 id) 令 $f : A \to B$ 为集合间的映射，A 为非空集合，试证：

(1) f 为单射 $\Leftrightarrow \exists g : B \to A \text{ s.t. } g \circ f = \mathrm{id}_A$;

证明. $(\Rightarrow) f$ 为单射，则 $\forall b \in B$，b 无原像或有唯一原像. 定义

$$g : b \to \begin{cases} A\text{中任意元素}, & \text{当}b\text{没有原像} \\ f^{-1}(b), & \text{当}b\text{有原像}f^{-1}(b) \end{cases}$$

则 $g \circ f = \mathrm{id}_A$.
$(\Leftarrow)$ 反证法，若 f 不是单射但 g 存在，则 $\exists a_1 \neq a_2, b \in B \text{ s.t. } f(a_1) = f(a_2) = b$. 又 $g \circ f = \mathrm{id}_A$，则 $g(b) = a_1 = a_2$ 有两个不同的值，与函数的定义矛盾. □

(2) f 为满射 $\Leftrightarrow \exists h: B\to A$ s.t. $f\circ h=\mathrm{id}_B$;

证明. $(\Rightarrow) f$ 为满射，则 $\forall b\in B$，存在原像 $f^{-1}(b)=\{x\mid f(x)=b\}\neq\varnothing$(该集合不一定只有一个元素)

对所有的 b 选择 $f^{-1}(b)$ 中的一个元素 $f_1^{-1}(b)$（这里用到了**选择公理**，参见**引理 3.66**. 事实上 (1) 的证明中"A 中任意元素" 的表述也用到了选择公理）

令 $h: B\to A, b\mapsto f_1^{-1}(b)$，则 $f\circ h=\mathrm{id}_B$.

$(\Leftarrow)$ 反证法，若 f 不为满射但 h 存在，则 $\exists b\in B$ s.t. $\forall a\in A, f(a)\neq b$. 则由 $h(b)\in A$ 有 $f(h(b))\neq b$，与 $f\circ h=\mathrm{id}_B$ 矛盾. □

(3) f 为双射 $\Leftrightarrow$ 存在唯一的 $g: B\to A$ s.t. $f\circ g=\mathrm{id}_B, g\circ f=\mathrm{id}_A$.

证明. 存在性由 (1)(2) 立得. 只需证明 f 为双射时 $g=f^{-1}$ 唯一. 若不然，则存在两个映射 $g_1\neq g_2$ 满足 $f\circ g_1=f\circ g_2=\mathrm{id}$. 由于 g_1,g_2 不同，必存在 $b\in B$ s.t. $g_1(b)\neq g_2(b)$，故 $f(g_1(b))=f(g_2(b))=b$，与 f 是单射矛盾. □

说明 这里的 g 称为 f 的**逆映射**，通常记为 f^{-1}. 证明双射的逆映射也是双射，并讨论逆映射与映射的原像集合之间的关系.

证明. 留给读者. □

1.1.3 如果 $f: A\to B, g: B\to C$ 均是一一对应，则 $g\circ f: A\to C$ 也是一一对应，且 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$.

证明. $g\circ f$ 是单射：对 $a_1,a_2\in A, a_1\neq a_2$，因 f 为单射有 $f(a_1)\neq f(a_2)$，因 g 为单射有 $g(f(a_1))\neq g(f(a_2))$.

$g\circ f$ 是满射：对 $\forall c\in C$，因 g 为满射存在 $g^{-1}(c)\in B$，对 $\forall b\in B$ 因 f 为满射存在 $f^{-1}(b)\in A$，这导致 $\forall c\in C, \exists f^{-1}(g^{-1}(c))\in A$.

易见上述 $g^{-1}(c), f^{-1}(g^{-1}(c))$ 唯一，故得结论. □

1.1.4 设 $P(A)$ 是集合 A 的全部子集构成的集族，$M(A)$ 为一切 A 到集合 $\{0,1\}$ 的映射构成的集合，试构造 $M(A)$ 到 $P(A)$ 的双射. 特别地，若 A 为有限集，试证 $|P(A)|=2^{|A|}$，换言之，n 元集合共有 2^n 个子集.

解. 令

$$f: P(A)\to M(A), P\subset A\mapsto \left(g_P: A\to\{0,1\}, x\mapsto \begin{cases}1, & \text{当} x\in P\\ 0, & \text{当} x\notin P\end{cases}\right)$$

我们证明 f 是双射.

f 为单射：若 $P_1\neq P_2$，则存在 x 使得 $x\in P_1, x\notin P_2$ 或 $x\in P_2, x\notin P_1$，于是 $f(P_1)(x)=1, f(P_2)(x)=0$ 或者 $f(P_1)(x)=0, f(P_2)(x)=1$，故 $f(P_1)\neq f(P_2)$.

f 为满射：令 m 为 $M(A)$ 中任意元素，定义 $M^+=\{x\in A\mid m(x)=1\}$，则 $f(M^+)=m$.

于是 f 是双射，利用**习题 1.1.8(1)** 可知 $|P(A)|=|M(A)|=2^{|A|}$.

1.1.5 设 X 是无限集合，Y 为 X 的有限子集，证明存在双射 $X-Y\to X$.

证明. 构造单射 $f:\mathbb{N}\to X$（X 无限，因此这是可以做到的），其中 $\{0,1,...,|Y|-1\}\mapsto Y$. 令

$$g:X-Y\to X, z\mapsto\begin{cases}z, & \text{当}z\notin f(\mathbb{N})\\ f(w-|Y|), & \text{当}z=f(w),\text{其中}w\in\mathbb{N}\end{cases}$$

易验证 g 为双射. □

1.1.6 证明等价关系的三个条件是互相独立的，也就是已知任意两个条件不能推出第三个条件.

证明. 对称性独立：$a\sim a,b,c$；$b\sim b,c$；$c\sim c$，不满足对称性，满足自反和传递性.

传递性独立：$a\sim a,b$；$b\sim a,b,c$；$c\sim b,c$，不满足传递性，满足自反和对称性.

自反性独立：$a\sim a,b$；$b\sim a,b$；$c\nsim a,b,c$，对 c 不满足自反性，满足对称和传递性. □

1.1.7 设集合 A 中关系满足对称性和传递性，且 A 中任意元素都和某元素有关系，证明此关系为等价关系.

证明. 对任意 $a\in A$ 仍记 $[a]=\{b\in A\mid b\sim a\}$. 与**定义 1.9** 不同，我们不确定 $a\in[a]$，但 $[a]\neq\varnothing$，于是 $\exists b$ s.t. $b\sim a$，由对称性 $a\sim b$，由传递性 $a\sim a$，故 $a\in[a]$，类 $[a]$ 满足**定义 1.9** 的所有性质，$\sim$ 为等价关系. □

1.1.8 设 A,B 为两个有限集.

(1) A 到 B 的不同映射有多少个?

解. 对 $\forall b\in B$，$f(b)$ 有 $|A|$ 种不同选法. 因 $b_1\neq b_2$ 时 $f(b_1)$ 和 $f(b_2)$ 的选取不相干涉，故共有 $|B|^{|A|}$ 种不同选法，即 $|B|^{|A|}$ 个不同映射.

(2) A 上不同的二元运算有多少个?

解. 二元运算为 $A\times A$ 到 A 的映射，在 (1) 中令 $A=A\times A$，$B=A$，得 $|A|^{|A|^2}$ 个不同的二元运算.

1.1.9 证明容斥原理（命题 1.1）

证明. 已知 $|A\cup B|=|A|+|B|-|A\cap B|$，故 $n=2$ 时命题成立，对 n 作数学归纳法，已知命题对 $n\leqslant k$ 成立，下证命题对 $k+1$ 成立.

$$
\begin{aligned}
&|A_1 \cup A_2 \cup \cdots \cup A_{k+1}| \\
=&|(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}| \\
=&|A_1 \cup A_2 \cup \cdots \cup A_k| + |A_{k+1}| - |(A_1 \cup A_2 \cup \cdots \cup A_k) \cap A_{k+1}| && \text{(利用 } n=2 \text{ 的情形)} \\
=&\sum_{j=1}^{k}(-1)^{j-1}\left(\sum_{\{i_1,\ldots,i_j\}\subseteq\{1,\ldots,k\}}|A_{i_1}\cap\cdots\cap A_{i_j}|\right) && \text{(利用 } n=k \text{ 的情形，记此项为 } a) \\
&+|A_{k+1}| \\
&-|(A_1\cap A_{k+1})\cup\cdots\cup(A_k\cap A_{k+1})| && \text{(利用\textbf{习题 1.1.1(1)})} \\
=&\,a+|A_{k+1}| \\
&-\sum_{j=1}^{k}(-1)^{j-1}\left(\sum_{\{i_1,\ldots,i_j\}\subseteq\{1,\ldots,k\}}|(A_{i_1}\cap A_{k+1})\cap\cdots\cap(A_{i_j}\cap A_{k+1})|\right) && \text{(利用 } n=k \text{ 的情形)} \\
=&\,a+|A_{k+1}| \\
&-\sum_{j=1}^{k}(-1)^{j-1}\left(\sum_{\substack{\{i_1,\ldots,i_{j+1}\}\subseteq\{1,\ldots,k,k+1\}\\ i_{j+1}=k+1}}|A_{i_1}\cap\cdots\cap A_{i_j}\cap A_{k+1})|\right) && (*) \\
=&\sum_{j=1}^{k}(-1)^{j-1}\left(\sum_{\substack{\{i_1,\ldots,i_j\}\subseteq\{1,\ldots,k+1\}\\ \forall 1\leqslant l\leqslant j, i_k\neq k+1}}|A_{i_1}\cap\cdots\cap A_{i_j}|\right) \\
&+\sum_{j=1}^{1}(-1)^{j-1}\left(\sum_{\substack{\{i_1,\ldots,i_j\}\subseteq\{1,\ldots,k+1\}\\ i_j=k+1}}|A_{i_1}|\right) && \text{(注意这里 } j \text{ 恒等于 } 1) \\
&+\sum_{j=2}^{k+1}(-1)^{j-1}\left(\sum_{\substack{\{i_1,\ldots,i_j\}\subseteq\{1,\ldots,k+1\}\\ i_j=k+1}}|A_{i_1}\cap\cdots\cap A_{i_j}|\right) && \text{(这里的 } j \text{ 是 } (*) \text{ 中的 } j+1) \\
=&\sum_{j=1}^{k+1}(-1)^{j-1}\left(\sum_{\{i_1,\ldots,i_j\}\subseteq\{1,\ldots,k+1\}}|A_{i_1}\cap\cdots\cap A_{i_j}|\right)
\end{aligned}
$$

由数学归纳法即得结论. □

1.2 群的基本概念和例子

1.2.1 令 A 为非空集合，G 是群，$\mathrm{Map}(A,G)$ 为 A 到 G 的一切映射集合，对任意 $f,g\in\mathrm{Map}(A,G)$ 定义 $fg:\forall a\in A fg(a)=f(a)g(a)$. 试证 $\mathrm{Map}(A,G)$ 是群.

证明. $(fg)h=f(gh)$：$\forall a\in A,(fg)h(a)=fg(a)h(a)=f(a)g(a)h(a)=f(a)gh(a)=f(gh)(a)$

单位元 $1_{\mathrm{Map}(A,G)}$ 存在：$1_{\mathrm{Map}(A,G)}:\forall a\in A,a\mapsto 1_G$，易验证它满足条件.

逆元 $f^{-1}_{\mathrm{Map}(A,G)}$ 存在：$f^{-1}_{\mathrm{Map}(A,G)}:\forall a\in A,a\mapsto f(a)^{-1}_G$，易验证它满足条件. □

1.2.2 设 A 为集合，$P(A)$ 为 A 的子集构成的集族，在 $P(A)$ 上定义乘法运算：

$$X\triangle Y=(X\cap Y^c)\cup(X^c\cap Y)$$

试证 $(P(A),\triangle)$ 构成交换群，且 $\forall X\in P(X),X^{-1}_{\triangle}=X$.

证明. 结合律：$(X\triangle Y)\triangle Z$

$=((X\triangle Y)\cap Z^c)\cup((X\triangle Y)^c\cap Z)$

$=(((X\cap Y^c))\cup(X^c\cap Y))\cap Z^c)\cup(((X\cap Y^c)^c\cap(X^c\cap Y)^c)\cap Z)$

$=(X\cap Y^c\cap Z^c)\cup(X^c\cap Y\cap Z^c)\cup(((X^c\cup Y)\cap(X\cup Y^c))\cap Z)$

注意到 $((X^c\cup Y)\cap(X\cup Y^c))=(X^c\cap X)\cup(Y\cap X)\cup(X^c\cap Y^c)\cup(Y\cap Y^c)=(X\cap Y)^(X^c\cap Y^c)$

则上式 $=(X\cap Y^c\cap Z^c)\cup(X^c\cap Y\cap Z^c)\cup(X^c\cap Y^c\cap Z)\cup(X\cap Y\cap Z)$

该式关于 X,Y,Z 对称，故 $(X\triangle Y)\triangle Z=(Y\triangle Z)\triangle X=X\triangle(Y\triangle Z)$（$\triangle$ 的交换性由定义立得）

单位元 $1_{P(A),\triangle}=\varnothing$：因对任意 $X\subseteq A$，$X\triangle\varnothing=(X\cap A)\cup(X^c\cap\varnothing)=X$.

X 的逆是自身：$X\triangle X=(X\cap X^c)\cup(X^c\cap X)=\varnothing$. □

1.2.3 试证平面保距映射都是双射，且在函数复合意义下构成群.

证明. 令 $f:A_1\to A_2$ 为保距映射.

函数复合意义下构成群：留给读者.

单射性：若 $f(\alpha)=f(\beta)$，则 $|\alpha-\beta|=|f(\alpha)-f(\beta)|=0,\alpha=\beta$.

满射性：任取 A_2 中点 γ_2. 由单射性 A_2 中有原像的点多于一个，设 $\alpha_2\neq\beta_2$ 是这样的两个点，$|\alpha_2-\gamma_2|=b,|\beta_2-\gamma_2|=a,|\alpha_2-\beta_2|=c$，则 $a+b\geqslant c,a-b\leqslant c$，故 α_2 和 β_2 由距离 b,a 至少确定一点且至多确定两点（请读者想象以 α_2 为中心 b 为半径的圆，β_2 为中心 a 为半径的圆，两圆依条件不相离不相包含，则必相交或相切的情况），这两点关于直线 $\alpha_2\beta_2$ 对称（或为此直线上一点），其中一个为 γ_2，另一个为 ω_2（若为一点，则 $\omega_2=\gamma_2$）

考虑 α_2,β_2 的原像 α_1,β_1，它们满足 $|\alpha_1-\beta_1|=c$. 故 α_1 和 β_1 由距离 b,a 同样在 A_1 中至少确定一点且至多确定两点，由保距性，它们的像只能是 γ_2,ω_2. 若 $\omega_2=\gamma_2$，则 γ_2 已经有原像. 若 $\omega_2\neq\gamma_2$，则 $a+b\neq c,a-b\neq c$（即 $\alpha_2\beta_2\gamma_2$ 为非退化三角形），故 A_1 中一定确定了两点（同上分析，并且这时两圆不相切），这两点的像只能在 ω_2,γ_2 当中取，由单射性，γ_2 和 ω_2 都有原像，故得满射性. □

1.2.4 设 G 是群，$x,y\in G$. 试证：$(x^{-1})^{-1}=x,(xy)^{-1}=y^{-1}x^{-1}$.

证明. (1) $xx^{-1}=x^{-1}x=1$, 由 x 在 G 中的任意性以 x^{-1} 代替 x 有 $x^{-1}(x^{-1})^{-1}=(x^{-1})^{-1}x^{-1}=1$, 由消去律得 $(x^{-1})^{-1}=x$.

(2) $y^{-1}x^{-1}xy=y^{-1}\cdot 1\cdot y=1, xyy^{-1}x^{-1}=x\cdot 1\cdot x^{-1}=1$. □

1.2.5 判断以下哪些 2 阶方阵集合在乘法意义下构成群:

(1) $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$, $ac\neq b^2$.

解. $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}$ 结果不满足条件，该集合对二元运算不封闭.

(2) $\begin{pmatrix} a & b \\ c & a \end{pmatrix}$, $a^2\neq bc$.

解. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}=\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ 结果不满足条件，该集合对二元运算不封闭.

(3) $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $ac\neq 0$.

证明. $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}=\begin{pmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$

由于 $a_1a_2c_1c_2=(a_1c_1)(a_2c_2)\neq 0$，故集合对二元运算封闭.

结合律由矩阵乘法结合律得到.

单位元存在：集合中有矩阵乘法的单位元 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$，它也一定是该集合中的单位元.

逆元：$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c^{-1} \end{pmatrix}=\begin{pmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 由于 $ac\neq 0$, a^{-1}, c^{-1} 存在且 $a^{-1}c^{-1}\neq 0$，故逆元存在.

综上，该集合在矩阵乘法下为群. □

(4) $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a,b,c,d\in\mathbb{Z}, ad\neq bc$.

解. 只需观察某些矩阵的 $ad-bc\neq 1$ 即可知这样的矩阵中有一部分是逆元不在集合内的.

1.2.6 试证集合 $\bigcup_{n\geqslant 1}\mu_n=\{\zeta_n^i \mid 0\leqslant i\leqslant n-1\}$ 在复数乘法意义下构成群.

证明. 只证该集合对二元运算封闭，单位，结合，逆元留给读者.

$\zeta_{n_1}^{i_1}\cdot\zeta_{n_2}^{i_2}$

$=\exp(2\pi i\cdot\frac{i_1}{n_1})\exp(2\pi i\cdot\frac{i_2}{n_2})$

$=\exp(2\pi i\cdot\frac{i_1n_2+i_2n_1}{n_1n_2})$

$=\exp(2\pi i\cdot\frac{i_1n_2+i_2n_1-kn_1n_2}{n_1n_2})$ 其中 $0\leqslant i_1n_2+i_2n_1-kn_1n_2<n_1n_2$.

$\in \mu_{n_1 n_2}$
$\subseteq \bigcup_{n\geqslant 1} \mu_n$. □

1.2.7

(1) 若群 $A \leqslant G, B \leqslant H$，则 $A \times B \leqslant G \times H$.

证明. 令 $a = \{a_A, a_B\}, b = \{b_A, b_B\}$ 为 $A \times B$ 中元素. 则 $ab^{-1} = \{a_A b_A^{-1}, a_B b_B^{-1}\} \in G \times H$，然后利用**命题 1.31**. □

(2) 举例说明不是所有 $\mathbb{Z} \times \mathbb{Z}$ 的子群都是如此得到的.

解. 令 $A = \{a, 2a\}(a \in \mathbb{Z})$ 为 $\mathbb{Z} \times \mathbb{Z}$ 的子群，则 $\{1, 2\} \in A, \{2, 4\} \in A, \{1, 4\} \notin A$，$A$ 不是两个集合的直积.

1.2.8 设 $(G, \cdot)$ 为群，试证 $G^{\mathrm{op}} = (G, \circ), a \circ b = b \cdot a$ 也是群. 称为 G 的**反群**.

证明. 集合对二元运算封闭显然.

结合律：$(a \circ b) \circ c = (b \cdot a) \circ c = c \cdot b \cdot a = (b \circ c) \cdot a = a \circ (b \circ c)$

单位：$1_G \circ a = a \circ 1_G = a \cdot 1_G = 1_G \cdot a = a$，故 $1_{G^{\mathrm{op}}} = 1_G$.

逆元：$a \cdot a_G^{-1} = a_G^{-1} \cdot a = 1 \Leftrightarrow a_G^{-1} \circ a = a \circ a_G^{-1} = 1$，故 $a_{G^{\mathrm{op}}}^{-1} = a_G^{-1}$. □

1.2.9 设 G 是含幺半群. 试证其中可逆元 $G^\times$ 构成群.

证明. 只需要证 $G^\times$ 对乘法运算封闭：$\forall a, b \in G^\times, abb^{-1}a^{-1} = b^{-1}a^{-1}ab = 1$. 故 $(ab)^{-1} = b^{-1}a^{-1}$ 为 ab 的逆元，$ab \in G^\times$. □

1.2.10 令 G 是 n 阶有限群，$a_1, ..., a_n$ 为群 G 的任意 n 个元素，不一定两两不同. 试证：存在 $p, q \in \mathbb{Z}, 1 \leqslant p \leqslant q \leqslant n$, s.t. $a_p a_{p+1} ... a_q = 1$.

证明. 考虑 $a_1, a_1a_2, ..., a_1a_2...a_j, ..., a_1a_2...a_n$ 是群 G 中 n 个元素，若其中有元素等于 1，则结论已经成立，否则这 n 个元素只有 1 以外的 $n-1$ 个取值.

故由抽屉原理 $\exists p \neq q \in \mathbb{Z}$ s.t. $a_1a_2...a_p = a_1a_2...a_q$. 此时由消去律 $a_{p+1}a_{p+2}...a_q = 1$，$p+1$ 和 q 满足条件，结论成立. □

1.2.11 设 G 是群，$A, B, H \leqslant G, H \subseteq (A \cup B)$，试证 $H \subseteq A$ 或 $H \subseteq B$.

证明. 反证法，若结论不成立，则 $\exists a, b \in H$ s.t. $a \in A, a \notin B, b \in B, b \notin A$.

考虑 $ab \in H$. 若 $ab \in A$，则 $a^{-1} \in A$ 推出 $b = a^{-1}ab \in A$，矛盾. 若 $ab \in B$，则 $b^{-1} \in B$ 推出 $a = abb^{-1} \in B$，矛盾，故 $ab \notin A \cup B$，与 $H \subseteq A \cup B$ 矛盾. □

1.2.12 试证在偶数阶群 G 中 $x^2 = 1$ 总有偶数个解.

证明. $x^2 = 1 \Leftrightarrow x = x^{-1}$. 由于 $(x^{-1})^{-1} = x$，故满足 $x \neq x^{-1}$ 的元素总是成对出现的，故 $x^2 \neq 1$ 有偶数个解，由总元素为偶数，$x^2 = 1$ 也有偶数个解. □,

1.2.13 验证以下事实：

(1) $\mathrm{SL}_n(F), T_n(F), \mathrm{Diag}_n(F), B_n(F) \leqslant \mathrm{GL}_n(F), T_n(F) \leqslant \mathrm{SL}_n(F), \mathrm{Diag}_n(F) \leqslant B_n(F)$.

(2) $\mathrm{O}_n(\mathbb{R}) \leqslant \mathrm{GL}_n(\mathbb{R}), \mathrm{O}_{p,q}(\mathbb{R}) \leqslant \mathrm{GL}_{p+q}(\mathbb{R}), \mathrm{Sp}_{2n}(\mathbb{R}) \leqslant \mathrm{GL}_{2n}(\mathbb{R})$.

(3) $\mathrm{U}(n) \leqslant \mathrm{GL}_n(\mathbb{C})$.

证明. 留给读者. □

1.2.14 试证群 G 的任意多个子群的交仍是 G 的子群.

证明. 留给读者. □

1.2.15 设 A, B 是群 G 的两个子群，试证：$A \cup B$ 是 G 的子群的充要条件是 $A \leqslant B$ 或 $B \leqslant A$，利用该事实证明：G 不能表为两个真子群的并.

证明. 充分性显然，下证必要性：

在**习题 1.2.11** 中令 $H = A \cup B$，得 $A \cup B \subseteq A$ 或 $\subseteq B$，即 $A \subseteq B$ 或 $B \subseteq A$.

若 $A \neq G, B \neq G$ 为真子群，由 $A \cup B \subseteq A$ 或 B 知 $A \cup B \neq G$. □

1.2.16 设 A, B 是群 G 的两个子群，试证 AB 是 G 的子群 $\Leftrightarrow AB = BA$.

证明. $(\Rightarrow)\forall a \in A, b \in B, ba = (a^{-1}b^{-1})^{-1} \in AB$，由 a, b 的任意性有 $BA \subseteq AB$，反之 $\forall a \in A, b \in B, (ab)^{-1} = (b^{-1}a^{-1}) \in BA$，故 $AB = (AB)^{-1} \subseteq BA$，故 $AB = BA$.

$(\Leftarrow)AB$ 中任取元素 c_1, c_2，下证 $c_1c_2^{-1} \in AB$：

$c_1 = a_1b_1, c_2 = a_2b_2$ 其中 $a_1, a_2 \in A, b_1, b_2 \in B$. 故 $c_1c_2^{-1} = a_1b_1b_2^{-1}a_2^{-1}$，有 $b_1b_2^{-1} \in B$，$a_2^{-1} \in A$，由 $BA = AB$ 得 $\exists a_3 \in A, b_3 \in B$ s.t. $b_1b_2^{-1}a_2^{-1} = a_3b_3$，故 $c_1c_2^{-1} = a_1a_3b_3$，由 $a_1a_3 \in A$，$c_1c_2^{-1}$ 属于 AB，由**命题 1.31** 即得结论. □

1.2.17 设 A 和 B 为有限群 G 的两个非空子集，若 $|A| + |B| > |G|$，证明 $|G| = AB$，特别地，如果 G 有子集 S，$|S| > |G|/2$，证明对任意 $g \in G, \exists a, b \in S$ s.t. $g = ab$.

证明. 反证法，若结论不成立，则 $\exists g \in G$ s.t. $\forall a \in A, b \in B, g \neq ab$，故 $a^{-1}g \neq b$，左边由消去律，不同的 a 导致不同的 $a^{-1}g$，故可取 $|A|$ 个不同值，右边有 $|B|$ 个不同取值，任何左边值不能等于任何右边值导致两边有 $|A| + |B| > |G|$ 个不同值，但两边都是 G 的元素，矛盾. □

1.2.18

(1) 确定 $\mathbb{Z}$ 的所有子群.

解. 令 $A \leqslant \mathbb{Z}$，要么 $A = \{0\}$，要么存在 a 使得它是 A 中绝对值最小的数，若 $a < 0$ 则 $-a \in A$，故不妨设 $a > 0$，由贝祖定理（《**代数学 I: 代数学基础》定理 3.6**）知对 A 中任意元素 b, c，$\gcd(b, c) \in A$，由 a 的最小性，它是所有 A 中元素的最大公约数，故 $A \subseteq a\mathbb{Z}$，易验证 $a \in A \Rightarrow a\mathbb{Z} \subseteq A$，故 $A = a\mathbb{Z}$.

故 $\mathbb{Z}$ 的所有子群为 $\{a\mathbb{Z} \mid a \in \mathbb{N}\}$.

(2) 确定 $\mathbb{Z}/n\mathbb{Z}, n \in \mathbb{N}, n \geqslant 2$ 的所有子群.、

解. 请读者仿照 (1) 自证，注意子群中必有元素 $\overline{n} = \overline{0}$. 所有子群为 $\{a\mathbb{Z}/n\mathbb{Z} \mid a \in \mathbb{N}, a \mid n\}$.

1.2.19 试证：映射 $f : G \to G, a \mapsto a^{-1}$ 是 G 的自同构当且仅当 G 是阿贝尔群.

证明. 由于 $(a^{-1})^{-1} = a$，故 f 为双射显然. f 为同态 $\Leftrightarrow \forall a, b \in G, (ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow \forall a, b \in G, a^{-1}b^{-1} = b^{-1}a^{-1} \Leftrightarrow \forall a, b \in G, ab = ba$. □

1.2.20 设 G_1, G_2, G_3 为群，试证 $G_1 \times G_2 \cong G_2 \times G_1$，$(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$.

证明. 留给读者. □

1.2.21 对下面每一情形，确定是否 $G \cong H \times K$：

(1) $G = \mathbb{R}^\times, H = \{\pm 1\}, K = \mathbb{R}_+^\times$

证明. 类似 (3)，留给读者. □

(2) $G = B_n(F), H = \mathrm{Diag}(F), K = T_n(F)$

解. 由于 G, H, K 的乘法一致，H, K 可看作 G 的子群，若 $G \cong H \times K$ 则 $H \mapsto \{H, 1_K\}$ 和 $K \mapsto \{1_H, K\}$ 中元素应该互相交换. 但与 K 中所有元素都交换的矩阵是数量矩阵 xI_n，于是有两种情况：

(i) $F \neq \mathbb{F}_2$，此时 F 中有多于一个非零元素，取对角线上元素不全相同的可逆对角阵，则它与 K 中元素不全交换，故同构不成立.

(ii) $F = \mathbb{F}_2$，此时 H 为平凡群 $\{I_n\}$，并且 $K \cong G$，自然有 $G \cong H \times K$.

故 $G \cong H \times K$ 当且仅当 $F = \mathbb{F}_2$.

(3) $G = \mathbb{C}^\times, H = S^1, K = \mathbb{R}_+^\times$

证明. 令 $f : \mathbb{C}^\times \to \mathbb{R}_+^\times \times S^1, z = re^{i\theta} \mapsto \{r, e^{i\theta}\}$，由于 $z \neq 0$，易验证 f 是双射且是同态，故同构成立. □

1.2.22 证明有理数加法群 $\mathbb{Q}$ 和有理数乘法群 $\mathbb{Q}^\times$ 不同构.

证明. 反证法，若同构 $f : \mathbb{Q} \to \mathbb{Q}^\times$ 存在，则 $\exists a \in \mathbb{Q}$，使得 $f(a) = 2$，因 $b = \frac{a}{2} \in \mathbb{Q}$，由同态的性质 $f(b)^2 = 2$，而 $f(b) \in \mathbb{Q}^\times, f(b) = \frac{p}{q}$ $(p, q \in \mathbb{Z}, \gcd(p, q) = 1)$，得 $p^2 = 2q^2 \Rightarrow 2 \mid p^2 \Rightarrow 2 \mid p \Rightarrow 2(\frac{p}{2})^2 = q^2 \Rightarrow 2 \mid q^2 \Rightarrow 2 \mid q \Rightarrow 2 \mid \gcd(p, q)$，矛盾. □

1.2.23

(1) 令 G 是实数对 (a, b) $(a \neq 0)$ 的集合. 在 G 上定义乘法 $(a, b)(c, d) = (ac, ad + b)$，试证 G 是群.

证明. G 对乘法封闭：$ac \neq 0 \Leftarrow a \neq 0, c \neq 0$.

单位元：$(1, 0)(c, d) = (c, d + 0) = (c, d), (a, b)(1, 0) = (a, 0 + b) = (a, b)$，故 $(1, 0)$ 是 G 的单位.

逆元：$(a,b)(1/a,-b/a)=(1,-b+b)=(1,0),(1/a,-b/a)(a,b)=(1,b/a-b/a)=(1,0)$，故 $(a,b)_G^{-1}=(1/a,-b/a)$.

结合律：$((a,b)(c,d))(e,f)=(ac,ad+b)(e,f)=(ace,acf+ad+b),(a,b)((c,d)(e,f))=(a,b)(cd,d+cf)=(ace,acf+ad+b)$. 两者相同. □

(2) 试证 G 同构于 $\mathrm{GL}_2(\mathbb{R})$ 的子群

$$H=\left\{\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}|a\in\mathbb{R}^\times,b\in\mathbb{R}\right\}$$

.

证明. 同构映射显然，只证同态性，其他留给读者.

$$\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\begin{pmatrix}c & d\\ 0 & 1\end{pmatrix}=\begin{pmatrix}ac+0 & ad+b\\ 0+0 & 0+1\end{pmatrix}=\begin{pmatrix}ac & ad+b\\ 0 & 1\end{pmatrix}$$

□

1.2.24 群 G 的自同构 α 称为没有不动点，是指对 G 的任意元素 $g\neq 1_G,\alpha(g)\neq g$. 如果 α 为没有不动点的自同构且 $\alpha^2=\mathrm{id}$，证明 G 为奇数阶阿贝尔群.

证明. 由于 $\alpha(\alpha(g))=g\neq\alpha(g),\forall g\neq 1$，因此 G 中非 1_G 元素成对出现，G 的阶为奇数.

以下证明 G 为阿贝尔群的过程可以仔细思考**习题 1.3.15** 的证明过程得到：

考虑 $f:G\to G,x\mapsto x\alpha(x)^{-1}$,

若 $f(x_1)=f(x_2)$，则 $x_1\alpha(x_1)^{-1}=x_2\alpha(x_2)^{-1}\Leftrightarrow x_2^{-1}x_1=\alpha(x_2)^{-1}\alpha(x_1)\Leftrightarrow x_2^{-1}x_1=\alpha(x_2^{-1}x_1)$. 因 α 没有不动点，得 $x_2^{-1}x_1=1_G$，即 $x_1=x_2$. 故 f 是单射. 由于 f 是 G 到自身的映射，因此 f 也是满射.

故 $\forall y\in G,\exists x$ s.t. $y=x\alpha(x)^{-1}$，$\therefore\alpha(y)=\alpha(x)\alpha(\alpha(x^{-1}))=(\alpha(x)^{-1})^{-1}x^{-1}=y^{-1}$，即 α 将每个元素映射至其逆元.

由**习题 1.2.19** 知 G 是阿贝尔群. □

1.3 子群与陪集分解

1.3.1 设 $A=\begin{pmatrix}0&-1\\1&0\end{pmatrix}, B=\begin{pmatrix}0&1\\-1&1\end{pmatrix}$，试求 A, B, AB, BA 在 $\mathrm{GL}_2(\mathbb{R})$ 中的阶.

解. (1) $A^2=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}, A^4=I$. A 的阶为 4.

(2) $B^2=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}, B^3=I$. B 的阶为 3.

(3) $AB=\begin{pmatrix}1&1\\0&1\end{pmatrix}, (AB)^n=\begin{pmatrix}1&n\\0&1\end{pmatrix}\neq I$. AB 的阶为 ∞.

(4) $BA=\begin{pmatrix}1&0\\-1&1\end{pmatrix}, (AB)^n=\begin{pmatrix}1&0\\-n&1\end{pmatrix}\neq I$. BA 的阶为 ∞.

1.3.2 试证群中元素 a 的阶 $\leqslant 2$ 当且仅当 $a=a^{-1}$.

证明. 留给读者. □

1.3.3 设 a, b 为群 G 中的两个元素，a 的阶为 7 且 $a^3b=ba^3$. 试证 $ab=ba$.

证明. $ab=a^{15}b=a^{12}ba^3=a^9ba^6=a^6ba^9=a^3ba^{12}=ba^{15}=ba$. □

1.3.4 设 x 在群中阶为 n，求 x^k $(k\in\mathbb{Z})$ 的阶.

解. 考虑 x 生成的子群 $\langle x\rangle$. 请读者利用**命题 1.54** 得到结果 $\frac{n}{\gcd(k,n)}$.

1.3.5

(1) 设 G 是有限阿贝尔群，试证：

$$\prod_{g\in G} g=\prod_{\substack{a\in G\\ a^2=1}} a$$

证明. $\because g\in G\Rightarrow g^{-1}\in G$，故 $g\neq g^{-1}$ 的项两两积为 1 可消去，余下的项满足 $g=g^{-1}, g^2=1$. □

(2) 证明 Wilson 定理：p 是素数则 $(p-1)!\equiv -1 \mod p$.

证明. $(p-1)!=\prod_{g\in\mathbb{F}_p} g=\prod_{a\in\mathbb{F}_p, a^2=1} a$. 此时 $a^2=kp+1$ $(k\in\mathbb{Z})$,

$\therefore (a-1)(a+1)=kp, p\mid (a-1)(a+1)$，由 p 为素数，$p\mid a-1$ 或 $p\mid a+1$.

故 $a\equiv\pm 1 \mod p$，在 $\mathbb{F}_p$ 中即为 $a=1$ 或 $p-1$，故原式 $\equiv 1\cdot(p-1)\equiv -1 \mod p$. □

1.3.6 证明 $f=\frac{1}{x}, g=\frac{x-1}{x}$ 生成一个函数群，合成法则是函数的合成，它同构于二面体群 D_3.

证明. 群的性质请读者自证.

$f^2(x)=f(f(x))=x$，故 $f^2=\mathrm{id}$.

$g^2(x)=g(g(x))=-\frac{1}{x-1}, g^3(x)=g(g^2(x))=x$，故 $g^3=\mathrm{id}$.

$f\circ g(x)=\frac{x}{x-1}, g^2\circ f(x)=g^2(f(x))=-\frac{x}{1-x}=\frac{x}{x-1}$,

将 f 看作反射，g 看作旋转，有 $\langle f,g\rangle=\langle f,g:f^2=g^3=1,fg=g^{-1}f\rangle\cong D_3$. □

1.3.7

(1) S^1 的任意有限阶子群都是循环群.

证明. 因该子群有限，可取该群中 1 以外辐角主值最小者为 $e^{i\theta_0}$.

若有任何（包括 $1=e^{2k\pi i}$）元素 $e^{i\theta}$ 使得 θ 不为 θ_0 的倍数，则必有 $e^{i\theta}=e^{k\theta_0+\theta_1}$ $(0<\theta_1<\theta_0), e^{i\theta}(e^{i\theta_0})^{-k}=e^{i\theta_1}$ 也是群中元素，与 θ_0 最小性矛盾.

故 $\{e^{im\theta_0}\mid m\in\mathbb{N}\}$ 为群中全部元素，并且 2π 为 θ_0 的倍数，该群同构于 $\mathbb{Z}/k\mathbb{Z}$ 其中 $k=2\pi/\theta_0\in\mathbb{Z}$. □

(2) $\mathbb{Q}$ 不是循环群，但它的任意有限生成的子群都是循环群.

证明. 若 $\mathbb{Q}$ 是循环群，设它的生成元为 g，则 $\frac{g}{2}\neq kg$ $(\forall k\in\mathbb{Z})$ 是 $\mathbb{Q}$ 的元素，矛盾.

设 $A=\langle a_1,a_2,...,a_n\rangle\subset\mathbb{Q}$. 由于 A 有限，令 A 中所有元素的分母的最大公倍数为 k，则 $kA=\{kx\mid x\in A\}\cong A$，且 $kA\leqslant\mathbb{Z}$. 而 $\mathbb{Z}$ 的一切子群都是循环群，故 A 也是循环群. □

(3) 设 p 为素数，

$$G=\{x\in\mathbb{C}\mid\exists n\in\mathbb{N}\text{ s.t. }x^{p^n}=1\}$$

的任意真子群都是有限阶循环群.

证明. 设真子群为 G_0，则 $\exists a\notin G_0, a\in G, G_0\leqslant G$，则 $\exists n_0$ s.t. $a^{p^{n_0}}=1$ 且 $a^{p^{n_0-1}}\neq 1$，即 a 是 p^{n_0} 次本原单位根.

对任意 $k\in\mathbb{Z}$ 且 $p\nmid k$，由数论知 $\exists m\in\mathbb{Z}$ s.t. $km\equiv\gcd(k,p^{n_0})=1 \mod p^{n_0}, a=(a^k)^m$. 因此 $a\notin G_0\Rightarrow a^k\notin G_0$，即 p^{n_0} 次本原单位根均不在 G_0 中. 对 p^n $(n>n_0)$ 次单位根，由于它的 p^{n-n_0} 次幂是 p^{n_0} 次本原单位根，故也不在 G_0 中.

n_0 为 a 的函数，对一切 a 取最小的 n_0 则 G_0 含有 p^{n_0-1} 次本原单位根，并且易得到 G_0 是所有 p^{n_0-1} 次单位根的集合，它同构于 $\mathbb{Z}/p^{n_0-1}\mathbb{Z}$，为有限阶循环群. □

1.3.8 设 a 和 b 是群 G 的元素，阶数分别是 n 和 m，$\gcd(n,m)=1$ 且 $ab=ba$，试证 $\langle ab\rangle$ 是 G 的 mn 阶循环子群.

证明. 由于 a,b 交换，则 $(ab)^k=a^kb^k$. 我们只需证 $mn\nmid k$ 时 $a^kb^k\neq 1$，$a^{mn}b^{mn}=1$ 即可. 对于后者，$a^{mn}b^{mn}=(a^n)^m(b^m)^n=1$.

对于前者，$mn\nmid k$ 时因 $\gcd(m,n)=1$ 有 $m\nmid k$ 或 $n\nmid k$，我们有 $a^k\neq 1$ 或 $b^k\neq 1$. 不妨设 $a^k\neq 1$，此时 $n\nmid k$，若 $b^k=(a^k)^{-1}$，则 $a^{mk}=b^{-m}=1$，由于 m,n 互素，我们有 $n\nmid mk$，与 a 的阶是 n 矛盾. 故 $b^k\neq(a^k)^{-1}, a^kb^k\neq 1$. □

1.3.9 设 p 为奇素数，X 是 n 阶整系数方阵，如果 $I+pX\in \mathrm{SL}_n(\mathbb{Z})$ 的阶有限, 证明 $X=0$.

证明. 令 $X\neq 0$，若 $I+pX$ 的阶有限，则存在 $n\in\mathbb{Z}_+$ s.t. $(I+pX)^n=I$，也就是

$$p^nX^n+np^{n-1}X^{n-1}+...+\frac{n(n-1)}{2}p^2X^2=-npX \qquad (*)$$

我们记 $u=\gcd(X)$，是指整系数方阵 X 中所有元素的最大公约数为 u. 取 k 使得 $p^k\mid \gcd(X)$，$p^{k+1}\nmid \gcd(X)$，则 $k\geqslant 0$. 我们说 u 整除整系数方阵 X，是指 X 中所有元素被 u 整除.

(i) 当 $p\nmid n$ 时 $(*)$ 右边不被 p^{k+2} 整除，左边各项分别被 $p^{nk+n},p^{(n-1)k+(n-1)},...,p^{2k+2}$ 整除，故它被 p^{2k+2} 整除，但 $2k+2\geqslant k+2$，与右边不被 p^{k+2} 整除矛盾.

(ii) 当 $n=p$ 时，$(*)$ 右边不被 p^{k+3} 整除，左边每项各被 $p^{pk+p},p^{(p-1)k+p-1+1},...,p^{2k+3}$ 整除（注意 p 为奇素数，有 $p\geqslant 3$ 和 $p\mid \frac{p(p-1)}{2}$），故它被 p^{2k+3} 整除，但 $2k+3\geqslant k+3$，与右边不被 p^{k+3} 整除矛盾.

(iii) 一般情况，此时 $(I+pX)^{p^ms}=I$，其中 $p\nmid s,m\geqslant 0$.

若 $m\geqslant 1$，令 $(I+pX)^{p^{m-1}s}=I+pY$（左边二项展开除 I 以外的项被 p 整除），则 $(I+pY)^p=I$，由 (ii) 知 $Y=0$，即 $(I+pX)^{p^{m-1}s}=I$，对 m 作归纳可归结到 $m=0$ 的情形 $(I+pX)^s=I$，由 (i) 知 $X=0$. □

1.3.10 设 g_1,g_2 是群 G 的元素，H_1,H_2 是 G 的子群，证明以下两个条件等价：

（1）$g_1H_1\subseteq g_2H_2$；（2）$H_1\subseteq H_2$ 且 $g_2^{-1}g_1\in H_2$.

证明. （2）⇒（1）因为消去律成立，只需证 $g_2^{-1}g_1H_1\subseteq H_2$ 即可. 因 $\forall h_1\in H_1\Rightarrow h_1\in H_2$，又 $g_2^{-1}g_1\in H_2$，则 $g_2^{-1}g_1h_1\in H_2$，（1）成立.

（1）⇒（2）$\because g_1H_1\subseteq g_2H_2,\therefore \forall h_{11}\in H_1,\exists h_{21}$ s.t. $g_1h_{11}=g_2h_{21}$，且 $\forall h_{12}\in H_1,h_{11}h_{12}\in H_1\Rightarrow \exists h_{22},g_1h_{11}h_{12}=g_2h_{22}$.

即 $g_2h_{22}=g_1h_{11}h_{12}=g_2h_{21}h12$，故 $h_{12}=h_21^{-1}h_22\in H_2$，由 h_{12} 的任意性知 $H_1\subseteq H_2$.

于是（1）⇒ $\forall h_1\exists h_2$ s.t. $g_1h_1=g_2h_2\Leftrightarrow g_2^{-1}g_1=h_2h_1^{-1}$，$h_1^{-1}\in H_1\subseteq H_2$ 故右边属于 H_2，故 $g_2^{-1}g_1\in H_2$. □

1.3.11 设 G 是 n 阶有限群，若对 n 的每一个因子 m，G 中至多只有一个 m 阶子群，则 G 是循环群.

证明. G 中的所有 m 阶元素属于 m 阶子群，这些子群至多只有一个.

该子群中只有 $\varphi(m)=|\{u\mid \gcd(u,m)=1\}|$ 个 m 阶元素，所以 m 阶元素个数 $c(m)\leqslant\varphi(m)$.

因为 $\forall m,m\mid |G|$，因此 $|G|=\sum_{m||G|}c(m)$. 但 $\sum_{m||G|}\varphi(m)=|G|$（该式证明见《代数学 I：代数学基础》，也可考虑 $|G|$ 阶循环群来证明）

故对一切 $m\mid |G|,c(m)=\varphi(m)$，特别地，$G$ 中存在 $|G|$ 阶元素，故为循环群. □

1.3.12 举一个无限群的例子，它的任意阶数不为 1 的子群都有有限指数.

解. 由**习题 1.2.18(1)**，$\mathbb{Z}$ 的子群为 0 或 $n\mathbb{Z}$ $(n\in\mathbb{Z}_+)$，故它的任意阶数不为 1 的子群都有有限指数 n.

1.3.13

(1) 设 G 是阿贝尔群，H 是 G 中所有有限阶元素构成的集合，证明 H 是 G 的子群.

证明. 只需证 H 对乘法和逆运算封闭. $\forall h_1, h_2 \in H, \exists k_1, k_2 \in \mathbb{Z}_+$ s.t. $h_1^{k_1} = 1, h_2^{k_2} = 1$，则 $(h_1 h_2^{-1})^{\mathrm{lcm}(k_1,k_2)} = h_1^{\mathrm{lcm}(k_1,k_2)} h_2^{-\mathrm{lcm}(k_1,k_2)} = 1$，故 $h_1 h_2^{-1} \in H$. □

(2) 举例说明上述结论对一般群不正确.

解. 在**习题 1.3.1** 中令 $G = \mathrm{GL}_2(\mathbb{R})$，$H$ 为其中有限阶元集合，则 $A, B \in H$，$AB, BA \notin H$，H 不是子群.

1.3.14

(1) 设 G 是奇数阶阿贝尔群，证明由 $\varphi(x) = x^2$ 定义的映射 $\varphi : G \to G$ 是一个自同构.

(2) 推广 (1) 的结果.

证明. 我们只证：若 G 是阿贝尔群，$p \nmid |G|$ (p为素数)，则 $\varphi(x) = x^p, \varphi : G \to G$ 是自同构. (1) 的结论取 $p = 2$ 立得.

由交换性易得 φ 是同态，我们只需证明 φ 是满射.

若不然，则 $\exists x \neq y, x^p = y^p$，故 $(xy^{-1})^p = 1_G$，xy^{-1} 不是单位元，它必是 p 阶元，则它生成的 p 阶循环群是 G 的子群，$p \mid |G|$，矛盾, □

1.3.15 设 G 是阿贝尔群，$\alpha \in \mathrm{Aut}(G)$ 且 $\alpha^2 = \mathrm{id}$，令

$$G_1 = \{g \in G \mid \alpha(g) = g\}, G_{-1} = \{g \in G \mid \alpha(g) = g^{-1}\}.$$

(1) 如果 G 是奇数阶有限群，试证：$G = G_1 G_{-1}$ 且 $G_1 \bigcap G_{-1} = \{1\}$.

证明. 利用**习题** 1.3.14(1) 的结果，G 为奇数阶阿贝尔群 $\Rightarrow \varphi(x) = x^2$ 是自同构，故是满射，即对 $\forall g \in G$，存在唯一的 $h \in G$ 使得 $h^2 = g$. 以下利用本题第 (2) 问的结果即可. □

(2) 设 G 满足对 $\forall g \in G$，存在唯一的 $h \in G$ 使得 $h^2 = g$. 则 (1) 中结论仍成立.

证明. $g \in G_1 \bigcap G_{-1} \Rightarrow \alpha(g) = g = g^{-1}$，即 $g^2 = 1$. 若 $g \neq 1$ 则 $\forall g_0 \in G, \exists h \in G$ s.t. $g_0 = h^2 = h^2 g^2 = (hg)^2$，而 $h' = hg \neq h$，与 h 唯一矛盾.

故 $G_1 \bigcap G_{-1} = \{1\}$，且 $g^2 = 1 \Rightarrow g = 1$ 对任意 $g \in G$ 成立 (*).

$\forall g \in G, \exists h, j \in G$ s.t. $g = h^2, \alpha(g) = j^2$.

则 $\alpha(hj)^2 (hj)^{-2}$

$= \alpha(h^2 j^2) h^{-2} j^{-2}$

$= \alpha(g\alpha(g)) g^{-1} \alpha(g)^{-1}$

$= \alpha(g)\alpha(\alpha(g))(\alpha(\alpha(g)))^{-1} \alpha(g)^{-1}$

$= 1$

即 $(\alpha(hj)(hj)^{-1})^2 = 1 \Rightarrow \alpha(hj)(hj)^{-1} = 1(*) \Rightarrow hj = \alpha(hj) \in G_1$.

同样，$(\alpha(hj^{-1})hj^{-1})^2$

$= \alpha(h^2j^{-2})h^2g^{-2}$

$= \alpha(g\alpha(g)^{-1})g\alpha(g)^{-1}$

$= \alpha(g)\alpha(\alpha(g^{-1}))g\alpha(g)^{-1}$

$= \alpha(g)g^{-1}g\alpha(g)^{-1}$

$= 1$

$\Leftrightarrow \alpha(hj^{-1})hj^{-1} = 1 \quad (*)$

$\alpha(hj^{-1}) = (hj^{-1})^{-1}$

$hj^{-1} \in G_{-1}$.

故 $\forall g \in G, g = h^2 = (hj)(hj^{-1}) \in G_1G_{-1}$. □

(2i) 由 (2) 证明：任何域 F 上的矩阵可以写成对称阵和反对称阵之和.

证明. 在 (2) 中取 $\alpha : A \mapsto A^T$，取 G 为矩阵加法群，则 $h = \frac{A}{2}$，G_1 为对称阵集合，G_{-1} 是反对称阵集合. 由 (2) 可得结论. □

(2ii) 由 (2) 证明：任何函数 $f : \mathbb{R} \to \mathbb{R}$ 可以写成奇函数和偶函数之和.

证明. 在 (2) 中取 $\alpha : f \mapsto f^T, f^T(x) = f(-x)$，取 G 为 f 的集合，加法为函数的加法 $(f+g)(x) = f(x)+g(x)$，则 G 为阿贝尔群，$h(x) = \frac{g(x)}{2}$，G_1 为偶函数集合，G_{-1} 为奇函数集合，由 (2) 可得结论. □

1.3.16

(1) 求有理数加法群的自同构群 $\mathrm{Aut}(\mathbb{Q})$.

解. $\forall f \in \mathrm{Aut}(\mathbb{Q}), 1 \neq 0 \Rightarrow f(1) \neq f(0) = 0, f(1) \in \mathbb{Q}^\times$. 对 $f(m), m \in \mathbb{Z}_+$ 有 $f(m) = f(\underbrace{1+...+1}_{m个} = mf(1)), f(-m) = -f(m)$，故对 $f(a), a \in \mathbb{Q} - \{0\}$ 有 $a = \frac{p}{q}, p, q \in \mathbb{Z}, qf(a) = f(p) = pf(1), f(a) = af(1)$.

另一方面，$f : \mathbb{Q} \to \mathbb{Q}, x \mapsto ax, a \in \mathbb{Q}^\times$ 确为 $\mathbb{Q}$ 的同构，且 $fg(x) = a_fa_gx$. 故 $\mathrm{Aut}(\mathbb{Q}) \cong \mathbb{Q}^\times$.

(2) 求整数加法群的自同构群 $\mathrm{Aut}(\mathbb{Z})$.

解. 类似 (1)，只有 $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto ax$ 满足条件. 由 $f(1), f^{-1}(1) \in \mathbb{Z}$ 知 $a, a^{-1} \in \mathbb{Z}$，只有 $a = \pm 1$，即 $\mathrm{Aut}\,\mathbb{Z} = \{\pm 1\}^\times \cong \mathbb{Z}/2\mathbb{Z}$.

(3) 计算 $K_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 的自同构群.

解. $K_2 = \{1, a, b, ab \mid ba = ab, a^2 = b^2 = 1\}$，易知 $\forall f \in \mathrm{Aut}(K_2), f(b) \neq f(a), f(b), f(a) \neq 1$ 且 $f(ab) = f(a)f(b) \neq 1$ 由 $f(a)$ 和 $f(b)$ 唯一确定. 故 $\mathrm{Aut}(K_2) \cong S_3$.

(4) 求非零有理数乘法群 $\mathbb{Q}^\times$ 的自同构群 $\mathrm{Aut}\,\mathbb{Q}^\times$.

解. $\forall x \in \mathbb{Q}^\times$，由算术基本定理，$x$ 可唯一写作

$$x = \prod_{p_i \in P} p_i^{n_i}, n_i \in \mathbb{Z}\text{且只有有限多个 } n_i \text{ 不为 } 0,\ P \text{ 为所有质数的集合}$$

于是 f 由 $\{f(p_i) \mid p_i \in P\}$ 唯一确定，而 $f(p_i) = \prod_{p_j \in P} p_j^{a_{ij}}$. $f(x) = \prod_{p_j \in P} p_j^{\sum_{i=1}^{\infty} a_{ij} n_i}$.

要使 f 为双射，$b_j = \sum_{i=1}^{\infty} a_{ij} n_i$，则 $\{b_j\}$（只有有限项不为 0）和 $\{n_i\}$（只有有限项不为 0）应当互相唯一确定.

令 $A = \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots \\ \vdots & \ddots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}, B = (b_1, ..., b_j, ...), N = (n_1, ..., n_i, ...)$，则 $B = NA, N = BA^{-1}$.

即 $\mathrm{Aut}(\mathbb{Q}^\times) = \{A \mid \forall$整系数有限项不为 0 的向量$B, N = BA^{-1}$为整系数有限项不为 0 向量, $\forall$整系数有限项不为 0 的向量$N, B = NA$为整系数有限项不为 0 向量$\}$

1.3.17

(1) 设 p 是素数，p 方幂阶群是否一定含有 p 阶元?

解. 是的，因为此群非平凡，其中必有阶不为 1 的元素，设非单位元的最小阶为 k，则 $k \mid p^n, k = p^m (m \geqslant 1), g^k = 1 \Rightarrow (g^{p^{k-1}})^p = 1$，$g^{p^{k-1}}$ 为 p 阶元.

(2) 35 阶群是否一定同时含有 5 阶和 7 阶元素?

证明. 是的，G 中非单位元的阶只可能是 $5, 7, 35$. 若 G 中有 35 阶元 g，则 g^5 是 7 阶元，g^7 是 5 阶元. 假设 G 中不含 35 阶元并只有 5 阶非单位元. $\forall a, b \in G - \{1\}$，则 $a^5 = b^5 = 1$，5 为素数，$b = (b^2)^3 = (b^3)^2 = (b^4)^4$，$\{a, a^2, a^3, a^4\}, \{b, b^2, b^3, b^4\}$ 要么不交，要么重合. 故 G 由 1 和若干个 4 元集的不交并组成，但 $4 \nmid 35 - 1$，矛盾.

同理 $6 \nmid 35 - 1 \Rightarrow$ 不可能 G 中不含 35 阶元并只有 7 阶非单位元. □

(3) 若有限群 G 含有 10 阶元 x 和 6 阶元 y，那么 G 的阶应该满足什么条件?

解. $|\langle x \rangle| \mid |G|, |\langle y \rangle| \mid |G| \Rightarrow 30 \mid |G|$. 另一方面 $\mathbb{Z}/30n\mathbb{Z}$ 满足条件，故 G 应满足 $30 \mid |G|$.

1.3.18 如果 H 与 K 是 G 的子群且阶互素，证明 $H \bigcap K = \{1\}$.

证明. $H \bigcap K$ 是 H 和 K 的子群，故 $|H \bigcap K| \mid |H|, |K| \Rightarrow |H \bigcap K| \mid \gcd(|H|, |K|) = 1$，故 $|H \bigcap K| = 1$，它是平凡群. □

1.3.19 设 $\mathbb{R}^m$ 为 m 维实向量空间，A 是任意 $n \times m$ 实矩阵，$W = \{X \in \mathbb{R}^m \mid AX = 0\}$

证明线性方程 $AX = B$ 的解空间或是空集，或是加法群 $\mathbb{R}^m$ 关于 W 的陪集.

证明. 若解空间不空，$\forall x_1, x_2$ s.t. $AX = B$ 有 $Ax_1 = Ax_2 = B \Rightarrow A(x_1 - x_2) = 0 \Leftrightarrow x_1 - x_2 \in W$，由**引理 1.56**，陪集 $x_1+W = x_2+W$. 且任意 $x_3 \in W, Ax_1 = B \Leftrightarrow A(x_1+x_3) = Ax_1+Ax_3 = B+0 = B$，故解空间由且只由这一个陪集组成. □

1.3.20 设 H 和 K 分别是有限群 G 的两个子群，$HgK = \{hgk \mid h \in H, k \in K\}$，试证：

$$|HgK| = |H| \cdot (K : g^{-1}Hg \bigcap K)$$

证明. 陪集 $(H)gk_1$ 与 $(H)gk_2$ 相同
$\Leftrightarrow gk_1k_2^{-1}g^{-1} \in H$
$\Leftrightarrow k_1k_2^{-1} \in g^{-1}Hg$
又 $k_1k_2^{-1} \in K$，故 $k_1k_2^{-1} \in g^{-1}Hg \bigcap K$（记后者为 L），易证 L 为 K 的子群.

故使 Hgk 相异的 k_1, k_2 分属于 L 的不同陪集 Lk_1 与 Lk_2，即 k 共有 $(K : L)$ 种取法，又每个陪集 Hgk 有 $|H|$ 个元素，故 $|HgK| = |H| \cdot (K : L)$. □

1.3.21 设 a, b 是群 G 的任意两个元素，试证 a 与 a^{-1}，ab 与 ba 两对元素各有相同的阶.

证明. 令 a 的阶为 k，则 $(a^{-1})^k = (a^k)^{-1} = 1$，反之亦然.

ab 的阶为 m，ba 的阶为 n，则 $(ba)^m = a^{-1}(ab)^m a = a^{-1}a = 1, (ab)^n = b^{-1}(ba)^n b = b^{-1}b = 1$，故 $m \mid n$ 且 $n \mid m$，$n = m$. □

1.3.22 设 $f : G \to H$ 是群同态，如果 g 是 G 的有限阶元，则 $f(g)$ 的阶整除 g 的阶.

证明. $f(g)^n = f(g^n) = 1$. □

1.3.23

(1) 设 A 是群 G 的有限指数子群，试证：存在 G 的一组元素 $g_1, ..., g_n$ 可作 A 在 G 中的右陪集代表元系，又可作 A 在 G 中的左陪集代表元系.

此证法来源于文献 [3]

证明. 将 G 分拆为双陪集 $G = \bigsqcup_{x \in J_1} AxA$，易见 Ax_1（或 x_1A）与 AxA 要么不交，要么属于 AxA. 故只须对每一个双陪集 AxA 寻找 $\{s_i \mid i \in I\}, \{t_i \mid i \in I\} \subseteq A$ 使得 $AxA = \bigsqcup_{i \in I} Axt_i = \bigsqcup_{i \in I} s_ixA$，此时 s_ixt_i 为 AxA 中 A 的左陪集和右陪集的代表元系（$\because As_1xt_i = Axt_i, s_ixt_iA = s_ixA$）. 由**习题 1.3.20** 的证明过程，$AxA$ 中 A 的右陪集个数应等于 $(A : x^{-1}Ax \bigcap A) = |I|$.

对不同的 $i, j \in I$，$(s_ixt_i)(s_jxt_j)^{-1} \notin A, (s_ixt_i)^{-1}(s_jxt_j) \notin A$，得 $t_it_j^{-1} \notin x^{-1}Ax, s_i^{-1}s_j \notin xAx^{-1}$，记 $x^{-1}Ax \bigcap A = B$，$A \bigcap xAx^{-1} = C$. 则 $Bt_i \neq Bt_j, s_iC \neq s_jC$.

将 A 拆分为 B 的右陪集 $A = \bigsqcup_{i \in I_1} By_i$，$C$ 的左陪集 $A = \bigsqcup_{i \in I_2} z_iC$. 注意到 $xBx^{-1} = C$，B 与 C 共轭，且 $(A : B) \leqslant (G : B) \leqslant (G : A)(G : x^{-1}Ax) = (G : A)^2$ 有限，故 $|I| = |I_1| = |I_2| = (A : B) = (A : C)$，令 $s_i = z_i$，$t_i = y_i$，则 s_ixt_i 为 AxA 中 A 的左（右）陪集代表元系. 对所有不同的 AxA 重复上述过程即得结论. □

(2) 举例说明 $(G:A)$ 和 $|A|$ 均无限时上述结论可以不成立.

解. $A=\langle a,b\rangle, G=\langle a,b,x \mid x^{-1}ax=a^2, x^{-1}bx=b^2\rangle$，则 $B=\langle a^2,b^2\rangle, C=A$，$(A:B)=\infty, (A:C)=1$，$I_1$ 和 I_2 之间不存在双射.

1.3.24 （线性代数）

1.3.25 对于有限群 G 设 $d(G)$ 为最小的正整数 s 使得 $\forall g\in G, g^s=1$.

(1) $d(G)$ 是 $|G|$ 的因子，它等于 G 中所有元素阶的最小公倍数.

证明. 设 a 的阶为 m，则 $a^p=1\Leftrightarrow m\mid p$，由公倍数的性质立得 $d(G)$ 为所有 m 的最小公倍数. 因 $|G|$ 为各 m 的公倍数，故 $d(G)\mid |G|$. □

(2) 如果 G 为阿贝尔群，则 G 中存在元素阶为 $d(G)$.

证明. 由算术基本定理，$d(G)=\prod_{i=1}^n p_i^{n_i}$，其中 $\{p_i\}$ 为各异的素数. 由最小公倍数的性质对任意 p_i 有 G 的元素 g_i 阶为 $p_i^{n_i}s$，于是 $h_i=g_i^s$ 的阶为 $p_i^{n_i}$.

设 G 中两个元素 a,b 的阶各为 m,n 且 m,n 互素，则由**习题 1.3.8** 知 ab 的阶为 mn.

假设 $\prod_{i=1}^s h_i$ 的阶为 $\prod_{i=1}^s p_i^{n_i}$，若 $s<n$，则存在 h_{s+1} 且阶 $\prod_{i=1}^s p_i^{n_i}$ 与 $p_{s+1}^{n_{s+1}}$ 互素，故 $\prod_{i=1}^{s+1} h_i$ 的阶为 $\prod_{i=1}^{s+1} p_i^{n_i}$. 由于当 $s=1$ 时假设成立，故 $s=n$ 时假设成立，此时 $\prod_{i=1}^n h_i$ 的阶为 $d(G)$. □

(3) 有限阿贝尔群 G 为循环群 $\Leftrightarrow d(G)=|G|$.

证明. ($\Rightarrow$) 显然，($\Leftarrow$) 利用 (2) 的结论，G 中存在 $|G|$ 阶元，故为循环群. □

1.4 正规子群与商群

1.4.1 令 $G=\{(a,b)|a\in\mathbb{R}^\times,b\in\mathbb{R}\}$. 乘法定义为

$$(a,b)(c,d)=(ac,ad+b)$$

则 $K=\{(1,b)|b\in\mathbb{R}\}$ 为 G 的正规子群且 $G/K\cong\mathbb{R}^\times$.

证明. 令 $g=(a,b)$ 则 $gK=\{(a,ab_k+b)\mid b_k\in\mathbb{R},a\neq0\}=\{(a,c)\mid c\in\mathbb{R},a\neq0\}$. $Kg=\{(a,b+b_k)\mid b_k\in\mathbb{R},a\neq0\}=\{(a,c)\mid c\in\mathbb{R},a\neq0\}$, 故对任何 g 有 $gK=Kg$, K 为 G 的正规子群. 且 $h:gK\to R^\times,\{(a,c)\mid c\in\mathbb{R},a\neq0\}\mapsto a\ (a\neq0)$ 为一一对应.

$g_1Kg_2K=(a_1,c_1)(a_2,c_2)\quad(c_1,c_2\in\mathbb{R})=(a_1a_2,a_1c_2+c_1)$ 故 $h(g_1Kg_2K)=a_1a_2$, h 是同态, 故为同构. $G/K\cong\mathbb{R}^\times$ □

1.4.2 证明行列式为正的实矩阵组成的 $G=\mathrm{GL}_n(\mathbb{R})$ 的子集 H 构成一个正规子群, 并描述商群 G/H.

证明. 由行列式在矩阵乘法中的性质知 H 对乘法和逆封闭, 故 H 是子群. $\forall h\in H$ 有 $hH=H=Hh$, $\forall h\notin H$ 有 $hH=G-H=Hh$, 故 H 为 G 的正规子群. 令 $G-H=J$, 则 $J=AH,A=\begin{pmatrix}0&1&\cdots&\cdots\\1&0&\cdots&\cdots\\\vdots&\vdots&\ddots&\vdots\\\cdots&\cdots&\cdots&1\end{pmatrix}$ 为第二类初等矩阵. $A^2=I$, $G/H\cong\{1,-1\}^\times\cong\mathbb{Z}/2\mathbb{Z}$. □

1.4.3 设 G 为群, $N\leqslant M\lhd G$.

(1) 若 $N\lhd G$ 则 $N\lhd M$.

证明. $N\lhd G\Leftrightarrow\forall g\in G,gN=Ng$. $N\lhd M\Leftrightarrow\forall g\in M,gN=Ng$. 前者为后者充分条件. □

(2) 若 $N\lhd M$ 是否一定 $N\lhd G$?

解. 否, 考虑交换群 A_4, $B=\{\mathrm{id},(12)(34),(13)(24),(14)(23)\}\cong K_2$, $C=\{\mathrm{id},(12)(34)\}\cong\mathbb{Z}/2\mathbb{Z}$, 则 $C\lhd B,B\lhd A_4$, 但 C 不是 A_4 的正规子群.

1.4.4

(1) 试证: 群 G 的中心 $Z(G)$ 是 G 的正规子群.

证明. 因为 $Z(G)$ 中元素各自成一个共轭类, 故它是共轭类之并, 只需证明 $Z(G)$ 是子群.

$\forall z_1,z_2\in Z(G),\forall g\in G,g^{-1}z_1z_2^{-1}g=g^{-1}z_1gg^{-1}z_2^{-1}g=g^{-1}z_1g(g^{-1}z_2g)^{-1}=z_1z_2^{-1}$, 故 $z_1z_2^{-1}\in Z(G)$, $Z(G)$ 是子群. □

(2) 群 G 的指数为 2 的子群一定是 G 的正规子群.

证明. $(G:H)=2$, 则 G 的陪集分解为 $G=H\bigsqcup gH=H\bigsqcup Hg\quad(g\notin H)$, 故 $gH=Hg$ 对 $g\notin H$ 成立, 从而也对一切 $g\in G$ 成立, H 是正规子群. □

1.4.5 试证直积群 $G\times G'$ 的子集 $G\times 1$ 是一个与 G 同构的正规子群，且 $G\times G'/G\times 1\cong G'$.

证明. 两个同构请读者自证. $\forall g=(g_1,g_2)\in G\times G', g^{-1}(G\times 1)g=\{(g^{-1}hg,g_2^{-1}g_2)\}\quad (h\in G)$
$=\{(h',1)|h'=g^{-1}hg\in G\}$
$=G\times 1.$ □

1.4.6 若 $G/Z(G)$ 是循环群，则 G 为阿贝尔群.

证明. 令 $G/Z(G)=\langle a\rangle Z(G)$，$\forall g_1,g_2\in G$，有 $g_1=a^{n_1}z_1, g_2=a^{n_2}z_2$，其中 $z_1,z_2\in Z(G)$. $g_1g_2g_1^{-1}g_2^{-1}=a^{n_1}z_1a^{n_2}z_2z_1^{-1}a^{-n_1}z_2^{-1}a^{-n_2}$.

由于 $z_1,z_2,z_1^{-1},z_2^{-1}\in Z(G)$ 与 G 中一切元素交换，上式 $=a^{n_1}a^{n_2}a^{-n_1}a^{-n_2}z_1z_1^{-1}z_2z_2^{-1}=1$.

故 $z_1z_2=z_2z_1$. □

1.4.7 设 $G_i\quad (1\leqslant i\leqslant n)$ 为 n 个群. 则 $(1)Z(\prod_{i=1}^n G_i)=\prod_{i=1}^n Z(G_i)$, $(2)\prod_{i=1}^n G_i$ 为阿贝尔群 $\Leftrightarrow\forall i, g_i$ 为阿贝尔群.

证明. 留给读者. □

1.4.8 设 G 为群.

(1) 对于 $x\in G$，证明映射 $\sigma_x: g\mapsto xgx^{-1}$ 是 G 的自同构，σ_x 称为**内自同构**.

证明. 易验证 $\sigma_x^{-1}: g\mapsto x^{-1}gx$ 是 σ_x 的唯一逆映射，故 σ_x 是双射.

$\sigma_x(g_1)\sigma_x(g_2)=xg_1x^{-1}xg_2x^{-1}=xg_1g_2x^{-1}=\sigma_xg_1g_2$，故 σ 是同态，故为自同构. □

(2) 令 $I(G)$ 为所有 $\sigma_x: x\in G$ 构成的集合，试证 $I(G)$ 为 $\mathrm{Aut}(G)$ 的子群，称为**内自同构群**.

证明. 只需证 $I(G)$ 对乘法和逆封闭即可. $\sigma_{x_1}\sigma_{x_2}^{-1}(g)=\sigma_{x_1}(x_2^{-1}gx_2)=x_1x_2^{-1}gx_2x_1^{-1}=\sigma_{x_1x_2^{-1}}(g)$. □

(3) 证明 $I(G)\cong G/Z(G)$.

证明. 构造同态 $\varphi: G\to I(G); x\mapsto\sigma_x$，显然它是满射. 若 $x\in\ker(\varphi)$ 则 $I(x)=\mathrm{id}\Leftrightarrow\forall g, xgx^{-1}=g\Leftrightarrow\forall g, xg=gx\Leftrightarrow x\in Z(G)$，故 $\ker\varphi=Z(G)$，由第一同构定理即得结论. □

1.4.9 线性代数

1.4.10 设 $f: G\to H$ 为同态，$M\leqslant G$. 试证 $f^{-1}(f(M))=KM, K=\ker f$.

证明. 由 $f(K)=1$ 知 $f(KM)=f(M)$. 只需证 $\forall g\notin KM, f(g)\notin f(M)$. 事实上，此时 $\forall m\in M, gm^{-1}\notin K, f(gm^{-1})\neq 1$，由消去律 $f(g)=f(gm^{-1})f(m)\neq f(m)$ 对所有 $m\in M$ 成立. □

1.4.11 设 $M,N\lhd G$.

(1) 若 $M\bigcap N=\{1\}$ 则 $\forall a\in M,b\in N,ab=ba$.

证明. 令 $g=aba^{-1}b^{-1}$，则 $g=(aba^{-1})b^{-1}=b_1b^{-1}\in N$，$g=a(ba^{-1}b^{-1})=aa_1\in M$，故总有 $g=1,ab=ba$. □

(2) 在此基础上，若 $MN=G$ 则 $G\cong M\times N$.

证明. 令 $f:G\to MN;g=ab\mapsto(a,b),\quad(a\in M,b\in N)$，$G=MN$ 导致 G 中任何元素都有像，我们只需证明 f 是良好定义的，即像 (a,b) 唯一.

事实上，$g=a_1b_1=a_2b_2\Rightarrow a_1a_2^{-1}=b_1^{-1}b_2$，左边属于 M，右边属于 N，故两边均等于 1，即 $a_1=a_2,b_1=b_2$，(a,b) 唯一确定.

$g_1g_2=a_1b_1a_2b_2=a_1a_2b_1b_2(\because ab=ba\forall a\in M,b\in N)=(a_1a_2)(b_1b_2)$，故 f 为同态且 $\ker f=1$，故 $G\cong M\times N$. □

1.4.12 设 $N\lhd G$，g 是 G 的任一元素，若 g 的阶和 $|G/N|$ 互素，则 $g\in N$.

证明. g 的阶为 $m,g\in bN$ 则 $(bN)^m=gN^m=1\cdot N^m=N$，故 bN 在 G/N 中的阶 n 整除 m，但 n 整除 $|G/N|$，故 n 是 g 的阶和 $|G/N|$ 的公约数，而两者互素，只能 $n=1,bN=N$，即 $g\in N$. □

1.4.13 证明非阿贝尔群的自同构群不是循环群.

证明. 反证法，若 $\mathrm{Aut}(G)$ 是循环群，则 $I(G)$ 为它的子群，从而也是循环群。由**习题 1.4.8**，$G/Z(G)\cong I(G)$ 也是循环群，由**习题 1.4.6**，G 是阿贝尔群，矛盾. □

1.4.14 线性代数

第二章　群在集合上的作用

2.1 对称群

2.1.1 把置换 $\sigma=(456)(567)(761)$ 写作不相交轮换之积.

解. $(456)(567)(761)=(16)(45)$

2.1.2 直接证明置换 $(123)(45)$ 与 $(241)(35)$ 共轭.

解. $(1243)[(123)(45)](1243)^{-1}=(241)(35)$.

2.1.3 讨论置换 $\begin{pmatrix}1 & 2 & \cdots & n\\ n & n-1 & \cdots & 1\end{pmatrix}$ 的奇偶性.

解. $n=4k,4k+1$ 时为偶置换，$4k+2,4k+3$ 时为奇置换. $(k\in\mathbb{N})$，证明留给读者.

2.1.4 一个置换的阶为它的轮换表示中各个轮换的长度的最小公倍数.

证明. 留给读者. □

2.1.5

(1) 证明 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $n!/\prod_{i=1}^n\lambda_i!i^{\lambda_i}$ 个.

证明. 将 $1,2,...,n$ 排序，共有 $n!$ 中排法. 对每一个排序按照如下形式划分：

前 λ_1 个元素各自成一类，各放入一个 1 轮换中.

其后 $2\lambda_2$ 个元素相邻每 2 个成一类，各放入一个 2 轮换中.

...

最后 $n\lambda_n$ 个元素相邻每 n 个成一类，各放入一个 n 轮换中.

则该置换满足题意所述的型. 但交换各 i 组中 λ_i 个轮换的排列顺序，则置换不变，有 $\lambda_i!$ 种变换方式. 对以上每一种变换方式，交换任一轮换中排序，有以下轮换等价 $(a_1a_2...a_k)=(a_2a_3...a_ka_1)=\cdots=(a_ka_1...a_k-1)$，又有对每一轮换 i 种方式，对所有 λ_i 个 i 轮换有 i^{λ_i} 种方式. 故第 i 组有 $\lambda_i!i^{\lambda_i}$ 中排法对应同一置换，综合各组则每一置换对应 $\prod_{i=1}^n\lambda_i!i^{\lambda_i}$ 种排法. □

(2) 由 (1) 证明

$$\sum_{\substack{\lambda_i\geqslant 0\\ \lambda_1+2\lambda_2+...+n\lambda_n=n}}\frac{1}{\prod_{i=1}^n\lambda_i!i^{\lambda_i}}=1.$$

证明. 两边同乘 $n!$，则右边为 S_n 总元素个数，左边为 S_n 种对每一型的元素个数遍历所有型求和，两边自然相等. □

2.1.6 试确定 S_n $(n\geqslant 2)$ 的全部正规子群.

解. 设 $G\lhd S_n$，G 为 S_n 中一些共轭类之并，G 包含一个 i 轮换则 G 包含所有 i 轮换. 以下讨论 $n\geqslant 3$ 的情况. 当 $n\leqslant 2$ 时易见 $G=S_n$ 或 $G=\{1\}=A_n$.

若 $G \neq \{1\}$ 则 G 中包含 k 轮换其中 $k \geqslant 2$，故包含所有 k 轮换. 若 $k < n$ 我们有

$$(i_1 i_2 \cdots i_{k-1} i_k)(j_1 i_2 \cdots i_{k-1} i_k)^{-1} = (i_1 j_i i_k) \in G,$$

其中 $i_1, i_2, ..., i_k, j_1$ 为 $\{1, 2, ..., n\}$ 中任意不同的 $k+1$ 个元素. 故 G 包含一个 3 轮换. 若 $k = n$ 则 $(1234\cdots n)(2134\cdots n)^{-1} = (1n2) \in G$，$G$ 同样包含一个 3 轮换.

故 G 包含一切 3 轮换. 由**引理 2.21**，3 轮换生成 A_n，故 $A_n \leqslant G$，又 A_n 在 S_n 中指数为 2，只能 $(A : G) = 2, G = S_n$ 或 $(A : G) = 1, G = A_n$.

综上，$\{1\}, A_n, S_n$ 为 S_n 的全部正规子群.

2.1.7 置换 σ 的交错数 $n(\sigma)$ 定义为集合 $\{(i,j) \mid \sigma(i) > \sigma(j)$ 但 $i < j\}$ 的阶.

(1) 试证：$n(\sigma) = \sum_{i=1}^{n} |\{j \mid \sigma(j) > i$ 且 $j < \sigma^{-1}(i)\}|$.

证明. $\sum_{i=1}^{n} |\{j \mid \sigma(j) > i$ 且 $j < \sigma^{-1}(i)\}|$
$= \sum_{p=1}^{n} |\{j \mid \sigma(j) > \sigma(p)$ 且 $j < p\}|$
$= |\{(j,p) \mid \sigma(j) > \sigma(p)$ 且 $j < p\}|$
$= n(\sigma)$. □

(2) 证明 σ 可写作 $n(\sigma)$ 个对换的乘积.

证明. 引理：令 $d(\sigma) = \min\{j - i \mid \sigma(i) > \sigma(j)$ 且 $i < j\}$，若题述集合中的一个 (i,j) 对满足 $j - i = d(\sigma)$ 则不存在题述集合中的 (i_1, j_1) 对使得 $i < i_1 < j$ 或 $i < j_1 < j$.

引理的证明. 若 $i < i_1 < j$，则 ① $\sigma(i) > \sigma(j)$;

② $\sigma(i) < \sigma(i_1)$（否则 (i, i_1) 属于题述集合，与 d 的最小性矛盾）;

③ $\sigma(i_1) < \sigma(j)$（否则 (i_1, j) 属于题述集合，与 d 的最小性矛盾）;

①②③ 推出矛盾，故不存在 $i < i_1 < j$（请读者自行完成 $i < j_1 < j$ 部分） □

故 $\sigma = \sigma_1 \cdot (ij)$，其中 σ_1 为 σ 中 i 和 j 交换，$\sigma(i), \sigma(j)$ 不变而成，σ_1 的题述集合和 σ 的题述集合相比，除了不含 (i,j)，由引理三其余元素均不受影响. 故 $n(\sigma_1) = n(\sigma) - 1$，重复此过程直至 $n(\sigma_{n(\sigma)}) = 0$ 则由题述集合的定义 $\sigma_{n(\sigma)}$ 必为恒等置换，σ 为 $n(\sigma)$ 个对换和恒等置换之积. □

2.1.8

(1) 试证 A_5 中置换的型为 $1^5, 2^2 \cdot 1^1, 3^1 \cdot 1^2, 5^1.1$

证明. A_5 的型为 $1^{\lambda_1} 2^{\lambda_2} 3^{\lambda_3} 4^{\lambda_4} 5^{\lambda_5}$，其中 $\sum_i \lambda_i = 5$，$2 \mid \sum_i (i-1)\lambda_i$，枚举即得结论. □

(2i) 证明 A_5 中型为 $2^2 \cdot 1^1$ 的置换共轭.

证明. 只需证明类中任意两元素共轭即可. 令 $\sigma_1 = (i_1 i_2)(j_1 j_2), \sigma_2 = (i_3 i_4)(j_3 j_4)$，

$$\tau = \begin{pmatrix} i_1 & i_2 & j_1 & j_2 \\ i_3 & i_4 & j_3 & j_4 \end{pmatrix}$$

则 $\tau\sigma_1\tau^{-1}=\sigma_2$，若 τ 为偶置换，则两 σ 共轭，若 τ 为奇置换，则

$$\tau'=\begin{pmatrix} i_1 & i_2 & j_1 & j_2 \\ i_4 & i_3 & j_3 & j_4 \end{pmatrix}$$

$=(i_3i_4)\tau$，为偶置换，$\tau'\sigma_1\tau'^{-1}=\sigma_2$，仍有两 σ 共轭. □

(2ii) 证明 A_5 中型为 $3^1\cdot 1^2$ 的置换也共轭.

证明. 只需证明类中任意两元素共轭即可. 令 $\sigma=(i_1i_2i_3),\sigma'=(i_4i_5i_6)$，则 i_4,i_5,i_6 中必有一个与 i_1,i_2,i_3 中一个相同. 由于轮换的表示中可把任意一个元素放在首位而对其他元素依次进行轮换，不改变该轮换本身，故不妨假设 $i_1=i_4$，令

$$\tau'=\begin{pmatrix} i_1 & i_2 & i_3 & i_5 & i_6 \\ i_1 & i_5 & i_6 & i_2 & i_3 \end{pmatrix}$$

则 $\tau\sigma\tau^{-1}=\sigma^{\times}$，若 τ 为偶置换则 σ 和 σ' 共轭. 若 τ 为奇置换，则

$$\tau'=\begin{pmatrix} i_1 & i_2 & i_3 & i_5 & i_6 \\ i_1 & i_5 & i_6 & i_3 & i_2 \end{pmatrix}$$

等于 $(i_2i_3)\tau$ 为偶置换 τ'，且 $\tau'\sigma\tau'^{-1}=\sigma'$. 仍有两者共轭. □

(3) 试求 A_5 中型为 5^1 的置换的共轭类.

解. 设 $\sigma_1=(i_1i_2i_3i_4i_5),\sigma_2=(j_1j_2j_3j_4j_5),\tau=\begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 \\ k_1 & k_2 & k_3 & k_4 & k_5 \end{pmatrix}$ 则 $\tau\sigma_1\tau^{-1}=\sigma_2\Leftrightarrow k_i=j_{i+p \bmod 5}, p=0,1,2,3,4$ 若所有满足 $\tau\sigma_1\tau^{-1}=\sigma_2$ 的 τ 都是偶置换，则 σ_1 和 σ_2 在 A_5 中共轭. 若有一个满足条件 τ_0 为奇置换，则所有满足条件的 τ 为 $\alpha^p\tau_0$ 形式，其中 $\alpha=(k_1k_2k_3k_4k_5),p=0,1,2,3,4$. 因 α 为偶置换，所以所有的 τ 为奇置换，σ_1 和 σ_2 在 A_5 中不共轭.

故 σ_1,σ_2 共轭 $\Leftrightarrow\begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 \\ j_1 & j_2 & j_3 & j_4 & j_5 \end{pmatrix}\in A_5\Leftrightarrow\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}$ 和 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ j_1 & j_2 & j_3 & j_4 & j_5 \end{pmatrix}$ 奇偶性一致，故有 2 个共轭类，由 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}$ 的奇偶性决定，且两个类各有一半该型中元素.

(4) 由此证明 A_5 为单群.

证明. 由**习题** 2.1.5 计算和 (1)(2)(3) 可知：

A_5 中 1^5 型有 1 个，且是单位元，$2^2\cdot 1^1$ 型有 15 个，$3^1\cdot 1^2$ 型有 20 个（以上均各自为一个共轭类），5^1 型有 24 个，并且有 2 个共轭类，各有 12 个元素. 故 A_5 的正规子群的阶数只可能为

$$1+15i_1+20i_2+12i_3,\quad i_1,i_2=0,1,\ i_3=0,1,2$$

$=1,16,21,36,13,28,33,48,25,40,45,60.$

但其中只有 1 和 60 整除 $|A_5|=60$，故 A_5 仅有平凡正规子群. □

2.1.9 试证：当 $n \geqslant 3$ 时 $Z(S_n) = \{\mathrm{id}\}$.

证明. 由**命题 2.10** 可知 $Z(S_n)$ 为元素的共轭类仅有 1 个元素的元素之并，由**习题 2.1.5** 计算可知当 $n \geqslant 3$ 时这样的类只有 1^n，即 $Z(S_n)$ 只有单位元. □

2.1.10 试证 A_4 没有 6 阶子群.

证明. $|A_4| = 12$，6 阶子群指数为 2，由**习题 1.4.4(2)** 知它一定是正规的.

但 A_4 中（请读者仿照**习题 2.1.8** 证明）共轭类元素个数为 1（单位），4（3 轮换，有 2 个这样的共轭类），3（型为 2^2 的置换）

故 A_4 的正规子群的阶数只可能为 $1, 4, 5, 8, 9, 12$，矛盾. □

2.1.11 试计算：

(1) S_6 中 2 阶元的个数.

解. 2 阶元为 $2^1 \cdot 1^4, 2^2 \cdot 1^2, 2^3$ 型，由**习题 2.1.5**，这三个型各有 $15, 45, 15$ 个元素，共 75 个.

(2) A_8 中阶最大的元素数.

解. 由于 8 轮换为奇置换，故 A_8 中 $7^1 \cdot 1^1$ 型（7 轮换）阶最大，为 7.

由**习题 2.1.5**，该类元素有 $8!/(1!7^1 1!1^1) = 5760$ 个.

2.1.12 计算 S_n 中使任意指标都变动的置换的个数.

解. 由**习题 2.1.5**，结果为

$$\sum_{\substack{\lambda_i \geqslant 0 \\ 2\lambda_2 + \cdots + n\lambda_n = n}} \frac{n!}{\prod_{i=2}^{n} \lambda_i! i^{\lambda_i}}.$$

2.1.13 证明当 $n \geqslant 2$ 时 A_n 是 S_n 唯一指数为 2 的子群.

证明. 由**习题 1.4.4(2)**，指数为 2 的子群一定是正规的. 由**习题 2.1.6**，S_n 的非平凡正规子群只有 A_n. □

2.1.14 当 $n \geqslant 2$ 时，(12) 和 $(123\cdots n)$ 为 S_n 的一组生成元.

证明. 由**命题 2.11(2)**，$(12), (13), \cdots, (1n)$ 生成 S_n.

令 $\sigma = (12), \tau = (123\cdots n)$ $\tau\sigma\tau^{-1} = (23), \tau^2\sigma\tau^{-2} = (34), \cdots$

故 σ 和 τ 生成 $(i\ i+1), i = 1, 2, \cdots, n, (n\ n+1) = (n\ 1)$. 由于 $(1j)(j\ j+1)(1j) = (1\ j+1)$，故 σ 和 τ 生成 $(12), (13), \cdots, (1n)$，从而生成 S_n. □

2.2 群在集合上的作用

2.2.1 设群 G 在集合 Σ 上的作用是传递的. N 是 G 的正规子群. 则 Σ 在 N 作用下的每个轨道有同样多的元素.

证明. 对任意两个不属于同一个 $N-$ 轨道的元素 $x_1, x_2 \in \Sigma$，有 $\exists g \in G, gx_1 = x_2$.

记 $N_x = \{n \in N \mid nx = x\}$. 则 $n \in N_{x_2} \Leftrightarrow nx_2 = x_2 \Leftrightarrow ngx_1 = gx_1 \Leftrightarrow g^{-1}ngx_1 = x_1$. 由于 $N \lhd G$，故 $g^{-1}ng \in N$，故 $g^{-1}ng \in N_{x_1}, N_{x_2} = gN_{x_1}g^{-1}$ 与 N_{x_1} 在 G 中共轭. 故 $|O_{x_1}| = (N : N_{x_1}) = (G : N_{x_1})/(G : N) = (G : N_{x_2})/(G : N) = (N : N_{x_2}) = |O_{x_2}|$. 即任意两个轨道元素个数相同. □

2.2.2 设 X 是 $\mathbb{R}$ 上所有函数的集合. 验证 $a \circ f(x) = f(ax)$ $(a \in \mathbb{R}^\times)$ 给出乘法群 $\mathbb{R}^\times$ 在 X 上的作用，并确定所有稳定子群为 $\mathbb{R}_+^\times$ 的函数 f.

解. 对任意的 $a, b \in \mathbb{R}^\times, x \in \mathbb{R}, f \in X, a \circ f(x) = f(1 \cdot x) = f(x); a \circ (b \circ f)(x) = f(abx) = (ab) \circ f(x)$，故 $a \circ f = f, a \circ (b \circ f) = (ab) \circ f$，故乘法群是 X 上的作用.

若 f 满足稳定子群为 $\mathbb{R}_+^\times$，则 $\forall a > 0$，a 在 f 上作用平凡，且 -1 在 f 上作用不平凡. 得 $f(x) = f(1), \forall x > 0, f(x) = f(-1), \forall x < 0, f(1) \neq f(-1)$.

故 $f : x \mapsto \begin{cases} c_1, & x > 0 \\ c_2, & x = 0 \\ c_3, & x < 0 \end{cases}$, $c_1 \neq c_3$.

2.2.3 集合 $A \subseteq \mathbb{R}^n$ 的对称群是指将 A 映为自身的所有刚体变换得到的群.

(1) 求正方形，除正方形外的长方形，除正方形外的菱形，圆的对称群.

解. 只给出结果，请读者自证.

正方形：D_4.

长方形：$\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} = K_2$，其中 $(1,4), (2,3)$ 各表示一对对角顶点.

菱形：$\{\mathrm{id}, (23), (14), (14)(23)\} = K_2$，其中 $(1,4), (2,3)$ 各表示一对对角顶点.

圆：$\mathrm{O}_2(\mathbb{R})$.

(2) 求正四，六，八，十二，二十面体的对称群各有多少元素？这五个对称群中是否有同构的？

解. 元素个数为（某一顶点可被变换到的不同顶点数）和（该顶点所相邻顶点构成的多边形的对称群元素数）之积.

正四面体：$4 \times (3 \times 2) = 24$.

正立方体：$8 \times (3 \times 2) = 48$.

正八面体：$6 \times (4 \times 2) = 48$.

正十二面体：$20 \times (3 \times 2) = 120$.

正二十面体：$12 \times (5 \times 2) = 120$.

由于以一个正立方体各面的中心为顶点，相邻面的中心连接为棱则得一个唯一的正八面体（反之亦然），故正立方体和正八面体的对称群同构. 同理，正十二面体和正二十面体的对称群同构.

2.2.4 设群 G 作用在集合 Σ 上. 令 t 表示 Σ 在 G 作用下的轨道个数. 对 G 中任意元素 g 令 $f(g)$ 表示 Σ 在 g 作用下的不动点个数. 试证

$$\sum_{g\in G} f(g) = t|G|.$$

证明. $\sum_{g\in G} f(g) = |\{(g,x) \mid gx = x, x \in \Sigma, g \in G\}| = \sum_{x\in\Sigma} |\operatorname{Stab}_G(x)|$. 将 Σ 分为不同的轨道 $\Sigma = \bigsqcup_{x\in I} O_x$，其中 I 为各轨道中各取一元素的集合.

若 $x \in \Sigma, x_1 \in O_x$，则 $\exists a \in G, x_1 = ax$，由**命题 2.32**，$\operatorname{Stab}_G(x_1) = a\operatorname{Stab}_G(x)a^{-1}$ 与 $\operatorname{Stab}_G(x)$ 共轭，

故 $|\operatorname{Stab}_G(x_1)| = |\operatorname{Stab}_G(x_1)|, \sum_{x\in O_x} |\operatorname{Stab}_G(x)| = |O_x||\operatorname{Stab}_G(x)| = |G|$（**推论 2.31(1)**），

$\sum_{x\in\Sigma} |\operatorname{Stab}_G(x)| = \sum_{x\in I}\sum_{x\in O_x} |\operatorname{Stab}_G(x)| = \sum_{x\in I} |G| = |I||G| = t|G|$. □

2.2.5 线性代数

2.2.6 设群 H 作用在群 N 上，且每个元素 $g \in H$ 诱导了 N 上的群同构，即同态 $\varphi(g) : H \to \operatorname{Aut}(N)$，令 $G = N \times H$，定义运算

$$(x_1, y_1)(x_2, y_2) = (x_1 \cdot \varphi(y_1)(x_2), y_1y_2)$$

(1) 证明 G 在此运算下成为群，称为 N 和 H 的**半直积**，记为 $G = N \rtimes H$.

证明. 结合律：$[(x_1, y_1)(x_2, y_2)](x_3, y_3)$

$= (x_1 \cdot \varphi(y_1)(x_2), y_1y_2)(x_3, y_3)$

$= (x_1 \cdot \varphi(y_1)(x_2) \cdot \varphi(y_1y_2)(x_3), y_1y_2y_3)$

$(x_1, y_1)[(x_2, y_2)(x_3, y_3)]$

$= (x_1, y_1)(x_2 \cdot \varphi(y_2)(x_3), y_2y_3)$

$= (x_1 \cdot \varphi(y_1)(x_2 \cdot \varphi(y_2)(x_3)), y_1y_2y_3)$

$= (\because \varphi(y_1)$是同态$)(x_1 \cdot \varphi(y_1)(x_2)\varphi(y_1)(\varphi(y_2)(x_3)), y_1y_2y_3)$

故只需证 $\varphi(y_1y_2)(x_3) = \varphi(y_1)(\varphi(y_2)(x_3))$.

由 φ 是同态，$\varphi(y_1y_2)(x) = (\varphi(y_1) \cdot \varphi(y_2))(x) = \varphi(y_1)(\varphi(y_2)(x))$，故上式成立.

单位元：由于 $\varphi(y_1)$ 是同构，它将 N 中的单位元 1_N 映射到自身，φ 是同态，它将 1_H 映射到 $\operatorname{Aut}(N)$ 的单位元 id_N，故 $(x_1, y_1)(1_N, 1_H) = (x_1 \cdot \varphi(y_1)1_N, y_1) = (x_1 \cdot 1_N, y_1) = (x_1, y_1)$，$(1_N, 1_H)(x_2, y_2) = (1_N \cdot \varphi(1_H)(x_2), y_2) = (1_N \cdot \mathrm{id}_N(x_2), y_2) = (x_2, y_2)$，故 $(1_N, 1_H) = 1_G$ 为 G 中的单位元.

逆元：$(x_1, y_1)(\varphi(y_1)^{-1}x_1^{-1}, y_1^{-1}) = (x_1 \cdot \varphi(y_1)\varphi(y_1)^{-1}(x_1^{-1}), 1_H) = (x_1x_1^{-1}, 1_H) = (1_N, 1_H)$.

注意到 $\varphi(y_1)$ 是同构，它的逆映射 $\varphi(y_1)^{-1}$ 也是同构.

我们有 $(\varphi(y_1)^{-1}x_1^{-1}, y_1^{-1})(x_1, y_1) = (\varphi(y_1)^{-1}(x_1^{-1}) \cdot \varphi(y_1)^{-1}(x_1), 1_H) = (\varphi(y_1)^{-1}(x_1^{-1}x_1), 1_H) = (\varphi(y_1)^{-1}(1_N), 1_H) = (\because \varphi(y_1)^{-1}$是同构$)(1_N, 1_H)$

故 $(\varphi(y_1)^{-1}x_1^{-1}), y_1^{-1})$ 是 (x_1, y_1) 的逆元. □

(2a) 证明 H 同构于 G 的一个子群.

证明. 我们证明 $H \cong G_H = \{(1_N, h) \mid h \in H\}$. 只需证 $\forall h_1, h_2 \in H, (1_N, h_1)(1_N, h_2)^{-1} \in G_H$.

$(1_N, h_1)(1_N, h_2)^{-1} = (1_N, h_1)(\varphi(h_1)^{-1} \cdot 1_N, h_1 h_2^{-1})$

$= (1_N \cdot \varphi(h_1)\varphi(h_1)^{-1}(1_N), h_1 h_2^{-1})$

$= (1_N, h_1 h_2^{-1})$. □

(2b) 证明 N 同构于 G 的一个正规子群.

证明. 我们证明 $N \cong G_N = \{(n, 1_H \mid n \in N)\} \lhd G$.

G_N 是子群: $\forall n_1, n_2 \in N, (h_1, 1_H)(h_2, 1_H)^{-1}$

$= (h_1, 1_H)(\varphi(1_H)^{-1}(h_2^{-1}), 1_H^{-1})$

$= (h_1, 1_H)(\mathrm{id}^{-1}(h_2^{-1}), 1_H)$

$= (h_1 \cdot \varphi(1_H)(h_2^{-1}), 1_H)$

$= (h_1 h_2^{-1}, 1_H)$.

正规性: $(n_1, h_1)(n, 1_H)(n_1, h_1)^{-1}$

$= (n_1, h_1)(n, 1_H)(\varphi(h_1)^{-1}(x_1^{-1}), y_1^{-1})$

$= (n_1, h_1)(n \cdot \varphi(1_H)(\varphi(h_1)^{-1}(x_1^{-1})), y_1^{-1})$

$= (n_1, h_1)(n \cdot \varphi(h_1)^{-1}(x_1^{-1}), y_1^{-1})$

$= (n_1 \cdot \varphi(h_1)(n) \cdot \varphi(h_1)(\varphi(h_1)^{-1}(x_1^{-1})), 1_H)$

$= (n_1 \cdot \varphi(h_1)(n) n_1^{-1}, 1_H) \in G_N$. □

(2c) 由 (2a) 和 (2b) 说明上述定义等价于

$$N \lhd G, H \leqslant G, G = NH, N \bigcap H = \{1\}$$

.

证明. 留给读者. □

(2d) 此时 H 在 N 上的作用为内自同构.

证明. 在 (2b) 的正规性证明中令 $n_1 = 1_N$, 则 $\forall h_1 \in H, \varphi(h_1)(n) = (1_N \cdot \varphi(h_1)(n) 1_N^{-1}, 1_H) = (1_N, h_1)(n, 1_H)(1_N, h_1)^{-1} = h_1 n h_1^{-1}$, 故 $\varphi(h_1)$ 为内自同构. □

(3) 证明 $G/N \cong H$.

证明. 留给读者. □

(4) 证明 $S_n = A_n \rtimes \langle (12) \rangle$, 其中 $n \geqslant 3$.

证明. (2c) 中的条件我们只需证明 $S_n = A_n \bigcap A_n(12)$ 即可, 其余都是显然的.

设 $\sigma \in S_n - A_n$ 为奇置换, 则 $\sigma(12)$ 是偶置换, $\sigma = \sigma(12)(12)$. □

2.2.7 正四面体的 4 个顶点用 4 种颜色染色，求真正不同的染色方案的个数.

解. 题意实际要求的是：设正四面体到自身的变换群 G 作用在所有 4^4 种染色方案的集合 Σ 上，求 Σ 在 G 作用下的轨道个数 t. 由**习题 2.2.4**，这相当于求 $t=(\sum_{g\in G} f(g))/|G|$，其中 $f(g)$ 为在 g 作用下不变的染色方案个数. 题意明确了正四面体到自身的空间旋转变换会导致两个真正相同的染色方案，但并未明确是否允许正四面体的反射变换，我们分两种情况讨论.

(1) 只允许空间旋转，此时 G 为交错群 A_4. 其中有单位元，3 轮换 8 个，还有 2^2 型置换 3 个（这些个数由**习题 2.1.5** 得到，下同）.

对单位元，则 $f(\mathrm{id})=|\Sigma|=4^4=256$.

对 3 轮换，则这 3 个顶点必须同色才能在作用下不变，有 4 种染法，第四个顶点独立地有 4 种染法，$f(g)=4^2=16$.

对 2^2 型置换，有两组顶点，组之间独立染色，有 $f(g)=4^2=16$ 种染法.

故共有 $(256+8\times 16+3\times 16)/12=36$ 种染法.

(2) 允许反射变换，此时 G 为正四面体的对称群 S_4. 其中有 A_4 中的全部元素，加 2 轮换 6 个，4 轮换 6 个.

对 2 轮换，轮换涉及的两个顶点必须染相同色，这两个为一组，另两个各为一组，三组之间独立染色有 $4^3=64$ 种染法，$f(g)=64$.

对 4 轮换，四点必须同色，$f(g)=4^1=4$.

故共有 $(256+8\times 16+3\times 16+6\times 64+6\times 4)/24=35$ 种染法.（两个结果仅差 1 是可以理解的，事实上，S_4 下的轨道中仅有四点各异色的染法在 A_4 下分裂为两个轨道，其余各轨道中各元素均在某个对换（它是奇置换）下不动，因此 A_4 下的该轨道也是 S_4 下的一个轨道）

2.3 群在自身上的作用

2.3.1 确定 $G=\mathrm{GL}_2(\mathbb{F}_5)$ 中 $B=\begin{pmatrix}1&0\\0&2\end{pmatrix}$ 的共轭类的阶.

解. $|G|=(5^2-1)(5^2-5)=480$. 又 $|G|=|\mathrm{Conj}_G(B)||Z(B)|$，我们只要求得 $|Z(B)|$ 即可.

令 $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ 则 $ABA^{-1}=B$

$$\Leftrightarrow \begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}\begin{vmatrix}a&b\\c&d\end{vmatrix}^{-1}=\begin{pmatrix}1&0\\0&2\end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix}ad-2bc&-ab+2ab\\cd-2dc&-bc+2ad\end{pmatrix}=\begin{pmatrix}ad-bc&0\\0&2ad-2bc\end{pmatrix}, ad-bc\neq 0$$

$$\Leftrightarrow ab=0, cd=0, bc=0, ad-bc\neq 0$$

$$\Leftrightarrow a\equiv 1,2,3,4 \mod 5,\ d\equiv 1,2,3,4 \mod 5,\ b\equiv c\equiv 0 \mod 5$$

故满足条件的 A 共有 16 个，$|\mathrm{Conj}_G(B)=|G|/|Z(B)|=480/16=30$.

2.3.2 设 p 是素数，G 是 p 的方幂阶的群，试证 G 子群中非正规子群的个数一定是 p 的倍数.

证明. 考虑任何一个 G 的非正规子群 H，X_H 为所有与 H 共轭的群的集合，则 $X_H>1$，又 $|G|=|N_G(H)|\cdot|X_H|=p^n$，只能 $p\mid|X_H|$，故所有满足条件的 H 按共轭分类，每一类中的群个数都被 p 整除. □

2.3.3 令 G 是单群，如果存在 G 的真子群 H 使得 $(G:H)\leqslant 4$ 则 $|G|\leqslant 3$.

证明. 考虑 G 在 H 的左陪集表示，得群同态

$$\rho_H: G\to S_m,\ m=(G:H),$$

由于 $\ker\rho_H$ 为 G 的正规子群，若 $\ker\rho_H=G$，则 $G=\ker\rho_H=\bigcap_{a\in G}a^{-1}Ha\lhd H$ 与 H 是 G 的真子群矛盾. 故 $\ker\rho_H=\{1\}$，$G\cong G/\ker\rho_H\cong\mathrm{im}\,\rho_H\leqslant S_m$，即 G 为 S_1,S_2,S_3,S_4 其中一个的子群.

易验证 S_1,S_2,S_3 的所有单群子群为 $\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/3\mathbb{Z}$，对于 S_4，它的子群元素个数若 >3 则必须为 $24,12,8,6,4$，我们逐一对这些情况寻找 $|G|$ 的非平凡正规子群，从而否定这些情况.

$|G|=24, G=S_4$，此时 A_4 是它的非平凡正规子群.

$|G|=12$，G 是 S_4 的指数为 2 的子群，必是 S_4 的非平凡正规子群，由**习题 2.1.6**，$G=A_4$，此时 $\{\mathrm{id},(12)(34),(13)(24),(14)(23)\}\cong K_2$ 为 G 的非平凡正规子群.

$|G|=8$，其元素只能是 $1,2,4,8$ 阶，且 8 阶元素 b 可推出 4 阶元素 b^2 存在. 若 G 包含 4 阶元 a，则 $\{1,a,a^2,a^3\}$ 指数为 2，是 G 的非平凡正规子群，若 G 中非单位元全为 2 阶，由**引理 1.66**，G 是阿贝尔群，任何 2 阶元素生成的子群都是非平凡正规子群.

$|G|=6$，其元素只能是 $1,2,3,6$ 阶，且 6 阶元素 b 可推出 3 阶元素 b^2 存在. 若 G 包含 3 阶元 a，则 $\{1,a,a^2\}$ 指数为 2，是 G 的非平凡正规子群，若 G 中非单位元全为 2 阶，同上可得任何 2 阶元素生成的子群都是非平凡正规子群.

$|G|=4$，其元素只能是 $1,2,4$ 阶，且 4 阶元素 b 可推出 2 阶元素 b^2 存在. 故 G 必包含 2 阶元 a，则 $\{1,a\}$ 指数为 2，是 G 的非平凡正规子群. □

2.3.4 设 H 是无限群 G 的有限指数真子群，则 G 一定包含一个有限指数的真正规子群且它 $\leqslant H$.

证明. 我们沿用**习题 2.3.3** 中的 ρ_H，则 $\ker\rho_H \lhd G, G/\ker\rho_H \leqslant S_m, (G:\ker\rho_H) \leqslant m!$ 为有限整数的阶乘，故有限. 又 $\ker\rho_H = \bigcap_{a\in G} a^{-1}Ha \leqslant H, H \neq G$，故 $\ker\rho_H \neq G$，它是 G 的有限指数真正规子群. □

2.3.5 证明 $\mathrm{GL}_n(\mathbb{R})$ 的上三角阵组成的子群 H_1 与下三角阵组成的子群 H_2 共轭.

证明. 取 $C = \begin{pmatrix} \cdots & \cdots & \cdots & 1 \\ \vdots & \vdots & \iddots & \vdots \\ 0 & 1 & \cdots & \cdots \\ 1 & 0 & \cdots & \cdots \end{pmatrix}$ $\forall A \in H_1, B \in H_2, CAC^{-1} \in H_2, CBC^{-1} \in H_1$. □

2.3.6 证明**命题 2.43**.

证明. 因 $|X| = \sum_{x\in I}(G:\mathrm{Stab}_G(x)), \forall x(G:\mathrm{Stab}_G(x))$ 或者被 p 整除或者为 1，且 $p\nmid|X|$，故必存在 x 使得 $(G:\mathrm{Stab}_G(x)) = 1, G = \mathrm{Stab}_G(x)$，即 x 为 G 作用下的不动点. □

2.3.7 证明 $\mathrm{GL}_n(\mathbb{C})$ 不含有限指数的真子群.

证明. 反证法，若它含有有限指数的真子群，由**习题 2.3.4** 它也含有有限指数的真正规子群，故不妨设 $H \lhd G, H \neq G$.

令 $m = (G:H)$，则 G 在 H 的左陪集上的表示 $\rho_H : G \to S_m$，$\ker\rho_H = \bigcap_{a\in G} aHa^{-1} = H$. 故 $G/H \to S_m$ 为单同态，$G/H \leqslant S_m$，它的阶也整除 S_m，故任意元素的 S_m 次方为任意元素的 $|G/H|$ 次方的次方，从而为单位元 H.

任取 $gH \in G/H, (gH)^{|S_m|} = H$，即 $g^{p!} \in H$.

对于任意 $a \in \mathbb{C}$，因为 $\mathbb{C}$ 是代数封闭域，存在 $b \in \mathbb{C}$ 使得 $b^{p!} = a$，从而 $(I - E_{ii} + bE_{ii})^{p!} = I - E_{ii} + aE_{ii}$，当 $a \neq 0$ 时 $b \neq 0$，前者属于 G，故后者属于 H.

而 $(I + a/p! \cdot E_{ij})^{p!} = I + aE_{ij}$ $(i \neq j)$，前者属于 G，故后者属于 H.

故所有的第一类和第三类初等矩阵都属于 H，类似**习题 1.3.24(2)**，可证明 H 的元素生成 G，与 $H \neq G$ 矛盾. □

2.3.8 令 G 是阶数为 $2^n m$ 的群，其中 m 是奇数. 如果 G 含有一个 2^n 阶的元素，则 G 含有一个指数为 2^n 的正规子群.

正规性的证明由文献 [11] 给出.

证明. 仿照**命题 2.38**，我们可以证明当 G 的阶为 $2^k m$ 其中 m 是奇数，并存在一个 2^k 阶元素 σ 时 G 有一个指数为 2 的子群，且 σ^2 在此子群中.

考虑 G 的左乘表示 $\rho : G \hookrightarrow S_{2^k m}$，则 $\ker\rho = 1$，$G \leqslant S_{2^k m}$，令 $H = G\bigcap A_{2^k m}$，则 $G/H \leqslant S/A, (G/H) \leqslant 2$，我们要证明 G 中存在奇置换，则 $(G:H) = 2$.

事实上，取 2^k 阶元素 σ，则 σ 的左乘作用没有不动点且全部由 2^k 轮换组成，故为 m 个 2^k 轮换的乘积，奇偶性为 $m(2^k - 1)$ 为奇置换. σ^2 为偶置换，故在 H 中.

当 $n = 1$ 时，取 $k = 1$ 即得指数为 2 阶数为 m 的子群，它一定是正规的.

假设我们已证 $n=s$ 时 2^sm 阶群 G_s 存在阶数为 2^s 的元素则存在指数为 2^s 阶数为 m 的正规子群 $G_0 \lhd G_s$. 对 $n=s+1$，令 σ 为 2^{s+1} 阶元素，则我们得到阶数为 2^sm，在 G_{s+1} 中指数为 2 的子群 $G_s \lhd G_{s+1}$，并且 σ^2 为其中的 2^s 阶元素，根据归纳假设有 m 阶子群 $G_0 \lhd G_s$. 我们证明 G_0 是 G_s 中唯一的 m 阶子群.

假设 P 是另一个 G_s 中的 m 阶子群. 由于 $G_0 \lhd G_s$, $PG_0 = G_0P$, 由**习题 1.2.16** 知 PG_0 是 G_s 的子群, 由**定理 1.70** 知 $|PG_0| = |P||G_0|/|P \bigcap G_0| = m^2/|P \bigcap G_0|$, 故 $|PG_0|$ 是奇数. 如果 $|P \bigcap G_0| < m$，则 $|PG_0| > m$，但 $|PJ|$ 是 G_s 的因子，$G_s = 2^sm$ 没有大于 m 的奇因数，矛盾，故 $|P \bigcap G_0| = m$，即 $P = G_0$.

考虑 G_{s+1} 中任意元素的共轭作用，则它把正规子群 G_s 映射到 G_s，从而在 G_s 上的限制是内自同构. 而 G_s 中只有一个 m 阶子群 G_0，它被内自同构映射到一个 G_s 中的 m 阶子群即 G_0 本身，故任何 G_{s+1} 中的共轭作用在 G_0 上平凡，$G_0 \lhd G_{s+1}$.

由数学归纳法即得结论. □

2.3.9 将 S_n 视为 $\mathrm{GL}_n(\mathbb{R})$ 的置换矩阵构成的子群，确定 S_n 在 $\mathrm{GL}_n(\mathbb{R})$ 中的正规化子.

解. $A \in N_{\mathrm{GL}_n(\mathbb{R})}(S_n) \Leftrightarrow AS_n = S_nA$. 由线性代数可知 AS_n 和 S_nA 分别为 A 的行任意重新排列和列任意重新排列的结果.

要使 A 满足条件，则 A 的任一行的元素任意重新排列，仍是 A 的一行. 由于 A 仅有 n 行，因此 A 的任一行任意重排至多有 n 种不同结果，即该行由 $n-1$ 个 a 和一个 b 组成（可以 $a=b$）

故令 U 为各元素全为 1 的矩阵，$N_{\mathrm{GL}_n(\mathbb{R})}(S_n) = \{aU + bS \mid S \in S_n, a, b \in \mathbb{R}\}$.

2.3.10 求对称群 S_3 的自同构群 $\mathrm{Aut}(S_3)$.

解. S_3 由 2 阶元生成，这些 2 阶元只有 3 个，且 2 阶元被同构仍映射到 2 阶元，故 $\mathrm{Aut}(S_3) \leqslant S_3$. 又 S_3 的内自同构群为 S_3，故 $\mathrm{Aut}(S_3) \geqslant S_3$，故 $\mathrm{Aut}(S_3) = S_3$.

2.3.11 设 α 是有限群 G 的自同构. 若 α 把每个元素都变到它在 G 种的共轭元素，即对任意 $g \in G$, g 和 $\alpha(g)$ 共轭，则 α 的阶的素因子都是 $|G|$ 的因子.

证明由文献 [20] 给出

证明. 反证法. 若 α 的阶含有素因子 $p \nmid |G|$，则设其阶为 ps，则 α^s 满足条件且阶为 p. 以下我们设 α 的阶为 p.

在 $|G|$ 的某一个共轭类内，α 生成的 p 阶子群作用于其上，它的各轨道的元素个数整除 p，即为 p 或 1，若全部为 p，则该共轭类 $\mathrm{Conj}_G(x)$ 的元素个数有素因子 p，故 $|G| = |\mathrm{Conj}_G(x)||Z_G(x)|$ 有素因子 p，矛盾. 故存在元素个数为 1 的轨道，即该共轭类内有 α 作用下的不动点.

令 $G = \bigsqcup_{i \in I} K_i$ 为共轭类之并，每一个共轭类内取不动点 $k_i \in K_i$，令 $H = \langle k_1, k_2, ..., k_n \rangle$，由 α 的同态性，不动点的积和逆也是不动点，故 H 中所有元素满足 $\alpha(h) = h$. 又 $k_1, k_2, ..., k_n \subseteq H$，故 $G = \bigsqcup_{i \in I} K_i = \bigsqcup_{i \in I} \bigcup_{g \in G} gk_ig^{-1} \subseteq \bigcup_{g \in G} gHg^{-1}$，即 H 的共轭子群覆盖整个 G，但由**习题 2.3.17**，H 不能是 G 的真子群，即 $H = G$，α 在整个 G 上作用平凡，其为恒等映射，阶为 $1 \neq p$，矛盾. □

2.3.12 设 p 是 G 的最小素因子，若 p 阶子群 $A \lhd G$，则 $A \leqslant Z(G)$.

证明. A 是 G 中一些共轭类之并. 以下记 $C_x := \mathrm{Conj}_G(x)$:

$$A = \bigsqcup_{x\in I_A} C_x = (\bigsqcup_{\substack{|C_x|=1\\ C_x\subseteq A}} C_x)\bigsqcup(\bigsqcup_{\substack{|C_x|\neq 1\\ C_x\subseteq A}} C_x) = (Z(G)\bigcap A)\bigsqcup(\bigsqcup_{\substack{|C_x|\neq 1\\ C_x\subseteq A}} C_x)$$

由于 p 是 $|G|$ 的最小素因子，当然也是其最小因子，当 $|C_x| \neq 1$ 时有 $|C_x| \geqslant p$, 又 $|A| = p$ 且 $1_G \in Z(G)\bigcap A \neq \varnothing$, 故 $|A|$ 为不小于 1 的左项 $|Z(G)\bigcap A|$ 和 m 个不小于 p 的项构成的右项 $\bigsqcup_{\substack{|C_x|\neq 1\\ C_x\subseteq A}} C_x$ 之和，即 $m = 0$，$A = Z(G)\bigcap A$. □

2.3.13 试求中心化子:

(1) 群 S_4 中元素 $(12)(34)$.

解. 令 $x = (12)(34)$，则 $yx = xy \Leftrightarrow y(1) = x(y(2)), y(2) = x(y(1)), y(3) = x(y(4)), y(4) = x(y(3))$.

故符合条件的 y 集合为 $\{\mathrm{id}, (12), (34), (12)(34), (13)(24), (14)(32), (1324), (1423)\}$.

(2) 群 S_n 中元素 $(123\cdots n)$.

解. 记 $x = (123\cdots n)$，则 $yx = xy \Leftrightarrow y(a+\overline{1}) = y(a) + \overline{1}$，这里 $1, 2, ..., n$ 视为 $\mathbb{Z}/n\mathbb{Z}$ 中元素 $\overline{1}, \overline{2}, ..., \overline{n-1}, \overline{0}$.

故 $y(b) = y(\overline{1}) + \overline{b-1}$. y 由 $y(1)$ 唯一确定. 此时 $y = x^{y(1)-1}$，$Z(x) = \{x^m \mid m = 0, 1, 2, ..., n-1\}$.

2.3.14 p 是素数，试求非交换 p^3 阶群 G 的共轭类个数以及每个共轭类元素个数.

证明. 以下记 $C_x := \mathrm{Conj}_G(x)$.

(i) $|Z(G)| = p$.

由于 p 是 $|G|$ 的唯一素因子，故也是所有 $|C_x|$ ($C_x \neq \{x\}$) 的素因子. 由**公式 2.19**，$p \mid Z(G)$. 又 G 非交换，故 $|Z(G)| = p$ 或 p^2.

但若 $|Z(G)| = p^2$，令 $x \notin Z(G)$，则 $Z(X) \supsetneqq Z(G)$，得 $p^2 < |Z(x)|, |Z(x)| \mid |G|$，得 $|Z(x)| = p^3, Z(x) = G, x \in Z(G)$，矛盾，故 $|Z(G)| = p$.

(ii) $|C_x| \neq 1 \Rightarrow |C_x| = p$.

$|C_x| \neq 1$ 时，$x \notin Z(G)$，$|Z(x)| > |Z(G)| = p, |Z(x)| < |G| = p^3, |Z(x)| \mid |G|$，只能 $|Z(x)| = p^2$，此时 $|C_x| = |G|/|Z(x)| = p$.

综上 G 中有 $|Z(G)| + (|G| - |Z(G)|)/p = p^2 + p - 1$ 个共轭类，其中 p 个类有 1 个元素，$p^2 - 1$ 个类有 p 个元素. □

2.3.15 线性代数

2.3.16 设 $N \lhd G, M \leqslant G, N \leqslant M$. 则 $N_G(M)/N = N_{\overline{G}}(\overline{M})$，其中 $\overline{G} = G/N, \overline{M} = M/N$.

证明. $N_G(M)/N = \{gN \mid gMg^{-1} = M, g \in G\}$,

$N_{G/N}M/N = \{gN \in G/N \mid (gN)(MN)(gN)^{-1} = MN\}$

$= \{gN | gMg^{-1}N = MN\}$ ($\because N \leqslant M, \therefore NMN = M$)

$= \{gN | gMg^{-1} = M, g \in G\}$ ($\because N \leqslant M, \therefore MN = M$).

两者一致. □

2.3.17

(1) 试证有限群 G 的一个真子群的全部共轭子群不能覆盖整个群 G.

证明. $H \leqslant N_G(H) \Rightarrow (G : N_G(H)) \leqslant (G : H)$. 又 $X_H := \{gHg^{-1} \mid g \in G\}$ 满足 $|G| = |N_G(H)||X_H|$(**公式 2.22**)

故 $|X_H| = (G : N_G(H)) \leqslant (G : H) = |G|/|H|$. 又所有 X_H 中的元素子群至少有 1_G 为公共元素,

$\therefore |\{x \mid x \in gHg^{-1} \in X_H\} \leqslant 1 + |X_H|(|H| - 1)$

$= 1 + |X_H||H| - |X_H| \leqslant 1 + |G| - |G|/|H|$

$< 1 + |G| - 1\ (\because (G : H) > 1) = |G|$.

故全部共轭子群之并的元素数小于 $|G|$ 的阶数. □

(2) 试证无限群 G 的一个有限指数真子群 H 同样满足上述结论.

证明由文献 [23] 给出.

证明. 由**习题 2.3.4**, $\exists N \lhd G$ s.t. $N \leqslant H, (G : N) < \infty$.

令 $\varphi : G \to G/N$, 由第四同构定理 (**定理 1.84**), H 在 G 中的共轭子群为 $\varphi^{-1}(H')$, 其中 H' 为 H/N 在 G/N 中的共轭子群, 而 G/N 有限, H/N 为其真子群, 故由 (1) 的结果即得 $\bigcup H' \subsetneqq G/N$, $\bigcup \varphi^{-1}(H') \subsetneqq G$. □

(3) (1) 中的结论对一般无限群是否成立?

解. 否, 有如下反例.

(i) 固定不全为 0 的实常数 c_1, c_2, c_3, 则 $\{a + b(c_1 i + c_2 j + c_3 k) \mid a, b \in \mathbb{R}\}$ 为四元数乘法群 $\mathbb{H}^\times$ 的子群, 其共轭子群的并为 $\mathbb{H}^\times$.

(ii) $G = \mathrm{GL}_n(F), H = B_n(F)$ 为上三角阵构成的子群, 令 F 为代数封闭域, 则 H 的共轭子群覆盖 G.

2.3.18 设 K 是群 G 的一个 2 阶正规子群, 且设 $\overline{G} = G/K$. 设 $\overline{C}$ 是 $\overline{G}$ 的一个共轭类, 设 S 是 $\overline{C}$ 在 G 中的逆像, 证明下列两种情形之一必成立:

(i)$S = C$ 是单独一个共轭类且 $|C| = 2|\overline{C}|$;

(ii)$S = C_1 \bigcup C_2$ 由两个共轭类组成且 $|C_1| = |C_2| = |\overline{C}|$.

证明. 设 $K = 1_G, x$, 则 K 为子群 $\Rightarrow x^2 = 1$, K 是共轭类之并, 1_G 为单独一个共轭类, 故 x 也是单独一个共轭类, 即它与 G 中所有元素都交换.

设 $\overline{C} = \{\overline{c_1}, \overline{c_2}, ..., \overline{c_n}\}$, 则 $\forall 1 \leqslant i, j \leqslant n\ \exists \overline{g} \in \overline{G}$ s.t. $\overline{c_i} = \overline{g}^{-1}\overline{c_j}\,\overline{g}$.

显然如果 G/K 中的像不共轭, 则逆像也不共轭, 故我们只需讨论 S 中元素共轭关系即可.

在 $\overline{c_1}$ 中任选一个代表元 c_1. 因 $\overline{c_1} = \overline{g}^{-1}\overline{c_2}\,\overline{g}$. 则要么:

(u) $c_1 = g^{-1}c_{2,\mathrm{or}}g$ 或 $c_1 = (gx)^{-1}c_{2,\mathrm{or}}(gx)$, 由 x 的交换性, 两种情况是等价的. 于是 $c_{2,\mathrm{or}}$ 与 c_1 在 G 中共轭, 记 $c_2 = c_{2,\mathrm{or}}$.

(v) $c_1 = g^{-1}c_{2,\mathrm{or}}xg$ 或 $c_1 = (gx)^{-1}c_{2,\mathrm{or}}x(gx)$，由 x 的交换性，两种情况是等价的. 于是 $c_{2,\mathrm{or}}x$ 与 c_1 在 G 中共轭，记 $c_2 = c_{2,\mathrm{or}}x$.

类似我们可以选定 $c_3, c_4, ...c_n$ 使得 c_i 是 $\overline{c_i}$ 的代表元，且 c_i 和 c_{i+1} 在 G 中共轭. 由共轭关系是等价关系，$c_1, c_2, ..., c_n$ 在 G 中共轭.

(i) 若存在 c_i 使得 c_i 与 c_ix 在 G 中共轭，即 $\exists h \in G, c_i = h^{-1}c_ixh$，那么

$\because \exists g_{ij} \in G$ s.t. $c_i = g_{ij}c_jg_{ij}^{-1}$，$\therefore c_ixhg_{ij}x = hc_ig_{ij}x = hg_{ij}c_jx$

$\Leftrightarrow c_ihg_{ij}x^2 = hg_{ij}c_jx$

$\Leftrightarrow c_i(hg_{ij}) = hg_{ij}c_jx$

$\Leftrightarrow c_i = (hg_{ij})(c_jx)(hg_{ij})^{-1}$

故 c_i 与 c_jx 在 G 中共轭. 由 j 的任意性，$c_1, c_2, ..., c_n$ 与 $c_1x, c_2x, ..., c_nx$ 同属一个共轭类，我们有 (i) 的结论.

(ii) 不存在 c_i 使得它与 c_ix 共轭，此时 c_ix 在 $\{c_1, c_2, ..., c_n\}$ 之外的共轭类中.

且 $c_i = g_{ij}c_jg_{ij}^{-1} \Leftrightarrow c_ix = g_{ij}c_jg_{ij}^{-1}x \Leftrightarrow c_ix = g_{ij}(c_jx)g_{ij}^{-1}$，

于是 $\forall i, j, c_ix$ 与 c_jx 共轭，此时 $\{c_1x, c_2x, ..., c_nx\}$ 是一个共轭类，我们有 (ii) 中的结论. □

2.3.19

(1) 若 $G/Z(G)$ 是循环群，证明 G 为阿贝尔群，故非交换有限群 G 的中心 $Z(G)$ 的指数 $\geqslant 4$.

证明. 对 $x \in G$，$\sigma_x : g \mapsto xgx^{-1}$ 为 G 的内自同构，由**习题 1.4.8**，这些自同构构成的群 $I(G) \cong G/Z(G)$，因此题述条件即 $I(G) = \langle y \rangle$.

对 $\forall a, b \in G, \sigma_a : g \mapsto aga^{-1} = \sigma_y^i : g \mapsto y^igy^{-i}, \sigma_b : g \mapsto bgb^{-1} = \sigma_y^j : g \mapsto y^jgy^{-j}$,

于是 $aba^{-1}b^{-1} = (y^iby^{-i})b^{-1} = y^i(by^{-i}b^{-1}) = y^iy^jy^{-i}y^{-j} = 1$，即 $ab = ba$. □

(2) 如果 G 为 n 阶有限群，t 为 G 中共轭类的各述，$c = \frac{t}{n}$，证明 $c = 1$ 或 $c \leqslant \frac{5}{8}$.

证明. 显然 G 是阿贝尔群 $\Leftrightarrow c = 1$.

若 G 是非交换群，由 (1) 的结果 $(G : Z(G)) \geqslant 4 \Rightarrow |Z(G)| \leqslant \frac{n}{4}$.

故 G 中共轭类个数 $t = |Z(G)| + \sum_{|\mathrm{Conj}_G(x)| \neq 1} 1$，但 $|G| - |Z(G)| = \sum_{|\mathrm{Conj}_G(x)| \neq 1} |\mathrm{Conj}_G(x)| \geqslant \sum_{|\mathrm{Conj}_G(x)| \neq 1} 2 = 2\sum_{|\mathrm{Conj}_G(x)| \neq 1} 1$,

故 $t \leqslant Z(G) + \frac{1}{2}(|G| - |Z(G)|) = \frac{n}{2} + \frac{Z(G)}{2} \leqslant \frac{n}{2} + \frac{n}{8} = \frac{5n}{8}$，$c = \frac{t}{n} \leqslant \frac{5}{8}$. □

2.4 西罗定理及其应用

2.4.1 若 p 是 $|G|$ 的素因子，则群 G 必有 p 阶元素.

证明. 设 H 为 G 的西罗 p-子群，则 $\exists h \neq 1_G \in H$，h 的阶整除 p^r 记为 p^i $(i \geqslant 1)$，则 $h^{p^{i-1}}$ 为 p 阶元. □

2.4.2 给出 $G = \mathrm{GL}_n(\mathbb{F}_p)$ 的一个西罗 p-子群，并求出 $\mathrm{GL}_n(\mathbb{F}_p)$ 中西罗 p-子群的个数.

解. $|\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{i=0}^{n-1}(p^n - p^i) = p^{n(n-1)/2}\prod_{i=1}^{n}(p^i-1)$, 由于 $p \nmid p^i - 1$, 故其中 p 部分为 $p^{n(n-1)/2}$. 而对角线元全为 1 的上三角阵集合 $T = T_n(\mathbb{F}_p)$ 有 $p^{n(n-1)/2}$ 个元素且是子群，它是一个满足条件的西罗 p-子群.

由线性代数可知 $N_G(T) = B_n(\mathbb{F}_p)$ 为可逆上三角阵集合，$N(p) = (G : N_G(T)) = |G|/|B| = |G|/p^{n(n-1)/2}(p-1)^n = \prod_{i=1}^{n}\frac{p^i-1}{p-1}$.

2.4.3 证明**定理 2.53**.

(1) 设 $p^k \mid |G|$，p 为素数，则 G 中存在 p^k 阶子群.

证明. 设 $X = \{U \subseteq G \mid |U| = p^k\}$，$|G| = p^r m$ $(p \nmid m)$.

则 $N = |X| = \binom{mp^r}{p^k} = \frac{mp^r(mp^r-1)\cdots(mp^r-p^k+1)}{1\cdot 2\cdots p^k}$.

由于 i 与 $mp^r - i$ $(1 \leqslant i \leqslant p^k - 1)$ 被 p 整除的次数一样, 我们有 $p^{r-k} \mid N$ 且 $p^{r-k+1} \nmid N$. 考虑 G 在 X 上的左乘作用, 由于 $p^{r-k+1} \nmid N$, 故必存在一个轨道 O_U 使得 $p^{r-k+1} \nmid |O_U|$. 而 $U = \bigcup_{x\in U}\mathrm{Stab}_G(U)x$ 是 $\mathrm{Stab}_G(U)$ 的一些陪集的的并，故 $|\mathrm{Stab}_G(U)| = p^s$，$0 \leqslant s \leqslant k$，又 $|\mathrm{Stab}_G(U)||O_U| = |G| = p^r m$，故 $|O_U| = p^{r-k}m, |\mathrm{Stab}_G(U)| = p^k$，$\mathrm{Stab}_G(U)$ 满足条件. □

(2) G 中 p^k 阶子群个数模 p 余 1.

证明由文献 [24] 给出.

证明. 令 $|G| = p^k m$，其中 m 不一定与 p 互素. $X = \{A \subseteq G \mid |A| = p^k\}, |X| = \binom{p^k m}{p^k}$.

由**推论 2.3.1**，$p^k m = |O_A| \cdot |\mathrm{Stab}_G(A)|$, $\forall A \in X$.

事实 1. $1 \in A \Rightarrow \mathrm{Stab}_G(A) \subseteq A$.

理由：$g \in \mathrm{Stab}_G(A) \Rightarrow gA = A \Rightarrow g \cdot 1 \in A$.

事实 2. $|\mathrm{Stab}_G(A)| \mid |A| = p^k$.

理由：$\mathrm{Stab}_G(A)A = A \Rightarrow A = \bigsqcup_{i=1}^{r}\mathrm{Stab}_G(A)x_i$ 是 $\mathrm{Stab}_G(A)$ 的右陪集之并.

将 X 分解为 G 作用下的轨道之并：$X = \bigsqcup_{i=1}^{t} O_{A_i}$，若 $1 \notin A_i$，则取 $x \in A_i$ 有 $x^{-1}A_i$ 满足 $1 \in x^{-1}A_i$ 且 $O_{A_i} = O_{x^{-1}A_i}$. 因此在讨论轨道时不妨假定 $1 \in A_i$, $\forall i$.

事实 3. $|O_{A_i}| = m \Leftrightarrow A_i$ 为 G 的子群.

理由：$1 \in A_i$, (事实 1) $\mathrm{Stab}_G(A_i) \subseteq (A_i)$. $\therefore |O_{A_i}| = m \Leftrightarrow |\mathrm{Stab}_G(A_i)| = p^k = |A_i| \Leftrightarrow \mathrm{Stab}_G(A_i) = A_i \Leftrightarrow A_i \leqslant G$.

事实 4. $|O_{A_i}| = m \Leftrightarrow O_{A_i} = \{gA_i \mid g \in G\}$.

理由：$(\Leftarrow)$ $|O_{A_i}| = (G : A_i) = m$ $(\Rightarrow)$ $|O_{A_i}| = m \Rightarrow A_i \leqslant G$，又 $|A_i| = p^r$，我们有 $O_{A_i} = \{gA_i\}$.

故我们有双射

$$\{\text{元素数为 } m \text{ 的轨道}\} \longleftrightarrow \{\text{阶为 } p^k \text{ 的子群}\}$$

，又 $|O_{A_i}| \neq m \Rightarrow \mathrm{Stab}_G(A_i) \subsetneqq A_i$. 故 $|\mathrm{Stab}_G(A_i)| = p^{k-u}$, $(u \geqslant 1)$，故此时 $|O_{A_i}| = p^{u_i}m, pm \mid |O_{A_i}|$.

因此如有 l 个 p^k 阶子群，则有 l 个元素个数为 m 的轨道，其余轨道有 $p^{u_i}m$ 个元素.

$$\binom{mp^r}{p^k} = |X| = \sum_{i=1}^{l} m + \sum_{j} p^{u_j}m \equiv lm \mod pm.$$

故独立于 G 的结构我们有 $\binom{mp^r}{p^k} \equiv lm \mod pm.$，取 $G_0 = \mathbb{Z}/p^k m\mathbb{Z}$ 得 $l_{G_0} = 1, |X| \equiv m \mod pm$，故 $l \equiv 1 \mod p$. □

2.4.4 设 G 是 n 阶群，p 是 n 的素因子，证明 $x^p = 1$ 在 G 中解的个数是 p 的倍数.

证明. 由**定理 2.5.3**，G 中有 $np+1$ $(n \in \mathbb{N})$ 个 p 阶子群. 若这样的两个子群 P_1, P_2 满足 $P_1 \bigcap P_2 \supsetneqq \{1\}$，则 $1 < |P_1 \bigcap P_2| \mid |P_1| = p$，只能 $|P_1| = |P_2| = |P_1 \bigcap P_2| = p$，即 $P_1 = P_2$，故两个不同的 p 阶子群有且仅有 1 为公共元素.

$\therefore |\{x \mid x^p = 1\}| = (np+1)(p-1) + 1 = np^2 + p - np - 1 + 1 \equiv 0 \mod p.$ □

2.4.5 证明 6 阶非阿贝尔群只有 S_3.

证明. 设这样的群为 G，若 G 中有 6 阶元，则它是循环群，矛盾. 故其中非单位元素阶数为 2 或 3.

G 的西罗 3-子群个数为 $\equiv 1 \mod 3$ 且整除 2，故只能为 1，G 中有且只有 2 个 3 阶元，故其他 3 个元素均为 2 阶.

由**习题 2.3.19**，$G/Z(G)$ 不是循环群，故其阶只能为 6，即 $Z(G) = \{1_G\}$，$G \cong G/Z(G) \cong I(G)$，我们只要求得内自同构群 $I(G)$ 即可.

G 只有 3 个 2 阶子群，同构 α 将这三个子群仍映到三个子群，有 $\varphi : I(G) \to S_3$. 若 $\alpha \in \ker\varphi$，则三个子群 $\{1_G, a_1\}, \{1_G, a_2\}, \{1_G, a_3\}$ 皆在 α 作用下不动，故 $1_G, a_1, a_2, a_3$ 都是 α 的不动点，由同态性，不动点的积和逆也是不动点，故 α 的不动点构成群 $H, |H| \geqslant 4, |H| \mid |G|$，只有 $|H| = |G| = 6$，即 $\ker\varphi = \{\mathrm{id}\}$，$G \cong I(G) \cong I(G)/\ker\varphi \cong \mathrm{im}\,\varphi \leqslant S_3$，但 $|G| = 6$，只有 $G = S_3$. □

2.4.6 证明 $148, 200, 224$ 阶群不是单群.

证明. (i) $148 = 2^2 \cdot 37$，由**命题 2.56(2)** 即得.

(ii)$200 = 2^3 \cdot 5^2$. $N(5) \equiv 1 \mod 5$ 且 $N(5) \mid 8$，得 $N(5) = 1$，西罗 5-子群是正规子群.

(iii)$224 = 2^5 \cdot 7$. $N(2) \equiv 1 \mod 2$ 且 $N(2) \mid 7$. 得 $N(2) = 1$（即得结论）或 7.

若 $N(2) = 7$，则记 X_H 为所有西罗 2-子群的集合.

G 在 X_H 上的共轭作用诱导同态: $\rho : G \to S_7$. 若 $\ker\rho = \{1\}$, 则 $G \leqslant S_7$, 但 $|S_7| = 7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, $|G| = 2^5 \cdot 7$，$|G| \nmid |S_7|$，矛盾. 故 $\ker\rho \neq \{1\} \lhd G$. □

2.4.7 求 S_4 的自同构群 $\mathrm{Aut}(S_4)$.

解. $|S_4| = 24 = 2^3 \cdot 3$，西罗 3-子群个数为 1 或 4.

因 $H_1 = \{\mathrm{id}, (234), (243)\}, H_2 = \{\mathrm{id}, (134), (143)\}, H_3 = \{\mathrm{id}, (124), (142)\}, H_4 = \{\mathrm{id}, (123), (132)\}$ 为西罗 3-子群，因此它们是 S_4 全部的西罗 3-子群.

讨论 S_4 的任何 6 阶子群 M，它的西罗 3-子群 H 指数为 2，一定是正规的，若这 $H = H_1$，则若 M 中存在一个把 $2, 3, 4$ 中一个变为 1 的置换，则与 $H_1 \lhd M$ 矛盾，故 M 是 1 的稳定子群 $M_1 \cong S_3$ 的子群，而 M_1 阶数为 6，所以它就是 M. 同理，所有的 M 为 $M_i = Stab_{S_4} i, i = 1, 2, 3, 4$.

考虑 $\mathrm{Aut}(S_4)$ 在 M_i 上的作用：$\varphi : \mathrm{Aut}(S_4) \to S_4$. 由于 $\varphi(I(S_4)) = S_4$，故 $\mathrm{im}\,\varphi = S_4$，我们来证明 $\ker\varphi = \mathrm{id}_{\mathrm{Aut}}$.

事实上，$\alpha \in \ker\varphi$ 使得所有 H_i 不动，故使得所有 M_i 不动，对任意对换 $(i_1 i_2)$，同时属于 M_{i_3}, M_{i_4} $(i_3, i_4 \neq i_1, i_2)$ 的对换有且仅有它，故 α 保持该对换不动，由于 S_4 由对换生成，保持任意对换不动的 α 为恒等映射.

故 $\mathrm{Aut}(S_4) \cong \mathrm{Aut}(S_4)/\ker\varphi \cong \mathrm{im}\,\varphi = S_4$.

2.4.8 设 N 是有限群 G 的正规子群. 如果 p 和 $|G/N|$ 互素，则 N 包含 G 的所有西罗 p-子群.

证明. $|G| = p^r m, p \nmid m, p \nmid (G : N) \Rightarrow N = p^r m_1, m_1 \mid m$. 故 N 的西罗 p-子群也是 G 的西罗 p-子群. 设 A 为 N 的一个西罗 p-子群，则 G 的所有西罗 p-子群有形式 $\{gAg^{-1} \mid g \in G\}$，而 $A \subseteq N \Rightarrow \forall g, gAg^{-1} \subseteq gNg^{-1} = N$，故得结论. □

2.4.9 设 G 是有限群，N 是 G 的正规子群，P 是 G 的一个西罗 p-子群. 证明：

(1) $N \bigcap P$ 是 N 的西罗 p-子群.

证明. 若 $p \nmid |N|$，N 的西罗 p-子群为平凡群，且 $|P|$ 与 $|N|$ 互素，由**习题 1.3.18**，$N \bigcap P$ 也是平凡群.

若 $p \mid |N|$，由西罗第二定理，存在 g 使得 $P' = gPg^{-1}$ 使得 $P' \bigcap N$ 是 N 的西罗 p-子群，其共轭 $g^{-1}(P' \bigcap N)g = g^{-1}P'g \bigcap g^{-1}Ng = P \bigcap N \subseteq N$ 也是 N 的西罗 p-子群. □

(2) PN/N 是 G/N 的西罗 p-子群.

证明. $|G| = p^r m, |N| = p^k m_1, r \geqslant k, p \nmid m, m_1, m_1 \mid m, |G/N| = p^{r-k}(m/m_1)$，$G/N$ 的西罗 p-子群为 p^{r-k} 阶. 而（第二同构定理）$PN/N \cong P/P \bigcap N$，由 (1) 知 $|P \bigcap N| = p^k$，$|P/P \bigcap N| = p^{r-k}$. □

(3) $N_G(P)N/N \cong N_{G/N}(PN/N)$.

证明. 由第二同构定理，只需证 $N_G(P)/N_G(P) \bigcap N \cong N_G(P/N \bigcap P)N$（右边是因映射 $h \mapsto hN$ 诱导 PN/N 与 $P/N \bigcap P$ 的同构）

令 $\varphi : N_G(P) = \{g \mid g^{-1}Pg = P, g \in G\} \to N_G(P/N \bigcap P)N = \{gN \mid g^{-1}P(N \bigcap P)g = P(N \bigcap P)\} = \{gN \mid g^{-1}Pg = P\}$，易见 φ 是满射，其核 $\ker\varphi = \{n \mid n^{-1}Pn = P, n \in N\} = N_G(P) \bigcap N$，由第一同构定理即得结论. □

2.4.10 令 $P_1, P_2, ..., P_N$ 是有限群 G 的全部西罗 p-子群，若对任意 $i \neq j$ 总有

$$(P_i : P_i \bigcap P_j) \geqslant p^r,$$

则 $N \equiv 1 \mod p^r$.

证明. 由 P_i 是 p-群，$(P_i : P_i \bigcap P_j) = p^{r+s}, s \geqslant 0$.

类似西罗第三定理，令 $|G|=p^u m, p \nmid m$. G 在 $P = \{P_1, P_2, ..., P_N\}$ 上的共轭作用可迁，$N = (G : N_G(P_1))$.

将 P 分解为 P_1 在其上共轭作用的轨道，若 O_{P_i} 仅有一个元素 P_i，则 $P_1 \leqslant N_G(P_i)$，而 $P_i \lhd N_G(P_i)$ 为 $N_G(P_i)$ 的唯一西罗 p-子群，故 $P_i = P_1$，仅有一个元素的轨道仅有 $\{P_1\}$.

对于其他轨道 O_{P_j}，考虑 $N_G(P_j) \bigcap P_1$，它的阶整除 $|P_1|$ 故是 p-群，又是 $N_G(P_j)$ 的子群，从而（**推论 2.51**）是 $N_G(P_j)$ 的一个西罗 p-子群的子群，但 $P_j \lhd N_G(P_j)$ 为 $N_G(P_j)$ 的唯一西罗 p-子群，故 $N_G(P_j) \bigcap P_1 \leqslant P_j$ 是 $P_1 \bigcap P_j$ 的子群，$p^r \mid p^r + s = (P_1 : P_1 \bigcap P_j) \mid (P_1 : N_G(P_j) \bigcap P_1)$，又 $|O_{P_j}| = (P_1 : N_{P_1}(P_j)) = (P_1 : P_1 \bigcap N_G(P_j))$，故 $|O_{P_j}|$ 被 p^r 整除.

综上，$N \equiv |O_{P_1}| + \sum_{j \neq 1, O_{P_j} \text{各异}} |O_{P_j}| \equiv 1 + \sum_{j \neq 1, O_{P_j} \text{各异}} 0 \equiv 1 \mod p^r$. □

2.4.11 试证：若 G 的阶为 $n = p^e a, 1 \leqslant a < p, e \geqslant 1$，则 G 一定有真正规子群.

证明. 当 $a > 1$ 时，仿照**命题 2.56(2)** 的证明即可.

当 $a = 1$ 时，由**命题 2.42**，G 的中心非平凡，若 G 不是阿贝尔群，则 $Z(G)$ 是 G 的真正规子群. 若 G 是阿贝尔群，当 $e > 1$ 时，由**定理 2.53**，对任何 $0 < k < e$，G 的任何 p^k 阶子群存在并是 G 的真正规子群.

当 $a = e = 1$ 时，G 是素数阶循环群，故是单群，结论不成立. □

2.4.12 令 G 是集合 Σ 上的对称群，P 是 G 的西罗 p-子群，如果 p^m 整除 $|Ga|$，则 p^m 整除 $|Pa|$.

证明. $|G| = p^r m_0 = |Ga||\operatorname{Stab}_G(a)|$，$|P| = p^r = |Pa||\operatorname{Stab}_P(a)|$. 而 $\operatorname{Stab}_P(a) \leqslant \operatorname{Stab}_G(a)|$，所以 $|\operatorname{Stab}_P(a)| \mid |\operatorname{Stab}_G(a)|$.

若 $|\operatorname{Stab}_G(a)| = p^{k_1} m_1$，有 $k_1 \leqslant r - m, m_1 \mid m_0$，则 $|\operatorname{Stab}_P(a)| = p^{k_2}, k_2 \leqslant k_1$. $|Pa| = p^r / p^{k_2} = p^{r-k_2}$ 被 p^m 整除. □

2.4.13 令 G 是集合 Σ 上的对称群，对任意 $a \in \Sigma$，设 P 是稳定子群 $\operatorname{Stab}_G(a)$ 的西罗 p-子群，Δ 是轨道 Ga 在 P 作用下的所有不动点集合，证明 $N_G(P)$ 在 G 上的作用是传递的.

证明. 若 $b \in \Delta$，则 $b \in Ga$，$\exists g$ s.t. $b = ga$. 而 $P \in \operatorname{Stab}_G b$，又 $\operatorname{Stab}_G(b)$ 与 $\operatorname{Stab}_G(a)$ 共轭（**命题** 2.32(1)），所以 P 是 $\operatorname{Stab}_G(b)$ 的西罗 p-子群. 对群 gPg^{-1} 来说，$gPg^{-1}b = gPa$，而 $P \subseteq \operatorname{Stab}_G(a)$，故 $Pa = a$，$gPa = ga = b$，故 $gPg^{-1} \in \operatorname{Stab}_G(b)$，它也是 $\operatorname{Stab}_G(b)$ 的西罗 p-子群. 故 $\exists h \in \operatorname{Stab}_G(b)$，使得 $h(gPg^{-1})h^{-1} = P$，故 $hg \in N_G(P)$，且 $hga = hb = b$，即 $N_G(P)$ 在 Δ 上可迁. □

2.4.14 证明对 24 阶群 G，G 的中心平凡则 G 同构于 S_4.

证明.

(1) G 的西罗 3-子群不能只有 1 个.

反证法，若只有一个这样的子群，则它是正规子群，记为 $N_3 \cong \mathbb{Z}/3\mathbb{Z}$. 考虑 G 的一个西罗 2-子群 H_8，我们有 $|H_8| = 8$. 由于 N_3H_8 的阶整除 24 且被 3 和 8 整除，故为 24，即 $N_3H_8 = G$，类似地，3 和 8 互素表明 $N_3 \bigcap H_8 = \{1_G\}$.

因此 N_3, H_8 满足**习题 2.2.6(2)** 中的全部条件，$G \cong N_3 \rtimes H_8$，有 $\varphi : H_8 \to \mathrm{Aut}(N_3), h \mapsto (\sigma_h : a \mapsto h^{-1}ah)$.

若 $h \in Z(H_8)$ 且 $\sigma_h = \mathrm{id}$，则在 G 中 $(1_N, h)(x_2, y_2) = (1_N \cdot \sigma_h(x_2), hy_2) = (x_2 \cdot y_2(1_N), y_2h) = (x_2, y_2)(1, h)$ 对任意 $x_2 \in N_3, y_2 \in H_8$ 成立，即 $(1, h) \in Z(G)$. 故若 $h \neq 1_H \in Z(H_8)$ 则 G 的中心非平凡，矛盾，下证这样的 h 存在.

记 $N_3 = \{1, b, b^2\}$，$\mathrm{Aut}(N_3) \cong \mathbb{Z}/2\mathbb{Z} = \{\mathrm{id}_N, \rho\}, \rho^2 = \mathrm{id}_N$.

(1a) 若 H_8 中存在 4 阶元，记为 a，则 $\{1, a, a^2, a^3\}$ 在 H_8 中指数为 2，为正规子群，并且由 4 阶元的共轭也是 4 阶元，有 $\forall c \in H_8$ 有 $c^{-1}ac = a$ 或 $c^{-1}ac = a^3$，此时 $c^{-1}a^2c = (c^{-1}ac)^2 = a^2$ 或 $a^6 = a^2$，故 $a^2 \in Z(H_8)$ 且由 $\varphi(a) = \mathrm{id}_N$ 或 ρ 得 $\varphi(a^2) = \varphi(a)^2 = \mathrm{id}_N$. a^2 是满足条件的 h.

(1b) H_8 中仅有 $1, 2$ 阶元，由**引理 1.66**，H_8 为阿贝尔群，任何元素都在中心中，且 $|\operatorname{im}\varphi| \leqslant 2$ 导致 $|\ker\varphi| \geqslant 4$，任取 $\ker\varphi$ 中非单位元即为满足条件的 h.

(2) 由 (1) 且 $N(3) \equiv 1 \mod 3, N(3) \mid 8$ 得 $N(3) = 4$. 令 $H = \{H_1, H_2, H_3, H_4\}$ 为 G 中西罗 3-子群的集合. 由 $|G| = |H_i||N_G(H_i)|$ 得 $N_G(H_i) = 6$.

又 H_i 彼此共轭，$\forall u \in N_G(H_i), uH_iu^{-1} = H_i$，则 $\forall j \in \{1, 2, 3, 4\} \exists g \in G$ 使得 $gH_ig^{-1} = H_j$，故 $gug^{-1}H_j(gug^{-1})^{-1} = gug^{-1}H_jgu^{-1}g^{-1} = guH_iu^{-1}g^{-1} = gH_ig^{-1} = H_j$，即 $gug^{-1} \in N_G(H_j)$，故 $N_G(H_i)\ i = 1, 2, 3, 4$ 彼此共轭，又 $|N_G(H_i)| = 6$，我们分情况讨论证明 $\bigcap_{i=1}^4 N_G(H_i) = \{1_G\}$.

(2a) $N_G(H_1)$ 为阿贝尔群，则由西罗定理 $N_G(H_1)$ 中既存在 2 阶元，也存在 3 阶元，由**习题 1.3.25(2)**，$6 \mid d(G)$ 使得 $d(G) = 6$，G 中存在 6 阶元，故为循环群 $\mathbb{Z}/6\mathbb{Z}$，所有的 $N_G(H_i)$ 由共轭性也有此结构.

$H_i = \{1, a_i^2, a_i^4\}$ 是 $N_G(H_i) = \{1, a_i, a_i^2, a_i^3, a_i^4, a_i^5\}$ 的唯一 3 阶子群，由于 $H_i \bigcap H_j \neq H_i$，它的阶数不为 3 且整除 3，只能为 1，故 $H_i\ i = 1, 2, 3, 4$ 中 8 个 3 阶元彼此相异 (*)，而 a_i, a_i^5 的平方各是 a_i^2, a_i^4，故也彼此相异.

若 $\bigcap_{i=1}^4 N_G(H_i)$ 非平凡，只能 $u = a_1^3 = a_2^3 = a_3^3 = a_4^3$. 但这时 u 与 G 内 17 个各异元素交换，$|C_G(u)| \geqslant 17, |C_G(u)| \mid |G| = 24$，只能 $C_G(u) = 24$，即 $u \in Z(G)$，与中心平凡矛盾.

(2b) $N_G(H_1)$ 为非阿贝尔群，由**习题 2.4.5** 知 $N_G(H_i) \cong S_3 = \{1, b, b^2, a, ab = b^2a, ab^2 = ba \mid b^3 = a^2 = 1\}$，$b, b^2 \in H_i$，$N_G(H_i) - H_i$ 中元素都是 2 阶，且两个不同的 2 阶元素之积属于 $H_i - \{1_G\}$.

若 $N_G(H_i) - H_i$ 和 $N_G(H_j) - H_j$ 有 2 个以上相同元素，则它们的积又在 $H_i - \{1_G\}$ 中又在 $H_j - \{1_G\}$ 中，由上述 (*) 得矛盾，故若 $\bigcap_{i=1}^4 N_G(H_i)$ 非平凡，则有且只有一个 u 为 $N_G(H_i)$ 的非平凡公共元素.

对 $\forall g \in G$，g 的共轭作用得 $gN_G(H_i)g^{-1} = N_G(H_{\sigma(i)}), \sigma \in S_4$. 因此 $u \in N_G(H_i), \forall i \Rightarrow gug^{-1} \in N_G(H_{\sigma(i)}), \forall i$，因此 $gug^{-1} \in \bigcap_{i=1}^4 N_G(H_i)$，又 $gug^{-1} \neq 1_G$，得 $gug^{-1} = u, \forall g \in G$，即 $u \in Z(G)$，矛盾.

(2c) 综上,$\bigcap_{i=1}^{4} N_G(H_i) = \{1_G\}$. 考虑 G 的内自同构 $I(G)$ 作用在 H 的置换上,有同态 $\varphi : I(G) \to S_4$, $\sigma \in \ker\varphi \Leftrightarrow \sigma(H_i) = g_\sigma H_i g_\sigma^{-1} = H_i, \forall i \Leftrightarrow g_\sigma \in \bigcap_{i=1}^{4} N_G(H_i) \Leftrightarrow g_\sigma = 1_G \Leftrightarrow \sigma = \mathrm{id}_H$ 故 $\ker\varphi = \mathrm{id}_H$, $G \cong G/Z(G) \cong I(G) \cong I(G)/\ker\varphi \cong \mathrm{im}\,\varphi \leqslant S_4$, 但 $|G| = |S_4|$, 只有 $G = S_4$. □

2.4.15 设 P 是 G 的西罗 p-子群且 $N_G(P)$ 是 G 的正规子群, 证明 P 是 G 的正规子群.

证明. 若 $P' \neq P$ 与 P 共轭, 则 (参照**习题 2.4.14** 的证明 (2) 部分) 有 $N_G(P)$ 与 $N_G(P')$ 共轭, 故 $N_G(P') = N_G(P)$. 于是 $P \lhd N_G(P), P' \lhd N_G(P)$ 是 $N_G(P)$ 的两个西罗 p-子群, 它们彼此共轭, 与它们的正规性矛盾. 故 $P \lhd G$. □

2.5 自由群与群的表现

2.5.1 证明或否定：2 个生成元的自由群同构于两个无限循环群的积.

解. 否，前者是非阿贝尔群，后者是阿贝尔群.

2.5.2 设 F 是 x, y 生成的自由群.

(1) 证明两个元素 $u = x^2$ 和 $v = y^3$ 生成 F 的一个子群，它同构于 u, v 上的自由群.

证明. $\langle x^2, y^3\rangle = \{x^{k_1}y^{l_1}\cdots x^{k_s}y^{l_s}, k_i = 2n_i > 0$或$k_1 = 0, l_i = 3m_i > 0$或$l_s = 0\}$，（注：取 $s = 1, k_1 = l_1 = 0$ 即得单位元），它到 $\langle u, v\rangle$ 有自然的双射 $\langle u, v\rangle = \{u^{n_1}v^{m_1}\cdots u^{n_s}y^{m_s}, n_i > 0$或$n_1 = 0, m_i > 0$或$m_s = 0\}$，故 $\langle u, v\rangle \cong \langle x^2, y^3\rangle$. □

(2) 证明三个元素 $u = x^2, v = y^2, z = xy$ 生成 F 的一个子群，它同构于 u, v, z 上的自由群.

证明. $\langle x^2, y^2, xy\rangle = \{y^{k_0}x^{k_1}y^{k_2}\cdots x^{k_{2n+1}}y^{k_{2n}}, n \geqslant 0, k_0, k_{2n} \geqslant 0, k_i \geqslant 1\,(0 < i < 2n), k_0 \equiv 0 \mod 2, k_{2i-1} \equiv k_{2i} \mod 2\}$，它到 $\langle u, v, z\rangle$ 有自然的双射

$$\langle u, v, z\rangle = v^{\frac{k_0}{2}}u^{\lfloor\frac{k_1}{2}\rfloor}z^{k_1 \bmod 2}v^{\lfloor\frac{k_2}{2}\rfloor}\cdots u^{\lfloor\frac{k_{2n-1}}{2}\rfloor}z^{k_{2n-1} \bmod 2}v^{\lfloor\frac{k_{2n}}{2}\rfloor}$$

（$\lfloor a\rfloor := \max\{b \leqslant a \mid b \in \mathbb{Z}\}$ 是不超过 a 的最大整数）故 $\langle u, v, z\rangle \cong \langle x^2, y^2, xy\rangle$. □

2.5.3 若 n 为正奇数，求证：$D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}$.

证明. $D_n = \langle \sigma, \tau, \beta \mid \sigma^n = \tau^2 = (\sigma\tau)^2 = 1\rangle$，$D_{2n} = \langle \alpha, \tau \mid \alpha^{2n} = \tau^2 = (\alpha\tau)^2 = 1\rangle$.

记 $\alpha' = (\sigma^{(n+1)/2}, \beta)$，其中 $\beta \in \mathbb{Z}/2\mathbb{Z}, \beta^2 = 1$，则 $\alpha'^k = (1, 1) \Leftrightarrow 2 \mid k$ 且 $n \mid (n+1)k/2$，即 $k = 2k_0$ 且 $n \mid (n+1)k_0$ $(k_0 \in \mathbb{Z})$，然而 n 与 $n+1$ 互素，故 $n \mid k_0, 2n \mid k$，即 α' 为 $2n$ 阶元.

记 $\tau' = (\tau, 1)$，则 $\tau'^2 = (1, 1)$，由 $\tau\sigma\tau = \sigma^{-1}$ 可得 $\sigma^l\tau = \tau\sigma^{-l}, \forall l \in \mathbb{Z}$. 于是 $(\alpha'\tau')^2 = (\sigma^{(n+1)/2}\tau\sigma^{(n+1)/2}\tau, \beta^2) = (\tau\sigma^{-(n+1)/2}\sigma^{(n+1)/2}\tau, 1) = (\tau^2, 1) = (1, 1)$.

由于生成关系唯一确定该群，$\varphi : D_n \times \mathbb{Z}/2\mathbb{Z} \to D_{2n}, \alpha' \mapsto \alpha, \tau' \mapsto \tau, (1, \beta) \mapsto \alpha^n$ 是同构. □

2.5.4 若 $n \geqslant 3$，$A_n \times \mathbb{Z}/2\mathbb{Z}$ 与 S_n 是否同构?

解. 否，$\mathbb{Z}/2\mathbb{Z}$ 是 $A_n \times \mathbb{Z}/2\mathbb{Z}$ 的正规子群，若有同构，则它也是 S_n 的正规子群，但由**习题 2.1.6**，这意味着 $\mathbb{Z}/2\mathbb{Z}$ 同构于 $\{1\}, A_n, S_n$ 当中的一个，比较阶可得 $2 = 1$ 或 $n!/2$ 或 $n!$，当 $n \geqslant 3$ 时矛盾.

2.5.5 设 $G = G_1 \times G_2 \times \cdots \times G_n, H \leqslant G$，问 H 是否一定形如 $H = H_1 \times H_2 \times \cdots \times H_n$，其中 $H_i \leqslant G_i, \forall 1 \leqslant i \leqslant n$.

解. 否，令 $G = \mathbb{Z} \times \mathbb{Z}$，$H = \langle(1, 1)\rangle \subsetneqq G$. 对任意 $k \in \mathbb{Z}$ 有 $(k, k) \in H$，若 $H = H_1 \times H_2$，则 $\mathbb{Z} \subseteq H_1, H_2$，得 $H = G$，矛盾，故 H 不满足结论.

2.5.6 设 G_1 和 G_2 是两个非交换单群，证明 $G_1 \times G_2$ 的非平凡正规子群只有 G_1 和 G_2.

证明. 设 $H \lhd (G_1 \times G_2)$，令 $H_1 = \{a \mid (a,b) \in H\}, H_2 = \{b \mid (a,b) \in H\}$，则 H_i 是 G_i 的子群，$H_1 \lhd G_1$，$H_2 \lhd G_2$，这导致 $H_1 = \{1\}$ 或 G_1，$H_2 = \{1\}$ 或 G_2（请读者自证!）

若 H_1 或 H_2 是平凡群，则 H 是平凡群或 $\{1_{G_1}\} \times G_2 \cong G_2$ 或 $G_1 \times \{1_{G_2}\} \cong G_1$. 我们考虑 $H_1 = G_1, H_2 = G_2$ 的情况.

对 $\forall b_0 \in G_2, \exists a_0 \in G_1$ s.t. $(a_0, b_0) \in H$. 由 H 的正规性，$\forall b_1 \in G_2$，$(1_{G_1}, b_1)(a_0, b_0)(1_{G_1}, b_1)^{-1} = (a_0, b_1 b_0 b_1^{-1}) \in H$，故 $(a_0, b_1 b_0 b_1^{-1})(a_0, b_0)^{-1} = (1_{G_1}, b_1 b_0 b_1^{-1} b_0^{-1}) \in H$. 由 b_0, b_1 的任意性，$\{1_{G_1}\} \times [G_2, G_2] = \{1_{G_1}\} \times G_2' \subseteq H$，但 $G_2' \lhd G_2, G_2' \neq \{1_{G_2}\}$($G_2$ 是非交换的)，故 $G_2 \cong \{1_{G_1}\} \times G_2 \subseteq H$，同理 $G_1 \cong G_1 \times \{1_{G_2}\} \subseteq H$.

由于上述两个群生成整个 G，我们有 $H = G$，综合四种状况可得结论. □

2.5.7 证明 $455 = 5 \cdot 7 \cdot 13$ 阶群 G 一定是循环群.

证明. $N(7) \equiv 1 \mod 7, N(7) \mid 65, N(13) \equiv 1 \mod 13, N(13) \mid 35$，得 $N(7) = N(13) = 1$，西罗 7-,13-子群 $H_7 \lhd G, H_{13} \lhd G$. 考虑 $H_7 H_{13}$，由正规性 $H_7 H_{13} = H_{13} H_7$，故 $H_7 H_{13}$ 是 G 的子群，$H_7 \lhd H_7 H_{13}$，由 7 与 13 互素，$H_7 \bigcap H_{13} = \{1_G\}, |H_7 H_{13}| = 91$. 由**习题 2.2.6**，$H_7 H_{13} = H_7 \rtimes H_{13}$.

我们有同态：$\varphi_1 : H_{13} \to \mathrm{Aut}(H_7) \cong \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) = (\mathbb{Z}/7\mathbb{Z})^\times$，后者阶数为 6. 故 $\mathrm{im}\,\varphi_1$ 的阶数整除 6（因它是 $\mathrm{Aut}(H_7)$ 的子群）和 13（因它是 H_{13} 的商群 $H_{13}/\ker\varphi_1$），它只能是平凡群，即 H_{13} 在 H_7 上作用平凡，$H_7 H_{13} = H_7 \rtimes H_{13} = H_7 \times H_{13} = \mathbb{Z}/91\mathbb{Z}$，记为 H_{91}.

$\forall i \in H_7, j \in H_{13}$，由正规性 $\forall g \in G, gig^{-1} = i' \in H_7, gjg^{-1} = j' \in H_{13}$，故 $g(ij)g^{-1} = gig^{-1}gjg^{-1} = i'j' \in H_7 H_{13}$，$H_7 H_{13} = H_{91}$ 是 G 的正规子群. 记 G 的任何一个西罗 5-子群为 H_5，因 5 与 91 互素，$H_5 \bigcap H_{91} = \{1_G\}, |H_5 H_{91}| = 455 = |G|$. 由**习题 2.2.6**，$G = H_{91} H_5 = H_{91} \rtimes H_5$.

我们有同态：$\varphi_2 : H_5 \to \mathrm{Aut}(H_{91}) \cong \mathrm{Aut}(\mathbb{Z}/91\mathbb{Z}) = (\mathbb{Z}/91\mathbb{Z})^\times$，后者阶数为 $(7-1) \times (13-1) = 72$. 故 $\mathrm{im}\,\varphi_2$ 的阶数整除 72（因它是 $\mathrm{Aut}(H_{91})$ 的子群）和 5（因它是 H_5 的商群 $H_5/\ker\varphi_2$），它只能是平凡群，即 H_5 在 H_{91} 上作用平凡，$G = H_{91} H_5 = H_{91} \rtimes H_5 = H_{91} \times H_5 = \mathbb{Z}/455\mathbb{Z}$，它是循环群. □

2.5.8 求 (1) 圆 (2) 球 (3) 圆柱体的对称群.

解. (1)$\mathrm{O}_2(\mathbb{R})$ (2)$\mathrm{O}_3(\mathbb{R})$ (3)$\mathrm{O}_2(\mathbb{R}) \times \mathbb{Z}/2\mathbb{Z}$ ，请读者自行完成证明.

2.5.9 给定两个水平平面，在顶面有三个点，它们在底面有正投影. 把顶面的三个点与底面的正投影分别用三根不相交的绳子连接起来，且每根绳子与两平面之间的每一个水平面恰好相交一次，这样的绳子称为一个 **3-辫子**. 给定两个 3-辫子 a, b，将 b 放在 a 下面连接起来得到一个新的辫子，称为 a 和 b 的乘法. 试证明所有的 3-辫子构成一个群，并确定它的表现.

解. $G = \langle a, b \mid aba = bab \rangle$，理由见文献 [28].

2.5.10 设 G 由 n 个元素生成，而 G 的子群 A 具有有限指数. 求证：A 可由 $2n(G:A)$ 个元素生成.

证明由文献 [15] 给出，该处还有人给出了更严格的上界 $(n-1)(G:A)+1$.

证明. 设 $G = \langle X \rangle$, 记 $Y = X \bigcup X^{-1}$，则 $|Y| \leqslant 2n$，且 $\forall g \in G, g = y_1 y_2 \cdots y_{r(g)}$，其中 $y_i \in Y$，不一定两两不同.

对 A 的所有右陪集 Ax 选定一个代表元，令 $f(x)=\begin{cases}1, & x\in A\\ Ax\text{的代表元}, & x\notin A\end{cases}$ 其中 A 的一个右陪集代表元系 $S=\{1,x_1,...,x_{(G:A)-1}\}$ 为 $f(x)$ 的 $(G:A)$ 个不同值，即 $\forall x_1,x_2\in G, Ax_1=Ax_2\Rightarrow f(x_1)=f(x_2)$. 我们记 $[x]:=f(x)$. 我们有 $\forall x,v\in G, x[x]^{-1}=x(ax)^{-1}\ (a\in A)=a^{-1}\in A, [[x]]=[x], [[x]v]=[xv]$.

$\forall h\in A, h=y_1y_2\cdots y_r$

$$=\underbrace{y_1[y_1]^{-1}}_{z_1}\cdot\underbrace{[y_1]y_2[[y_1]y_2]^{-1}}_{z_2}\cdot\underbrace{[[y_1]y_2]y_3[[[y_1]y_2]y_3]^{-1}}_{z_3}\cdot\cdots\cdot\underbrace{[[\cdots[[y_1]y_2]\cdots]y_{r-1}]y_r[[[\cdots[[y_1]y_2]\cdots]y_{r-1}]y_r]^{-1}}_{z_r}$$
$$\cdot\underbrace{[[[\cdots[[y_1]y_2]\cdots]y_{r-1}]y_r]}_{z_{r+1}}$$

而 $z_{r+1}=[y_1y_2\cdots y_r]=[h]=1\ (\because h\in A)$，$z_1,z_2,...,z_r\in SY[SY]^{-1}=\{sy[sy]^{-1}\mid s\in S,y\in Y\}\subseteq A$. 因此 $SY[SY]^{-1}$ 生成 A，它有至多 $|S||Y|\leqslant(G:A)\cdot 2n$ 个元素，故结论成立. □

2.5.11 令 $G=G_1\times G_2\times\cdots\times G_n$ 且对任意 $i\neq j$，$|G_i|$ 和 $|G_j|$ 互素. 证明 G 的任意子群 H 都是它的子群 $H\bigcap G_i\ (i=1,2,...,n)$ 的直积.

证明. 记 $H_i=\{a_i\mid(a_1,...,a_n)\in H\}$，易见 $H_i\leqslant G_i$. 考虑 $H_{12}=\{(a_1,a_2)\mid(a_1,...,a_n)\in H\}\leqslant G_1\times G_2$，对 H_{12} 中第一项的每一个相异值选定一个元素，得 $H_{12,1}=\{(a_1,f(a_1))\mid(a_1,a_2)\in H_{12}\}$，则 $\varphi:H_{12,1}\to H_1,(a_1,f(a_1))\mapsto a_1$ 为双射.

令 $N_{12,2}=\{(1,a_{2z})\mid(1,a_{2z})\in H_{12}\}$，则对任意 H_{12} 中第一项相同的元素 x,y，有 $x=(a_1,a_{2x}),y=(a_1,a_{2y}),xy^{-1}=(1,a_{2x}a_{2y}^{-1})\in N_{12,2}$，特别地，$(a_1,f(a_1)a_{2y}^{-1})\in N_{12,2}$，且不同的 a_{2y} 得到 $N_{12,2}$ 中不同元素. 反之，对 $N_{12,2}$ 中元素 a_{2z} 有 $(a_1,f(a_1))(1,a_{2z})=(a_1,f(a_1)a_{2z})\in H_{12}$，且不同的 a_{2z} 得到不同的 $f(a_1)a_{2z}$，也就是 H_{12} 中不同的第一项为 a_1 的元素. 故 $H_{12}=\bigsqcup_{a_i\in H_1}\{(a_1,f(a_1)a_{2z})\mid(1,a_{2z})\in N_{12,2}\}=H_{12,1}\times N_{12,2}$，$|H_1|=|H_{12,1}|\mid|H_{12}|$. 同理（构造 $H_{12,2},N_{12,1}$）$|H_2|\mid|H_{12}|$.

但 $|H_1|\mid|G_1|$，$|H_2|\mid|G_2|$，导致 $|H_1|$ 与 $|H_2|$ 互素，即 $|H_1||H_2|\mid|H_{12}|\leqslant|H_1\times H_2|=|H_1||H_2|$，只有 $|H_{12}|=|H_1||H_2|, H_{12}=H_1\times H_2$.

由于 $|G_1\times G_2|=|G_1||G_2|$ 与 $|G_3|$ 互素，同理有 $H_{12}3=\{(a_1,a_2,a_3)\mid(a_1,a_2,...,a_n)\in H\}=H_{12}\times H_3=H_1\times H_2\times H_3$，继续这一过程可得结论. □

2.6 有限生成阿贝尔群的结构

2.6.1

(1) 将 33 阶群分类.

解. $N(11)\equiv 1 \mod 11$ 且 $N(11)\mid 3$ 得 $N(11)=1$, 西罗 11-子群是循环群 $N_{11}=\langle a\mid a^{11}=1\rangle \lhd G$. 设 $H_3=\{1_G,b,b^2\}$ 是 G 的一个西罗 3-子群, 则 3 与 11 互素 $\Rightarrow N_{11}\bigcap H_3=\{1_G\}, |N_{11}H_3|=|N_{11}||H_3|=|G|\Rightarrow N_{11}H_3=G, G=N_{11}\rtimes H_3$.

G 由 $\varphi: H_3\to \mathrm{Aut}(N_{11}): g\mapsto \sigma_g: a\mapsto g^{-1}ag$ 唯一确定. 因 $\mathrm{Aut}(N_{11})=\mathrm{Aut}(\mathbb{Z}/11\mathbb{Z})=(\mathbb{Z}/11\mathbb{Z})^\times$ 有 10 个元素, $\mathrm{im}\,\varphi$ 整除 10 和 3, 故为平凡群, $G=N_{11}\times H_3=\mathbb{Z}/33\mathbb{Z}$ 是同构意义下唯一的 33 阶群.

(2) 将 18 阶群分类.

解.

(2a) 阿贝尔群, 这时初等因子组为 $\{2,9\}$ 或 $\{2,3,3\}$, 得阿贝尔群有两类: $G_1=\mathbb{Z}/18\mathbb{Z}, G_2=\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

(2b) 非阿贝尔群, 这时西罗 3-子群指数为 2, 一定是正规的, 记为 $H_9\lhd G$. 由 9 和 2 互素, 类似 (1) 的推理有 $G=H_9\rtimes\{1_G,c\}$, $c^2=1_G$. 记 $C=\{1_G,c\}$. 由**命题 2.45**, $H_9=\mathbb{Z}/9\mathbb{Z}$ 或 $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$.

(2ba) $H_9=\mathbb{Z}/9\mathbb{Z}=\langle a\mid a^9=1\rangle$. 由 H_9 正规知 $ca=a^rc$, 即 $cac^{-1}=a^r$, 此时 $ca^rc^{-1}=(cac^{-1})^r=a^{r^2}$, 又 $ca^rc^{-1}=c^{-1}a^rc=a$, 得 $a=a^{r^2}$, 即 $r^2\equiv 1 \mod 9$, 得 $r\equiv 1$ 或 8, 若 $r=1$, 则 c 在 H_9 上作用平凡, G 为阿贝尔群, 若 $r=8$, 则 $G_3=\langle a,c\mid a^9=1, cac^{-1}=a^{-1}\rangle\cong D_9$.

(2bb) $H_9=(\mathbb{Z}/3\mathbb{Z})^2=\langle a,b\mid ab=ba, a^3=b^3=1\rangle$

我们有半直积下的作用: $\varphi_1: C\to\mathrm{Aut}(H_9), \sigma_{1_G}=\mathrm{id}_{H_9}, \sigma_c: g\mapsto cgc^{-1}$, 可见内自同构 σ_c 确定 G. $\sigma_c^2=\mathrm{id}_{H_9}$.

对任意 $\alpha\in\mathrm{Aut}(H_9)$, $G\to G: (g,c_0)\mapsto(\alpha(g),c_0)$ $c_0\in C$ 是 G 的自同构, 这时 σ_c 变为 $\sigma_{c,\alpha}:\alpha(g)\mapsto c\alpha(g)c^{-1}, \sigma_{c,\alpha}=\alpha^{-1}\sigma_c\alpha$, 由 α 的任意性, σ_c 在 $\mathrm{Aut}(H_9)$ 中的共轭元在 G 的同构意义下等价, 故我们只需考虑 σ_c 在 $\mathrm{Aut}(H_9)$ 中可取的共轭类个数.

我们来分析 $\mathrm{Aut}(H_9)$ 的结构. $(\mathbb{Z}/3\mathbb{Z})^2$ 的全部 3 阶子群为 $M_1=\{1,a,a^2\}, M_2=\{1,b,b^2\}, M_3=\{1,ab,a^2b^2\}, M_4=\{1,a^2b,ab^2\}$, 记这四个子群的集合为 M. 于是 $\varphi\in\mathrm{Aut}(H_9)$ 诱导 M 上的置换 $m(\varphi)$.

令 $\varphi_{34}(a)=a^2, \varphi_{34}(b)=b$, 则 $m(\varphi_{34})=(34)$.

令 $\varphi_{3412}(a)=b, \varphi_{3412}(b)=ab$, 则 $m(\varphi_{3412})=(34)(12)$.

由**命题 2.11(2)**, (34) 和 (3412) 生成 S_4, 故 m 是满射. 又对 $\mathrm{Aut}(H_9)$, $\varphi(a)$ 有非单位元的 8 中取法, $\varphi(b)$ 有不属于 $\langle\varphi(a)\rangle$ 的 6 种取法, $|\mathrm{Aut}(H_9)|=6\times 8=48$, $|\ker m|=|\mathrm{Aut}(H_9)|/|\mathrm{im}\,m|=2$, 又 $\varphi_{\mathrm{id}}:\varphi(a)=a^2, \varphi(b)=b^2\in\ker m$, 故 $\ker m=\{\mathrm{id}_(H_9), \varphi_{\mathrm{id}}\}=T$ 为 $\mathrm{Aut}(H_9)$ 的正规子群, φ_{id} 与 $\mathrm{Aut}(H_9)$ 中的一切元交换, 记它为 τ.

在**习题 2.3.18** 中取 $K=T, G=\mathrm{Aut}(H_9), \overline{G}=G/T\cong \mathrm{im}\, m=S_4$，我们得到 S_4 中的任一共轭类 $\overline{E}$ 对应: (1) 一个共轭类, 当 $\overline{E}$ 中任一元素 σ_e 的逆像 φ_e 和 $\varphi_e\tau$ 共轭. (2) 两个共轭类, 当对一切 $e\in\overline{E}$, φ_e 和 $\varphi_e\tau$ 不共轭. （我们任意在逆像中选定 φ_e，两个值相差 τ，由于 $hgh^{-1}=g'\Leftrightarrow (h\tau)g(h\tau)^{-1}=g'$，故讨论共轭关系时选择哪个值无关紧要）

(2bba) $\overline{E}=\mathrm{id}_{S_4}$，此时 id_{H_9} 与 τ 当然不共轭.

(2bbb) $\overline{E}$ 是 S_4 中对换，令 $\varphi_{12}: a\mapsto b, b\mapsto a; \varphi_{34}: a\mapsto a^2, b\mapsto b$，则 $m(\varphi_{12})=(12), m(\varphi_{34})=(34), \varphi_{12}^{-1}\varphi_{34}\varphi_{12}(a)=a=\tau(a^2), \varphi_{12}^{-1}\varphi_{34}\varphi_{12}(b)=b^2=\tau(b), \varphi_{12}^{-1}\varphi_{34}\varphi_{12}=\varphi_{34}\tau$，故 φ_{34} 与 $\varphi_{34}\tau$ 共轭，$\overline{E}$ 的逆像 φ_E 对应一个共轭类.

(2bbc) $\overline{E}$ 为 2^2 型置换，令 $\varphi_{12,34}: a\mapsto b^2, b\mapsto a$，则 $m(\varphi_{12,34})=(12)(34), \varphi_{12}^{-1}\varphi_{12,34}\varphi_{12}(a)=b=\tau(b^2), \varphi_{12}^{-1}\varphi_{12,34}\varphi_{12}(b)=a^2=\tau(a), \varphi_{12}^{-1}\varphi_{12,34}\varphi_{12}=\varphi_{12,34}\tau$，故 $\varphi_{12,34}$ 与 $\varphi_{12,34}\tau$ 共轭，$\overline{E}$ 的逆像 φ_E 对应一个共轭类.

(2bbd) $\overline{E}$ 为 3 或 4 轮换，共轭类讨论省略，理由见下.

要使 $\sigma_c=\varphi$，必有 $\varphi^2=\sigma^2=\mathrm{id}_{H_9}$，当 $\overline{E}$ 为阶不为 $1,2$ 的置换时，$(\varphi T)^2\neq T, \varphi^2\neq \mathrm{id}_{H_9}$. 对 2^2 型置换对应的共轭类，有 $\varphi_{12,34}^2=\tau\neq \mathrm{id}_{H_9}$ 为非 2 阶元，故其余所有的 φ_E 也是非二阶元，以上均可排除，只有以下三种情况:

$\sigma_c=\mathrm{id}_{H_9}$，此时 G 为阿贝尔群.

$\sigma_c=\tau$，此时 $G_4=\langle a,b,c\mid a^3=b^3=c^2=1, ab=ba, cac=a^{-1}, cbc=b^{-1}\rangle$.

$\sigma_c=\varphi_E$ 其中 $\overline{E}$ 为对换，此时（在同构意义下不妨取 $\sigma_c=\varphi_{34}$）b 与 c 交换，$G_5=\langle a,b,c\mid a^3=b^3=c^2=1, ab=ba, cac=a^{-1}, bc=cb\rangle=\langle a,c\mid a^3=c^2=1, cac=a^{-1}\rangle\times\langle b\mid b^3=1\rangle=S_3\times\mathbb{Z}/3\mathbb{Z}$.

综上，18 阶群在同构意义下有 5 类:

$G_1=\mathbb{Z}/18\mathbb{Z}$;

$G_2=\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$;

$G_3=D_9$;

$G_4=\langle a,b,c\mid a^3=b^3=c^2=1, ab=ba, cac=a^{-1}, cbc=b^{-1}\rangle$;

$G_5=S_3\times\mathbb{Z}/3\mathbb{Z}$.

2.6.2 有限生成阿贝尔群 G 是自由阿贝尔群 $\Leftrightarrow$ G 的所有非零元都是无限阶.

证明. 由**定义 2.78**，应证即扭子群 $G_t=\{0\}\Leftrightarrow G=\mathbb{Z}(S)$，即 $m_1=\cdots=m_s=1\Leftrightarrow G=\mathbb{Z}^r$，而这是显然的. □

2.6.3

(1) 正有理数乘法群 $\mathbb{Q}_+^\times$ 是自由阿贝尔群，全部素数是它的一组基.

证明. 对任意该群中元素 a，有 $a=\frac{m}{n}$，其中 $\gcd(m,n)=1$. 由算术基本定理，$m=\prod_{i=1}^{r}p_i^{\alpha_i}$，$n=\prod_{j=1}^{s}q_j^{\beta_j}$，其中 p_i 为各异素数，q_j 也为各异素数，$\alpha_i,\beta_j\in\mathbb{Z}_+$（若 m 或 $n=1$，则 r 或 $s=0$）. 由 m,n 互素知 p_i 和 q_j 也彼此相异.

故有唯一的表示形式 $a=\prod_{k=1}^{\infty}r_k^{\theta_k}$，其中 $\theta_k=\begin{cases}0, & r_k\notin\{p_i\}\bigsqcup\{q_j\}\\ \alpha_i, & r_k=p_i\\ -\beta_i, & r_k=q_j\end{cases}$，$\{r_k\}$ 为全部素数，$\theta_i\in\mathbb{Z}$.

反之，任一表示形式 $\prod_{k=1}^{\infty}r_k^{\theta_k}$，$\theta_k\in\mathbb{Z}$ 确定一个有理数 a.

故 $\mathbb{Q}_+^{\times}$ 与 $\mathbb{Z}(S)$ 之间有自然的双射（请读者验证它是同态!），其中 $S=\{r_k\}$ 为全体素数. □

(2) 该群不是有限生成的.

证明. 对任意有限集 S_1，若 $\mathbb{Q}_+^{\times}=\mathbb{Z}(S_1)\subseteq\mathbb{Z}(S_2)$，其中 S_2 为 S_1 中元素分子或分母的素因子（故也是有限集合），在数论中熟知素数有无限多个（请读者自证!），故存在 $p\notin S_2, p\in\mathbb{Z}(S_2), p=\frac{m}{n}, m,n\in\mathbb{N}(S_2)$，$m,n$ 为 S_2 中元素的正整数幂次之积. 因而 $p\mid m=\prod_{i\in S_2}i^{\theta_i}$，$\theta_i\in\mathbb{N}$. 由 p 是素数知存在 $i\in S_2$ 使得 $p\mid i^{\theta_i}$，得 $p\mid i$，然而 p 和 i 是不同的素数，矛盾. 故 $\mathbb{Q}_+^{\times}$ 不是有限生成的. □

2.6.4 加法群 $\mathbb{Q}^+$ 不是自由阿贝尔群.

证明. 生成元集合中可删去单位元 0 而群不变，以下设生成元不为 0.

若 $\mathbb{Q}^+$ 由至少 2 个生成元生成，设 $x=\frac{m_1}{n_1}, y=\frac{m_2}{n_2}, m_1,m_2,n_1,n_2\in\mathbb{Z}-\{0\}$ 是两个生成元，则 $n_1m_2, n_2m_1\neq 0$. 因此在自由阿贝尔群中，$n_1m_2x+n_2m_1(-y)\neq 0$，与在 $\mathbb{Q}$ 中 $n_1m_2x-n_2m_1y=0$ 矛盾.

若 $\mathbb{Q}^+$ 由 1 个生成元 x 生成，则 $\frac{x}{2}\notin\langle x\rangle$，矛盾. □

2.6.5 设有限阿贝尔群

$$A\cong\bigoplus_{i=1}^{s}\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, p_i\text{为素数}, \alpha_i\in\mathbb{Z}^+$$

证明 A 的任何子群都同构于 $\bigoplus_{i=1}^{s}\mathbb{Z}/p_i^{\beta_i}\mathbb{Z}, 0\leqslant\beta_i\leqslant\alpha_i$.

证明. 留给读者. □

2.6.6 设 G 是有限生成的自由阿贝尔群，$\operatorname{rank}(G)=r$，若 $g_1,g_2,...,g_n$ 是 G 的一组生成元，则 $n\geqslant r$.

证明. 在**定义 2.75** 的注记中取 $n=r, m=n, y_i=g_i$，则 $AB=I_r$（因为 g_i 不是基，$BA=I_n$ 不一定成立），$A\in M_{r\times n}(\mathbb{Z}), B\in M_{n\times r}(\mathbb{Z})$，由线性代数知 $r=\operatorname{rank}(AB)\leqslant\min(\operatorname{rank}(A),\operatorname{rank}(B))\leqslant\min(n,r)$，故 $n\geqslant r$. □

2.6.7 设 A 为有限阿贝尔群，对于 $|A|$ 的每个正因子 d，$|A|$ 均有 d 阶子群和 d 阶商群.

证明. 设 $|A|=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$，$p_1,...,p_r$ 为各异素数，因 $|A|$ 有限，$A_t=A$. 由有限生成阿贝尔群的结构定理，

$$A\cong\bigoplus_{i=1}^{r}(\bigoplus_{j=1}^{f(i)}\mathbb{Z}/p_i^{\beta_{ij}}\mathbb{Z}), \sum_{j=1}^{f(i)}\beta_{ij}=\alpha_i \qquad (*)$$

即 A 是 r 个阶为 $p_i^{\alpha_i}$ 的有限阿贝尔群 A_i 的直积. 令 $d=\prod_{i=1}^r p_i^{\gamma_i}$，则 $d\mid |A| \Leftrightarrow 0\leqslant \gamma_i\leqslant \alpha_i$. 我们只需证：每个阶为 $p_i^{\alpha_i}$ 的有限阿贝尔群 A_i 都有 $p_i^{\gamma_i}$ 阶子群和商群.

令 $A_i=\bigoplus_{j=1}^k \mathbb{Z}/p_i^{a_k}\mathbb{Z}, \sum_{j=1}^k a_j=\alpha_i$. 由于 $0\leqslant\gamma_i\leqslant\alpha_i$，我们可对所有的 i 取 $0\leqslant b_i\leqslant a_i$ 使得 $\sum_{j=1}^k b_j=\gamma_i$，$B_i=\bigoplus_{j=1}^k \mathbb{Z}/p_i^{b_k}\mathbb{Z}$ 是 A_i 的 $p_i^{\gamma_i}$ 阶子群，$C_i=\bigoplus_{j=1}^k \mathbb{Z}/p_i^{a_k-b_k}\mathbb{Z}$ 是 A_i 的 $p_i^{\alpha_i-\gamma_i}$ 阶子群，A_i/C_i 是 A_i 的 $p_i^{\gamma_i}$ 阶商群，□

2.6.8 设 H 是有限阿贝尔群 A 的子群，则存在 A 的子群同构于 A/H.

证明. 与**习题 2.6.7** 同样，A 是素数幂次阿贝尔群的直积，由**习题 2.5.11**，我们只需证明 $|A|$ 为素数幂次的情形.

设 A 为 p^α 阶阿贝尔群，它的子群 H 一定是 p^β 阶阿贝尔群，$0\leqslant\beta\leqslant\alpha$. 由有限生成阿贝尔群的结构定理，

$$A\cong\bigoplus_{i=1}^n \mathbb{Z}/p^{a_i}\mathbb{Z}, \text{其中}\sum_{i=1}^n a_i=\alpha.$$

其中阶数小于等于 p^j 的元素个数为 $\prod_{p^{a_i}\geqslant p^j} p^j=p^{\sum_{a_i\geqslant j} j}=p^{|\{i|a_i\geqslant j\}|}$.

而由有限生成阿贝尔群的结构定理，$H\cong\bigoplus_{i=1}^m \mathbb{Z}/p^{b_i}\mathbb{Z}, \text{其中}\sum_{i=1}^m b_i=\beta$. H 是 A 的子群 $\Rightarrow \forall j\in\mathbb{Z}, H$ 中阶数小于等于 p^j 的元素个数 $p^{|\{i|b_i\geqslant j\}|}$ 小于 A 中阶数小于等与 p^j 的元素个数，即 $0\leqslant |\{i\mid b_i\geqslant j\}|\leqslant |\{i\mid a_i\geqslant j\}|$ 对一切 j 成立，故 $m\leqslant n$，我们不妨按降序重新排列 a_i, b_i（若 $m<n$，我们令 $b_r=0, m<r\leqslant n$，在同构意义下不改变 H）则 A, H 在同构意义下不变，这时 $a_k=u\Rightarrow |\{i\mid a_i\geqslant u+1\}|<k\Rightarrow |\{i\mid b_i\geqslant u+1\}|<k\Rightarrow b_k<u+1, b_k<u=a_k$ 对一切 $1\leqslant k\leqslant n$ 成立.

故 $A/H\cong\bigoplus_{i=1}^n \mathbb{Z}/p^{a_i-b_i}\mathbb{Z}$，（由上述推理恒有 $a_i-b_i\geqslant 0$）它显然是 A 的子群. □

2.6.9 如果有限阿贝尔群 A 不是循环群，则存在素数 p 使得 A 有子群同构于 $(\mathbb{Z}/p\mathbb{Z})^2$.

证明. 在**习题 2.6.7** 证明的 $(*)$ 式中：

若 $\forall i$ 有 $f(i)=i$，则 $A\cong\bigoplus_{i=1}^r \mathbb{Z}/p_i^{\beta_{i1}}\mathbb{Z}$，$p_i$ 为各异素数，由中国剩余定理（**例 3.57**，或参考《代数学 I：代数学基础》）知 $A\cong\mathbb{Z}/\prod_{i=1}^r p_i^{\beta_{i1}}\mathbb{Z}$，它是循环群.

故 $\exists i$ 使得 $f(i)\geqslant 2$，$\beta_{i1}, \beta_{i2}\geqslant 1$.

因此 $(\mathbb{Z}/p_i^1\mathbb{Z})\oplus(\mathbb{Z}/p_i^1\mathbb{Z})\leqslant(\mathbb{Z}/p_i^{\beta_{i1}}\mathbb{Z})\oplus(\mathbb{Z}/p_i^{\beta_{i2}}\mathbb{Z})\leqslant\bigoplus_{j=1}^{f(i)}\mathbb{Z}/p_i^{\beta_{ij}}\mathbb{Z}\leqslant A$. □

2.6.10 求出 $\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$ 的不变因子和初等因子.

解. 留给读者.

2.6.11 求出 $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/9\mathbb{Z}\oplus\mathbb{Z}/35\mathbb{Z}$ 的不变因子和初等因子.

解. 留给读者.

2.6.12 设 n 为正整数，问有多少个 n 阶阿贝尔群：

解. $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ 为 n 的素因子分解. 请读者自证满足条件的群个数为 $p(\alpha_1)p(\alpha_2)\cdots p_n(\alpha_n)$，其中 $p(x):=\{(a_1,a_2,...,a_n)\mid a_i\in\mathbb{Z}_+, 1\leqslant n\leqslant x, \sum_{i=1}^n a_i=x\}$ 为 x 的分拆函数.

2.6.13 令 p 为素数，$\mathbb{Z}/p^2\mathbb{Z}\oplus\mathbb{Z}/p^3\mathbb{Z}$ 共有多少个 p^2 阶子群?

解. 设群为 G，子群为 H，在**习题 2.5.11** 中令 $G_1=\mathbb{Z}/p^2\mathbb{Z}, G_2=\mathbb{Z}/p^3\mathbb{Z}$，则 $H=H_{12,1}\oplus N_{12,2}$ 仍成立（p^2,p^3 不互素，我们未必有 $|H|=|H_1||H_2|$），分情况讨论：

(1)$|N_{12,2}|=p^2, |H_{12,1}|=1$，此时 $H=\langle(0,p)\rangle$.

(2)$|N_{12,2}|=p, |H_{12,1}|=p$，此时 $N_{12,2}=\langle(0,p^2)\rangle, H_{12,1}=\langle(p,m)\rangle, 0\leqslant m<p^3$，又 $p(p,m)=(0,pm)\in N_{12,2}$，故 $p\mid m$. （这里我们选择 $f(a_i)$ 使得 $H_{12,1}$ 是 G 的子群，由于 H 是子群，因此这种选择是可以做到的）

但对 m 的两个不同值 m_1,m_2，当且仅当 $m_1-m_2\mid p^2$ 时所得的 H 一致（因 $\langle(0,p^2)\rangle=N_{12,2}$），故 $H=\langle\{(0,p^2),(p,m)\mid m=0,p,...,p^2-p\}\rangle$，这样的 H 有 p 个.

(3)$|N_{12,2}=1$，$|H_{12,1}|=p^2, N_{12,1}=\{(0,0)\}$，此时 $H=\langle(1,m)\langle$，其中 $p^2m\equiv 0 \mod p^3$，即 $p\mid m$，$m=0,p,...,p^3-p$ 共有 p^2 种取法，这样的 H 有 p^2 种取法.

综上，G 有 p^2+p+1 个 p^2 阶子群.

2.6.14 $\mathbb{C}^\times$ 的每个有限子群都是循环群. 由此求出 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}^\times$ 的所有群同态.

证明. 若该有限子群包含模不为 1 的元素 $a=re^{i\theta}$，则 $\forall i,j\in\mathbb{N}$，a^i 和 a^j 具有不同的模 r^i,r^j，得 a 生成一个无限群，矛盾. 故该有限子群是 S^1 的子群.

由**习题 1.3.7(1)**，该子群总是循环群 $\langle e^{2\pi i/m}\rangle\cong\mathbb{Z}/m\mathbb{Z}, m\in\mathbb{Z}_+$.

若 $\mathbb{Z}/n\mathbb{Z}$ 到 $\mathbb{C}^\times$ 有同态 φ，则 $\operatorname{im}\varphi$ 是这样一个有限子群，必为 $\mathbb{Z}/m\mathbb{Z}$，并且它是 $\mathbb{Z}/n\mathbb{Z}$ 的商群，即 $m\mid n$. 故 φ 由 $a=\varphi(1)$ 唯一确定，且 a 是 n 次单位根.

故一切的群同态为 $\{\varphi_s:k\mapsto(e^{2\pi is/n})^k\mid s=0,1,...,n-1\}$，其像同构于 $\mathbb{Z}/(n/\gcd(n,s))\mathbb{Z}$. □

2.6.15 设 G,A,B 为有限阿贝尔群，若 $G\oplus A\cong G\oplus B$，则 $A\cong B$.

证明. 留给读者. □

2.6.16 设有限生成阿贝尔群的秩为 1，$f:G\to\mathbb{Z}$ 为满同态，则 $G=\mathbb{Z}\oplus\ker f$，即 $\ker f$ 为 G 的扭子群.

证明. $\forall a\in G_t$，a 的阶有限，记为 m，若 $f(a)\neq 0$，则 $mf(a)\neq 0$ 与 $f(ma)=f(0)=0$ 矛盾，故 $\ker f\geqslant G_t$. 令 $f':G/G_t\to\mathbb{Z}$，则 f 是良好定义的，且 $\operatorname{im}f'=\operatorname{im}f/\{0\}=\mathbb{Z}$，又 $G/G_t\cong\mathbb{Z}$，故 $\ker f'=\{0\}$，$\ker f=G_t\ker f'=G_t$. □

2.6.17 有限生成自由阿贝尔群有什么样的泛性质?

解. 秩为 n 的有限生成自有阿贝尔群可看作 n 维向量空间的子集，全部生成元为向量空间的一组基.

2.6.18 将 $\mathbb{F}_p$ 上的 n 维向量空间 $\mathbb{F}_p^n$ 作为加法群.

(1) 试求 $\mathbb{F}_p^n$ 中 p^{n-1} 阶子群的个数.

解. 由本题 (2)，只需求 p 阶子群个数即可，$\mathbb{F}_p^n$ 中每个非单位元（这样的元素有 p^n-1 个）生成一个 p 阶子群，同时一个 p 阶子群可由 $p-1$ 个非单位元素中任意一个生成，故所求个数为 $\frac{p^n-1}{p-1}$.

(2) 证明 $\mathbb{F}_p^n$ 中 p^k 阶子群的个数等于 p^{n-k} 阶子群的个数.

证明. 由于 $\mathbb{F}_p$ 中元素都是整数，向量空间 $\mathbb{F}_p^n$ 的数乘某元素可以通过该元素重复加自身得到，故每一个子群都是子空间，反之亦然.

我们有一一对应

p^k 阶子群 $\leftrightarrow k$ 维子空间 $A\leftrightarrow$ 与 A 正交的唯一 $n-k$ 维子空间 $B\leftrightarrow p^{n-k}$ 阶子群. □

第三章　环和域

3.1 环和域的定义

3.1.1 设 $n \geqslant 2$ 是正整数，

(1) 环 $\mathbb{Z}/n\mathbb{Z}$ 中元素 a 可逆的充要条件是 $\gcd(a,n)=1$.

(2) 若 p 为素数，则 $\mathbb{Z}/p\mathbb{Z}$ 为域，若 $n \geqslant 2$ 不为素数，则 $\mathbb{Z}/n\mathbb{Z}$ 不是整环.

证明. 留给读者. □

3.1.2 证明 $\mathbb{H}$ 中任何非零元素均乘法可逆.

证明. 令 $p = t + xi + yj + zk \neq 0 \in \mathbb{H}$，我们有 $t^2 + x^2 + y^2 + z^2 \neq 0$.

定义 p 的共轭 $p^* = t - xi - yj - zk$，则 $pp^* = p^*p = (t^2+x^2+y^2+z^2) + (tx - tx - yz - (-yz))i + (ty - ty - zx - (-zx))j + (tz - tz - xy - (-xy))k = t^2 + x^2 + y^2 + z^2 \in \mathbb{R} - \{0\}$

故 $p^{-1} = p^*/(t^2+x^2+y^2+z^2)$ 满足 $pp^{-1} = p^{-1}p = 1$. □

3.1.3 设 $d \geqslant 1$ 为正整数，利用 $R = \mathbb{Z}[\sqrt{-d}] \subseteq \mathbb{C}$ 说明 R 是整环，并确定 R 的单位群.

解. R 的零因子也是 $\mathbb{C}$ 的零因子，然而后者没有零因子，故 R 是整环.

对 R 中任意元素 $y = a + b\sqrt{-d} \neq 0$, y 在 R 中可逆 $\Leftrightarrow y_{\mathbb{C}}^{-1} = \frac{a-b\sqrt{-d}}{a^2+b^2d} \in R$, 即 $a^2+b^2d \mid a, a^2+b^2d \mid -b$.

若 $|a| > 1$，则 $a^2 > |a|, a^2 + b^2d \geqslant a^2 > |a|$，与整除矛盾.

若 $|a| = 1$，则 $1 + b^2d \mid \pm 1$，又 $d \geqslant 1$，只能 $b^2 = 0$，即 $y = \pm 1$.

若 $|a| = 0$，则 $b^2d \mid -b$，得 $bd = \pm 1$ 或 0，又 $d \neq 0, a^2 + b^2d \neq 0$，只能 $b = \pm 1$ 且 $d = 1$.

因此 $U(R) = \begin{cases} \{\pm 1\}, & \text{当} d > 1 \\ \{\pm 1, \pm\sqrt{-1}\}, & \text{当} d = 1 \end{cases}$.

3.1.4 设 A 是阿贝尔群（其上的运算称为加法），$\mathrm{End}(A)$ 是群 A 的全部自同态构成的集合，对于 $f, g \in \mathrm{End}(A)$，定义

$$(f+g)(a) = f(a) + g(a), (f \cdot g)(a) = f(g(a)), \forall a \in A$$

证明 $\mathrm{End}(A)$ 对上述运算是含幺环，并求出单位群.

证明. 定义 $(-g)(a) = -g(a), \forall a \in A$，则对任意 $f, g \in \mathrm{End}(A)$，$-g$ 也是 A 到自身的同态，$(f + (-g))(a) = f(a) - g(a) = -g(a) + f(a) = (-g + f)(a)$，故 $\mathrm{End}(A)$ 对加法是阿贝尔群（结合律请自证），并有加法单位元：$f_0(a) : a \mapsto 0_A$.

又 $((fg) \cdot h)(a) = f(g(h(a))) = (f \cdot (gh))(a)$，且 $f_1(a) : a \mapsto a$ 满足 $f_1 \cdot g = g \cdot f_1 = g$，故 $\mathrm{End}(A)$ 对乘法为含幺半群.

又 $((f+g) \cdot h)(a) = (f+g)(h(a)) = f(h(a)) + g(h(a)) = (f \cdot h + g \cdot h)(a)$（同理可证左分配律），故 $\mathrm{End}(A)$ 和上述运算是含幺环. □

解. $\exists f^{-1}$ s.t. $f(f^{-1}(a)) = f^{-1}(f(a)) = a = f_1(a), \forall a \in A \Leftrightarrow f$ 是同构，故 $U(\mathrm{End}(A)) = \mathrm{Aut}(A)$.

3.1.5 设 G 是乘法群，R 为含幺环，定义集合 $R[G]=\{\sum_{g\in G}r_g g \mid r_g\in R$且只有有限多个$r_g\neq 0_R\}$，在集合 $R[G]$ 上定义

$$\sum_{g\in G}r_g g+\sum_{g\in G}t_g g=\sum_{g\in G}(r_g+t_g)g;\ \left(\sum_{g\in G}r_g g\right)\left(\sum_{g\in G}t_g g\right)=\sum_{g\in G}\left(\sum_{g'g''=g}r_{g'}t_{g''}\right)g$$

(1) 求证：上面定义的加法和乘法是集合 $R[G]$ 中的二元运算（警告：这不是显然的!），并且 $R[G]$ 由此形成环，称为群 G 在环 R 上的**群环**.

证明. 令 $T_1=\{g\mid r_g\neq 0\}$，$T_2=\{g\mid t_g\neq 0\}$，由定义他们都是有限集.

对 $r+t$ 的指标集 r_g+t_g，$\{g\mid r_g+t_g\neq 0\}\subseteq T_1\bigcup T_2$，故它是有限集，故加法为 $R[G]$ 上的二元运算.

对 rt 的指标集，$g\neq T_1T_2\Rightarrow\sum_{g'g''=g}r_{g'}t_{g''}=\sum_{g'g''=g}0\cdot 0=0$，故 $\{g\mid\sum_{g'g''=g}r_{g'}t_{g''}\neq 0\}\subseteq T_1\cdot_G T_2$，它也是有限集，故乘法为 $R[G]$ 上的二元运算.

$R[G]$ 的加法为阿贝尔群：留给读者.

$R[G]$ 的乘法为含幺半群：

结合律：

$$\begin{aligned}
&\left(\left(\sum_{g\in G}r_g g\right)\left(\sum_{g\in G}t_g g\right)\right)\left(\sum_{g\in G}s_g g\right)\\
=&\left(\sum_{g\in G}\left(\sum_{g'g''=g}r_{g'}t_{g''}\right)g\right)\left(\sum_{g\in G}s_g g\right)\\
=&\sum_{g\in G}\left(\sum_{g_{12}g'''=g}\left(\sum_{g'g''=g_{12}}r_{g'}t_{g''}\right)s_{g'''}\right)g\\
=&\sum_{g\in G}\left(\sum_{g'g''g'''=g}r_{g'}t_{g''}s_{g'''}\right)g \qquad (*)
\end{aligned}$$

同理可证 $\left(\sum_{g\in G}r_g g\right)\left(\left(\sum_{g\in G}t_g g\right)\left(\sum_{g\in G}s_g g\right)\right)=(*)$.

乘法单位元：

$$
\begin{aligned}
&\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} 1_g g\right) && (g=1_G \Rightarrow 1_g=1_R, g\neq 1_G \Rightarrow 1_g=0_R)\\
=&\sum_{g\in G}\left(\sum_{g'g''=g} r_{g'}1_{g''}\right) g\\
=&\sum_{g\in G}\left(\sum_{g'1_G=g} r_{g'}1_R\right) g+\left(\sum_{\substack{g'g''=g\\ g''\neq 1_G}} r_{g'}0_R\right) g\\
=&\sum_{g\in G}\left(\sum_{g'1_G=g} r_{g'}1_R\right) g\\
=&\sum_{g\in G} r_g g && (**)
\end{aligned}
$$

同理可证 $\left(\sum_{g\in G} 1_g g\right)\left(\sum_{g\in G} r_g g\right)=(**)$.

分配律：只证右分配律，请读者完成左分配律.

$$
\begin{aligned}
&\left(\left(\sum_{g\in G} r_g g\right)+\left(\sum_{g\in G} t_g g\right)\right)\left(\sum_{g\in G} s_g g\right)\\
=&\left(\sum_{g\in G}(r_g+t_g)g\right)\left(\sum_{g\in G} s_g g\right)\\
=&\sum_{g\in G}\left(\sum_{g'g''=g}(r_{g'}+t_{g'})s_{g''}\right) g\\
=&\sum_{g\in G}\left(\sum_{g'g''=g}(r_{g'}s_{g''}+t_{g'}s_{g''})\right) g\\
=&\sum_{g\in G}\left(\sum_{g'g''=g} r_{g'}s_{g''}\right) g+\sum_{g\in G}\left(\sum_{g'g''=g} t_{g'}s_{g''}\right) g\\
=&\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} s_g g\right)+\left(\sum_{g\in G} t_g g\right)\left(\sum_{g\in G} s_g g\right)
\end{aligned}
$$

故 $R[G]$ 有环结构. □

(2) $R[G]$ 是交换环 $\Leftrightarrow$ R 是交换环且 G 是阿贝尔群.

($\Leftarrow$) 请读者自证.

($\Rightarrow$) 反证法，当 R 不是交换环时，$\exists r_1t_1 \neq t_1r_1, r_1, t_1 \in R$，令 $r_g = r_1, t_g = t_1$ 当 $g = 1_G$，$r_g = t_g = 0_R$ 当 $g \neq 1_G$，则 $\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} t_g g\right) = r_1t_11_G$，$\left(\sum_{g\in G} t_g g\right)\left(\sum_{g\in G} r_g g\right) = t_1r_11_G$，两者不等，故 $R[G]$ 不是交换环.

当 G 不是阿贝尔群时，$\exists ab \neq ba, a, b \in G$，令 $r_g = 1_R$ 当 $g = a$，$r_g = 0_R$ 当 $g \neq a$，$t_g = 1_R$ 当

$g=b$，$t_g=0_R$ 当 $g\neq b$，则 $\left(\sum_{g\in G}r_gg\right)\left(\sum_{g\in G}t_gg\right)=1_Rab$，$\left(\sum_{g\in G}t_gg\right)\left(\sum_{g\in G}r_gg\right)=1_Rba$，两者不等，故 $R[G]$ 不是交换环.

由反证法即得结论.

(3) 如果环 R 的单位元为 1_R，群 G 的单位元为 e，则 1_Re 是群环 $R[G]$ 的单位元.

证明. 留给读者. □

(4) 可以将 R 自然看作 $R[G]$ 的子环:

解. R 到 $R[G]$ 有单同态 $f:r\mapsto r1_G$，证明留给读者.

(5) 试确定

(5a) $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ 的单位群.

解. $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ 的元素有 $a\cdot 1+b\cdot x$ 的形式，其中 $x^2=1$，$1\cdot x=x\cdot 1=x$，故 $a\cdot 1+b\cdot x$ 可记为 $a+bx$ $(a,b\in\mathbb{Z})$.

由于 $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ 的单位元为 $1+0x$，则

$$
\begin{aligned}
&(a+bx)(c+dx)=1+0x && (a,b,c,d\in\mathbb{Z})\\
\Leftrightarrow&ac+bd=1,ad-bc=1 && (a,b,c,d\in\mathbb{Z})\\
\Rightarrow&a^2+b^2=1,c^2+d^2=1,ad-bc=0 && (a,b,c,d\in\mathbb{Z})\\
\Rightarrow&a+bx=\pm1,\pm x,c+dx=\mp1,\mp x
\end{aligned}
$$

易验证上述四个元素的确是 $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ 的单位，即 $U(\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}])=\{\pm1,\pm x\}$.

(5b) $R[\mathbb{Z}]$ 的单位群，其中 R 为整环.

解. 将 $\mathbb{Z}$ 看作秩为 1 的自由阿贝尔群，其生成元记为 x，则 $R[\mathbb{Z}]$ 中的非零元有形式 $r=x^u(a_0+a_1x+\cdots+a_mx^m)=x^uf(x),0\leqslant m<\infty,u\in\mathbb{Z},a_i\in R$，$s=x^v(b_0+b_1x+\cdots+b_nx^n=x^vg(x),0\leqslant n<\infty,v\in\mathbb{Z},b_j\in R$. 此时 f,g 为多项式环 $R[x]$ 中的元素且常数项不为 0_R，由 R 是整环，$f(x)g(x)$ 的常数项也不为 0_R，且 $rs=x^{u+v}f(x)g(x)$，要使 $rs=1_{R[\mathbb{Z}]}$，只能 $u+v=0$，$f(x)g(x)=1_R$，我们有 $\deg fg=0$，由**命题 4.21**（读者也可自证）$\deg f+\deg g=0$，即 f,g 为常数多项式，$fg=1$ 得到 $f=a_0\in U(R),g=b_0\in U(R)$.

故 $U(R[\mathbb{Z}])$ 为 $\{x^ua_0\mid a_0\in U(R),u\in\mathbb{Z}\}$.

3.1.6 令 $R=\{a=(a_1,a_2,...)\mid a_n\in\mathbb{Z},0\leqslant a_n\leqslant p^n-1,a_n\equiv a_{n+1}\mod p^n\}$，设 $a,b\in R$，定义

$$a+b=c,0\leqslant c_n\leqslant p^n-1,c_n\equiv a_n+b_n\mod p^n,$$

$$ab=d,0\leqslant d_n\leqslant p^n-1,d_n\equiv a_nb_n\mod p^n.$$

(1) R 成为一个含幺交换环，称为 p 进整数环，记为 $\mathbb{Z}_p$.

证明. 我们只证两个元素的和、积满足仍满足 $f_n \equiv f_{n+1} \mod p^n$，其余请读者自己完成. 由于 p^n 整除 p^{n+1}，我们有 $a+b=c \Rightarrow c_{n+1} \equiv a_{n+1}+b_{n+1} \mod p^{n+1} \equiv a_{n+1}+b_{n+1} \mod p^n \equiv a_n+b_n \mod p^n \equiv c_n \mod p^n$. $ab=d \Rightarrow d_{n+1} \equiv a_{n+1}b_{n+1} \mod p^{n+1} \equiv a_{n+1}b_{n+1} \mod p^n \equiv a_nb_n \mod p^n \equiv c_n \mod p^n$.

请读者自己证明 $(1,1,1,...)$ 是 R 中的单位元. □

(2) $\mathbb{Z}$ 可自然看成是 $\mathbb{Z}_p$ 的子环.

证明. 请读者自己证明 $\mathbb{Z} \to \mathbb{Z}_p, a_0 \mapsto (a_0 \mod p, a_0 \mod p^2, ...)$ 为单射且保持环 $\mathbb{Z}$ 的加法与乘法. □

(3) 试确定 $\mathbb{Z}_p$ 的单位群.

解. 对任意环 R 中元素 $a=(a_1,a_2,...)$，若 $a_1=0$，则对环 R 中任意元素 b，$ab=(0b_1,a_2b_2,...)=(0,a_2b_2,...) \neq (1,1,...)=1_R$，故 a 不是单位. 若 $a_1 \neq 0$，则 $\gcd(a_1,p)=1$，并且我们有 $a_i=m_ip+a_1, m_i \in \mathbb{N}, \gcd(a_i,p^i)=1$. 由贝祖定理，存在 b_i 使得 $a_ib_i+p^ik=\gcd(a_i,p^i)=1$，即 $a_ib_i \equiv 1 \mod p^i$，且 $a_nb_{n+1} \equiv a_{n+1}b_{n+1} \mod p^n \equiv (1 \mod p^{n+1}) \mod p^n \equiv 1 \mod p^n$，故 $a_n(b_{n+1}-b_n) \equiv 0 \mod p^n$，由 $p \nmid a_n$ 知 $b_{n+1}-b_n \equiv 0 \mod p^n$，即 $b_{n+1} \equiv b_n \mod p^n$ 对一切 $n \geqslant 1$ 成立. 故 $b=(b_1,b_2,...) \in R$ 满足 $ab=(1,1,...)$ 是 a 在 R 中的逆元，$U(R)=\{(a_1,a_2,...) \mid a_n \in \mathbb{Z}, a_1 \neq 0, 0 \leqslant a_n \leqslant p^n-1, a_n \equiv a_{n+1} \mod p^n\} = \mathbb{Z}_p - p\mathbb{Z}_p$.

3.1.7 设 $d \in \mathbb{Q}^\times - (\mathbb{Q}^\times)^2$. 证明 $\mathbb{Q}[\sqrt{d}]=\{a+b\sqrt{d} \mid a,b \in \mathbb{Q}\}$ 是 $\mathbb{C}$ 的子域，并确定 $\mathbb{Q}[\sqrt{d}]$ 的全部子域.

证明. 请读者自证 $\mathbb{Q}[\sqrt{d}] \subseteq \mathbb{C}$，我们只需证 $\mathbb{Q}[\sqrt{d}]$ 对加减乘除封闭. 加减法请读者自证. 对任意该集合中元素 $a+b\sqrt{d}, c+e\sqrt{d}$，$(a,b,c,d \in \mathbb{Q})$，我们有 $(a+b\sqrt{d})(c+e\sqrt{d})=(ac+bed)+(ae+bc)\sqrt{(d)} \in \mathbb{Q}[\sqrt{d}]$，当 $a+b\sqrt{d} \neq 0$ 时 a,b 不同时为 0，又 $d \notin (\mathbb{Q}^\times)^2$，有 $d \neq (\frac{a}{b})^2$，即 $a^2-b^2d \neq 0$，我们有 $(a+b\sqrt{d})(\frac{a-b\sqrt{d}}{a^2-b^2d})=1$ 其中 $(\frac{a-b\sqrt{d}}{a^2-b^2d})=a/(a^2-b^2d)-b/(a^2-b^2d)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$，故每个非零元均有逆元. □

解. 对任何 $\mathbb{Q}[\sqrt{d}]$ 的子域 F，由于 $1 \in F$，得到 $\mathbb{Q} \subseteq F$，并且 $\mathbb{Q}$ 满足条件. 若存在 $e \neq 0$ 使得 $c+e\sqrt{d} \in F$，则 $\sqrt{d}=\frac{1}{e} \cdot (c+e\sqrt{d}-c) \in F$，得 $\forall a,b \in \mathbb{Q}, a+b\sqrt{d} \in F$，即 $F=\mathbb{Q}[\sqrt{d}]$，故子域只有两个，$\mathbb{Q}$ 和 $\mathbb{Q}[\sqrt{d}]$ 本身.

3.1.8 设 R 为环，$a \in R$，求证 $S=\{r \in R \mid ar=ra\}$ 为 R 的子环.

证明. 易见 $0_R \in S, 1_R \in R \Rightarrow 1_R \in S$，我们只要证明 $\forall r,s \in S, r-s \in S, rs \in S$.

$(r-s)a=ra-sa=ar-as=a(r-s), (rs)a=r(sa)=ras=ars=a(rs)$. □

3.1.9 设 U 是一个集合，$S=\{X \mid X \subseteq U\}$，对 $A,B \in S$，定义

$$A-B=\{c \in U \mid c \in A, c \notin B\},$$

$$A+B=(A-B) \cup (B-A), A \cdot B = A \cap B.$$

求证 $(S,+,\cdot)$ 是含幺交换环.

证明. 加法和乘法的二元运算性、交换性留给读者自证.

加法结合律:

$$
\begin{aligned}
&(A+B)+C\\
=&((A-B)\cup(B-A))+C\\
=&(((A-B)\cup(B-A))-C)\cup(C-((A-B)\cup(B-A)))\\
=&((A-(B\cup C))\cup(B-(A\cup C)))\cup((C-(A\cup B))\cup(C\cap A\cap B))\\
=&(A-(B\cup C))\cup(B-(A\cup C))\cup(C-(A\cup B))\cup(A\cap B\cap C) \qquad (*)
\end{aligned}
$$

注意 $(*)$ 式关于 A,B,C 对称，故 $(*)=(A+B)+C=(B+C)+A=A+(B+C)$.

加法单位元: $0_S=\varnothing$ 满足 $A+\varnothing=\varnothing+A=(A-\varnothing)\cup(\varnothing-A)=A$.

加法逆元: $\forall A\in S, A+A=(A-A)\cup(A-A)=\varnothing=0_S$，故任何元素的逆元是它自身. （警告: 这里 $A+(-B)=A+B\neq A-B$，故上文定义的 $A-B$ 不是 S 的减法）

乘法结合律: $(A\cdot B)\cdot C=A\cap B\cap C=A\cdot(B\cdot C)$.

乘法单位元: $1_S=U$ 满足 $A\cdot 1_S=1_S\cdot A=A\cap U=A$.

分配律:

$$
\begin{aligned}
&(A+B)\cdot C\\
=&((A-B)\cup(B-A))\cap C\\
=&((A\cap C)-(B\cap C))\cup((B\cap C)-(A\cap C))\\
=&(A\cap C)+(B\cap C)\\
=&A\cdot C+B\cdot C
\end{aligned}
$$

同理可证左分配律.

综上，$(S,+,\cdot)$ 是含幺交换环. □

3.1.10 设 R 为环，如果每个元素 $a\in R$ 均满足 $a^2=a$，称 R 为**布尔环 (Boolean ring)**，求证:

(1) 布尔环必交换，且对任意 $a\in R, a+a=0_R$.

证明. $a+a=(a+a)^2=a^2+a^2+a^2+a^2=(a+a)+(a+a)$，故 $0_R=a+a$.

对任意元素 a,b，$a+b=(a+b)^2=a^2+b^2+ab+ba=a+b+ab+ba$，故 $ab+ba=0_R$，但 $ab+ab=0_R$，有 $ab-ba=0_R$ 恒成立，R 是交换环. □

(2) **习题 3.1.9** 中的环 S 是布尔环.

证明. 留给读者. □

3.1.11 非零有限整环 R 必为域.

证明. 因 $1_R \in R$，若 R 无 $0_R, 1_R$ 以外元素，则 $R \cong \mathbb{F}_2$ 为域，否则对任意 $x \neq 0_R, 1_R$，令 $\varphi : \mathbb{N} \to \{x^i \mid i \in \mathbb{N}\}, i \mapsto x^i$，由于 $\{x^i \mid i \in \mathbb{N}\} \subseteq R$ 是有限集，$\mathbb{N}$ 是无限集，故 φ 不是单射，$\exists i \neq j$ 使得 $x^i = x^j$，不妨设 $j > i$，即 $j \geqslant i+1$，则 $(x^{j-i} - 1_R)x^i = x^j - x^i = 0_R$，由 R 是整环，x 不是零因子，导致 $x^i \neq 0_R$，并且它也不是零因子，只能 $(x^{j-i} - 1_R) = 0$，即 $x^{j-i} = 1_R, x^{j-i-1}x = 1_R$，$x^{j-i-1}$ 为 x 的逆元. □

3.1.12 环 R 中元素 a 叫做幂零的，是指存在正整数 m 使得 $a^m = 0$.

(1) 证明：若 R 是交换环，a, b 为幂零元素，则 $a+b$ 也是幂零元素.

证明. 若 $a^n = 0, b^m = 0$，则

$$
\begin{aligned}
(a+b)^{n+m} &= \sum_{0 \leqslant i \leqslant m+n} \binom{m+n}{i} a^i b^{m+n-i} \\
&= \sum_{n \leqslant i \leqslant m+n} \binom{m+n}{i} a^n a^{i-n} b^{m+n-i} + \sum_{0 \leqslant i < n} \binom{m+n}{i} a^i b^m b^{n-i} \\
&= \sum_{n \leqslant i \leqslant m+n} \binom{m+n}{i} 0 \cdot a^{i-n} b^{m+n-i} + \sum_{0 \leqslant i < n} \binom{m+n}{i} a^i \cdot 0 \cdot b^{n-i} \\
&= 0
\end{aligned}
$$

故 $a+b$ 为幂零元. □

(2) 如果 R 不为交换环，则 (1) 中结论是否仍旧成立?

解. 未必成立，令 $R = M_2\mathbb{Z}$，$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in R$，则 $a^2 = b^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_R, a+b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, (a+b)^2 = I_2, (a+b)^n = I_2$ 或 $a+b$，故 $a+b$ 不是幂零元.

(3) 证明如果 x 是幂零的，那么 $1+x$ 是单位.

证明. 若 $x^n = 0$ $(n \in \mathbb{Z}_+)$，则令 $y = (1 - x + x^2 - \cdots + (-1)^{n-1}x^{n-1})$，有 $y(1+x) = (1+x)y = 1 + (-1)^n x^n = 1$，故 $1+x$ 是单位. □

3.1.13 设 a, b 是含幺环 R 中的元素，则 $1-ab$ 可逆 $\Leftrightarrow 1-ba$ 可逆.

证明. $(\Rightarrow)(1-ba)^{-1} = 1 + ba + baba + \cdots = 1 + b \cdot 1 \cdot a + b(ab)a + b(abab)a + \cdots = 1 + b(1 + ab + abab + \cdots)a = 1 + b(1-ab)^{-1}a$. 证明此式严格成立需要更深知识，参见文献 [21]. 这里我们不做，而是直接证明结果成立：

已知 $1-ab$ 可逆，令 $u = 1 + b(1-ab)^{-1}a \in R$，则 $u(1-ba) = 1 - ba + b(1-ab)^{-1}a - b(1-ab)^{-1}aba = 1 - ba + (b(1-ab)^{-1} - b(1-ab)^{-1}ab)a = 1 - ba + b(1-ab)^{-1}(1-ab)a = 1 - ba + ba = 1$.

$(1-ba)u = 1-ba+b(1-ab)^{-1}a-bab(1-ab)^{-1}a = 1-ba+b((1-ab)^{-1}a-ab(1-ab)^{-1}a) = 1-ba+b(1-ab)(1-ab)^{-1}a = 1-ba+ba = 1$. 故存在 u 是 $1-ba$ 的逆元.

($\Leftarrow$) 交换 a,b 的地位即可. □

3.1.14 含幺环中元素有多于一个右逆 $\Rightarrow$ 它有无限多个右逆.

证明思路由文献 [26] 给出，但细节为作者补完

证明. 设 u 有多个右逆. 若 u 有左逆，则由**引理 3.12(1)**，u 的左逆等于右逆且唯一，矛盾. 故 u 没有左逆.

考虑元素 $v = v_0 + (1-v_0u)u^k$，其中 $k \in \mathbb{N}$ 且 $uv_0 = 1$，即 v_0 是 u 的任何一个右逆. 我们有 $uv = uv_0 + u^{k+1} - uv_0uu^k = 1 + u^{k+1} + u \cdot 1 \cdot u^k = 1$，故 v 是 u 的右逆. 当 $i \neq j$ 时，不妨设 $j > i$，则 $v_i = (1-v_0u)u^i = v_j = (1-v_0u)u^j \Rightarrow u^i - u^j - v_0u^{i+1} + v_0u^{j+1} = 0 \Rightarrow (u^i - u^j - v_0u^{i+1} + v_0u^{j+1})v_0^j = 0 \Rightarrow v_0^{j-i} - 1 + v_0v_0^{j-i-1} + v_0u = 0 \Rightarrow v_0u = 1$，即 v_0 是 u 的左逆，矛盾，故 $f : \mathbb{N} \Rightarrow \{v_0 + (1-v_0u)u^k \mid k \in \mathbb{N}\}, k \mapsto v_0 + (1-v_0u)u^k$ 是单射，满足条件的 v 有无限多个. □

证明. 另一个证明，令 $S = \{x \mid ux = 1\}, T = \{xu - 1 + s_0 \mid x \in S\}$，其中固定 $s_0 \in S$.

由 u 没有左逆知 $xu - 1 + s_0 \neq s_0$，故 $s_0 \in S - T$. 但 $\forall y \in T, y = xu - 1 + s_0$，有 $uy = uxu - u + us_0 = u - u + 1 = 1$，故 $T \subseteq S$. 令 $f : S \to T, x \mapsto xu - 1 + s$，则由 u 没有左逆，$x \neq z \Rightarrow (x-z)u \neq 0 \Rightarrow f(x) = xu - 1 + s \neq zu - 1 + s = f(z)$，即 f 是单射，由 T 的定义知 f 是满射，故 S 到其真子集 T 有双射 f，这迫使 S 为无限集. □

3.1.15 令 $C(\mathbb{R})$ 为连续实函数 $f : \mathbb{R} \to \mathbb{R}$ 构成的集合，定义 $(f+g)(a) = f(a) + g(a), (fg)(a) = f(a)g(a), \forall a \in \mathbb{R}$，证明：

(1) $C(\mathbb{R})$ 为含幺交换环.

证明. 留给读者. □

(2) $C(\mathbb{R})$ 是否为整环?

解. 否，请读者自证 $C(\mathbb{R})$ 中的加法单位元为 $f_0 : a \mapsto 0, \forall a \in A$.

令 f, g 使得 $f^{-1}(0) = A \subsetneq \mathbb{R}, g^{-1}(0) = B \subsetneq \mathbb{R}$，$A \cup B = \mathbb{R}$，则易见 $fg = f_0$，故该环不是整环.

(3) 该环是否有幂零元?

解. 否，若存在 $m \in \mathbb{Z}_+$ 使得 $f_{C(\mathbb{R})}^m = f_0$，则 $\forall a \in \mathbb{R}, (f(a))^m = 0$，只能 $f(a) = 0$，故 $f = f_0$.

(4) 该环的单位群是什么?

解. 请读者自行证明单位群是 $\{f \mid f \in C(\mathbb{R}), \forall a \in R, f(a) \neq 0\}$，由 f 是连续的，该单位群也可写作 $\{f \mid f \in C(\mathbb{R}), \forall a \in R, f(a) > 0\} \cup \{f \mid f \in C(\mathbb{R}), \forall a \in R, f(a) < 0\}$.

3.1.16 设 D 为有限体，证明对任意 $a \in D$，$a^{|D|} = a$.

证明. $D^\times = D - \{0\}$ 为乘法群，$|D| = |D^\times| + 1$，由**推论 1.61**，$\forall a \neq 0 \in D$ 有 $a^{|D^\times|} = 1$，即 $a^{|D|} = a^{|D^\times|+1} = a$，又 $0^{|D|} = 0$ 显然，故得结论. □

3.2 环的同态与同构

3.2.1 证明整环 $\mathbb{Z}[\sqrt{d}]$ 的任何一个非零理想都包含一个非零整数.

证明. 题意似乎认为 d 是整数，以下我们假定 d 为整数.

记该理想为 I，则存在 $a+b\sqrt{d}\in I$，使得 a,b 为不全为 0 的整数. 此时 $(a+b\sqrt{d})(a-b\sqrt{d})=a^2-b^2d\in I$.

若 $a^2-b^2d=0$，则若 $b=0$，有 $a=0$ 得矛盾，故 $b\neq 0$，d 为整数的平方，此时 $\mathbb{Z}[\sqrt{d}]\cong\mathbb{Z}$ 其元素皆为整数，显然结论成立.

若 $a^2-b^2d\neq 0$，则它是 I 中非零整数.

事实上，可以证明对于 d 为代数数的情形，结论总是成立的. □

3.2.2

(1) 确定 $\mathrm{Aut}(\mathbb{Q}[\sqrt{d}])$，$d\in\mathbb{Q}^\times-(\mathbb{Q}^\times)^2$

解. 设 $\sigma\in\mathrm{Aut}(\mathbb{Q}[\sqrt{d}])$，易见 σ 在 $\mathbb{Q}$ 上的限制为恒等映射.

令 $\sigma(\sqrt{d})=c$，则 $c^2=\sigma(\sqrt{d}^2)=\sigma(d)=d$，故 $c=\pm\sqrt{d}$. 故 $\forall a,b\in\mathbb{Q},\sigma(a+b\sqrt{d})=a\pm b\sqrt{d}$，$\mathrm{Aut}(\mathbb{Q}[\sqrt{d}])\subseteq\{\mathrm{id},\mathrm{conj}\}$ 其中 $\mathrm{conj}:a+b\sqrt{d}\mapsto a-b\sqrt{d}$，容易验证当 $d\in\mathbb{Q}^\times-(\mathbb{Q}^\times)^2$ 时 conj 确实是 $\mathbb{Q}[\sqrt{d}]$ 的自同构，且 $\mathrm{conj}^2=\mathrm{id}$，故 $\mathrm{Aut}(\mathbb{Q}[\sqrt{d}])\cong\mathbb{Z}/2\mathbb{Z}$.

(2) 确定 $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$

解. 平凡群，请读者自证.

3.2.3 证明复数域 $\mathbb{C}$ 可嵌入到环 $M_2(\mathbb{R})$ 中.

证明. 做映射 $f:\mathbb{C}\to M_2(\mathbb{R}),a+bi\mapsto\begin{pmatrix}a&b\\-b&a\end{pmatrix}$，请读者自证 f 是同态. □

3.2.4 求下列环同态的核的生成元.

(1) $\varphi:\mathbb{R}[x,y]\to\mathbb{R},f(x,y)\mapsto f(0,0)$

解. $\ker\varphi=(x,y)_{\mathrm{Ideal}}$，请读者自证.

(2) $\varphi:\mathbb{R}[x]\to\mathbb{C},f(x)\mapsto f(2+i)$

解. $\ker\varphi$ 为 $\mathbb{R}[x]$ 的理想，记为 I，易见一次以下的非零多项式不在 I 中，而 $x^2-4x+5\in I$，即它是 I 中非零多项式中次数最低的，由**命题 3.40** 的证明可知 $I=(x^2-4x+5)_{\mathrm{Ideal}}$ 为主理想，x^2-4x+5 为生成元.

3 $\varphi:\mathbb{Z}[x]\to\mathbb{R}:f(x)\mapsto f(1+\sqrt{2})$

解. 讨论 $\varphi':\mathbb{Q}[x]\to\mathbb{R}:f(x)\mapsto f(1+\sqrt{2})$

$\ker\varphi'$ 为 $\mathbb{Q}[x]$ 的理想, 记为 I, 易见一次以下的非零多项式不在 I 中, 而 $x^2-2x-1\in I$, 即它是 I 中非零多项式中次数最低的, 由**命题 3.40** 的证明可知 $I=(x^2-2x-1)_{\mathrm{Ideal},\mathbb{Q}[x]}=(x^2-2x-1)g(x),g(x)\in\mathbb{Q}[x]$, 由于 x^2-2x-1 的容积 $c(f)=1$, 由**命题 4.29**, $g(x)$ 的容积为整数才能 $(x^2-2x-1)g(x)\in\mathbb{Z}[x]$, 故 $g(x)\in\mathbb{Z}[x],\ker\varphi=\ker\varphi'\cap\mathbb{Z}[x]=(x^2-2x-1)_{\mathrm{Ideal},\mathbb{Z}[x]}$, 生成元为 x^2-2x-1.

(4) $\varphi:\mathbb{C}[x,y,z]\to\mathbb{C}[t]:x\mapsto t,y\mapsto t^2,z\mapsto t^3$.

解. 对任意 $f(x,y,z)\in\mathbb{C}[x,y,z]$, 将 f 中一个 z 替换为 x^3 得到 f', 则 $\varphi(f)=\varphi(f')$, 且 $f=n+mz(n\in\mathbb{C}[x,y],m\in\mathbb{C}[x,y,z]),f'=n+mx^3=f+m(x^3-z)$, 故 f 与 f' 总是只相差 x^3-z 在 $\mathbb{C}[x,y,z]$ 中的倍数.

同理, 一个 y 可替换为 x^2 而使 f 的改变量为 x^2-y 在 $\mathbb{C}[x,y,z]$ 中的倍数.

令 $\ker\varphi=I$ 是 $\mathbb{C}[x,y,z]$ 的理想, $f\in I\Leftrightarrow\varphi(f)=0\Leftrightarrow f$ 可由上述变换得到零多项式, 故 $I=(x^2-y,x^3-z)_{\mathrm{Ideal}}$, 生成员为 x^2-y,x^3-z.

3.2.5

(1) 求环同态 $\varphi:\mathbb{C}[x,y]\to\mathbb{C}[t];x\mapsto t+1,y\mapsto t^3-1$ 的核 K.

解. $K=(y-(x^3-3x^2+3x-2))_{\mathrm{Ideal}}$, 请读者仿照上一题 (4) 自证.

(2) $\mathbb{C}[x,y]$ 的任意理想 $I\supseteq K$ 可由 2 个元素生成.

证明. 对任意 $g(x,y)\in I$, 将 y 替换为 x^3-3x^2+3x-2, 得到 $g'(x,y)$, 仿照上一题 (4) 有 $g'(x,y)-g(x,y)=(y-(x^3-3x^2+3x-2))m(x,y),m(x,y)\in\mathbb{C}[x,y]$, 由于 $y-(x^3-3x^2+3x-2)\in K\subseteq I$ 知 $(y-(x^3-3x^2+3x-2))m(x,y)\in I$, 我们有 $g'(x,y)\in I\Leftrightarrow g(x,y)\in I$.

故 I 的生成元中, 除 $y-(x^3-3x^2+3x-2)$ 以外含有 y 的元均可一步一步消去 y 得到 $\mathbb{C}[x]$ 中元而不改变 I, 而由**命题 3.40**, $\mathbb{C}[x]$ 为 PID, 故所有属于 $\mathbb{C}[x]$ 的生成元由一个 $h(x)$ 生成, 故 $I=(h(x),y-(x^3-3x^2+3x-2))_{\mathrm{Ideal}}$. □

3.2.6 设 I,J 是环 R 的理想, 求证:

(1) $IJ=\{\sum_{k=1}^{n}a_kb_k\mid a_k\in I,b_k\in J\}$ 也是环 R 的理想, 且 $IJ\subseteq I\cap J$.

证明. $\forall u_1,u_2\in IJ,u_1=\sum k=1^{n_1}a_kb_k,u_2=\sum_{k=1}^{n_2}a'_kb'_k$, 此时 $u_1+u_2=\sum_{m=1}^{n_1+n_2}a_mb_m\in IJ$ 其中 $a_m=\begin{cases}a_m, & m\leqslant n_1\\ a'_{m-n_1}, & m>n_1\end{cases},b_m=\begin{cases}b_m, & m\leqslant n_1\\ b'_{m-n_1}, & m>n_1\end{cases}$. 同样, $\forall r\in R,u_1r=(\sum_{k=1}^{n_1}a_kb_k)\,r=\sum_{k=1}^{n_1}a_k(b_kr)$ 其中 $b_kr\in J$, $ru_1=r\,(\sum_{k=1}^{n_1}a_kb_k)=\sum_{k=1}^{n_1}(ra_k)b_k$ 其中 $ra_k\in I$, 故两者都属于 IJ, IJ 为 R 的理想. 由 I 是理想, $J\subseteq R$ 得 $IJ\subseteq I$ 同理 $IJ\subseteq J$, 故 $IJ\subseteq I\cap J$. □

(2) $I+J$ 也是环 R 的理想，并且它恰好是包含 I 和 J 的最小理想.

证明. $(I+J)+(I+J)=I+I+J+J\subseteq I+J, (I+J)R=IR+JR\subseteq I+J, R(I+J)=RI+RJ\subseteq I+J$，故 $I+J$ 是 R 的理想，又若理想 K 满足 $I,J\subseteq K$，则 $I+J\subseteq K+K\subseteq K$，故任何包含 I,J 的理想都包含 $I+J$，得到结论. □

(3) 设 $I=n\mathbb{Z}, J=m\mathbb{Z}$ $(m,n\geqslant 1)$ 为 $\mathbb{Z}$ 的理想，求 $IJ, I+J, I\cap J$.

解. 只给出结果，请读者自证. $IJ=nm\mathbb{Z}, I+J=\gcd(n,m)\mathbb{Z}, I\cap J=\operatorname{lcm}(n,m)\mathbb{Z}$.

3.2.7 设 I 是交换环 R 中的理想，定义 $\sqrt{I}=\{r\in R\mid \exists n\geqslant 1 \text{ s.t. } r^n\in I\}$,

(1) 证明 $\sqrt{I}$ 是 R 的理想.

证明. 对任何 $r,s\in\sqrt{I}$，有 $r^n\in I, s^m\in I$，此时 $(rR)^n\in IR^n\subseteq IR\subseteq I, (Rr)^n\in R^nI\subseteq RI\subseteq I$，在商环 R/I 中，r,s 为幂零元素，由**习题 3.1.12(1)**，$r+s$ 也是 R/I 中的幂零元素，即存在正整数 k 使得 $(r+s+I)^k=(r+s)^k+\sum_{j=1}^{k}\binom{k}{j}(r+s)^{k-j}I^j\subseteq I+0$，故 $(r+s)^k=(r+s+I)^k-\sum_{j=1}^{k}\binom{k}{j}(r+s)^{k-j}I^j\subseteq I$，即 $r+s\in\sqrt{I}$. □

(2) 证明 $\sqrt{I}=R\Leftrightarrow I=R$.

证明. $(\Leftarrow)$ 请读者自证.

$(\Rightarrow)\sqrt{I}\in R\Rightarrow 1\in\sqrt{I}\Rightarrow\exists n\geqslant 1 \text{ s.t. } 1^n\in I$，但对任何 $n\geqslant 1$ 均有 $1^n=1$，故 $1\in I\Rightarrow I=R$. □

(3) 证明 $\sqrt{\sqrt{I}}=\sqrt{I}$.

证明. 留给读者. □

(4) 证明 $\sqrt{I+J}=\sqrt{\sqrt{I}+\sqrt{J}}, \sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}=\sqrt{IJ}$.

证明. (i) 由于 $I\subseteq\sqrt{I}$，故 $\sqrt{I+J}\subseteq\sqrt{\sqrt{I}+\sqrt{J}}$，只需证反之也成立，即 $\forall g\in\sqrt{\sqrt{I}+\sqrt{J}}$ 有 $g\in\sqrt{I+J}$. 令 k 满足 $g^k=a+b$，其中 $a\in\sqrt{I}, b\in\sqrt{J}, a^n\in I, b^m\in J$，则 $(a+b)^{m+n}=\sum_{i=0}^{m+n}\binom{m+n}{i}a^ib^{m+n-i}=\sum_{i=0}^{n}\binom{m+n}{i}a^ib^mb^{n-i}+\sum_{i=n+1}^{m+n}\binom{m+n}{i}a^na^{i-n}b^{m+n-i}\in\sum_{i=0}^{n}\binom{m+n}{i}a^iJb^{n-i}+\sum_{i=n+1}^{m+n}\binom{m+n}{i}Ia^{i-n}b^{m+n-i}\subseteq RJR+RIR\subseteq I+J$. 故我们有 $\sqrt{I+J}\supseteq\sqrt{\sqrt{I}+\sqrt{J}}$.

(ii)① $g\in\sqrt{I\cap J}\Leftrightarrow\exists k\in\mathbb{Z}_+ \text{ s.t. } g^k\in I$ 且 $g^k\in J$

② $g\in\sqrt{I}\cap\sqrt{J}\Leftrightarrow\exists m,n\in\mathbb{Z}_+ \text{ s.t. } g^m\in I$ 且 $g^n\in J$

③ $g\in\sqrt{IJ}\Leftrightarrow\exists k\in\mathbb{Z}_+ \text{ s.t. } g^k\in IJ$.

① ⇒ ② 显然.

② ⇒ ③ $g^{m+n}=g^mg^n\in IJ$，故取 $k=m+n$ 即可.

③ ⇒ ① 由**习题 3.2.6(1)**，$IJ\subseteq I\cap J$ 即得.

综上三种条件等价，三个集合相同. □

3.2.8 设 R 为含幺环，集合 $C(R)=\{c\in R\mid\forall r\in R, rc=cr\}$ 叫做环 R 的中心.

(1) 证明 $C(R)$ 为 R 的子环.

证明. 只需证 $C(R)$ 对加减乘封闭. $\forall c_1, c_2 \in C(R)$ 有 $rc_1 = c_1 r, rc_2 = c_2 r \Rightarrow r(c_1 \pm c_2) = rc_1 \pm rc_2 = c1_r \pm c_2 r = (c_1 \pm c_2)r; rc_1 c_2 = c_1 rc_2 = c_1 c_2 r$, 故 $C(R)$ 是 R 的子环. □

(2) $C(R)$ 不一定是 R 的理想.

解. 在环 $R = M_n(F)$ 中 $C(M_n(F)) = \{\lambda I_n \mid \lambda \in F\}$ 为数量矩阵（参见**例 1.77**，请读者自证细节），$I_n \in C(R)$，但当 $n \geqslant 2$ 时 $C(R) \neq R$，故当 $n \geqslant 2$ 时 $C(M_n(F))$ 不是 $M_n(F)$ 的理想.

3.2.9 证明只有有限个理想的整环 R 是域.

证明. 反证法，若 R 是整环但不是域，则 R 交换，一个元素 x 生成的理想即 xR，取任意非零乘法不可逆元 a，则 $\forall r, a^{i+1}r = a^i(ar)$，其中有 $ar \in R$，故 $(a^{i+1})_{\text{Ideal}} \subseteq (a^i)_{\text{Ideal}}$，又若 $a^i \in (a^{i+1})_{\text{Ideal}}$，则存在 r 使得 $a^i = a^{i+1}r \Rightarrow a^i(1 - ar) = 0$，由于 R 是整环，a 不是零因子，只能 $1 - ar = 0$，即 r 为 a 的逆元，矛盾.

故 $\forall i \in \mathbb{N}$，$(a^i)_{\text{Ideal}} \supsetneqq (a^{i+1})_{\text{Ideal}}$，$\{(a^k)_{\text{Ideal}} \mid k \in \mathbb{N}\}$ 为 R 的无限多个两两不同的理想，与题设矛盾. □

3.2.10 设 $f : R \to S$ 是环同态，如果 R 是体，求证 f 或者是零同态，或者是嵌入.

证明. $I = \ker f \subseteq R$ 为 R 的理想，若 $\ker f = \{0\}$，则 f 为嵌入. 否则令 x 为任何一个 $\ker f$ 的非零元，则 $xx^{-1} = 1 \in IR \in I$，故 $I = R$，f 为零同态. □

3.2.11 设 $\forall k \in \mathbb{Z}_+$，$I_k$ 为 R 的理想，且 $I_k \subseteq I_{k+1}$，求证 $\bigcup_{i=1}^{\infty} I_i$ 也是 R 的理想.

证明. 令 $a, b \in \bigcup_{i=1}^{\infty} I_i, r \in R$，则 $\exists k_1, k_2 \in \mathbb{Z}_+$ 使得 $a \in I_{k_1}, b \in I_{k_2}$，不妨设 $k_1 < k_2$，则 $a + b \in (I_{k_1} + I_{k_2}) \subseteq (I_{k_2} + I_{k_2}) \subseteq I_{k_2} \subseteq \bigcup_{i=1}^{\infty} I_i$，且 $ra, ar \in RI_{k_1}, IR_{k_1} \subseteq I_{k_1} \subseteq \bigcup_{i=1}^{\infty} I_i$，故得结论. □

3.2.12 线性代数

3.2.13 线性代数

3.2.14 验证实矩阵集合

$$\begin{pmatrix} x & -y & -z & -w \\ y & x & -w & z \\ z & w & x & -y \\ w & -z & y & x \end{pmatrix}$$

在矩阵加法和乘法意义下构成环. 证明它同构于四元数体 $\mathbb{H}$.

证明. 设该矩阵集合为 $M_{\mathbb{H}}$，令 $f : M_{\mathbb{H}} \to \mathbb{H}; \begin{pmatrix} x & -y & -z & -w \\ y & x & -w & z \\ z & w & x & -y \\ w & -z & y & x \end{pmatrix} \mapsto x + yi + zj + wk$，显然 f 将单位元 I_4 映射到 $1_{\mathbb{H}}$，且保持加法. 只需证明它保持乘法即可.

令 $Q_1 = \begin{pmatrix} x_1 & -y_1 & -z_1 & -w_1 \\ y_1 & x_1 & -w_1 & z_1 \\ z_1 & w_1 & x_1 & -y_1 \\ w_1 & -z_1 & y_1 & x_1 \end{pmatrix}, Q_2 = \begin{pmatrix} x_2 & -y_2 & -z_2 & -w_2 \\ y_2 & x_2 & -w_2 & z_2 \\ z_2 & w_2 & x_2 & -y_2 \\ w_2 & -z_2 & y_2 & x_2 \end{pmatrix}$.

则

$$Q_1Q_2 = \begin{pmatrix} x_1x_2-y_1y_2-z_1z_2-w_1w_2 & -x_1y_2-y_1x_2-z_1w_2+w_1z_2 & -x_1z_2+y_1w_2-z_1x_2-w_1y_2 & -x_1w_2-y_1z_2+z_1y_2-w_1x_2 \\ y_1x_2+y_2x_1-w_1z_2+z_1w_2 & -y_1y_2+x_1x_2-w_1w_2-z_1z_2 & -y_1z_2-x_1w_2-w_1x_2+z_1y_2 & -y_1w_2+x_1z_2+w_1y_2+z_1x_2 \\ z_1x_2+w_1y_2+x_1z_2-y_1w_2 & -z_1y_2+w_1x_2+x_1w_2+y_1z_2 & -z_1z_2-w_1w_2+x_1x_2-y_1y_2 & -z_1w_2+w_1z_2-x_1y_2-y_1x_2 \\ w_1x_2-z_1y_2+y_1z_2+x_1w_2 & -w_1y_2-z_1x_2+y_1w_2-x_1z_2 & -w_1z_2-z_1w_2+y_1x_2+x_1y_2 & -w_1w_2-z_1z_2-y_1y_2+x_1x_2 \end{pmatrix},$$

因此 Q_1Q_2 在 f 的定义域中, 并且 $f(Q_1Q_2) = (x_1x_2-y_1y_2-z_1z_2-w_1w_2)+(y_1x_2+x_1y_2+z_1w_2-w_1z_2)i+(z_1x_2+x_1z_2+w_1y_2-y_1w_2)j+(w_1x_2+x_1w_2+y_1z_2-z_1y_2)k$, 而 $f(Q_1) = x_1+y_1i+z_1j+w_1k, f(Q_2) = x_2+y_2i+z_2j+w_2k$, 易验证 f 保持乘法并是双射, 故 f 是同构. □

3.2.15 复变函数

3.3 环的同态基本定理

3.3.1 证明交换环 R 中全部幂零元素组成的集合 $N=\mathrm{Nil}(R)$ 是环 R 的理想，并且商环 R/N 中只有零元素是幂零的.

证明. 若 a,b 为幂零元素，则由**习题 3.1.12(1)** 知 $a+b$ 也是幂零元素，对任意 $r\in R$，因 R 交换有 $a^k=0\Rightarrow (ar)^k=a^kr^k=0r^k=0$，故 ar（同理 ra 也）是幂零元素，N 是 R 的理想.

对于商环 R/N，若 $a+N\in R/N$ 是幂零元，我们有 $(a+N)^k=\sum_{i=0}^k\binom{k}{i}a^{k-i}N^i\in N$，由于 $\sum_{i=1}^k\binom{k}{i}a^{k-i}N^i\in RN+\cdots+RN\in N$，因此 $a^k=\sum_{i=0}^k\binom{k}{i}a^{k-i}N^i-\sum_{i=1}^k\binom{k}{i}a^{k-i}N^i\in N$，故存在 l 使得 $(a^k)^l=0\Rightarrow a^{kl}=0$，即 $a\in N, a+N=0+N$ 是 R/N 中的零元素. □

3.3.2 线性代数

3.3.3 设 $f:R\to S$ 是环之间的同态，I 和 J 是环 R 和 S 的理想，并且 $f(I)\subseteq J$，按如下方式作商环之间的映射：

$$\overline{f}:R/I\to S/J,\overline{a}\mapsto[f(a)],$$

其中对 $a\in R,\overline{a}=a+I$ 为 R/I 中元素，$[f(a)]=f(a)+J$ 为 S/J 中元素.

(1) 证明上述映射 $\overline{f}$ 是良好定义的，并且是环同态.

证明. 如 $\overline{a_1}=\overline{a_2}$，则 $a_1+I=a_2+I$ 即 $a_1-a_2\in I$，故 $f(a_1)-f(a_2)=f(a_1-a_2)\in J$，$[f(a_1)]-f[(a_2)]=f(a_1)-f(a_2)+J=J$ 为 S/J 中零元素，即 $\overline{f}(\overline{a_1})=[f(a_1)]=[f(a_2)]=\overline{f}(\overline{a_1})$，故 $\overline{f}$ 是良好定义的.

又 $\overline{f}(\overline{a}+\overline{b})=f(a+b)+J=f(a)+J+f(b)+J=\overline{f}(\overline{a})+\overline{f}(\overline{b}),\overline{f}(\overline{a}\overline{b})=f(ab)+J=f(a)f(b)+J=f(a)f(b)+f(a)J+Jf(b)+J$（因 J 是 S 的理想）$=(f(a)+J)(f(b)+J)=\overline{f}(\overline{a})\overline{f}(\overline{b})$，且 $\overline{f}(\overline{1_R})=f(1_R)+J=1_S+J=1_{S/J}$，故 $\overline{f}$ 是同态. □

(2) 证明 $\overline{f}$ 是环同构 $\Leftrightarrow f(R)+J=S$ 且 $I=f^{-1}(J)$.

证明. ($\Rightarrow$) 留给读者.

($\Leftarrow$)$\overline{f}$ 是单射：若 $\overline{a_1}\neq\overline{a_2}$，则 $a_1-a_2\notin I$，由 $I=f^{-1}(J)$ 知 $f(a_1-a_2)\notin J$，故 $f(a_1)-f(a_2)\notin J$，$[f(a_1)]=f(a_1)+J$ 与 $[f(a_2)]=f(a_2)+J$ 为 S/J 中不同元素.

$\overline{f}$ 是满射：对 $\forall u+J\in S/J$，则 $u\in S$，由于 $f(R)+J=S$，则存在 u_0 使得 $u_0+j_0=u,j_0\in J,u_0\in f(R)$，故 $u+J=u_0+j_0+J=u_0+J$，令 $f(r_0)=u_0$，则 $\overline{f}(\overline{r_0})=u_0+J=u+J$. □

3.3.4 设 $(R,+,\cdot)$ 是含幺环，定义 $a\oplus b=a+b+1, a\otimes b=ab+a+b$，证明 $(R,\oplus,\otimes)$ 也是含幺环，并且与环 $(R,+,\cdot)$ 同构.

证明. 加法为阿贝尔群：

加法满足结合律：$(a\oplus b)\oplus c=a\oplus(b\oplus c)=a+b+c+1+1\in R$.

加法有单位元：R 中存在 $1_{R,+,\cdot}$ 的逆元 $-1_{R,+,\cdot}$，对任意 $a\in R$ 满足 $a\oplus(-1)=(-1)\oplus a=a-1+1=a$，故 $0_{R,\oplus,\odot}=-1_{R,+,\cdot}$.

加法有逆元：令 $\ominus a=-a+(-1)+(-1)$，则 $a\oplus(\ominus a)=(\ominus a)\oplus a=-a+(-1)+(-1)+a+1=-1=0_{R,\oplus,\odot}$.

加法交换：$a\oplus b=b\oplus a=a+b+1\in R$.

乘法满足结合律：$(a\odot b)\odot c=(ab+a+b)\odot c=(ab+a+b)c+(ab+a+b)+c=abc+bc+ac+ab+a+b+c$，$a\odot(b\odot c)=a\odot(bc+b+c)=a(bc+b+c)+(bc+b+c)+a=abc+bc+ac+ab+a+b+c$，两者一致.

乘法有单位元：R 中存在加法单位元 $0_{R,+,\cdot}$，对任意 $a\in R$ 满足 $a\odot 0=a\cdot 0+a+0=a, 0\odot a=0\cdot a+0+\qquad a=a$，故 $1_{R,\oplus,\odot}=0_{R,+,\cdot}$.

分配律：$\lambda\odot(a\oplus b)=\lambda\odot(a+b+1)=\lambda a+\lambda b+\lambda+\lambda+a+b+1$，$(\lambda\odot a)\oplus(\lambda\odot b)=(\lambda a+\lambda+a)\oplus(\lambda b+\lambda+b)=\lambda a+\lambda b+\lambda+\lambda+a+b+1$，两者相等. $(a\oplus b)\odot\lambda=(a+b+1)\odot\lambda=a\lambda+b\lambda+\lambda+\lambda+a+b+1$，$(a\odot\lambda)\oplus(b\odot\lambda)=(a\lambda+\lambda+a)\oplus(b\lambda+\lambda+b)=a\lambda+b\lambda+\lambda+\lambda+a+b+1$，两者相等.

综上，$(R,\oplus,\odot)$ 为含幺环.

同构性：令 $f:(R,+,\cdot)\to(R,\oplus,\odot);u\mapsto u-1_{R,+,\cdot}$，则 $f(a+b)=a+b-1=(a-1)+(b-1)+1=f(a)\oplus f(b)$，$f(ab)=ab-1=ab-a-b+1+a-1+b-1=(a-1)(b-1)+(a-1)+(b-1)=f(a)\odot f(b)$，$f(1_{R,+,\cdot})=0_{R,+,\cdot}=1_{R,\oplus,\odot}$，易见 f 为双射，故 f 为同构. □

3.3.5

(1) 证明主理想环的每个同态像也是主理想环.

证明. 设 $\varphi:R\to S$ 为环同态，R 为主理想环.

则 $\ker\varphi$ 是主理想，$\ker\varphi=(x)_{\mathrm{Ideal},R}=Rx+xR+RxR$，且 $\operatorname{im}\varphi$ 与 $R/\ker\varphi$ 同构. 设 J 为 $\operatorname{im}\varphi$ 的任意理想，则 $f^{-1}(J)$ 为 $R/\ker\varphi$ 的理想，$f^{-1}(J)+\ker\varphi$ 为 R 的理想（请读者自证!），因 R 为主理想环，存在 $y\in R$ 满足 $f^{-1}(J)+\ker\varphi=Ry+yR+RyR$，故 $f^{-1}(J)=R(y-x)+(y-x)R+R(y-x)R$，$J=f(R)f(y-x)+f(y-x)f(R)+f(R)f(y-x)f(R)=\operatorname{im}\varphi f(y-x)+f(y-x)\operatorname{im}\varphi+\operatorname{im}\varphi f(y-x)\operatorname{im}\varphi=(y-x)_{\mathrm{Ideal},\operatorname{im}\varphi}$ 为 $\operatorname{im}\varphi$ 的主理想，即 $\operatorname{im}\varphi$ 是主理想环. □

(2) 求证 $\mathbb{Z}/m\mathbb{Z}$ $(m\geqslant 1)$ 为主理想环.

证明. 留给读者. □

3.3.6 设 S,R_i $(i\in I)$ 为环，$R=\prod_{i\in I}R_i$ 为 R_i 的笛卡尔积.

(1) 令 $\pi_i:R\to R_i,(a_j)_{j\in I}\mapsto a_i$，证明 π_i 为环同态，这样的环同态称为正则投射.

(2) 设对于每个 $i\in I,\varphi_i:S\to R_i$ 均为环同态，求证存在唯一的环同态 $\varphi:S\to R$ 使得对任意 $i\in I$ 均有 $\pi_i\circ\varphi=\varphi_i$.

证明. 留给读者. □

3.3.7 设 D 为整环，m,n 为互素的正整数，$a,b\in D$，若 $a^m=b^m,a^n=b^n$，证明 $a=b$. ，**证明**. 对任意非零元 $d\in D$，D 没有零因子使得 $ad=bd\Leftrightarrow(a-b)d=0\Leftrightarrow a-b=0\Leftrightarrow a=b$，即消去律成立：

等式两边可消去 d. 当 $a=0$ 或 $b=0$ 时，由 b 或 a 不是零因子得到 $b=0$ 或 $a=0$，结论显然成立，因此我们以下假定 $a,b\neq 0$，故 a,b 的任意方幂均不为 0，满足消去律.

不妨设 $m>n$，因 m,n 为正整数，存在 k_0 使得 $m=k_0n+r_0, k_0\in\mathbb{Z}_+, 0\leqslant r_0<n$，则 $a^m=b^m\Leftrightarrow (a^n)^{k_0}a^{r_0}=(b^n)^{k_0}b^{r_0}\Leftrightarrow (a^n)^{k_0}a^{r_0}=(a^n)^{k_0}b^{r_0}$，故由消去律 $a^{r_0}=b^{r_0}$. 此时我们有 $\gcd(m,n)=\gcd(m-k_0n,n)=\gcd(n,r_0)$.

由 m,n 的任意性，我们对 n,r_0 同样操作得到 $a^{r_1}=b^{r_1}$，其中 $n=k_1r_0+r_1, k_1\in\mathbb{Z}_+, 0\leqslant r_1<r_0, \gcd(n,r_0)=\gcd(r_0,r_1)=\gcd(m,n)$.

当 $r_{j-1}>0$ 时继续这个过程，我们有 $a^{r_j}=b^{r_j}$，其中 $r_{j-2}=k_jr_{j-1}+r_j, k_j\in\mathbb{Z}_+, 0\leqslant r_j<r_{j-1}, \gcd(r_{j-1},r_j)=\gcd(r_{j-2},r_{j-1})=\gcd(m,n)$.

由于 $0\leqslant r_j<r_{j-1}$，该过程可以持续到 $r_l=0$，此时 $\gcd(r_{l-1},0)=\gcd(m,n)$，我们有 $r_{l-1}=\gcd(m,n)$，$a^{\gcd(m,n)}=b^{\gcd(m,n)}$，在本题中 $\gcd(m,n)=1$，我们有 $a=b$. □

注记. 本题的证明即对 a,b 的指数使用欧几里得算法.

3.3.8 设 $I_1,I_2,...,I_n$ 为 R 的理想，且：

(1) $I_1+\cdots+I_n=R$.

(2) $\forall 1\leqslant i\leqslant n, I_i\cap(I_1+\cdots+I_{i-1}+I_{i+1}+\cdots+I_n)=\{0\}$

求证 $R\cong\prod_{i=1}^n I_i$.

证明. 由 $\sum_{i=1}^n I_i=R$ 知 $\forall r\in R$ 有形式 $r'=(a_1,a_2,...,a_n)$ 使得 $r=\sum_{i=1}^n a_i$ 且 $a_i\in I_i, \forall 1\leqslant i\leqslant n$，并且给定 $a_1,a_2,...,a_n$ 其中 $a_i\in I_i, \forall 1\leqslant i\leqslant n$ 有 $r=\sum_{i=1}^n a_i\in R$. 我们只要证明这形式唯一即可，即若 $r\in R, r=\sum_{i=1}^n a_i=\sum_{i=1}^n b_i, a_i,b_i\in I_i$ 则 $\forall 1\leqslant i\leqslant n, a_i=b_i$.

这时 $0=r-r=\sum_{i=1}^n a_i-b_i, a_i-b_i\in I_i$，$a_k-b_k=-\sum_{\substack{1\leqslant i\leqslant n\\ i\neq k}} a_i-b_i$，左边属于 I_i，右边属于 $I_1+\cdots+I_{i-1}+I_{i+1}+\cdots+I_n$，由条件 (2) 知两边必须为 0，即 $a_i=b_i$ 对一切 $1\leqslant i\leqslant n$ 成立，上述形式是唯一的. □

3.3.9 环 R 中元素 e 叫做幂等元素，是指 $e^2=e$. 若 e 又属于环 R 的中心，则称 e 为中心幂等元素. 设 R 是含幺环，e 为 R 的中心幂等元素，证明

(1) $1-e$ 也是中心幂等元素.

证明. 已知 $e^2=e$，$\forall r\in R$ 有 $er=re$，则 $(1-e)^2=1-e-e+e^2=1-e+0=1-e, r(1-e)=r-re=r-er=(1-e)r$，故得结论. □

(2) eR 和 $(1-e)R$ 均是 R 的理想，且 $R\cong eR\times(1-e)R$.

证明. $e,(1-e)\in C(R)$ 已证. 故 $eR=eR+Re+ReR$ 和 $(1-e)R=(1-e)R+R(1-e)+R(1-e)R$ 为 R 的理想，又 $\forall r\in R, r=er+(1-e)r$，故 $eR+(1-e)R=R$，且 $er_1=(1-e)r_2\Rightarrow e^2r_1=e(1-e)r_2\Rightarrow e^2r_1=0\Rightarrow er_1=0, er_1=(1-e)r_2\Rightarrow(1-e)er_1=(1-e)^2r_2\Rightarrow 0=r_2-er_2-er_2+e^2r_2\Rightarrow 0=(1-e)r_2$，即 $eR\cap(1-e)R=\{0\}$，在**习题 3.3.8** 中令 $I_1=eR, I_2=(1-e)R$ 即得结论. □

3.3.10 本题有错误见文献

3.3.11 环 R 中幂等元素集合 $\{e_1, e_2, ..., e_n\}$ 叫做正交的, 是指当 $i \neq j$ 时 $e_i e_j = 0$, 设 $R, R_1, R_2, ..., R_n$ 为含幺环, 则下列两个条件等价:

(1) $R \cong R_1 \times R_2 \times \cdots \times R_N$.

(2) R 具有正交的中心幂等元集合 $\{e_1, e_2, ..., e_n\}$ s.t. $e_1 + e_2 + \cdots e_n = 1_R$, 且 $e_i R \cong R_i$ $(\forall 1 \leqslant i \leqslant n)$

证明. ($\Rightarrow$) 取 $e_i = (a_{i1}, a_{i2}, ..., a_{in})$ 其中 $a_i i = 1 \forall i, a_i j = 0 \forall i \neq j$, 则易验证 $\{e_i \mid 1 \leqslant i \leqslant n\}$ 满足 (2) 的条件.

($\Leftarrow$) 由于 $e_i \in C(R)$, 故 $(e_i)_{\mathrm{Ideal},R} = e_i R$ 为 R 的理想, $\forall r \in R$ 有 $e_1 r + e_2 r + \cdots + e_n r = r$ 故 $e_1 R + e_2 R + \cdots + e_n R = R$, 考虑任何元素 $e_i r_i \in e_i R \cap (e_1 R + \cdots + e_{i-1} R + e_{i+1} R + \cdots + e_n R)$, 存在 $r_j (j \neq i)$ 使得 $e_i r_i = \sum_{j \neq i} e_j r_j$, 两边同乘 e_i 得 $e_i R_i = e_i^2 r_i = \sum_{j \neq i} e_i e_j r_j = \sum_{j \neq i} 0 r_j = 0$, 故 $e_i R \cap (e_1 R + \cdots + e_{i-1} R + e_{i+1} R + \cdots + e_n R) = \{0\}$, 在**习题 3.3.8** 中令 $I_i = e_i R$ 即得结论. □

3.4 整环与域

3.4.1 设 R 是含幺交换环, $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_m$ 为 R 的素理想, 而 A 为 R 的理想, 如果 $A \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_m$, 则必存在某个 $i\ (1 \leqslant i \leqslant m)$ 使得 $A \subseteq \mathfrak{p}_i$.

证明由文献 [25] 给出.

证明. 用数学归纳法.

当 $m = 1$ 时, 结论显然成立. 当 $m = 2$ 时, 若结论不成立, 则存在 $a_1, a_2 \in A, a_1 \in \mathfrak{p}_1 - \mathfrak{p}_2, a_2 \in \mathfrak{p}_2 - \mathfrak{p}_1$, 若 $a_1 + a_2 \in \mathfrak{p}_1$, 则 $a_2 = a_1 + a_2 - a_1 \in \mathfrak{p}_1 - \mathfrak{p}_1 \subseteq \mathfrak{p}_1$, 矛盾, 同理 $a_1 + a_2 \in \mathfrak{p}_2$, 两者综合与 $a_1 + a_2 \in A \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2$ 矛盾.

假设我们已有 $m = k$ 时结论成立, 下证 $m = k + 1$ 时结论成立, 用反证法. 若不存在 $\mathfrak{p}_i$ 包含 A, 则固定 $1 \leqslant i \leqslant k + 1$, 因 $m = k$ 时对 $\mathfrak{p}_j\ (j \neq i)$ 结论不成立, 则条件也不成立, 即 $A \nsubseteq \bigcup_{\substack{1 \leqslant j \leqslant k+1 \\ j \neq i}} \mathfrak{p}_j$, 但 $A \subseteq \bigcup_{\substack{1 \leqslant j \leqslant k+1 \\ j \neq i}} \mathfrak{p}_j \cup \mathfrak{p}_i$, 故存在 $a_i \in A$ 使得 $a_i \in \mathfrak{p}_i, a_i \notin \mathfrak{p}_j\ (j \neq i)$.

考虑元素 $b = \prod_{i=1}^{k} a_i, c = b + a_{k+1}$, 则对 $1 \leqslant i \leqslant k$ 有 $b \in \mathfrak{p}_i$, 且由 $\mathfrak{p}_{k+1}$ 是素理想, $a_i \notin \mathfrak{p}_{k+1}, \forall 1 \leqslant i \leqslant k$ 有 $b \notin \mathfrak{p}_{k+1}$, 又 $a_{k+1} \in \mathfrak{p}_{k+1}, a_{k+1} \notin \mathfrak{p}_j\ (j \neq k+1)$, 若 $c \in \mathfrak{p}_{k+1}$, 则 $b = c - a_{k+1} \in \mathfrak{p}_{k+1} - \mathfrak{p}_{k+1} \subseteq \mathfrak{p}_{k+1}$, 矛盾. 故由 $c \in A \subseteq \bigcup_{i=1}^{k+1} \mathfrak{p}_i$, 存在 $1 \leqslant i \leqslant n$ 使得 $c \in \mathfrak{p}_i$, 此时 $a_{k+1} = c - b \in \mathfrak{p}_i - \mathfrak{p}_i \subseteq \mathfrak{p}_i$, 矛盾. 故 $m = k + 1$ 时结论成立.

综上, m 为一切正整数时结论成立. □

3.4.2 有限含幺交换环的素理想必是极大理想.

证明. $\mathfrak{p}$ 是 R 的素理想 $\Leftrightarrow R/\mathfrak{p}$ 是整环, 由 $\mathfrak{p}$ 是真理想, $R/\mathfrak{p}$ 非零, 又 R 有限, 故 $R/\mathfrak{p}$ 是非零有限整环, 由**习题 3.1.11**, $R/\mathfrak{p}$ 必为域, 故 $\mathfrak{p}$ 为极大理想. □

3.4.3 交换环 R 中所有素理想均包含 $\mathrm{Nil}(R)$

证明. 对任意 $a \in \mathrm{Nil}(R)$, 由于素理想 p 为真理想, 故存在 $b \in R, b \notin \mathfrak{p}$. 由于 $\exists m \in \mathbb{Z}_+$ 使得 $a^m = 0$, 因此 $a^m b = 0 \in \mathfrak{p}$, 若 $a \notin \mathfrak{p}$, 则 $a^{m-1} b \in \mathfrak{p}, \cdots, a^0 b = b \in \mathfrak{p}$, 矛盾. 故 $a \in \mathfrak{p}$, 由 a 的任意性即得结论. □

3.4.4 设 $\mathfrak{p}$ 是含幺交换环 R 的素理想, $I_1, ..., I_n$ 为 R 的理想, 如果 $\mathfrak{p} = \bigcap_{i=1}^{n} I_i$, 则 $\mathfrak{p}$ 必等于某个 I_i.

证明. 由**习题 3.2.6(1)**, $\prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i = \mathfrak{p}$, 有 $I_n \subseteq \mathfrak{p}$ 或 $\prod_{i=1}^{n-1} I_i \subseteq \mathfrak{p}$, 继续归纳下去即得存在 $i\ (k < i \leqslant n)$ 使得 $I_i \subseteq \mathfrak{p}$ 或 $\prod_{i=1}^{k} I_i \subseteq \mathfrak{p}$, 取 $k = 0$, 即结论成立或 $1 = \prod_{i=1}^{0} I_i \subseteq \mathfrak{p}$, 后者与 $\mathfrak{p}$ 是真理想矛盾, 故结论成立. □

3.4.5 设 $f : R \to S$ 是交换环的满同态, $K = \ker f$.

(1) 若 $\mathfrak{p}$ 是 R 的素理想并且 $\mathfrak{p} \supseteq K$, 则 $f(\mathfrak{p})$ 也是 S 的素理想;

证明. 若 $cd \in f(\mathfrak{p})$, 由于 f 是满射, 任选 $a, b \in R$ 使 $f(a) = c, f(b) = d$, 由 $f(ab) = cd \in f(\mathfrak{p})$, 得 $ab + k \in \mathfrak{p}$, 其中 $k \in \ker f = K \subseteq \mathfrak{p}$, 故 $ab \in \mathfrak{p}$. 由 $\mathfrak{p}$ 是素理想, $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$, 我们有 $c = f(a) \inf(\mathfrak{p})$ 或 $d = f(b) \in f(\mathfrak{p})$.

我们仍需验证 $f(\mathfrak{p})$ 是 S 的真理想即得结论. 由同态性 $f(\mathfrak{p})$ 对加减法自封，而 f 是满射，对任意 $s\in S, c\in f(\mathfrak{p})$ 有 $r\in R, f(r)=s, a\in\mathfrak{p}$ 使得 $sc=f(r)f(a)=f(ta)$，其中 $ra\in\mathfrak{p}$，故 $sc\in f(\mathfrak{p})$，$f(\mathfrak{p})$ 为理想，若 $f(\mathfrak{p})=S$，则 $R=f^{-1}(S)+\ker f=\mathfrak{p}+K\subseteq\mathfrak{p}$，与 $\mathfrak{p}$ 为真理想矛盾，故 $f(\mathfrak{p})$ 是 S 的真理想. □

(2) 若 $\mathfrak{q}$ 是 S 的素理想，则 $f^{-1}(\mathfrak{q})$ 也是 R 的素理想.

证明. 若 $ab\in f^{-1}(\mathfrak{q})$, 则 $f(a)f(b)=f(ab)\in\mathfrak{q}$, 由 $\mathfrak{q}$ 是素理想, $f(a)\in\mathfrak{q}$ 或 $f(b)\in\mathfrak{q}$, 故 $a\in f^{-1}(\mathfrak{q})$ 或 $b\in f^{-1}(\mathfrak{q})$.

我们仍需验证 $f^{-1}(\mathfrak{q})$ 是 R 的真理想即得结论. 由同态性 $f(\mathfrak{p})$ 对加减法自封，对任意 $r\in R, a\in f^{-1}(\mathfrak{q})$ 有 $s=f(r)\in S, c=f(a)\in\mathfrak{q}$ 使得 $ra=(f^{-1}(s)+k_1)(f^{-1}(c)+k_2)=f^{-1}(sc)+k_1f^{-1}(c)+k_2f^{-1}(s)+k_1k_2$ 其中 $k_1,k_2\in K$，由于 $0\in\mathfrak{q}$，故 $K\subseteq f^{-1}(\mathfrak{q})$，又 $sc\in\mathfrak{q}$，故 $ra\in f^{-1}(\mathfrak{q})+KR+KR+KK\in f^{-1}(\mathfrak{q})$，$f^{-1}(\mathfrak{q})$ 是理想，若 $f^{-1}(\mathfrak{q})=R$，则由 f 是满射 $\mathfrak{q}=S$，与 $\mathfrak{q}$ 为真理想矛盾，故 $f^{-1}(\mathfrak{q})$ 是 R 的真理想. □

(3a) S 中的素理想和 R 中包含 K 的素理想是一一对应的.

证明. 我们已经有 (1)(2) 的结果，我们只需验证对不同的 R 的理想 $\mathfrak{p}_1\supseteq K, \mathfrak{p}_2\supseteq K$，它们的像不同即可.

不妨设 $a\in R, a\in\mathfrak{p}_1, a\notin\mathfrak{p}_2$，则若 $f(a)\in f(\mathfrak{p}_2)$，有 $b\in\mathfrak{p}_2$ 使得 $a-b\in K$，但 $K\subseteq\mathfrak{p}_2$，即 $a=a-b+b\in K+\mathfrak{p}_2\in\mathfrak{p}_2$，矛盾.

对于 $a\in R, a\notin\mathfrak{p}_1, a\in\mathfrak{p}_2$，交换两个理想的地位讨论即可. 故 f 诱导 R 中包含 K 的素理想到 S 中的素理想的双射. □

(3b) S 中的极大理想和 R 中包含 K 的极大理想是一一对应的.

证明. 若 $\mathfrak{p}$ 是 R 中包含 K 的极大理想，则 $R/\mathfrak{p}$ 为域并且 $f':R/\mathfrak{p}\to S/f(\mathfrak{p})$ 中 $f^{-1}(f(\mathfrak{p}))=\mathfrak{p}$, $f(R)+f(\mathfrak{p})=S+f(\mathfrak{p})=S$，故由**习题 3.3.3(2)**，$f'$ 是良好定义的环同构，故 $S/f(\mathfrak{p})$ 为域，$f(\mathfrak{p})$ 为 S 的极大理想.

反之，若 $\mathfrak{q}$ 为 S 的极大理想，则 $S/\mathfrak{q}$ 为域且同理 $g':R/f^{-1}\mathfrak{q}\to S/\mathfrak{q}$ 是良好定义的环同构，故 $R/f^{-1}\mathfrak{q}$ 为域，$f^{-1}\mathfrak{q}$ 为 R 的包含 K 的极大理想.

由 (3a) 的证明不同的理想 $\mathfrak{p}_1,\mathfrak{p}_2$ 若均包含 K 则它们的像不同，故故 f 诱导 R 中包含 K 的极大理想到 S 中的极大理想的双射. □

3.4.6 设 I 是环 R 的理想，求证 R/I 中素理想均可写成 $\mathfrak{p}/I$ 的形式，其中 $\mathfrak{p}$ 是 R 中包含 I 的素理想. 由此证明交换环 R 的素谱 Spec$R$ 与 $R/\mathrm{Nil}(R)$ 的素谱 Spec$R/\mathrm{Nil}(R)$ 一一对应.

证明. $\mathfrak{q}$ 是 R/I 的素理想 $\Leftrightarrow\forall a+I, b+I\in\mathfrak{q}$ 有 $(a+I)(b+I)=ab+aI+Ib+II=ab+I\in\mathfrak{q}\Rightarrow(a+I)\in\mathfrak{q}$ 或 $b+I\in\mathfrak{q}$ 故 $\mathfrak{p}=\{x\mid x+I\in\mathfrak{q}\}$ 满足 $ab\in\mathfrak{p}\Rightarrow a\in\mathfrak{p}$ 或 $b\in\mathfrak{p}$，且 $0\in\mathfrak{q}\Rightarrow I\in\mathfrak{p}$，故 $\mathfrak{p}$ 为包含 I 的素理想，且 $\mathfrak{p}/I=\mathfrak{q}$.

反之，R 的包含 I 的素理想 $\mathfrak{p}$ 满足 $ab\in\mathfrak{p}\Rightarrow a\in\mathfrak{p}$ 或 $b\in\mathfrak{p}$, 即 $(a+I)(b+I)=ab+aI+Ib+II\in\mathfrak{p}+I\Rightarrow(a+I)\in\mathfrak{p}+I$ 或 $b+I\in\mathfrak{p}+I$，又 $I\subseteq\mathfrak{p}$，故 $\mathfrak{p}/I$ 是良好定义的，为 R/I 的素理想.

由**习题 3.4.3**，素谱 Spec$R$ 总满足其中元素包含理想 Nil(R)（**习题 3.3.1**），故上述包含性可以省去，并且由**习题 3.4.5(3a)** 的证明，Spec$R$ 中不同元素总有在 $R/\mathrm{Nil}R$ 中不同的像，故得结论. □

3.4.7 设 $m \geqslant 2$，确定 Spec($\mathbb{Z}/m\mathbb{Z}$) 和 Max($\mathbb{Z}/m\mathbb{Z}$).

解. 易见 $\mathbb{Z}/m\mathbb{Z}$ 的理想只有 $R_n = n\mathbb{Z}/m\mathbb{Z}$ 其中 $n \mid m$，并且 $(\mathbb{Z}/m\mathbb{Z})/R_n \cong \mathbb{Z}/n\mathbb{Z}$，它是整环（域）当且仅当 n 为素数.

故 $\mathrm{Spec}(\mathbb{Z}/m\mathbb{Z}) = \mathrm{Max}(\mathbb{Z}/m\mathbb{Z}) = \begin{cases} m\mathbb{Z}/m\mathbb{Z} = \{0\}, & m\text{为素数时} \\ n\mathbb{Z}/m\mathbb{Z}, & m\text{不为素数时，其中}n\text{是}m\text{的素因子} \end{cases}$.

注：这里认为零环不是整环，以与素理想的定义一致，参见文献 [9] 从

3.4.8 确定环 $\mathbb{Z}[x]/(x^2+3, p)$ 的结构，其中 $p = 3, 5$.

解. 只给出结果，请读者自证.

$\mathbb{Z}[x]/(x^2+3, 3)_{\mathrm{Ideal}} = \{a + bx \mid a, b \in \mathbb{F}_3\}$;

$\mathbb{Z}[x]/(x^2+3, 5)_{\mathrm{Ideal}} = \mathbb{F}_5[\sqrt{2}]$.

3.4.9 确定下面每个环的极大理想.

(1) $\mathbb{R} \times \mathbb{R}$;

解. 设该环的一个理想为 I，若 $(a, b) \in I$ 其中 $a \neq 0, b \neq 0$，则 $(1, 1) = (a, b)(a^{-1}, b^{-1}) \in I$，$I = \mathbb{R} \times \mathbb{R}$，因此若 I 是真理想，必有 a 或 b 恒等于 0，这时 I 同构于 $\mathbb{R}$ 上的理想，后者只可能是 $\{0\}$ 或 $\mathbb{R}$，因此真理想只有三种可能：$\{0\} \times \{0\}$、$\{0\} \times \mathbb{R}$ 和 $\mathbb{R} \times \{0\}$. 显然后两者为极大理想.

(2) $R = \mathbb{R}[x]/(x^2)_{\mathrm{Ideal}}$

解. 考虑 $I \subsetneqq R$ 为 R 的理想，由于 $x^2 \equiv 0$，故 R 中元素为 x 的零次或一次式，若 $ax + b \in I$ $(a, b \in \mathbb{R})$，则当 $b \neq 0$ 时 $(ax + b)(-ax/b^2 + 1/b) = 1 \in I$，$I = R$ 矛盾，故 $b = 0$，若 $a \neq 0$，则 $I = (ax)(cx + d) = \{adx \mid d \in \mathbb{R}\} = \{a'x \mid a' \in \mathbb{R}\}$. 若 $a = 0$，则 $I = \{0\}$. 故 $\{ax \mid a \in \mathbb{R}\}$ 为 R 的极大理想.

(3) $R = \mathbb{R}[x]/(x^2 - 3x + 2)_{\mathrm{Ideal}}$.

解. 由于 $x^2 \equiv 3x - 2$，故 R 中元素为 x 的零次或一次式，考虑理想 $I \subsetneqq R$，若 $ax + b \in I$ $(a, b \in \mathbb{R})$，则当 $2a + b \neq 0, a + b \neq 0$ 时 $(ax + b)(cx + d) = 1, I = R$ 矛盾，其中当 $b \neq 0$ 时 $c = -a/(2a + b)(a + b), d = 1 + 2ac/b$，当 $b = 0$ 时 $c = -1/2a, d = 3/2a$.

若 $a + b = 0, a \neq 0$，则 $(ax - a)(cx + d) = a(2c + d)(x - 1)$，$(ax - a)_{\mathrm{Ideal}} = \{ax - a \mid a \in R\}$. 若 $ex + f \in I$ 并且 $e + f$ 为非零实数，则 $(ex + f) - (ex - e) = e + f \in I, 1 = (e + f)(e + f)^{-1} \in I, I = R$，矛盾，故 $I = \{ax - a \mid a \in R\} = (x - 1)_{\mathrm{Ideal}}$.

若 $2a + b = 0, a \neq 0$，则 $(ax - 2a)(cx + d) = a(c + d)(x - 2)$，同理可证 $I = (x - 2)_{\mathrm{Ideal}}$.

若 I 不含 $a \neq 0$ 的元素 $ax + b$，则易见 I 为真理想迫使 $I = \{0\}$.

故 R 的真理想 I 为 $\{0\}, (x - 1)_{\mathrm{Ideal}}, (x - 2)_{\mathrm{Ideal}}$，后两者是极大理想.

(4) $R=\mathbb{R}[x]/(x^2+x+1)_{\text{Ideal}}$.

解. 易见 x^2+x+1 在 $\mathbb{R}[x]$ 中不可约，此时由**例 3.64** 它是域，只有平凡理想，故极大理想是 $\{0\}$.

3.4.10

(1) 描述环 $R=\mathbb{Z}[i]/(2+i)_{\text{Ideal}}$.

解. 我们可证明 $R\cong\mathbb{Z}/5\mathbb{Z}$.

证明. 令 $\varphi:\mathbb{Z}\to R, n\mapsto\overline{n}$. 由 $\overline{i}=\overline{-2}$，$\varphi$ 为满射，若 $n\in\ker\varphi$，则 $\overline{n}=\overline{0}\Rightarrow(2+i)(x+yi)=n\Rightarrow x=-2y, n=-5y$，即 $n\in5\mathbb{Z}$. 反之，$n\in5\mathbb{Z}\Rightarrow n=5x=(2+i)(2x-xi)$，故 $n\in\ker\varphi$，$\ker\varphi=5\mathbb{Z}, \mathbb{Z}/\ker\varphi=\mathbb{Z}/5\mathbb{Z}$ 与 $\operatorname{im}\varphi=R$ 同构. □

(2) 描述环 $R=\mathbb{Z}[x]/(x^2-3,2x+4)_{\text{Ideal}}$.

解. 我们可证明 $R\cong\mathbb{Z}/2\mathbb{Z}$.

证明. 因 $\overline{2x+4}=\overline{0}$，$\overline{x}\overline{2x+4}=\overline{2x^2+4x}=\overline{6+4x}=\overline{0}, \overline{2}=\overline{22x+4}-\overline{6+4x}=\overline{0}$.

故 $R\cong\mathbb{Z}/2\mathbb{Z}[x]/(x^2-3,2(x+2))_{\text{Ideal}}\cong\mathbb{Z}/2\mathbb{Z}[x]/((x+1)^2)_{\text{Ideal}}$，得 $\overline{x}=\overline{1}, \overline{x+1}=\overline{0}$.

故 $R\cong\mathbb{Z}/2\mathbb{Z}$. □

3.4.11 证明**习题 3.1.6** 中的 $\mathbb{Z}_p$ 为 PID，且仅有唯一的极大理想 $p\mathbb{Z}_p$.

证明. 设 I 是 $\mathbb{Z}_p$ 的理想，则 $I=\{0\}\cup\bigsqcup_i a_i$，其中 a_i 为非零元素.

当 I 不为零理想时，令 k_i 为满足 p^{k_i} 整除 $a_i=(a_{i1},a_{i2},...)$ 各项的最大整数（因为各项中必有至少一项不为 0，因此这是可以做到的），则 $a_i=p^{k_i}b_i$，其中 $b_i\notin p\mathbb{Z}_p$，由**习题 3.1.6(3)** 知存在 $c_i\in\mathbb{Z}_p$ 使得 $b_ic_i=(1,1,1,...)$ 为单位元，即 $(b_i)_{\text{Ideal}}=\mathbb{Z}_p$，故 $(a_i)_{\text{Ideal}}=p^{k_i}\mathbb{Z}_p$ 是 a_i 生成的理想.

故 $I\supseteq\bigsqcup_i p^{k_i}\mathbb{Z}_p=p^{\min_i\{k_i\}}\mathbb{Z}_p$，若 I 还包含其他元素，该元素必定有项不被 $p^{\min_i\{k_i\}}$ 整除，也就是不被所有 p^{k_i} 整除，与 $I=\{0\}\cup\bigsqcup_i a_i$ 矛盾，故 $I=p^k\mathbb{Z}_p$ 为 $(0,0,...,p^k,p^k,...)=(c_1,c_2,...)$ 生成的理想或零理想，其中当 $i\leqslant k$ 时 $c_i=0$，$i>k$ 时 $c_i=p^k$，$k=\min_i\{k_i\}\in\mathbb{N}$，故 I 是主理想.

易见 $k_1<k_2$ 时 $p^{k_1}\mathbb{Z}_p\supsetneq p^{k_2}\mathbb{Z}_p$，且 $k\geqslant1$ 时 $p^k\mathbb{Z}_p$ 为真理想，故唯一的极大理想即 $p\mathbb{Z}_p$. □

3.4.12 设 R 为环，$\mathfrak{m}$ 为 R 的一个理想，假设 R 的每一个不属于 $\mathfrak{m}$ 的元素都是 R 中的单位，证明 $\mathfrak{m}$ 为 R 的唯一极大理想.

证明. 题意并未明确排除 $\mathfrak{m}=R$，但这种情况明显不合题意，以下我们认为 $\mathfrak{m}$ 为真理想，此时 $R/\mathfrak{m}$ 不是零环.

令 $a+\mathfrak{m}\in R/\mathfrak{m}$ 为商环中的非零元, 此时 $a\notin\mathfrak{m}$, 它在 R 中有逆 a^{-1}, 若 $a^{-1}\in\mathfrak{m}$, 则 $1=aa^{-1}\in\mathfrak{m}$, 与 $\mathfrak{m}$ 是真理想矛盾，故 $a+\mathfrak{m}$ 在 $R/\mathfrak{m}$ 中有逆 $a^{-1}+\mathfrak{m}$，$R/\mathfrak{m}$ 是域，$\mathfrak{m}$ 为极大理想.

设 $\mathfrak{n}$ 为 R 的任意一个极大理想，若存在 $a\in R, a\in\mathfrak{n}$ 且 $a\notin\mathfrak{m}$，则 a 可逆，$1=aa^{-1}\in\mathfrak{n}R\subseteq\mathfrak{n}$，迫使 $\mathfrak{n}=R$，与极大理想为真理想矛盾. 故 $\mathfrak{n}\in\mathfrak{m}$，由前者的极大性质，$\mathfrak{n}=\mathfrak{m}$，故 $\mathfrak{m}$ 为唯一的极大理想. □

3.4.13 设 R 为 PID，F 是它的商域，$S \supseteq R$ 是 F 的子环，证明 S 是 PID.

证明. 对 R 上任意元素 a, b，两个元素生成的理想是主理想 $(c)_{\mathrm{Ideal},R}$，我们将这个主理想的生成元 c 记作 $\gcd(a,b)$.

对 S 上任意元素 $\frac{x}{y}$, $\gcd(x,y)$ 在 x,y 生成的 R-理想中，故存在 $m,n \in R$ 使得 $mx+ny=\gcd(x,y)$，这时 $m\frac{x}{y}+n=\frac{\gcd(x,y)}{y} \in RS+R \subseteq S$，并且 $x=x'\gcd(x,y)$，$y=y'\gcd(x,y)$.

易见 $\frac{x}{y}=\frac{x'}{y'}$，记后者为前者的简化形式. 同时 $\frac{\gcd x,y}{y} \in S$ 的简化形式为 $\frac{1}{y'}$. 如果我们把 S 中所有元素皆写为简化形式，得到引理：$\frac{x}{y} \in S \Rightarrow \frac{1}{y} \in S$.

由于 $R \subseteq S$，故反过来也成立，$S=T^{-1}R$，其中 T 为 S 中所有出现在简化形式中的分母的集合，由引理，对任意 $t_1,t_2 \in T, \frac{1}{t_1}, \frac{1}{t_2} \in S$，故 $\frac{1}{t_1t_2} \in S$（显然它也是简化形式），即 T 是乘法集.

考虑 S 上任意理想 $I=\bigsqcup \frac{a_i}{b_i}$，记 J 为所有分子 a_i 生成的理想. 由于 $b_i \in R$，故对任何 a_i 有 $a_i \in R$，即 $J \subseteq I$，又全部分子为 1 的分数 $T^{-1} \in S$，故 $T^{-1}J \subseteq I$，且若 I 有任何其他元素，其分子不能在 J 中，矛盾. 故 J 的生成元 d ($dR=J$) 满足 $dS=dT^{-1}R=T^{-1}dR=T^{-1}J=I$，即任意理想 I 都是主理想. □

3.4.14 设 D 为整环，K 是 D 的商域，集合 $S \subseteq D$ 为乘法集，即满足条件

(i) $0 \notin S, 1 \in S$.

(ii) 对 $\forall x,y \in S, xy \in S$.

定义

$$S^{-1}D=\left\{\frac{m}{n} \mid m \in D, n \in S\right\} \subseteq K$$

试证：

(1) $S^{-1}D$ 是 K 中包含 D 的子环.

证明. 留给读者. □

(2) $S^{-1}D$ 中的素理想必有 $S^{-1}\mathfrak{p}=\left\{\frac{m}{n} \mid m \in \mathfrak{p}, n \in S\right\}$ 的形式，其中 $\mathfrak{p}$ 是 D 的素理想.

证明. 先证 $S^{-1}D$ 的理想 $\mathfrak{q}$ 必有 $S^{-1}A=\left\{\frac{m}{n} \mid m \in A, n \in S\right\}$ ($A \subseteq D$) 的形式.

任取 $\frac{m}{n_1} \in \mathfrak{q}$，对任意 $n_2 \in S$ 有 $\frac{n_1}{n_2} \in S^{-1}D$，得 $\frac{m}{n_2}=\frac{m}{n_1}\cdot\frac{n_1}{n_2} \in \mathfrak{q}$，故令 $A=\left\{m \mid \frac{m}{n} \in \mathfrak{q}\right\}$，对 A 中一切元素应用上述推理即有 $\mathfrak{q} \supseteq S^{-1}A$，前者若包含后者没有的元素，则与它们的定义矛盾，故两者只能一致.

再证 $\mathfrak{q}$ 是素理想时 A 为 D 的素理想. 对任意 $m_1,m_2 \in D$，若 $m_1m_2 \in A$，则 $\frac{m_1m_2}{1} \in \mathfrak{q}$，故由 $\mathfrak{q}$ 为素理想，$\frac{m_1}{1} \in \mathfrak{q}$ 或 $\frac{m_2}{1} \in \mathfrak{q}$，得 $m_1 \in A$ 或 $m_2 \in A$. □

(3a) $\mathrm{Spec}(S^{-1}D)$ 与集合 $\{\mathfrak{p} \in \mathrm{Spec}D \mid p \cap S=\varnothing\}$ 一一对应.

证明. $\forall \mathfrak{q} \in \mathrm{Spec}(S^{-1}D)$，由 (2) 有 $\mathfrak{p}=\{m_1 \mid \frac{m_1}{n_1} \in \mathfrak{q}\} \in \mathrm{Spec}D$，若 $\mathfrak{p} \cap S \neq \varnothing$，取 $n_p \in \mathfrak{p} \cap S$，则 $1=\frac{n_p}{n_p} \in \mathfrak{q}$，与 $\mathfrak{q}$ 是真理想矛盾，故 $\mathfrak{p} \cap S=\varnothing$，并且显然 $\mathfrak{p}$ 由 $\mathfrak{q}$ 唯一确定.

另一方面，给定 $\mathfrak{p} \in \mathrm{Spec}D$ 且 $\mathfrak{p}capS=\varnothing$，请读者自证 $S^{-1}\mathfrak{p}$ 是 $S^{-1}D$ 的理想，且 $\frac{m_1}{n_1}\cdot\frac{m_2}{n_2} \in S^{-1}\mathfrak{p} \Leftrightarrow m_1m_2 \in \mathfrak{p} \Leftrightarrow m_1 \in \mathfrak{p}$ 或 $m_2 \in \mathfrak{p} \Leftrightarrow \frac{m_1}{n_1} \in S^{-1}\mathfrak{p}$ 或 $\frac{m_2}{n_2} \in S^{-1}\mathfrak{p}$，且 $\mathfrak{p}capS=\varnothing \Rightarrow 1=\frac{u}{u} \notin \mathfrak{p}$，$S^{-1}\mathfrak{p}$ 为真理想且满足素理想的条件.

我们只需证明 $\mathfrak{p}$ 唯一确定 $\mathfrak{q}=S^{-1}\mathfrak{p}$ 即可. 因 $\mathfrak{p}$ 是素理想，任何 $\mathfrak{q}$ 中元素 $\frac{m}{n}, m\in\mathfrak{p}$ 中元素若有等价形式 $\frac{m'}{n'}$，则 $mn'=nm'$，左边属于 $\mathfrak{p}$，右边有 $n\notin\mathfrak{p}$，故 $m'\in\mathfrak{p}$，即 $\mathfrak{q}$ 中所有元素的分子的集合与 $\mathfrak{p}$ 完全相等，故不同的 $\mathfrak{p}$ 确定不同的 $\mathfrak{q}$. □

(3b) 举例说明若不要求两者为素理想，$S^{-1}D$ 上的理想可以不与 D 上不与 S 相交的理想一一对应，并说明 (3a) 的证明不再成立的理由.

解. 令 $D=\mathbb{Z}$，$S=\mathbb{Z}-3\mathbb{Z}$，则 D 上的理想 $3\mathbb{Z}$ 与 $6\mathbb{Z}$ 确定同样的 $S^{-1}\mathfrak{p}$. 在上节的证明中，$\mathfrak{p}$ 不为素理想导致 $m'\in\mathfrak{p}$ 不一定成立.

(4) 设 $D=\mathbb{Z},\mathfrak{p}=p\mathbb{Z},S=\mathbb{Z}-\mathfrak{p}$，试证 $\mathbb{Z}/\mathfrak{p}=\mathbb{Z}/p\mathbb{Z}\cong S^{-1}\mathbb{Z}/S^{-1}\mathfrak{p}$.

证明. 对任意 $\frac{m}{n}\in S^{-1}\mathbb{Z}/S^{-1}\mathfrak{p}$，由于 $n\notin\mathfrak{p}$，故 n 在 $\mathbb{Z}/p\mathbb{Z}$ 中可逆，记 $n^{-1}\in\mathbb{Z}-\mathfrak{p}$ 满足 $nn^{-1}\equiv 1 \mod p$，则 $\frac{m}{n}-n^{-1}m=\frac{m-(ps+1)m}{n}, s\in\mathbb{Z}=-\frac{psm}{n}\in S^{-1}\mathfrak{p}$. 故 $\frac{m}{n}$ 和 $n^{-1}m$ 在 $S^{-1}\mathbb{Z}/S^{-1}\mathfrak{p}$ 中总表示同一元素. 定义 $f:S^{-1}\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}, \frac{m}{n}\mapsto n^{-1}m$，则 $n^{-1}m\equiv 0 \mod p\Rightarrow m\equiv 0 \mod p$，故 $\ker f=S^{-1}\mathfrak{p}$，由环同态基本定理即得同构. □

(5) 设 $\mathfrak{p}$ 是 D 的素理想，$S=D-\mathfrak{p}$，问何时 $D/\mathfrak{p}$ 同构于 $S^{-1}D/S^{-1}\mathfrak{p}$.

解. $S/\mathfrak{p}$ 中一切元素在 $D/\mathfrak{p}$ 中有同构. 该条件的充分性请读者类似上小节证明，下证必要性.

若 $\overline{n}$ 在 $D/\mathfrak{p}$ 中不可逆，由于 $n\notin\mathfrak{p}$ 知 $\frac{n}{1}$ 在 $S^{-1}D/S^{-1}\mathfrak{p}$ 中不等于零，$\frac{1}{n}\cdot\frac{n}{1}=\frac{1}{1}$ 得 $\frac{n}{1}$ 在 $S^{-1}D/S^{-1}$ 中可逆，与同构性矛盾.

3.4.15 设 R 为整环，F 为 R 的分式域，$\mathfrak{p}$ 为 R 的素理想，R 在 $\mathfrak{p}$ 处的局部化 $R_{\mathfrak{p}}$ 是指 F 的子环 $(R-\mathfrak{p})^{-1}R=\{\frac{a}{d}\mid a,d\in R,d\notin\mathfrak{p}\}$ 试确定 $R_{\mathfrak{p}}$ 的所有极大理想.

解. 记 $(R-\mathfrak{p})=S$，由**习题 3.4.14(2)**，$R_{\mathfrak{p}}$ 的一切素理想均有形式 $S^{-1}\mathfrak{q}$，其中 $\mathfrak{q}$ 为 R 的素理想. 由于极大理想均是素理想，因此也有此形式.

若 $\exists u\in\mathfrak{q},u\notin\mathfrak{p}$，则 $1=\frac{u}{u}\in S^{-1}\mathfrak{q}$ 与 $S^{-1}\mathfrak{q}$ 为真理想矛盾. 故 $\mathfrak{q}\subseteq\mathfrak{p}$.

若 $\exists a\in\mathfrak{p},a\notin\mathfrak{q}$ 则考虑 $\frac{a}{d}+S^{-1}\mathfrak{q}$ 为 $S^{-1}R/S^{-1}\mathfrak{q}$ 中非零元，由 $S^{-1}\mathfrak{q}$ 为极大理想，$S^{-1}R/S^{-1}\mathfrak{q}$ 是域，故该非零元可逆，存在 $\frac{b}{c}\neq 0\in S^{-1}R/S^{-1}\mathfrak{q}, \frac{e}{f}=0\in S^{-1}R/S^{-1}\mathfrak{q}$，满足 $c,e\notin\mathfrak{p},b\notin\mathfrak{q},f\in\mathfrak{q}$ 使得

$$\frac{a}{d}\cdot\frac{b}{c}=\frac{1}{1}+\frac{f}{e}\text{ 即 }abe=edc+fdc, abe-fdc=edc.$$

由 $a\in\mathfrak{p},f\in\mathfrak{q}\subseteq\mathfrak{p}$ 知 $edc=abe-fdc\in\mathfrak{p}$，由 $\mathfrak{p}$ 为素理想，e 或 d 或 $c\in\mathfrak{p}$，矛盾. 故 $\mathfrak{p}\subseteq\mathfrak{q}$.

故只能 $\mathfrak{q}=\mathfrak{p}$，易验证 $S^{-1}R/S^{-1}\mathfrak{p}$ 是域，故 $S^{-1}R$ 的极大理想只有 $S^{-1}\mathfrak{p}$.

第四章　因子分解

4.1 唯一因子分解环

4.1.1 设 R 为 UFD，a,b,c 为 R 中非零元素. 证明：

(1) $ab\sim \gcd(a,b)\operatorname{lcm}(a,b)$.

证明. 若 a 的因子分解为 $uc_1c_2\cdots c_n$，b 的因子分解为 $vd_1d_2\cdots d_m$，两者中的非单位重复元素（这里的重复是指相伴）为 $c_1,c_2,...,c_l\sim d_1,d_2,...,d_l$（不妨设重新排列后重复的元素居前），则 $\gcd(a,b)\sim c_1c_2\cdots c_l$，$\operatorname{lcm}(a,b)\sim c_1c_2\cdots c_l\cdot c_{l+1}c_{l+2}\cdots c_n\cdot d_{l+1}d_{l+2}\cdots d_m$，$ab\sim c_1c_2\cdots c_l\cdot c_{l+1}c_{l+2}\cdots c_n\cdot d_1d_2\cdots d_l\cdot d_{l+1}d_{l+2}\cdots d_m\sim c_1c_2\cdots c_l\cdot c_{l+1}c_{l+2}\cdots c_n\cdot d_{l+1}d_{l+2}\cdots d_m\cdot c_1c_2\cdots c_l$，故得结论. □

(2) 若 $a\mid bc$，$\gcd(a,b)\sim 1$，则 $a\mid c$.

证明. 由 $\gcd(a,b)\sim 1,\gcd(ac,bc)\sim c$. 又 $\gcd(a,ac)\sim a$，故 $\gcd(a,c)\sim\gcd(a,(ac,bc))\sim\gcd((a,ac),bc)\sim\gcd(a,bc)\sim a$，即 $a\mid c$. □

4.1.2 设 R 为 PID. 证明：

(1) $(a)_{\text{Ideal}}\cap(b)_{\text{Ideal}}=(a)_{\text{Ideal}}(b)_{\text{Ideal}}\Leftrightarrow\gcd(a,b)\sim 1$；

证明. $(a)_{\text{Ideal}}\cap(b)_{\text{Ideal}}=(\operatorname{lcm}(a,b))_{\text{Ideal}}$，$(a)_{\text{Ideal}}(b)_{\text{Ideal}}=(ab)_{\text{Ideal}}$；因此题述左侧成立当且仅当 $\operatorname{lcm}(a,b)\sim ab$，由**习题 4.1.2** 知这等价于 $\gcd(a,b)\sim 1$. □

(2) 方程 $ax+by=c$ 在 R 中有解 (x,y) 的充要条件是 $\gcd(a,b)\mid c$.

证明. 题述左侧成立即理想 $(a,b)_{\text{Ideal}}\supseteq(c)_{\text{Ideal}}$，由于 PID 上所有理想都是主理想，当然有限生成的理想都是主理想，故 PID 都是贝祖环，$(a,b)_{\text{Ideal}}\supseteq(\gcd(a,b))_{\text{Ideal}}$，又易验证 $(a,b)_{\text{Ideal}}\subseteq(\gcd(a,b))_{\text{Ideal}}$，故二理想相等，$(\gcd(a,b))_{\text{Ideal}}\supseteq(c)_{\text{Ideal}}$ 的充要条件是 $\gcd(a,b)\mid c$. □

4.1.3 设 $n\geqslant 3$ 为无平方因子的整数，$R=\mathbb{Z}[\sqrt{-n}]=\{a+b\sqrt{-n}\mid a,b\in\mathbb{Z}\}$.

(1) 证明 2，$\sqrt{-n}$ 和 $1+\sqrt{-n}$ 在 R 上均为不可约元.

证明. 令 $N:R\to\mathbb{N},N(a+b\sqrt{-n})=(a+b\sqrt{-n})(a-b\sqrt{-n})=a^2+nb^2$，则

(i) $N(x)=0\Leftrightarrow x=0,N(1)=1$，

(ii) $N(xy)=N(x)N(y)$.

(iii) $N(x)=1\Leftrightarrow x\in U(R)\Leftrightarrow x=\pm 1$.

$N(2)=4$，若 $2=xy$，其中 x 不是平凡因子，则 x,y 都不是单位，$N(x)=N(y)=2$，但 $a^2+nb^2=2$ 在 $n\geqslant 3$ 时没有整数解，矛盾.

$N(\sqrt{-n})=n$，若 $\sqrt{-n}=xy$，其中 x 不是平凡因子，则 x,y 都不是单位，$1<N(x)\mid n$，此时由于 n 无平方因子，$N(x)$ 也没有平方因子且小于 n，$a^2+nb^2=N(x)$ 仍然没有整数解，矛盾.

$N(1+\sqrt{-n})=n+1$，若 $1+\sqrt{-n}=xy$，其中 x 不是平凡因子，则 x,y 都不是单位，$1<N(x)\mid n+1$，由于 $n+1$ 与 n 互素，故 $N(x)$ 小于 n，即 $x=a+b\sqrt{n},a^2+nb^2<n$，故 $b=0$，$x\in\mathbb{Z}$，同理 $y\in\mathbb{Z}$，故 $1+\sqrt{n}=xy\in\mathbb{Z}$，矛盾.

故三者皆是不可约元. □

(2) 证明 $\sqrt{-n}$ 和 $1+\sqrt{-n}$ 在 R 上不能同时为素元.

证明. 由于 $n \geqslant 3$，故 n 和 $n+1$ 不能同时为素数.

若 n 不是素数，则存在 n 的非平凡因子 a, b. 此时 $\sqrt{-n} \mid n = \sqrt{-n} \cdot -\sqrt{-n} = ab$，由于 $N(a)$，$N(b)$ 为整数的平方，$N(\sqrt{-n}) = n$ 没有平方因子，且 $n^2 = a^2b^2$，若 $n \mid a^2$，则 $1 \neq b^2 \mid n$，矛盾，故 $n \nmid a^2$，由 (1)(ii)，$\sqrt{n}$ 也不整除 a，同理它也不整除 b，$\sqrt{n}$ 不是素元.

若 $n+1$ 不是素数, 则存在 $n+1$ 的非平凡因子 a, b. 此时 $1+\sqrt{n} \mid n+1 = (1+\sqrt{-n})(1-\sqrt{-n}) = ab$，若 $1+\sqrt{n} \mid a$，则 $(1+\sqrt{-n})(c+d\sqrt{-n} = a)$，得 $c-nd = a, c+d = 0, a = (1+n)c$，即 $1+n \mid a$，与 a 是 $n+1$ 的非平凡因子矛盾，同理 $1+\sqrt{n} \nmid b$，即 $1+\sqrt{-n}$ 不是素元. □

4.1.4 设 p 是 $\mathbb{Z}$ 上的奇素数，n 为正整数. 证明 $x^n - p$ 是 $\mathbb{Z}[i]$ 上的不可约多项式.

证明. □

4.1.5 证明 $x^3 + nx + 2$ 对所有 $n \neq 1, -3, -5$ 是 $\mathbb{Z}$ 上的不可约多项式.

证明. 若 $x^3 + nx + 2$ 在 $\mathbb{Z}$ 中可约，则它必有一次因式 $(ax+b)$，由余数定理（**推论 4.24**），它必有有理根 $-\frac{b}{a}$ 其中 $\gcd(a, b) = 1$.

故 $b^3 + nba^2 + 2a^3 = 0$，故 $b \mid b^3 + nba^2 = -2a^3$，$a \mid nba^2 + a^3 = -b^3$，但 a, b 互素，故 $a \mid 1, b \mid 2$，有理根为 $\pm 1, \pm 2$，依次带入得 $n = 1, -3, -5$. □

4.1.6 设 R 是整环，证明多项式环 $R[x]$ 是 PID 当且仅当 R 是域.

证明. ($\Leftarrow$) 即**命题 3.40**.

($\Rightarrow$) 反证法，若 R 不是域，任取其中不可逆元 a，考虑理想 $(a, x)_{\mathrm{Ideal}, R[x]}$，则它不等于 R，若它是主理想，则该理想中有常数迫使它的生成元是常数 b，但 $x \in (b)_{\mathrm{Ideal}, R[x]}$，迫使 b 是 R 中单位，与 (b) 是真理想矛盾，故 $R[x]$ 不是 PID. □

4.1.7 设 R 为整环，$a, b \in R - \{0\}, a \sim b$，求证：

(1) 若 a 为不可约元，则 b 也为不可约元；

证明. b 的非平凡真因子也是 a 的非平凡真因子，故得结论. □

(2) 若 a 为素元，则 b 也为素元.

证明. 任给 c, d，$a \mid cd \Rightarrow a \mid c$ 或 $a \mid d$ 为条件.

若 $b \mid cd$，则 $a \mid cd$，故 $a \mid c$ 或 $a \mid d$，推出 $b \mid c$ 或 $b \mid d$，故得结论. □

4.1.8 设 a 为主理想整环 D 中非零元，求证：若 a 为素元，则 $D/(a)_{\mathrm{Ideal}, D}$ 为域；若 a 不是素元，则 $D/(a)_{\mathrm{Ideal}, D}$ 不是整环.

证明. (i) 若 a 为素元，则对任意 $b \in D$ 有 $\gcd(a, b) \sim a$ 或 $\gcd(a, b) \sim 1$.

若 $\gcd(a, b) \sim a$，则 $b \in (a)_{\mathrm{Ideal}, D}$，$b$ 对应 $D/(a)_{\mathrm{Ideal}, D}$ 中零元素；

若 $\gcd(a,b)\sim 1$，则由 D 是贝祖环，存在 $x,y\in D$ 使得 $ax+by=1$，此时 $b+(a)_{\mathrm{Ideal},D}$ 在 $D/(a)_{\mathrm{Ideal},D}$ 中逆元为 $y+(a)_{\mathrm{Ideal},D}$.

综上，$D/(a)_{\mathrm{Ideal},D}$ 为域.

(ii) 若 a 不是素元，则 a 可写作非平凡真因子的积 $a=bc$，其中 $b,c\notin(a)_{\mathrm{Ideal},D}$，故 $(b+(a)_{\mathrm{Ideal},D})(c+(a)_{\mathrm{Ideal},D})=(a)_{\mathrm{Ideal},D}$，$(b+(a)_{\mathrm{Ideal},D})$ 是 $D/(a)_{\mathrm{Ideal},D}$ 的零因子. □

4.1.9 下列哪些环是 PID? 哪些环是 ED?

(1) $\mathbb{Z}[\sqrt{-2}],\mathbb{Z}[\sqrt{-3}]$.

解. (i)$\mathbb{Z}[\sqrt{-2}]$ 是 ED，从而也是 PID.

证明. 令 $\varphi:\mathbb{Z}[\sqrt{-2}]\to\mathbb{N},a+b\sqrt{-2}\mapsto a^2+2b^2$.

若 $\alpha,\beta\in\mathbb{Z}[\sqrt{-2}]$，则 $\frac{\alpha}{\beta}=x+y\sqrt{-2}\in\mathbb{Q}[\sqrt{-2}]$，在 $\mathbb{Z}$ 中选择 x_0,y_0 使得 $|x-x_0|\leqslant\frac{1}{2},|y-y_0|\leqslant\frac{1}{2}$，则

$\alpha=(x_0+y_0\sqrt{-2})\beta+((x-x_0)+(y-y_0)\sqrt{-2})\beta=q\beta+\gamma$，$\varphi(\gamma)=\varphi(\beta)\varphi(x-x_0+(y-y_0)\sqrt{-2})=\varphi(\beta)((x-x_0)^2+2(y-y_0)^2)\leqslant\frac{3}{4}\varphi(\beta)\leqslant\varphi(\beta)$.

故 $\mathbb{Z}[\sqrt{-2}]$ 是 ED. □

(ii)$\mathbb{Z}[\sqrt{-3}]$ 甚至不是 UFD，从而也不是 PID 或 ED.

证明. $4=2\times 2=(1+\sqrt{-3})(1-\sqrt{-3})$，我们来说明 2，$1\pm\sqrt{-3}$ 均是 $\mathbb{Z}[\sqrt{-3}]$ 中的不可约元.

沿用**习题 4.1.3** 中的记号. $N(2)=N(1\pm\sqrt{-3})=4$，若 $2=xy$ 或 $1\pm\sqrt{-3}=xy$，其中 x 不是平凡因子，则 x,y 都不是单位，$N(x)=N(y)=2$，但 $a^2+3b^2=2$ 没有整数解，矛盾.

由于 $\mathbb{Z}[\sqrt{-3}]$ 中的单位只有 ±1，故三者彼此不相伴，$\mathbb{Z}[\sqrt{-3}]$ 不是 UFD. □

(2) $\mathbb{R}[x,y]$.

解. 该环不是 PID，从而也不是 ED.

证明. 考虑理想 $(x,y)_{\mathrm{Ideal}}$，若它是主理想，则该理想中包含 x 为 y 的零次式，y 为 x 的零次式，故其生成元只能是实常数，但该理想中不含实常数，矛盾. □

(3) $\mathbb{Z}[\omega]$，其中 $\omega=\frac{-1+\sqrt{-3}}{2}$.

解. (i)$\mathbb{Z}[\omega]$ 是 ED，从而也是 PID.

证明. 首先，$\omega^3=1$，$\omega^2=-\omega-1$，故 $\mathbb{Z}[\omega]$ 中元素均有 $a+b\omega$ $(a,b\in\mathbb{Z})$ 的形式.

令 $\varphi:\mathbb{Z}[\omega]\to\mathbb{Z},a-b\omega\mapsto|a^2+ab+b^2|=|(a-b\omega)(a-b\omega^2)|=|(a+b+b\omega)(a-b\omega)|$.

由于 $\mathbb{C}$ 没有零因子，故 $\varphi(a-b\omega)=0\Rightarrow b\omega=0$ 且 $a+b=0$ 或 $a=0\Rightarrow a-b\omega=0$，$\varphi$ 将环中非零元映射到正整数.

若 $\alpha,\beta\in\mathbb{Z}[\omega]$，则 $\frac{\alpha}{\beta}=x-y\omega\in\mathbb{Q}[\omega]$，在 $\mathbb{Z}$ 中选择 x_0,y_0 使得 $|x-x_0|\leqslant\frac{1}{2},|y-y_0|\leqslant\frac{1}{2}$，则

$\alpha=(x_0-y_0\omega)\beta+((x-x_0)-(y-y_0)\omega)\beta=q\beta+\gamma$，$\varphi(\gamma)=\varphi(\beta)\varphi(x-x_0-(y-y_0)\omega)=\varphi(\beta)|(x-x_0)^2+(x-x_0)(y-y_0)+(y-y_0)^2|\leqslant\frac{3}{4}\varphi(\beta)\leqslant\varphi(\beta)$.

故 $\mathbb{Z}[\omega]$ 是 ED. □

4.1.10 设 D 是 PID，E 是整环，并且 D 是 E 的子环，$a,b\in D-\{0\}$，如果 d 是 a 和 b 在 D 中的最大公因子，证明 d 也是 a 和 b 在 E 中的最大公因子.

证明. 显然 d 也是 a 和 b 在 E 中的公因子，只需证明若 f 是 a 和 b 在 E 中的公因子则 $f\mid d$ 即可.

由于 D 是贝祖环，存在 $x,y\in D$ 使得 $ax+by=d$，故 $f\mid ax, f\mid by\Rightarrow f\mid ax+by=d$. □

4.2 高斯整数和二平方和问题

该节不加说明地引用了 Legendre 符号 $\left(\frac{p}{q}\right)$（本书记为 $\left(\frac{p}{q}\right)_{\text{Le}}$），没有学习过的读者请参考《代数学 I：代数学基础》）

4.2.1 设 p 是奇素数，$p\equiv 1 \mod 4$. 如果 (a,b) 是不定方程 $x^2+y^2=p$ 的一组整数解，则它的全部整数解为 $(x,y)=(\pm a,\pm b),(\pm b,\pm a)$

证明. 易验证上面 8 组整数确实是解，根据**定理 4.20**，该方程只有 8 组解，故得结论. □

4.2.2 将 60 和 $81+8\sqrt{-1}$ 在环 $\mathbb{Z}[\sqrt{-1}]$ 中分解为不可约元之积.

解. $60=2*2*3*5$，其中 3 为高斯素数，$2,5$ 为共轭的高斯素数之积，易见 $2=(1+i)(1-i)=-i(1+i)^2$，$5=(1+2i)(1-2i)$ 为在相伴意义下唯一的高斯素数分解，故 $60=-3(1+i)^4(1+2i)(1-2i)$.

我们沿用正文 4.2 节中的记号，$\varphi(81+8\sqrt{-1})=6625=5^3\times 53$，其中 $5=1^2+2^2$ 和 $53=2^2+7^2$ 都是共轭的高斯素数之积. 故 $(81+8\sqrt{-1})(81-8\sqrt{-1})=6625=\epsilon_0(1+2i)^3(1-2i)^3(2+7i)(2-7i)$，由于 $81+8\sqrt{-1}$ 和 $81-8\sqrt{-1}$ 共轭，故前者的非单位高斯素因子只有 4 个，易见 $5\nmid 81+8\sqrt{-1}, 53\nmid 81+8\sqrt{-1}$，故因子分解只能是 $81+8\sqrt{-1}=\epsilon_1(1\pm 2i)^3(2\pm 7i)$ 的形式，其中 $\epsilon_i=1,-1,i,-i$ 为单位. 依次验证可知 $81+8\sqrt{-1}=-i(1-2i)^3(2-7i)$.

4.2.3 试求方程 $x^2+y^2=585$ 的所有整数解.

解. $585=3^2\times 5\times 13$，其中 3 是高斯素数，$5=1^2+2^2$，$13=2^2+3^2$，故 $585=a\overline{a}$ 其中 $a=\epsilon_1\pi_1^{\beta_{11}}\overline{\pi}_1^{\beta_{12}}\pi_2^{\beta_{21}}\overline{\pi}_2^{\beta_{22}}\cdot 3$，$\pi_1\overline{\pi}_1=5,\pi_2\overline{\pi}_2=13,\beta_{11}+\beta 12=\beta 21+\beta 22=1$.

选择 $\pi_1=1+2i,\pi_2=2+3i$，则 $a=\epsilon_1 b\cdot 3$，其中 $b=-4+7i,8+i,-4-7i,8-i$，故方程有 16 组整数解：$(\pm 12,\pm 21),(\pm 21,\pm 12),(\pm 3,\pm 24),(\pm 24,\pm 3)$.

4.2.4 利用正文的方法研究如下问题：

(1) 对于正整数 n，$x^2+2y^2=n$ 何时有整数解？有多少组整数解？

解. 由**习题 4.1.9(1)** 知 $\mathbb{Z}[\sqrt{-2}]$ 是 ED，我们称之为 2-高斯整数环，元素称为 2-高斯整数，其素元称为 2-高斯素数. 定义 $\varphi:\mathbb{Z}[\sqrt{-2}]\to\mathbb{N}, a+b\sqrt{-2}\mapsto a^2+2b^2$，类似正文我们有（请读者自行补充详细）：

2-高斯整数环的单位群 $U(\mathbb{Z}[\sqrt{-2}])=\{\pm 1\}$.

(1) 设 p 为素数，则 p 或为 2-高斯素数或为两个共轭的 2-高斯素数之积.

(2) 设 π_0 为 2-高斯素数，则 $\pi_0\overline{\pi}_0$ 或为素数，或为素数的平方.

(3) 素数 p 为 2-高斯素数当且仅当 $p\equiv 5,7 \mod 8$.

(4) 设 p 为素数，则下列条件等价：

(i) p 为两个共轭的 2-高斯素数之积.

(ii) $p=a^2+2b^2$，$a,b\in\mathbb{Z}$.

(iii) $x^2=-2 \mod p$ 有整数解，即 $\left(\frac{-2}{p}\right)_{\text{Le}}=1$ 或 0.

(iv) $p\equiv 1,3 \mod 8$ 或 $p=2$.

证明. (1)(2) 与正文类似.

(3) 注意奇素数模 8 只能余 $1,3,5,7$. 我们只要证 $p\equiv 5,7 \mod 8$ 则 p 是 2-高斯素数，另一方面的证明由 (4) 即知. 如果 p 不是高斯素数，则

$$p=\pi_0\overline{\pi}_0=\varphi(\pi_0)=a^2+2b^2,\pi_0=a+b\sqrt{-2},$$

则 $p\equiv 0,1,2,3,4,6 \mod 8$，即 $p\not\equiv 5,7 \mod 8$.

(4) (i) $\Leftrightarrow$ (ii) 显然.

(ii) $\Rightarrow$ (iii) 如果 $p=a^2+2b^2$，则 $0<2b^2<p$，故 b 在 $\mathbb{F}_p$ 中可逆，令 $\bar{c}=\overline{b}^{-1}$，则 $(ac)^2+2=a^2c^2+2b^2c^2\equiv 0 \mod p$，即 ac 满足条件.

(iii) $\Leftrightarrow$ (iv) 如果 p 为奇素数，则 $\left(\frac{-2}{p}\right)_{\mathrm{Le}}=\left(\frac{-1}{p}\right)_{\mathrm{Le}}\left(\frac{2}{p}\right)_{\mathrm{Le}}=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$，前者在 $p\equiv 1,5 \mod 8$ 时为 1，$p\equiv 3,7 \mod 8$ 时为 -1，后者在 $p\equiv 1,7 \mod 8$ 时为 1，$p\equiv 3,5 \mod 8$ 时为 -1，两者相乘即得结论. 如果 $p=2$，取 $x=0$ 即可.

(iii) $\Leftarrow$ (i) 由 $p\mid x^2+2=(x+\sqrt{-2})(x-\sqrt{-2})$，但易见 $p\nmid x\pm\sqrt{-2}$，则 p 不是素元，由 (1) 知 p 必是共轭 2-高斯素数之积. □

故设 $n\geqslant 1$ 的（整数-）素因子分解为 $2^\alpha\prod_{i=1}^s p_i^{\beta_i}\prod_{j=1}^t q_j^{\gamma_j}$，其中 $p_i\equiv 1,3 \mod 8, q_j\equiv 5,7 \mod 8$，则 $n=a^2+2b^2$ 有整数解当且仅当 γ_j $(1\leqslant j\leqslant t)$ 全为偶数，此时共有 $2\prod_{i=1}^s(\beta_i+1)$ 对解.（当 $n=1$ 时，α 和 β_i,γ_j 全部为 0，有 2 组解）

证明. 与正文一致，但把 $1\pm i$ 换作 $\pm 2i$，同时注意单位 ϵ 只有 2 种而不是 4 种可能的取值. □

(2) 对于正整数 n，$x^2+xy+y^2=n$ 何时有整数解？有多少组整数解？

解. 由**习题 4.1.9(3)** 知 $\mathbb{Z}[\omega]$ 是 ED，我们称之为 ω-高斯整数环，元素称为 ω-高斯整数，其素元称为 ω-高斯素数. 定义 $\varphi:\mathbb{Z}[\omega]\to\mathbb{N},a-b\omega\mapsto a^2+ab+b^2$，（注意，$a^2+ab+b^2=(a+b/2)^2+3/4\cdot b^2$，故当 a,b 不全为零时 $\varphi(a+b\omega)$ 为正）类似正文我们有（请读者自行补充详细）：

ω-高斯整数环的单位群 $U(\mathbb{Z}[\omega])=\{\pm 1,\pm\omega,1\pm\omega\}$.

(1) 设 p 为素数，则 p 或为 ω-高斯素数或为两个共轭的 ω-高斯素数之积.

(2) 设 π_0 为 ω-高斯素数，则 $\pi_0\overline{\pi}_0$ 或为素数，或为素数的平方.

(3) 素数 p 为 ω-高斯素数当且仅当 $p\equiv 2 \mod 3$.

(4) 设 p 为奇素数，则下列条件等价：

(i) p 为两个共轭的 ω-高斯素数之积.

(ii) $p=a^2+ab+b^2$，$a,b\in\mathbb{Z}$.

(iii) $x^2=-3 \mod p$ 有整数解，即 $\left(\frac{-3}{p}\right)_{\mathrm{Le}}=1$ 或 0.

(iv) $p\equiv 1 \mod 3$ 或 $p=3$.

证明. (1)(2) 与正文类似.

(3) 注意非 3 的素数模 3 只能余 $1,2$. 我们只要证 $p\equiv 2 \mod 3$ 则 p 是 ω-高斯素数，另一方面的证明由 (4) 即知. 如果 p 不是高斯素数，则

$$p=\pi_0\overline{\pi}_0=\varphi(\pi_0)=a^2+ab+b^2,\pi_0=a-b\omega,\overline{\pi}_0=a-b\omega^2$$

当 a^2 或 $b^2 \equiv 0 \mod 3$ 时 $ab \equiv 0 \mod 3$，由于 b^2 或 a^2 模 3 不可能余 2，故 $p = a^2 + b^2 + ab \equiv 0$ 或 $1 \mod 3$.

当 $a^2 \equiv b^2 \equiv 1 \mod 3$ 时 ab 不可能被 3 整除，故故 $p = a^2 + b^2 + ab \equiv 1 + 1 + 1$ 或 $1 + 1 + 2 \bmod 3 \equiv 0$ 或 $1 \mod 3$，综上 $p \not\equiv 2 \mod 3$.

(4) (i) $\Leftrightarrow$ (ii) 显然.

(ii) $\Rightarrow$ (iii) 如果 $p = a^2 + ab + b^2$，则 $0 < 3/4 \cdot b^2 < p$，又 $p \geqslant 2$，故 b 在 $\mathbb{F}_p$ 中可逆，令 $\overline{c} = \overline{b}^{-1}$，则 $(2ac+1)^2 + 3 = 4((ac)^2 + ac + 1) = 4(a^2c^2 + abc^2 + b^2c^2) \equiv 0 \mod p$，即 $2ac + 1$ 满足条件.

(iii) $\Leftrightarrow$ (iv) 如果 p 为奇素数，则 $\left(\frac{-3}{p}\right)_{\mathrm{Le}} = \left(\frac{-1}{p}\right)_{\mathrm{Le}} \left(\frac{3}{p}\right)_{\mathrm{Le}} = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)_{\mathrm{Le}}^{-1} (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} = \left(\frac{p \bmod 3}{3}\right)_{\mathrm{Le}}$，当 $p \equiv 1 \mod 3$ 时为 1，当 $p \equiv 2 \mod 3$ 时为 -1. 如果 $p = 3$，取 $x = 0$ 即可.

(iii) $\Leftarrow$ (i) 由 $p \mid x^2+3 = (x-1)^2+2(x-1)+4 = (x-1-2\omega)(x-1-2\omega^2) = (x-1-2\omega)(x+1+2\omega)$，但易见 $p \nmid x \pm 1 \pm 2\omega$，则 p 不是素元，由 (1) 知 p 必是共轭 ω-高斯素数之积. □

注意到 $p = 2$ 时 $a^2 + ab + b^2$ 无整数解，此时 p 为 ω-高斯素数.

故设 $n \geqslant 1$ 的（整数-）素因子分解为 $3^\alpha \prod_{i=1}^{s} p_i^{\beta_i} \prod_{j=1}^{t} q_j^{\gamma_j}$，其中 $p_i \equiv 1 \mod 3$，$q_j \equiv 2 \mod 3$，则 $n = a^2 + ab + b^2$ 有整数解当且仅当 γ_j $(1 \leqslant j \leqslant t)$ 全为偶数，此时共有 $6 \prod_{i=1}^{s} (\beta_i + 1)$ 对解.（当 $n = 1$ 时，α 和 β_i, γ_j 全部为 0，有 6 组解 $(\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1)$）

证明. 与正文一致，但把 $1 + i$ 换作 $2 + \omega$，$1 - i$ 换作 $2 + \omega^2 = 1 - \omega$，同时注意单位 ϵ 有 6 种而不是 4 种可能的取值. □

4.3 多项式环与高斯引理

4.3.1 证明**命题 4.21**.

证明. 令 $u=\deg f, v=\deg g, f=\sum_{i=0}^{u} a_i x^i, g=\sum_{j=0}^{v} b_j x^j$.

(i) 在 $f+g$ 中次数高于 $\max\{u,v\}$ 的项为 0，故 $\deg f+g \leqslant \max\{u,v\}$.

(ii) 在 fg 中次数高于 $u+v$ 的项为 $\sum_{i=0}^{w} a_i b_{w-i} x^w = \sum_{i=0}^{u} a_i\cdot 0\cdot x^w + \sum_{i=w-v}^{w} 0\cdot b_i x^w + \sum_{i=u+1}^{w-v-1} 0\times 0\cdot x^w = 0\ ((u+v)<w)$，$u+v$ 次项为 $a_u b_v$ 其中 $a_u, b_v \neq 0$，故 $\deg fg \leqslant u+v$ 且当首项系数 a_u 和 b_v 不为零因子时 $a_u b_v \neq 0$，$\deg fg = u+v$. □

4.3.2 设 R 是环，$f(x)=a_0+a_1x+\cdots+a_nx^n \in R[x]$. 证明：

(1) $f(x)$ 可逆当且仅当 $a_0 \in U(R)$ 且 $a_1, a_2, \cdots, a_n \in \mathrm{Nil}(R)$.

证明. ($\Rightarrow$) 若 $f(x)$ 的逆 $g(x)=b_0+b_1x+\cdots+b_mx^m$ 存在，则 $a_0b_0=1_R$，故 $a_0, b_0 \in U(R)$.

由于当 $r \geqslant 1$ 时 $\sum_{i=0}^{r} a_i b_{r-i} = 0$，当 $r=m+n$ 时有 $a_nb_m=0$，当 $r=m+n-1$ 时 $a_{n-1}b_m+a_nb_{m-1}=0$，两边同乘 a_n 得 $a_n^2b_{m-1}=0$，依次类推得 $a_n^jb_{m+1-j}=0$，$a_n^{m+1}b_0=0$，两边同乘 a_0 得 $a_n^{m+1}=0$，故 a_n 是幂零元素，从而 $-a_nx^ng(x)$ 也是，由**习题 3.1.12(3)** 知 $1-a_nx^ng(x)=g(x)(f(x)-a_nx^n)$ 也是单位，由 $f(x)$ 是单位，$f_1(x)=f(x)-a_nx^n=f(x)g(x)(f(x)-a_nx^n)$ 也是单位，从而 f_1 的首项 a_{n-1} 也是幂零元素，依次推理得 $a_1, ..., a_n$ 都是幂零元素.

($\Leftarrow$) 令 $b_0=a_0^{-1}$，则 $b_0f(x)=1+xh(x)$，且 $h(x)$ 的系数 b_0a_i $(1 \leqslant i \leqslant n)$ 都是幂零的，从而 $xh(x)$ 各项 $b_0a_ix^i$ $(1 \leqslant i \leqslant n)$ 在 $R[x]$ 中幂零，由**习题 3.1.12(1)**，$xh(x)$ 也是幂零的，由**习题 3.1.12(3)**，$1+xh(x)$ 是 $R[x]$ 中单位，即可逆. □

证明. ($\Rightarrow$) 另一种证法（只适用于 R 为交换环），可得到更多对于素理想的理解. 该证法由 [6] 给出.

引理. 交换环 R 中所有素理想的交集为 $\mathrm{Nil}(R)$.

引理的证明. 由**习题 3.4.3** 我们已经知道任何素理想包含 $\mathrm{Nil}(R)$，我们只需证明若 $a \notin \mathrm{Nil}(R)$ 则存在素理想 $\mathfrak{p}$ 使得 $a \notin \mathfrak{p}$ 即可.

令 $S=\langle a\rangle$，则 $0 \notin S$，S 是乘法集，我们在 R 上定义局部化 $\frac{r}{s}$ 其中 $(r,s) \sim (r',s')$ 如果 $\exists t \in S$ s.t. $t(r's-s'r)=0$（这里与整环的局部化稍有区别，t 对 $\sim$ 的传传递性是必要的，并且 R 未必同构于 $S^{-1}R$ 的一个子环：若存在 $t \in S$ 使得 $t(a-b)=0$ 则 a, b 在 $S^{-1}R$ 中的像一致），类似**习题 3.4.14(3)** 我们有 $S^{-1}R$ 的素理想与 R 中与 S 不交的素理想一一对应，由 $S^{-1}R$ 中极大理想存在（当然它也是素理想）知 R 中有与 S 不交的素理想，它当然不包含 a. □

考虑 R 的任意素理想 $\mathfrak{p}$，此时 $R/\mathfrak{p}$ 是整环，令 $\varphi: R \to R/\mathfrak{p}$，则 $\varphi(f)$ 的逆是 $\varphi(g)$，由 $\varphi(g)$ 的最高次项不为 $\overline{0}$ 知 $\varphi(f)$ 的非常数项都是 0，即 $a_1, a_2, ..., a_n$ 在 $\mathfrak{p}$ 中，由 $\mathfrak{p}$ 的任意性，$a_1, a_2, ..., a_n$ 是幂零元. □

(2) $f(x)$ 幂零当且仅当 $a_0, a_1, ..., a_n$ 幂零.

证明. ($\Leftarrow$) 设 $r_0, r_1, ..., r_n$ 满足 $a_i^{r_i}=0$. 当 $u > \sum_{i=0}^{n}(r_i-1)$ 时 $f(x)^u$ 展开后所有项的系数都必然有某个 $a_i^{r_i}$ 为因子，故为 0，即 $f(x)^u=0$，$f(x)$ 为幂零元.

($\Rightarrow$) 若 $f(x)^v=0$, 则 $a_n^v x^{nv}=0$, 故 a_nx^n 是 $R[x]$ 中幂零元, 从而 $-a_nx^n$ 也是. 由**习题 3.1.12(1)**, $f_1(x)=f(x)-a_nx^n=a_0+a_1+\cdots+a_{n-1}x^{n-1}$ 也是 $R[x]$ 中幂零元, 对 $f_1(x)$ 同样推理知 $a_{n-1}x^{n-1}$ 幂零.

依次推理下去得 a_ix^i 都是幂零元, 从而 a_i $(0\leqslant i\leqslant n)$ 也都是. □

(3) $f(x)$ 是零因子当且仅当存在 $0\neq a\in R$ 使得 $af(x)=0$.

证明由文献 [8] 给出.

证明. 题设条件似乎假定 R 是交换环, 否则还应有条件 $f(x)a=0$.

令 $g(x)$ 为零化 $f(x)$ 的多项式中次数最小的, 即 $g(x)f(x)=0$ 且当 $0\leqslant \deg h<\deg g$ 时 $h(x)f(x)\neq 0$.

令 $f(x)=\sum_{i=0}^n a_ix^i$, $g(x)=\sum_{i=0}^m b_ix^i$, 则 $a_nb_m=0$, 故 $a_ng(x)$ 为次数小于 m 的多项式且 $a_ng(x)f(x)=0$, 只能 $\deg a_ng(x)=-\infty, a_ng(x)=0$, 故 $f_1(x)=\sum_{i=0}^{n-1}a_ix_i=f(x)-a_nx^n$ 满足 $g(x)f_1(x)=g(x)f(x)-g(x)a_nx^n=0$, 依次类推有 $a_ig(x)=0$ $(0\leqslant i\leqslant n)$, 故 $a_ib_m=0$ $(0\leqslant i\leqslant n)$, 即 $f(x)b_m=0$. □

4.3.3 设 D 为 UFD, F 为 D 的商域, $f(x)$ 为 $D[x]$ 中首一多项式. 证明: $f(x)$ 在 $F[x]$ 中的每个首一多项式因子必属于 $D[x]$.

证明. $f(x)$ 可在 $D[x]$ 上分解为不可约元之积, 由**引理 4.31**, 该分解式也是 $f(x)$ 在 $F[x]$ 上的一个分解式 $\prod_i g_i(x)$, 由 $f(x)$ 首一, 该分解式可调整为使各 $g_i(x)$ 也是首一多项式. 由因式分解的唯一性, 该分解式与 $f(x)$ 在 $F[x]$ 上的任何另外一个分解式 $\prod_i h_i(x)$ (重新排列后) 各因子只相差一个常数因子 a_i, 若对某个 i 有 $h_i(x)$ 首一, 则 $a_i=1$, $h_i(x)=g_i(x)\in D[x]$. □

4.3.4 将 x^n-1 $(3\leqslant n\leqslant 10)$ 在 $\mathbb{Z}[x]$ 中作素因子分解.

警告: 读者必须证明所得的结果全部是 $\mathbb{Z}[x]$ 中不可约多项式, 才算完成此题.

解. 一次多项式都是不可约的. 由**例 4.34**, $3,5,7$ 次分圆多项式 $f_3(x)=x^2+x+1, f(5)x=x^4+x^3+x^2+x^1+1, f_7(x)=x^6+x^5+x^4+x^3+x^2+x^1+1$ 在 $\mathbb{Z}[x]$ 上不可约.

$x^3-1=(x-1)(x^2+x+1)$.

$x^4-1=(x-1)(x+1)(x^2+1)$, 最后一项没有实根, 故没有一次实因式, 故在 $\mathbb{R}[x]$ 中不可约, 从而在 $\mathbb{Z}[x]$ 中也不可约.

$x^5-1=(x-1)(x^4+x^3+x^2+x+1)$.

$x^6-1=(x^3-1)(x^3+1)=(x+1)(x-1)(x^2+x+1)(x^2-x+1)$, 最后一项为 $f_3(-x)$, 故也在 $\mathbb{Z}[x]$ 中不可约.

$x^7-1=(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$.

$x^8-1=(x+1)(x-1)(x^2+1)(x^4+1)$, 在最后一项 x^4+1 中以 $x+1$ 代替 x 得 $x^4+4x^3+6x^2+4x+2$, 取 $p=2$ 满足艾森斯坦判别法的条件, 故 x^4+1 也在 $\mathbb{Z}[x]$ 中不可约.

$x^9-1=(x-1)(x^2+x+1)(x^6+x^3+1)$, 在最后一项 x^6+x^3+1 中以 $x+1$ 代替 x 得 $x^6+6x^5+15x^4+21x^3+18x^2+9x+3$, 取 $p=3$ 满足艾森斯坦判别法的条件, 故 x^6+x^3+1 也在 $\mathbb{Z}[x]$ 中不可约.

$x^{10}-1=(x+1)(x-1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)$，最后一项为 $f_5(-x)$，故也在 $\mathbb{Z}[x]$ 中不可约.

4.3.5 设 F 为域，$d:F[x]\to F[x]$ 为线性映射，若对于任意的 $f,g\in F[x], d(fg)=(df)g+f(dg)$，则称 d 为 $F[x]$ 上的一个**线性导子**. 请找出 $f[x]$ 上所有线性导子.

解. $d(1\cdot g)=(d1)g+1\cdot d(g)$，故 $(d1)g=0$ 对一切 $g\in F[x]$ 成立，故 $(d1)=0$，由 d 是线性映射，$d(F)=0$.

$d\left(\sum_i a_ix^i\right)=\sum_i d(a_ix^i)=\sum_i(d(a_i)x^i+a_id(x^i))=\sum_i(0\cdot x^i+a_i(\sum_{j=1}^i x^{j-1}d(x)x^{i-j}))=\sum_i\sum_{j=1}^i a_ix^{i-1}d(x)=\sum_i ia_ix^{i-1}d(x)$

故 $d(f)=f'd(x)$ 是形式微商的 $d(x)$ 倍，其中 $d(x)\in F[x]$.

4.3.6 设 $f(x)$ 是 $\mathbb{Q}[x]$ 中奇次不可约多项式，α 和 β 是 $f(x)$ 在 $\mathbb{Q}$ 的某个扩域中两个不同的根，求证 $\alpha+\beta\notin\mathbb{Q}$.

证明由文献 [12] 给出.

证明. 由于 $\mathbb{Q}$ 的代数闭包存在（见**例 5.21**），因此 $f(x)$ 在代数闭包 $\overline{\mathbb{Q}}$ 或者它的任何扩域中有奇数个不同的根.

对 $f(x)$ 的任意一个根 u，由 $f(x)$ 不可约且不是一次多项式 $((x-\alpha)(x-\beta)\mid f(x)$，有 $u\notin\mathbb{Q}$，定义同态 $\varphi_u:\mathbb{Q}[x]\to\overline{\mathbb{Q}}, f(x)\mapsto f(u)$，则 $(f(x))_{\mathrm{Ideal},\mathbb{Q}[x]}\subseteq\ker\varphi_u$，由 $\mathbb{Q}$ 是域，$\mathbb{Q}[x]$ 是 PID，故也是贝祖环，当 $g(x)\notin(f(x))_{\mathrm{Ideal},\mathbb{Q}[x]}$ 时因 $f(x)$ 不可约，$\gcd(f(x),g(x))=1, af(x)+bg(x)=1\ (a,b\in\mathbb{Q}[x]), bg(u)=af(u)+bg(u)=\varphi_u(1)=1$，故 u 不是 $g(x)$ 的根，$\ker\varphi_u\subseteq(f(x))_{\mathrm{Ideal},\mathbb{Q}[x]}$，故 $\ker\varphi_u=(f(x))_{\mathrm{Ideal},\mathbb{Q}[x]}$，$\mathbb{Q}[x]/f(x)=\mathbb{Q}[x]/\ker\varphi_u\cong\operatorname{im}\varphi_u=\mathbb{Q}[u]$.

由 u 的任意性，对 $f(x)$ 的任意一个根 γ，$\varphi_{\gamma\alpha^{-1}}=\varphi_\gamma\circ\varphi_\alpha^{-1}$ 诱导 $\mathbb{Q}[\alpha]$ 通过 $\mathbb{Q}[x]/f(x)$ 到 $\mathbb{Q}[\gamma]$ 的同构 $f(\alpha)\mapsto f(\gamma)$，该同构在 $\mathbb{Q}$ 上的限制为恒等映射，令 $r=\alpha+\beta$.

若 $r\in\mathbb{Q}$，则 $\beta\in\mathbb{Q}[\alpha], \varphi_{\gamma\alpha^{-1}}(\beta)=\varphi_{\gamma\alpha^{-1}}(r-\alpha)=r-\gamma$，且 $f(r-\gamma)=\varphi_{\gamma\alpha^{-1}}(f(\beta))=\varphi_{\gamma\alpha^{-1}}(0)=0$，故对任意一个根 γ 总有另一个根 $\varphi_{\gamma\alpha^{-1}}(\beta)$ 与它的和是 r，由于 $\alpha\neq\beta$，易见这两个根 γ 和 $\varphi_{\gamma\alpha^{-1}}(\beta)$ 不同.

故 $f(x)$ 在 $\overline{\mathbb{Q}}$ 中的根成对出现，与根为奇数个矛盾，故 $r\notin\mathbb{Q}$. □

4.3.7 设 R 是含幺环，定义集合

$$R[[x]]=\left\{\sum_{n=0}^{+\infty}a_nx^n\mid a_n\in R\ (n=0,1,2,...)\right\},$$

每个元素 $\sum_{n=0}^{+\infty}a_nx^n$ 叫做 R 上的**形式幂级数**. 定义

$$\sum a_nx^n+\sum b_nx^n=\sum(a_n+b_n)x^n,$$

$$\left(\sum a_nx^n\right)\left(\sum b_nx^n\right)=\sum\left(\sum_{i+j=n}a_ib_j\right)x^n.$$

(1) $R[[x]]$ 对于上述加法和乘法形成含幺环，叫做环 R 上关于 x 的**形式幂级数环**.

证明. 留给读者. □

(2) 若 R 为交换环，则 $R[[x]]$ 也是交换环.

证明. 留给读者. □

(3) 多项式环 $R[x]$ 可自然看成是 $R[[x]]$ 的子环.

证明. 易见 $R[[x]]$ 中的只有有限个 a_n 不为 0_R 的元素与 $R[x]$ 中的元素一一对应，并且保持加法和乘法. □

(4) 设 R 是含幺交换环，$f(x)=\sum_{i=0}^{\infty}a_ix^i\in R[[x]]$，则 $f(x)$ 可逆当且仅当 $a_0\in R^\times$.

证明. ($\Leftarrow$) 当 a_0 在 R 中可逆时我们构造 $f(x)$ 的逆 $g(x)=\sum_{i=0}^{\infty}b_ix^i$:

$b_0=a_0^{-1}\in R$.

假设我们对一切 $i<s\in\mathbb{Z}_+$ 得到了 $b_i\in R$, 由 $\sum_{j=1}^{s}a_jb_{s-j}+a_0b_s=0$ 得到 $b_s=-a_0^{-1}\sum_{j=1}^{s}a_jb_{s-j}$.

对一切 $s\in\mathbb{N}$ 计算 b_s，则 $f(x)g(x)$ 满足对一切 $s\in\mathbb{Z}_+,\sum_{j=1}^{s}a_jb_{s-j}+a_0b_s=0,a_0b_0=1$，故 $f(x)g(x)=1$ 是 $R[[x]]$ 中的单位元.

($\Rightarrow$) 若 a_0 在 R 中不可逆，则 $1\notin a_0R$，但 $f(x)g(x)$ 的常数项一定在 a_0R 中，故 $f(x)g(x)\neq 1$，$f(x)$ 在 $R[[x]]$ 中不可逆. □

(5) 若 R 为域，则 $R[[x]]$ 是 PID 且只有唯一的极大理想 $\mathfrak{m}$，求出 $R[[x]]$ 的所有理想.

证明. 设 I 是 $R[[x]]$ 的理想，则 $I=\{0\}\cup\bigsqcup_i f_i(x)$，其中 $f_i(x)$ 为非零元素.

当 I 不为零理想时，令 k_i 为 f_i 的次数 (因为 $f\neq 0$，因此 $k_i>-\infty$ 为整数)，则 $f_i(x)=x^{k_i}g_i(x)$，其中 $g_i\notin xR[[x]]$, g_i 的常数项不为 0, 由于 R 是域, 因此 g_i 的常数项可逆, 由 (4) 知存在 $h_i(x)\in R[[x]]$ 使得 $g_ih_i=1$ 为单位元，即 $(g_i)_{\mathrm{Ideal},R[[x]]}=R[[x]]$，故 $(f_i)_{\mathrm{Ideal},R[[x]]}=x^{k_i}R[[x]]$ 是 f_i 生成的理想.

故 $I\supseteq\bigsqcup_i x^{k_i}R[[x]]=x^{\min_i\{k_i\}}R[[x]]$，若 I 还包含其他元素，该元素必定有项不被 $x^{\min_i\{k_i\}}$ 整除，也就是不被所有 x^{k_i} 整除，与 $I=\{0\}\cup\bigsqcup_i f_i$ 矛盾，故 $I=x^kR[[x]]$ 为 x^k 生成的理想，其中 $k=\min_i\{k_i\}\in\mathbb{N}$，故 I 是主理想，$R[[x]]$ 的所有理想为 $x^kR[[x]]$ 或 $\{0\}$.

易见 $k_1<k_2$ 时 $x^{k_1}R[[x]]\supsetneqq x^{k_2}R[[x]]$，且 $k\geqslant 1$ 时 $x^kR[[x]]$ 为真理想，故唯一的极大理想即 $\mathfrak{m}=xR[[x]]$. □

(6) 本题与**习题 3.1.6, 3.4.11** 有什么联系?

证明. $\varphi:\mathbb{Z}_p\to\mathbb{Z}[[x]]/(x-p),(a_1,a_2,...)\mapsto\sum_{i=0}^{+\infty}\frac{a_{i+1}-a_i}{p^i}x^i(a_0=0)$, 由于 $a_{i+1}\equiv a_i \mod p^i, a_{i+1}-a_i<p^{i+1}$，故 φ 是良好定义的，请读者自行证明 φ 是同构. □

4.3.8 试确定 $\mathbb{R}[x]$ 和 $\mathbb{Z}[x]$ 的所有素理想和极大理想.

解. (i) 由于 $\mathbb{R}[x]$ 是整环，因此零理想是素理想. 由于 $\mathbb{R}$ 是域，因此 $\mathbb{R}[x]$ 是 PID.

考虑理想 $I=(f(x))_{\mathrm{Ideal},\mathbb{R}[x]}$，其中 $f(x)\neq 0$. 若 $f(x)$ 在 $\mathbb{R}[x]$ 中可约，则它的两个非平凡因子都不在 I 中，乘积却在 I 中，因此 I 不是素理想. 反之，若 $f(x)$ 在 $\mathbb{R}[x]$ 中不可约，则 $ab\in I\Rightarrow\exists u,v$

s.t. $u \mid a, v \mid b, uv = f(x)$，只能 $u \sim f(x), v \sim 1$ 或 $u \sim 1, v \sim f(x)$，故 a 或 b 在 I 中，I 是素理想. 故 I 中素理想为零理想和 $\mathbb{R}[x]$ 中不可约多项式生成的理想.

由代数基本定理，$\mathbb{R}[x]$ 中多项式 f 也是 $\mathbb{C}[x]$ 中多项式且有 $\deg f$ 个根，即它在 $\mathbb{C}[x]$ 中分解为一次因式. 由于复共轭是 $\mathbb{C}[x]$ 的自同构且保持 $\mathbb{R}[x]$ 不变，因此 $a+bi$ 是 f 的根 $(a, b \in \mathbb{R}) \Leftrightarrow a-bi$ 是 f 的根，故当 $b \neq 0$ 时 $(x-a-bi)(x-a+bi) = x^2 - 2ax + a^2 + b^2$ 是 f 的因式，它属于 $\mathbb{R}[x]$，且它的判别式 $4a^2 - 4a^2 - 4b^2 = -4b^2 < 0$，故它没有实数根，在 $\mathbb{R}[x]$ 中不可约. 综上，$\mathbb{R}[x]$ 中不可约多项式为一次因式或判别式小于 0 的二次因式.

故 $\mathbb{R}[x]$ 的所有素理想为 $\{0\}, (x-a)_{\mathrm{Ideal}}\ (a \in \mathbb{R}), (x^2+bx+c)_{\mathrm{Ideal}}\ (b, c \in \mathbb{R}, b^2 - 4c < 0)$.

除零理想外，令 I 是不可约多项式 $f(x)$ 生成的理想，若 $J \supsetneqq I$ 是理想，则它也是多项式生成的理想 $(g(x))_{\mathrm{Ideal}}$，故 $g(x) \mid f(x), g(x) \nsim f(x)$，由 $f(x)$ 不可约，只能 $g(x) \sim 1$，即 $J = \mathbb{R}[x]$，故不可约多项式生成的理想 $(x-a)_{\mathrm{Ideal}}\ (a \in \mathbb{R}), (x^2+bx+c)_{\mathrm{Ideal}}\ (b, c \in \mathbb{R}, b^2 - 4c < 0)$ 都是 $\mathbb{R}[x]$ 的极大理想.

(ii) 该部分证明由文献 [17] 给出.

若 $\mathfrak{p}$ 是 $\mathbb{Z}[x]$ 的素理想，考虑 $\mathfrak{p} \cap \mathbb{Z}$，若 $a, b \in \mathbb{Z}, ab \in \mathfrak{p} \cap \mathbb{Z}$，则 a 或 $b \in \mathfrak{p}$，即 a 或 $b \in \mathfrak{p} \cap \mathbb{Z}$，故 $\mathfrak{p} \cap \mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想，这只能有两种情况：

(iia) $\mathfrak{p} \cap \mathbb{Z} = (0)$. 我们可能有 $\mathfrak{p} = (0)$，若不然，则令 $S = \mathfrak{Z} - \{0\}$，S 是 $\mathbb{Z} - \{0\}$ 上乘法含幺半群，故有整环 $S^{-1}\mathbb{Z}[x] = \mathbb{Q}[x]$，由**习题 3.4.14(3)**，$S^{-1}\mathfrak{p}$ 是 $\mathbb{Q}[x]$ 的素理想，而 $\mathbb{Q}[x]$ 是 PID，故 $S^{-1}\mathfrak{p} = (q(x))_{\mathrm{Ideal},\mathbb{Q}[x]}$，其中 $q(x)$ 是 $\mathbb{Q}[x]$ 中不可约多项式. 若 $q(x)$ 的容积不为 1 而为 $c(q)$，则用 $c(q)^{-1}q(x)$ 替代 $q(x)$，理想不变，故可假定 $q(x)$ 的容积为 1.

由于 $S^{-1}\mathfrak{p} \cap \mathbb{Z}[x] = \mathfrak{p}$（否则设 $a \in S^{-1}\mathfrak{p}, a \notin \mathfrak{p}$，则对任意 $s \in S$，$s \in \mathbb{Z}$，若 $sa \in \mathfrak{p}$ 则由素理想的性质，$s \in \mathfrak{p}$（与 (iia) 条件矛盾）或 $a \in \mathfrak{p}$（仍然矛盾），故 $sa \notin \mathfrak{p}, a = s^{-1}sa \notin s^{-1}\mathfrak{p}$ 对所有 $s \in S$ 成立，与 $a \in S^{-1}\mathfrak{p}$ 矛盾），由 $q(x)$ 容积为 1，$(q(x))_{\mathrm{Ideal},\mathbb{Z}[x]} \subseteq \mathfrak{p}$. 若 $f(x) = \frac{r}{s}q(x) \in \mathbb{Z}[x]$，则 $f(x)$ 的容积为 $\frac{r}{s}$ 为整数，故 $\frac{r}{s}$ 为整数，$f(x) \in \mathfrak{p}$，故 $(q(x))_{\mathrm{Ideal},\mathbb{Z}[x]} = \mathfrak{p}$ 为 $\mathbb{Q}[x]$ 上整系数不可约本原多项式生成的理想，即 $\mathbb{Z}[x]$ 上一次以上不可约多项式生成的理想.

(iib) $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$，令 $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]/p\mathbb{Z} \cong \mathbb{F}_p[x]$，则 φ 是满同态，由**习题 3.4.5(1)**，$\varphi(\mathfrak{p})$ 是 $\mathbb{F}_p[x]$ 的素理想.

由于 $\mathbb{F}_p$ 是域，$\mathbb{F}_p(x)$ 为 PID，其素理想为 $(q(x))_{\mathrm{Ideal},\mathbb{F}_p(x)}$ 其中 $q(x)$ 为 $\mathbb{F}_p[x]$ 上不可约多项式或零理想，对于后一种情况我们有 $\mathfrak{p} = p\mathbb{Z}[x]$.

对于前一种情况，由于 $\mathbb{F}_p$ 是域，若 $q(x)$ 的首项系数不为 1 而为 $a_n(q)$，则用 $p(x) = a_n(q)^{-1}q(x)$ 替代 $q(x)$，则 $(p(x))_{\mathrm{Ideal},\mathbb{F}_p(x)} = (q(x))_{\mathrm{Ideal},\mathbb{F}_p(x)}$，若 $p(x)$ 在 $\mathbb{Z}[x]$ 中可约，则它在 $\mathbb{F}_p[x]$ 中也可约，矛盾，故 $p(x)$ 是 $\mathbb{Z}[x]$ 中不可约多项式.

显然 $(p, p(x))_{\mathrm{Ideal},\mathbb{Z}[x]} \subseteq \mathfrak{p}$，反之，若 $r(x) \in \mathfrak{p}$，则 $\varphi(r(x)) \in (p(x))_{\mathrm{Ideal},\mathbb{F}_p[x]}$，存在 $\mathbb{F}_p[x]$ 中多项式 $s(x)$ 使得 $s(x)p(x) \equiv r(x)$，故 $s(x)p(x) - r(x) \in p\mathbb{Z}[x]$，$r(x) = s(x)p(x) + pu(x)$ 其中 $u(x) \in \mathbb{Z}[x]$，故 $r(x) \in (p, p(x))_{\mathrm{Ideal},\mathbb{Z}[x]}$，故 $\mathfrak{p} = (p, p(x))_{\mathrm{Ideal},\mathbb{Z}[x]}$.

综上，$\mathbb{Z}[x]$ 中的一切素理想如下：

(A) $\{0\}$；

(B) $(f(x))_{\mathrm{Ideal}}$，其中 $f(x)$ 是 $\mathbb{Z}[x]$ 内一次以上不可约多项式；

(C) $p\mathbb{Z}[x]$；

(D) $(p, f(x))_{\mathrm{Ideal}}$，其中 $f(x)$ 是 $\mathbb{F}_p[x]$ 内不可约多项式.

其中 (A) (C) 当然不是极大理想，对 (B)，若对一切素数 p 有 $f(x)$ 在 $\mathbb{F}_p[x]=\mathbb{Z}[x]/p\mathbb{Z}[x]$ 中可约，则由中国剩余定理，$f(x)$ 在 $\mathbb{Z}[x]\cong\mathbb{Z}[x]/\bigcap_{p_i\text{为一切素数}}p_i\mathbb{Z}[x]\cong\prod_{p_i\text{为一切素数}}\mathbb{F}_{p_i}[x]$ 中可约，矛盾，故存在 p 使得 $f(x)$ 在 $\mathbb{F}_p[x]$ 内也是不可约多项式，存在 (D) 中的某个素理想包含 $(f(x))_{\text{Ideal}}$.

对 (D)，若 $p_1\neq p_2$，则 $(p_1,f(x))_{\text{Ideal}},(p_2,g(x))_{\text{Ideal}}$ 仅考虑与 $\mathbb{Z}$ 的交集就互不包含，故只需讨论 p 固定的情况.

若 $(p,f(x))_{\text{Ideal},\mathbb{Z}[x]}\supsetneq(p,g(x))_{\text{Ideal},\mathbb{Z}[x]}$，则 $g(x)\equiv f(x)r(x)\mod p$，即在 $\mathbb{F}_p(x)$ 中 $f(x)\mid g(x),g(x)\nmid f(x)$，迫使 $f(x)\sim 1$，与 $f(x)$ 不可约矛盾.

综上，$\mathbb{Z}[x]$ 的极大理想即上述情况 (D).

4.3.9 试确定 $\mathbb{Z}[x]$，$\mathbb{Q}[x]$ 的自同构群.

解. (i) 令 $\varphi\in\mathrm{Aut}(\mathbb{Z}[x])$，则 φ 在 $\mathbb{Z}$ 上的限制为恒等映射. 令 $\varphi(x)=f(x)$，由同构是双射，$f(x)\notin\mathbb{Z}$. 由**习题 4.3.8** 知对任意素数 p，$(p,x)_{\text{Ideal},\mathbb{Z}[x]}$ 都是极大理想，故 $f(x)$ 也需满足 $(p,f(x))_{\text{Ideal},\mathbb{Z}[x]}$ 也是极大理想，即 $f(x)$ 对任意素数 p 都是 $\mathbb{F}_p$ 中不可约多项式.

若 $f(x)$ 的次数 $\geqslant 2$，令 $f(x)=a_nx^n+\cdots+a_1x+a_0$，$c$ 为任意整数，则 $f(x)=f(c)+(x-c)g(x)$，若有素数 p 整除 $f(c)$，则 $(x-c)$ 是 $\mathbb{F}_p(x)$ 中 $f(x)$ 的因式，矛盾. 故 $f(c)=1$ 对任何 c 成立，得 $f(x)=1$，矛盾.

故 $\varphi(x)=ax+b$，其中 $a,b\in\mathbb{Z},a\neq 0$，若 $a\neq\pm1$，则 $\varphi^{-1}(x)=a^{-1}(x-b)\notin\mathbb{Z}[x]$，矛盾，故 $a=\pm1$，$\mathrm{Aut}(\mathbb{Z}[x])\cong D_\infty=\langle\sigma,\tau\mid\tau\sigma\tau^{-1}=\sigma^{-1},\tau^2=\mathrm{id}\rangle=\mathbb{Z}\rtimes(\mathbb{Z}/2\mathbb{Z})$.

(ii) $\mathbb{Q}$ 是域，类似**习题 4.3.8** 的讨论知 $\mathbb{Q}[x]$ 上的极大理想是不可约多项式生成的理想，即 $\mathbb{Q}[x]$ 的自同构 φ 应把不可约多项式映射到不可约多项式，特别地，$\varphi(x)=f(x)$ 为不可约多项式.

故 φ 诱导同构 $\tau:\mathbb{Q}\cong\mathbb{Q}[x]/(x)_{\text{Ideal}}\leftrightarrow\mathbb{Q}[x]/f(x)_{\text{Ideal}}\cong\mathbb{Q}(\alpha)$，其中 α 是 $f(x)$ 的一个根. 若 $\deg f\geqslant 2$，则 $f(x)$ 不可约导致它没有有理根，必有 $\alpha\notin\mathbb{Q}$，但域的同构 τ 必将 $\mathbb{Q}$ 映射到它本身，而 $\mathbb{Q}(\alpha)$ 包含无理数，即 τ 必不是满射，矛盾.

故 $\varphi(x)=ax+b,a,b\in\mathbb{Q},a\neq 0$，$\mathrm{Aut}(\mathbb{Q}[x])$ 同构于 $\mathbb{Q}$ 上 2 阶一般线性群 $\mathrm{GL}_2(\mathbb{Q})$ 的子群

$$\left\{\begin{pmatrix}k&l\\0&1\end{pmatrix}\mid l\in\mathbb{Q},k\in\mathbb{Q}^\times\right\}.$$

.

4.3.10 设 $c_0,c_1,\cdots,c_n$ 是整环 D 中两两相异的 $n+1$ 个元素，$d_0,d_1,\cdots,d_n$ 是 D 中任意 $n+1$ 个元素，证明：

(1) 在 $D[x]$ 中至多存在一个次数 $\leqslant n$ 的多项式 $f(x)$ 使得 $f(c_i)=d_i(\forall 0\leqslant i\leqslant n)$；

证明. 若存在次数 $\leqslant n$ 的两个不同多项式 f,g 满足要求，则非零多项式 $h(x)=f(x)-g(x)$ 满足 $h(c_i)=0$ 对所有 $0\leqslant i\leqslant n$ 成立，即 h 有全部 c_i 即 $n+1$ 个不同根，而 $\deg h\leqslant n$，与**推论 4.25** 矛盾. □

(2) 若 D 是域，则 (1) 中所述多项式存在.

证明. 令 $g_i(x)=\prod_{\substack{j=0\\j\neq i}}^{n}(x-c_j)$，则对 $j\neq i$ 有 $g_i(c_j)=0$，且由 c_i 彼此相异，$g_i(c_i)\neq 0$，记它为 a_i.

令 $h_i(x)=d_i/a_i\cdot g_i(x)$，则 $h(x)=\sum_{i=0}^n h_i(x)$ 满足条件. □

4.3.11 判断下列元素是否为 $\mathbb{Z}[x],\mathbb{Q}[x],\mathbb{R}[x],\mathbb{C}[x],\mathbb{Z}[[x]]$ 中的可逆元? 是否为不可约元?

(1) $2x+2$; (2) x^2+1; (3) $x+1$; (4) x^2+3x+2.

解. 对于前四个环，n 次多项式生成的理想中元素（除 0 外）次数都 $\geqslant n$，故一次以上多项式总是不可逆的，在 $\mathbb{Z}[[x]]$ 中则不然，由**习题 4.3.7(4)** 知当且仅当常数项在 $\mathbb{Z}$ 中可逆（即为 ±1 时 $f(x)$ 总是单位.

故在前四个环中，四个多项式都不可逆，而在 $\mathbb{Z}[[x]]$ 中 (2)(3) 可逆.

$2x+2=2(x+1)$，它在 $\mathbb{Z}[x]$ 中不是不可约元，而在 $\mathbb{Q}[x],\mathbb{R}[x],\mathbb{C}[x]$ 中由于 2 是单位，它是不可约元，而在 $\mathbb{Z}[[x]]$ 中，$x+1$ 是单位，2 却不是，故也是不可约元.

x^2+1 没有实根，故在 $\mathbb{Z}[x],\mathbb{Q}[x],\mathbb{R}[x]$ 中都是不可约元，而在 $\mathbb{C}[x]$ 中它等于 $(x+i)(x-i)$，不是不可约元，在 $\mathbb{Z}[[x]]$ 中它是单位，故不是不可约元.

$x+1$ 为本原一次多项式，在前四个环中都是不可约元，在 $\mathbb{Z}[[x]]$ 中它是单位，故不是不可约元.

$x^2+3x+2=(x+1)(x+2)$，在前四个环中都不是不可约元，在 $\mathbb{Z}[[x]]$ 中 $(x+1)$ 是单位而 $(x+2)$ 不是，故是不可约元.

4.3.12 设 $f=\sum a_ix^i\in\mathbb{Z}[x]$ 为首 1 多项式，p 为素数，以 $\overline{a}$ 表示 $a\in\mathbb{Z}$ 在环的自然同态 $\mathbb{Z}\to\mathbb{F}_p$ 中的像，而令 $\overline{f}(x)=\sum\overline{a_i}x^i\in\mathbb{F}_p[x]$,

(1) 求证：若对某个素数 p，$\overline{f}(x)$ 在 $\mathbb{F}_p[x]$ 中不可约，则 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约.

证明. 若 $f(x)$ 可约，则它是至少 2 个非单位因子的积，并且由高斯引理，这些非平凡因子都是首一多项式，从而也是首一的一次以上多项式，故在同态下的像也是首一的一次以上多项式，$\overline{f}(x)$ 也是至少 2 个非单位因子的积，从而在 $\mathbb{F}_p[x]$ 中可约，矛盾. □

(2) 若 $f(x)$ 不是 $\mathbb{Z}[x]$ 中首一多项式，(1) 的结论是否成立?

解. 否，$f(x)=2x^2+3x+1=(2x+1)(x+1)$ 为 $\mathbb{Z}[x]$ 中可约多项式，但若 $p=2$，$\overline{f}=x+1$ 是 $\mathbb{F}_2[x]$ 中一次式，它是不可约的.

4.3.13 设 F 为域，$a,b\in F$ 且 $a\neq0$. 证明 $f(x)$ 在 $F[x]$ 中不可约当且仅当 $f(ax+b)$ 在 $F[x]$ 中不可约.

证明. 若 $f(x)$ 有非平凡素因子分解 $f(x)=\prod_{i=1}^n g_i(x)$，则 $f(ax+b)=\prod_{i=1}^n g_i(ax+b)$，其中 $1\leqslant\deg g_i(ax+b)=\deg g_i<\deg f$, 故是 $f(ax+b)$ 的非平凡素因子分解. 反之, $f(x)=f(a'(ax+b)+b')$, 其中 $a'=a^{-1},b'=-a^{-1}b$ 也是 F 中元素，类似上述推理即可. □

4.3.14 设 p 是 $\mathbb{Z}$ 上的奇素数，n 为正整数. 证明 x^n-p 是 $\mathbb{Z}[i]$ 上的不可约多项式.

证明. p 是高斯素数或两个共轭的高斯素数之积 $\pi_i\overline{\pi_i}$. 由艾森斯坦判别法（**定理 4.33**），我们只要证明 $\pi_i^2\nmid p$，$\overline{\pi_i}^2\nmid p$ 即可，这只需要证 $\pi_i=a+bi,\overline{\pi_i}=a-bi$ 彼此不相伴即可. 由 $\varphi(\pi_i)=p$ 无平方因子知 $a,b\neq0$，且 $\gcd(a,b)^2\mid p$ 得 $\gcd(a,b)=1$.

若 $a+bi$ 被 $a-bi$ 整除，则 $(a+bi)=(c+di)(a-bi)$，即 $a(c-1)=-bd, b(c+1)=ad, c^2-1=\frac{-bd}{a}\cdot\frac{ad}{b}=-d^2$，若 $d=0$，因 $c-1$ 与 $c+1$ 不同时为 0，得 a 或 $b=0$，矛盾，若 $d=\pm1$，则 $c=0, a=\pm b$，$p=(a+ai)(a-ai)=2a^2$ 与 p 是奇素数矛盾，故 $a+bi$，$a-bi$ 彼此不相伴. □

4.3.15 证明两个整多项式在 $\mathbb{Q}[x]$ 中互素当且仅当它们在 $\mathbb{Z}[x]$ 中生成的理想含有一个整数.

证明. ($\Rightarrow$) 由 $\mathbb{Q}$ 是域，$\mathbb{Q}[x]$ 是 PID，故也是贝祖环，两个互素的整多项式 f,g 满足 $m(x)f(x)+n(x)g(x)=1, m,n\in\mathbb{Q}[x]$. 令 $\frac{p_1}{q_1},\frac{p_2}{q_2}$ 为 m,n 的容积，则 q_1q_2m, q_1q_2n 为整多项式，$q_1q_2=q_1q_2mf+q_1q_2ng$ 在 $(f,g)_{\mathrm{Ideal},\mathbb{Z}[x]}$ 中.

($\Leftarrow$) 我们有整数 $u=f(x)r(x)+g(x)s(x)$，其中 $r,s\in\mathbb{Z}[x]$. 故 $\gcd(f,g)\mid u$，这只能 $\gcd(f,g)\sim1$ 为非零有理常数. □

4.3.16 设 $f(x)=\sum_{i=0}^n a_ix^i\in\mathbb{Z}[x], \deg f=n$. 若存在素数 p 和整数 k $(0<k<n)$ 使得：

$$p\nmid a_n, p\nmid a_k, p\mid a_i\ (0\leqslant i\leqslant k-1), p^2\nmid a_0.$$

求证 $f(x)$ 在 $\mathbb{Z}[x]$ 中必存在次数 $\geqslant k$ 的不可约因子.

证明. 令 $f_0(x)=f(x)$，我们构造一串多项式 $f_j(x)=\sum_{i=0}^{n_j}a_{ij}x^i\in\mathbb{Z}[x]$ 使得 $p\nmid a_{n_j}, p\nmid a_{k_j}, p\mid a_i\ (0\leqslant i\leqslant k_j-1), p^2\nmid a_0j$ 且 $n_{j+1}<n_j, k_{j+1}\geqslant k_j$.

若 $f_j(x)$ 不可约，则由 $k_j\geqslant k_0=k$ 我们得到结论. 否则，设 $f_j(x)=g(x)h(x)$ 为非平凡素因子分解，$\deg g,h<\deg f_j$，$g(x)=\sum_{i=0}^m b_ix^i$，$h(x)=\sum_{i=0}^l c_ix^i$. 比较首项系数知 $m+l=n_j$ 且 $p\nmid b_mc_l=a_{n_j}$，故 $p\nmid b_m, c_l$. 比较常数项系数，我们有 $p\mid b_0c_0$ 且 $p^2\nmid b_0c_0$. 不妨设 $p\mid b_0$ 且 $p\nmid c_0$. 令 s 满足 $p\mid b_i, i<s$ 且 $p\nmid b_s$，则

$$a_{sj}=b_sc_0+b_{s-1}c_1+\cdots+b_0c_s.$$

当 $s<k_j$ 时 $p\mid a_{sj}$，但 $p\nmid b_sc_0$，$p\mid b_uc_{s-u}\ (u<s)$，故 $p\nmid a_{sj}$，矛盾. 故 $s\geqslant k_j$，我们记 $k_{j+1}=s$ 得 $f_{j+1}(x)=g(x)$.

由于 n_j 严格递减，k_j 不减少，因此这个过程不能无限继续下去，要么提前因 f_j 不可约而终止，要么当 j 足够大时 f_j 满足 $n_j=k_j$，此时 $s\geqslant k_j$ 和 $s<n_j$ 不能同时成立，矛盾，即 $f(j)$ 不可约，并是 $k_j\geqslant k$ 次多项式. □

4.3.17 设 D 是整环，$0\neq f(x)=a_0+a_1x+\cdots+a_nx^n\in D[x]$. 若 $(a_0,a_1,\cdots,a_n)\sim1$，则 $f(x)$ 在 $D[x]$ 中不可约分解若存在则必唯一.

证明. 由于 $c(f)\sim1$，$f(x)$ 的两个因式分解必为

$$f(x)=ug_1(x)g_2(x)\cdots g_s(x)=vh_1(x)h_2(x)\cdots h_t(x),$$

并且 $g_i(x)$ 和 $h_j(x)$ 的容积全为单位. 故 $g_1(x)g_2(x)\cdots g_s(x)\sim_{D[x]}vh_1(x)h_2(x)\cdots h_t(x)$，它们在 D 的商域的多项式环 $F[x]$ 中也相伴，由 $F[x]$ 中因式分解的唯一性，在合适次序下 $s=t, g_i(x)\sim_{F[x]}h_i(x)$，但 g_i,h_i 的容积都是 D 中单位，从而它们在 D 中也相伴. □

第五章　域扩张理论

5.1 域扩张基本理论

本节中称 α 在域 K 上代数次数为 n 是指 $[K(\alpha):K]=n$.

5.1.1 设 F/K 为域的扩张，$u\in F$ 是 K 上的奇次代数元素，求证 $K(u)=K(u^2)$.

证明. 显然我们只需证 $u\in K(u^2)$ 即可. 令 $f(x)$ 是 u 在 K 上的的最小多项式，则 $f(u)=0$，将偶数次项移到右边得 $ug(u^2)=h(u^2)$，则由 u 的代数次数为奇数知 $g(x)\neq 0$，故 $u=\frac{h(u^2)}{g(u^2)}\in K(u^2)$. □

5.1.2 设 p 为素数，求扩张 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 的次数，其中 $\zeta_n=e^{\frac{2\pi i}{n}}$ 为辐角主值最小的 n 次本原单位根. 对一般的 n，扩张 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 的次数是多少?

解. (i) ζ_p 是 p 次分圆多项式（**例 4.34**）的根，该多项式在 $\mathbb{Q}[x]$ 中不可约，故是 ζ_p 的最小多项式，其次数 $p-1$ 即扩张的次数.

(ii) 由**习题 4.3.4**，x^4+1 在 $\mathbb{Q}[x]$ 中不可约且 ζ_8 是它的根，故它的次数 4 即扩张的次数.

(iii) 我们利用本节知识证明 n 次分圆多项式 $f(x)=\prod_{\gcd(k,n)=1}(x-\zeta_n^k)$ 是 $\mathbb{Q}[x]$ 中不可约多项式（n 不一定是素数）.

证明. $\langle\zeta_n\rangle\cong\mathbb{Z}/n\mathbb{Z}=G$，而 $\mathrm{Aut}(G)$ 为 $(\mathbb{Z}/n\mathbb{Z})^\times$，且 $\mathbb{Q}(\zeta_n)$ 中的元素均能表示为 G 中元素的线性组合，故 G 的自同构诱导了 $\mathbb{Q}(\zeta_n)$ 到自身的自同构，该同构在 $\mathbb{Q}$ 上的限制必然是恒等映射，令 $\varphi\in\mathrm{Aut}(G)$，则 φ 将本原单位根 ζ_n 映射到本原单位根 ζ_n^k $(\gcd(n,k)=1)$，由**命题 5.18**（取 $F=\mathbb{Q},K=\mathbb{Q}(\zeta_n)$），一切 n 次本原单位根有相同的最小多项式 $g(x)$，全部 n 次本原单位根都是 $g(x)$ 的根，故 $f(x)\mid g(x)$（我们现在尚不确定 $f(x)$ 在 $\mathbb{Q}[x]$ 中）

由于 x^n-1 没有重根且是 ζ_n 的化零多项式，$g(x)\mid x^n-1$，故 $g(x)$ 无重根，我们只需证明 $g(x)$ 没有任何 $f(x)$ 的根以外根即可。若有这样的根，则该根也是 x^n-1 的根，故为 n 次单位根，令该根为 ζ_n^r，则 $\gcd(n,r)\neq 1$，且在**命题 5.19** 中取 $F=\tilde{F}=\mathbb{Q},K=\tilde{K}=\mathbb{Q}(\zeta_n)$，最小多项式为 $g(x)$，则存在域同构 φ_1 使得它保持有理数不变且 $\varphi_1(\zeta_n)=\zeta_n^r$，故 $\varphi_1(\zeta_n^{n/\gcd r,n})=\zeta_n^{rn/\gcd r,n}=(\zeta_n^n)^{r/\gcd r,n}=1$，但 $n/\gcd r,n<n$，$\zeta_n^{n/\gcd r,n}\neq 1$，与 φ_1 保持 1 不变矛盾，故 $g(x)$ 无任何其他根，$g(x)=f(x)$ 为不可约多项式. □

这样，扩张 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 的次数即 $\deg f=|\{k\mid\gcd(k,n)=1\}|=\phi(x)=|(\mathbb{Z}/n\mathbb{Z})^\times|$.

5.1.3 求元素 $u=\sqrt{2}+\sqrt{3}$ 在域 K 上的极小多项式，其中

(1) $K=\mathbb{Q}$;

解. u 是 $f(x)=x^4-10x^2+1=0$ 的根，由**命题 4.26**，有理根只可能为 ±1，代入即得它们都不是根，故 $f(x)$ 若在 $\mathbb{Z}[x]$ 内可约则为 $f(x)=(x^2+ax+\pm1)(x^2+bx\pm1)$ 的形式，得 $a=-b,ab\pm2=-10$，即 $a^2=8$ 或 12，该方程无整数解，故 $f(x)$ 在 $\mathbb{Z}[x]$ 内不可约，由**定理 4.35**，$f(x)$ 在 $\mathbb{Q}[x]$ 内也不可约，为 u 的最小多项式.

(2) $K=\mathbb{Q}(\sqrt{2})$;

解. u 是 $f(x)=\sqrt{2}u^2-4u-\sqrt{2}$ 的根，故 u 的 K-代数次数最多为 2. 若 $u\in\mathbb{Q}(\sqrt{2})$，则 $u-\sqrt{2}=\sqrt{3}\in\mathbb{Q}(\sqrt{2})$，即 $\sqrt{3}=a\sqrt{2}+b$ $(a,b\in\mathbb{Q})$，即 $3=2a^2+b^2+\sqrt{2}ab$，得 $ab=0,2a^2+b^2=3$，

a 或 $b=0$，$a^2=\frac{3}{2}$ 或 $b^2=3$，与 a,b 是有理数矛盾，故 u 的 K-代数次数不为 1，$f(x)$ 是 u 的最小多项式.

(3) $K=\mathbb{Q}(\sqrt{6})$.

解. u 是 $f(x)=u^2-(5+2\sqrt{6})$ 的根，故 u 的 K-代数次数最多为 2. 若 $u\in\mathbb{Q}(\sqrt{6})$，则 $\sqrt{2}+\sqrt{3}=a\sqrt{6}+b\,(a,b\in\mathbb{Q})$，即 $6a^2+b^2+2\sqrt{6}ab=5+2\sqrt{6}$，$6a^2+b^2=5, ab=1$，$b^4-5b^2+6=0$，得 $b^2=2$ 或 3，与 b 是有理数矛盾，故 u 的 K-代数次数不为 1，$f(x)$ 是 u 的最小多项式.

5.1.4 证明 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证明. 我们只需证明 $\sqrt{2}$ 和 $\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ 即可. 令 $u=\sqrt{2}+\sqrt{3}$，则 $\sqrt{2}=(u^2-9u)/2, \sqrt{3}=-(u^2-11u)/2$. □

5.1.5 设 F/K 为域的代数扩张，D 为整环且 $K\subseteq D\subseteq F$，求证 D 为域.

证明. 只需证明 D 中任意元素 u 在 D 中可逆即可. 由于 u 在 K 上代数，$f(u)=0$ 其中 $f(x)\in K[x]\subseteq D[x]$，由 $f(u)$ 在 K 上不可约，其常数项不为 0，故 $g(u)u+f_0=0, -f_0^{-1}g(u)u=1$，其中 $g(x)\in K[x]\subseteq D[x]$，即 $-f_0^{-1}g(u)\in D$ 为 u 在 D 中的逆. □

5.1.6 设 u 属于域 F 的某个扩域，并且 u 在 F 上代数. 如果 $f(x)$ 为 u 在 F 上的最小多项式，则 $f(x)$ 必为 $F[x]$ 中不可约元. 反之，若 $f(x)$ 是 $F[x]$ 中首一不可约多项式，并且 $f(u)=0$，则 $f(x)$ 为 u 在 F 上的最小多项式.

证明. (i) 若 $f(x)$ 有非平凡素因子分解 $f(x)=g(x)h(x), 1\leqslant\deg g,h<\deg f$，则 $g(u)$ 或 $h(u)=0$，与最小多项式的定义矛盾.

(ii) 令 u 在 F 上的最小多项式为 $g(x)$，则 $f(x)=g(x)h(x)+r(x)$，其中 $\deg r<\deg g$，且 $r(u)=f(u)-g(u)h(u)=0-0\cdot h(u)=0$，由最小多项式的定义，只能 $r(x)=0$，又 $f(x)$ 不可约，只能 $h(x)\in U(F[x])=F-\{0\}$，又 f,g 均首一，只能 $h(x)=1, f(x)=g(x)$. □

5.1.7 设 K/F 为域扩张，$a\in K$. 若 $a\in F(a^m), m>1$，则 a 在 F 上代数.

证明. 我们有 $a-g(a^m)=0$, 由于 $m>1$, $f(x)=x-g(x^m)$ 不是零多项式, 即 $f(a)=a-g(a^m)=0$, a 在 F 上代数. □

5.1.8 设 $K(x_1,x_2,\cdots,x_n)$ 为 n 元多项式环 $K[x_1,x_2,\cdots,x_n]$ 的商域，若 $K(x_1,x_2,\cdots,x_n), u\notin K$，则 u 在 K 上超越.

证明. 反证法，若 $u=f/g$ $(g\neq 0, f,g\in K[x_1,x_2,\cdots,x_n])$ 在 K 上代数，则 $a_r(f/g)^r+a_{r-1}(f/g)^{r-1}+\cdots+a_0=0$ 其中 $a_i\in K$ $(0\leqslant i\leqslant r)$，故 $a_rf^r+a_{r-1}f^{r-1}g+\cdots+a_0g^r=0$，即 $f\mid g^r, g\mid f^r$，若 $f\neq 0$，则 f 的不可约（自然是素的）因子都是 g 的不可约因子，反之亦然. 故 $f\sim g$ 或 $f=0$，$u=f/g\in U(K[x_1,x_2,\cdots,x_n])\cup\{0\}=K$，矛盾. □

5.1.9 设 K 为域，$u \in K(x), u \notin K$，证明 x 在 $K(u)$ 上代数.

证明. $u = f(x)$，其中 $f(x)$ 为一次以上 K-系数多项式，故 $f(x) - u$ 是一次以上 $K(u)$-系数多项式，它是 x 在 $K(u)$ 中的化零多项式. □

5.1.10 令 $K = \mathbb{Q}(\alpha)$，其中 α 是方程 $x^3 - x - 1 = 0$ 的一个根，求 $\gamma = 1 + \alpha^2$ 在 $\mathbb{Q}$ 上的最小多项式.

证明. 由**命题 4.26**，$x^3 - x - 1 = 0$ 的有理根只可能为 ± 1，代入知 $x^3 - x - 1 = 0$ 没有有理根，故 $[\mathbb{Q}(\alpha) : \mathbb{Q}]$=3.

显然 $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha)$，故 $[\mathbb{Q}(\gamma) : \mathbb{Q}]$=3 或 1. 若 $\mathbb{Q}(\gamma) = \mathbb{Q}$，则 $1 + \alpha^2 \in \mathbb{Q}$，$\alpha$ 在 $\mathbb{Q}$ 上代数次数最多为 2，矛盾. 故 γ 的最小多项式为 3 次.

设 $\gamma^3 + a\gamma^2 + b\gamma + c = 0$，则 $(7 + 3a + b)\alpha^2 + (5 + a)\alpha + (2 + a + b + c) = 0$，由于 $\alpha^2, \alpha, 1$ 在 $\mathbb{Q}$ 上线性无关，故 $7 + 3a + b = 0, 5 + a = 0, 2 + a + b + c = 0$，解得 $a = -5, b = 8, c = -5$，故 $x^3 - 5x^2 + 8x - 5$ 是 γ 在 $\mathbb{Q}$ 上的最小多项式. □

5.1.11 设 a 是正有理数且不是 $\mathbb{Q}$ 中数的平方，证明 $[\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}] = 4$.

证明. 显然 $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2, \mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\sqrt[4]{a})$，并且 $(\sqrt[4]{a})^2 = \sqrt{a} \in \mathbb{Q}(\sqrt{a})$，故 $[\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}(\sqrt{a})] \leqslant 2$，只需 $\sqrt[4]{a} \notin \mathbb{Q}(\sqrt{a})$ 即可. 若不然，则 $\sqrt[4]{a} = b + c\sqrt{a}$，得 $= b^4 + 6b^2c^2a^2 + c^4 - a + 4bc(ac^2 + b^2)\sqrt{a} = 0$，只能 $b = 0$ 或 $c = 0$，即 $a = c^4$ 或 b^4，矛盾. □

5.1.12 设 u 是多项式 $x^3 - 6x^2 + 9x + 3$ 的根.

(1) 求证 $[\mathbb{Q}(u) : \mathbb{Q}] = 3$.

证明. 由艾森斯坦判别法（取 $p = 3$）得上述多项式在 $\mathbb{Q}[x]$ 中不可约，故 u 的 $\mathbb{Q}$-代数次数为 3. □

(2) 试将 $u^4, (u + 1)^{-1}, (u^2 - 6u + 8)^{-1}$ 表示为 $1, u, u^2$ 的线性组合.

解. $u^3 = 6u^2 - 9u - 3$.

(i) $u^4 = 6u^3 - 9u^2 - 3u = 36u^2 - 54u - 18 - 9u^2 - 3u = 27u^2 - 57u - 18$.

(ii) $(u + 1)(u^2 - 7u + 16) = 13$，故 $(u + 1)^{-1} = (u^2 - 7u + 16)/13$.

(iii) 设 $(u^2 - 6u + 8)^{-1} = au^2 + bu + c$，则 $au^4 + (-6a + b)u^3 + (8a - 6b + c)u^2 + (-6c + 8b)u + 8c = 1$，即 $-a + c = 0, -3a - b - 6c = 0, -3b + 8c - 1 = 0$，解得 $c = 1/35, a = 1/35, b = -9/35$，即 $(u^2 - 6u + 8)^{-1} = (u^2 - 9u + 1)/35$.

5.1.13 设 $d \geqslant 3$ 为无平方因子的整数，$K = \mathbb{Q}(\sqrt{d})$.

(1) 证明 K 中任意元素在 $\mathbb{Q}$ 上的最小多项式是 1 次或 2 次.

证明. $x^2 - d$ 是 $\sqrt{d}$ 在 $\mathbb{Q}$ 上的最小多项式，故 $[K : \mathbb{Q}] = 2$，对 K 中任意元素 α 有 $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$，故 $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ 只能为 1 或 2，故得结论. □

(2) 设 $\mathcal{O}$ 是 K 中所有在 $\mathbb{Q}$ 上的最小多项式为首一整系数多项式元素的集合，试求 $\mathcal{O}$.

解. $\mathbb{Q}[\sqrt{d}]$ 中元素 u 均有 $a+b\sqrt{d}$ 的形式，其中 $a,b\in\mathbb{Q}$. 若最小多项式为一次，则 $b=0$, $x-a=0$ 为 a 的最小多项式，故 $u\in\mathbb{Z}$.

若最小多项式为二次，则 $b\neq 0, x^2+ex+f=0$，其中 $e,f\in\mathbb{Z}$. 故 $a^2+b^2d+ea+f+(2ab+eb)\sqrt{d}=0$，我们有 $a=-e/2, -e^2/4+b^2d\in\mathbb{Z}$，若 e 为偶数，则 $a,-e^2/4$ 为整数，b^2d 为整数，又 d 没有平方因子，迫使 b 为整数，故 a,b 为整数时满足条件，此时 $x^2-2ax+a^2-b^2d=0$ 为最小多项式.

若 e 为奇数，则 $e^2\equiv 1 \mod 4$，故 $4b^2d=h$ 其中 $h\equiv 1 \mod 4$，设 $b=p/q$ $(\gcd(p,q)=1)$，则 $4p^2d=hq^2$，由 p^2,q^2 互素得 $q^2\mid 4d$，由于 d 没有平方因子，只能 $q^2=4$，即 $q=2, p^2d=h$，p 是奇数，两边模 4 得 $d\equiv 1 \mod 4$ 时这样的 p 存在.

由于当 $2a,2b$ 均为奇数，$d\equiv 1 \mod 4$ 时 $x^2-2ax+a^2-b^2d$ 确实为整系数多项式，故当 $d\equiv 2,3 \mod 4$ 时 $\mathcal{O}=\mathbb{Z}\cup\{a+b\sqrt{d}\mid a,b\in\mathbb{Z}\}$，当 $d\equiv 1 \mod 4$ 时 $\mathcal{O}=\mathbb{Z}\cup\{a+b\sqrt{d}\mid a,b\in\mathbb{Z}\}\cup\{a+b\sqrt{d}\mid 2a,2b\in\mathbb{Z}-2\mathbb{Z}\}$.

5.1.14 设 x 是 $\mathbb{Q}$ 上的超越元且 $u=x^3/(x+1)$，求 $[\mathbb{Q}(x):\mathbb{Q}(u)]$.

解. 由于 $x^3-ux-u=0$，故 $\{x^3,x^2,x,1\}$ 在 $\mathbb{Q}(u)$ 上线性相关，$[\mathbb{Q}(x):\mathbb{Q}(u)]\leqslant 3$，若 $[\mathbb{Q}(x):\mathbb{Q}(u)]<3$，则 x^3-ux-u 不是 $\mathbb{Q}(u)$ 上的不可约多项式，它必有一次因式，即 $[\mathbb{Q}(x):\mathbb{Q}(u)]=1$，故我们只需要证明 $x\notin\mathbb{Q}(u)$ 即证明了 $[\mathbb{Q}(x):\mathbb{Q}(u)]=3$.

若 $x=\frac{f(u)}{g(u)}$，设 $\deg f=a,\deg g=b$，则 $f(u)(x+1)^a$ 是 x 的 $3a$ 次多项式，$g(u)(x+1)^b$ 是 x 的 $3b$ 次多项式，若 $a>b$ 则 $xg(u)(x+1)^b(x+1)^{a-b}=f(u)(x+1)^a$，左边为 $1+a+2b$ 次多项式，右边为 $3a$ 次多项式，但 $b\leqslant a-1$，即 $1+a+2b\leqslant 3a-1<3a$，矛盾. 若 $a<b$ 则 $xg(u)(x+1)^b=f(u)(x+1)^a(x+1)^{b-a}$，左边为 $1+3b$ 次多项式，右边为 $2a+b$ 次多项式，但 $b\geqslant a+1$，$1+3b\geqslant 3+2a+b>2a+b$，矛盾. 若 $a=b$，则 $xg(x)(x+1)^a=f(x)(x+1)^a$，左边为 $3a+1$ 次多项式，右边为 $3a$ 次多项式，矛盾. 故 $x\notin\mathbb{Q}(u)$，$[\mathbb{Q}(x):\mathbb{Q}(u)]=3$.

5.1.15 试写出二元域 $\mathbb{F}_2$ 的一个 2 次不可约多项式 $f(x)$. 设 u 是 $f(x)$ 的一个根，写出 $\mathbb{F}_2(u)$ 的全部元素及它们的加法表和乘法表.

解. $\mathbb{F}_2[x]$ 中的一次多项式只有 x 和 $x+1$，由于 $x^2+x+1=(x+1)x+1$，故 x^2+x+1 是不可约多项式，$u^2+u+1=0\Rightarrow u^2=u+1$（请注意 $+1$ 与 -1 并无差别）. 故 $\mathbb{F}_2(u)=\{0,1,u,u+1\}$，加法表如下：

$+$	0	1	u	$u+1$
0	0	1	u	$u+1$
1	1	0	$u+1$	u
u	u	$u+1$	0	1
$u+1$	$u+1$	u	1	0

乘法表如下（0 省略）：

$\times$	1	u	$u+1$
1	1	u	$u+1$
u	u	$u+1$	1
$u+1$	$u+1$	1	u

5.1.16 设 M/K 为域的扩张，M 中元素 u,v 分别是 K 上的 m 次和 n 次代数元素，$F=K(u)$，$E=K(v)$.

(1) 求证 $[FE:K]\leqslant mn$.

证明. F 中任意元素均能表示成 $1,u,\cdots,u^{m-1}$ 的线性组合，另一方面 E 中任意元素均能表示成 $1,v,\cdots,v^{n-1}$ 的线性组合，故 FE 中任意元素均能表示成 u^iv^j $(0\leqslant i<m,0\leqslant j<n)$ 的线性组合，即 mn 个元素的线性组合，故由线性代数知 $[FE:K]$ 至多为 mn. □

(2) 如果 $\gcd(m,n)=1$，则 $[FE:K]=mn$.

证明. 由于 F 和 E 都是 FE 的子域，故 $m=[F:K]\mid[FE:K],n=[E:K]\mid[FE:K]$，$\operatorname{lcm}(m,n)\mid[FE:K]$，当 $\gcd(m,n)=1$ 时 $\operatorname{lcm}(m,n)=mn$，再由 (1) 可知只能 $[FE:K]=mn$. □

5.1.17 设 K,L 为域 F 的扩张且均在 F 的某给定代数封闭域中. 称 L 在 F 上**线性不相交**于 K 是指 L 中任何 F-线性无关有限集还是 K-线性无关集. 即对 L 的任意子集合 $\{x_i\mid i\in I\}$ 如它在 F 上线性无关，则它也在 K 上线性无关.

(1) 证明：如 L 在 F 上线性不相交于 K，则 K 在 F 上线性不相交与 L.

证明. 如 L 在 F 上线性不相交于 K，任取 L 的一组 F-基 $\{x_i\mid i\in I_L\}$ 和 K 的一组 F-基 $\{y_j\mid j\in J_K\}$，则 $\sum_i b_ix_i=0$ $(b_i\in K)\Rightarrow b_i=0,\forall i$，将 b_i 用 K 的 F-基表示即 $\sum_{i,j}c_{ij}x_iy_j=0$ $(c_{ij}\in F)\Rightarrow c_{ij}y_j=0,\forall i\Rightarrow c_{ij}=0,\forall i,j$，即 x_iy_j 是 F-线性无关集.

反之，若 L 在 F 上线性相交于 K，取 K-线性相关但 F-线性无关的集合 $\{x_i'\mid i\in S\}$，则它可以扩充为一组 F-基 $\{x_i\mid i\in I_L\}$ 并同样 K-线性相关，$\sum_i b_ix_i=0$ 其中 $b_i\in K$ 不全为零，将 b_i 用 K 中 F-基表示则 $\sum_{i,j}c_{ij}x_iy_j=0$ $(c_{ij}\in F)$，其中 c_{ij} 不全为 0，即 x_iy_j 是 F-线性相关集.

同样，若 K 在 F 上线性相交于 L，则 x_iy_j 也是 F-线性相关集，矛盾. 故得结论. □

(2) 设 K 与 L 均是 F 的有限扩张. 证明：L 在 F 上线性不相交于 K 当且仅当 $[KL:F]=[K:F]\cdot[L:F]$.

证明. 线性不相交关系 $\Leftrightarrow$ 任取 L,K 的 F-基，其 $[K:F][L:F]$ 个乘积元素 F-线性无关，$[KL:F]\geqslant[K:F]\cdot[L:F]$ 又因**习题 5.1.16**，$[KL:F]=[K:F]\cdot[L:F]$. 反之，若 L 在 F 上线性相交于 K，则设 x_i,y_j 各是 L,K 的一组 F-基，则 x_iy_j 是 F-线性相关集合，故是少于 $[K:F]\cdot[L:F]$ 个元素 z_k 的线性组合，KL 上任何元素都是 x_iy_j 的 F-线性组合，故也是 z_k 的 F-线性组合，即 $[KL:F]<[K:F]\cdot[L:F]$. □

5.1.18 设 F 为特征 p 域，p 为素数，$c\in F$

(1) 证明 x^p-x-c 在 $F[x]$ 中不可约当且仅当 x^p-x-c 在 F 中无根.

证明. ($\Rightarrow$) 显然.

($\Leftarrow$) 证明由文献 [5] 给出.

(证明 1) 令 $f(x)=x^p-x-c$, 考虑双射 $\varphi:F[x]\to F[x],x\mapsto x+1$, 则 $\varphi(f)=f$, 故 φ 将 f 的不可约因子变作 f 的不可约因子, 令 f 在 $F[x]$ 上的因子分解为 $f=ug_1g_2\cdots g_n$, 由于 f 无根, 没有一次因式, 因此 $n<p$.

由于 $\varphi^p:x\mapsto x+p=x$ 为恒等映射, 故 $\langle\varphi\rangle\cong\mathbb{Z}/p\mathbb{Z}$, 该 p 阶循环群作用在 $M=\{g_1,g_2,\cdots,g_n\}$ 上, 有同态 $\tau:\mathbb{Z}/p\mathbb{Z}\to S_n$, 由于 $n<p$, $p\nmid n!$, $|\operatorname{im}\tau|\mid n!,|\operatorname{im}\tau|\mid p$, 只能 $|\operatorname{im}\tau|=1$, 即 $\langle\varphi\rangle$ 在 M 上作用平凡, 任意 f 的不可约因子在 φ 下不变.

令 $r=\deg g_1$, 则 $g_1=a_rx^r+a_{r-1}x^{r-1}+\cdots+a_0$ $(a_r\neq0)$, $\varphi(g_1)=a_rx^r+(ra_r+a_{r-1})x^{r-1}+\cdots+b$, 即 $\overline{r}a_r=\overline{0}$, 由于 F 没有零因子, 只能 $\overline{r}=\overline{0}$, 即 $p\mid r$, 又 $1\leqslant r\leqslant p$, 只能 $r=p$, 即 $g_1=f$, f 为不可约多项式.

(证明 2) 读者应当在学习第六章伽罗瓦理论后再次体会这种证法.

由于 f 的形式微商 $f'=-1$, 故 $\gcd(f,f')=1$, f 无重根. 令 K 为 F 的代数闭包, 则 f 在 K 中有 p 个根 $\alpha_1,\cdots,\alpha_p$. $L\subseteq K$ 为 $F(\alpha_1,\cdots,\alpha_p)$, 记 $\operatorname{Gal}(L/F)$ 为 L 的所有 F-自同构构成的集合, 在其上定义映射复合为乘法运算. 令 $\tau:\operatorname{Gal}(L/F)\to\mathbb{Z}/p\mathbb{Z},\sigma\mapsto\sigma(\alpha_1)-\alpha_1$, 我们证明 τ 是良好定义的.

由**命题 5.18**, $\sigma(\alpha_1)$ 也是 $f=\sigma(f)$ 的根, 记为 α_i, 则 $\tau(\sigma)=\alpha_i-\alpha_1$. 由于 $\alpha_i^p-\alpha_i-c=\alpha_1^p-\alpha_1-c=0$, 故 $\alpha_i-\alpha_1=\alpha_i^p-\alpha_1^p\equiv(\alpha_i-\alpha_1)^p \mod p$, 即在 F 中 $\alpha_i-\alpha_1$ 是 x^p-x 的根, 但由**推论 1.63**, F 中所有整数 $0,1,\cdots,p-1$ 都是 x^p-x 的根, 故由**推论 4.25**, x^p-x 在 L 中只有这 p 个根, 即 $\alpha_i-\alpha_1\in\mathbb{Z}/p\mathbb{Z}$.

由于 p 阶循环群只有平凡子群, 若 $\operatorname{im}\tau=\mathbb{Z}/p\mathbb{Z}$, 则 $\operatorname{Gal}(L/F)$ 将 α_1 映射到 p 个不同值, 故 $[L:F]\geqslant|\operatorname{Gal}(L/F)|=p$ (**定理 6.8**), 又 f 是所有 α_i 的化零多项式, 故 $[L:F]\leqslant p$, 故 $[L:F]=p$, 且由 $\alpha_i\notin F$, α_i 的最小多项式为 p 次, 故为 f, 即 f 不可约.

若 $\operatorname{im}\tau$ 是平凡群, 则 σ 保持一切 α_i 不变, 故是 L 上的恒等映射, 由**例 6.15**, **命题 6.16** 和**定理 6.24** 知 L/F 是伽罗瓦扩张, $[L:F]=|\operatorname{Gal}(L/F)|=1$, 即 $\alpha_i\in F$, 矛盾. □

(2) 若 $\operatorname{char}F=0$ 时, 试问 (1) 中结论是否仍然成立?

解. 否, 例如 $F=\mathbb{Q}$, $f=x^5-x-15=(x^2-x+3)(x^3+x^2-2x-5)$ 是可约多项式, 但 f 没有有理根 (对每个因式考虑有理根, 第一个只能为 ±3, 第二个只能为 ±5, 代入即否定).

5.1.19

(1) 设 F 为特征不为 2 的域, 证明 F 的每个二次扩张均有形式 $F(\sqrt{a})$, 其中 $a\in F-F^2$.

证明. 令 K/F 为二次扩张, 任选 $\alpha\in K-F$, 则 α 的最小多项式为 x^2+bx+c, 故 $2\alpha+b=\pm\sqrt{b^2-4c},\alpha\in F(\sqrt{b^2-4c})$, 若 $b^2-4c\in F^2$, 则 $\alpha=1/2(\pm\sqrt{b^2-4c}-b)\in F$, 矛盾, 故 $b^2-4c\in F-F^2$, 令 $a=b^2-4c$ 即得结论. □

(2) 若 $\operatorname{char}F=2$, 则 (1) 的结论是否仍然成立?

解. 否，考虑**习题 5.1.15** 的结果，由于 $\mathbb{F}_2(u)$ 有 4 个元素，显然 $\mathbb{F}_2(u)/\mathbb{F}_2$ 是二次扩张，但 $u^2 = u+1 \notin \mathbb{F}_2$.

以下参照文献 [10].

事实上，令 $K = F[t]/(t^2-t+\alpha)$，$\alpha \in F$. 如果 α 不是 $x^2-x, x \in F$ 的形式，那么 $t^2-t+\alpha$ 是 $F[t]$ 中不可约多项式，K 是域，K/F 是二次扩张.

5.1.20 设 $K = \mathbb{Q}(\alpha)$ 是 $\mathbb{Q}$ 的单扩张，其中 α 在 $\mathbb{Q}$ 上代数，证明 $|\operatorname{Aut}(K)| \leqslant [K:\mathbb{Q}]$.

证明. 令 φ 是 K 的 $\mathbb{Q}$-自同构，则对 α 在 $\mathbb{Q}$ 上的最小多项式 $f(x)$，$\varphi(\alpha)$ 仍是 $f(x)$ 的根（**命题 5.18**），并唯一确定 φ，由**推论 4.25**，这样的不同根最多有 $\deg f = [K:\mathbb{Q}]$ 个，即 $\operatorname{Aut}(K)$ 最多有 $[K:\mathbb{Q}]$ 个元素.

注记. 等号不成立即 f 有重根或者 f 在 K 上不分裂，$\alpha \mapsto$ 另一个根 β 有可能不是 K 的自同构的情形，参见第六章第一节. □

5.2 尺规作图问题

5.2.1 下列哪些量可以尺规作出?

(1) $\sqrt[4]{3+5\sqrt{8}}$;

解. 可以，因为 $\sqrt[4]{a}$ 即 $\sqrt{\sqrt{a}}$，由有理数作加减乘除和开方即能得到.

(2) $\frac{3\sqrt{5}}{\sqrt{7}-4}$;

解. 可以，理由同上.

(3) $2+\sqrt[5]{7}$;

解. 不可以，若该量可以尺规作出，则 $a=\sqrt[5]{7}$ 也可以尺规作出，a 是 $x^5-7=0$ 的根，取 $p=7$ 由艾森斯坦判别法知该多项式在 $\mathbb{Q}[x]$ 中不可约，$[\mathbb{Q}(a):\mathbb{Q}]=5$ 不是 2 的幂.

(4) x^5-3x^2+6 的一个根 α.

解. 不可以，取 $p=3$ 由艾森斯坦判别法知该多项式在 $\mathbb{Q}[x]$ 中不可约，$[\mathbb{Q}(\alpha):\mathbb{Q}]=5$ 不是 2 的幂.

5.2.2 证明可以尺规三等分 45° 和 54° 角.

证明. 若角 α,β 可以尺规作出，则 $\cos\alpha,\cos\beta,\sin\alpha,\sin\beta$ 可以尺规作出，故 $\cos(\alpha\pm\beta)=\cos\alpha\cos\beta\mp\sin\alpha\sin\beta$ 也可以尺规作出，即 $\alpha\pm\beta$ 可以尺规作出（也可以由几何知识直接得到该结论）.

熟知 $\cos 60^\circ=\frac{1}{2}$ 可以尺规作出，故给定 45° 可以作 $15^\circ=60^\circ-45^\circ$，给定 54° 可以作 $6^\circ=60^\circ-54^\circ$，将该角再三倍即得 18°. □

5.2.3 能否尺规作立方体，其体积为原立方体的 2 倍?

解. 否，题意即尺规作出 $a=\sqrt[3]{2}$，由于 a 满足 $x^3-2=0$，取 $p=2$ 由艾森斯坦判别法知该多项式在 $\mathbb{Q}[x]$ 中不可约，$[\mathbb{Q}(a):\mathbb{Q}]=3$ 不是 2 的幂.

5.2.4 设 $3\leqslant n\leqslant 10$ 为正整数，则正 n 边形是否可以尺规作出?

解. $n=3$：$\cos\frac{2\pi}{3}=-\frac{1}{2}$ 为可构造数，故正三角形可.

$n=4$：$\cos\frac{2\pi}{4}=0$ 为可构造数，故正方形可.

$n=5$：$\cos\frac{2\pi}{5}=a$，其中 a 满足 $2a^2-1=\cos\frac{4\pi}{5}=\cos\frac{6\pi}{5}=4a^3-3a$，故 $4a^3-2a^2-3a+1=(a-1)(4a^2+2a-1)=0$，又 $a\neq 1$，故 $4a^2+2a-1=0$，$[\mathbb{Q}(a):\mathbb{Q}]\leqslant 2$，即 a 为可构造数，故正五边形可.

$n=6$：$\cos\frac{2\pi}{6}=\frac{1}{2}$ 为可构造数，故正六边形可.

$n=7$：$\cos\frac{2\pi}{7}=a$，其中 a 满足 $2(2a^2-1)^2-1=\cos\frac{8\pi}{7}=\cos\frac{6\pi}{7}=4a^3-3a$，故 $8a^4-4a^3-8a^2+3a+1=(a-1)(8a^3+4a^2-4a-1)=0$，又 $a\neq 1$，故 $8a^3+4a^2-4a-1=0$，该方程的有理根

（**命题 4.26**）只能是 $\pm1, \pm1/2, \pm1/4, \pm1/8$，代入即得该方程没有有理根，从而没有一次因式，从而是 $\mathbb{Q}[x]$ 中不可约多项式，$[\mathbb{Q}(a):\mathbb{Q}]=3$ 不是 2 的幂，正七边形不能尺规作出.

$n=8$：$\cos\frac{2\pi}{8}=\frac{\sqrt{2}}{2}$，由 2 是可构造数，$\sqrt{2}$ 也是，故 $\frac{\sqrt{2}}{2}$ 可构造，正八边形可.

$n=9$：若正九边形可尺规作出，则 40° 可构造，又 60° 可构造，则 20° 可构造，与**推论 5.35** 矛盾，故正九边形不能尺规作出.

$n=10$：沿用 $n=5$ 时的 a，则 $\cos\frac{2\pi}{10}=b, 2b^2-1=a, b=\pm\sqrt{\frac{a+1}{2}}$，由 a 可构造推出 b 可构造，故正十边形可以尺规作出.

5.3 代数基本定理

5.3.1 证明 $\mathbb{C}[x]$ 的极大理想与复平面上的点一一对应. $\mathbb{R}[x]$ 的极大理想可以自然地对应到复平面上的什么?

解. 类似**习题 4.38** 知对于域上的多项式环，极大理想即不可约多项式生成的理想.

由代数基本定理，$\mathbb{C}[x]$ 上的极大理想即一次多项式 $(x-a)$ 生成的理想，该一次多项式的根与复平面上的点一一对应.

由于实系数多项式的虚根两两共轭，$\mathbb{R}[x]$ 上的极大理想即一次多项式 $(x-a)$ 或二次不可约多项式 $(x-z)(x-\bar{z})$ 生成的理想，一次多项式的实根与实轴上的点一一对应，二次不可约多项式的一对共轭虚根与上半平面上的点一一对应.

5.4 有限域的理论

5.4.1 构造一个 8 元域，并写出它的加法表和乘法表.

解. $\mathbb{F}_2$ 上的一次多项式只有 x 和 $x+1$.

$x^2 = x\cdot x$，$x^2+1=(x+1)^2$，$x^2+x=x(x+1)$，只有 $x^2+x+1=x(x+1)+1$ 是不可约 2 次多项式.

令 $f(x)=x^3+x+1$，则 $f(x)=x(x+1)^2+1=x(x^2+x+1)+(x+1)^2$，故它是不可约多项式，令其一个根为 u，则 $\{au^2+bu+c \mid a,b,c\in\mathbb{F}_2\}$ 为 8 元域.

加法表如下：

$+$	0	1	u	$u+1$	u^2	u^2+1	u^2+u	u^2+u+1
0	0	1	u	$u+1$	u^2	u^2+1	u^2+u	u^2+u+1
1	1	0	$u+1$	u	u^2+1	u^2	u^2+u+1	u^2+u
u	u	$u+1$	0	1	u^2+u	u^2+u+1	u^2	u^2+1
$u+1$	$u+1$	u	1	0	u^2+u+1	u^2+u	u^2+1	u^2
u^2	u^2	u^2+1	u^2+u	u^2+u+1	0	1	u	$u+1$
u^2+1	u^2+1	u^2	u^2+u+1	u^2+u	1	0	$u+1$	u
u^2+u	u^2+u	u^2+u+1	u^2	u^2+1	u	$u+1$	0	1
u^2+u+1	u^2+u+1	u^2+u	u^2+1	u^2	$u+1$	u	1	0

乘法表如下（0 省略）：

$\times$	1	u	$u+1$	u^2	u^2+1	u^2+u	u^2+u+1
1	1	u	$u+1$	u^2	u^2+1	u^2+u	u^2+u+1
u	u	u^2	u^2+u	$u+1$	1	u^2+u+1	u^2+1
$u+1$	$u+1$	u^2+u	u^2+1	u^2+u+1	u^2	1	u
u^2	u^2	$u+1$	u^2+u+1	u^2+u	u	u^2+1	1
u^2+1	u^2+1	1	u^2	u	u^2+u+1	$u+1$	u^2+u
u^2+u	u^2+u	u^2+u+1	1	u^2+1	$u+1$	u	u^2
u^2+u+1	u^2+u+1	u^2+1	u	1	u^2+u	u^2	$u+1$

（注：显然该题还有一种答案，取 u 为 x^3+x^2+1（也是不可约多项式）的根）

5.4.2 列出 $\mathbb{F}_2$ 上全部次数 $\leqslant 4$ 的不可约多项式，列出 $\mathbb{F}_3$ 上全部 2 次不可约多项式.

解. $\mathbb{F}_2$ 中次数 $\leqslant 2$ 的不可约多项式已在**习题 5.4.1** 列出.

对 3 次情况，$x^8-x=\prod_{d|r}\prod_{\substack{f\text{首一不可约}\\ \deg f=d}} f(x) = x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1) = x(x-1)(x^3+x+1)(x^3+x^2+1)$，我们在**习题 5.4.1** 已经知道 $g(x)=x^3+x+1$ 是不可约多项式，$x^3+x^2+1=g(x+1)$ 也是不可约多项式，故 $g(x)$ 和 $g(x+1)$ 是全部的 3 次不可约多项式.

对 4 次情况，$x^16-x=\prod_{d|r}\prod_{\substack{f\text{首一不可约}\\ \deg f=d}} f(x) = x(x^15-1) = x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^8-x^7+x^5-x^4+x^3-x+1) = x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$，该结果中若 4 次式可约，则必有一次或二次因子，但所有的一、二次因子已经出现在 x^16-x 中，这导致 x^16-x 有重复的不可约因子，矛盾，故 $x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$ 是全部的 4 次不可约多项式.

对 $\mathbb{F}_3$，$x^9-x=\prod_{d|r}\prod_{\substack{f\text{首一不可约}\\ \deg f=d}}f(x)=x(x^8-1)=x(x-1)(x+1)(x^2+1)(x^4+1)=x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$，由于所有的一次因子已经出现，故 x^2+1,x^2+x+2,x^2+2x+2 是全部的 $\mathbb{F}_3$ 中 2 次不可约多项式.

5.4.3 设 p,l 为素数，n 为正整数，试求 $\mathbb{F}_p[x]$ 中 l^n 次首一不可约多项式的个数.

解. $x^{p^{l^n}}-x=\prod_{d|l^n}\prod_{\substack{f\text{首一不可约}\\ \deg f=d}}f(x)=\prod_{d|l^{n-1}}\prod_{\substack{f\text{首一不可约}\\ \deg g=d}}g(x)\prod_{\substack{f\text{首一不可约}\\ \deg f=l^n}}f(x)=x^{p^{l^{n-1}}}-x\prod_{\substack{f\text{首一不可约}\\ \deg f=l^n}}f(x)$，令 $|f_i(x)|=a$，则比较两边次数可得 $p^{l^n}=p^{l^{n-1}}al^n$，故 $a=\frac{p^{l^n}-p^{l^{n-1}}}{l^n}$.

5.4.4 设 $u_1^2=2,u_2^2=3$，求 u_1+u_2 在 $\mathbb{Q},\mathbb{F}_5,\mathbb{F}_7$ 上的最小多项式.

解. 由**习题 5.1.3(1)** 知 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}$ 上的最小多项式为 $x^4-10x^2+1=(x^2-2\sqrt{2}x-1)(x^2+2\sqrt{2}x-1)=(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$，故无论 u_1,u_2 的正负性 $x^4-10x+1$ 都是它在 $\mathbb{Q}$ 上的最小多项式.

对 $\mathbb{F}_5$，由**例 5.44** 得最小多项式为 x^2-3 或 x^2-2.

对 $\mathbb{F}_7$，由**例 5.44** 得最小多项式为 $x^2\pm x-1$.

5.4.5 设 p 为素数，u_1 和 u_2 为 $\mathbb{F}_p$ 的代数闭包 $\overline{\mathbb{F}}_p$ 中的元素且 $u_1^2=2,u_2^2=3$. 试对所有的 p，求 $[\mathbb{F}_p(u_1,u_2):\mathbb{F}_p]$.

解. $[\mathbb{F}_p(u_1:\mathbb{F}_p]\leqslant 2,\mathbb{F}_p(u_2:\mathbb{F}_p]\leqslant 2$，我们分四种情况讨论.

(i) $[\mathbb{F}_p(u_1:\mathbb{F}_p]=[\mathbb{F}_p(u_2:\mathbb{F}_p]=1$，此时易见 $[\mathbb{F}_p(u_1,u_2):\mathbb{F}_p]=1$，并且这种情况当且仅当 $x^2=2,x^3=3$ 在 $\mathbb{F}_p$ 中有解，即勒让德符号 $\left(\frac{2}{p}\right)_{\mathrm{Le}}=\left(\frac{3}{p}\right)_{\mathrm{Le}}=1,0$，或 $p=2$，此时有 $p\equiv 1,7 \mod 8$ 且（$p\equiv 1,11 \mod 12$ 或 $p=3$）或 $p=2$，即 $p\equiv 1,23 \mod 24$ 或 $p=2$.

(ii) $[\mathbb{F}_p(u_1:\mathbb{F}_p]=2,[\mathbb{F}_p(u_2:\mathbb{F}_p]=1$，此时易见 $[\mathbb{F}_p(u_1,u_2):\mathbb{F}_p]=2$，并且这种情况当且仅当勒让德符号 $\left(\frac{2}{p}\right)_{\mathrm{Le}}=-1,\left(\frac{3}{p}\right)_{\mathrm{Le}}=1,0$，此时有 $p\equiv 3,5 \mod 8$ 且（$p\equiv 1,11 \mod 12$ 或 $p=3$），即 $p\equiv 11,13 \mod 24$ 或 $p=3$.

(iii) $[\mathbb{F}_p(u_1:\mathbb{F}_p]=1,[\mathbb{F}_p(u_2:\mathbb{F}_p]=2$，此时易见 $[\mathbb{F}_p(u_1,u_2):\mathbb{F}_p]=2$，且这种情况当且仅当勒让德符号 $\left(\frac{2}{p}\right)_{\mathrm{Le}}=1,0,\left(\frac{3}{p}\right)_{\mathrm{Le}}=-1$，此时有 $p\equiv 1,7 \mod 8$ 且 $p\equiv 5,7 \mod 12$，即 $p\equiv 7,17 \mod 24$.

(iv) $[\mathbb{F}_p(u_1:\mathbb{F}_p]=2,[\mathbb{F}_p(u_2:\mathbb{F}_p]=2$，此时 $2,3$ 都是二次非剩余，我们证明 $[\mathbb{F}_p(u_1,u_2):\mathbb{F}_p]=2$ 即 $u_2\in\mathbb{F}_p(u_1)$. 由于 $\mathbb{F}_p(u_1)$ 中元素均为 au_1+b $(a,b\in\mathbb{F}_p)$ 的形式，故该条件即为关于 a,b 的方程 $(au_1+b)^2\equiv 3$ 有解，即 $2a^2+b^2+2abu_1\equiv 3$，由于 $u_1\notin\mathbb{F}_p$，故 $2ab\equiv 0$，$a\equiv 0$ 或 $b\equiv 0$，前者推出 $b^2\equiv 3$，矛盾，故 $b\equiv 0,2a^2\equiv 3,a^2\equiv 3(p+1)/2$，若 $3(p+1)/2$ 是二次非剩余，则由 2 是二次非剩余知 $3(p+1)$ 是二次剩余，即 3 是二次剩余，矛盾. 故 $3(p+1)/2$ 是二次剩余，a 有 $\mathbb{F}_p$ 中的解. 此时有 $p\equiv 3,5 \mod 8$ 且 $p\equiv 5,7 \mod 12$，即 $p\equiv 5,19 \mod 24$.

综上，$[\mathbb{F}_p(u_1,u_2):\mathbb{F}_p]=1$ 当且仅当 $p\equiv 1,23 \mod 24$ 或 $p=2$，其他时候 $[\mathbb{F}_p(u_1,u_2):\mathbb{F}_p]=2$.

5.4.6 设 p 是素数.

(1) 证明 $f(x^p)=f(x)^p$ 对任意 $f(x)\in\mathbb{F}_p[x]$ 成立.

证明. 由费马小定理，$a=a^p$ 对 $\mathbb{F}_p[x]$ 中所有的常值多项式成立，又 $x^p=x^p$，故 x 也满足条件. 若 $f(x),g(x)$ 满足条件，则 $f(x^p)+g(x^p)=f(x)^p+g(x)^p=\sum_{i=0}^{p}\binom{p}{i}f(x)^ig(x)^{p-i}=(f(x)+g(x))^p$，故 $f(x)+g(x)$ 也满足条件，同时 $f(x^p)g(x^p)=f(x)^pg(x)^p=(f(x)g(x))^p$，故 $f(x)g(x)$ 满足条件，由此推出结论. □

(2) 设整数 $m\geqslant n\geqslant 0$. 证明：$\binom{pm}{pn}\equiv\binom{m}{n} \mod p$.

证明. 令 $f(x)=(x+1)^m$，则我们有 $(x^p+1)^m\equiv(x+1)^pm \mod p$，左边 pn 次项系数为 $\binom{m}{n}$，右边 pn 次项系数为 $\binom{pm}{pn}$，故得结论. □

5.4.7 设 $f(x)$ 是 $\mathbb{F}_p[x]$ 中首一不可约多项式.

(1) 若 u 为 $f(x)$ 的一个根，则 $f(x)$ 共有彼此不同的 $n=\deg f$ 个根，并且它们为 $u,u^p,u^{p^2},\cdots,u^{p^{n-1}}$；

证明. 参见**定理 5.42** 的注记. □

(2) 若 $f(x)$ 的一个根 u 为域 $F=\mathbb{F}_p(u)$ 的乘法循环群 $F^\times$ 的生成元，则 $f(x)$ 的每个根也都是 $\mathbb{F}^\times$ 的生成元，这样的多项式称为 $\mathbb{F}_p[x]$ 中的**本原多项式**.

证明. 由于 $\tau:x\mapsto x^p$ 是 F 的自同构，$\tau^j:x\mapsto x^{p^j}$ $(0\leqslant j<n)$ 也是 F 的自同构，生成元在 τ^j 下的像和原像都是生成元，由 u 是生成元即得结论. □

(3) 证明 $\mathbb{F}_p[x]$ 中 n 次本原多项式共有 $\varphi(p^n-1)/n$ 个，其中 φ 是欧拉函数.

证明. $\mathbb{F}^\times\cong\mathbb{Z}/(p^n-1)\mathbb{Z}$，其生成元即 $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ 中的元素，有 $\varphi(p^n-1)$ 个，它们都是 n 次本原多项式的根，各 n 次本原多项式的乘积是 $x^{p^n}-x$ 的因子，后者在 $\mathbb{F}_p$ 的代数闭包中无重根，故 $\varphi(p^n-1)$ 个生成元可以 n 个分成一组（按照所属本原多项式），故本原多项式共有 $\varphi(p^n-1)/n$ 个. □

5.4.8 当 $n\geqslant 3$ 时，$x^{2^n}+x+1$ 是 $\mathbb{F}_2[x]$ 中可约多项式.

证明由文献 [27] 给出.

证明. 我们证明 $x^{2^n}+x+1$ 的不可约因子为 k 次其中 $k\mid 2n$.

设 a 是 $x^{2^n}+x+1$ 的任何一个根，则 $a^{2^n}\equiv a+1, a^{2^{2n}}\equiv(a+1)^{2^n}\equiv(a^{2^n})+1\equiv a+1+1\equiv a$（注：$(a+1)^2\equiv a^2+1,(a+1)^4\equiv(a^2+1)^2\equiv(a^2)^2+1\equiv a^4+1$，依次类推即得 $(a+1)^{2^n}\equiv a^{2^n}+1$），故 $x^{2^n}+x+1$ 的所有根都满足 $a^{2^{2n}}=a$，故它们在 $\mathbb{F}_{2^{2n}}$ 中，因此 $k=[\mathbb{F}_2(a):\mathbb{F}_2]\mid[\mathbb{F}_{2^{2n}}:\mathbb{F}_2]=2n$.

当 $n\geqslant 3$ 时，$2n<2^n$，故 $k<2^n$，$x^{2^n}+x+1$ 有低于 2^n 次数的不可约因子，为可约多项式. □

5.4.9

(1) 证明 x^4+x+1 为 $\mathbb{F}_2$ 中本原多项式.

证明. 令 a 是 $f(x)=x^4+x+1$ 的根，则 $a^{15}=1, a\neq 1$，要使 a 为生成元只需证明对 $b\mid 15, b\neq 15$，$a^b\neq 1$ 即可.

若 $a^3=1$，则 $a^3-1=0$，与最小多项式次数为 4 矛盾.

若 $a^5=1$，则 $a^2+a-1=0$，仍与最小多项式次数为 4 矛盾. □

(2) 列出 16 元域 $\mathbb{F}_16=\mathbb{F}_2[u]$ 中唯一的 4 元子域的全部元素，这里 u 是 $x^4+x+1\in\mathbb{F}_2[x]$ 的一个根.

解. 4 元子域中的元素 b 满足 $b^3=1$，故该子域的乘法群为 $\mathbb{F}_16$ 的 15 阶乘法循环群的 3 阶循环子群.

故满足条件的 b 为 $1,u^5,u^10$，它们与 0 共同构成 4 元子域的全部元素.

(3) 求出 u 在 $\mathbb{F}_4$ 上的最小多项式.

解. 令 $b=u^5$，则 $b=u(u^4)=u^2+u$，u 是 x^2+x+b 的根，且 $[\mathbb{F}_{16}\mathbb{F}_4]=2$，故 x^2+x+b 是 u 在 $\mathbb{F}_4$ 上的最小多项式.

5.4.10

(1) 证明 $x^4+x^3+x^2+x+1$ 为 $\mathbb{F}_2[x]$ 中不可约多项式但不是本原多项式.

证明. 不可约性在**习题 5.4.2** 已证. 由于 $x^4+x^3+x^2+x+1\mid x^5-1$，故它的根都满足 $x^5=1$，不是 $\mathbb{F}_{2^4}$ 的 15 阶乘法循环群里的生成元. □

(2) 令 u 为 $x^4+x^3+x^2+x+1\in\mathbb{F}_2[x]$ 的一个根，试问 $\mathbb{F}_{16}=\mathbb{F}_2(u)$ 中哪些元素是 $\mathbb{F}_{16}-\{0\}$ 的乘法生成元?

解. 这些元素 a 需要不是单位且 $a^3\neq1,a^5\neq1$. 显然 $u,u^2,u^3,u^4=u^3+u^2+u+1$ 不满足 $a^5\neq1$. $(u^3+u^2)^3=u^9+3u^8+3u^7+u^6=1$，故它不满足 $a^3\neq1$，其平方 $(u^3+u^2)^2=u^4+u$ 也不满足.

故 $\mathbb{F}_{16}$ 中元素除 $0,1,u,u^2,u^3,u^4,u^3+u^2,u^4+u$ 外都是乘法群的生成元.

5.4.11 设 F 是有限域，$a,b\in F^\times$. 求证：对每个 $c\in F$，方程 $ax^2+by^2=c$ 在域 F 中均有解 (x,y).

证明. 若 F 的特征 p 为奇素数，则由 $x^2=y^2,x\neq y\Leftrightarrow x=-y$ 知 F 中乘法群元素可以依其平方两两配对，故再加上零有 $|C|=|\{x^2\mid x\in F\}|=(|F|-1)/2+1=(|F|+1)/2$，由于 a,b 在 $F^\times$ 中可逆，$z\mapsto az,z\mapsto bz$ 为 F 到自身的双射，令 $A=\{ax^2\mid x\in F\},B=\{by^2\mid y\in F\}$，则 $|A|=|B|=(|F|+1)/2,|A|+|B|>|F|$,由**习题 1.2.17**(考虑加法群),$F=A+B=\{ax^2+by^2\mid x,y\in F\}$，故得结论.

若 F 的特征为 2，则 $x^2=y^2$ 必然导致 $x=y$，故 $|F|$ 个不同元素平方也是 $|F|$ 个不同元素，$|C|=|\{x^2\mid x\in F\}|=|F|$，同上推理得到 $|A|=|B|=|F|,|A|+|B|>|F|$，同样得到结论. □

5.4.12 证明多项式 $f(x)=x^3+x+1$ 和 $g(x)=x^3+x^2+1$ 在 $\mathbb{F}_2[x]$ 上是不可约的. 设 K 是通过添加 f 的一个根得到的 $\mathbb{F}_2$ 的扩域，L 是添加 g 的一个根得到的扩域，具体描述一个从 K 到 L 的同构.

解. 由**习题 5.4.2**，我们已经有不可约性只需找出 $\mathbb{F}_2(u),f(u)=0$ 的一个元素 v，它的最小多项式是 $g(x)$，令同构为 $u\mapsto v$ 即可.

由于 $(x+1)^3+(x+1)^2+1=x^3+x^2+x+1+x^2+1+1=x^3+x+1=0$，故 $x+1$ 的一个化零多项式为 $g(y)=y^3+y^2+1$，该多项式是不可约的，因此是 $x+1$ 的最小多项式，即 $x\mapsto x+1$ 是 K 到 L 的同构.

5.4.13 设 K 是有限域，证明 K 中非零元素的乘积为 -1.

证明. 在**习题 1.3.5** 中令 $G = K^\times$，则所求乘积为所有平方为 1 的元素的乘积.

若 $\mathrm{char}K \neq 2$，则 $a^2 = 1 \Leftrightarrow (a-1)(a+1) = 0 \Leftrightarrow a = 1$ 或 -1，两者乘积为 -1.

若 $\mathrm{char}K = 2$，则 $a^2 = 1 \Leftrightarrow (a-1)^2 = 0 \Leftrightarrow a = 1$，乘积中只有 1 一个元素故为 1，但 $-1 = 1$，我们仍有结论. □

5.4.14 在域 $\mathbb{F}_3$ 上分解 $x^9 - x$ 和 $x^{27} - x$.

解. 在**习题 5.4.2** 中我们已经得到 $x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$.

$x^{27} - x = x(x+1)(x+2)\prod_i g_i(x)$，其中 $g_i(x)$ 是全部 3 次不可约多项式，由于三次多项式若可约则有一次因式，故 $0, 1, 2$ 均不是 $g_i(x)$ 的根 $\Leftrightarrow g_i(x)$ 不可约.

令 $g_i(x) = x^3 + ax^2 + bx + c$，则 $c \neq 0, 1 + a + b + c \neq 0, 2 + a + 2b + c \neq 0$. 解得 $g_i(x) = x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+1, x^3+2x^2+x+1, x^3+2x^2+2x+2$（这些即是 $x^{27} - x$ 的所有非一次不可约因子，因子分解式不再重复）

5.4.15 设 p 为素数，F 是 p^n 元域，$G = \mathrm{Aut}(F)$. 对于每个 $a \in F$，令

$$\mathrm{Tr}(a) = \sum_{\sigma \in G} \sigma(a), N(a) = \prod_{\sigma \in G} \sigma a.$$

证明:

(1) $\mathrm{Tr} : F \to \mathbb{F}_p$ 是加法群的满同态.

证明由文献 [4] 给出.

证明. 我们首先证明 Tr 是良好定义的. 若 a 在 $\mathbb{F}_p$ 上的最小多项式为 d 次，则 $d \mid n$ 且 $[\mathbb{F}_p(a) : \mathbb{F}_p] = d, a \in \mathbb{F}_{p^d}, a^{p^d} = a$，记 $\tau : x \mapsto x^p$，则 τ 是 G 的生成元，$\mathrm{Stab}_G(a) = \langle \tau^d \rangle$，$\mathrm{Tr}(a) = n/d \sum_{\sigma \in G/\mathrm{Stab}_G(a)} \sigma(a)$ 为 a 的 $\mathbb{F}_p$ 上最小多项式的所有根的和的 n/d 倍，故为 a 的 $\mathbb{F}_p$ 上最小多项式的次项系数的 $-n/d$ 倍，它必然在 $\mathbb{F}_p$ 中.

如果 $\mathrm{im}\,\mathrm{Tr}$ 不是平凡群，则它只能是 $\mathbb{F}_p$，我们即得到结论. 由于 $\sigma = \tau^k, k = 0, 1, \cdots, n-1$，故对 F 中乘法群的生成元 u，$\mathrm{Tr}(u)$ 是 u 的 p^{n-1} 次多项式，该多项式至多有 p^{n-1} 个根，若它等于 0，则它有 $|F| = p^n$ 个根，矛盾，故它不为 0，$\mathrm{im}\,\mathrm{Tr}$ 不是平凡群. □

(2) $N : F^\times \to \mathbb{F}_p^\times$ 是乘法群的满同态.

证明由文献 [14] 给出.

证明. 任取 $F^\times$ 的生成元 a，则 $N(a) = a^{1+p+\cdots+p^{n-1}} = a^b$ 其中 $b = \frac{p^n-1}{p-1}$，故 $N(a)$ 在 $F^\times$ 的阶为 $p-1$，$N(a)^p = N(a)$，由**定理 5.42** 这意味着 $N(a) \in \mathbb{F}_p - \{0, 1\}$，故 $\langle N(a) \rangle = (\mathbb{F}_p)^\times$，$N$ 是满同态. □

5.4.16 设 F 为 $q = p^n$ 元域，p 为素数. H 是 $\mathrm{Aut}(F)$ 的 m 阶子群. $K = \{a \in F \mid \text{对每个}\sigma \in H, \sigma(a) = a\}$. 证明:

(1) $m \mid n$;

证明. 只需留意 $\mathrm{Aut}(F) = \mathbb{Z}/n\mathbb{Z}$ 即可. □

(2) K 是 F 中唯一的 $p^{n/m}$ 元子域.

证明. $\mathrm{Aut}(K) = G/H = \mathbb{Z}/(n/m)\mathbb{Z}$. 故 K 是 F 中的 $p^{n/m}$ 元子域. 由于 F 的代数闭包中只有唯一的 $p^{n/m}$ 元子域（**定理 5.42(2)**），故有唯一性. □

5.4.17 设 F 为 $q = p^n$ 元域. p 为素数. $f(x)$ 为 $F[x]$ 中不可约多项式. 证明：

(1) $f(x)$ 有重根当且仅当存在 $g(x) \in F[x]$，使得 $f(x) = g(x^p)$；

证明. （⇒）与**引理 6.12** 的证明完全一致，本书不再赘述.

（⇐）由于 $F^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$，且 $\gcd(p, q-1) = 1$，故 p 在 $\mathbb{Z}/(q-1)\mathbb{Z}$ 内可逆，记为 p^{-1}，则对任意 $a \in F^\times$，有 $a^{q-1} = 1, (a^{p^{-1}})^p = a^{1+k(q-1)} = a(a^{q-1})^k = a$，即存在 $b = a^{p^{-1}}$ 使得 $b^p = a$. 令 $g(x^p) = \sum_{i=0}^n a_{pi}x^{pi}$，则 $g(x^p) = \sum_{i=0}^n b_{pi}^p x^{pi} = (\sum_{i=0} b_{pi}x^i)^p$，由于 $p \geqslant 2$，故该多项式有重根，且所有的根至少为 p 重. □

(2) 如果 $f(x) = g(x^{p^n})$，其中 $g(x) \in F[x]$，但是不存在 $\tilde{g}(x) \in F[x]$ 使得 $f(x) = \tilde{g}(x^{p^{n+1}})$，则 $p^n \mid m = \deg f$，并且 $f(x)$ 共有 m/p^n 个不同的根，每个根的重数均为 p^n.

证明. 由于 F 中任何元素都满足 $a^{p^n} = a$ 且 $\binom{p^n}{i}$ $(1 \leqslant i \leqslant p^n) \equiv 0 \mod p$，故类似**习题 5.4.6(1)** 的证明我们有 $f(x) = (g(x))^{p^n}$，且由条件可知 $g(x)$ 不满足 $g(x) = h(x^p)$，故 $g(x)$ 无重根，$f(x)$ 的每个根重数都为 p^n，故共有 m/p^n 个根. □

5.4.18 线性代数

第六章　伽罗瓦理论

6.1 伽罗瓦理论的主要定理

6.1.1 设 $F=\mathbb{F}_q$ 为 q 元有限域，$\gcd(n,q)=1$，E 为 x^n-1 在 F 上的分裂域. 证明 $[E:F]$ 等于满足 $n\mid q^k-1$ 的最小整数 k.

证明. x^n-1 一定有根在 E 的乘法群上阶为 n，而 E 的乘法群为 $q^{[E:F]}-1$ 阶，故 $n\mid q^{[E:F]}-1$. 另一方面，令 k 满足 $n\mid q^k-1$，则 $\mathbb{F}_{q^k}$ 上有 n 个元素（记该域的乘法群生成元为 a，则 $a^{q^k-1/n}$ 生成的乘法子群有 n 个元素满足 $x^n-1=0$，故 x^n-1 在该域上分裂.

若存在异于 $\mathbb{F}_{q^k}$ 的另一个域 $\mathbb{F}_{q^l}$ 使得 x^n-1 在该域上也分裂，则 $n\mid q^l-1$，故 $n\mid q^l-q^k$，$n\mid q^{l-k}-1$. 但 $q^k\equiv 1 \mod n$ 且 $1<s<k$ 时 $q^s\not\equiv 1 \mod n$，故 $q^r\equiv 1 \mod n$ 当且仅当 $k\mid r$，故 $k\mid l-k$，$k\mid l$，由**定理 5.42(6)**，$\mathbb{F}_{q^l}\supseteq\mathbb{F}_{q^k}$，故 $\mathbb{F}_{q^k}$ 是 x^n-1 在 F 上的分裂域. □

6.1.2 设 F 为域，$f(x)$ 为 $F[x]$ 中 n 次多项式，E 为 $f(x)$ 在 F 上的分裂域. 求证：$[E:F]\mid n!$.

证明由文献 [7] 给出.

证明. 当 $n=1$ 时，结论显然成立. 假设我们对 $n<k+1$ 有结论成立，对 $n=k+1$ 的情况，对 f 的可约性分情况讨论：

若 f 可约，令 $g(x)$ 为 f 的一个不可约因子，$\deg g=u,\deg f/g=k+1-u$，则 $u,k+1-u\leqslant k$. 令 L 是 g 在 F 上的分裂域，则 K 是 f/g 在 L 上的分裂域（请读者自行将 g 和 f/g 写作 K 中的因式分解证明这一点），故有 $[L:F]\mid u!,[K:L]\mid (k+1-u)!$，但 $(k+1)!/u!(k+1-u)!=\binom{k+1}{u}$ 为整数，故 $[K:F]\mid u!(k+1-u)!\mid k!$.

若 f 不可约，令 $L=F[x]/(f)_{Ideal,F[x]}\cong F(\alpha)$，其中 α 是 f 的一个根，此时 $[L:F]=\deg f=k+1$，K 是 $f(x)/(x-\alpha)$ 在 L 上的分裂域，由归纳假设 $[K:L]\mid k!$，$[K:F]\mid (k+1)k!=(k+1)!$. □

6.1.3 设 E 为 x^8-1 在 $\mathbb{Q}$ 上的分裂域，求 $E/\mathbb{Q}$ 的扩张次数，并确定伽罗瓦群 $\mathrm{Gal}(E/\mathbb{Q})$.

解. x^8-1 的所有根都是 8 次本原单位根 ζ_8 的方幂，故 $E=\mathbb{Q}(\zeta_8)$，且 ζ_8 在 $\mathbb{Q}$ 上的最小多项式为 $x^4+1=0$，故 $[E:\mathbb{Q}]=4$.

对 $\mathrm{Gal}(E/\mathbb{Q})$，它将 x^4-1 的根 8 次本原单位根 ζ_8 映射到 8 次本原单位根 $\zeta_8,\zeta_8^3,\zeta_8^5,\zeta_8^7$，记这些映射为 $\mathrm{id},\tau_3,\tau_5,\tau_7$，易见 τ_i 都是 2 阶元，故 $\mathrm{Gal}(E/\mathbb{Q})\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

6.1.4 设 E/F 是域的扩张. 如果对每个元素 $\alpha\in E$，$a\notin F$，α 在 F 上均是超越元，则称 E/F 是**纯超越扩张**. 证明：

(1) $F(x)/F$ 是纯超越扩张.

证明. 对一次以上多项式 $f(x)$，若它在 F 上代数，则由于它不在 F 内，存在二次以上多项式 $g(x)$ 使得 $g(f(x))=0$，但 $\deg g(f(x))\geqslant 2$，矛盾. □

(2) 对于任意域扩张 E/F，存在唯一的中间域 M 使得 E/M 为纯超越扩张，而 M/F 为代数扩张.

证明. 令 M 为所有 E 中 F 上的代数元集合，易验证 M 构成域. 显然 M/F 为代数扩张，若 $E-M$ 中有元素在 M 上代数，由**定理 5.16**，该元素在 F 上也代数，与 M 的定义矛盾，故 E/M 是

纯超越扩张.

唯一性? 令 M_1 是另外一个这样的域, 显然 M_1 不含 F 上的超越元, 故 $M_1 \subseteq M$, 若 $\alpha \in M$ 但 $\alpha \notin M_1$, 则 α 在 F 上代数推出 α 在 M_1 上代数, 与 E/M_1 为纯超越扩张矛盾, 故 $M_1 = M$. □

6.1.5 证明: F 是完全域当且仅当 F 的所有有限扩张都是可分扩张.

证明. 正文对完全域的定义不包括 $\mathrm{char}F = 0$ 的情况, 但本题 (和一般的对完全域的定义) 都包括. 当 $\mathrm{char}F = 0$ 时, 结论显然成立, 以下设 $\mathrm{char}F = p$.

($\Rightarrow$) 由**命题 6.18** 立得.

($\Leftarrow$) 我们只需证明 F 中存在 α 使得不存在 $\beta^p = \alpha, \beta \in F$ 时 $F[x]$ 上存在有重根的不可约多项式即可.

考虑 $f(x) = x^p - \alpha = (x-\beta)^p$, 其中 $\beta \notin F$ 是 F 的代数闭包中元素. 若 $f(x)$ 在 $F[x]$ 上可约, 必有 $(x-\beta)^k \in F[x]$ 其中 $1 \leqslant k < p$, 故 $\beta^k \in F$, 由 $\gcd(k,p) = 1$, 必有整数 u 使得 $ku = pv + 1$, 故 $\beta = (\beta^k)^u \alpha^{-v} \in F$, 矛盾. 故 $f(x)$ 是 $F[x]$ 上不可约多项式, 它有 p 重根 β. □

6.1.6 设 F 为特征 0 域, $f(x)$ 为 $F[x]$ 中的非常值首一多项式, $d(x) = \gcd(f, f')$. 求证: $g(x) = f(x)/d(x)$ 和 $f(x)$ 有同样的根, 并且 $g(x)$ 无重根.

证明. 考虑 $f(x)$ 的任意一个根 c, 其重数为 k, 即 $f(x) = (x-c)^k h(x)$ 且 $x - c \nmid h(x)$, 故 $f'(x) = k(x-c)^{k-1}h(x) + (x-c)^k h'(x) = (x-c)^{k-1}(kh(x) + (x-c)h'(x))$, 我们有 $x - c \nmid kh(x)$, $(x-c) \nmid (kh(x) + (x-c)h'(x))$, 故 $d(x) = (x-c)^{k-1}r(x)$ 其中 $x - c \nmid r(x)$, $g(x) = (x-c)h(x)/r(x)$, 即 c 是 $g(x)$ 的根且重数为 1. □

6.1.7 本题参考**习题 5.4.17**, 本书不再赘述. (未完)

6.1.8 设 E/F 为可分扩张, M 为 E/F 的中间域, 求证 E/M 和 M/F 均是可分扩张.

证明. E 上的所有元都是 F-可分元, 故 M 上的所有元也是, 故 M/F 是可分扩张.

对 E/M, 由于 E 上元素在 M 上的最小多项式是它在 F 上的最小多项式的因子, 后者没有重根导致前者也没有, 故 E/M 也是可分扩张. □

6.1.9 设 F 为特征 $p > 0$ 域, E/F 为代数扩张, 证明对每个 $\alpha \in E$ 均存在整数 $n \geqslant 0$ 使得 α^{p^n} 在 F 上可分.

证明. 设 α 在 F 上的最小多项式为 $f(x)$, 若 $f(x)$ 无重根, 取 $n = 0$ 即可, 否则由**习题 5.4.17**, $f(x) = g(x^{p^n})$ 且不存在 $\tilde{g}(x)$ 使得 $f(x) = \tilde{g}(x^{p^{n+1}})$, 故 $g(x)$ 不满足 $g(x) = h(x^p)$, 由**习题 5.4.17(1)** 知 $g(x)$ 无重根, 但 α^{p^n} 是 $g(x)$ 的根, 故 α^{p^n} 的最小多项式整除 $g(x)$, 它也没有重根, 故得结论. □

6.1.10 设 $E = \mathbb{F}_p(x,y), F = \mathbb{F}_p(x^p, y^p)$, p 为素数. 证明:

(1) $[E:F] = p^2$;

证明. 请读者自行验证 $\{x^i y^j \mid i,j \in \mathbb{F}_p\}$ 是 E 的一组 F-基.

另一种证法：请读者验证 $t^p - x^p$ 是 x 在 F 上的最小多项式，令 $L = \mathbb{F}_p(x, y^p)$，则 $[L : F] = p$. $t^p - y^p$ 是 y 在 L 上的最小多项式，则 $[E : L] = p$. □

(2) E/F 不是单扩张.

以下 (2)(3) 由文献 [2] 给出.

证明. E 中常数满足 $\alpha^p \in F$，且 x, y 也满足该条件. 由于 $(\alpha+\beta)^p = \alpha^p + \beta^p$，故 E 中满足 $\alpha^p \in F$ 的元素构成域，这导致 E 中一切元素都满足 $\alpha^p \in F$，$[F(\alpha) : F] \leqslant p < [E : F]$，故 E/F 不是单扩张. □

(3) E/F 有无限多个中间域.

证明. 令 z 为 E 中任意非零元素，$w = x + zy$，则 $w \notin F$，$[F(w) : F] > 1$，又 $w^p = x^p + z^p y^p \in F$，故 $[F(w) : F] \leqslant p$，又 $[F(w) : F] \mid [E : F]$，只能 $[F(w) : F] = p$.

若还存在 $z' \neq z, 0$ 使得 $w' = x + z'y \in F(w)]$，则 $(z' - z)y \in F(w)$，$(z' - z) \neq 0$，故 $y \in F(w)$，又 $z^{-1}x + y \in F(w), z'^{-1}x + y \in F(w)$，同理有 $x \in F(w)$，故 $F(w) = E$，矛盾. 故不同的非零 z 导致不同的 $F(w)$，而 E 中有无限多个元素，故中间域 $F(w)$ 有无限多个. □

6.1.11

(1) 若 E/F 为代数扩张，F 为完全域，则 E 也为完全域；

证明. F 上的所有不可约多项式均无重根，由 E/F 是代数扩张，E 上的任意不可约多项式为前者中某元素的因子，故也无重根，故 E 是完全域. □

(2) 若 E/F 为有限生成扩张，E 为完全域，则 F 也为完全域.

证明. 反证法，若 F 不是完全域，则 F 的特征为 p.

由**习题 6.1.4**，存在 M 使得 E/M 是纯超越扩张而 M/F 是代数扩张. 由于 M/F 也是有限生成的，故 M/F 是有限扩张. 我们证明 M 不是完全域.

F 中存在 a 使得 $c^p = a$ 在 F 中无根. 令 $f(x) = x^{p^n} - a$. 设 $c^{p^n} = a$ 其中 c 是 F 的代数闭包中元素，$F_1 = F(c)$，由于 $(a \pm b)^p = a^p \pm b^p, (a \pm b)^{p^n} = a^{p^n} + b^{p^n}$，故 $f(x) = (x - c)^{p^n}$. 设 $g(x)$ 是 c 在 F 上的最小多项式，则 $g(x) = (x - c)^r$，若 $r \nmid p^n$ 则存在整数 s 使得 $p^n = rs + t, 0 < t < r$，故 $(x - c)^t = f(x)g(x)^{-s}$ 也是 $f(x)$ 的 F 上不可约分解式中元素，与 $g(x)$ 的定义矛盾. 故 $r \mid p^n$，$r = p^d$. $g(x) = (x - b)^{p^d} = x^{p^d} - b^{p^d}, b^{p^d} \in K$，若 $d \neq n$，则 $(b^{p^d})^{p^{n-d-1}} \in K$ 是 $c^p = a$ 的根，矛盾，故 $d = n$，$f = g$ 是不可约多项式.

若 M 是完全域，a 必有 $p, p^2, \cdots, p^n$ 次方根，故 $b \in M$，$f(x)$ 是 b 的 F 上最小多项式，故 $[M : F] \geqslant \deg f = p^n$，但 $[M : F]$ 有限，与 n 的任意性矛盾，故 M 不是完全域.

令 $a \in M$ 使得 $c^p = a$ 在 M 中无根，若它在 E 中有根 a，则 c 在 M 上代数，与 E/M 是纯超越扩张矛盾. 而 $a \in E$，故 E 不是完全域，矛盾.

综上，E 为完全域则 F 也为完全域. □

注记. 若 g 是 f 的所有根的最小多项式，则 $f = ug^m$，其中 u 是常数. 理由如下：

$f = u_1 \prod_i (x-\alpha_i)^{k_i}$, 设 m 是使得 $g^m \mid f$ 的最大整数, $f/g^m = u_2 \prod_i (x-\alpha_i)^{l_i}$, 若 $l_j \neq 0$, 则 f/g^m 是 α_j 的化零多项式, $g \mid f/g^m, g^{m+1} \mid f$, 矛盾. 故 $f/g^m = u_2$.

(3) 若 E/F 为代数扩张（不必为有限扩张）, 问 (2) 中结论是否成立?

解. 否, 取任何非完全域 F 的代数闭包 E, E/F 是代数扩张, E 是代数封闭域, 故由完全域的定义它必然是完全域, 这就否证了 (2) 的结论.

6.1.12 设 $E = \mathbb{Q}(\alpha)$, 其中 $\alpha^3 + \alpha^2 + 2\alpha - 1 = 0$, 证明:

(1) $\alpha^2 - 2$ 也是 $x^3 + x^2 - 2x - 1 = 0$ 的根.

证明. $\alpha^3 = -\alpha^2+2\alpha+1$. α^2-2 代入方程即得左边 $= a^6-5a^4+6a^2-1 = (a^3)(a^3)-5a(a^3)+6a^2-1 = a^4+a^3-2a^2-a = 0 \cdot a = 0$. □

(2) $E/\mathbb{Q}$ 是正规扩张.

证明. x^3+x^2-2x-1 在 $\overline{\mathbb{Q}}$ 中只有 3 个根, 令 $f(x) = x^3+x^2-2x-1$, 则 $g(x) = f'(x) = 3x^2+2x-1$, $\gcd(f, f' = 1$, f 无重根, 故 $\alpha \neq \alpha^2 - 2$, 且设 f 的另一个根为 β, 则 $\beta + \alpha + (\alpha^2 - 2) = -1$（次项系数乘以 -1）, 故 $\beta \in E$, $E/\mathbb{Q}$ 是正规扩张. □

6.1.13 设 E/F 和 K/F 都是正规扩张, 求证 EK/F 也是正规扩张.

证明利用了文献 [16] 的思想, 但引理由作者完成, 文献中并未证明.

证明. **引理**. 设 K/F 为代数扩张, α 的 F-共轭元都在 K 中, β 的 F-共轭元也都在 K 中, 则 $u\alpha$ ($u \in F^\times$) 和 $\alpha + \beta$ 的共轭元也都在 K 中.

证明. 设 α 在 F 上的最小多项式为 $f(x) = \prod_{i\in I}(x-\alpha_i) \in F[x]$, 其中 $\alpha_1 = \alpha, \alpha_i$ 不一定两两不同, 则 α_i 都在 K 中.

β 在 F 上的最小多项式为 $g(x) = \prod_{j\in J}(x-\beta_j) \in F[x]$, 其中 $\beta_1 = \beta, \beta_j$ 不一定两两不同. 则 β_j 都在 K 中.

则 $f(x/u) = \prod_i (x/u - \alpha_i) = u^{-|I|} \prod_i (x - u\alpha_i)$ 是 $u\alpha$ 在 $F[x]$ 上的化零多项式, 故 $u\alpha$ 的 F-共轭元只可能是 $u\alpha_i$, 它在 K 中.

考虑 $h(x) = \prod_{i\in I, j\in J}(x - (\alpha_i + \beta_j))$, 则它的任何项的系数 h_i 在 I 到自身的置换和 J 到自身的置换下均不变.

故 $h_i \in F(\{\alpha_i\})(\{\beta_j\})$ 是 $\{\alpha_i\}$ 的对称多项式, 即为 α_i 的初等对称多项式的 $F(\{\beta_j\})$ 系数多项式, 但 α_i 的初等对称多项式都是 $f(x)$ 的系数, 故 $h_i \in F(\{\beta_j\})$, 它还是 $\{\beta_j\}$ 的对称多项式, 即为 β_j 的初等对称多项式的 F 系数多项式, 但 β_j 的初等对称多项式都是 $g(x)$ 的系数, 故 $h_i \in F$, $h(x) \in F[x]$ 是 $\alpha + \beta$ 的化零多项式, 故 $\alpha + \beta$ 的 F-共轭元只可能是 $\alpha_i + \beta_j$, 它在 K 中. □

令 $\{x_1, \cdots, x_n\}$ 为 E 的一组 F-基, $\{y_1, \cdots, y_m\}$ 为 K 的一组 F-基, 则 $\{x_i y_j \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$ 是 EK 的一组 F-向量空间生成元, x_i 和 y_j 的 F-共轭元都在 EK 中, 故由引理 EK 中所有元素的 F-共轭元都在 EK 中, EK/F 也是正规扩张. □

6.1.14

(1) 如果 E/M 和 M/F 均是域的正规扩张，试问 E/F 是否一定为正规扩张?

证明由文献 [1][19] 给出.

解. 否，令 $F=\mathbb{Q}, M=\mathbb{Q}(\sqrt{2}), E=\mathbb{Q}(\sqrt[4]{2})$，由于这些域的特征都是 0，故非伽罗瓦扩张都不是正规的.

易见 $[M:F]=2,[E:M]=2$，且 $\sigma_1:\sqrt{2}\mapsto-\sqrt{2}, \sigma_2:\sqrt[4]{2}\mapsto-\sqrt[4]{2}$ 各是 $\mathrm{Gal}(M/F), \mathrm{Gal}(E/M)$ 的非单位元，故 $|\mathrm{Gal}(M/F)|=|\mathrm{Gal}(E/M)|=2$，$M/F$ 和 E/M 都是伽罗瓦扩张，故是正规扩张.

考虑 E 的 F-自同构 τ，它由 $\tau(\sqrt[4]{2})$ 唯一确定，由于 $a\tau(\sqrt[4]{2})^4=\tau(2)=2$，故 $a^4=2$，但 $E\subseteq\mathbb{R}$ 且这方程只有两个实根 $\pm\sqrt[4]{2}$，故 $|\mathrm{Gal}(E/F)|=2<4$，E/F 不是伽罗瓦扩张，故不是正规扩张.

注记. 事实上，x^4-2 在 $\mathbb{Q}$ 上的分裂域为 $L=\mathbb{Q}(i,\sqrt[4]{2})$，可以证明 x^4-2 在 $\mathbb{Q}(i)$ 上也不可约，故 $[L:\mathbb{Q}(i)]=4, [L:F]=4[\mathbb{Q}(i):F]=8\neq[E:F]$.

(2) 如果 E/F 是正规扩张，M 是它们的中间域，试问 E/M 和 M/F 是否为正规扩张?

解. 前者是，后者否. E/F 正规，故对任意 $\alpha\in E$，α 在 F 上的最小多项式 $f(x)$ 在 E 上分裂，令 $g(x)$ 为 α 在 M 上的多项式，则 $g(x)\mid f(x)$，故它也在 E 上分裂，E/M 为正规扩张.

对于后者，令 $F=\mathbb{Q}$，E 是 x^3-2 在 F 上的分裂域 $\mathbb{Q}(\sqrt[3]{2},\omega)$ 其中 ω 为 3 次本原单位根. 令 $M=\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{R}$ 则它是中间域，并且 $\sqrt[3]{2}$ 的 F-共轭元 $\sqrt[3]{2}\omega$ 不在 M 中，M/F 不是正规扩张.

6.1.15 设 E/F 为代数扩张，证明 E/F 为正规扩张当且仅当对于 $F[x]$ 中任意不可约多项式 $f(x)$，$f(x)$ 在 $E[x]$ 中的所有不可约因子都有相同的次数.

证明. ($\Leftarrow$) 若 $\alpha\in E$，则 α 在 $F[x]$ 上的最小多项式在 $E[x]$ 上有一次因式 $(x-\alpha)$，故在 $E[x]$ 上所有因式都是一次因式，即 $f(x)$ 在 E 上分裂，故 E/F 为正规扩张.

以下由文献 [18] 给出.

($\Rightarrow$) 设 $f(x)$ 为任意一个 $F[x]$ 中不可约多项式，L 为 $f(x)$ 的分裂域，$f(x)$ 在 $E[x]$ 上的不可约分解为 $uq_1(x)\cdots q_m(x)$（由于 $f(x)$ 乘除非零常数不影响结论，我们不妨假定 $f(x)$ 首一，$u=1$，$q_i(x)$ 也首一）

若 α 是 $q_1(x)$ 的根，β 是 $q_i(x)$ 的根，则 q_1 是 α 在 K 上的最小多项式，q_i 是 β 在 K 上的最小多项式.

由**引理 6.33**，存在 L 的 F-自同构 σ 使得 $\sigma(\alpha)=\beta$，由**命题 5.18**，对任意 $a\in K$，$\sigma(a)$ 与 a 有相同的最小多项式，故是 a 的 F-共轭元，$\sigma(a)\in K$，故 $\sigma(K)=K$.

考虑 $\sigma(q_1(x))\in\sigma(K[x])=K(x)$，它是 β 的化零多项式，故 $q_i(x)\mid\sigma(q_1(x))$，但 $\sigma(q_1(x))$ 也是不可约多项式，故二者次数相等，即 $\deg q_i=\deg q_1$ 对一切 $1\leqslant i\leqslant m$ 成立，故得结论. □

6.2 方程的伽罗瓦群

6.2.1 设 F 为实数域 $\mathbb{R}$ 的子域. $f(x)$ 为 $F[x]$ 中三次不可约多项式. 证明若 $D(f)>0$，则 $f(x)$ 有三个实根；若 $D(f)<0$，则 $f(x)$ 只有一个实根.

证明. F 的特征为 0，$f(x)$ 为不可约多项式，故 $f(x)$ 无重根. 令 $E=F(\alpha_1,\alpha_2,\alpha_3)$ 为 $f(x)$ 的分裂域，显然复共轭 $\tau\in\mathrm{Gal}(E/F)$，并且 $\mathrm{Gal}(E/F)$ 中元素由它在 $A=\{\alpha_1,\alpha_2,\alpha_3\}$ 上的作用唯一确定，即为 S_3 中元素. 由于 $\tau^2=\mathrm{id}$，故 τ 为 S_3 中单位元或对换.

若 $D(f)>0,\sqrt{D}\in\mathbb{R}-\{0\}$，故 $\tau(\sqrt{D})=\sqrt{D}\neq-\sqrt{D}$，若 $D(f)<0,\sqrt{D}\in i\mathbb{R}-\{0\}$，故 $\tau(\sqrt{D})=-\sqrt{D}\neq\sqrt{D}$，由于 τ 不是 3 轮换，故前者只能在 τ 为单位元时取得，即三个根都是实根，后者只能在 τ 为对换时取得，即 $\tau=(ij)$，α_i 和 α_j 为共轭虚根，另一个根被 τ 固定，只能为实根，故得结论. □

6.2.2 设 F 是特征不为 2 的域，求 $f(x)$ 在 F 上的伽罗瓦群，其中

(1) $f(x)=x^3+x+1$;

解. 题目并未给定 $f(x)$ 在 F 上不可约，我们没有能力对一切域讨论 $f(x)$ 的可约性，只能给出一般情况.

若 $f(x)$ 在 F 上有两个以上根（重根重复计算），则第三个根加前两个根为 -1，故也在 F 中，则 $f(x)$ 的分裂域即 F，显然 $\mathrm{Gal}(F/F)$ 是平凡群.

若 $f(x)$ 在 F 上有一个根（不重复）α，则 $f(x)=(x-\alpha)(x^2+\alpha x+\alpha^2+1)$，且后者是 F 上的不可约多项式，它的判别式 $D=-3/4\alpha^2-1$（题设排除了 $\mathrm{char}F=2$），若 $\sqrt{D}\in F$，则 $f(x)=(x-\alpha)(x+\sqrt{D})(x-\sqrt{D})$，与它在 F 上只有一个根矛盾，故 $f(x)$ 的分裂域为 $K=F(\sqrt{D})$ 其中 $\sqrt{D}\notin F$，此时 $\mathrm{Gal}(K/F)=\{1,\sigma\}\cong\mathbb{Z}/2\mathbb{Z}$，其中 $\sigma(\sqrt{D})=-\sqrt{D}$.

若 $f(x)$ 在 F 上无根，则它是 $F[x]$ 上不可约多项式. 由**例 6.32**，$D=-4-27=-31$，由**命题 6.30**，当 $d^2=-31$ 在 F 中无解时 $\mathrm{Gal}(K/F)\not\subseteq A_3$，又 $\mathrm{Gal}(K/F)$ 在 $\alpha_1,\alpha_2,\alpha_3$ 上作用可迁，故只能 $\mathrm{Gal}(K/F)=S_3$. 当 $d^2=-31$ 在 F 中有解时，$\mathrm{Gal}(K/F)\subseteq A_3$，又 $\mathrm{Gal}(K/F)$ 在 $\alpha_1,\alpha_2,\alpha_3$ 上作用可迁，故只能 $\mathrm{Gal}(K/F)=A_3$.

(2) $f(x)=x^3+x^2+1$;

解. F 中一个以上根的情形与 (1) 类似.

$f(x)$ 不可约时，$D=(-1)^3\prod_{i=1}3(3\alpha_i^2+2\alpha_i)=-31$，故伽罗瓦群与 (1) 的结果完全一致. 事实上，令 y 是 x^3+x^2+1 的根，则 $y\neq0$ 且 $1/y$ 是 x^3+x+1 的根，故给定任意 F，两方程的伽罗瓦群完全一致是可以理解的.

6.2.3 确定 $f(x)$ 在域 F 上的伽罗瓦群，其中

(1) $f(x)=x^4-5,F=\mathbb{Q},\mathbb{Q}(\sqrt{5})$ 和 $\mathbb{Q}(\sqrt{-5})$.

解. 易验证 $f(x)$ 的分裂域 $K=\mathbb{Q}(i,\sqrt[4]{5})$. $F_1=\mathbb{Q}$ 时, 若 $\sigma\in\mathrm{Gal}(K/F_1)$, 则 $\sigma(i)^2=\sigma(-1)=-1$, 故 $\sigma(i)=\pm i$. 由于 $a=\sqrt[4]{5}$ 是 x^4-5 的根且该方程的根为 $a,ia,-a,-ia$, 故 $\sigma(a)=a,ia,-a,-ia$. 由于 σ 由 $\sigma(i),\sigma(a)$ 唯一确定, 讨论它们之间的乘法关系即得 $\mathrm{Gal}(K/F_1)\cong D_4=\langle\sigma_a,\sigma_i\rangle$, 其中 $\sigma_i(i)=-i,\sigma_i(a)=a,\sigma_a(i)=i,\sigma_a(a)=ia$.

对 $F_2=\mathbb{Q}(\sqrt{5})$, 注意 $F_1\subseteq F_2$, 故 $\mathrm{Gal}(K/F_2)$ 是上述 $\mathrm{Gal}(K/F_1)$ 的子群, 且 $\sigma(a^2)=\sigma(\sqrt{5})=\sqrt{5}=a^2$, 故 $\sigma(a)=\pm a$, $\mathrm{Gal}(K/F_2)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}=\langle\sigma_a^2,\sigma_i\rangle$.

对 $F_3=\mathbb{Q}(\sqrt{-5})$, 同理 $\mathrm{Gal}(K/F_3)$ 是上述 $\mathrm{Gal}(K/F_1)$ 的子群, 且 $\sigma(ia^2)=\sigma(\sqrt{-5})=\sqrt{-5}=ia^2$, 故有两种情况: $\sigma(i)=i$, 此时 $\sigma(a)=\pm a$, 或者 $\sigma(i)=-i$, 此时 $\sigma(a)=\pm ia$, 故 $\mathrm{Gal}(K/F_3)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}=\langle\sigma_a\sigma_i,\sigma_a^3\sigma_i\rangle$.

(2) $f(x)=x^4-10x^2+4$, $F=\mathbb{Q}$.

解. x^2 是 $x^2-10x+4$ 的根, 故 $x^2=5\pm\sqrt{21}\notin F$. 令 $\alpha_1,-\alpha_1,\alpha_2,-\alpha_2$ 为 $f(x)$ 的四个根, K 为分裂域, $\alpha_1^2=5+\sqrt{21},\alpha_2^2=5-\sqrt{21}$, 则若 $\sigma\in\mathrm{Gal}(K/F)$, 我们有 $\sigma(-\alpha_1)=-\sigma(\alpha_1),\sigma(-\alpha_2)=-\sigma(\alpha_2)$, 故 σ 保持 $\alpha_1(-\alpha_1)$ 和 $\alpha_2(-\alpha_2)$ 或将他们交换, 即 $\sigma\in\langle(1324)(12)\rangle\cong D_8$, $\mathrm{Gal}(K/F)\cong D_8\subseteq S_4$.

(3) $f(x)=x^5-6x+3$, $F=\mathbb{Q}$.

解. 由艾森斯坦判别法 ($p=3$), $f(x)$ 是 $F[x]$ 中不可约多项式, 作图像知它有三个实根, 即两个复根, 由**定理 6.34**, $\mathrm{Gal}(K/F)\cong S_5$.

6.2.4 设 p 为素数, $a\in\mathbb{Q}$, x^p-a 为 $\mathbb{Q}[x]$ 中不可约多项式. 证明 x^p-a 在 $\mathbb{Q}$ 上的伽罗瓦群同构于 p 元域 $\mathbb{F}_p$ 上 2 阶一般线性群 $\mathrm{GL}_2(\mathbb{F}_p)$ 的子群

$$\left\{\begin{pmatrix}k&l\\0&1\end{pmatrix}\mid l\in\mathbb{F}_p,k\in\mathbb{F}_p^\times\right\}.$$

证明. x^p-a 的根为 $b\zeta_p^i$, 其中 $0\leqslant i<p,b^p=a,b^r\notin\mathbb{Q}\ (0<r<p)$. 记 $F=\mathbb{Q}$, 若 $\sigma\in\mathrm{Gal}(K/F)$ 其中 K 为 x^p-a 的分裂域, 则必有 $\sigma(b)=b\zeta_p^l\ (l\in\mathbb{F}_p)$, 并且 $\sigma(b\zeta_p^u)/\sigma(b\zeta_p^{u-1})=\sigma(\zeta_p)$, 后者是 ζ_p 的 $\mathbb{Q}$-共轭元, 故为 p 次本原单位根 $\zeta_p^k\ (k\in\mathbb{F}_p^\times)$, 故 $\sigma(b\zeta_p^u)=\sigma(\zeta_p)^u\sigma(b)=b\zeta_p^{ku+l}\ (0\leqslant u<p)$, 可验证 (详细见下) 上述映射决定了 K 的 F-自同构, 故 $\mathrm{Gal}(K/F)=\{\sigma_1\mid\sigma_1\in S_p,\sigma_1(u)\equiv ku+l\mod p,1\leqslant k<p,0\leqslant l<p\}$, 将 $\mathrm{Gal}(K/F)$ 作用在 $\mathbb{F}_p$ 中元素 u 上, 则它相当于矩阵 $\left\{\begin{pmatrix}k&l\\0&1\end{pmatrix}\mid l\in\mathbb{F}_p,k\in\mathbb{F}_p^\times\right\}$ 左乘作用在列向量 $\begin{pmatrix}u\\1\end{pmatrix}$ 上, 故我们得到题目所给的同构.

验证: 我们已经知道 $\mathrm{Gal}(K/F)\leqslant\{\sigma_1\mid\sigma_1\in S_p,\sigma_1(u)\equiv ku+l\mod p,1\leqslant k<p,0\leqslant l<p\}$, 我们需要验证等号成立, 即 $\sigma:b\zeta_p^u\mapsto b\zeta_p^{ku+l},b\mapsto b\zeta_p^l,\zeta_p\mapsto\zeta_p^k$ 是 K 的 F-自同构. 由于 $K=F(\zeta_p,b)$, K 中元素必有 $\sum_{i=0}^{p-1}b^ig_i(x)$ 的形式, 其中 $g_i(x)\in F(\zeta_p)[x]$. 由于 $f(x)$ 在 $F(\zeta_p)[x]$ 中不可约 (若不然, 则考虑其非平凡因子的常数项, 它必为 $b^n\zeta_p^r$, 其中 $1\leqslant n<p$, 我们取 b 为 x^p-a 的实根而不影响结论 (当 p 为奇素数时必然存在一个, $p=2$ 时若无实根则 $b\zeta_p^r$ 是虚数, 当然不是有理数), 则 $b^n\zeta_p^r$ 为有理数必然导致 $\zeta_p^r=\pm1,b^n$ 为有理数, 又 $b^p=a$ 为有理数, n,p 互素, 可推出 b 为有理数, 与 $f(x)$ 在有理数集中不可约矛盾)

故 $f(x)$ 在 $F(\zeta_p)[x]$ 中不可约, $1, b, \cdots, b^{p-1}$ 在 $F(\zeta_p)$ 上线性无关, 若 K 中任何元素 $\sum_{i=0}^{p-1} b^i g_i(x) \in F \subseteq F(\zeta_p)$, 则必有 $g_i(x) = 0$ $(1 \leqslant i < p)$, $g_0(x) \in F$, 故 $\sigma(\sum_{i=0}^{p-1} b^i g_i(x)) = \sigma(g_0(x))$, 由于 ζ 在 F 上的最小多项式为 $(x^p - 1)/(x - 1) = \prod_{i=1}^{p-1}(x - \zeta_p^i)$, 故 σ 在 $F(\zeta_p)$ 上的限制是 F-自同构, 故 $\sigma(g_0(x)) = g_0(x)$, 也就是 σ 是良好定义的 K 的 F-自同构. □

6.2.5 证明 $\mathbb{Q}(\sqrt[4]{2}(1 + \sqrt{-1}))$ 是四次扩张; 并求出它的伽罗瓦群.

证明. 令 $a = \sqrt[4]{2}(1 + \sqrt{-1})$, $b = \sqrt[4]{2}$, 则 a 是 $f(x) = x^4 + 8$ 的根, $f(x)$ 的有理根只可能为 $\pm 1, \pm 2, \pm 4, \pm 8$, 它们都不是根, 故 $f(x)$ 是 $\mathbb{Q}[x]$ 上不可约多项式, 是 a 的四次最小多项式, 故 $\mathbb{Q}(a)/\mathbb{Q}$ 是四次扩张 □

解. a 的 $\mathbb{Q}$-共轭元为 $x^4 + 8$ 的根 $a, ia, -a, -ia$, 我们来说明 $ia, -ia \notin K = \mathbb{Q}(a)$.

由于 $a = b(1 + i)$, 若 ia 在 K 中, 则 $a - ia = a(1 - i) = 2b$ 也在 K 中, 由于 $1, a, a^2, a^3$ 是 K 的一组基, 则 $2b = c_0 + c_1 a + c_2 a^2 + c_3 a^3 = c_0 + (1 + i)c_1 b + 2ic_2 b^2 + 2(i - 1)c_3 b^3$, 其中 $c_i \in \mathbb{Q}$. 易验证 $x^4 - 2$ 是 $\mathbb{Q}[x]$ 上不可约多项式, 故 $1, b, b^2, b^3$ 在 $\mathbb{Q}$ 上线性无关, 得 $2b = (1 + i)c_1$, 与 c_1 是有理数矛盾. 故 ia 不在 K 中, 易知 $-ia$ 也不在 K 中.

故若 $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, 则 $\sigma(a) = \pm a$, 故 $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

6.2.6 任一有限群均是某个域上可分多项式的伽罗瓦群.

证明. 即**定理 6.37** 的注记, 本书不再赘述. □

6.3 伽罗瓦扩张的一些例子

6.3.1 设 F 为域，$c\in F$，p 为素数.

(1) 当 $\mathrm{char}F=p$ 时，证明 x^p-c 在 $F[x]$ 中不可约当且仅当 x^p-c 在 F 中无根.

证明. ($\Rightarrow$) 显然.

($\Leftarrow$) 设 $b^p=c$, 其中 b 是 F 的代数闭包中元素, 则 $x^p-c=(x-b)^p$, 故 $b\notin F$. 若 $x^p-c=(x-b)^p$ 在 $F[x]$ 中可约，则 $(x-b)^k$ $(1\leqslant k<p)$ 是它的非平凡因子且 $(x-b)^k\in F[x]$，故 $b^k\in F$，但 k 与 p 互素，故存在整数 u,v 使得 $ku=1+pv$，故 $b=b^{ku-pv}=(b^k)^uc^{-v}\in F$，矛盾. 故 x^p-c 在 $F[x]$ 中不可约. □

(2) 当 $\mathrm{char}F\neq p$ 时，证明 F 有 p 个不同的 p 次单位根. 由此证明 x^p-c 在 $F[x]$ 中不可约当且仅当 x^p-c 在 F 中无根.

证明. 题目实际所指的是：F 的代数闭包中存在 p 个不同的 p 次单位根.

令 $g(x)=x^p-1$，则 $g'(x)=px^{p-1}\neq 0$，故 $\gcd(g,g')=1$，g 在 F 的代数闭包中没有重根.

我们只需证根的不存在性导致 $f(x)=x^p-c$ 的不可约性即可. 设 f 的一个根为 α，则 f 的所有根为 $g(x)$ 的所有根的 α 倍，故 f 在 F 的代数闭包中也无重根.

令 x^p-c 在 F 上的分裂域为 K，则 K/F 为伽罗瓦扩张，类似**习题 6.2.4** 我们知道 $\mathrm{Gal}(K/F)\leqslant\left\{\begin{pmatrix}k&l\\0&1\end{pmatrix}\mid l\in\mathbb{F}_p,k\in\mathbb{F}_p^\times\right\}\leqslant S_p$.（第一个等号不一定成立，因为右边群中元素不一定保持 F 不变），并且由它在 x^p-c 的所有 p 个根上的作用唯一确定.

若 $\mathrm{Gal}(K/F)$ 中存在 p 阶元，则它在 S_p 中必为 p-轮换，即它在根上的作用可迁，故所有的根均有相同的 F 上最小多项式，它是所有根的化零多项式且整除 $f(x)$，只能是 $f(x)$ 本身（f 无重根），即 $f(x)$ 在 $F[x]$ 上不可约.

若 $\mathrm{Gal}(K/F)$ 中不存在 p 阶元，则它不可能是平凡群（这导致 $f(x)$ 在 F 上分裂，与它无根矛盾），并且 (*) 不存在 $l_1\neq l_2$ 使得 $\sigma_1:\alpha_u\mapsto\alpha_{ku+l_1},\sigma_2:\alpha_u\mapsto\alpha_{ku+l_2}\in\mathrm{Gal}(K/F)$（若不然，则 $\sigma_1^{-1}\sigma_2:\alpha_u\mapsto\alpha_{u+(l_2-l_1)k^{-1}}$ 为 p 阶元，其中 k^{-1} 是 k 在 $\mathbb{F}_p$ 中的逆，矛盾），作同态 $\varphi:\left\{\begin{pmatrix}k&l\\0&1\end{pmatrix}\mid l\in\mathbb{F}_p,k\in\mathbb{F}_p^\times\right\}\to\mathbb{F}_p^\times,\begin{pmatrix}k&l\\0&1\end{pmatrix}\mapsto k$，由于 $\mathbb{F}_p^\times$ 为 $p-1$ 阶循环群，考虑它的子群 $\varphi(\mathrm{Gal}(K/F))$，它也是循环群，记其生成元为 k_1，则 $k_1\neq 1$，其原像（由 (*)，它必然是唯一的）为 $\sigma':\alpha_u\mapsto\alpha_{k_1u+l}$，则由 (*)，$\mathrm{Gal}(K/F)$ 中不含任何 $\langle\sigma'\rangle$ 以外元素，故 σ'（考虑它作为 S_p 的元素作用在 x^p-c 的所有根上）的不动点 α_{lm} $(m(1-k_1)\equiv 1\bmod p)$ 是 $\mathrm{Gal}(K/F)$ 的不动点. 由于 K/F 为伽罗瓦扩张，故 $f(x)$ 的一个根 $\alpha_{lm}\in F$，矛盾. 故本情况不存在，必有 $\mathrm{Gal}(K/F)$ 中存在 p 阶元且它在 α_i 上的作用可迁. □

注记. 文献 [13] 给出了一种简单得多的证法，但它不涉及伽罗瓦群，考虑到本题的出现位置，本书并未采用那种证法.

6.3.2 试求出库默尔扩张的伽罗瓦群.

解. 令 m 是最小的满足 $\alpha^m \in F$ 的整数，则由 $\alpha^n = a \in F$，读者可自行推出 $m \mid n$.

故 $\sigma(\alpha^m) = \zeta_n^{im}\alpha^m = \alpha^m$，即 $im \equiv 0 \mod n$，i 必须是 n/m 的倍数，故 $\mathrm{Gal}(K/F) \cong \mathbb{Z}/m\mathbb{Z}$.

6.3.3 设 E 为 $x^4 - 2$ 在 $\mathbb{Q}$ 上的分裂域.

(1) 试求出 $E/\mathbb{Q}$ 的全部中间域.

解. 易验证 $E = \mathbb{Q}(i, \sqrt[4]{2})$，记 $a = \sqrt[4]{2}$，则 x^4-2 的全部四个根为 $a, ia, -a, -ia$. 类似**习题 6.2.3(1)** 我们有 $G = \mathrm{Gal}(K/F) \cong D_4 = \langle \sigma_a, \sigma_i \rangle$，其中 $\sigma_i(i) = -i, \sigma_i(a) = a, \sigma_a(i) = i, \sigma_a(a) = ia$.

G 的所有非平凡子群如下：

中心 $H_1 = \{\mathrm{id}, \sigma_a^2\}$. 此时 σ_a^2 将 a 变为 $-a$，i 保持不变，故 $F_1 = \mathbb{Q}(i, \sqrt{2})$ 是 H_1 的不变域.

其他 2 阶子群: $H_{20} = \{\mathrm{id}, \sigma_i\}, H_{21} = \{\mathrm{id}, \sigma_a\sigma_i\}, H_{22} = \{\mathrm{id}, \sigma_a^2\sigma_i\}, H_{23} = \{\mathrm{id}, \sigma_a^3\sigma_i\}$，此时这四个子群的非单位元在四个根上作用分别为：

$a, ia, -a, -ia \mapsto a, -ia, -a, ia$;

$a, ia, -a, -ia \mapsto ia, a, -ia, -a$;

$a, ia, -a, -ia \mapsto -a, ia, a, -ia$;

$a, ia, -a, -ia \mapsto -ia, -a, ia, a$.

故 $F_{20} = \mathbb{Q}(a), F_{21} = \mathbb{Q}(a + ia), F_{22} = \mathbb{Q}(ia), F_{23} = \mathbb{Q}(a - ia)$ 各是这四个子群的不变域.

克莱茵群子群：$H_{30} = \{\mathrm{id}, \sigma_i, \sigma_a^2, \sigma_a^2\sigma_i\} = H_{20}H_{22}, H_{31} = \{\mathrm{id}, \sigma_a\sigma_i, \sigma_a^2, \sigma_a^3\sigma_i\} = H_{21}H_{23}$，此时 $F_{30} = F_{20} \cap F_{22} = \mathbb{Q}(\sqrt{2}), F_{31} = F_{21} \cap F_{23} = \mathbb{Q}(i\sqrt{2})$ 各是这两个子群的不变域.

最大循环真子群：$H_4 = \langle \sigma_a \rangle$，此时 $F_4 = \mathbb{Q}(i)$ 是该子群的不变域.

以上 $F_1, F_{20}, F_{21}, F_{22}, F_{23}, F_{30}, F_{31}, F_4$ 是 $E/\mathbb{Q}$ 的全部中间域，其中 H_1, H_{30}, H_{31}, H_4 是正规子群，故 $F_1, F_{30}, F_{31}, F_4/\mathbb{Q}$ 是伽罗瓦扩张，H_{20} 与 H_{22} 共轭，H_{21} 与 H_{23} 共轭，故 F_{20} 与 F_{22} 共轭，F_{21} 与 F_{23} 共轭.

6.3.4 设 E 为 $x^4 - 2$ 在 $\mathbb{F}_5$ 上的分裂域，试求出 $E/\mathbb{F}_5$ 的伽罗瓦群和全部中间域.

解. 记 $F = \mathbb{F}_5$，设 a 是 $x^4 - 2$ 在 E 上的一个根，显然 $a, a^2 \notin F$，且 $a, 2a, 3a, 4a$ 是 $x^4 - 2$ 的根，故它们是 $x^4 - 2$ 在 E 上的全部根，$E = F(a)$ 是库默尔扩张，由**习题 6.3.2** 和 $a^2 \notin F$ 知 $\mathrm{Gal}(E/F) \cong \mathbb{Z}/4\mathbb{Z} \cong F^\times$.

该伽罗瓦群只有一个非平凡子群 $\mathbb{Z}/2\mathbb{Z}$，由于 $\sigma : a \mapsto 4a = -a$ 是伽罗瓦群中唯一的 2 阶元，故子群 $\{\mathrm{id}, \sigma\}$ 作用下的不变域 $F(a^2)$ 即 E/F 的唯一中间域.

6.3.5 对于 $n = 8, 9, 12$，求出 $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$，并列出 G 的全部子群和它们对应的 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 的中间域.

解. 以下记 $K = \mathbb{Q}(\zeta_n), F = \mathbb{Q}$.

(1) $n = 8$，$G = (\mathbb{Z}/8\mathbb{Z})^\times \cong K_2$ 为克莱茵群，其 2 阶元为 $\sigma_{3,5,7}, \sigma_i : \zeta_8 \mapsto \zeta_8^i$. 易验证 σ_3 固定 $\sqrt{2}i = \zeta_8 + \zeta_8^3$，$\sigma_5$ 固定 $i = \zeta_8^2$，σ_7 固定 $\sqrt{2} = \zeta_8 + \zeta_8^7$. 故中间域 $F_3 \supseteq F(\sqrt{2}i), F_5 \supseteq F(i), F_7 \supseteq F(\sqrt{2})$，易见 ζ_8 在右边三个域上的最小多项式分别为 $(x^2 - \sqrt{2}ix - 1), (x^2 - i), (x^2 - \sqrt{2}x + 1)$（请读者自证不

可约性)，故 K 在右边三个域上的指数都是 2，故它们是各非平凡子群 $\{\mathrm{id},\sigma_3\},\{\mathrm{id},\sigma_5\},\{\mathrm{id},\sigma_7\}$ 的不变域.

(2) $n=9$，$G=(\mathbb{Z}/9\mathbb{Z})^\times\cong\mathbb{Z}/6\mathbb{Z}$，其非平凡子群为唯一的 2 阶和唯一的 3 阶子群，2 阶元为 σ_8，3 阶元为 σ_4,σ_7，6 阶元为 σ_2,σ_5，其中 $\sigma_i:\zeta_9\mapsto\zeta_9^i$.

对 2 阶子群 $\{\mathrm{id},\sigma_8\}$，它固定 $\zeta_9+\zeta_9^8\in\mathbb{R}$ 不变，故中间域 $F_1\supseteq F(\zeta_9+\zeta_9^8)$，后者是 $\mathbb{R}$ 的子域，故不是 K，且 ζ_9 在 $F(\zeta_9+\zeta_9^8)$ 上有化零多项式 $x^2-(\zeta_9+\zeta_9^8)x+1$，若它可约，则 $\zeta_9\in F(\zeta_9+\zeta_9^8)$，矛盾，故 $[K:F(\zeta_9+\zeta_9^8)]=2$，$F(\zeta_9+\zeta_9^8)=F_1$ 就是 $\{\mathrm{id},\sigma_8\}$ 的不变域.

对 3 阶子群 $\{\mathrm{id},\sigma_4,\sigma_7\}$，它固定 $\zeta_9^3=\omega$ 不变. 故中间域 $F_2\supseteq F(\omega)$. ζ_9 在 $F(\omega)$ 上的化零多项式为 $f(x)=x^3-\omega=(x-\zeta_9)(x-\zeta_9\omega)(x-\zeta_9\omega^2)$，若它在 $F(\omega)$ 上可约，则它有一次因式，$\zeta_9\omega^i$ $(i=0,1,2)\in F(\omega)$，$\zeta_9\in F(\omega)$，$K=F(\omega)$，但 $[F(\omega):F]=2$（读者请自证），与 $[K:F]\geqslant|\mathrm{Gal}(K/F)|=6$ 矛盾，故 $f(x)$ 在 $F(\omega)$ 上不可约，是 ζ_9 的最小多项式，$[K:F(\omega)]=3$，$F(\omega)=F_2$ 就是 $\{\mathrm{id},\sigma_4,\sigma_7\}$ 的不变域.

(3) $n=12$，$G=(\mathbb{Z}/12\mathbb{Z})^\times\cong K_2$ 为克莱茵群，其 2 阶元为 $\sigma_{5,7,11},\sigma_i:\zeta_{12}\mapsto\zeta_{12}^i$.

对 2 阶子群 $\{\mathrm{id},\sigma_{11}\}$，它固定 $\zeta_{12}+\zeta_{12}^{11}\in\mathbb{R}$ 不变，故中间域 $F_1\supseteq F(\zeta_{12}+\zeta_{12}^{11})$，后者是 $\mathbb{R}$ 的子域，故不是 K，且 ζ_{12} 在 $F(\zeta_{12}+\zeta_{12}^{11})$ 上有化零多项式 $x^2-(\zeta_{12}+\zeta_{12}^{11})x+1$，若它可约，则 $\zeta_{12}\in F(\zeta_{12}+\zeta_{12}^{11})$，矛盾，故 $[K:F(\zeta_{12}+\zeta_{12}^{11})]=2$，$F(\zeta_{12}+\zeta_{12}^{11})=F_1$ 就是 $\{\mathrm{id},\sigma_{11}\}$ 的不变域.

对 2 阶子群 $\{\mathrm{id},\sigma_7\}$，它固定 $\zeta_{12}^2=\omega+1$ 不变，故中间域 $F_2\supseteq F(\omega)$. ζ_{12} 在 $F(\omega)$ 上的化零多项式为 $f(x)=x^2-(\omega+1)=(x-\zeta_{12})(x-\zeta_{12}\omega)$，若它在 $F(\omega)$ 上可约，则它有一次因式，$\zeta_{12}\omega^i$ $(i=0,1)\in F(\omega)$，$\zeta_{12}\in F(\omega)$，$K=F(\omega)$，但 $[F(\omega):F]=2$（读者请自证），与 $[K:F]\geqslant|\mathrm{Gal}(K/F)|=4$ 矛盾，故 $f(x)$ 在 $F(\omega)$ 上不可约，是 ζ_{12} 的最小多项式，$[K:F(\omega)]=2$，$F(\omega)=F_2$ 就是 $\{\mathrm{id},\sigma_7\}$ 的不变域.

对 2 阶子群 $\{\mathrm{id},\sigma_5\}$，它固定 $\zeta_{12}^3=i$ 不变，故中间域 $F_3\supseteq F(i)$. ζ_{12} 在 $F(i)$ 上的化零多项式为 $f(x)=x^2-ix-1$，但显然 $\zeta_{12}\notin F(i)$，故 $f(x)$ 在 $F(i)$ 上不可约，$[K:F(i)]=2$，$F(i)=F_3$ 就是 $\{\mathrm{id},\sigma_5\}$ 的不变域.

6.3.6 设 $n\geqslant2$ 为正整数，证明 $\mathbb{Q}(\zeta_n)\cap\mathbb{R}=\mathbb{Q}(\zeta_n+\zeta_n^{-1})$.

证明. 题意要求的集合必在复共轭的不变域中，类似正文的讨论（复共轭未必是伽罗瓦群中唯一 2 阶元，但我们已经特定了复共轭的不变域，请读者自己完成）即得 $\mathbb{Q}(\zeta_n)\cap\mathbb{R}\subseteq\mathbb{Q}(\zeta_n+\zeta_n^{-1})$，又 $\zeta+\zeta_n^{-1}\in\mathbb{R}$，故 $\mathbb{Q}(\zeta_n)\cap\mathbb{R}\supseteq\mathbb{Q}(\zeta_n+\zeta_n^{-1})$，得到结论. □

6.3.7 设 p 是奇素数，$\left(\frac{a}{p}\right)_{\mathrm{Le}}$ 是勒让德符号，设**高斯和**

$$g=\sum_{a\in\mathbb{F}_p}\zeta_p^a\left(\frac{a}{p}\right)_{\mathrm{Le}}.$$

证明：

(1) $\sum_{a\in\mathbb{F}_p}\zeta_p^a=0$.

证明. 注意 x^p-1 的次项系数为 0 即可. □

(2) $g\cdot\overline{g}=p$，其中 $\overline{g}$ 是 g 的复共轭.

证明. $u=g\overline{g}=\sum_{a\in\mathbb{F}_p}\zeta_p^a\left(\frac{a}{p}\right)_{\mathrm{Le}}\sum_{b\in\mathbb{F}_p}\zeta_p^{-b}\left(\frac{b}{p}\right)_{\mathrm{Le}}=\sum_{i=0}^{p-1}g_i\zeta_p^i$，其中 $g_i=\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)_{\mathrm{Le}}\left(\frac{a-i}{p}\right)_{\mathrm{Le}}$.

g_0 容易计算，因为 $a\neq 0$ 时 $\left(\frac{a^2}{p}\right)_{\mathrm{Le}}$ 由定义等于 1，$a\neq 0$ 时它等于 0. 故 $g_0=\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)_{\mathrm{Le}}\left(\frac{a}{p}\right)_{\mathrm{Le}}=\sum_{a\in\mathbb{F}_p}\left(\frac{a^2}{p}\right)_{\mathrm{Le}}=0+\underbrace{1+\cdots+1}_{p-1\text{个}}=p-1$.

由于当 $j\neq 0$ 时 $g_1=\left(\frac{j^2}{p}\right)_{\mathrm{Le}}g_1=\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)_{\mathrm{Le}}\left(\frac{a-1}{p}\right)_{\mathrm{Le}}\left(\frac{j^2}{p}\right)_{\mathrm{Le}}=\sum_{a\in\mathbb{F}_p}\left(\frac{ja}{p}\right)_{\mathrm{Le}}\left(\frac{ja-j}{p}\right)_{\mathrm{Le}}$，由于 j 与 p 互素，$a\mapsto ja$ 是 $\mathbb{F}_p$ 到自身的双射，故上式 $=\sum_{a'\in\mathbb{F}_p}\left(\frac{a'}{p}\right)_{\mathrm{Le}}\left(\frac{a'-j}{p}\right)_{\mathrm{Le}}=g_j$，故 $g_1,\cdots,g_{p-1}$ 都相等.

考虑 $\sum_{i=0}^{p-1}g_i=\sum_{i\in\mathbb{F}_p}\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)_{\mathrm{Le}}\left(\frac{a-i}{p}\right)_{\mathrm{Le}}=\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)_{\mathrm{Le}}\left(\sum_{i\in\mathbb{F}_p}\left(\frac{a-i}{p}\right)_{\mathrm{Le}}\right)$，由于 a 固定，i 取 $\mathbb{F}_p$ 上各值时 $a-i$ 也取 $\mathbb{F}_p$ 上不重复的各值，且（读者可自行考虑 $\mathbb{F}_p$ 上的生成元 σ，则二次剩余为 σ^2 生成的指数为 2 的子群）勒让德符号有性质 $\sum_{l\in\mathbb{F}_p}\left(\frac{l}{p}\right)_{\mathrm{Le}}=0$，故 $\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)_{\mathrm{Le}}\left(\sum_{i\in\mathbb{F}_p}\left(\frac{a-i}{p}\right)_{\mathrm{Le}}\right)=\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)_{\mathrm{Le}}\cdot 0=0$，即 $\sum_{i=1}^{p-1}g_i=-g_0=-(p-1)$，$g_1=g_2=\cdots=g_{p-1}=-1$.

$u=\sum_{i=0}^{p-1}g_i\zeta_p^i=p-1-\sum_{i=1}^{p-1}\zeta_p^i=p-\sum_{i=0}^{p-1}\zeta_p^i=p-0=p$. □

(3) $\overline{g}=\sum_{a\in\mathbb{F}_p}\zeta_p^{-a}\left(\frac{a}{p}\right)_{\mathrm{Le}}=\sum_{a\in\mathbb{F}_p}\zeta_p^a\left(\frac{-a}{p}\right)_{\mathrm{Le}}=\sum_{a\in\mathbb{F}_p}\zeta_p^a\left(\frac{a}{p}\right)_{\mathrm{Le}}\left(\frac{-1}{p}\right)_{\mathrm{Le}}=g\left(\frac{-1}{p}\right)_{\mathrm{Le}}=(-1)^{(p-1)/2}g$.

故 $g^2=g\overline{g}(-1)^{-(p-1)/2}=(-1)^{-(p-1)/2}p=(-1)^{(p-1)/2}$（因 $(p-1)/2$ 是整数），即得结论.

(4) $\mathbb{Q}(\zeta_p)$ 有唯一的二次子域 $K=\mathbb{Q}(g)$.

证明. 令 $\sigma:\zeta_p\mapsto\zeta_p^r$ 是 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\cong(\mathbb{Z}/p\mathbb{Z})^\times$ 的一个生成元，则 $\sigma^2:\zeta_p^u\mapsto\zeta_p^{ur^2}$，$r^2$ 是模 p 的二次剩余，故 $\left(\frac{u}{p}\right)_{\mathrm{Le}}=\left(\frac{ur^2}{p}\right)_{\mathrm{Le}}$，即 σ^2 保持 g 不变. σ^2 的不变域 K_1 包含 K（易验证 $g\notin\mathbb{Q}$）.

另一方面，$\langle\sigma^2\rangle$ 是 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 的唯一指数为 2 的子群，故 $[K_1:\mathbb{Q}]=2=[K:\mathbb{Q}]$，故 $K_1=K$，K 是 $\mathbb{Q}(\zeta_p)$ 的唯一二次子域. □

6.4 方程的根式可解性

6.4.1 设 p,q 为不同的素数，证明：

(1) p 的幂次阶群是可解群.

证明. 设 $|G|=p^n$，当 $n=0$ 时，平凡群是可解群，当 $n=1$ 时，G 是素数阶循环群，它显然是可解群.

若 $n<k$ 时结论成立，则若 $|G|=p^k$，由**命题 2.42**，$|G|$ 的中心非平凡，故 $|Z(G)|=p^r$ $(1\leqslant r\leqslant k)$，$|G/Z(G)|=p^{k-r}$ $(0\leqslant k-r\leqslant k-1)$，且 $Z(G)\lhd G$，故要么 $G=Z(G)$，此时 G 是阿贝尔群，故为可解群，要么 $Z(G)$ 和 $G/Z(G)$ 的阶都满足归纳假设，它们都是可解群，故由**命题 6.44(1)**，G 也是可解群. □

(2) pq 阶群是可解群.

证明. 不妨设 $p<q$，则由**命题 2.56(1)**，G 的西罗 q-子群 H 是 G 的正规子群，它是可解群. G/H 的阶为 p，故它也是可解群，故由**命题 6.44(1)**，G 也是可解群. □

(2) p^2q 阶群是可解群.

证明. 由**命题 2.56(2)**，存在两种情况：

(i) G 的西罗 q-子群 H 是 G 的正规子群，它是可解群. G/H 的阶为 p^2，故它也是可解群.

(ii) G 的西罗 p-子群 H 是 G 的正规子群，它的阶为 p^2，故是可解群. G/H 的阶为 q，故它也是可解群.

由**命题 6.44(1)**，G 也是可解群. □

6.4.2 对于群 G，定义 $G^{(1)}=G'$ 为 G 的换位子群，并归纳定义 $G^{(i+1)}=G^{(i)\prime}$，证明 G 是可解群当且仅当存在 $n\geqslant 1$，$G^{(n)}=1$.

证明. 由**命题 2.69**，对任意群 H 有 $H'\lhd H$，且 H/H' 为阿贝尔群，故 $G\rhd G^{(1)}\rhd\cdots\rhd G^{(n)}$ 是可解列，当它终结于 $\{1\}$ 时 G 可解.

反之，若 G 不可解，由 $G^{(1)}\lhd G$ 知 $G^{(1)}$ 和 $G/G^{(1)}$ 中必有一个不可解，但后者是阿贝尔群，故 $G^{(1)}$ 不可解，同样推理即 $G^{(n)}$ 不可解对一切 $n\geqslant 1$ 成立，故无论 n 取何正整数 $G^{(n)}$ 不可能等于 $\{1\}$. □

以下适用于 6.4.3-6.4.5 题. 设 G 是群. 我们定义 $C_1(G)=Z(G)$ 为 G 的中心，并归纳定义 $C_{i+1}(G)$ 为 $Z(G/C_i(G))$ 在映射 $G\to G/C_i(G)$ 的原像. 如存在 $n\geqslant 1$ 使得 $C_n(G)=G$，则称 G 为**幂零群**.

注记. 该定义实际定义了 G 的**上中心系列**，G 是幂零群即上中心系列终结于 G，此时它是 1 到 G 的**中心系列**（中心系列的定义见文献 [29]）

解. 我们证明以下事实以供下面几题使用. 我们定义 $C_0(G)=\{1\}$，易见这定义是平滑的，即 $C_1(G)=Z(G)$ 也是 $Z(G/\{1\})$ 在映射 $\mathrm{id}:G\to G/\{1\}$ 的原像.

(i) $C_i(G)$ 是 G 的正规子群.

证明. $C_1(G)=Z(G)$ 显然是 G 的正规子群. 若 $C_i(G)\lhd G$，则由 $Z(G/C_i(G))\lhd G/C_i(G)$ 知 $gC_{i+1}(G)g^{-1}=gZ(G/C_i(G))C_i(G)g^{-1}$(请理解为 $C_i(G)$ 的陪集!)$=gC_i(G)Z(G/C_i(G))(gC_i(G))^{-1}C_i(G)=Z(G/C_i(G))C_i(G)=C_{i+1}(G)$，故 $C_{i+1}(G)\lhd G$. □

(ii) $C_i(G)\geqslant[C_{i+1}(G),(G)]$，其中 $[H,G]$ 为 H 和 G 的换位子群 $hgh^{-1}g^{-1}$（注：等号未必成立，即使 $i+1<n$ 且 G 是幂零群，见文献 [29] 中 $C_2\times Q_8$ 的例子）.

证明. 考虑 $C_{i+1}(G)$ 中任意元素 u，则由定义 $uC_igC_i(uC_i)^{-1}(gC_i)^{-1}=C_i$ 对一切 g 成立，故 $ugu^{-1}g^{-1}\in C_i$. □

定义. G 的**下中心系列**是指 $G_0=G$（注：有些文献给出 $G_1=G$），递归定义 $G_{i+1}=[G_i,G]$. 由于 $g[a,b]g^{-1}=[a,g]^{-1}[a,gb]$，故 G_i 是 G 的正规子群. 可以证明当且仅当存在 n 使 $G_n=\{1\}$ 时，G 是幂零群且上中心系列和下中心系列长度一致，详细证明见文献 [22]，本书不再赘述.

6.4.3 幂零群一定是可解群.

证明. $C_n=G,C_{n-1}\geqslant[G,G]=G_1,C_{n-2}\geqslant[C_{n-1},G]\geqslant[G_1,G]=G_2,\cdots C_0\geqslant G_n$. 但 $C_0=\{1\}$，故 $G_n=\{1\}$.

$G_1=[G,G]=G^{(1)}$，若 $G^i\leqslant G_i$，则 $G^{i+1}=[G^i,G^i]\leqslant[G^i,G]\leqslant[G_i,G]=G_{i+1}$，故 $G^k\leqslant G_k$ 对一切 n 成立，$G^n\leqslant G_n=\{1\}$，由**习题 6.4.2**，G 是可解群. □

6.4.4 证明对称群 S_3 和 S_4 是可解群，但不是幂零群.

证明. 由于 S_n $(n\geqslant 3)$ 的中心平凡，$C_1(G)=C_2(G)=\cdots C_i(G)=\{1\}$，故 S_n 在 $n\geqslant 3$ 时不是幂零群.

A_n 是 S_n 的正规子群，且 $S_n/A_n\cong\mathbb{Z}/2\mathbb{Z}$ 是阿贝尔群. A_3 是 3 阶循环群，它自身即阿贝尔群，A_4 有正规子群 $K_2:\{\mathrm{id},(12)(34),(13)(24),(14)(23)\}$，$A_4/K_2$ 的阶为 3，K_2 的阶为 $4=2^2$，它们都是阿贝尔群，故 S_3 和 S_4 可解. □

6.4.5 设 N 为群 G 的正规子群，如果 N 和 G/N 都是幂零群，G 是否也是幂零群?

解. 不一定，取 $G=A_4$，$N=K_2$，则 N,G/N 的阶分别为 4 和 3，它们都是阿贝尔群，故幂零，但 A_4 的中心平凡，故不是幂零群.

6.4.6 试导出三次方程的求根公式：设 F 是特征 0 域，

$$f(x)=x^3-t_1x^2+t_2x-t_3\in F(t_1,t_2,t_3)[x].$$

解. 作移轴变换 $y=x-t_1/3$，则 $y^3+py+q=0$，其中 $p=-\frac{1}{3}t_1^2+t_2,q=-\frac{2}{27}t_1^3+\frac{1}{3}t_1t_2-t_3$.

采用正文 6.2 节的记号，$\Delta^2=-((p/3)^3+(q/2)^2)*108$，故根的偶置换 A_3 的不变域为 $F(\Delta)$，且 $f(x)$ 的分裂域 K 满足 $[K:F(\Delta)]=|A_3|=3,\mathrm{Gal}(K/F(\Delta))=\mathbb{Z}/3\mathbb{Z}$.

故 $\mathrm{Gal}(K(\omega)/F(\Delta,\omega))=\{1\}$ 或 $\mathbb{Z}/3\mathbb{Z}$，我们考虑后一种情况，即 $K(\omega)/F(\Delta,\omega)$ 是三次扩张. 令 y_i $(i=1,2,3)$ 为 $f(x)$ 的三个根，则由 K/F 是平凡扩张或三次扩张，$K=F(y_1)$，令 $\sigma:y_1\mapsto y_2,y_2\mapsto y_3,y_3\mapsto y_1\in\mathrm{Gal}(K(\omega)/F(\Delta,\omega))$，则 $\sigma^3=\mathrm{id}$. 令 $d_1=y_1+y_2\omega+y_3\omega^2,d_2=y_1+y_2\omega^2+y_3\omega,d_3=y_1+y_2+y_3$，则 $\sigma(d_1)=d_1\omega^2,\sigma(d_2)=d_2\omega,\sigma_(d_3)=d_3=0$，且 $K=F(\Delta,\omega,d_1)$，$d_1^3\in F(\Delta,\omega)$. 我们来计算 d_1^3.

注意 $\Delta=(y_1-y_2)(y_2-y_3)(y_3-y_1)$，$y_1+y_2+y_3=0, y_1y_2+y_2y_3+y_3y_1=p, y_1y_2y_3=q$. $d_1^3=(y_1^3+y_2^3+y_3^3+6y_1y_2y_3)+3\omega(y_1^2y_2+y_2^2y_3+y_3^2y_1)+3\omega(y_1^2y_3+y_2^2y_1+y_3^2y_2)=(y_1+y_2+y_3)^3-3(y_1+y_2+y_3)(y_1y_2+y_2y_3+y_3y_1)-9y_1y_2y_3+3/2\cdot\omega((y_1+y_2+y_3)(y_1y_2+y_2y_3+y_3y_1)-\Delta+3y_1y_2y_3)+3/2\cdot\omega^2((y_1+y_2+y_3)(y_1y_2+y_2y_3+y_3y_1)+\Delta+3y_1y_2y_3)=-9q-\frac{3\omega}{2}\cdot\Delta+\frac{9\omega q}{2}+\frac{3\omega^2}{2}\cdot\Delta+\frac{9\omega^2 q}{2}=-\frac{27}{2}q-\frac{3\sqrt{3}i}{2}\cdot\Delta=-\frac{27}{2}q+27\sqrt{(q/2)^2+(p/3)^3}$.

故 $d_1=\sqrt[3]{-\frac{27}{2}q+27\sqrt{(q/2)^2+(p/3)^3}}=3\sqrt[3]{-\frac{q}{2}+\sqrt{(q/2)^2+(p/3)^3}}$，记它为 3α.

由于 $\tau: y_1\mapsto y_1, y_2\mapsto y_3, y_3\mapsto y_2$ 保持 $F(t_1,t_2,t_3)$ 不变并将 Δ 映射到 $-\Delta$，d_1 映射到 d_2，故 $d_2^3=-\frac{27}{2}q+\frac{3\sqrt{3}i}{2}\cdot\Delta$，$d_2=3\sqrt[3]{-\frac{q}{2}-\sqrt{(q/2)^2+(p/3)^3}}$，记它为 3β.

解方程 $y_1+y_2+y_3=d_3=0, y_1+\omega y_2+\omega^2 y_3=3\alpha, y_1+\omega^2 y_2+\omega y_3=3\beta$，得 $y_1=\alpha+\beta, y_2=\omega\alpha+\omega^2\beta, y_3=\omega^2\alpha+\omega\beta$，且 $p=y_1y_2+y_2y_3+y_3y_1=(1+\omega+\omega^2)\alpha^2+(1+\omega+\omega^2)\beta^2-3\alpha\beta=-3\alpha\beta$，故 α,β 需要满足 $\alpha\beta=-p/3$.

6.4.7 将 $\cos 20^\circ$ 和 $\cos\frac{360^\circ}{7}$ 表示为根式形式.

解. $\cos\frac{\pi}{9}$ 的最小多项式为 $x^3-\frac{3}{4}x-\frac{1}{8}$（**推论 5.35**），利用**习题 6.4.6** 的结果，$\alpha_0=\sqrt[3]{\frac{1}{16}+\frac{\sqrt{3}i}{16}}=\sqrt[3]{\frac{\zeta_6}{8}}=\zeta_{18}/2$（取幅角主值最小），$\beta_0=\sqrt[3]{\frac{1}{16}-\frac{\sqrt{3}i}{16}}=\sqrt[3]{\frac{\zeta_6^5}{8}}=\zeta_{18}^{17}/2$（取幅角主值最大），显然 $\alpha_0\beta_0=1/4=-p/3$，方程的三个根为 $\alpha_0+\beta_0=(\zeta_{18}+\zeta_{18}^{17})/2$，$\alpha_0\omega+\beta_0\omega^2, \alpha_0\omega^2+\beta_0\omega$，第一个根是实数，故它是 $\cos 20^\circ$，即 $\cos 20^\circ=\sqrt[3]{\frac{1}{16}+\frac{\sqrt{3}i}{16}}+\sqrt[3]{\frac{1}{16}-\frac{\sqrt{3}i}{16}}=\frac{1}{2}(\sqrt[3]{\frac{1+\sqrt{3}i}{2}}+\sqrt[3]{\frac{1-\sqrt{3}i}{2}})$.

$\cos\frac{2\pi}{7}$ 的最小多项式由**习题 5.2.4** 为 $a^3+1/2a^2-1/2a-1/8=0$. 利用**习题 6.4.6** 的结果，$p=-7/12, q=-7/216, t_1/3=-1/6$. $\alpha=\sqrt[3]{\frac{7+21\sqrt{3}i}{432}}, \beta=\sqrt[3]{\frac{7-21\sqrt{3}i}{432}}$，由于 α^3,β^3 彼此共轭，取 α_0 为幅角主值最小的立方根，β_0 为幅角主值最大的立方根，它们彼此共轭，满足 $(\alpha\beta)^3=343/46656=(-p/3)^3$，且 $\cos\frac{2\pi}{7}=-1/6+\alpha_0+\beta_0$.

故 $\cos\frac{2\pi}{7}=-1/6+\sqrt[3]{\frac{7+21\sqrt{3}i}{432}}+\sqrt[3]{\frac{7-21\sqrt{3}i}{432}}=\frac{1}{6}(-1+\sqrt[3]{\frac{7+21\sqrt{3}i}{2}}+\sqrt[3]{\frac{7-21\sqrt{3}i}{2}})$.

6.4.8 求下列方程在复数域 $\mathbb{C}$ 中的根：

(1) $x^3-2x+4=0$.

解. 该方程的有理根只可能为 $\pm1,\pm2,\pm4$，经检验 -2 是根，故 $x^3-2x+4=(x+2)(x^2-2x+2))$，对后者求根得 $x^2-2x+2=(x-(1+i))(x-(1-i))$，故 $-2, 1+i, 1-i$ 是根.

(2) $x^3-15x+4=0$.

解. 该方程的有理根只可能为 $\pm1,\pm2,\pm4$，经检验 -4 是根，故该多项式可分解为 $(x+4)(x^2-4x+1)$，对后者求根得 $x^2-4x+1=(x-\sqrt{3}-2)(x+\sqrt{3}-2)$，故 $-4, \sqrt{3}+2, 2-\sqrt{3}$ 是根.

(3) $x^4-2x^3-8x-3=0$.

解. 该方程的有理根只可能为 $\pm1,\pm3$，经检验 3 是根，故该多项式分解为 $(x-3)(x^3+x^2+3x+1)$.

由卡尔达诺公式考虑三次方程 x^3+x^2+3x+1 的根，此时 $p=8/3, q=2/27$,

$\alpha=\sqrt[3]{-1/27+\sqrt{19/27}},\beta=\sqrt[3]{-1/27-\sqrt{19/27}}$，$\alpha^3,\beta^3$ 都是实数，取它们的实数立方根得 $\gamma_1=1/3(-1+\sqrt[3]{-1+\sqrt{19}}+\sqrt[3]{-1-\sqrt{19}})$，$\gamma_2=1/3(-1+\sqrt[3]{-1+\sqrt{19}}\omega+\sqrt[3]{-1-\sqrt{19}}\omega^2),\gamma_3=1/3(-1+\sqrt[3]{-1+\sqrt{19}}\omega^2+\sqrt[3]{-1-\sqrt{19}}\omega)$，$(\omega=(-1+\sqrt{3}i)/2=\zeta_3)$. 故 $3,\gamma_1,\gamma_2,\gamma_3$ 是根.

6.4.9 证明方程 $x^p-x-t=0$ 在 $\mathbb{F}_p(t)$ 上根式不可解，但是多项式 x^p-x-t 在 $\mathbb{F}_p(t)$ 上的伽罗瓦群是循环群，这表明在**定理 6.42** 中 $\mathrm{char}F=0$ 的条件一般是不能去掉的.

证明. 令 $F=\mathbb{F}_p(t)$，设 K 是 $x^p-x-t=0$ 的分裂域，由**习题 5.1.18** 的证明 2，x^p-x-t 的所有根之差是 $\mathbb{F}_p$ 中常数，即若 α 是 x^p-x-t 的一个根，则另一个根 $\beta=\alpha+c,c\in\mathbb{F}_p$，故 $K=F(\alpha),[K:F]=p$，由前述证明过程（显然 x^p-x-t 在 $\mathbb{F}_p$ 中无根，故）知 $\mathrm{Gal}(K/F)\to\mathbb{Z}/p\mathbb{Z}$ 为满同态，但 $|\mathrm{Gal}(K/F)|\leqslant[K:F]=p$，故只能 $\mathrm{Gal}(K/F)\cong\mathbb{Z}/p\mathbb{Z}$ 为循环群，K/F 为伽罗瓦扩张.

故 K/F 若有根式扩张塔，由 $[K:F]=p$ 只能 $K=F(\sqrt[p]{u(t)})$，由于 $x^p-u(t)=0$ 的全部根为 p 重的 $\sqrt[p]{u(t)}$，故 $\mathrm{Gal}(K/F)=\{1\}$，与 $\mathrm{Gal}(K/F)=\mathbb{Z}/p\mathbb{Z}$ 矛盾，故根式扩张塔不存在，x^p-x-t 在 $\mathbb{F}_p(t)$ 上根式不可解. □

6.5 主要定理的证明

6.5.1 设 $E=\mathbb{C}(t)$ 为有理函数域，$\sigma,\tau\in G=\mathrm{Gal}(E/\mathbb{C})$，其中 $\sigma(t)=\zeta_3 t,\tau(t)=t^{-1}$. 证明：

(1) τ 和 σ 生成的群 H 是 G 的 6 阶子群；

证明. 易验证 $\tau\sigma\tau^{-1}=\sigma^{-1},\tau^2=\mathrm{id},\sigma^3=\mathrm{id}$，故 $H=\cong S_3$. □

(2) $\mathrm{Inv}(H)=E^H=\mathbb{C}(t^3+t^{-3})$.

证明. $[E:E^H]=|H|=6$，易验证 $\mathbb{C}(t^3+t^{-3})$ 在 σ,τ 作用下不变，故 $E^H\supseteq\mathbb{C}(t^3+t^{-3})$. 但 t 在 $\mathbb{C}(t^3+t^{-3})$ 上的化零多项式为 $x^6-x^3(t^3+t^{-3})+1$，故 $[E:\mathbb{C}(t^3+t^{-3})]\leqslant 6\leqslant[E:E^H]$，故只能 $E^H=\mathbb{C}(t^3+t^{-3})$. □

6.5.2 设域 F 的特征为素数 p，$\sigma\in G=\mathrm{Gal}(F(x)/F)$，其中 $\sigma(x)=x+1$. 令 H 为由 σ 生成的 G 的子群，证明 $|H|=p$. 试确定 $\mathrm{Inv}(H)=F(x)^H$.

解. 易验证 $|H|\cong\mathbb{Z}/p\mathbb{Z},|H|=p,[F(x):F(x)^H]=p$. 由于 $f(x^p-x)$ 在 σ 下作用不变，故 $F(x)^H\supseteq F(x^p-x)$，记 $u=x^p-x$，则 x 在 $F(u)$ 上的化零多项式为 x^p-x-u，故 $[F(x):F(u)]\leqslant p\leqslant[F(x):F(x)^H]$，故只能 $F(x)^H=F(x^p-x)$.

6.5.3 设域 F 的特征为素数 p，$a\in F$，如果 x^p-x-a 在 $F[x]$ 中不可约，令 α 为它的一个根，证明 $F(\alpha)/F$ 为伽罗瓦扩张并计算出它的伽罗瓦群.

证明. 请读者复习**习题 6.4.9** 和 **5.1.18** 证明 2 来完成，本节不再赘述. □

6.5.4 设 L 和 M 都是域 E 的子域.

(1) 证明如果 $L/L\cap M$ 为有限伽罗瓦扩张，则 LM/M 也为有限伽罗瓦扩张，并且

$$\mathrm{Gal}(LM/M)\cong\mathrm{Gal}(L/L\cap M).$$

证明. 利用**引理 6.47** 的注记，取 $E=M,F=L\cap M,K=L$，我们得到大部分结论，只需证明 $\mathrm{Gal}(LM/M)\to\mathrm{Gal}(L/L\cap M)$ 是满同态即可，即右边元素自然确定一个左边元素.

对 $\sigma\in\mathrm{Gal}(L/L\cap M)$，它在 $\alpha\in L$ 和 α 的 $L\cap M$-共轭元上作用传递，令 α 的最小多项式为 $f(x)$，而对 LM 中元素 $\alpha\beta$ 其中 $\beta\in M$，$\alpha\beta$ 是多项式 $f(x/\beta)$ 的根，所有 α 的 $L\cap M$-共轭元乘以 β 也是多项式 $f(x/\beta)$ 的根，故 L 的 $L\cap M$-同构可以自然延拓为 LM 的 M-同构而保持该伽罗瓦群在 $\alpha\beta$ 的 M-共轭元（它们必然是 $L\cap M$-共轭元）上传递. □

(2) 举例说明如果 L/F 不是伽罗瓦扩张，$[LM:M]$ 与 $[L:F]$ 不一定相等.

解. 使用**习题 6.3.3** 的记号，$F=\mathbb{Q},L=F_{20}=\mathbb{Q}(a),M=F_{21}=\mathbb{Q}(a+ia)$，则 $LM=E=\mathbb{Q}(i,a)$，$[LM:M]=2,[L:F]=4$. 易验证此时 L/F 不是正规扩张，故不是伽罗瓦扩张.

6.5.5 设 E/F 为有限伽罗瓦扩张，N 和 M 为中间域，$E \supseteq N \supseteq M \supseteq F$，并且

$$N = \bigcap_{M \leqslant K \leqslant \overline{M}, K/F\text{正规}} K$$

是 M 在 K 上的正规闭包. 证明

$$\mathrm{Gal}(E/N) = \bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma \mathrm{Gal}(E/M)\sigma^{-1}.$$

证明. 由于 M 的 F-共轭元都在 N 中，因此 $N \geqslant \bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma M = N_0$，设 $M = F(\{\alpha_i\})$，所有 α_i 的 F-共轭元是 $\{\beta_j\}$，则 $N_0 = F(\{\beta_j\})$ 且 N_0/F 是正规扩张，故 $N = N_0$.

考虑 $\sigma^{-1}\mathrm{Gal}(E/N)\sigma$，其中 $\sigma \in \mathrm{Gal}(E/F)$. σ 将 M 变动到 $\sigma M \subseteq N$，$\mathrm{Gal}(E/N)$ 的任意元素保持 N 不变故保持 σM 中所有元素不动，σ^{-1} 将 σM 变回 M，易验证这样的变换是 M-自同构，故 $\sigma^{-1}\mathrm{Gal}(E/N)\sigma \subseteq \mathrm{Gal}(E/M)$ 对一切 σ 成立，$\mathrm{Gal}(E/N) \leqslant \bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma \mathrm{Gal}(E/M)\sigma^{-1}$.

反之，对 $\bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma \mathrm{Gal}(E/M)\sigma^{-1}$ 中元素，对任意 σ 它在 $\sigma\mathrm{Gal}(E/M)\sigma^{-1}$ 中，故保持 σM 不变，故保持 N_0 不变，是 N-同构，故它属于 $\mathrm{Gal}(E/N)$.

综上我们有要求的等式. □

6.5.6 设 E/F 为有限伽罗瓦扩张. 如果对任一域 $K, F \subsetneqq K \subsetneqq E$，$K$ 对 F 均有相同的扩张次数 $[K:F]$，则 $[E:F] = p$ 或者 p^2.

证明. 由伽罗瓦理论基本定理，这相当于若群 G 的所有非平凡子群都有相同阶数，则 $|G| = p$ 或 p^2.

若存在不同的素数 $p \mid |G|, q \mid |G|$，则 G 的西罗 p-,q-子群阶数不同. 故 $|G| = p^r$. 当 $r = 1$ 时，结论显然成立.

由**定理 2.53**，当 $0 < k < r$ 时 $|G|$ 中存在 p^k 阶子群，故 k 只能有一个取值，即 $r = 2$. □

6.5.7

(1) 证明 $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ 是伽罗瓦扩张，并求出伽罗瓦群；

证明. 由于 $a = \sqrt{2}, b = \sqrt{3}, c = \sqrt{5}$ 的平方都是有理数，故 $\mathbb{Q}(a,b,c)$ 中元素必能表示为 $1, a, b, c, ab, ac, bc, abc$ 的线性组合，故 $[\mathbb{Q}(a,b,c)/\mathbb{Q}] \leqslant 8$.

记 $\sigma_a : a \mapsto -a, \sigma_b : b \mapsto -b, \sigma_c : c \mapsto -c$，易验证它们生成 $\mathrm{Gal}(\mathbb{Q}(a,b,c)/\mathbb{Q})$ 且彼此交换，且都是 2 阶元，故伽罗瓦群同构于 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 记该群为 G，则 $|G| = 8 \leqslant [\mathbb{Q}(a,b,c)/\mathbb{Q}]$，这说明后者只能为 8，故 $\mathbb{Q}(a,b,c)/\mathbb{Q}$ 是伽罗瓦扩张. □

(2) 求元素 $\sqrt{6} + \sqrt{10} + \sqrt{15}$ 在 $\mathbb{Q}$ 上的最小多项式.

证明. $ab + bc + ca$ 被且只被 $H = \{\mathrm{id}, \sigma_a\sigma_b\sigma_c\}$ 固定，故它在 $K = \mathrm{Inv}(H)$ 中，$[\mathbb{Q}(a,b,c) : K] = 2$，$[K : \mathbb{Q}] = 4$，即 $x = ab + bc + ca$ 在 $\mathbb{Q}$ 上的最小多项式最多次数为 4.

（读者可以将 $x^4, x^3, x^2, x, 1$ 表示为 $ab, bc, ca, 1$ 的线性组合解出）由于 x 满足 $x^4 - 62x^2 - 240x - 239 = 0$，因 239 是素数，该方程的有理根只能是 $\pm 1, \pm 239$，它们都不是根，故该多项式在有理数集内不可约，是 x 在 $\mathbb{Q}$ 上的最小多项式. □

(3) 证明 $\sqrt{6} \in \mathbb{Q}(\sqrt{6}+\sqrt{10}+\sqrt{15})$;

证明. $\sqrt{6} = ab$ 被 $H = \{\mathrm{id}, \sigma_a\sigma_b\sigma_c\}$ 固定，故它在 $K = \mathrm{Inv}(H)$ 中, 取上文的 $x = ab+bc+ca$，由于 $[\mathbb{Q}(x) : \mathbb{Q}] = 4$（最小多项式的次数），故 $K = \mathbb{Q}(x)$，即 $\sqrt{6}$ 在 $\mathbb{Q}(x)$ 中. □

(4) 求 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{6}+\sqrt{10}+\sqrt{15})$ 上的最小多项式.

证明. $\sqrt{2}+\sqrt{3}$ 不被 $\sigma_a\sigma_b\sigma_c$ 固定，故它不属于 $\mathbb{Q}(x)$，又 $[\mathbb{Q}(a,b,c) : \mathbb{Q}(x)] = 2$，所以最小多项式为 2 次. 又因 $\sigma_a\sigma_b\sigma_c$ 是 $\mathbb{Q}(a,b,c)$ 的 $\mathbb{Q}(x)$-自同构，故 $\sqrt{2}+\sqrt{3}$ 与 $\sigma_a\sigma_b\sigma_c(\sqrt{2}+\sqrt{3}) = -\sqrt{2}-\sqrt{3}$ 有相同的 $\mathbb{Q}(x)$ 上最小多项式，它必然被 $(x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3}) = x^2-2\sqrt{6}-5$ 整除. 由于它的次数为 2，故它就是所求的最小多项式. □

参考文献

[1] zcn (https://math.stackexchange.com/users/115654/zcn). *Is normal extension of normal extension always normal?* Mathematics Stack Exchange. (version: 2014-08-06). eprint: https://math.stackexchange.com/q/888841. URL: https://math.stackexchange.com/q/888841.

[2] Jyrki Lahtonen (https://math.stackexchange.com/users/11619/jyrki-lahtonen). *Intermediate fields of a finite field extension that is not separable.* Mathematics Stack Exchange. (version: 2016-06-13). eprint: https://math.stackexchange.com/q/1824104. URL: https://math.stackexchange.com/q/1824104.

[3] Geoff Robinson (https://math.stackexchange.com/users/13147/geoff-robinson). *Mutual set of representatives for left and right cosets: what about infinite groups?* Mathematics Stack Exchange. (version: 2013-01-01). eprint: https://math.stackexchange.com/q/268274. URL: https://math.stackexchange.com/q/268274.

[4] Ted (https://math.stackexchange.com/users/15012/ted). *The trace of finite dimensional extension F over the finite field K is surjective.* Mathematics Stack Exchange. (version: 2016-11-28). eprint: https://math.stackexchange.com/q/2034062. URL: https://math.stackexchange.com/q/2034062.

[5] MooS (https://math.stackexchange.com/users/211913/moos). *$x^p - x - c$ is irreducible over a field of characteristic p if it has no root in the field.* Mathematics Stack Exchange. (version: 2015-04-28). eprint: https://math.stackexchange.com/q/1256120. URL: https://math.stackexchange.com/q/1256120.

[6] Bill Dubuque (https://math.stackexchange.com/users/242/bill-dubuque). *Polynomial $p(x)$ is a unit (invertible) $\iff$ $p_0 = p(0)$ is a unit, all other coefficients are nilpotent.* Mathematics Stack Exchange. (version: 2021-02-21). eprint: https://math.stackexchange.com/q/83886. URL: https://math.stackexchange.com/q/83886.

[7] Zev Chonoles (https://math.stackexchange.com/users/264/zev-chonoles). *the degree of a splitting field of a polynomial.* Mathematics Stack Exchange. (version: 2018-06-23). eprint: https://math.stackexchange.com/q/62792. URL: https://math.stackexchange.com/q/62792.

[8] Tsemo Aristide (https://math.stackexchange.com/users/280301/tsemo-aristide). *Zero divisor for polynomial ring*. Mathematics Stack Exchange. (version: 2019-09-07). eprint: https://math.stackexchange.com/q/3347812. URL: https://math.stackexchange.com/q/3347812.

[9] rschwieb (https://math.stackexchange.com/users/29335/rschwieb). *Is the zero ring a domain?* Mathematics Stack Exchange. (version: 2017-04-13). eprint: https://math.stackexchange.com/q/1326600. URL: https://math.stackexchange.com/q/1326600.

[10] Pete L. Clark (https://math.stackexchange.com/users/299/pete-l-clark). *Quadratic extensions in characteristic* 2. Mathematics Stack Exchange. (version: 2013-01-30). eprint: https://math.stackexchange.com/q/290032. URL: https://math.stackexchange.com/q/290032.

[11] Shubhodip Mondal (https://math.stackexchange.com/users/32215/shubhodip-mondal). *Show group of order $4n + 2$ has a subgroup of index 2.* Mathematics Stack Exchange. (version: 2014-11-14). eprint: https://math.stackexchange.com/q/229187. URL: https://math.stackexchange.com/q/229187.

[12] Slade (https://math.stackexchange.com/users/33433/slade). *Irreducible polynomial over $\mathbb{Q}[x]$ has even degree if the sum of two distinct roots lies in $\mathbb{Q}$*. Mathematics Stack Exchange. (version: 2019-02-25). eprint: https://math.stackexchange.com/q/3126329. URL: https://math.stackexchange.com/q/3126329.

[13] Camilo Arosemena-Serrato (https://math.stackexchange.com/users/33495/camilo-arosemena-serrato). *$x^p - c$ has no root in a field F if and only if $x^p - c$ is irreducible?* Mathematics Stack Exchange. (version: 2019-09-24). eprint: https://math.stackexchange.com/q/403963. URL: https://math.stackexchange.com/q/403963.

[14] Dylan Moreland (https://math.stackexchange.com/users/3701/dylan-moreland). *Show the norm map is surjective*. Mathematics Stack Exchange. (version: 2017-04-13). eprint: https://math.stackexchange.com/q/143719. URL: https://math.stackexchange.com/q/143719.

[15] HallaSurvivor (https://math.stackexchange.com/users/655547/hallasurvivor). *Prove any subgroup A of n-elements-generated group G has can be generated by $2n[G : A]$ elements*. Mathematics Stack Exchange. (version: 2021-01-13). eprint: https://math.stackexchange.com/q/3983366. URL: https://math.stackexchange.com/q/3983366.

[16] awllower (https://math.stackexchange.com/users/6792/awllower). *About some properties of composites of field extesions*. Mathematics Stack Exchange. (version: 2016-05-11). eprint: https://math.stackexchange.com/q/1780896. URL: https://math.stackexchange.com/q/1780896.

[17] Arturo Magidin (https://math.stackexchange.com/users/742/arturo-magidin). *Classification of prime ideals of $\mathbb{Z}[X]$*. Mathematics Stack Exchange. (version: 2017-10-05). eprint: https://math.stackexchange.com/q/174713. URL: https://math.stackexchange.com/q/174713.

[18] Arturo Magidin (https://math.stackexchange.com/users/742/arturo-magidin). *Why does an irreducible polynomial split into irreducible factors of equal degree over a Galois extension?* Mathematics Stack Exchange. (version: 2011-11-29). eprint: https://math.stackexchange.com/q/86786. URL: https://math.stackexchange.com/q/86786.

[19] H.E (https://math.stackexchange.com/users/74823/h-e). *find a degree and splitting field for* $x^4 - 2$ *over* $\mathbb{Q}(i)$. Mathematics Stack Exchange. (version: 2013-11-20). eprint: https://math.stackexchange.com/q/575060. URL: https://math.stackexchange.com/q/575060.

[20] Nicky Hekster (https://math.stackexchange.com/users/9605/nicky-hekster). *order of a class-preserving automorphism of G have all its prime factor divides* $|G|$. Mathematics Stack Exchange. (version: 2021-02-01). eprint: https://math.stackexchange.com/q/4007847. URL: https://math.stackexchange.com/q/4007847.

[21] Victor Protsak (https://mathoverflow.net/users/5740/victor-protsak). *How would you solve this tantalizing Halmos problem?* MathOverflow. (version: 2010-07-14). eprint: https://mathoverflow.net/q/31790. URL: https://mathoverflow.net/q/31790.

[22] Groupprops contributors. *Equivalence of definitions of nilpotency class*. Groupprops, The Group Properties Wiki (beta). URL: https://groupprops.subwiki.org/w/index.php?title=Equivalence_of_definitions_of_nilpotency_class&oldid=18932.

[23] Groupprops contributors. *Union of all conjugates of subgroup of finite index is proper*. Groupprops, The Group Properties Wiki (beta). URL: https://groupprops.subwiki.org/w/index.php?title=Union_of_all_conjugates_of_subgroup_of_finite_index_is_proper&oldid=33133.

[24] p Groups (https://math.stackexchange.com/users/301282/p-groups). *The number of p-subgroups of a group*. Mathematics Stack Exchange. (version: 2015-12-30). eprint: https://math.stackexchange.com/q/1593829. URL: https://math.stackexchange.com/q/1593829.

[25] Kiyoshi Igusa. *MATH205BNOTES 2010 COMMUTATIVE ALGEBRA*. URL: http://people.brandeis.edu/~igusa/Math205bS10/Math205b_S10_12.pdf.

[26] Kar Shum and Y Guo. "A NEW PROOF OF KAPLANSKY-JACOBSON THEOREM ON ONE-SIDED INVERSES". In: *Scientiae Mathematicae Japonicae Online* (Jan. 2003), pp. 431–433.

[27] user26857. *On irreducible factors of* $x^{2^n} + x + 1$ *in* $\mathbb{Z}_2[x]$. Mathematics Stack Exchange. (version: 2017-10-06). eprint: https://math.stackexchange.com/q/508932. URL: https://math.stackexchange.com/q/508932.

[28] Wikipedia contributors. *Braid goup — Wikipedia, The Free Encyclopedia*. [Online; accessed 4-Feburary-2021]. 2021. URL: https:/en.wikipedia.org/w/index.php?title=Braid_group&oldid=1000230639.

[29] Wikipedia contributors. *Central series — Wikipedia, The Free Encyclopedia*. [Online; accessed 5-March-2021]. 2021. URL: https://en.wikipedia.org/w/index.php?title=Central_series&oldid=1000227178.