近世代数题解

第一章　基本概念

§1. 1

1.

证　任取 $x\in A\cap(B\cup C)$，则

$$x\in A\text{ 且 }x\in B\cup C.\quad\text{从而 }x\in B\text{ 或 }x\in C.$$

若 $x\in B$，则 $x\in A\cap B$. 从而 $x\in(A\cap B)\cup(A\cap C)$. 因此

$$A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C).$$

反之，任取 $x\in(A\cap B)\cup(A\cap C)$，类似可得 $x\in A\cap(B\cup C)$.

故

$$(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C).$$

因此，$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

同理可得 4)中另一等式.

2. 若 $A\cap B=A\cap C$，问：是否 $B=C$？把 $\cap$ 改成 $\cup$ 时又如何？

解　不一定有 $B=C$. 例如

$$A=\{1\},\quad B=\{1,2\},\quad C=\{1,3\}.$$

把 $\cap$ 改成 $\cup$ 后也不一定有 $B=C$. 例如

$$A=\{1\},\quad B=\{2\},\quad C=\{1,2\}.$$

3. 设 A 是有限集合，且 $|A|=n$. 证明：$|P(A)|=2^n$.

证　因为 $|A|=n$，故 A 的含 k $(0\leqslant k\leqslant n)$ 个元素的子集共有 C_n^k 个，从而 A 共有

$$2^n=(1+1)^n=C_n^0+C_n^1+\cdots+C_n^n$$

个子集，即 $|P(A)|=2^n$.

4.

证　设 $|A|=m$，$|B|=n$，$|A\cap B|=k$，则显然

$$|A\cup B|=m+n-k,$$

由此即得要证的等式.

5.

证　设 $x\in(A\cup B)'$，即 $x\notin A\cup B$. 故 $x\notin A$ 且 $x\notin B$. 从而

$$x\in A'\text{ 且 }x\in B'.\quad\text{故 }x\in A'\cap B'.$$

从而 $(A\cup B)'\subseteq A'\cap B'$. 反推上去得 $A'\cap B'\subseteq(A\cup B)'$. 故得证.

另一等式可类似证明.

近世代数题解　§1. 2

2.

解　φ 是映射，且是满射，但不是单射.

3.

解 设 $B=CAC^{-1}$（C 为 F 上 n 阶满秩方阵）. 若 $f(A)=g(A)$，则

$$f(B)=f(CAC^{-1})=Cf(A)C^{-1}$$
$$=Cg(A)C^{-1}=g(CAC^{-1})=g(B).$$

即 φ 是 $F[A]$到 $F[B]$的一个映射. 又类似易知，φ 是单射和满射，从而 φ 是双射.

近世代数题解　§1. 3

1. 解　1)与 3)是代数运算，2)不是代数运算.

2. 解　这实际上就是 M 中 n 个元素可重复的全排列数 n^n.

3. 解　例如 $A\circ B=E$ 与 $A\circ B=AB-A-B$.

4.

解　$|T(M)|=27, |S(M)|=6$. 乘法表从略.

5.

解　例如σ: $1\longrightarrow 2, 2\longrightarrow 1$，其余 $x\longrightarrow x$；

τ: $1\longrightarrow 3, 3\longrightarrow 1$，其余 $x\longrightarrow x$.

近世代数题解　§1. 4

1.

解　结合律和交换律都不满足. 例如

$$(1\circ 0)\circ 0=4,\quad 1\circ(0\circ 0)=2,$$

故$(1\circ 0)\circ 0\neq 1\circ(0\circ 0)$. 又 $1\circ 0=2, 0\circ 1=3$，故 $1\circ 0\neq 0\circ 1$.

2.

解　1) 交换律满足，但结合律不满足. 例如

$$(1\circ 1)\circ 0=4,\quad 1\circ(1\circ 0)=2.$$

2) 结合律、交换律都满足. 因为易知$(a\circ b)\circ c$ 与 $a\circ(b\circ c)$都等于

$$a+b+c-ab-bc-ac+abc.$$

3. 解　1) 略 2) 例如规定

$$a\circ a=a,\quad a\circ b=c.$$

其中 $a, b, c\in M$，但 a, b, c 互异.

4.

解　$\circ$显然是代数运算且满足交换律. 又结合律也满足，因为根据最高公因式的性质知：

$$f\circ(g\circ h)=(f,(g,h))=((f,g),h)=(f\circ g)\circ h.$$

5. 略

近世代数题解　§1. 5

1. 解　1)是自同态映射，但非满射和单射；2)是双射，但不是自同构映射 3)是自同态映射，但非满射和单射. 4)是双射，但非自同构映射.

2. 略

3.

解　例如，φ: $x\longrightarrow 2x$ ($\forall x\in \mathbf{Q}$). 显然，把 2 换成任意一个非 0 及 1 的有理数后，φ 均为 $\mathbf{Q}$ 的非恒等自同构.

4.

解 当$\circ$满足结合律时，$\circ$不一定满足. 例如，M为整数集，代数运算是减法（不满足结合律）；又$\overline{M}=\{1\}$，代数运算为乘法（当然满足结合律）. 但显然

$$\varphi: x \longrightarrow 1 \quad (\forall x \in M)$$

是M到$\overline{M}$的同态满射，故$M \sim \overline{M}$.

5.

证 1) 由$M_1 \cong M_2$，设$\varphi: x \longrightarrow y$ ($\forall x \in M_1$)是其一同构映射，则$\varphi^{-1}: y \longrightarrow x$ (其中$\varphi(x)=y$)显然是M_2到M_1的一个同构映射，故$M_2 \cong M_1$.

2) 同理，由$M_1 \cong M_2$，$M_2 \cong M_3$，分别设有同构映射σ, τ且

$$\sigma: a \longrightarrow b, \qquad \tau: b \longrightarrow c.$$

则$\tau\sigma: a \longrightarrow c$是$M_1$到$M_3$的同构映射，故$M_1 \cong M_3$.

（应注意，$\tau\sigma$不能写成$\sigma\tau$. 因为此时$\sigma\tau$是无意义的.）

§1. 6

1.

解 R是M的一个关系. 又显然满足对称性. 但是，反身性和传递性不满足. 例如，$1 \overline{R} 1$；又显然

$$4 \mid 3+1, \ 4 \mid 1+7, \quad \text{但是} \ 4 \nmid 3+7,$$

即$3R1, 1R7$，但是$3 \overline{R} 7$.

2. 解 1)不是. 因为不满足对称性；2)不是. 因为不满足传递性；
3)是等价关系；4)是等价关系.

3. 解 3)每个元素是一个类，4)整个实数集作成一个类.

4.

解 上面第2题中1)与2)是符合本题题意的两个例子. 又设$\mathbf{Q}$是有理数集，规定

$$aRb \Longleftrightarrow a^2+b^2=0 \quad (a, b \in \mathbf{Q}).$$

则易知此关系不满足反身性，但是却满足对称性和传递性（若把$\mathbf{Q}$换成实数域的任一子域均可；实际上这个例子只有数0和0符合关系，此外任何二有理数都不符合关系）.

5.

证 若M中二元素a与b符合关系就记为(a, b). 现在一切这样的(a, b)作成的集合记为R_1，它是R的一个子集.

反之，设$R_2 \subseteq R$. 则规定：a与b符合关系当且仅当

$$(a, b) \in R_2.$$

即R的子集可决定M的一个关系.

6. 证 1) 略 2)

由1)及分配性以及习题1.1第5题可知：

$$(A \cup B) - (A \cap B) = (A \cup B) \cap (A \cap B)'$$

$$=(A\cup B)\cap(A'\cup B'); \qquad (1)$$

又$(A-B)\cup(B-A)=(A\cap B')\cup(B\cap A')$

$$=[(A\cap B')\cup B]\cap[(A\cap B')\cup A']$$

$$=[(A\cup B)\cap(B\cup B')]\cap[(A\cup A')\cap(A'\cup B')]$$

$$=(A\cup B)\cap(A'\cup B'). \qquad (2)$$

由(1)与(2)知,得证.

7.

证 1) 任取 $x\in A$,则 $\varphi(x)\in\varphi(A)$. 从而

$$x\in\varphi^{-1}(\varphi(A)),\quad \text{故 } A\subseteq\varphi^{-1}(\varphi(A)).$$

若 φ 是单射,则任取 $y\in\varphi^{-1}(\varphi(A))$,必 $\varphi(y)\in\varphi(A)$,从而有 $x\in A$ 使 $\varphi(x)=\varphi(y)$. 但因 φ 是单射,故

$$y=x\in A,\quad \varphi^{-1}(\varphi(A))\subseteq A.$$

因此 $\varphi^{-1}(\varphi(A))=A$.

2) 任取 $y\in\varphi(\varphi^{-1}(B))$,则有 $x\in\varphi^{-1}(B)$使 $y=\varphi(x)$. 但由于 $x\in\varphi^{-1}(B)$,故 $\varphi(x)\in B$,即 $y=\varphi(x)\in B$. 因此

$$\varphi(\varphi^{-1}(B))\subseteq B.$$

又当 φ 为满射时,任取 $x'\in B$,则存在 $x\in X$ 使 $\varphi(x)=x'$. 于是

$$x\in\varphi^{-1}(B),\quad \varphi(x)\in\varphi(\varphi^{-1}(B)),$$

即 $x'\in\varphi(\varphi^{-1}(B))$,故又有 $B\subseteq\varphi(\varphi^{-1}(B))$,因此

$$\varphi(\varphi^{-1}(B))=B.$$

8.

证 1) 任取 $y\in\varphi(A\cup B)$,则存在 $x\in A\cup B$,使 $y=\varphi(x)$.

若 $x\in A$,则 $\varphi(x)\in\varphi(A)$,于是

$$y=\varphi(x)\in\varphi(A)\cup\varphi(B);$$

若 $x\in B$,则同理可得上式. 因此

$$\varphi(A\cup B)\subseteq\varphi(A)\cup\varphi(B).$$

反之,任取 $y\in\varphi(A)\cup\varphi(B)$,不妨设 $y\in\varphi(A)$,于是存在 $x\in A$使 $y=\varphi(x)$. 而 $x\in A\subseteq A\cup B$,因此

$$y=\varphi(x)\in\varphi(A\cup B),$$

从而 $\varphi(A)\cup\varphi(B)\subseteq\varphi(A\cup B)$. 故

$$\varphi(A)\cup\varphi(B)=\varphi(A\cup B).$$

2) 任取 $y\in\varphi(A\cap B)$,则有 $x\in A\cap B$ 使 $\varphi(x)=y$.

由于 $x\in A\cap B$,故 $x\in A$,$x\in B$. 从而

$$y=\varphi(x)\in\varphi(A),\quad y=\varphi(x)\in\varphi(B),$$

因此,$y\in\varphi(A)\cap\varphi(B)$. 故

$$\varphi(A\cap B)\subseteq\varphi(A)\cap\varphi(B).$$

9.

证 1) 乘积 $\tau\sigma$ 是集合 A 到 C 的映射. 设 $x_1, x_2 \in A$, 且 $x_1 \neq x_2$, 则由于 σ 是单射, 故

$$\sigma(x_1) \neq \sigma(x_2);$$

又由于 τ 是单射, 因此

$$\tau(\sigma(x_1)) \neq \tau(\sigma(x_2)), \quad \text{即} (\tau\sigma)(x_1) \neq (\tau\sigma)(x_2),$$

故 $\tau\sigma$ 是集合 A 到 C 的单射.

反之, 设 $\tau\sigma$ 是 A 到 C 的单射, 则对 A 中任二不同元素 x_1, x_2 有

$$(\tau\sigma)(x_1) \neq (\tau\sigma)(x_2), \quad \tau[\sigma(x_1)] \neq \tau[\sigma(x_2)].$$

从而 $\sigma(x_1) \neq \sigma(x_2)$, 即 σ 是 A 到 B 的单射.

2) 设 σ, τ 都是满射, 则任取 $c \in C$, 由于 τ 是满射, 故存在 $b \in B$ 使

$$\tau(b) = c. \tag{1}$$

又由于 σ 是 A 到 B 的满射, 故对于 $b \in B$ 有 $a \in A$ 使

$$\sigma(a) = b. \tag{2}$$

从而由(1), (2)得

$$\tau[\sigma(a)] = c, \quad \text{即} (\tau\sigma)(a) = c.$$

亦即 $\tau\sigma$ 是 A 到 C 的满射.

反之, 设乘积 $\tau\sigma$ 是 A 到 C 的满射. 则任取 $c \in C$, 必有 $a \in A$ 使

$$(\tau\sigma)(a) = c, \quad \text{即} \tau[\sigma(a)] = c.$$

现令 $b = \sigma(a) \in B$, 则 $\tau(b) = c$. 故 τ 是集合 B 到 C 的满射.

注 应注意, 当 $\tau\sigma$ 是单射时, τ 不一定是单射. 例如, A 是正整数集合, B 与 C 都是整数集合, 又

$$\sigma: A \longrightarrow B, \quad a \longrightarrow a^2$$
$$\tau: B \longrightarrow C, \quad b \longrightarrow |b|,$$

则易知乘积 $\tau\sigma$ 是单射, 但 τ 不是单射.

对满射也可举出类似例子.

10.

证 1) 设 σ 是单射, 令 $B' = \{b' \mid b' \in B, b' \notin \sigma(A)\}$, 则

$$B = \sigma(A) \cup B', \quad \text{且} \sigma(A) \cap B' = \varnothing$$

现任取一固定 $a' \in A$, 则由于 σ 是单射, 故易知

$$\tau: b \longrightarrow a, \quad \text{当} b \in \sigma(A), b = \sigma(a);$$
$$b' \longrightarrow a', \quad \text{当} b' \in B'.$$

是集合 B 到 A 的一个映射, 且对任意 $a \in A$ 都有

$$(\tau\sigma)(a) = a, \quad \text{即} \tau\sigma = 1_A.$$

反之, 若存在映射 $\tau: B \longrightarrow A$ 使 $\tau\sigma = 1_A$, 则因 1_A 是双射, 当然是单射, 故由上题知, σ 是单射.

2) 设 σ 是满射，则任取 $b\in B$，在 A 的子集 $\sigma^{-1}(b)$ 中任意取定一个元素 a，并令

$$\tau: B\longrightarrow A,\quad b\longrightarrow \tau(b)=a,$$

其中 $\sigma(a)=b$. 于是显然对任意 $b\in B$ 都有

$$(\sigma\tau)(b)=\sigma(\tau(b))=\sigma(a)=b.$$

因此 $\sigma\tau=1_B$.

反之，若存在映射 $\tau: B\longrightarrow A$ 使 $\sigma\tau=1_B$，则由于 1_B 是双射，当然是满射，故由上题知，σ 是满射.

11.

证 1) 设 σ 是单射，且 $\sigma\tau_1=\sigma\tau_2$，其中 τ_1,τ_2 都是集合 X 到 A 的映射，则任取 $a\in X$，有

$$(\sigma\tau_1)(a)=(\sigma\tau_2)(a),\quad \sigma(\tau_1(a))=\sigma(\tau_2(a)).$$

因为 σ 是单射，故 $\tau_1(a)=\tau_2(a)$，从而 $\tau_1=\tau_2$.

反之，设对任意集合 X 到 A 的任意映射 τ_1,τ_2，由 $\sigma\tau_1=\sigma\tau_2$ 可得 $\tau_1=\tau_2$，则 σ 必为单射. 因若不然，则在 A 中存在元素 $a_1\neq a_2$，使 $\sigma(a_1)=\sigma(a_2)$. 今取 $X=A$，并令 $\tau_1: x\longrightarrow a_1$ 与 $\tau_2: x\longrightarrow a_2$ $(\forall x\in X)$，则

$$(\sigma\tau_1)(x)=\sigma(\tau_1(x))=\sigma(a_1),$$
$$(\sigma\tau_2)(x)=\sigma(\tau_2(x))=\sigma(a_2).$$

但因 $\sigma(a_1)=\sigma(a_2)$，故 $(\sigma\tau_1)(x)=(\sigma\tau_2)(x)$，从而

$$\sigma\tau_1=\sigma\tau_2.$$

又由于 $\tau_1(x)=a_1\neq a_2=\tau_2(x)$，故 $\tau_1\neq\tau_2$. 这与假设矛盾. 因此 σ 必为单射.

2) 设 σ 为满射，且 $\tau_1\sigma=\tau_2\sigma$，其中 τ_1,τ_2 是集合 B 到集合 Y 的两个映射. 则对任意 $b\in B$ 有 $a\in A$ 使 $\sigma(a)=b$. 于是

$$(\tau_1\sigma)(a)=(\tau_2\sigma)(a),\quad \tau_1(b)=\tau_2(b).$$

因此 $\tau_1=\tau_2$.

反之，设对 B 到任意集合 Y 的任意映射 τ_1,τ_2 有 $\tau_1\sigma=\tau_2\sigma$ 必有 $\tau_1=\tau_2$，则 σ 必为满射. 因若不然，则必

$$B'=B-\sigma(A)\neq\varnothing;$$

再任取一个阶不小于 2 的集合 Y，则在 Y 中任意取定元素 y 及 $y_1\neq y_2$，易知

$$\tau_1: b\longrightarrow y, b'\longrightarrow y_1 \quad 与 \quad \tau_2: b\longrightarrow y, b'\longrightarrow y_2$$

是 B 到 Y 的两个不同映射，其中

$$b\in\sigma(A),\qquad b'\in B'.$$

且对集合 A 中任意元素 a 都有

$$(\tau_1\sigma)(a)=\tau_1(\sigma(a))=y,$$
$$(\tau_2\sigma)(a)=\tau_2(\sigma(a))=y.$$

从而 $\tau_1\sigma=\tau_2\sigma$. 但是 $\tau_1\neq\tau_2$，矛盾.

因此，σ 必为满射.

12.

证　反证法. 假设 $P(A)$ 与 A 之间存在双射 f，令

$$A_1=\{f(M)\mid M\in P(A), f(M)\notin M\}.$$

下面来考察 $f(A_1)$.

若 $f(A_1)\in A_1$，则根据 A_1 之定义，A_1 中无 $f(A_1)$，矛盾；若 $f(A_1)\notin A_1$，则同样根据 A_1 之定义，又有 $f(A_1)\in A_1$，也矛盾. 因此，$P(A)$ 与 A 之间不存在双射.

第二章　群

§2. 1　群的定义和初步性质

一、主要内容

1. 群和半群的定义和例子特别是一船线性群、n 次单位根群和四元数群等例子.

2. 群的初步性质

1) 群中左单位元也是右单位元且惟一；

2) 群中每个元素的左逆元也是右逆元且惟一；

3) 半群 G 是群 $\Leftrightarrow$ 方程 $ax=b$ 与 $ya=b$ 在 G 中有解（$\forall a, b\in G$）.

4) 有限半群作成群 $\Leftrightarrow$ 两个消去律成立.

二、释疑解难

有资料指出，群有 50 多种不同的定义方法. 但最常用的有以下四种：

1) 教材中的定义方法. 简称为“左左定义法”；

2) 把左单位元换成有单位元，把左逆元换成右逆元（其余不动）. 简称为“右右定义法”；

3) 不分左右，把单位元和逆元都规定成双边的，此简称为“双边定义法”；

4) 半群 G 再加上方程 $ax=b$ 与 $ya=b$ 在 G 中有解（$\forall a, b\in G$）. 此简称为“方程定义法”.

“左左定义法”与“右右定义法”无甚差异，不再多说.“双边定义法”缺点是定义中条件不完全独立，而且在验算一个群的实例时必须验证单位元和逆元都是双边的，多了一层手续（虽然这层手续一般是比较容易的）；优点是：①不用再去证明左单位元也是右单位元，左逆元也是右逆元；②从群定义本身的条件直接体现了左与右的对称性.

在数的运算中，如果 $ax=b$（$a\neq0$），则 $x=\frac{b}{a}$，体现了在数中可以施行除法运算，即乘法的逆运算. 如果我们把群的运算也叫做“乘法”，那么在群中方程 $ax=b$（a,b 是群中任意元素，无任何限制）有解，记为 $x=\frac{b}{a}$（实为 $a^{-1}b$）；同时方程 $ya=b$ 也有解，也暂时记为 $y=b/a$（实为 ba^{-1}）. 当然，由于“乘法”不一定可换，$\frac{b}{a}$ 与 b/a（即 $a^{-1}b$ 与 ba^{-1}）不一定相等. 但无论如何这体现了在群中可以施行“除法运算”，即“乘法”的逆运算. 因此，群的‘方程定义法”直接体现了在群中可以施行“乘法与除法”运算. 于是简言之，可以施行乘法与除法运算的半群就是群.

为了开阔视野，再给出以下群的另一定义.

定义　一个半群 G 如果满足以下条件则称为一个群：对 G 中任意元素 a，在 G 中都存在元素 a^{-1}，对 G 中任意元素 b 都有

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

这个定义与前面 4 种定义的等价性留给读者作为练习.

2．在群的“方程定义法”中，要求方程 $a\,x=b$ 与 $y\,a=b$ 都有解缺一不可．即其中一个方程有解并不能保证另一个方程也有解．

例 1 设 G 为阶大于 1 的任意集合，规定

$$a\circ b=b \quad (\forall\, a,b\in G).$$

则 G 对运算$\circ$显然作成一个半群，且方程 $ax=b$（这里省略符号$\circ$）在 G 中有解 $x=b$．但是方程 $ya=b\ (a\neq b)$ 在 G 中却无解．实际上，此时 G 对$\circ$只能作成半群而不能作成群．

同理在 G 中若规定 $a\circ b=a\ (\forall\, a,b\in G)$，则方程 $ya=b$ 在 G 中有解而 $ax=b\ (a\neq b)$ 在 G 中无解．

3．群定义中说：“每个元素都有左逆元”是对同一个左单位元来说的．

例 2 设 $G=\{e_1,e_2\}$，规定 $ab=b\ (\forall\, a,b\in G)$．则 G 作成半群，且显然 e_1 与 e_2 都是 G 的左单位元．又因为

$$e_1e_1=e_1,\quad e_2e_1=e_1;\quad e_2e_2=e_2,\quad e_1e_2=e_2,$$

即对左单位元 e_1 来说，e_1 有左逆元 e_1 及 e_2；而对左单位元 e_2 来说，e_2 也有左逆元 e_1 及 e_2．就是说，虽然 G 中每个元素都有左逆元，但不是对同一个左单位元有左逆元，因此 G 不作成群．

4．关于结合律

若代数运算不是普通的运算(例如，数的普通加法与乘法，多项式的普通加法与乘法以及矩阵、变换和线性变换的普通加法或乘法)，则在一般情况下，验算结合律是否成立比较麻烦．因此在代数系统有限的情况下，有不少根据乘法表来研究检验结合律是否成立的方法．但无论哪种方法，一般都不是太简单．

5．关于消去律．

根据教材推论 2，对有限半群是否作成群只用看消去律是否成立．而消去律是否成立，从乘法表很容易看出，因为只要乘法表中每行和每列中的元素互异即可．

6．在群定义中是否可要求有“左”单位元而每个元素有“右”逆元呢？

答　不可以，例如上面例 2 就可以说明这个问题，因为 e_1 是左单位元，而 e_1 与 e_2 都有右逆元且均为 e_1．但 G 并不是群．

7．群与对称的关系．

1)世界万物，形态各异．但其中有无数大量事物部具有这样或那样的对称性．而在这些具有对称性的万事万物中，左右对称又是最为常见的．

由群的定义本身可知，从代数运算到结合律，特别是左、右单位元和左、右逆元，均体现出左右对称的本质属性．

2)几何对称．

设有某一几何图形，如果我们已经找到了它的全部对称变换(即平常的反射、旋转、反演和平移变换的统称)，则此对称变换的全体关于变换的乘法作成一个群，称为该图形的完全对称群．这个图形的对称性和它的完全对称群是密切相关的．凡对称图形(即经过对称变换保持不变的图形、亦即完成这种变换前后的图形重合)，总存在若干个非恒等对称变换和恒等变换一起构成该图形的完全对称群．反之，如果一个图形存在着非平凡的对称变换，则该图形就是对称图形．不是对称的图形，就不能有非恒等的对称变换．显然，一个图形的对称程度越高，则该图形的对称变换就越多．也就是说它的完全对称群的阶数就越高，即图形对称程度的高低与其对称群的阶数密切相关．因此；这就启发人们用群去刻面对称图形及其性质，用群的理论去研究对称．所以人们就把群论说成是研究对称的数学理论．

3）代数对称．

数域 F 上任何一个 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 总有集合 $S=\{x_1,x_2,\cdots,x_n\}$ 上的 n 次置换使 f 不变；至少恒等变换就是一个．由于使 f 不变的任二 n 次置换之积显然仍使 f 不变，故由教材 §3 可知，使 f 不变的全体 n 次置换作成一个 n 次置换群．它是 S 上 n 次对称群 S_n 的一个子群，我们称其为 n 元多项式 f 的 n 次置换群．

显然，每个 n 元多项式都有一个确定的 n 次置换群：例如 n 元多项式

$$f(x_1,x_2,\cdots,x_n)=x_1+2x_2+\cdots+nx^n$$

的置换群是恒等置换，而 $g(x_1,x_2,\cdots,x_n)=a$（常数）的置换群是 n 次对称群 S_n，等等.

例 3 求三元多项式

$$f(x_1,x_2,x_3)=(x_1-x_2)(x_1-x_3)(x_2-x_3)$$

的置换群.

解 为了书写方便起见，在以下置换中我们把 x_i 简记为 i. 易知 f 的置换群为由置换

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

作成的 3 阶群.

例 4 求四元多项式 $g=x_1x_2-x_3x_4$ 的置换群.

解 易知 g 的置换群为由置换

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

作成的 4 阶群.

例 5 求四元多项式 $h=x_1x_2+x_3x_4$ 的置换群.

解 易知，h 的置换群由 8 个置换组成. 其中 4 个即上例中的 4 个置换，另 4 个置换为：

$$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

例 6 任何 n 元对称多项式的置换群都是 n 次对称群.

很显然，一个多元多项式的置换群的阶数越高，这个多元多项式的对称性越强. 反之亦然. 因此，我们通常所熟知的多元对称多项式是对称性最强的多项式.

三、习题 2. 1 解答

1. 略

2.

解 可验算 N 对此代数运算作成可交换的幺半群（单位元是 $0\in\mathbf{N}$）. 但不是每个元素都有逆元，例如 1 就没有逆元：因若

$$x\circ 1=x+1+x=0,\quad \text{则 } 2x=-1.$$

从而 $x=-\frac{1}{2}\notin\mathbf{N}$. 故 N 对 $\circ$ 不作成群.

3.

证 设 $\boldsymbol{A},\boldsymbol{B}\in O_n(\mathbf{R})$，即

$$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}=\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}=\boldsymbol{E}.$$

由此得 $(\boldsymbol{A}\boldsymbol{B})(\boldsymbol{A}\boldsymbol{B})^{\mathrm{T}}=\boldsymbol{A}\boldsymbol{B}\cdot\boldsymbol{B}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}=\boldsymbol{E}$. 从而 $\boldsymbol{A}\boldsymbol{B}\in O_n(\mathbf{R})$. 又

$$\boldsymbol{A}^{-1}\cdot(\boldsymbol{A}^{-1})^{\mathrm{T}}=\boldsymbol{A}^{-1}\cdot(\boldsymbol{A}^{\mathrm{T}})^{-1}=\boldsymbol{A}^{-1}\cdot(\boldsymbol{A}^{-1})^{-1}=\boldsymbol{E},$$

故 $\boldsymbol{A}^{-1}\in O_n(\mathbf{R})$. 从而 $O_n(\mathbf{R})$ 作成群.

4.

证 新运算显然是 G 的一个代数运算. 结合律成立，验算从略. 又因为对 G 中任意元 a 有

$$u^{-1}\circ a=u^{-1}ua=a,\quad (uau)^{-1}\circ a=u^{-1},$$

故 u^{-1} 是 $(G,\circ)$ 的左单位元，$(uau)^{-1}$ 是 $(G,\circ)$ 中 a 的左逆元，故 G 对新运算也作成群.

5.

证 显然 G 非空. 又在 G 中任取 $(a,b),(c,d)$，其中 a,b,c,d 是实数且 $a\neq 0,c\neq 0$. 于是 $ac,ad+b$ 都是实数且 $ac\neq 0$，从而

$$(a,b)\circ(c,d)=(ac,ad+b)\in G.$$

即 $\circ$ 是 G 的一个代数运算.

再任取 $(e,f)\in G$，则有

$$\begin{aligned}[(a,b)\circ(c,d)]\circ(e,f)&=(ac,ad+b)\circ(e,f)\\&=(ace,acf+ad+b),\\(a,b)\circ[(c,d)\circ(e,f)]&=(a,b)\circ(ce,cf+d)\\&=(ace,acf+ad+b),\end{aligned}$$

从而 $[(a,b)\circ(c,d)]\circ(e,f)=(a,b)\circ[(c,d)\circ(e,f)]$，即 G 对 $\circ$ 满足结合律.

又易知 $(1,0)$ 是 G 的左单位元，且 (a,b) 的左逆元为

$$\left(\frac{1}{a},-\frac{b}{a}\right)\in G.$$

因此，G 对 $\circ$ 作成一个群.

又 G 不是交换群，因为例如易知

$$(3,6)=(1,2)\circ(3,4)\neq(3,4)\circ(1,2)=(3,10).$$

6.

证法 I 任取 $a,b\in G$，由于 $(ab)^2=a^2=b^2=e$，故

$$\begin{aligned}ab&=a(ab)^2b=a(ab)(ab)b\\&=a^2bab^2=ba.\end{aligned}$$

从而 $ab=ba$，所以 G 是交换群.

证法 II 任取 $a\in G$，由于 $a^2=e$，故 $a=a^{-1}$，即 G 中每个元素的逆元都是自身，从而

$$ab=(ab)^{-1}=b^{-1}a^{-1}=ba,$$

即 G 为交换群.

§2. 2 群中元素的阶

一、主要内容

1. 群中元素的阶的定义及例子. 周期群、无扭群与混合群的定义及例子. 特别，有限群必为周期群，但反之不成立.

2. 在群中若 $|a|=n$，则

1) $a^m=e\Longleftrightarrow n\mid m$；

2) $|a^k|=\dfrac{n}{(k,n)}$；

3) $|a^k|=n\Longleftrightarrow(k,n)=1$；

4) $|a|=n=st\Longrightarrow|a^s|=t$.

3. $|a|,|b|$ 与 $|ab|$ 各种关系及例子. 特别是：

$$(|a|,|b|)=1,ab=ba\Longrightarrow|ab|=|a|\cdot|b|.$$

4. 若 G 是交换群，又 G 中元素有最大阶 m，则 G 中每个元素的阶都是 m 的因子.

二、释疑解难

1. 有的书把群中元素的阶称为周期. 元素 a 的阶多用 $|a|$ 表示，但也有的书用 $o(a)$ 表示(取英文 order 的字首).

2. 由元素 a 的阶可以决定 a^k 的阶.

若 $|a|=\infty$，则当 k 为非零整数时，$|a^k|=\infty$ ($a^0=e$ 阶为 1).

若 $|a|=n$，则 $|a^k|=\dfrac{n}{(k,n)}$ (定理 3).

3. $|a|$、$|b|$ 与 $|ab|$ 的关系.

在群中，由元素 a 与 b 的阶一般决定不了乘积 ab 的阶，这由教材中所举的各种例子已经说明了这一点. 对此应十分注意. 但是，在一定条件下可以由阶 $|a|$ 与 $|b|$ 决定阶 $|ab|$，这就是教材中朗定理 4:

$$ab=ba,\ (|a|,|b|)=1 \Longrightarrow |ab|=|a|\cdot|b|.$$

4. 一个群中是否有最大阶元?

有限群中元素的阶均有限，当然有最大阶元. 无限群中若元素的阶有无限的(如正有理数乘群或整数加群)，则当然无最大阶元，若无限群中所有元素的阶均有限(即无限周期群)，则可能无最大阶元，如教材中的例 4:

$$U=\bigcup_{n=1} U_n,\quad U_n \text{ 为 } n \text{ 次单位根群.}$$

下面再举两个(一个可换，另一个不可换)无限群有最大阶元的例子.

例 1 用 Z_n 表示模 n 剩余类环(参考教材第四章 § 5)，$Z_n[x]$ 为环 Z_n 上的多项式环，它是一个无限交换环. 但作为加群，记为 $(Z_n[x],+)$，它是一个无限交换群，而且有最大阶元，其最大阶是 n(即环 Z_n 与 $Z_n[x]$ 的特征).

例 2 令 S_3 为三次对称群，C_6 是 6 阶循环群. 并令 G 为包含一切

$$(x,x_1,x_2,\cdots)$$

作成的集合，其中 $x\in S_3$，$x_i\in C_6$，但只有有限个 $x_i\neq e$. G 中元素相等当且仅当对应分量相等.

现对 G 规定乘法如下:

$$(x,x_1,x_2,\cdots)(y,y_1,y_2,\cdots)=(xy,x_1y_1,x_2y_2,\cdots).$$

则 G 对此运算显然作成一个群，又

$$((1),e,e,\cdots)$$

显然为其单位元且 $(x,x_1,x_2,\cdots)$ 的逆元为

$$(x^{-1},x_1^{-1},x_2^{-1},\cdots).$$

由于 S_3 是一个 6 阶非交换群，故显然 G 是一个无限非交换群. 又因 S_3 与 C_6 中元素的阶均有限，各为 1,2,3,6，从而 G 中元素的阶也如此. 并且 G 中元素的最大阶为 6.

5. 利用元素的阶对群进行分类，是研究群的重要方法之一. 例如，利用元素的阶我们可以把群分成三类，即周期群、无扭群与混合群. 而在周期群中又可分出 p—群 (p 是素数)，从而有 2—群、3—群、5—群等等. 再由教材 § 3. 9 知，每个有限交换群(一种特殊的周期群)都可惟一地分解为素幂阶循环 p—群的直积，从而也可见研究 p—群的重要意义.

三、习题 2. 2 解答

1.

证 1) 设 $|a|=n$，则 $(cac^{-1})^n=ca^nc^{-1}=e$.

又若 $(cac^{-1})^m=e$，则 $ca^mc^{-1}=e$，$a^m=e$. 从而

$$n|m,\quad \text{故 } |cac^{-1}|=n=|a|.$$

2) $ab=b^{-1}(ba)b$.

3) $abc=a(bca)a^{-1}=c^{-1}(cab)c$.

2.

解 1) 设

$$a=\begin{pmatrix}1 & 3\\ 0 & 2\end{pmatrix},\quad b=\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}.$$

则易知：$a^n=\begin{pmatrix}1 & *\\ 0 & 2^n\end{pmatrix}\neq\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$，故$|a|=\infty$.

又易知$|b|=2$. 但是

$$ab=\begin{pmatrix}1 & -2\\ 0 & -2\end{pmatrix}$$

的阶无限，即$|ab|=\infty$.

2) 例如，设

$$a=\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix},\quad b=\begin{pmatrix}1 & 3\\ 0 & -1\end{pmatrix}.$$

则易知：$|a|=\infty$，$|b|=2$，$|ab|=2$.

3.

证 若G中除e外其余元素的阶均无限，则结论已对；若G中非e的元素的阶都是n，且n是一个合数，设

$$n=mt,\quad 1<m,t<n.$$

则对G中任意元素a有$|a^m|=t\neq n$，这与G中非e的元素的阶都是n矛盾，故n必为一素数.

4.

证 1) 设G是一个有限群，a是G的任意一个阶大于2的元素，则显然

$$a\neq a^{-1}\ (\text{否则将有 } a^2=e).$$

但a与a^{-1}有相同的阶，即a^{-1}的阶也大于2.

又设b也是G中一个阶大于2的元素，且

$$b\neq a,\quad b\neq a^{-1},$$

则易知$b^{-1}\neq a$，$b^{-1}\neq a^{-1}$.

这就是说，G中阶大于2的元素是成对出现的. 由于G是有限群，故G的阶大于2的元素的个数必为偶数.

2) 设G是一个偶数阶有限群. 由于单位元是阶为1的惟一元素，又由1)知G中阶大于2的元素的个数是偶数，故G中阶数等于2的元素的个数一定是奇数.

5.

证 设$a^s=a^t$，则$a^{s-t}=e$. 由于$|a|=n$，故$n|(s-t)$. 反之，倒推回去即得.

6.

证　1）存在性. 由于$(m,n)=1$，故存在整数s,t使

$$ms+nt=1. \tag{1}$$

令$b=a^{nt}$，$c=a^{ms}$，则显然$a=bc=cb$. 又

$$b^m=(a^{nt})^m=(a^{mn})^t=e;$$

若又有$b^r=e$，则$a^{rnt}=e$. 但是$|a|=mn$，故

$$mn\mid rnt,\quad m\mid rt.$$

又由(1)知$(m,t)=1$，故$m\mid r$. 因此$|b|=m$.

同理可证$|c|=n$.

2）惟一性. 设另有b_1,c_1使

$$a=b_1c_1=c_1b_1,\quad |b_1|=m,\quad |c_1|=n,$$

则

$$a^{nt}=b_1^{nt}c_1^{nt}=b_1^{nt}. \tag{2}$$

但由(1)知，$nt=1-ms$，故

$$b_1^{nt}=b_1^{1-ms}=b_1(b_1^{ms})^{-1}=b_1.$$

从而由(2)知，$b_1=a^{nt}=b$.

由$b_1=b$又得

$$c_1=b_1^{-1}a=a^{-nt}a=a^{1-nt}=a^{ms}=c.$$

即$b_1=b,c_1=c$.

注　此题显然可推广到更一般的情形，即若

$$|a|=n=n_1n_2\cdots n_s,$$

其中正整数$n_1,n_2,\cdots,n_s$两两互素，则a可惟一地表示成

$$a=a_1a_2\cdots a_s,$$

其中$a_ia_j=a_ja_i$，又a_i是a的方幂，且$|a_i|=n_i$.

其证明方法是对s用数学归纳法.

§2.3　子　群

一、主要内容

1. 子群的定义和例子. 特别是，特殊线性群(行列式等于 1 的方阵)是一般线性群(行列式不等于零的方阵)的子群.

2. 群G的非空子集H作成子群的两个等价条件：

1) $a,b\in H\Longrightarrow ab\in H,a^{-1}\in H$(或$HH=H,H^{-1}=H$)；

2) $a,b\in H\Longrightarrow ab^{-1}\in H$(或$HH^{-1}=H$).

3. 二子群H与K之积HK仍是子群的充要条件为：$HK=KH$.

4. 群的中心元和中心的定义.

二、释疑解难

1．关于真子群的定义.

教材把非平凡的子群叫做真子群. 也有的书把非G的子群叫做群G的真子群. 不同的定义在讨论子群时各有利弊. 好在差异不大，看参考书时应予留意.

2. 如果H与G是两个群，且$H\subseteq G$，那么能不能说H就是G的子群?

答：不能. 因为子群必须是对原群的代数运算作成的群. 例如，设G是有理数加群，而H是正有理数乘群，二者都是群，且$H\subseteq G$但是不能说H是G的子群.

3. 定理 5 （$HK\leqslant G \Longleftrightarrow HK=KH$）的反例.

例 1 在三次对称群 S_3 中（参考第二章 §5），显然

$$H=\{(1),(12)\},\quad K=\{(1),(13)\}$$

都是 S_3 的子群. 但是易知：

$$HK=\{(1),(12),(13),(132)\},$$

$$KH=\{(1),(12),(13),(123)\},$$

从而 $HK\neq KH$，故 HK 不是子群. 对此例来说，也能直接看出 HK 不能作成子群，因为例如

$$(13),(132)\in HK,\quad \text{但是}(13)(132)=(23)\notin HK.$$

即乘积 HK 对置换的乘法不封闭.

4. 设 $H,K\leqslant G$，且 $HK=KH$. 这是否意味着 H 中元素与 K 中元素相乘时可以交换？

答：不能这样认为. 举例如下.

例2 设 G 是四元数群. 则显然 H 是 G 的两个子群且易知

$$HK=KH=\{1,-1,i,-i,j,-j,k,-k\}=G.$$

但是 $ij\neq ji$ $(i\in H,j\in K)$.

$HK=KH$ 是两个集合的相等. 因此，对 HK 中任一元素 hk $(h\in H,k\in K)$，必存在元素 $k_1\in K,h_1\in H$ 使

$$hk=k_1h_1.$$

反之亦然.

三、习题 2. 3 解答

1. 证 略.

2. 证 必要性显然，下证充分性.

设子集 H 对群 G 的乘法封闭，则对 H 中任意元素 a 和任意正整数 m 都有 $a^m\in H$.

由于 H 中每个元素的阶都有限，设 $|a|=n$，则

$$a^n=e\in H.$$

从而 $a\cdot a^{n-1}=e$，亦即又有 $a^{-1}=a^{n-1}\in H$. 故 $H\leqslant G$.

3.

证 设 H 是由交换群 G 中所有有限阶元作成的集合. 显然 $e\in H$，故 H 非空. 又若 $a,b\in H$，设 $|a|=m,|b|=n$. 因 G 可换，故 $(ab)^{[m,n]}=e$，从而 $ab\in H$. 又因 $|a^{-1}|=|a|$，故 $a^{-1}\in H$. 因此，$H\leqslant G$.

对非交换群一般不成立. 例如，有理数域 Q 上全体 2 阶可逆方阵作成的乘群中，易知

$$a=\begin{pmatrix}1 & 2\\ 0 & -1\end{pmatrix},\quad b=\begin{pmatrix}1 & 3\\ 0 & -1\end{pmatrix}$$

的阶有限，都是 2，但易知其乘积

$$ab=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

的阶却无限. 即其全体有限阶元素对乘法不封闭，故不能作成子群.

4. 证　由高等代数知，与所有 n 阶可逆方阵可换的方阵为全体纯量方阵，由此即得证.

5. 证　因为 $(m, n)=1$，故存在整数 s，t 使

$$ms+nt=1.$$

由此可得

$$a=a^{ms+nt}=(a^m)^s(a^n)^t.$$

但是由题设 $a^m, a^n\in H$，而 $H\leqslant G$，故

$$a=(a^m)^s\cdot(a^n)^t\in H.$$

6.

证法Ⅰ　由于 G 中每个元素都满足方程 $x^2=e$，而 $|e|=1$，故 G 中除 e 外的元素的阶都是 2，从而每个元素的逆元均为自身.

由于 $|G|>2$，在 G 中任取 $a\neq e, b\neq e, a\neq b$，则由此可知，$e, a, b, ab$ 是 G 中 4 个不同的元素. 而由习题 2.1 第 6 题知，G 又是一个交换群，从而易知

$$H=\{e, a, b, ab\}$$

是 G 的一个 4 阶子群.

证法Ⅱ　在 G 中任取元素 $a\neq e$，则由于 $a^2=e$，故

$$H=\{e, a\}\leqslant G.$$

又因为 $|G|>2$，故在 G 中存在元素 $b\notin H$，而

$$K=\{e, b\}\leqslant G.$$

又因为 G 是交换群，故 $HK=KH$，从而由定理 5 知：

$$HK=\{e, a, b, ab\}\leqslant G.$$

即 HK 是 G 的一个 4 阶子群.

7.

证　反证法. 假设群 G 是两个真子群 H, K 的并集，即 $G=H\cup K$.

由于 H, K 是 G 的真子群，故有 $a, b\in G$ 使

$$b\notin H,\quad a\notin K.$$

但由于 $G=H\cup K$，从而 $a\in H, b\in K$. 又因为

$$ab\in G=H\cup K,$$

故必

$$ab\in H\quad 或\quad ab\in K.$$

若 $ab=h\in H$，则由于 H 是子群，故 $b=a^{-1}h\in H$，矛盾；若 $ab=k\in K$，则同理 $a=kb^{-1}\in K$，也矛盾. 因此，原假设不成立，即 G 不能是二真子群的并集.

§2.4　循　环　群

一、主要内容

1. 生成系和循环群的定义.
2. 循环群中元素的表示方法和生成元的状况.

若$|a|=\infty$,则

$$\langle a\rangle=\{\cdots,a^{-2},a^{-1},e,a,a^2,\cdots\},$$

且有两个生成元a与a^{-1};

若$|a|=n$,则

$$\langle a\rangle=\{e,a,a^2,\cdots,a^{n-1}\}.$$

并且a^k $(1\leqslant k<n)$是生成元$\Longleftrightarrow(k,n)=1$,从而有$\varphi(n)$个生成元.

3. 循环群在同构意义下只有两类：整数加群和n次单位根乘群，其中$n=1,2,3,\cdots$.

4. 循环群的子群的状况.

无限循环群有无限多个子群. n阶循环群$\langle a\rangle$有$T(n)$(n的正出数个数)个子群，且对n的每个正因数k，$\langle a\rangle$有且仅有一个k阶子群$\left\langle a^{\frac{n}{k}}\right\rangle$.

二、释疑解难

1. 我们说循环群是一类完全弄清楚了的群，主要是指以下三个方面：

1)循环群的元素表示形式和运算方法完全确定.其生成元的状况也完全清楚(无限循环群有两个生成元，n阶循环群$\langle a\rangle$有$\varphi(n)$个生成元而且a^k是生成元$\Leftrightarrow(k\circ n)=1$)；

2)循环群的子群的状况完全清楚；

3)在同构意义下循环群只有两类：一类是无限循环群，都与整数加群同构；另一类是$n(n=1,2,\cdots)$阶循环群，都与n次单位根乘群同构.

2. 循环群不仅是一类完全弄清楚了的群，而且是一类比较简单又与其他一些群类有广泛联系的群类. 例如由下一章§9可知，有限交换群可分解为一些素幂阶循环群的直积. 更一般地，任何一个具有有限生成系的交换群都可分解成循环群的直积. 由于循环群已完全在我们掌握之中，所以这种群(具有有限生成系的交换群)也是一类研究清楚了的群类. 它在各种应用中有着非常重要的作用. 例如在组合拓扑学中它就是一个主要的工具.

三、习题§2. 4解答

1.

解 生成元有两个:a,a^5;子群有$T(6)=4$个,除e与G外另两个为:

$$\langle a^2\rangle=\{e,a^2,a^4\},\quad \langle a^3\rangle=\{e,a^3\}.$$

2.

证 若$s=\pm t$,则显然$\langle a^s\rangle=\langle a^t\rangle$.

反之,若$\langle a^s\rangle=\langle a^t\rangle$,则存在整数$m$使

$$a^s=(a^t)^m=a^{tm}.$$

但由$|a|=\infty$知,$s=tm$. 同理有整数n使$t=sn$. 于是

$$t=tmn,\quad \text{即 } mn=1.$$

但m,n都是整数,故$m=n=\pm1$,于是$s=\pm t$.

3.

证法Ⅰ 1) 若$\langle a^s\rangle=\langle a^t\rangle$,则$a^s\in\langle a^t\rangle$. 设

$$a^s=a^{tm},\quad a^{s-tm}=e.$$

但$|a|=n$,故$n|(s-tm)$. 令

$$s-tm=nq. \qquad (1)$$

同理，由 $a^t \in \langle a^s \rangle$，设 $a^t = a^{sk}$，则 $a^{t-sk} = e$. 再由 $|a| = n$ 可知 $n \mid (t - sk)$. 令

$$t - sk = nq'. \qquad (2)$$

由(1)知，$(t,n) \mid s$；由(2)知，$(s,n) \mid t$. 但是

$$(t,n) \mid n, \quad (s,n) \mid n,$$

故 $(t,n) \mid (s,n)$，$(s,n) \mid (t,n)$. 从而 $(s,n) = (t,n)$.

2) 设 $(s,n) = (t,n) = d$，则存在整数 u, v 使

$$tu + nv = d.$$

再令 $s = ds_1$，于是由于 $|a| = n$，则

$$a^s = a^{ds_1} = a^{(tu+nv)s_1} = (a^t)^{us_1} \cdot (a^n)^{vs_1} = (a^t)^{us_1}$$

属于 $\langle a^t \rangle$，从而 $\langle a^s \rangle \subseteq \langle a^t \rangle$.

同理有 $\langle a^t \rangle \subseteq \langle a^s \rangle$. 因此 $\langle a^s \rangle = \langle a^t \rangle$.

证法 Ⅱ 1) 设 $\langle a^s \rangle = \langle a^t \rangle$，则因 $|a| = n$，故由 §2 定理 3 知：

$$|a^s| = \frac{n}{(s,n)}.$$

同理，$|a^t| = \frac{n}{(t,n)}$. 但由于 $\langle a^s \rangle = \langle a^t \rangle$，故 $|a^s| = |a^t|$，从而

$$\frac{n}{(s,n)} = \frac{n}{(t,n)}, \quad (s,n) = (t,n).$$

2) 反之，若 $(s,n) = (t,n)$，则由上面知 $|a^s| = |a^t|$. 再由证法 Ⅰ 中的 2)知，$\langle a^s \rangle \subseteq \langle a^t \rangle$ 故

$$\langle a^s \rangle = \langle a^t \rangle.$$

4.

证 首先，由于 $a, b \in \langle a,b \rangle$，从而

$$ab \in \langle a,b \rangle, \quad \langle ab \rangle \subseteq \langle a,b \rangle;$$

其次，设 $|a| = m$，$|b| = n$，则 $(m,n) = 1$，且

$$a^m = e, \quad b^n = e. \qquad (1)$$

于是存在整数 s, t 使

$$ms + nt = 1. \qquad (2)$$

故由 $ab = ba$ 和(1)与(2)知：

$$(ab)^{nt} = a^{nt}b^{nt} = a^{nt} = a^{1-ms} = a \cdot (a^m)^{-s} = a.$$

但是 $(ab)^{nt} \in \langle ab \rangle$，故 $a \in \langle ab \rangle$. 从而

$$a^{-1} \in \langle ab \rangle, \quad a^{-1}(ab) = b \in \langle ab \rangle.$$

于是又有 $\langle a,b \rangle \subseteq \langle ab \rangle$. 因此，$\langle a,b \rangle = \langle ab \rangle$.

5.

证 1) 任取 $a,b\in G_p$，不妨设 $a\in U_{p^s}$，$b\in U_{p^t}$，且 $s\leqslant t$，则 $a,b\in U_{p^t}$. 于是 $ab^{-1}\in U_{p^t}$，$ab^{-1}\in G_p$. 由 §2 例 4 知，$G_p\leqslant U$ (U 是由全部单位根作成的乘群). 从而 G_p 作成群.

2) 首先，U_{p^i} $(i=1,2,\cdots)$显然都是 G_p 的真子群.

其次，令 $H<G_p$，则有 $a\in G_p$，但 $a\notin H$. 令 $|a|=p^s$，即 a 是 p^s 次原根，下证 H 中任何元素的阶均不大于 p^s.

因若不然，设 H 中有元素 h 的阶 $p^t>p^s$，则

$$a^{p^t}=(a^{p^t})^{p^{t-s}}=1,$$

即 a 是 p^t 次单位根，于是 $a\in\langle h\rangle\subseteq H$，矛盾.

设 p^m 是 H 中所有元素的最大阶，且 H 中元素 b 的阶是 p^m，则显然 $U_{p^m}=\langle b\rangle\subseteq H$.

另一方面，任取 $h\in H$，则由于交换群中每个元素的阶都整除最大阶，故 h 的阶整除 p^m，从而

$$h^{p^m}=1,$$

即 h 是 p^m 次单位根，$h\in\langle b\rangle$，即 $H\subseteq\langle b\rangle$. 故

$$H=\langle b\rangle=U_{p^m},$$

即 G_p 的真子群只有 U_{p^i}，$i=1,2,\cdots$.

6.

证 由题设可知 $G=H\cup M$，且 $H\cap M=\varnothing$.

显然，对任意 $x\in G$，若 $x\notin H$，则 $x\in M\subseteq\langle M\rangle$；若 $x\in H$，则因 H 是子群，故 $x^{-1}\in H$. 又由于 $H\neq G$，故有 $a\in G$，$a\notin H$，于是 $ax\notin H$，从而

$$ax\in M.$$

显然 $a^{-1}\notin H$，从而 $a^{-1}\in M$. 于是，

$$x=a^{-1}\cdot ax\in\langle M\rangle,$$

即 G 中任何元素都属于$\langle M\rangle$，故

$$G=\langle M\rangle.$$

7.

证 任取 $\frac{b}{a}\in\mathbf{Q}_+$，则由于

$$\frac{b}{a}=\frac{(a-1)!\,b}{a!},$$

故 $\frac{b}{a}$ 可表为若干个 $\frac{1}{a!}$ 的代数和，即 $\mathbf{Q}_+$ 可由(1)生成.

注 实际上(1)的任意一个无限子集均为 $\mathbf{Q}_+$ 的生成系. 事实上，在(1)中任取一无限子集，设为

$$\left\{\frac{1}{n_1!},\frac{1}{n_2!},\cdots,\right\},\qquad(2)$$

则总存在 $n_k\geqslant a$，并令 $ac=n_k!$，于是

$$\frac{b}{a}=\frac{bc}{ac}=\frac{bc}{n_k!},$$

即 $\frac{b}{a}$ 可表为若干个 $\frac{1}{n_k!}$ 的代数和，从而(2)也是 $\mathbf{Q}_+$ 的生成系.

§2. 5 变 换 群

一、主要内容

1．变换群、双射变换群(特别是集合 M 上的对称群和 n 次对称群)和非双射变换群的定义及例子.

2．变换群是双射变换群的充要条件；双射变换群与抽象群的关系.

1)集合 M 上的变换群 G 是双射变换群 $\Leftrightarrow$ G 含有 M 的单或满)射变换;

2)任何一个群都同一个(双射)变换群同构.

3．有限集及无限集上非双射变换群的例子(例 2 和例 3).

二、释疑解难

1．一般近世代数书中所说的“变换群”，都是由双射变换(关于变换乘法)所作成的群，即本教材所说的“双射变换群”. 而本教材所说的“变换群”则是由一个集合上的一些变换(不一定是双射变换)作成的群. 通过教材§5 定理 2 和推论 1 可知，实际上变换群可分成两类：一类是双射变换群(全由双射变换作成的群，即通常近世代数书中所说的“变换群”)，另一类是非双射变换群(全由非双射变换作成的群). 在学习本书时应留意这种差异.

2．本节教材定理 2(若集合 M 上的变换群 G 含有 M 的单射或满射变换. 则 G 必为 M 上的一个双射变换群，即 G 中的变换必全是双射变换)比有些书上相应的定理(若集合 M 上由变换作成的群 G 含有 M 的恒等变换，则 G 中的变换必全为双射变换)大为推广. 因为后者要求 G 包含恒等变换(一个特殊的双射变换)，而前者仅要求 G 包含一个单(或满)射变换即可. 因此，后音只是前者(本节教材定理 2)的一个推论，一种很特殊的情况. 两相比较，差异较大.

这种差异也说明，M 上的任何一个非双射变换群不仅不能包含恒等变换，而且连 M 的任何单射或满射变换也不能包含.

另外，在这里顺便指出，集合 M 上的任何双射变换群 G 的单位元必是 M 的恒等变换.

事实上，设 e 是 G 的单位元，则

$$\tau e=\tau \quad (\forall \tau\in G),$$

从而对任意 $x\in M$ 都有 $\tau(e(x))=\tau(x)$. 但 τ 是 M 的双射变换，故 $e(x)=x$，即 e 是 M 的恒等变换.

3．集合 M 上的全体变换作成的集合 $T(M)$，对于变换的乘法作成一个有单位元的半群. 在半群的讨论中，这是一类重要的半群. 并且本节习题中第 4 题还指出，当 $|M|>1$ 时 $T(M)$ 只能作成半群，而不能作成群.

三、习题§2. 5 解答

1．解　作成有单位元半群，τ 是单位元. 但不作成群，因为 σ 无逆元.

2.

解　易知：$\tau\sigma=\epsilon$. 但是，$\sigma\tau$: $1\longrightarrow 2, n\longrightarrow n\ (n>1)$，故 $\tau\sigma\neq\sigma\tau$.

3．解　G 作成群：因为易知

$$\tau_{(a,b)}\cdot\tau_{(c,d)}=\tau_{(ac,ad+b)},$$

即 G 对变换的乘法封闭；又 $\tau_{(1,0)}$ 是单位元，而 $\tau_{(a^{-1},-a^{-1}b)}$ 是 $\tau_{(a,b)}$ 的逆元.

又因为 $a\neq 0$，故显然 $\tau_{(a,b)}$ 是 M 的一个单射变换(若利用定理 2，则可知 G 是 M 的双射变换群). 再任取 $y\in M$，由于 M 是有理数集，故

$$x=\frac{y-b}{a}$$

是 y 在 $\tau_{(a,b)}$ 之下的逆象，即 $\tau_{(a,b)}$ 是满射，从而 G 是 M 的双射变换

4.

证　反证法. 设 $M=\{a,b,\cdots\}$ 且 $\sigma(x)=a,\tau(x)=b\ (\forall x\in M)$，则 σ,τ 是 M 的两个互异的非双射变换. 如果 M 的全体非双射变换作成群，则由于显然

$$\sigma\tau=\sigma,\quad \tau\sigma=\tau,$$

于是 σ 与 τ 都是此群的单位元，矛盾.

5.

证　由本节 Cayley 定理知，任何 n 阶群都同 n 次对称群 S_n 的一个子群同构，而 S_n 是 $n!$ 阶有限群，它只有有限个子群，故互不同构的 n 阶群只有有限个.

§2. 6　置　换　群

一、主要内容

1. 任何(非循环)置换都可表为不相连循环之积，任何置换都可表为若干个对换之积，且对换个数的奇阴偶性不变. 从而有奇、偶置换的概念，且全体 n 次置换中奇、偶置换个数相等，各为 $\frac{n!}{2}$ 个($n>1$).

2. k—循环的奇偶性、阶和逆元的确定方法，以及不相连循环乘积的奇偶性、阶和逆元的确定方法.

1) k—循环与 A 有相反奇偶性.

2) k—循环的阶为 k. 又 $(i_1,\ i_2\cdots i_k)^{-1}=(i_k,\ \cdots,\ i_2,\ i_1)$.

3) 若 σ 分解为不相连循环之积. 则其分解中奇循环个数为奇时 σ 为奇置换，否则 σ 为偶置换. σ 的阶为各因子的阶的最小公倍. 其逆元可由 k—循环的逆元来确定.

3. 由置换 σ，τ 求置换 $\sigma\tau\sigma^{-1}$ 的方法. n 次对称群 s_n 的中心.

4. 传递群的定义、例子和简单性质.

二、释疑解难

1. 研究置换群的重要意义和作用.

除了教材中已经指出的(置换群是最早研究的一类群，而且每个有限的抽象群都同一个置换群同构)以外，研究置换群的重要意义和作用至少还有以下几方面：

1)　置换群是一种具体的群，从置换乘法到判断置换的奇偶性以及求置换的阶和逆置换，都很具体和简单. 同时它也是元素不是数的一种非交换群. 在群的讨论中举例时也经常用到这种群.

2)　在置换群的研究中，有一些特殊的研究对象是别的群所没有的. 如置换中的不动点理论以及传递性和本原性理论等等.

3)　置换群中有一些特殊的子群也是一般抽象群所没有的. 例如，交代群、传递群、稳定子群和本原群等等. 就教材所讲过的交代群和传递群的重要性便可以知道，介绍置换群是多么的重要.

2. 用循环与对换之积来表出置换的优越性.

首先，书写大为简化，便于运算。另外还便于求置换的阶，判断置换的奇偶性和求逆置换. 因为我们知道：

k—循环的阶是 k；不相连循环之积的阶为各循环的阶的最小公倍；k—循环的奇偶性与 $k-1$ 的奇侣性相同；又 k—循环 $(i_1,\ i_2\cdots i_k)$ 的逆元为 $(i_1,\ i_2\cdots i_k)^{-1}=(i_k,\ \cdots,\ i_2,\ i_1)$.

3. 由教材本节例 3 可直接得出以下结论：n 次置换群 G 若包含有奇置换，则 $|G|$ 是一个偶数.

另外，由于偶置换之积仍为偶置换，故任何 n 次置换群 G 中的全体偶置换作成 G 的一个子群.

4. 在四次对称群 S_4 中有以下二子群：

$$K_1=\{(1),(12)(34),(13)(24),(14)(23)\},$$

$$H=\{(1),(12),(34),(12)(34)\}.$$

易知，$K_1\cong H$. 但是 Klein 四元群 $K_1\lhd S_4$，而 H 不是 S_4 的正规子群(参考第三章§2. 又(13)(12)(13)=(23)$\notin H$)；又 K_1 是传递群，而与其同构的群 H 却不是传递群(因为例如在 H 中没有置换把 1 变为 3). 这就是说，单纯作为群来说，K_1 与 H 同构，从而它们的代数性质完全一样. 但是作为置换群来说，它们却有很大的差别.

5. 在一般群中判断二元素是否共扼(参考第三章§6)并不容易，但是，在对称群 s_n 中二置换是否共扼却容易判断，即二者有相同的循环结构(参考习题 3. 9 第 30 题). 其证明要用到本节的定理5，这也是该定理的一个重要应用.

6. 法国数学家马蒂厄于 1861 年和 1873 年曾发现四个 4 重传递群，分别用 M_{11}，M_{12}，M_{23}，M_{24} 表示，后人称为马蒂厄群. 这四个群的阶数都很大，它们的阶数分别是：

$$|M_{11}|=8\cdot9\cdot10\cdot11,\quad |M_{12}|=8\cdot9\cdot10\cdot11\cdot12,$$

$$|M_{22}|=20\cdot21\cdot22\cdot48,\quad |M_{23}|=20\cdot21\cdot22\cdot23\cdot48,$$

$$|M_{24}|=20\cdot21\cdot22\cdot23\cdot24\cdot48.$$

三、习题§2. 6 解答

1. 略

2.

解 1) $\sigma^{-1}=\sigma_k\sigma_{k-1}\cdots\sigma_2\sigma_1$. 2) $(i_1i_2\cdots i_k)=(i_1i_k)(i_1i_{k-1})\cdots(i_1i_2)$.

3. 略

4. 略

5.

解 $\sigma^{-1}=(57)(431)$，$\sigma\tau\sigma^{-1}=(425)(26)(31)=(13)(2654)$；

$\sigma^{-1}\tau\sigma=(125)(26)(43)=(1265)(34)$.

6. 证 因为 H 有限，故要证 $H\leqslant s_4$ 只用验算 H 对置换乘法封闭即可.

7. 解 令 $\tau=(123456)$. 则 G 的全部 6 个置换是：

$$(1),\qquad \tau^3=(14)(25)(36),$$

$$\tau=(123456),\qquad \tau^4=(153)(246),$$

$$\tau^2=(135)(246),\quad \tau^5=(165432).$$

又易知：$\tau^k(1)=k+1$ $(k=1,2,3,4,5)$，故 G 为传递群. 又显然 G 中无 σ 使 $\sigma(1)=3,\sigma(2)=5$，因此，G 不是 2 重传递群.

§2. 7 陪集、指数和 Lagrange 定理

一、主要内容

1. 左、右陪集定义和简单性质.

1) 左陪集的五个基本性质：1)一5)；

2) 全体左陪集与全体右陪集之间可建立双射；

3) 群 G 关于子群 H 的左陪集分解式：

$$G=a_1H\cup a_2H\cup\cdots,\quad a_iH\cap a_jH=\varnothing\ (i\neq j).$$

2. 指数定义和性质. 性质有：设 $K\leqslant H\leqslant G$，则

$$(G:H)(H:K)=(G:K),$$

$$(G:H\cap K)\leqslant(G:H)(H:K).$$

3. Lagrange 定理：设 H 是有限群 G 的子群，则

$$|G|=|H|\cdot(G:H).$$

从而 $|H|$ 是 $|G|$ 的因数.

4. 有限子群乘积的阶同子群的阶的关系.

设 H, K 是群 G 的两有限子群，则

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}.$$

二、释题解难

1. 一般来说，两个陪集的乘积不再是一个陪集. 例如，对三次对称群 S_3 的子群 $H=\{(1),(12)\}$ 来说，$(1)H$ 与 $(13)H$ 是两个左陪集，但其乘积

$$(1)H\cdot(13)H=\{(13),(23),(123),(132)\}$$

不再是左陪集.

2. pq（p,q 是素数且 $p<q$）阶交换群必为循环群（参考第三章§2 定理 5）. 又 pq 阶非交换群 G 则由第三章§6 定理 3（或由 Sylow 定理）知，必有 p 阶与 q 阶子群. 再根据本节推论 3 知，G 有惟一的 q 阶子群，从而它是 G 的一个正规子群. 但是，其 p 阶子群可能不止一个. 例如三次对称群 S_3（$|S_3|=2\cdot3$）的 2 阶子群就有三个，即

$$H_1=\{(1),(12)\},\quad H_2=\{(1),(13)\},\quad H_3=\{(1),(23)\}.$$

3. 两个子群的乘积一般不再是子群.

例如上面的 H_1,H_2 都是 S_3 的子群，但是其乘积

$$H_1H_2=\{(1),(12),(13),(132)\}$$

当然不可能是 S_3 的子群，因为由 Lagrange 定理知，$|H_1H_2|=4$ 不能整除 $|S_3|=6$. 因此，定理 5 中的子群乘积 HK 只是群 G 的一个子集，而 $|HK|$ 是这个子集所包含的元素个数.

4. Lagrange 定理的逆定理不成立. 即若 $m\mid|G|$，则群 G 不一定有 m 阶子群. 例如四次交代群 A_4，6 是 $|A_4|=12$ 的一个因数，但是 A_4 并无 6 阶子群（参考习题 2.7 第 22 题）.

虽然如此，但对 $|G|$ 的一些特殊的因数 p^k（p 是素数），G 必有 p^k 阶子群（参考 Sylow 定理）. 特别重要的是，对于交换群，Lagrange定理总成立（参考第三章§9）.

5. 关于 Lagrange 群.

定义 若对有限群 G 的阶的每个正因数 m，G 都有 m 阶子群，则称 G 为一个Lagrange群.

上面已指出有限交换群必是 Lagrange 群. 又显然三次对称群 S_3 也是一个 Lagrange 群. 有不少数学家，例如 D. H. Mclain 于 1957 年和 J. F. Humphreys 于 1974 年（On groups satisfying the converse of Lagrange's Theorem, proc. Cambridge Philos. Sec. 75(1974),25 −32）都曾经研究过这种群.

可以证明，Lagrange 群必为可解群. 又 T. M. Gagen 于 1977 年又证明了可解群必可同构嵌入到一个 Lagrange 群中.

三、习题§2.7 解答

1．证　利用 Lagrange 定理即得.

2．略

3.

证　由于 $H\cap K\leqslant H, H\cap K\leqslant K$，故由 Lagrange 定理知：

$$|H\cap K|\mid m,\quad |H\cap K|\mid n.$$

故 $|H\cap K|$ 整除 (m,n). 但是 $(m;n)=1$，故必 $|H\cap K|=1$，从而 $H\cap K=\{e\}$.

4.

证　任取 $e\neq a\in G$. 由于 $|G|=p^m$，故由 Lagrange 定理知：

$$|\langle a\rangle| \text{即} |a| \text{是} |G|=p^m \text{的因数.}$$

因 p 是素数，故必 $|a|=p^s$　$(0<s\leqslant m)$. 从而 $|a^{p^{s-1}}|=p$，即 G 有 p 阶元.

若 $|b|=p$，则 $\langle b\rangle=\{e,b,b^2,\cdots,b^{p-1}\}$ 中的 $p-1$ 个元素 b，$b^2,\cdots,b^{p-1}$ 都是 G 的 p 阶元. 另外，若 $|b|=|c|=p$ 且 $\langle b\rangle\neq\langle c\rangle$ 时，必 $\langle b\rangle\cap\langle c\rangle=e$. 从而此时 p 阶元 $b,b^2,\cdots,b^{p-1}$ 与 p 阶元 $c,c^2,\cdots,c^{p-1}$ 中没有相等的. 因此可知，G 中 p 阶元的个数是 $p-1$ 的倍数.

5.

证　1）任取 $x\in G$. 由于 A 是 G 关于 H 的代表系，令

$$x\in a_iH,\quad \text{即 } a_i^{-1}x\in H.$$

又 B 是 H 关于 K 的代表系，令

$$a_i^{-1}x\in b_jK,\quad \text{即 } (a_ib_j)^{-1}x=b_j^{-1}\cdot a_i^{-1}x\in K.$$

因此，$xK=a_ib_jK$，$x\in a_ib_jK$.

2）设若 $a_ib_jK=a_sb_tK$，则

$$(a_ib_j)^{-1}(a_sb_t)=k\in K\leqslant H.$$

从而 $a_i^{-1}a_s=b_jkb_t^{-1}\in H$（因为 $b_j,b_t\in H$），$a_iH=a_sH$，$i=s$.

由此又得 $b_jK=b_tK$，从而 $j=t$. 得证.

6. 易知 S_3 的以下六个子集：$H_1=\{(1)\}$，$H_2=\{(1),(12)\}$，$H_3=\{(1),(13)\}$，$H_4=\{(1),(23)\}$，$H_5=\{(1),(123),(132)\}$，$H_6=S_3$ 都是 S_3 的子群.

下证 S_3 仅有这六个子群.

设 H 为 S_3 的任一非平凡子群，则由于 $|H|$ 是 $|S_3|=6$ 的因数，故只能 $|H|=2,3$.

当 $|H|=2$ 时，H 只能是 H_2，H_3，H_4.

当 $|H|=3$ 时，H 中元素的阶必为 3 的因数，即只能是 1 或 3. 因此，此时 H 中除单位元外，另两个元素必定都是 3 阶元. 但 S_3 中的三阶元有且仅有两个，即 (123) 和 (132)，因此，此时只能 $H=H_5$.

综上所述可知，S_3 有且仅有这六个子群.

解 易知 S_3 的以下六个子集

$H_1=\{(1)\}$，$H_2=\{(1),(12)\}$，$H_3=\{(1),(13)\}$，$H_4=\{(1),(23)\}$，$H_5=\{(1),(123),(132)\}$、$H_6=S_3$ 对置换乘法都是封闭的，因此都是 S_3 的子群.

下证 S_3 仅有这六个子群.

设 H 为 S_3 的任一非平凡子群，则由于 $|H|$ 是 $|S_3|=6$ 的因数，故只能 $|H|=2,3$.

当 $|H|=2$ 时，H 中除单位元(1)外，另一个元素只能是一个 2 阶元. 但 S_3 的 2 阶元只有三个，即(12)，(13)，(23)，因此，H 只能是 H_2,H_3,H_4.

当 $|H|=3$ 时，由 Lagrange 定理知，H 中元素的阶必为 3 的因数，即只能是 1 或 3. 因此，此时 H 中除单位元外，另两个元素必定都是 3 阶元. 但 S_3 中的三阶元有且仅有两个，即(123)和(132)，因此，此时只能 $H=H_5$.

综上所述可知，S_3 有且仅有以上六个子群.

7.

证 上述 4 个子群显然都是 G 的真子群，$\langle -1\rangle$ 的阶是 2，另三个的阶均为 4.

现设 H 为 G 的任一真子群. 由于 $|G|=8$，故必 $|H|=2$ 或 4. 若 $|H|=2$，则 H 中必含 2 阶元. 但 G 只有一个 2 阶元 -1，故必 $H=\langle -1\rangle$. 若 $|H|=4$，则由于 i,j,k 都是 4 阶元且 $i^2=j^2=k^2=-1$，故若 $i\in H$，必有 $H=\langle i\rangle$；若 $j\in H$，必有 $H=\langle j\rangle$；若 $k\in H$，必有 $H=\langle k\rangle$.

8.

证 1) 任取 $x\in A(B\cup C)$，令

$$x=ay,\quad \text{其中 } a\in A,y\in B\cup C.$$

若 $y\in B$，则 $x=ay\in AB$. 从而 $x\in AB\cup AC$；若 $y\in C$，则

$$x=ay\in AC,\quad \text{故 } x\in AB\cup AC.$$

从而 $A(B\cup C)\subseteq AB\cup AC$.

反之，任取 $x\in AB\cup AC$，则

$$x\in AB \quad \text{或} \quad x\in AC.$$

若 $x\in AB$，则令

$$x=ab,\quad \text{其中 } a\in A,b\in B.$$

于是 $b\in B\cup C$，从而 $x=ab\in A(B\cup C)$；若 $x\in AC$，同样有

$$x\in A(B\cup C).\quad \text{故 } AB\cup AC\subseteq A(B\cup C).$$

因此，$A(B\cup C)=AB\cup AC$.

2) 等式 $A(B\cap C)=AB\cap AC$ 一般不成立. 例如在四次对称群 S_4 中，令

$$A=\{(1),(12)\},\quad B=\{(1),(34)\},$$
$$C=\{(1),(12)(34),(13)(24),(14)(23)\}.$$

则易知 $A(B\cap C)=\{(1),(12)\}$，但是

$$AB\cap AC=\{(1),(12),(34),(12)(34)\},$$

从而 $A(B\cap C)\subset AB\cap AC$，即二者不相等.

9.

证 因为 $|H|=p^r$，$|K|=p^s$，$|G|=p^tm$ 以及

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}=\frac{p^{r+s}}{|H\cap K|},$$

故

$$|HK|\cdot|H\cap K|=p^{r+s}. \tag{1}$$

又由于 p 是素数，故 $|HK|$ 必为 p 的方幂，设

$$|HK|=p^r,\quad 0<r\leqslant s+t. \tag{2}$$

如果乘积 $HK\leqslant G$，则由 Lagrange 定理知：

$$|HK|\mid p^tm.$$

但 $p\nmid m$，故由 $|G|=p^tm$ 知，$r\leqslant t$. 于是由(1)与(2)得：

$$p^s=|K|\geqslant|H\cap K|=p^{(r+s)-r}.$$

由此又得 $t=r$，且 $|H\cap K|=p^s=|K|$. 但是 $H\cap K\leqslant K$，故得

$$H\cap K=K,\quad K\subseteq H.$$

这与题设 $K\not\subseteq H$ 矛盾. 故 HK 不是 G 的子群.

10.

证法 I 若 G 中的方阵全是降秩的，结论成立；若 G 中有方阵 $\boldsymbol{A}$ 是满秩的，则任取 $\boldsymbol{X}\in G$，由于 G 对方阵的普通乘法作成群，故有方阵 $\boldsymbol{Y}\in G$ 使

$$\boldsymbol{XY}=\boldsymbol{A}.$$

从而 $|\boldsymbol{X}|\cdot|\boldsymbol{Y}|=|\boldsymbol{A}|\neq 0$，于是 $|\boldsymbol{X}|\neq 0$，即方阵 X 是满秩的. 由 $\boldsymbol{X}$ 的任意性知，G 中的方阵全是满秩的.

证法 II 若 G 中有满秩方阵 $\boldsymbol{A}$，则 $\boldsymbol{A}$ 有逆方阵 $\boldsymbol{A}^{-1}$，使

$$\boldsymbol{AA}^{-1}=\boldsymbol{E}\quad(\boldsymbol{E}\text{ 为 }n\text{ 阶单位方阵}),$$

设 e 是 G 的单位元，于是

$$e\boldsymbol{A}=\boldsymbol{A},\quad e\boldsymbol{AA}^{-1}=\boldsymbol{AA}^{-1},\quad e\boldsymbol{E}=\boldsymbol{E},\quad e=\boldsymbol{E},$$

即 G 中的单位元就是 n 阶单位方阵 $\boldsymbol{E}$（由此立即可知，$\boldsymbol{A}$ 在 G 中的逆元就是 $\boldsymbol{A}$ 的逆方阵 $\boldsymbol{A}^{-1}$）.

现在在 G 中任取一个方阵 $\boldsymbol{B}$，而 $\boldsymbol{C}$ 是 $\boldsymbol{B}$ 在 G 中的逆元，则

$$\boldsymbol{BC}=\boldsymbol{E},\quad|\boldsymbol{B}|\cdot|\boldsymbol{C}|=|\boldsymbol{E}|=1.$$

从而 $|\boldsymbol{B}|\neq 0$，即 $\boldsymbol{B}$ 为满秩方阵. 由 $\boldsymbol{B}$ 的任意性知，G 中的每个方阵都是满秩的.

注 由证法 II 知，若由数域 F 上一些 n 阶满秩方阵对方阵的普通乘法作成群，则这个群的单位元就是 n 阶单位方阵，而每个方阵的逆元就是这个方阵的通常的逆方阵.

另外，由降秩方阵对普通乘法作成的群是存在的. 例如，由一切 2 阶方阵

$$\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\quad(0\neq a\in\mathbf{Q})$$

作成的群即是.

11.

证 依次用 $\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6$ 表示 G 中的 6 个元素，则根据所规定的运算可得 G 的乘法表如下：

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_1	σ_3
σ_5	σ_5	σ_3	σ_6	σ_1	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

由此表可知，G 对所规定的运算封闭，而且运算$\circ$显然满足结合律；又 σ_1 是单位元且 $\sigma_1,\sigma_2,\sigma_3,\sigma_6$ 的逆元均为自身，而 σ_4 与 σ_5 互为逆元. 因此，G 对所规定的运算作成一个群.（由于 G 有限，而且乘法表中各行各列元素互异，从而消去律成立，因此，G 作成群. 这是另一种证法.）

注 若令

$$\sigma_1(x)=x,\quad \sigma_2(x)=\frac{1}{x},\quad \sigma_3(x)=1-x,$$

$$\sigma_4(x)=\frac{1}{1-x},\quad \sigma_5(x)=\frac{x-1}{x},\quad \sigma_6(x)=\frac{x}{x-1},$$

则每个 σ_i 都是集合 $M=$（除 0，1 以外的全体有理数）上的双射变换. 由乘法表知 G 对变换乘法封闭，故 $G\leqslant S(M)$，从而 G 作成群.

12.

证 因为显然 $(ab)^{[m,n]}=e$，故 $|ab|\mid[m,n]$.

又设
$$m=p_1^{s_1}\cdots p_k^{s_k}p_{k+1}^{s_{k+1}}\cdots p_r^{s_r},$$
$$n=p_1^{t_1}\cdots p_k^{t_k}p_{k+1}^{t_{k+1}}\cdots p_r^{t_r},$$

其中 $p_1,p_2,\cdots,p_r$ 为互异素数，又 $s_i,t_i\geqslant 0$，但不同时为零，$i=1,2,\cdots,r$. 并假定

$$s_1\leqslant t_1,\quad s_2\leqslant t_2,\quad \cdots,\quad s_k\leqslant t_k;$$
$$t_{k+1}\leqslant s_{k+1},\quad t_{k+2}\leqslant s_{k+2},\quad \cdots,\quad t_r\leqslant s_r.$$

于是
$$[m,n]=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}p_{k+1}^{s_{k+1}}\cdots p_r^{s_r}.$$

但是
$$\left|a^{p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}}\right|=p_{k+1}^{s_{k+1}}\cdots p_r^{s_r},\quad \left|b^{p_{k+1}^{t_{k+1}}\cdots p_r^{t_r}}\right|=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k},$$

又因 $ab=ba$，$(p_{k+1}^{s_{k+1}}\cdots p_r^{s_r},p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k})=1$，故
$$\left|a^{p_1^{s_1}\cdots p_k^{s_k}}\cdot b^{p_{k+1}^{t_{k+1}}\cdots p_r^{t_r}}\right|=[m,n].$$

注 对 s 用数学归纳法，本题可进一步推广为：设群 G 中元素 $a_1,a_2,\cdots a_s$ 可两两交换且
$$|a_i|=m_i\quad (i=1,2,\cdots,s),$$
则由于
$$[[m_1,\cdots,m_{s-1}],m_s]=[m_1,\cdots,m_{s-1},m_s],$$
故可知群 G 中有阶为 $[m_1,\cdots,m_{s-1},m_s]$ 的元素.

13.

证 1) 令$[s,t]=ss'=tt'$，其中s'与t'为整数，则

$$a^{[s,t]}=(a^s)^{s'}=(a^t)^{t'}\in\langle a^s\rangle\bigcap\langle a^t\rangle.$$

因此 $$\langle a^{[s,t]}\rangle\subseteq\langle a^s\rangle\bigcap\langle a^t\rangle.$$

其次，任取$x\in\langle a^s\rangle\bigcap\langle a^t\rangle$，并令

$$x=a^{sr}=a^{tp},\quad (s,t)=d, \tag{1}$$

$$s=dm,\qquad t=dn. \tag{2}$$

则$(m,n)=1$. 于是存在整数u,v使

$$mu+nv=1,\quad [s,t]=dmn. \tag{3}$$

于是由(1)、(2)、(3)得

$$x^{mu}=(a^{tp})^{mu}=a^{dnpmu},$$

$$x^{nv}=(a^{sr})^{nv}=a^{dmnrv}.$$

上二式相乘，再根据(3)即得

$$x=x^{mu+nv}=a^{dmn(pu+rv)}$$

$$=(a^{[s,t]})^{pu+rv}\in\langle a^{[s,t]}\rangle,$$

即$x\in\langle a^{[s,t]}\rangle$. 因此又有$\langle a^s\rangle\bigcap\langle a^t\rangle\subseteq\langle a^{[s,t]}\rangle$. 故

$$\langle a^s\rangle\bigcap\langle a^t\rangle=\langle a^{[s,t]}\rangle.$$

2) 令$(s,t)=d$，则存在整数u,v使

$$su+tv=d. \tag{4}$$

任取$x\in\langle a^s\rangle\langle a^t\rangle$，并令

$$x=a^{sm}\cdot a^{tn}=a^{sm+tn}, \tag{5}$$

$$sm+tn=dq+r\quad(0\leqslant r<d), \tag{6}$$

由(6)及(4)又得

$$r=s(m-uq)+t(n-vq).$$

但由于d是集合$\{sg+th\mid g,h$是整数$\}$中最小的正整数，故由(4)及(6)知必$r=0$. 于是由(5)及(6)知：

$$x=a^{sm+tn}=(a^d)^q\in\langle a^d\rangle.$$

从而$\langle a^s\rangle\langle a^t\rangle\subseteq\langle a^d\rangle$.

反之，任取$a^{dp}\in\langle a^d\rangle$，则由(4)得

$$a^{dp}=a^{(su+tv)p}=(a^s)^{up}\cdot(a^t)^{vp}\in\langle a^s\rangle\langle a^t\rangle.$$

于是又有$\langle a^d\rangle\subseteq\langle a^s\rangle\langle a^t\rangle$. 从而

$$\langle a^s\rangle\langle a^t\rangle=\langle a^d\rangle=\langle a^{(s,t)}\rangle.$$

注 以上结论可推广到更一般情形(对n用数学归纳法证明)：

$$\langle a^{s_1}\rangle\langle a^{s_2}\rangle\cdots\langle a^{s_n}\rangle=\langle a^{(s_1,s_2,\cdots,s_n)}\rangle.$$

14. 证 若G是有限群，则G的子集个数是有限的，从而其子群个数当然也是有限的.

反之，若群G只有有限个子群，则G中显然不能有无限阶元素，因为无限循环群有无限个子群. 这样，G中每个元素的阶都有限. 任取$a_1\in G$，则$\langle a_1\rangle$是G的一个有限于群；再取$a_2\in G-\langle a_1\rangle$，于是$\langle a_2\rangle$是$G$的一个异于$\langle a_1\rangle$的有限于群. 再取

$$a_3\in G-\langle a_1\rangle\cup\langle a_2\rangle,$$

同理$\langle a_3\rangle$又是G的一个异于$\langle a_1\rangle$，$\langle a_2\rangle$的有限子群. 但G只有有限个子群，故这种过程不能无限地持续下去，从而必存在s使

$$G=\langle a_1\rangle\cup\langle a_2\rangle\cup\cdots\cup\langle a_s\rangle,$$

而每个$\langle a_i\rangle$都有限，于是G为有限群.

证 1) 令

$$A=\{h(H\cap K)\mid h\in H\},\quad B=\{xK\mid x\in G\},$$

则易知 $\varphi: h(H\cap K)\longrightarrow hK$ 是 A 到 B 的映射. 又因若

$$h_1K=h_2K\quad (h_1,h_2\in H),$$

则 $h_1{}^{-1}h_2\in K$, 从而

$$h_1{}^{-1}h_2\in H\cap K,\quad h_1(H\cap K)=h_2(H\cap K).$$

故 φ 是集合 A 到 B 的一个单射, 从而 $|A|\leqslant|B|$, 即

$$(H:H\cap K)\leqslant(G:K).$$

2) 当 $(G:K)$ 有限时, 设若 $(H:H\cap K)=(G:K)$, 则由上知, φ 是双射. 故对任意 $x\in G$ 必有 $h\in H$, 使

$$x\in xK=hK\subseteq HK.$$

从而 $G\subseteq HK$, 因此 $G=HK$.

反之, 若 $G=HK$, 则任取左陪集 xK $(x\in G)$, 令

$$x=hk\quad (h\in H,k\in K),$$

则 $xK=hkK=hK$. 从而 φ 是 A 到 B 的双射, 故

$$(H:H\cap K)=(G:K).$$

注 在 1) 中 $(H:H\cap K)$ 与 $(G:K)$ 也可以是无限的.

16.

证 显然, 即要证 G 有且仅有一个 2 阶元素.

由于阶数大于 2 的元素在 G 中成对出现, 而单位元 e 的阶是 1, 又 $|G|=2n$, 故 G 中必有 2 阶元素, 且有奇数个.

设 a 是 G 的一个 2 阶元素, 则 $H=\{e,a\}$ 便是 G 的一个 2 阶子群. 如果 G 另有 2 阶元素 $b\neq a$, 则 $K=\{e,b\}$ 便是 G 的一个异于 H 的子群. 由于 G 是交换群, 故易知

$$HK=\{e,a,b,ab\}$$

是 G 的一个 4 阶子群. 于是由 Lagrange 定理知,

$$|HK|\,\big|\,|G|,\quad \text{即 } 4\,|\,2n.$$

这与 n 是奇数矛盾. 故 G 只能有一个 2 阶元素, 即只能有一个 2 阶子群.

17.

证 任取 $a\in G$, 由于指数 $(G:H)$ 有限, 则

$$a,a^2,a^3,\cdots$$

不可能都属于 G 的不同的陪集. 设 a^s 与 a^t $(s>t)$ 在 G 的同一个陪集中, 于是

$$a^{-t}a^s=a^{s-t}\in H.$$

但 H 是周期群, a^{s-t} 的阶有限, 设为 m, 于是

$$(a^{s-t})^m=a^{(s-t)m}=e,$$

从而 a 的阶有限, 即 G 是周期群.

18.

证法 I 设 G 是一个 15 阶交换群. 在 G 中任取 $a\neq e$, 则由 Lagrange 定理知, $|a|\,\big|\,15$. 从而必

$$|a|=1,\ 3,\ 5,\ 15.$$

$|a|=1$ 不可能; 若 $|a|=15$, 则 $G=\langle a\rangle$ 已是循环群;

若 $|a|=3$, 则 $\langle a\rangle$ 是 G 的一个 3 阶循环子群. 又因 G 可换, 故

$$|G/\langle a\rangle|=15/3=5.$$

从而商群 $G/\langle a\rangle$ 是 5 阶循环群. 设

$$G/\langle a\rangle=\langle\bar{b}\rangle,\quad \text{其中 } b\in G, \text{且 } |\bar{b}|=5.$$

因为 $|b|\neq1$ 且 $|b|\neq3$ (否则, $|\bar{b}|=3$), 故 $|b|=5$ 或 15.

若 $|b|=15$, 则 $G=\langle b\rangle$ 已是循环群; 若 $|b|=5$, 则由于 $|a|=3$, G 又可换, 故 $|ab|=15$, 从而 $G=\langle ab\rangle$ 为循环群.

当$|a|=5$时，可类似推出G也是循环群.

证法Ⅱ 设G是一个15阶交换群，则除e外G中元素的阶不可能都是3：因若不然，设

$$|a|=|b|=3,\quad \text{且 } b\notin\langle a\rangle.\quad \text{其中 } a,b\in G.$$

则$H=\langle a\rangle, K=\langle b\rangle$是$G$的两个3阶子群，且其交为$e$. 由于$G$可换，故$HK\leqslant G$且由定理5知：

$$|HK|=|H|\cdot|K|=9.$$

从而由Lagrange定理得$9|15$，不可能.

同理，G中除e外不可能都是5阶元素.

因此G中必有3阶元素和5阶元素. 由于G可换，从而G必有15阶元素，即G必为循环群.

注 本题的更一般结论是：设p,q是两个互异素数，则pq阶交换群必为循环群. 其证法同上面的证法完全类似.

应留意，要求G是交换群是必要的，因为例如6阶群S_3就不是一个循环群.

另外，若利用第三章§2定理5或Sylow定理来证明本题，则更为直接简单：因为G有p阶元和q阶元，又G可换，从而G有pq阶元，因此G是循环群.

19.

证 设a是可逆元且b是它的逆元，即

$$ab=ba=e.$$

则 $aba=a(ba)=ae=a,\quad ab^2a=(ab)(ba)=e\cdot e=e.$

反之，设$aba=a$且$ab^2a=e$，则可得

$$ab=(aba)b=ab\cdot ab=(ab)^2,\qquad (1)$$

$$ba=b(aba)=ba\cdot ba=(ba)^2.\qquad (2)$$

由(1)得

$$(ab)(ba)=(ab)^2ba=(abab)(ba)$$

$$=ab(ab^2a)=ab\cdot e=ab.\qquad (3)$$

而$(ab)(ba)=ab^2a=e$，故由(3)得$ab=e$.

再由(2)得

$$(ab)(ba)=(ab)(ba)^2=(abba)(ba)$$

$$=(ab^2a)(ba)=e\cdot ba=ba,$$

但是$(ab)(ba)=e$，故由上式又得$ba=e$. 从而$ab=ba=e$.

因此，a是以b为逆元的可逆元素.

20.

证 设$G=\langle a\rangle$是无限循环群，且

$$\{e\}\neq H=\langle a^s\rangle\leqslant G,$$

其中s是H中所含元素的最小正指数. 下证

$$G/H=\{a^0H, aH,\cdots,a^{s-1}H\}.\qquad (1)$$

为此只需证明：

$$G=a^0H\cup aH\cup\cdots\cup a^{s-1}H,\qquad (2)$$

$$a^iH\cap a^jH=\varnothing\quad (0\leqslant i,j<s, i\neq j).\qquad (3)$$

任取$a^k\in G$，令$k=sq+r, 0\leqslant r<s$，则由于$H=\langle a^s\rangle$，故

$$a^k=a^{sq+r}=a^r(a^s)^q\in a^rH,$$

于是(2)式成立.

又若$x\in a^iH\cap a^jH$，其中$i\neq j$. 令

$$x=a^ih_1=a^jh_2\quad (h_i\in H),$$

且不妨设$i>j$，则由于H是子群，故

$$a^{i-j}=h_2h_1^{-1}\in H\quad (0<i-j<s).$$

这与对s的假设矛盾. 故(3)式也成立.

由(2)与(3)知，商群G/H为s阶有限群. 即指数$(G:H)$有限.

21.

解 有理数加群 $\mathbf{Q}_+$ 的任何真子群的指数均无限.

设 H 是 $\mathbf{Q}_+$ 的任一真子群，则 $\{0\}\subset H\subset\mathbf{Q}_+$.

1) 先证：存在有理数 $a\notin H$ 和素数 p 使 $pa\in H$.

首先，由于 $\{0\}\neq H\subset\mathbf{Q}_+$，故存在有理数 $\frac{d}{c}\neq 0$ 使 $\frac{d}{c}\in H$，则 $c\cdot\frac{d}{c}=d\in H$，从而 H 必含有正整数. 不妨设 $d>0$ 且

$$d=p_1p_2\cdots p_m\in H\quad(p_i\text{ 为素数}).$$

取 $a\notin H$. 若 a 是一个整数，则

$$ad\in H,\quad\text{即 }p_1p_2\cdots p_ma\in H.$$

由此可逐次考察 p_ma，$p_{m-1}p_ma$，…是否属于 H，即得所要结论；若 a 是一个分数，不妨设

$$a=\frac{t}{p_1p_2\cdots p_n}\quad(p_i\text{ 为素数}).$$

当 $t\notin H$ 时，则同样由于 $td\in H$ 可得素数 p 使 $pa\in H$；当 $t\in H$ 时，则由于

$$p_1p_2\cdots p_na=t\in H,$$

故可逐次考察 p_na，$p_{n-1}p_na$，…是否属于 H 即得所要结论.

总之，存在有理数 $a\notin H$ 和素数 p 使 $pa\in H$.

2) 由于 $a\notin H$，而 $H<\mathbf{Q}_+$，故

$$a,\frac{a}{p},\frac{a}{p^2},\cdots,\frac{a}{p^n},\cdots\qquad(1)$$

显然都不在 H 中. 再证它们关于子群 H 属于不同的陪集：因若

$$\frac{a}{p^m}=\frac{a}{p^n}+h,\text{ 其中 }h\in H,m>n$$

则有

$$a=p^{m-n}a+p^mh.\qquad(2)$$

但由 1)知，$pa\in H$，故 $p^{m-n}a\in H$. 又 $p^mh\in H$，从而由(2)知，$a\in H$，矛盾.

既然(1)中无限个有理数是属于关于 H 的不同的左陪集，故 H 在 $\mathbf{Q}_+$ 中的指数无限.

注 若利用习题 3.2 第 4 题，则证明极简单.

22. 证 反证法. 设 A_4 有 6 阶子群 H，则 H 除恒等置换(1)外，H 中的置换不可全是 2 阶元，因为 A_4 中 2 阶元只有三个，它们是 (12)(34)，(13)(24)，(14)(23)；也不可能全是 3 阶元，因为 A_4 中 3 阶元共有八个：其中

(123)与(132)互逆，(124)与(142)互逆，

(134)与(143)互逆，(234)与(243)互逆.

即 H 包含的 3 阶元必成对出现，再加上(1)，这与 $|H|=6$ 矛盾. 因此，H 中必包含有 2 阶元和 3 阶元(及其逆元). 设若

$$H=\{(1),(12)(34),(123),(132),\cdots\}.$$

但 H 是子群，故必

$$(12)(34)\cdot(123)=(243)\in H,\quad(123)\cdot(12)(34)=(134)\in H.$$

从而其逆元(234)，(143)$\in H$. 这与 $|H|=6$ 矛盾.

其余情况完全类似，故 A_4 无 6 阶子群.

注 上述证明可以说是最原始的一种证法. 本题至少还有另两种证法：①利用全体 3-循环是交代群 A_n $(n\geqslant 3)$ 的一个生成系(习题 3.9 第 27 题)和习题 3.2 第 2 题；②利用群的类等式. 参考本书第三章 §6 例 2.

23.

证 1) G_i 显然包括 M 的恒等变换，故非空. 又任取 $\tau_1,\tau_2\in G_i$，则

$$\tau_1(i)=\tau_2(i)=i.$$

从而 $\tau_1\tau_2(i)=i,\tau_1^{-1}(i)=\tau_1^{-1}(\tau_1(i))=i$. 于是

$$\tau_1\tau_2,\ \tau_1^{-1}\in G_i,$$

故 $G_i\leqslant G$.

2) 设 $s,t\in G(i)$，则有 $\tau_1,\tau_2\in G$ 使

$$s=\tau_1(i),\quad t=\tau_2(i).$$

于是令 $\sigma=\tau_2\tau_1^{-1}$，便有

$$\sigma(s)=\tau_2\tau_1^{-1}(s)=\tau_2(i)=t.$$

3) 令 $G(i)=\{\tau_1(i),\tau_2(i),\cdots,\tau_m(i)\}$ 且是 M 中 m 个互异的元素，即 $|G(i)|=m$. 下证：

$$G=\tau_1G_i\cup\tau_2G_i\cup\cdots\cup\tau_mG_i \qquad (1)$$

是 G 关于子群 G_i 的一个左陪集分解.

事实上，首先，若 $\tau_s^{-1}\tau_t\in G$，则

$$\tau_s^{-1}\tau_t(i)=i,\quad \tau_s(i)=\tau_t(i),$$

这只有 $s=t$.

其次，任取 $\tau\in G$，则 $\tau(i)\in G(i)$，从而有 τ_k $(1\leqslant k\leqslant m)$ 使

$$\tau(i)=\tau_k(i),\quad \tau_k^{-1}\tau(i)=i,$$

从而 $\tau_k^{-1}\tau\in G_i,\tau\in\tau_kG_i$. 即(1)确为 G 的左陪集分解，故

$$(G:G_i)=|G(i)|=m.$$

但是 $|G|=|G_i|(G:G_i)$，从而有

$$|G|=|G_i|\cdot|G(i)|.$$

24.

证 G_A 显然非空. 又任取 $\sigma,\tau\in G_A$，则对 A 中任意 i 有

$$\sigma(i)=i,\quad \tau(i)=i.$$

于是 $\sigma\tau^{-1}(i)=\sigma(i)=i,\sigma\tau^{-1}\in G_A$. 故 $G_A\leqslant G$.

可类似证明 $G^A\leqslant G$，且显然 $G_A\leqslant G^A$. 因此

$$G_A\leqslant G^A\leqslant G.$$

注 实际上有 $G_A\trianglelefteqslant G^A$：任取 $\tau\in G_A,\sigma\in G^A,i\in A$，则 $\sigma^{-1}\in G^A,\sigma^{-1}(i)\in A$ 且

$$\sigma\tau\sigma^{-1}(i)=\sigma\tau[\sigma^{-1}(i)]=\sigma[\sigma^{-1}(i)]$$
$$=(\sigma\sigma^{-1})(i)=\varepsilon(i)=i\quad(\varepsilon\text{是恒等置换}),$$

故 $\sigma\tau\sigma^{-1}\in G_A$. 从而 $G_A\trianglelefteqslant G^A$.

25.

证 1) 由于每个置换都可表为不相连循环之积，而每个循环又可表为若干个对换之积，如

$$(i_1i_2\cdots i_n)=(i_1i_n)(i_1i_{n-1})\cdots(i_1i_2),$$

故每个置换都可表为对换之积. 又因为

$$(ij)=(1i)(1j)(1i),$$

从而每个置换都可表为若干个含 1 的对换之积. 亦即

$$M_1=\{(12),(13),\cdots,(1n)\} \qquad (1)$$

是 S_n 的一个生成系.

2) 令 $a=(12),b=(12\cdots n)$，则对 i 用归纳法可证明：

$$b^{1-i}ab^{i-1}=(i,i+1)\in\langle a,b\rangle\quad(1\leqslant i\leqslant n-1).$$

当 $j>i+1$，即 $i<j-1$ 时，有

$$(j,j-1)\cdots(i+2,i+1)(i,i+1)(i+1,i+2)\cdots(j-1,j)$$
$$=(i,j)\in\langle a,b\rangle,$$

从而$\langle a,b\rangle$包含一切对换. 因此

$$\langle a,b\rangle=S_n,$$即 $M_2=\{a,b\}$也是 S_n 的一个生成系.

注 实际上，M_1 与 M_2 都是 S_n 的既约生成系. 即不管 M_1 或 M_2，再少一个循环就不是 S_n 的生成系了.

26.

1）使$\triangle ABC$不动，或者绕 O 点旋转 $k\cdot 360°$的运动，它使 A，B，C 三点仍分别变为 A，B，C，这个运动用 σ_0 表示，它是 A，B，C 三点的恒等变换.

2）分别以 OA、OB、OC 为轴在空间各旋转 180°的运动，也使$\triangle ABC$在旋转前后占同一位置. 而且这三种运动各使 A，B，C 三点分别不动，但另两个顶点位置互相交换. 这三种运动分别表示为

$$\sigma_1=\begin{pmatrix}A & B & C\\ A & C & B\end{pmatrix},\quad \sigma_2=\begin{pmatrix}A & B & C\\ C & B & A\end{pmatrix},\quad \sigma_3=\begin{pmatrix}A & B & C\\ B & A & C\end{pmatrix}.$$

3）在$\triangle ABC$所在的平面内，围绕中心 O，按逆时针方向旋转 120°和 240°的两个运动也使$\triangle ABC$仍占同一位置，这时三个顶点 A，B，C 分别变为 B、C、A 和 C、A、B. 于是这两个运动可表示为

$$\sigma_4=\begin{pmatrix}A & B & C\\ B & C & A\end{pmatrix},\quad \sigma_5=\begin{pmatrix}A & B & C\\ C & A & B\end{pmatrix}.$$

使$\triangle ABC$占同一空间位置的其他运动，都是以上六种运动中某些运动连续施行的结果，并且仍在这六个运动之中. 这就是说，使正$\triangle ABC$占同一空间位置的运动共有六个，并且它们关于运动的运算（即连续施行，亦即置换的乘法）作成一个群，它就是 $M=\{A,B,C\}$上的三次对称群.

第三章　正规子群和群的同态与同构

§3. 1 群同态与同构的简单性质　　一、主要内容

1. 在群 G 到 $\overline{G}$ 的同态映射 φ 之下，元素的象及逆象的特征：

$$\varphi(a^{-1})=\varphi(a)^{-1}(a\in G),\quad \varphi(e)=\overline{e}.$$

但是，$\overline{G}$ 的单位元$\overline{e}$的所有逆象（即教材第三章 §3 所说的同态核 $\mathrm{Ker}\,\varphi$）作成 G 的一个正规子群（当然包含 G 的单位元 e）. 若$\overline{e}$的逆象只有 e，即 $\mathrm{Ker}\,\varphi=\{e\}$时，$\varphi$ 为单射.

2. 在群 G 到 $\overline{G}$ 的同态映射 φ 之下，子群的象和逆象的特征：

1）当 $H\leqslant G$ 时，$\varphi(H)\leqslant\overline{G}$，且 $H\sim\varphi(H)$；

2）当 $\overline{H}\leqslant\overline{G}$ 时，$\varphi^{-1}(\overline{H})\leqslant G$.

3. 本节例 3 利用 Lagrange 定理与子群乘积的阶证明了，在同构意义下 6 阶群只有两个：一个是 6 阶循环群，另一个是三次对称群 S_3.

二、释疑解难

1. 对于群同态映射φ有时不必要求是满射，有时又必须要求是满射. 例如教材本节定理 1 中的同态映射必须是满射，而定理 2 和定理 3 的同态映射φ则不要求是满射. 原因很简单：因为定理 1 中的同态映射φ若不是满射，则$\overline{G}$中必有元素没有逆象，从而φ以及群 G中元素的性质对它们不会产生任何影响，此时$\overline{G}$当然就不一定作成群；然而定理 2 和定理 3 的情形可就不同了：因为这时$\overline{G}$也是群，而且在同态映射φ（不一定是满射）之下单位元必有逆象，而于群必含单位元，从而$\overline{G}$的子群$\overline{H}$必有逆象，不会是空集.

例 1　设 G加 F 零有理数乘群，$\overline{G}$为全体有理数对乘法作成的幺半群. 则

$$\varphi:\text{正有理数}\longrightarrow 1,\ \text{负有理数}\longrightarrow -1$$

是 G 到 $\overline{G}$ 的一个同态映射（不是满射），但 G 是群而 $\overline{G}$ 却不是群.

例 2　设 G 如上例，$\overline{G}$为有理数集对

$$a\circ b=a^2\quad(\forall a,b\in\overline{G})$$

作成的代数系统. 则

$$\varphi:x\longrightarrow 1\quad(\forall x\in G)$$

显然为 G 到 $\overline{G}$ 的一个同态映射(不是满射). 虽然 G 是群,但 $\overline{G}$ 对。不仅不是群,连半群也不是(因为其代数运算不满足结合律).

2. 关于教材例 3, 若利用第三章§6 定理 3(若 $|G|=pn$. 则群 G 有 p 阶元)的结论, 则其证明可大为简化. 现在本节是利用前面已学过的知识来证明, 这也是 Lagrange 定理和已知结论

$$|KN|=\frac{|K|\cdot|N|}{|K\cap N|}$$

的一种应用. 这样做虽然稍麻烦一点, 但也很有意义.

三、习题§3. 1 解答

1.

证 在 aHa^{-1} 中任取两元素 ah_1a^{-1}, ah_2a^{-1}, 其中 $h_1, h_2\in H$. 但 H 是子群,故 $h_1h_2^{-1}\in H$. 从而

$$(ah_1a^{-1})(ah_2a^{-1})^{-1}=a(h_1h_2^{-1})a^{-1}\in aHa^{-1}.$$

因此, $aHa^{-1}\leqslant G$.

又由于易知 $\varphi: h\longrightarrow aha^{-1}(\forall h\in H)$ 是子群 H 到 aHa^{-1} 的同构映射,故

$$H\cong aHa^{-1}.$$

2.

解 在同态映射下,元素与其象的阶不一定相等. 例如,设 G 为非零有理数乘群, $\overline{G}=\{1,-1\}$ 为对普通乘法作成的群. 则易知

$$\sigma: x\longrightarrow 1 \quad 与 \quad \tau: 正有理数\longrightarrow 1, 负有理数\longrightarrow -1$$

都是群 G 到 $\overline{G}$ 的同态映射(σ 不是满射, τ 是满射). 但 $\overline{G}$ 中 1 的阶是 1, -1 的阶是 2,而 G 中除去 ±1 外的元素的阶均无限.

若 φ 是群 G 到 $\overline{G}$ 的同构映射,则任何元素与其象的阶都相同. 这是因为,对任意 $a\in G$ 有

$$\varphi(a)^m=\varphi(a^m)=\overline{e}\Longleftrightarrow a^m=e.$$

3.

解 φ 显然是 $GL_n(F)$ 的双射变换,但不是自同构:因为一般

$$(AB)^T=B^TA^T\neq A^TB^T, \quad 即\ \varphi(AB)\neq\varphi(A)\cdot\varphi(B).$$

又 $\sigma: A\longrightarrow(A^{-1})^T$ 显然是双射变换且

$$\sigma(AB)=[(AB)^{-1}]^T=(B^{-1}A^{-1})^T$$
$$=(A^{-1})^T\cdot(B^{-1})^T=\sigma(A)\cdot\sigma(B),$$

故 σ 是群 $GL_n(F)$ 的自同构.

4.

证 由于 $G=\{e,a,b,b^2,ab,ab^2\}$ 且 $|a|=2, |b|=3$,故易知 ba 不等于 e,a,b,b^2. 又 $ba\neq ab$ (因若 $ab=ba$,则 $|ab|=6$,从而 G 为 6 阶循环群,这与 G 不是循环群的假设矛盾). 因此, $ba=ab^2$. 由此可得 G 的乘法表如下:

$\cdot$	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

再把 S_3 中六个置换按顺序(1),(12),(123),(132),(23),(13)列出乘法表(略去),即可知 φ 是 G 到 S_3 的同构映射.因此,$G\cong S_3$.

5. 证 因为 $|G|=4$, G 又不是循环群,从而 G 无 4 阶元.于是由 Lagrange 定理知,G 中除单位元 e 外每个元素的阶均为 2.因此,若令

$$G=\{e,a,b,c\},$$

则映射

$$\varphi:\quad e\longrightarrow(1),\ b\longrightarrow(34),\ a\longrightarrow(12),\ c\longrightarrow(12)(34)$$

是 G 到 Klein 四元群 $K_4=\{(1),(12),(34),(12)(34)\}$ 的同构映射.因此,$G\cong K_4$.

6.

证 显然 φ 是群 G 到群 $\overline{G}$ 的满射.

又由于当 $(ab,2)=1,(cd,2)=1$ 时显然有

$$(abcd,2)=1,$$

且
$$\varphi\left(2^n\cdot\frac{b}{a}\cdot 2^m\cdot\frac{d}{c}\right)=\varphi\left(2^{n+m}\cdot\frac{bd}{ac}\right)=n+m$$
$$=\varphi\left(2^n\cdot\frac{b}{a}\right)\varphi\left(2^m\cdot\frac{d}{c}\right),$$

故 φ 是正有理数乘群 G 到整数加群 $\overline{G}$ 的一个同态满射.

§3.2 正规子群和商群

一、主要内容

1. 正规子群定义、性质和例子.性质主要有

1) 设 $N\leqslant G$.则

$$N\lhd G\Longleftrightarrow aNa^{-1}\subseteq N\quad(\forall a\in G)$$

或
$$N\lhd G\Longleftrightarrow axa^{-1}\in N\quad(\forall a\in G,x\in N).$$

2) 正规子群在同态满射下的象和逆象均仍为正规子群.

3) 正规子群与子群之积是子群;正规子群与正规子群之积是正规子群.

2. 商群定义及商群的一个应用(Cauchy 定理 pn 阶交换群必有 p 阶子群,其中 p 为素数).

3. 介绍由正规子群来界定的两类群:哈密顿群和单群.这是两类在群论研究中占很重要地位的群.

二、释疑解难

1. 教材在本节所举的例子中,应该十分注意 S_4、及 $S_n(n\neq 4)$ 的正规子群的状况.因为这涉及 S_2, S_3 及 S_4 都是可解群(参考本节习题第 8 题),而当 $n\geq 5$ 时 S_n 不是可解群.这种名称来源于一般的二、三、四次代数方程都有求根公式,即可根式解,但一般的五次和五次以上助代数方程都没有求根公式,即不可根式解.

2. 若 $N\lhd G$,则对群 G 中任意元素 a,b 都有

$$(aN)(bN)=abN.$$

这是在教材中已经证明了的.对此也可以采取以下证法:

任取 $x\in(aN)(bN)$,并令

$$x=an_1\cdot bn_2\quad(n_1,n_2\in N).\qquad(1)$$

由于 $N\lhd G$,从而 $n_1b\in Nb=bN$.于是令

$$n_1b=bn_3\quad(n_3\in N).$$

由(1)得

$$x=a(n_1b)n_2=a(bn_3)n_2$$
$$=ab\cdot n_3n_2\in abN.$$

因此,$(aN)(bN)\subseteq abN$.

反之,任取 $x\in abN$,则类似可证 $x\in(aN)(bN)$.故又有

$$abN\subseteq(aN)(bN).$$

因此，$(aN)(bN)=abN$.

这种证法是最原始的一种证法，当然不如教材中的证法简单．其所以简单，是由于利用了子集乘法的性质 $(AB)C=A(BC)$ 以及 $Nb=bN$ 和 $N^2=N$.

3．在本教材中，共有三个定理(本节定理5、§6定理3及§8定理1)涉及 pn(p 是素数)阶群 G 必有 p 阶子群．从表面上看，这三个定理似有重复之感．实际上三者互相联系紧密，而且其中任何一个都不能由另一个所代替．这是因为，本节定理5是假设 G 为交换群，§6定理3并不假设 G 为交换群，但在证明中要用到本节定理5；又§8定理1(即第一 sylow 定理)又要用到§6定理3．因此，三者密不可分，而且哪一个也不是多余的．对此，示意如下：

pn 阶交换群必有 p 阶子群(本节定理5)⟶

凡 pn 阶群必有 p 阶子群(§6定理3)⟶p^sm 阶群必有 $p^i(i=0,1,\cdots,s)$ 阶子群(§8定理1)．

4．李型单群是李代数中谢瓦莱单群和单扭群的统称，它们是一些由矩阵作成的群．

三、习题§3．2解答

1．略

2．

证法Ⅰ 设 G 是群且 $N\leqslant G$，$(G:N)=2$．则有

$$G=N\cup aN,\quad N\cap aN=\varnothing.$$

任取 $n\in N$，$x\in G$，若 $x\in N$，则当然 $xnx^{-1}\in N$；

若 $x\notin N$，则必 $x\in aN$，从而可令

$$x=an_1\quad(n_1\in N).$$

设若 $xnx^{-1}\notin N$，则必 $xnx^{-1}\in aN$，从而可令

$$xnx^{-1}=an_2\quad(n_2\in N),$$

即 $an_1nn_1^{-1}a^{-1}=an_2$，从而 $a=n_2^{-1}n_1nn_1^{-1}\in N$，矛盾．故必 $xnx^{-1}\in N$.

因此，$N\trianglelefteqslant G$.

证法Ⅱ 令 N 与 G 为如上所设．则任取 $x\in G$，当 $x\in N$ 时当然有

$$xN=Nx=N.$$

当 $x\notin N$ 时，则由于 $(G:N)=2$，故

$$G=N\cup xN=N\cup Nx,$$

从而也有 $xN=Nx$，故 $N\trianglelefteqslant G$.

3．

证 设 $H\leqslant G$ 且 $|H|=n$．则对 G 中任意元素 a，易知 aHa^{-1} 也是 G 的一个 n 阶子群．

但由题设，G 的 n 阶子群只有一个，故

$$aHa^{-1}=H\quad(\forall a\in G),$$

从而 $H\trianglelefteqslant G$.

4．

证 由于 $H\leqslant G$，且 $(G:H)=m$，故商群 G/H 是一个 m 阶群．于是对 G 中任意元素 a，商群 G/H 中元素 $aH=\bar{a}$ 都满足方程

$$x^m=\bar{e}\quad(\bar{e}=H\text{ 是 }G/H\text{ 的单位元}).$$

于是 $\bar{a}^m=(aH)^m=a^mH=H$．因此 $a^m\in H$.

5．

证 任取 $a\in H$，$b\in K$．则因 $H\leqslant G$，$K\trianglelefteqslant G$，故

$$aba^{-1}b^{-1}\in H\cap K=\{e\}.$$

从而 $aba^{-1}b^{-1}=e$，$ab=ba$.

6．

证 首先，由于子群 H 含于群 G 的中心，故显然 $H \trianglelefteq G$.

当 G/H 是循环群，且 $G/H=\langle aH\rangle$ 时，令

$$xH, yH \in \langle aH\rangle, \quad \text{且 } xH=(aH)^s, yH=(aH)^t.$$

则 $xH=a^sH$，$yH=a^tH$，于是有 $h_1, h_2 \in H$ 使

$$x=a^sh_1, \quad y=a^th_2.$$

由于 H 中元素同 G 中任何元素可交换，故

$$xy=(a^sh_1)(a^th_2)=(a^th_2)(a^sh_1)=yx,$$

即 G 是交换群.

7.

证 任取 $a \in G$，则 $aN \in G/N$. 但因为商群 G/N 是周期群，故有正整数 m 使

$$(aN)^m=a^mN=N, \quad \text{即 } a^m \in N.$$

又因为 N 也是周期群，故又有正整数 n 使

$$(a^m)^n=a^{mn}=e,$$

从而 a 的阶有限，即 G 是一个周期群.

8.

证 因为 $e \trianglelefteq S_2$，而 $S_2/e \cong S_2$ 是交换群，故 S_2 是可解群.

又令 $H=\{(1),(123),(132)\}$，则由本节教材例 1 知：

$$e \trianglelefteq H \trianglelefteq S_3, \quad \text{且 } H/e, S_3/H \text{ 均可换.}$$

故 S_3 是可解群.

再由本节教材例 3 知：

$$e \trianglelefteq K_4 \trianglelefteq A_4 \trianglelefteq S_4.$$

而且 K_4/e、A_4/K_4、S_4/A_4 又都是交换群，故 S_4 是可解群.

注 因为当 $n \geqslant 5$ 时 A_n 是单群，故只有

$$e \trianglelefteq A_n \trianglelefteq S_n.$$

但是 $A_n/e \cong A_n$ 是非交换群，故此时 S_n 不是可解群.

§3.3 群同态基本定理

一、主要内容

1. 在同构意义下，每个群能而且只能与其商群同态. 即指以下两点：

   1) 设 $N \trianglelefteq G$，则 $G \sim G/N$ $(\tau: a \longrightarrow aN)$ 且 $\mathrm{Ker}\,\tau=N$；

   2) 反之，若 $G \overset{\tau}{\sim} \overline{G}$，则 $N=\mathrm{Ker}\,\tau \trianglelefteq G$ 且 $G/N \cong \overline{G}$.

2. 在同态映射下，循环群的同态象是循环群.

3. 若 $G \sim \overline{G}$，则群 G 的所有包含核的子群同已的 $\overline{G}$ 有于群间有一个保持包含关系的双射.

二、释疑解难

1. 设 $N \trianglelefteq G$，则称 $\tau: a \longrightarrow aN$ $(\forall a \in G)$ 为群 G 到商群的自

然同态. 应注意，除自然同态外，G 到 G/N 可能还有别的同态.

例 1 $N=\{(1),(12)\}\trianglelefteqslant G=\{(1),(12),(34),(12)(34)\}$. 又

$$G/N=\{N,(34)N\}.$$

易知 φ: $(1),(34)\longrightarrow N$, $(12),(12)(34)\longrightarrow(34)N$

也是 G 到商群 G/N 的同态满射，但它不是自然同态.

2. 应注意，教材中推论 1 的逆定理不成立. 即若有限群 $\overline{G}$ 的阶整除有限群 G 的阶，则不一定有 $G\sim\overline{G}$.

例 2 设 $\overline{G}$ 为三次对称群 S_3，G 为 12 次单位根乘群，则 $|\overline{G}|=6$ 整除 $|G|=12$. 但是不可能有 $G\sim\overline{G}$，因为 G 是交换群，其同态象必为交换群，但 S_3 不是交换群.

3. 教材定理 3 中的 $G\sim\overline{G}$ 必须强调是满同态. 若不是满同态，则定理 3 应改述为：若 φ 是群 G 到群 $\overline{G}$ 的一个同态映射，则当 G 为循环群时同态象 $\varphi(G)$ 也是循环群.

4. 教材定理 4 的两个条件“φ 是满同态”和“G 的含 K 的所有子群”不能少.

1) 例如，设 G 为任意群，$\overline{G}$ 为 2 阶群. 则显然

$$\varphi:\ x\longrightarrow\overline{e}\quad(\forall x\in G,\overline{e}\text{为}\overline{G}\text{的单位元})$$

是 G 到 $\overline{G}$ 的同态映射(但不是满射)，而 $\mathrm{Ker}\,\varphi=G$. 从而 G 的包含核的子群只有一个即 G 本身. 但 $\overline{G}$ 有两个子群，显然二者间不能建立双射.

2) 又例如，设 $|G|>1$，$|\overline{G}|=1$，则

$$\varphi:\ x\longrightarrow\overline{e}\quad(\forall x\in G)$$

是群 G 到 $\overline{G}$ 的同态满射，且核 $K=\mathrm{Ker}\,\varphi=G$. 若不强调“含 K”的所有子群，则 G 至少有两个子群 $\{e\}$ 及 G. 但 $\overline{G}$ 只有一个子群即 $\overline{G}$ 本身，二者间显然也不能建立双射.

三、习题 §3. 3 解答

1.

证 设 φ 是群 G 到群 $\overline{G}$ 的一个同态映射，且核为 K，又 G 中元素 x 在 φ 之下的象表示为 $\overline{x}$，即 $\overline{x}=\varphi(x)$. 则对任意 $a,b\in G$，若 $\overline{a}=\overline{b}$，则

$$\overline{a}\overline{b}^{-1}=\overline{e},\quad\overline{ab^{-1}}=\overline{e},\quad ab^{-1}\in K,$$

即 G 中元素 a 与 b 在 K 的同一陪集中.

反之，倒推回去即得.

注 本题原设 $G\sim\overline{G}$，但实际上对同态映射可不要求是满射.

2.

证 设 G 是单群，且 φ 是 G 到群 $\overline{G}$ 的一个同态满射. 又设 $\overline{N}\trianglelefteqslant\overline{G}$ 且 $\varphi^{-1}(\overline{N})=N\trianglelefteqslant G$. 但 G 是单群，故

$$N=G\quad\text{或}\quad N=\{e\}.$$

当 $N=G$ 时，$\overline{N}=\overline{G}$；当 $N=\{e\}$ 时，$\overline{N}=\{\overline{e}\}$. 即 $\overline{G}$ 是单群或单位元群.

3.

证 设 φ 为群 G 到商群 G/N 的自然同态，则对 G 中任意元素 x 有 $\varphi(x)=xN$. 由题设知，N 也是 H 的正规子群. 故若 $a\in H$，则 $\varphi(a)=aN\in H/N$. 从而 $\varphi(H)\subseteq H/N$.

又显然 $H/N\subseteq\varphi(H)$. 故 $\varphi(H)=H/N$.

4.

证　1) 设 $G=\langle a\rangle$ 是无限循环群，$\overline{G}=\langle b\rangle$ 是任一循环群，定义

$$\varphi: G\longrightarrow\overline{G},\ a^k\longrightarrow b^k,\ k\in\mathbf{Z}.$$

因为 $G=\langle a\rangle$ 是无限循环群，所以 $|a|=\infty$，从而

$$a^k=a^l\Longleftrightarrow k=l.$$

于是，若 $a^k=a^l$，则 $\varphi(a^k)=\varphi(a^l)$，故 φ 是无限循环群 G 到循环群 $\overline{G}$ 的映射.

又易知 φ 是满射且保持运算，因此 $G\sim\overline{G}$.

2) 设 $G=\langle a\rangle,\overline{G}=\langle b\rangle$ 是两个有限循环群且

$$|a|=m,\ |b|=n.$$

设 $G\sim\overline{G}$，且 ψ 为其一同态满射，则 $G/\mathrm{Ker}\,\psi\cong\overline{G}$. 但由于

$$|\overline{G}|=|G/\mathrm{Ker}\,\psi|$$

整除 $|G|$，故 $|\overline{G}|\mid|G|$.

反之，设 $|\overline{G}|\mid|G|$，即 $n\mid m$. 定义：

$$\varphi: G\longrightarrow\overline{G},\quad a^s\longrightarrow b^r.$$

其中 $s=nq+r,q,r\in\mathbf{Z}$ 且 $0\leqslant r<n$.

任取 $a^x,a^y\in\langle a\rangle$，且令

$$x=nq_1+r_1,\quad y=nq_2+r_2,\quad 0\leqslant r_1,r_2<n.$$

当 $a^x=a^y$，即

$$a^{x-y}=a^{n(q_1-q_2)+(r_1-r_2)}=e,$$

亦即 $n\mid[n(q_1-q_2)+r_1-r_2]$ 时，必有 $n\mid(r_1-r_2)$，但是

$$0\leqslant|r_1-r_2|<n,$$

故 $r_1-r_2=0$，即 $r_1=r_2$. 从而

$$\varphi(a^x)=b^{r_1}=b^{r_2}=\varphi(a^y),$$

故 φ 是从 G 到 $\overline{G}$ 的映射. 又易知 φ 是满射且保持运算，因此，$G\sim\overline{G}$.

5.

证法 I　反证法.

若不然，设加群 $\mathbf{Q}_+$ 与乘群 $\mathbf{Q}^*$ 同构且 φ 为其一同构映射，则令 $\varphi(a)=-1$ $(a\in\mathbf{Q}_+)$，于是

$$\varphi\left(\frac{a}{2}\right)^2=\varphi\left(\frac{a}{2}\right)\varphi\left(\frac{a}{2}\right)=\varphi\left(\frac{a}{2}+\frac{a}{2}\right)=\varphi(a)=-1.$$

即有有理数 $\frac{a}{2}$ 其平方等于 -1. 这是不可能的，因此，$\mathbf{Q}_+$ 与 $\mathbf{Q}^*$ 不同构.

证法 II　反证法.

若不然，设 $\mathbf{Q}_+\cong\mathbf{Q}^*$，且 φ 为其一同构映射，则由于 0 是 $\mathbf{Q}_+$ 的零元而 1 是 $\mathbf{Q}^*$ 的单位元，故必

$$\varphi(0)=1.\qquad(1)$$

又由于 $-1\in\mathbf{Q}^*$，故有 $x\in\mathbf{Q}_+$ 使 $\varphi(x)=-1$. 于是

$$\varphi(2x)=\varphi(x+x)=\varphi(x)\varphi(x)=(-1)\cdot(-1)=1.\qquad(2)$$

但 φ 是单射，故由(1)与(2)知，$2x=0,x=0$. 那么

$$\varphi(0)=-1.$$

这与(1)矛盾. 故 $\mathbf{Q}_+$ 与 $\mathbf{Q}^*$ 不同构.

§3.4　群的同构定理

一、主要内容

1. 本节主要介绍了群的三个同构定理. 它们是：

1) $G\overset{\varphi}{\sim}\overline{G}$, $\mathrm{Ker}\,\varphi\subseteq N\lhd G \Longrightarrow G/N\cong\varphi(G)/\varphi(N)$;

2) $H\leqslant G, N\lhd G \Longrightarrow H\cap N\lhd H, HN/N\cong H/(H\cap N)$;

3) $N\lhd G, \overline{H}\leqslant G/N \Longrightarrow G$ 有惟一子群 $H\supseteq N$ 使 $\overline{H}=H/N$;

若 $\overline{H}\lhd G/N \Longrightarrow$ 有惟一的 $H\lhd G$ 使 $\overline{H}=H/N$ 且

$$G/H\cong(G/N)/(H/N).$$

2. 借助同构定理，作为例子证明了以下两个结论；

1) $H, K\lhd G \Longrightarrow G/HK\cong(G/H)/(HK/H)$;

2) $S_4/K_4\cong S_3$ （K_4 为 Klein 四元群）.

二、释疑解难

1. 第一同构定理还有另一证法，见本节习题第 4 题，此外还应注意第一同构定理中的两个条件：

1) φ 必须是满同态.

因若不然，设 G 为任意群，$\overline{G}$ 为 2 阶群，则 $\varphi: x\longrightarrow\overline{e}\ (\forall x\in G)$ 是 G 到 $\overline{G}$ 的一个同态映射（但不是满射）. 此时 $\mathrm{Ker}\,\varphi=N=G$，而 $\overline{N}=\{\overline{e}\}$，从而 G/N 为 1 阶群，而 $\overline{G}/\overline{N}$ 为 2 阶群，二者当然不会同构.

2) G 的正规子群 N 必须包含核 $\mathrm{Ker}\,\varphi$.

因若不然，例如设 G 是 6 阶循环群，$\overline{G}=\{\overline{e}\}$ 是单位元群，则

$$\varphi: x\longrightarrow\overline{e}\quad(\forall x\in G)$$

是满同态，且 $\mathrm{Ker}\,\varphi=G$. 现取 G 的一个 2 阶子群 $N\supsetneq\mathrm{Ker}\,\varphi$，则此时 G/N 为 3 阶群，而 $\overline{G}/\overline{N}$ 为 1 阶群，二者当然不能同构.

因此，“φ 是满同态”与“G 的正规子群 N 包含核”这两个条件都不能少.

2. 关于第二同构定理的说明.

1) 条件要求：$H\leqslant G, N\lhd G$. 由此可得

$$H\cap N\lhd H,\qquad N\lhd HN.$$

（应注意，一般 $H\cap N\not\lhd N$，$H\not\lhd HN$. 读者作为练习可自己举例）. 而且商群 $H/(H\cap N)$ 与 $(HN)/N$ 同构. 再结合教材中所画的示意图，从而不难记住这个定理.

2) 关于本定理的证明，教材中是先证

$$\varphi: x\longrightarrow xN\quad(\forall x\in H)$$

是 H 到 HN/N 的同态满射，再证 $\mathrm{Ker}\,\varphi=H\cap N$（因为证明容易，教材中省略），故而得

$$H/(H\cap N)\cong HN/N. \qquad (1)$$

对此也可以采取另一种证法如下：令

$$\tau: x(H\cap N)\longrightarrow xN\quad(\forall x\in H).$$

可以证明，τ 是商群 $H/(H\cap N)$ 到 HN/N 的一个同构映射（此证明留给读者）. 因此可直接得(1).

至于定理的结论写成

$$H/(H\cap N)\cong HN/N \quad 或 \quad HN/N\cong H/(H\cap N),$$

这是无关紧要的，因为同构关系具有对称性.

3. 第一同构定理说明商群中子群的特征. 简言之，商群中的子群仍为一种商群；且商群之

商群可类似于普通分数那样$\left(\dfrac{b}{a}=\dfrac{b/c}{a/c}\right)$进行约分.

三、习题§3. 4解答

1.

证　设 φ 是群 G 到群 $\overline{G}$ 的同态满射，由题设知：

$$\mathrm{Ker}\,\varphi\subseteq N=\varphi^{-1}(\overline{N})\trianglelefteqslant G,$$

且 $\varphi(N)=\varphi[\varphi^{-1}(\overline{N})]=\overline{N}$. 于是由第一同构定理即得证.

2.

证　1) $H\cap K'\leqslant H\cap K$ 显然. 又设

$$a\in H\cap K',\quad x\in H\cap K,$$

则由于 $x,a\in H$，又 $H\leqslant G$，故 $xax^{-1}\in H$.

又由于 $a\in K'$，$x\in K$，而 $K'\trianglelefteqslant K$，故又有

$$xax^{-1}\in K'.$$

从而，$xax^{-1}\in H\cap K'$. 因此，$H\cap K'\trianglelefteqslant H\cap K$.

2) 易知

$$\varphi:\ x(H\cap K')\longrightarrow xK'\ (x\in H\cap K)$$

是群$(H\cap K)/(H\cap K')$到 K/K'的单同态，故由同态基本定理知：

$$(H\cap K)/(H\cap K')\cong\varphi((H\cap K)/(H\cap K'))\leqslant K/K'.$$

3.

证　任取 $x,y\in G$，由于 G/K 可换，故

$$xK\cdot yK=yK\cdot xK,\quad \text{即 } xyK=yxK.$$

从而$(xy)^{-1}(yx)\in K\leqslant H$. 因此，

$$(xy)^{-1}(yx)\in H,\quad xyH=yxH.$$

即 $xH\cdot yH=yH\cdot xH$，G/H 也是交换群.

4.

证　因为 φ 是满同态，故 σ 显然是 G 到 $\overline{G}/\overline{N}$ 的一个满射；又由于

$$\varphi(ab)\overline{N}=\varphi(a)\varphi(b)\overline{N}=\varphi(a)\overline{N}\cdot\varphi(b)\overline{N},$$

即 $\sigma(ab)=\sigma(a)\sigma(b)$，故 σ 是群 G 到 $\overline{G}/\overline{N}$ 的一个同态满射. 于是

$$G\sim\overline{G}/\overline{N}.$$

下面再证 $\mathrm{Ker}\ \sigma=N$.

首先，任取 $x\in N$，则 $\varphi(x)\in\overline{N}$，于是在 σ 之下

$$x\longrightarrow\varphi(x)\overline{N}=\overline{N},$$

故 $x\in\mathrm{Ker}\,\sigma$，$N\subseteq\mathrm{Ker}\,\sigma$；

其次，任取 $c\in\mathrm{Ker}\,\sigma$，则在 σ 之下有

$$c\longrightarrow\varphi(c)\overline{N}=\overline{N},$$

即 $\varphi(c)\in\overline{N}$. 但是 $\overline{N}=\varphi(N)$，故有 $x\in N$ 使

$$\varphi(x)=\varphi(c)\quad\text{或}\quad\varphi(x^{-1}c)=\overline{e},$$

其中$\overline{e}$是 $\overline{G}$ 的单位元. 于是

$$x^{-1}c\in\mathrm{Ker}\,\varphi\subseteq N,\quad c\in N,$$

即又有 $\mathrm{Ker}\,\sigma\subseteq N$，因此 $\mathrm{Ker}\,\sigma=N$.

既然同态 $G\sim\overline{G}/\overline{N}$ 的核是 N，于是由群同态基本定理知，

$$G/N\cong\overline{G}/\overline{N}.$$

5.

证　因为由群第二同构定理知：

$$H_i/(H_i\cap N)\cong H_iN/N\leqslant G/N\quad(i=1,2),$$

故$(H_i,N:N)=(H_i:H_i\cap N)$整除$(G:N)$. 又由 Lagrange 定理知：

$$|H_i|=|H_i\cap N|(H_i:H_i\cap N),$$

从而$(H_i,N:N)$也整除$|H_i|$. 因此，$(H_i,N:N)$整除$(|H_i|,(G:N))=1$. 这只有$(H_i,N:N)=1$，即 $H_iN=N$，从而 $H_i\leqslant N$，$H_1H_2\leqslant N$.

6.

证 设 φ 是群 G 到商群 G/N 的自然同态.

1) 设 N 是 G 的极大正规子群，下证：G/N 是单群.

任取 $K/N\lhd G/N$，且 $K/N\neq\{N\}$，则

$$\varphi^{-1}(K/N)\lhd G.$$

因为 $N\in K/N$，而 φ 是自然同态，故 $\varphi^{-1}(N)=N$，从而

$$N\subseteq\varphi^{-1}(K/N).$$

又因为 $K/N\neq\{N\}$，故 $N\neq\varphi^{-1}(K/N)$，即

$$N\subset\varphi^{-1}(K/N).$$

但 N 是群 G 的极大正规子群，因此

$$\varphi^{-1}(K/N)=G.\quad\text{故 } K/N=G/N.$$

即 G/N 只有平凡正规子群，从而为单群.

2) 设 G/N 是单群. 下证：N 是 G 的极大正规子群.

设 $N\subset K\lhd G$，则

$$\varphi(K)\lhd G/N.$$

但因 $N\subset K$，故 $\varphi(K)\neq\{N\}$；又因 G/N 是单群，故

$$\varphi(K)=G/N.$$

任取 $a\in G$，由于 $\varphi(K)=G/N=\varphi(G)$，故存在 $k\in K$ 使

$$\varphi(a)=\varphi(k),\quad\varphi(ak^{-1})=N,$$

从而 $ak^{-1}\in\operatorname{Ker}\varphi=N\subset K$，故 $a=ak^{-1}\cdot k\in K$，$G\subseteq K$. 于是 $K=G$.

即 N 是 G 的极大正规子群.

§3.5 群的自同构群

一、主要内容

1. 群的自同构群、内自同构群以及特征子群和全特征子群的定义和例子.

1) 群 G 的全体自同构关于变换的乘法作成一个群，称为 G 的自同构群. 记为 Aut$G$.

2) 群 G 的全体内自同构

$$\sigma_a:x\longrightarrow axa^{-1}\quad(\forall x,a\in G)$$

作成 Aut G 的一个正规子群，称为 G 的内自同构群，记为 Inn G.

3) 设 $N\leqslant G$. 若对群 G 的每个自同构 σ 都有

$$\sigma(N)\subseteq N,$$

则称 N 是 G 的一个特征子群.

4) 若对群 G 的每个自同态 Ψ 都有

$$\Psi(N)\subseteq N,$$

则称子群 N 为群 G 的一个全特征子群.

2. 群 G 的内自同构群 Inn G 与自同构群 Aut G 和其中心 C 间有以下重要关系：

$$G/C\cong\operatorname{Inn}G\lhd\operatorname{Aut}G.$$

二、释疑解难

1．教材中曾经指出，要从已知群定出其自同构群，一船而言，是非常困难的，这由教材中所举出的例子即可说明这一点．但是，对有些群却可定出其自同构群伪一些性质，就本教材而言，主要有：

1)定理 2 指出，从循环群可定出其自同构群的阶．

2)从教材本节例 1 和上节例 2 知；

Aut R 主 5：宣 5J／Ki“

从而 Nein 四元群 K_4 的自同构群是非常清楚的，它是一个 6 阶非交换群，而且其元素的阶以及子群和正规子群的状况都很清楚．

3)本节习题第 6 题指出，无中心群的自同构群仍是一个无中心群，从而由教材第二章§6 定理 6 可知．当 $n\geqslant 3$ 时，S_n 的自同构群是一个无中心群．

2．群 G 中元素 a 与 b 确定同一个内自同构($\sigma_a=\sigma_b$)的无要条件是：

$$aC=bC \quad (a,\ b\in C).$$

即 a 与 b 在同一个(关于 C 的)陪集中．因此，有多少个关于 C 的陪集就有多少个 G 的内自同构，即 $|\mathrm{Inn}G| =(G:C)$。其实这一点也是同构 $\mathrm{Inn}G\cong G/C$ 的直接结果，即

$$|\mathrm{Inn}\,G|=|G/C|=(G:C).$$

3.群 G 的自同构群显然是 G 上对称群 $S(G)$ (G 的全体双射变换关于变换乘法作成的群)的一个子群，即

$$\mathrm{Aut}\,G\leqslant S(G).$$

从而可知，当 $|G|=n$ 时，$\mathrm{Aut}\,G\leqslant S_n$．于是

$$|\mathrm{Aut}\,G|\ \Big|\ n!.$$

进一步，由于群的每个自同构部保持单位元 e 不变，因此实际上更有

$$\mathrm{Aut}\,G\leqslant S_{n-1}.\quad \text{从而}\ |\mathrm{Aut}\,G|\ \Big|\ (n-1)!.$$

4．由于

$$\text{全特征子群}\subset\text{特征子群}\subset\text{正规子群},$$

故特征子群是一类特殊的正规于群，而全特征子群又是一类特殊的特征子群．

我们知道，正规子群是不可传递的，即正规子群的正规子群不一定是原群的正规子群．但是，对于特征子群和全待征子群来说，却是可以传递的．即若 G_1 是群 G_2 的(全)持征子群，又 G_2 是群 G_3 的(全)持征子群，则 G_1 必是 G_3 的(全)特征子群．这个证明并不难，留给读者作为练习．

三、习题§3．5 解答

1.

证　由定理 2 知，n 阶循环群的自同构群是一个 $\varphi(n)$ 阶群，然而

$$\varphi(1)=\varphi(2)=1,\quad \varphi(3)=\varphi(4)=\varphi(6)=2,$$

故 1、2、3、4、6 阶循环群的自同构群显然都是循环群．

5 阶循环群 $\langle a\rangle$ 的自同构群是一个 $\varphi(5)=4$ 阶群．但易知

$$\tau:\ x\longrightarrow x^3\quad (\forall\, x\in\langle a\rangle)$$

是 $\langle a\rangle$ 的一个自同构，且 $|\tau|=4$．即 4 阶群中有 4 阶元，故 5 阶循环群的自同构群也是一个循环群．

7 阶循环群 $\langle b\rangle$ 的自同构群是一个 $\varphi(7)=6$ 阶群．但易知

$$\sigma:\ x\longrightarrow x^5$$

是 $\langle b\rangle$ 的一个自同构，且 $|\sigma|=6$．即 6 阶群中有 6 阶元，故 7 阶循环群的自同构群也是一个循环群．

注　问：8 阶循环群的自同构群是循环群吗？它与 Klein 四元群有何关系？(可参阅习题 4.12 第 16 题)

2.

证　设 G 是一个非交换群，$\mathrm{Aut}\,G$ 是 G 的自同构群，$\mathrm{Inn}\,G$ 是 G 的内自同构群，则由定理 4 知，

$$G/C\cong \mathrm{Inn}\,G,$$

其中 C 为群 G 中心. 但由于 G 是非交换群，由习题 3.2 第 6 题知，G/C 不是循环群，从而 $\mathrm{Inn}\,G$ 不是循环群. 由于循环群的子群是循环群，因此，$\mathrm{Aut}\,G$ 不是循环群.

3.

证　因为 $|\mathrm{Aut}\,G|=1$，从而 $|\mathrm{Inn}\,G|=1$. 但由定理 4，

$$\mathrm{Inn}\,G\cong G/C \quad (C \text{ 为 } G \text{ 的中心}),$$

从而 $|G/C|=1$. 故 $G=C$ 是交换群. 据此又易知

$$\tau: a \longrightarrow a^{-1} \quad (\forall a\in G)$$

是群 G 的自同构，从而 τ 是 G 的恒等自同构. 于是对 G 中任意元 a 都有 $a^{-1}=a$，即 $a^2=e$，得证.

4. 证　因为中心 $C\leqslant G$，而 G 是非交换单群，故只有 $C=\{e\}$. 从而由定理 4 知：

$\mathrm{Inn}\ G\cong G/C\cong G.$

因此，$G\cong \mathrm{Inn}G.$

5.

证　若对 G 的每个自同构 σ 都有 $\sigma(N)=N$，当然 $\sigma(N)\subseteq N$，故 N 是 G 的特征子群.

反之，设 N 是 G 的一个特征子群，而 σ 是 G 的任一自同构，则有 $\sigma(N)\subseteq N$. 又因 σ^{-1} 也是 G 的自同构，故又有

$$\sigma^{-1}(N)\subseteq N, \quad \sigma(\sigma^{-1}(N))\subseteq\sigma(N).$$

从而 $N\subseteq\sigma(N)$. 因此，$\sigma(N)=N$.

6.

证　任取 $\tau\in \mathrm{Aut}\,G$，但 τ 不是恒等自同构，则有 $a\in G$ 使

$$\tau(a)=b\neq a,$$

如果 τ 属于 $\mathrm{Aut}\,G$ 的中心，则 τ 必与群 G 的每个自同构可换，从而与 G 的内自同构 σ_a 可换：

$$\tau\sigma_a=\sigma_a\tau,$$

于是对任意 $x\in G$，令 $x=\tau(y)$，则有

$$\tau\sigma_a(y)=\sigma_a\tau(y) \text{ 或 } \tau(aya^{-1})=\sigma_a(x),$$

$$\tau(a)\tau(y)\tau(a)^{-1}=axa^{-1},$$

$$bxb^{-1}=axa^{-1},\ (a^{-1}b)x=x(a^{-1}b),$$

即 $a^{-1}b$ 是 G 的中心元素. 但 G 是无中心群，故

$$a^{-1}b=e, \quad b=a,$$

矛盾. 因此，$\mathrm{Aut}\,G$ 也是无中心群.

§3.6　共轭关系与正规化子

一、主要内容

1. 群中子集的共轭(特别是元素的共轭、子群的共轭)定义，和由此得到的共轭子集类(特别是共轭元素类和共轭子群类)以及群的类等式等概念.

2. 正规化子 $N(S)$ 与中心化于 $C(S)$ 的定义和性质有：

$$N(S)\leqslant G, \quad H\leqslant N(H), \quad C(H)\trianglelefteq N(H).$$

其中 S 是群 G 的子集，而 $H\leqslant G$.

3. 正规化子的作用(刻画一个共轭类中成员的个数)和一个应用(cauchy 定理：pn 阶群有 p 阶于群).

二、释疑解难

1．二元素是否共轭同此二元素所在的群的范围有关．就是说，设

$$a,\ b\in H\leqslant G,$$

则若 a 与 b 在 H 中共轭，当然在 G 中一定共轭；但是，当 a 与 b 在 G 中共轭时．则在 H 中不一定共轭．

例 1 交代群 A_4 中的元素(123)与(132)在 S_4 中共轭，因为有 $(12)\in S_4$ 使

$$(12)(123)(12)^{-1}=(132);$$

但是在 A_4 中不共轭，因为易知 A_4 有 4 个共轭类：

$\{(1)\}$，　　$\{(12)(34),(13)(24),(14)(23)\}$，

$\{(123),(134),(142),(243)\}$，　$\{(132),(143),(124),(234)\}$．

从而可知，(123)与(132)在 A_4 中不共轭．

另外，群 S_4（参考习题 3.9 第 30 题）及 A_4 的类等式分别为：

$$|S_4|=1+3+6+6+8,\quad |A_4|=1+3+4+4.$$

2．群的类等式有很多应用，教材中本节定理 3(cauchy 定理)的证明就是一个例子．下面再举一例，

例 2　证明：交代群 A_4 没有 6 阶子群．

证　反证法．设 A_4 有 6 阶于群 H，则 $(A_4:H)=2$．从而 H 是 A_4 的正规子群．但是，

H 是 A_4 的正规子群 $\Leftrightarrow$ H 是 A_4 的若干个共轭类的并(一般也成立，读者自证)而 A_4 的类等式为

$$|A_4|=1+3+4+4,$$

由于 4 个数 1，3，4，4 中任几个的和也不会是 6，矛盾．因此 A_4 无 6 阶子群．

3．若 $H\leqslant G$，则必 $H\subseteq N(H)$（实际是 $H\trianglelefteq N(H)$）．但是，对群 G 的子集 S 却不一定有 $S\subseteq N(S)$．

例 3 子集 $S=\{(12),(13)\}\subset S_3$．但易知

$$N(S)=\{(1),(23)\}.\quad \text{故 } S\not\subseteq N(S).$$

此外还有 $S\not\subseteq C(S)=\{(1)\}$．即使 S 是子群也不一定有 $S\subseteq C(S)$．

例如，$H=\{(1),(123),(132)\}\leqslant S_3$，但易知 $C(H)=\{(1)\}$，故

$$H\not\subseteq C(H).$$

另外应注意，教材定理 6 指出：$C(H)\trianglelefteq N(H)$，其中 H 是子群．其实对群的任何非空子集 S 均有 $C(S)\trianglelefteq N(S)$．因为定理 6 的证明并未用到 H 是子群的条件．这一点教材也明确指出来了．之所以定理 6 假设 H 是子群，是因为今后遇到最多的是这种情况．

4．对任二共轭的有限于群来说，由于二者包含的元素个数相等，当然不可能其中一个是另一个的真子群．但对无限子群来说，这种情况却可能发生．

例 4 令 $G=S(\mathbf{Z})$，即整数集 $\mathbf{Z}$ 上的对称群．再令

$$M=\{(12),(23),\cdots,(n,n+1),\cdots\}\subset S(\mathbf{Z}),\quad H=(M).$$

现在取 G 中元素

$$a=(\cdots,-k,\cdots,-2,-1,0,1,2,\cdots,k,\cdots),$$

则易知：$a(n,n+1)a^{-1}=(n+1,n+2)$（其中 n 为正整数）．从而

$$aHa^{-1}\subseteq H.$$

但是，$(12)\notin aHa^{-1}$，故 $aHa^{-1}\subset H$．即 H 的共轭子群 aHa^{-1} 是 H 的真子群．

三、习题§3．6　解答

1．略　　2．略

3．

证 1) 任取 $x\in C_1C_2$，则令

$$x=x_1x_2,\quad \text{其中 } x_1\in C_1, x_2\in C_2.$$

若群 G 中元素 y 与 x 共轭，且设

$$x=aya^{-1},\quad \text{其中 } a\in G.$$

因为 C_1, C_2 都是 G 的共轭元素类，故

$$a^{-1}x_1a\in C_1,\quad a^{-1}x_2a\in C_2.$$

于是有

$$y=a^{-1}xa=a^{-1}(x_1x_2)a=a^{-1}x_1a\cdot a^{-1}x_2a\in C_1C_2.$$

即凡与 C_1C_2 中元素共轭的元素必属于 C_1C_2. 因此，C_1C_2 是 G 中一些共轭元素类的并集.

注 应留意，但不能证明 C_1C_2 中任二元素必共轭.

2) 任取 $x, y\in C_1^m$，并令

$$x=x_1^m,\quad y=y_1^m,\quad \text{其中 } x_1, y_1\in C_1.$$

由于 C_1 是 G 的一个共轭元素类，故有 $b\in G$ 使 $x_1=by_1b^{-1}$. 从而有

$$x_1^m=(by_1b^{-1})^m=by_1^mb^{-1}.$$

即 $x=byb^{-1}$. 亦即 C_1^m 中任二元素必共轭.

其次，设 $x\in C_1^m$，$x=x_1^m$（$x_1\in C_1$）且 x 与 y 共轭，令 $x=CyC^{-1}(C\in G)$. 则因 C_1 是共轭元素类，故

$$y=C^{-1}xC=C^{-1}x_1^mC=(C^{-1}x_1C)^m\in C_1^m.$$

即凡与 C_1^m 中元素共轭的元素都属于 C_1^m.

因此，C_1^m 是群 G 的一个共轭元素类.

特别，当 $m=-1$ 时即得 C_1^{-1} 是 G 的一个共轭元素类.

4.

证 显然 $\langle a\rangle\subseteq N(a)$. 又对任意 $x\in N(a)$ 有

$$xa^mx^{-1}=a^m\in\langle a\rangle,\quad \text{故 } \langle a\rangle\trianglelefteqslant N(a).$$

又显然 $N(a)\subseteq N(\langle a\rangle)$，故 $N(a)\leqslant N(\langle a\rangle)$. 因此

$$\langle a\rangle\trianglelefteqslant N(a)\leqslant N(\langle a\rangle).$$

5.

证 任取 S_n 中的一个对换 (ij)，而 $\pi(ij)\pi^{-1}$ 为与 (ij) 共轭的任意一个置换，其中 π 是一个 n 次置换，则由第二章 §6 定理 5 知，

$$\pi(ij)\pi^{-1}=(\pi(i)\pi(j))$$

也是 S_n 的一个对换.

反之，设 (ij) 与 (st) 为 S_n 的任两个对换，则任取 S_n 中一个置换 π 使 $\pi(i)=s, \pi(j)=t$（显然这样的置换是存在的），则

$$\pi(ij)\pi^{-1}=(\pi(i)\pi(j))=(st),$$

即 (ij) 与 (st) 共轭. 因此，S_n 的全体对换作成一个共轭类.

注 由于 S_n 中对换的个数显然就是 n 个元素中每取两个的组合数（因为 $(ij)=(ji)$），故由此可知 S_n 共有

$$C_n^2=\frac{n(n-1)}{2}$$

个对换.

6.

证　因 G 是有限群，故可设 $(G:N(H))=k$，且由推论 2 知

$$x_1Hx_1^{-1},\quad x_2Hx_2^{-1},\quad \cdots,\quad x_kHx_k^{-1}$$

是与 H 共轭的全部子群，从而 $\bigcup\limits_{x\in G}xHx^{-1}=\bigcup\limits_{1}^{k}x_iHx_i^{-1}$.

设若 $G=\bigcup\limits_{x\in G}xHx^{-1}$，则由于 $H<G$，故 $k>1$ 且由于

$$H\leqslant N(H),$$

从而有

$$\begin{aligned}|G|&=\left|\bigcup_{x\in G}xHx^{-1}\right|=\left|\bigcup_{1}^{k}x_iHx_i^{-1}\right|\\&<k|H|\leqslant(G:N(H))\cdot|N(H)|=|G|,\end{aligned}$$

矛盾. 因此，$\bigcup\limits_{x\in G}xHx^{-1}\subset G$，即二者不能相等.

§3.7　群的直积

一、主要内容

1. 群的外直积和内直积的定义与关系.

2. 群 G 是 n 个子群 $G_1,G_2,\cdots,G_n$ 的内直积的充要条件；n 阶循环群是 s 个阶为 $p_i^{k_i}$ 的循环群的直积，其中

$$n=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s},\quad p_1,\cdots,p_s\text{ 为互异素数.}$$

3. 可分解群与不可分解群的定义和例子.

1) n 次对称群、有理数加群和无限循环群都是不可分解群.

2) n 阶循环群是不可分解群 $\Longleftrightarrow$ n 为素数的方幂.

二、释疑解难

1. 群的内直积在不同的书中常有不同的表述形式. 常见的大体上有以下四种形式,分别称其为定义 1,2,3,4.

定义 1 称群 G 为其子群 $G_1,G_2,\cdots,G_n$ 的(内)直积,若

1) $G_i \trianglelefteqslant G$, $i=1,2,\cdots,n$;

2) $G=G_1G_2\cdots G_n$;

3) $G_1G_2\cdots G_{i-1}\cap G_i=e$[①], $i=2,3,\cdots,n$.

定义 2 称群 G 为其子群 $G_1,G_2,\cdots,G_n$ 的(内)直积,若

1) $G=G_1G_2\cdots G_n$;

2) G 中每个元素表为 $G_1,G_2,\cdots,G_n$ 中元素之积是惟一的;

3) G_i 中元素与 $G_j(i\neq j)$ 中元素可换.

定义 3 称群 G 为其子群 $G_1,G_2,\cdots,G_n$ 的(内)直积,若

1) $G_i \trianglelefteqslant G$, $i=1,2,\cdots,n$;

2) $G=G_1G_2\cdots G_n$;

3) G 中每个元素表为 $G_1,G_2,\cdots,G_n$ 中元素之积是惟一的.

定义 4 称群 G 为其子群 $G_1,G_2,\cdots,G_n$ 的(内)直积,若

1) $G=G_1G_2\cdots G_n$;

2) $G_1G_2\cdots G_{i-1}G_{i+1}\cdots G_n\cap G_i=e$, $i=2,3,\cdots,n$;

3) G_i 中元素与 G_j 中元素可换$(i\neq j)$.

当然,以上四种定义是等价的. 教材采用定义 1,而把定义 2 作为等价的定理,即定理 3.

应注意,定义 1 中的条件 2)、3)或定义 2 中的条件 1)、2)或定义 3 中的条件 2)、3)或定义 4 中的条件 1)、2),均可合并为一个条

---

① 与教材保持一致,一个是只由单位元 e 作成的子群$\{e\}$,简记为 e.

件如下：

4) G 中每个元素都可惟一地表为 $G_1, G_2, \cdots, G_n$ 中元素之积.

另外，定义 1 中的条件 3)与定义 4 中的条件 2)也可互相代替.

证明如下：

任取 $x \in G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_n \cap G_i$，则

$$x \in G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_n, \quad x \in G_i.$$

令 $x = x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n (x_j \in G_j)$. 由于教材已证明定义 1 与定义 2 等价，故得

$$e = x_1 x_2 \cdots x_{i-1} x^{-1} x_{i+1} \cdots x_n.$$

由于元素表示法惟一，故 $x^{-1} = e, x = e$. 即定义 4 的条件 2)成立.

反之，由定义 4 也可推出定义 1 中的条件 3).

2. 群直积的重要意义.

1) 利用直积，可以由已知的群构造出一些新的群.

2) 反过来，如果一个群 G 可以分解成一些(正规)子群的直积，那么群 G 的结构决定于每个直积因子的结构. 只要每个直积因子研究清楚了，那么群 G 也就清楚了. 例如，教材本章 § 9 指出，有限交换群就是一类研究清楚了的群类，因为有限交换群基本定理指出：每个阶大于 1 的有限交换群都可惟一地分解为素幂阶循环群的直积. 而素幂阶循环群是完全清楚的一类群.

3) 再举一个简单例子说明这个问题.

例 1 设 G 是一个阶大于 1 的有限群，且每个元素都满足方程 $x^2 = e$. 则

$$G \cong C_2 \times C_2 \times \cdots \times C_2.$$

其中 C_2 为 2 阶循环群.

证 由习题 2.1 第 6 题知，G 是一个交换群且其中除 e 外每个元素的阶均为 2. 因此，G 中每个元素 $a = a^{-1}$.

现在假设 $a_1, a_2, \cdots, a_n$ 为 G 的一个元素个数最少的生成系. 于是 G 中每个元素都可表示成

$$a_1^{s_1}a_2^{s_2}\cdots a_n^{s_n}\quad(s_i=0\text{ 或 }1).$$

而且这种表示法是惟一的.因若

$$a_1^{s_1}a_2^{s_2}\cdots a_n^{s_n}=a_1^{t_1}a_2^{t_2}\cdots a_n^{t_n}\quad(t_i=0\text{ 或 }1),$$

不妨假设 $s_1\neq t_1$,则 $a_1^{s_1-t_1}=a_2^{t_2-s_2}a_3^{t_3-s_3}\cdots a_n^{t_n-s_n}$.从而可知 a_2, $a_3,\cdots,a_n$ 也是 G 的一个生成系.这与 $a_1,a_2,\cdots,a_n$ 是元素个数最少的生成系矛盾.

又由于 $|G|>1$,故 $a_1,a_2,\cdots,a_n$ 中不能有 e.即每个 a_i 都是 2 阶元.从而 $\langle a_i\rangle\cong C_2$.因此

$$G=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_n\rangle\cong C_2\times C_2\times\cdots\times C_2.$$

由此顺便得出这种群的阶 $|G|=2^n$.

这就是说,研究这种群可转化为研究 2 阶循环群.因此这种群完全在我们的掌握之中.

3. 定理 5 说明,完全可分解群的任何正规子群都是其直积因子.但这一结论对非完全可分解群不再成立.

例 2 三次对称群 S_3 是不可分解群,当然就不是完全可分解群.S_3 的非平凡正规子群只有

$$N=\{(1),(123),(132)\},$$

它当然不是群 S_3 的直积因子.

例 3 设 $G=\langle a\rangle$ 为 12 阶循环群.它是交换群,从而每个子群都是正规子群.但是,其非平凡子群共有 4 个:

$$H_2=\{e,a^6\},\qquad H_3=\{e,a^4,a^8\},$$
$$H_4=\{e,a^3,a^6,a^9\},\qquad H_6=\{e,a^2,a^4,a^6,a^8,a^{10}\}.$$

$H_2\trianglelefteqslant G$,但是 H_2 显然不是 G 的直积因子,因为

$$H_2\cap H_6=H_2\neq e.$$

4. 一个群不是可分解群就必然是不可分解群.另外,不要误认为不可分解群就一定简单,而可分解群就一定复杂.例如,n 次对称群、有理数加群和无限循环群等都是不可分解群,但它们并不比可分解群例如 C_6,C_{10},C_{15}(6,10,15 阶循环群)简单.

5. 直积的概念也可以推广到任意个群上去.

设 Ω 为任一指标集(有限或无限、可数或不可数),G_i(对每个 $i\in\Omega$) 为群. 则加氏积

$$G=\{(\cdots,a_i,\cdots)\mid i\in\Omega\}$$

对运算

$$(\cdots,a_i,\cdots)(\cdots,b_i,\cdots)=(\cdots,a_ib_i,\cdots)$$

作成一个群,称为一切群 $G_i(i\in\Omega)$的(外)直积. 记为

$$G=\prod_{i\in\Omega}G_i.$$

当 Ω 有限时,就得到教材中所说的直积.

6. 当 $G_1,G_2,\cdots,G_n$ 为交换群且代数运算用加号表示(即每个 G_i 都是加群)时,这时的"直积"称为"直和",并用符号

$$G_1\oplus G_2\oplus\cdots\oplus G_n$$

表示.

三、习题 3.7 解答

1. 设群 $G=G_1\times G_2\times\cdots\times G_n$. 证明:当 $i\neq j$ 时,

$$G_i\cap G_j=e.$$

证 因为 $i\neq j$,不妨设 $i<j$. 则由 $G=G_1\times G_2\times\cdots\times G_n$ 得

$$G_i\cap G_j\subseteq G_1G_2\cdots G_i\cdots G_{j-1}\cap G_j=e.$$

故 $G_i\cap G_j=e$.

2. 证明:定理 3 中的"每个元素表示法惟一"可改为"单位元表示法惟一".

证 若每个元素表示法惟一,则当然单位元表示法惟一. 反之,若单位元表示法惟一,任取 $a\in G$,令

$$a=a_1a_2\cdots a_n=b_1b_2\cdots b_n\quad(a_i,b_i\in G_i).$$

则 $e=a_1b_1^{-1}\cdot a_2b_2^{-1}\cdot\cdots\cdot a_nb_n^{-1}$,其中 $a_ib_i^{-1}\in G_i$. 但因 e 表示法惟一,故

$$a_ib_i^{-1}=e,\quad a_i=b_i\quad(i=1,2,\cdots,n).$$

即 G 中任何元素都表示法惟一.

3. 设群 $G=G_1\times G_2$，$G=G_1'\times G_2$. 证明：$G_1\cong G_1'$.

证 因为 $G=G_1\times G_2=G_1'\times G_2$，故由后面第 6 题知：

$$G_1\cong G/G_2,\quad G/G_2\cong G_1'.$$

从而 $G_1\cong G_1'$.

4. 设群 $G=G_1\times G_2\times\cdots\times G_n$. 证明：

$$\varphi_i:\ a_1a_2\cdots a_n\longrightarrow a_i\quad (a_i\in G_i)$$

是群 G 到 G_i 的满同态.

证 因为是直积，群中每个元素表示法惟一，故显然 φ_i 是群 G 到群 $G_i(i=1,2,\cdots,n)$的满射.

又因为是直积，G_i 与 $G_j(i\neq j)$中元素相乘可以交换，从而

$$\begin{aligned}&\varphi_i(a_1a_2\cdots a_i\cdots a_n\cdot b_1b_2\cdots b_i\cdots b_n)\\&=\varphi_i(a_1b_1\cdot a_2b_2\cdot\cdots\cdot a_ib_i\cdot\cdots\cdot a_nb_n)=a_ib_i\\&=\varphi_i(a_1a_2\cdots a_n)\cdot\varphi_i(b_1b_2\cdots b_n)\quad (a_i,b_i\in G_i).\end{aligned}$$

故 $G\sim G_i$.

5. 设 G_1，G_2 是两个群. 证明：$G_1\times G_2\cong G_2\times G_1$.

证 由于是直积，元素表示法惟一，故易知

$$\varphi:\ a_1a_2\longrightarrow a_2a_1\quad (a_i\in G_i)$$

是 $G_1\times G_2$ 到 $G_2\times G_1$ 的同构映射，因此，$G_1\times G_2\cong G_2\times G_1$.

6. 设群 G 是其子群 G_1 与 G_2 的直积，即

$$G=G_1\times G_2.$$

证明：$G/G_1\cong G_2$，$G/G_2\cong G_1$.

证 因为 $G=G_1\times G_2$，故

$$G/G_1=\{aG_1\mid a\in G_2\}.$$

现定义：$\varphi:\ G/G_1\longrightarrow G_2$，$aG_1\longrightarrow a$.

由 $G_1\cap G_2=\{e\}$知，对 aG_1，$bG_1\in G/G_1(a,b\in G_2)$有

$$\begin{aligned}&aG_1=bG_1\Longleftrightarrow a^{-1}b\in G_1\Longleftrightarrow a^{-1}b\in G_1\cap G_2\\&\Longleftrightarrow a^{-1}b=e\Longleftrightarrow a=b.\end{aligned}$$

又因为

$$\varphi(aG_1\cdot bG_1)=\varphi(abG_1)=ab=\varphi(aG_1)\varphi(bG_1),$$

故 φ 为同构映射，因此 $G/G_1\cong G_2$.

同理可证，$G/G_2\cong G_1$.

注 本题也可利用同构定理证明，即

$$G/G_1=G_1G_2/G_1\cong G_2/G_1\cap G_2=G_2/\{e\}\cong G_2.$$

7. 设群 $G=G_1\times G_2$，且 $N\trianglelefteqslant G_1$. 证明：$N\trianglelefteqslant G$.

证 任取 $x\in G$，则由 $G=G_1\times G_2$ 知，存在 $x_1\in G_1$，$x_2\in G_2$，使 $x=x_1x_2=x_2x_1$，且由于 $N\trianglelefteqslant G_1$，故有

$$x_2N=Nx_2.$$

再由 $N\trianglelefteqslant G_1$ 知，$x_1N=Nx_1$，故

$$xN=(x_1x_2)N=x_1Nx_2=N(x_1x_2)=Nx,$$

即 $N\trianglelefteqslant G$.

8. 设 $G_1,G_2,\cdots,G_n$ 是群 G 的正规子群且 $G=G_1G_2\cdots G_n$. 证明：

$$G_1G_2\cdots G_{i-1}\cap G_i=e\Longleftrightarrow G\text{ 中每个元素表示法惟一}.$$

证 设 $G_1G_2\cdots G_{i-1}\cap G_i=e$，$i=2,3,\cdots,n$，又 $a\in G$ 且

$$a=a_1a_2\cdots a_n=b_1b_2\cdots b_n\quad(a_j,b_j\in G_j).\qquad(1)$$

如果 a 的表示法不惟一，设 $a_i\neq b_i$，$a_{i+1}=b_{i+1}$，$\cdots$，$a_n=b_n$. 但由于 $G_j\trianglelefteqslant G$，故 $G_1G_2\cdots G_{i-1}\trianglelefteqslant G$，从而由(1)可得

$$(b_1\cdots b_{i-1})^{-1}(a_1\cdots a_{i-1})=b_ia_i^{-1}\in G_1\cdots G_{i-1}\cap G_i=e.$$

从而 $b_ia_i^{-1}=e$，$a_i=b_i$，矛盾.

反之，设 G 中每个元素表示法惟一，令

$$x_i=x_1x_2\cdots x_{i-1}\in(G_1G_2\cdots G_{i-1}\cap G_i),$$

其中 $x_j\in G_j$. 则得 $e=x_1x_2\cdots x_{i-1}x_i^{-1}$. 从而

$$x_1=x_2=\cdots=x_{i-1}=x_i^{-1}=e,\quad x_i=e.$$

即 $G_1G_2\cdots G_{i-1}\cap G_i=e$. 得证.

注 这里每个 G_i 都必须是正规子群. 否则，例如三次对称群 S_3 的子群

$$G_1=\{(1),(12)\},G_2=\{(1),(13)\},\ G_3=\{(1),(23)\},$$

有 $S_3=G_1G_2G_3$ 且

$$G_1\cap G_2=G_1G_2\cap G_3=e,$$

但 S_3 中元素表示方法不惟一.

§3.8 Sylow定理

一、主要内容

1. Sylow p-子群和重陪集定义，以及一个群关于两个子群的重陪集分解的概念.

2. 三个 Sylow 定理. 设 $|G|=p^s m$ (p 是素数，$p\nmid m$)

1) 第一 Sylow 定理(存在性和包含性). 对群 G 的每个 $p^i(i=0,1,\cdots,s-1)$阶子群 H，总有 G 的 p^{i+1} 阶子群 K 存在使 $H\lhd K$. 从而 G 有 Sylow p -子群.

2) 第二 Sylow 定理(共轭性). 群 G 的所有 Sylow p-子群恰好是 G 的一个共轭子群类.

3) 第三 Sylow 定理(计数定理). 若群 G 的 Sylow p-子群共有 k 个，则

$$k\,\Big|\,|G|,\quad 且\quad p|k-1.$$

3. p-群定义和有限群是 p-群的充要条件.

二、释疑解难

1. 三个 Sylow 定理对于 Sylow p-子群的讨论相当详尽和完美. 从其存在性、相互关系以及计数都给予了完满而彻底的回答. 在群论中，对一个问题的研究能得到如此圆满解决虽然也有一些，但为数并不太多. 特别是，由 Sylow 定理还可以推演出关于群的一些重要结论. 就本教材来说，至少有以下四点：

1) pq (p,q 是互异素数) 阶群当 $p\nmid q-1$ 且 $q\nmid p-1$ 时，必为循环群.

由此可知，凡阶为 15,33,35,51,65,69,…的群都是循环群.

此前我们曾经证明了：pq 阶交换群必为循环群；又当 $p<q$ 时，pq 阶群 G 有惟一的 q 阶正规子群，从而不是单群. 但对其 p 阶子群的状况由第三 Sylow 定理可知：若其 p 阶子群(它就是 G 的 Sylow p-子群)的个数为 k，则

$$k\,\Big|\,|G|=pq,\quad 且\quad p|k-1.$$

由此易推知，只有 $k=1$ 或 q. 当 $k=1$ 时，其 p 阶子群就是 G 的一个正规子群. 也就是说，此时 G 要么有一个 p 阶正规子群，要么有 q 个 p 阶子群. 例如，$6=2\cdot 3$ 阶交换群(当然是循环群)有一个 2 阶(正规)子群，而 6 阶非交换群 S_3 有 3 个 2 阶子群，等等.

2) 利用 Sylow 定理还可以确定一些群是不是单群. 例如，196 阶群、200 阶群都不是单群 (参考本节习题第 7 题及教材例 4)；又 np (p 是素数且 $n<p$) 阶群不是单群 (参考习题第 2 题)，从而可知凡 6,10,14,15,20,21,28,…阶群都不是单群.

3）任何有限交换群都是其所有 Sylow 子群的直积. 这使我们讨论有限交换群可以转化为讨论素幂阶交换群(或循环群).

4）利用 Sylow 定理证明了：对有限交换群来说，Lagrange 定理的逆定理成立. 这当然是一个很重要的结论.

2. 第二 Sylow 定理是说，有限群 G 的所有 Sylow p -子群恰好是一个共轭子群类. 由于共轭子群必同构；又若一个子群与一个 Sylow p -子群同构，它必然也是一个 Sylow p -子群，因此，G 的所有 Sylow p -子群不仅是一个共轭子群类，而且也是一个同构子群类.

3. p -群有很多重要性质. 例如：

1）有限群 G 是 p -群 $\Longleftrightarrow$ $|G|$ 是 p 的方幂.

2）阶大于 1 的有限 p -群的中心 $\supset\{e\}$.

3）p^2 阶群必为交换群.

4）如果有限 p -群 G 只有一个指数为 p 的子群，则 G 必为循环群.

5）p^n 阶群对每个 $i=1,2,\cdots,n-1$，都至少有一个 p^i 阶的正规子群.

三、习题 3.8 解答

1. 试求出四次交代群 A_4 的所有 Sylow 子群.

解 因为 $|A_4|=2^2\cdot 3$，故 A_4 有 Sylow 2 -子群(阶为 4)和 Sylow 3 -子群(阶为 3).

又因为 Klein 四元群

$$K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$$

显然是 A_4 的一个 Sylow 2 -子群，而 $K_4\trianglelefteq S_4$，从而 $K_4\trianglelefteq A_4$，故 K_4 是 A_4 的惟一的 Sylow 2 -子群.

由 A_4 的一切 3 -循环(阶为 3)生成的子群，显然是 A_4 的全部 Sylow 3 -子群，共有 4 个，它们是：

$$\langle(123)\rangle,\quad \langle(124)\rangle,\quad \langle(134)\rangle,\quad \langle(234)\rangle.$$

2. 设 G 是 np 阶群 (p 是素数). 证明：若 $n<p$，则 G 有 p 阶正规子群.

证 因为 $n<p$，故 G 的 Sylow p -子群是 p 阶循环群 C_p. 设这样的子群共有 k_p 个，则由 Sylow 定理知：

$$k_p=ps+1,\quad k_p\mid np,\quad \text{即}(ps+1)\mid np.$$

但因 $(ps+1,p)=1$，故 $(ps+1)\mid n$. 又因 $n<p$，故必 $s=0$，$k_p=1$. 因此对 G 中任何元素 a 都有 $aC_pa^{-1}=C_p$，从而 C_p 是 G 的 p 阶正规子群.

3. 设 G 是一个有限群，P 是 G 的一个 Sylow p -子群，H 是 G 的一个 p 子群. 证明：若 $H\subseteq N(P)$，则 $H\subseteq P$.

证 因为 $H\subseteq N(P)$，故对任意 $a\in H$，都有 $aP=Pa$. 从而 $HP=PH$，因此

$$HP\leqslant G\quad \text{且}\quad a^{-1}Pa=P.$$

现任意取 $ab\in HP(b\in P)$，由 $a^{-1}ba\in P$ 知，

$$(ab)^2=abab=a^2(a^{-1}ba)b=a^2b_1b=a^2b_2,$$

其中 $b_1=a^{-1}ba, b_2=b_1b\in P$. 再对 m 用归纳法易知

$$(ab)^m=a^mb_m \quad (b_m\in P). \tag{1}$$

又因 H 为 p -子群，故 a 的阶为 p 的方幂 p^r，从而由(1)知：

$$(ab)^{p^r}=a^{p^r}b_0=eb_0=b_0\in P.$$

同样，由 P 为 p -子群知 b_0 的阶为 p 的方幂，从而知 ab 的阶为 p 的方幂，即 HP 为 p 子群. 但子群 $HP\supseteq P$，而 P 是 G 的 Sylow p -子群，所以必有 $HP=P$，于是 $H\subseteq P$.

4. 设 K 是群 G 的一个有限正规子群，P 是 K 的一个 Sylow p -子群. 证明：$G=N(P)K$.

证 任取 $x\in G$，则由于 $P\leqslant K\lhd G$，故

$$xPx^{-1}\leqslant xKx^{-1}=K \quad (\forall x\in G).$$

但 P 是有限群 K 的一个 Sylow p -子群，故 xPx^{-1} 也是 K 的一个 Sylow p -子群. 于是，由 Sylow 定理知，P 与 xPx^{-1} 在 K 中共轭. 即有 $k\in K$ 使

$$xPx^{-1}=kPk^{-1}, \quad (k^{-1}x)P=P(k^{-1}x),$$

于是 $k^{-1}x\in N(P)$，从而

$$x\in K\cdot N(P),\ G\subseteq K\cdot N(P),\ G=K\cdot N(P).$$

又由于 $K\lhd G$ 及 $K\cdot N(P)=N(P)K$，因此

$$G=N(P)K.$$

5. 设 P 是有限群 G 的一个 Sylow p -子群. 证明：若 G 有子群 H 包含 $N(P)$，则 $N(H)=H$.

证 因为 H 是子群，故 $H\subseteq N(H)$. 下证 $N(H)\subseteq H$.

任取 $a\in N(H)$，则 $aH=Ha$ 或 $aHa^{-1}=H$. 但是

$$P\lhd N(P)\subseteq H,$$

故

$$aPa^{-1}\subseteq aHa^{-1}=H.$$

从而 P 与 aPa^{-1} 也是 H 的 Sylow p -子群，因而由 Sylow 定理知，P 与 aPa^{-1} 在 H 中共轭，即存在 $h\in H$ 使

$$h(aPa^{-1})h^{-1}=P \text{ 或 } (ha)P(ha)^{-1}=P,$$

$$P(ha)=(ha)P.$$

因此，$ha\in N(P)$. 但是 $N(P)\subseteq H, h\in H$，从而 $a\in H, N(H)\subseteq H$. 故

$$N(H)=H.$$

6. 证明：有限群 G 必有一个最大的正规 p -子群 H. 即 H 是 G 的正规 p -子群，又若 K 也是 G 的正规 p -子群，则必 $K\subseteq H$.

证 若 G 无阶数大于 1 的正规 p -子群，则显然 G 的单位元群就是 G 的最大正规 p -子群.

若 G 有阶数大于 1 的正规 p -子群，则 G 的一切正规子群之积仍为正规子群，且由下面第 8 题知，也是一个 p -子群. 因此，它是 G 的最大正规 p -子群.

7. 证明：196 阶群 G 必有一个阶大于 1 的 Sylow 子群，它是 G 的一个正规子群.

证 由于 $|G|=196=2^2\cdot 7^2$，令 P 是 G 的一个 Sylow 7 -子群，与其共轭的子群个数 $k=7q+1$ 应是 196 的因数. 但 $196=2^2\cdot 7^2$ 的正因数只有 1，2，4，7，14，28，49，98，196，这只有 $q=0$，即 $k=1$. 因此 P 是 G 的惟一的 Sylow p -子群. 从而 P 是 G 的一个阶大于 1 的 Sylow 子群且是 G 的正规子群.

于是 a 的阶是 p 的方幂，即 HK 为 p -子群.

证法Ⅱ 由于 $H\leqslant G, K\lhd G$，故 $HK\leqslant G$. 再任取 $hk\in K$，其中 $h\in H, k\in K$. 由于 $K\lhd G$，故对 G 中任意元素 x 都有

$$Kx=xK. \tag{1}$$

因 H 是 p -子群，设 $|h|=p^t$，例如 $|h|=3$ 时，由(1)有

$$(hk)^3=h(kh)(kh)k=h\cdot hk_1\cdot kh\cdot k=h^2(k_1k)h\cdot k$$
$$=h^2\cdot hk_2\cdot k=h^3\cdot k_3=k_3,$$

其中 $k_1, k_2\in K$ 且 $k_3=k_2k\in K$. 因此一般地有

$$(hk)^{p^t}=h^{p^t}k'=k'\in K.$$

但 K 也是 p -子群，设 $|k'|=p^t$，于是有

$$(hk)^{p^{s+t}}=(k')^{p^t}=e.$$

即 hk 的阶是 p 的方幂. 因此，HK 也是 G 的 p -子群.

§3.9 有限交换群

一、主要内容

1. 有限交换群基本定理：任何阶大于 1 的有限交换群 G，都可以惟一分解为素幂阶循环群的直积.

这些循环群的阶的全体，称为群 G 的初等因子组.

2. 有限交换群的不变因子定理：任何阶大于 1 的有限交换群 G，都可以惟一地分解为

$$G=\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_m\rangle,$$

其中 $|b_i|>1(i=1,2,\cdots,m)$ 且 $|b_i|\,\big|\,|b_{i+1}|(i=1,2,\cdots,m-1)$.

这些循环群的阶的全体，即 $\{|b_1|,|b_2|,\cdots,|b_m|\}$ 称为群 G 的不变因子组.

3. 阶大于 1 的二有限交换群 G_1 与 G_2 同构的充要条件：

$$G_1\cong G_2\Longleftrightarrow \text{二者有相同的初等因子组}$$

$$\Longleftrightarrow \text{二者有相同的不变因子组.}$$

二、释疑解难

1. 有限交换群基本定理的逆定理显然成立. 因此，该定理与其逆定理合起来可表述为：

群 G 可分解为素幂阶循环群的直积 $\Longleftrightarrow$ G 为有限交换群.

2. 交换群的基.

定义 设 $a_1, a_2, \cdots, a_m$ 是交换群 G 的一组元素. 如果由

$$a_1^{k_1}a_2^{k_2}\cdots a_m^{k_m}=e$$

必有

$$a_1^{k_1}=a_2^{k_2}=\cdots=a_m^{k_m}=e,$$

则称元素 $a_1, a_2, \cdots, a_m$ 是无关的. G 的一组无关的生成元称为 G 的一基.

交换群中元素无关很类似于域上线性空间中一组向量线性无关；交换群的基又类似于线性空间的基. 特别是，当交换群的代数运算改用加号时，这种类似程度就更加接近. 所不同的只是，普通所说的线性空间都是数域或域上的线性空间，而交换群则是整数环(系数是整数)上的“线性空间”，或者更正确地说，是整数环上的“模”.

教材定理 1 中的 $\{a_1, a_2, \cdots, a_n\}$ 以及定理 3 中的 $\{b_1, b_2, \cdots, b_m\}$ 都是各该交换群 G 的基.

3. 有限生成的交换群.

具有有限个生成元的交换群(不一定是有限群,例如无限循环群),称为有限生成的交换群. 有限交换群是一种特殊的有限生成交换群. 有限生成交换群有以下重要的结构定理:

有限生成交换群的基本定理:每一个有限生成的交换群 G 都可以惟一地分解为以下循环群的直积:

$$G=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_n\rangle\times\langle b_1\rangle\times\langle b_2\rangle\times\cdots\times\langle b_m\rangle,$$

其中 $n\geqslant 0,|a_i|=\infty;m\geqslant 0,|b_j|$ 均有限且 $|b_j|\mid|b_{j+1}|$ $(j=1,2,\cdots,m-1)$.

显然 $\{a_1,a_2,\cdots,a_n,b_1,b_2,\cdots,b_m\}$ 为群 G 的一基.

又当 $n=0$ 时,以上定理就变成教材中的定理 3(不变因子定理).

4. 为什么把教材定理 1(有限交换群基本定理)中的素数幂 $p_i^{\alpha_i}$ $(i=1,2,\cdots,n)$ 叫做初等因子,而把定理 3(不变因子定理)中的 $|b_j|$ $(j=1,2,\cdots,m)$ 叫做不变因子?

大概读者已经觉察到(甚至已经完全明白)关于有限交换群的初等因子、不变因子,同高等代数中 λ-矩阵的初等因子和不变因子是何等的类似. 在高等代数中,每个 $m\times n$ 的 λ-矩阵 $A(\lambda)$ 都可经过初等变换化为惟一的标准形,标准形的主对角线上全体非零多项式就是 $A(\lambda)$ 的不变因子. 次数大于零的不变因子的标准分解式中,全体不可约多项式的方幂就是 $A(\lambda)$ 的初等因子. 关于 λ-矩阵的初等因子和不变因子有以下基本而重要的事实:

1) 两个 $m\times n$ λ-矩阵等价的充要条件是,二者有相同的秩和初等因子.

2) 两个 $m\times n$ λ-矩阵等价的充要条件是,二者有相同的不变因子.

3) $A(\lambda)$ 的初等因子和不变因子都是惟一确定的. 由 $A(\lambda)$ 的秩和初等因子可以求不变因子,反之由不变因子(从理论上说)也可求初等因子.

λ-矩阵按等价分类,而有限交换群按同构分类. 二者相应的概念和联系,有以下对应关系:

λ-矩阵	有限交换群
标准形	不变因子分解式
不变因子	不变因子
初等因子	初等因子
等价	同构
等价的充要条件	同构的充要条件.

三、习题 3.9 解答

1. 证明：对任意素数 $p_1, p_2, \cdots, p_m$ 和任意正整数 $k_1, k_2, \cdots, k_m$，总存在有限交换群，其初等因子组为：

$$\{p_1^{k_1}, p_2^{k_2}, \cdots, p_m^{k_m}\}. \tag{1}$$

证 令 $t_i = p_i^{k_i}$ $(i=1,2,\cdots,m)$. 则显然群

$$G = C_{t_1} \times C_{t_2} \times \cdots \times C_{t_m}$$

即为初等因子组是(1)的有限交换群.

2. 设 p 是素数. 试给出同构意义下的所有 p^4 阶交换群.

解 因为 p^4 阶交换群的初等因子组共有五种，即

$$\{p^4\}, \{p, p^3\}, \{p^2, p^2\}, \{p, p, p^2\}, \{p, p, p, p\},$$

故互不同构的全部 p^4 阶交换群为：

$$C_{p^4}, \ C_p \times C_{p^3}, \ C_{p^2} \times C_{p^2}, \ C_p \times C_p \times C_{p^2}, \ C_p \times C_p \times C_p \times C_p.$$

3. 给出同构意义下的所有 108 阶交换群.

解 因为 $108 = 2^2 \cdot 3^3$，故 108 阶交换群的初等因子组共有六种，即

$$\{2^2, 3^3\}, \quad \{2^2, 3, 3^2\}, \quad \{2^2, 3, 3, 3\},$$
$$\{2, 2, 3^3\}, \quad \{2, 2, 3, 3^2\}, \quad \{2, 2, 3, 3, 3\}.$$

因此相应地，得互不同构的全部 108 阶交换群共有六个，即

$$C_4 \times C_{27}, \quad C_4 \times C_3 \times C_9, \quad C_4 \times C_3 \times C_3 \times C_3,$$
$$C_2 \times C_2 \times C_{27}, \quad C_2 \times C_2 \times C_3 \times C_9, \quad C_2 \times C_2 \times C_3 \times C_3 \times C_3.$$

4. 设 G 是阶大于 1 的有限交换群. 证明：若除 e 外其余元素的阶都相同，则 G 必为素幂阶群.

证 若有互异素数 p, q 使 $pq \mid |G|$，则由本章 § 2 定理 5(或本章 § 6 定理 3 以及 Sylow 定理)知，G 有 p 阶与 q 阶元素，这与题设矛盾. 因此，$|G|$ 必为素数 p 的方幂.

注 还可知这个相同的阶为 p. 因为任取 $e \neq a \in G$，且设 $|a| = p^s$. 则 $\left|a^{p^{s-1}}\right| = p$. 但由假设

$$|a| = \left|a^{p^{s-1}}\right|, \quad \text{即 } p^s = p, \quad \text{从而 } s = 1.$$

即 G 中任何非 e 元素的阶都是 p. 另外由证明可知，本题不需假设 G 交换.

5. 设 G 是有限交换群. 证明：G 是循环群的充要条件是，$|G|$ 是 G 中所有元素的阶的最小公倍.

证 设 G 为 n 阶循环群，则 G 当然有 n 阶元素，而 G 中别的元素的阶都是 n 的因数，因此，n 是 G 的所有元素的阶的最小公倍.

反之，设 n 是 n 阶交换群 G 中所有元素的阶的最小公倍，则由习题 2.7 第 12 题知，在 n 阶群 G 中有 n 阶元素. 从而可知 G 是循环群.

6. 用 C_k 表示 k 阶循环群. 证明：

$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}\cong C_{m_1m_2\cdots m_n}$$

当且仅当正整数 $m_1,m_2,\cdots,m_n$ 两两互素.

证 1) 对 n 用归纳法. 当 $n=1$ 时显然. 当 $n=2$ 时，只用证 $C_{m_1}\times C_{m_2}$ 中含有 m_1m_2 阶元素即可.

令 a 是 C_{m_1} 的一个生成元，b 是 C_{m_2} 的一个生成元，则

$$(a,b)\in C_{m_1}\times C_{m_2},$$

且
$$(a,b)^{m_1m_2}=(a^{m_1m_2},b^{m_1m_2})=(e_1,e_2).$$

其中 e_1 是 C_{m_1} 的单位元，e_2 是 C_{m_2} 的单位元.

又若 $(a,b)^s=(e_1,e_2)$，则 $(a^s,b^s)=(e_1,e_2)$，$a^s=e_1$，$b^s=e_2$，从而 $m_1\mid s$，$m_2\mid s$. 但是 $(m_1,m_2)=1$，故

$$m_1m_2\mid s.$$

因此 (a,b) 的阶是 m_1m_2. 而由于

$$|C_{m_1}\times C_{m_2}|=|C_{m_1}|\cdot|C_{m_2}|=m_1m_2,$$

故 $C_{m_1}\times C_{m_2}$ 是 m_1m_2 阶循环群. 由于凡同阶循环群都同构，故 $C_{m_1}\times C_{m_2}\cong C_{m_1m_2}$.

假设对 $n-1$ 成立，即有

$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_{n-1}}\cong C_{m_1m_2\cdots m_{n-1}}.$$

而 $C_{m_1}\times\cdots\times C_{m_{n-1}}\times C_{m_n}\cong(C_{m_1}\times\cdots\times C_{m_{n-1}})\times C_{m_n}$，故

$$C_{m_1}\times\cdots\times C_{m_{n-1}}\times C_{m_n}\cong C_{m_1m_2\cdots m_{n-1}}\times C_{m_n}.$$

又因 $m_1,m_2,\cdots,m_n$ 两两互素，故

$$(m_1m_2\cdots m_{n-1},m_n)=1.$$

再由上面所证 $n=2$ 的情形知，

$$C_{m_1m_2\cdots m_{n-1}}\times C_{m_n}\cong C_{m_1m_2\cdots m_{n-1}m_n}.$$

故
$$C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}\cong C_{m_1m_2\cdots m_n}.$$

2) 反之，设 $C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}$ 是循环群，则由于其阶为 $m_1m_2\cdots m_n$，故其必有阶为 $m_1m_2\cdots m_n$ 的元素（即其生成元的阶）.

如果 $m_1,m_2,\cdots,m_n$ 不两两互素，不妨设

$$(m_1,m_2)=d>1,\quad m_1=dm_1',\quad m_2=dm_2',$$

则 $dm_1'm_2'm_3\cdots m_n<m_1m_2m_3\cdots m_n$ 且对 $C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}$ 中任意元素 $(a_1,a_2,\cdots,a_n)$ 有

$$(a_1,a_2,\cdots,a_n)^{dm_1'm_2'm_3\cdots m_n}=(e_1,e_2,\cdots,e_n),$$

这与 $C_{m_1}\times C_{m_2}\times\cdots\times C_{m_n}$ 中有阶为 $m_1m_2\cdots m_n$ 的元素矛盾. 故 m_1，$m_2,\cdots,m_n$ 必两两互素.

7. 设 G 是群，$H\leqslant G$. 证明：如果关于 H 的任意两个左陪集的乘积仍是一个左陪集，则 $H\lhd G$.

证 任取 $a\in G$，则由于 H 的任两左陪集之积仍是一个左陪集，故可设

$$aH\cdot a^{-1}H=cH.$$

但由于 $H\leqslant G$，故 $e=ae\cdot a^{-1}e\in aH\cdot a^{-1}H$，即 $e\in cH$. 令

$$e=ch\quad(h\in H),$$

则 $c=h^{-1}\in H$，$cH=H$，即 $aH\cdot a^{-1}H=H$. 故对任意 $x\in H$，有

$$axa^{-1}=ax\cdot a^{-1}e\in aH\cdot a^{-1}H=H.$$

因此，$H\lhd G$.

8.

解 例如四元数群

$$G=\{1,i,j,k,-1,-i,-j,-k\},$$

其中心 $C=\{1,-1\}$. 然而易知商群为

$$G/C=\{C,iC,jC,kC\},$$

且 G/C 是一个交换群，因此，G/C 的中心即自身，其阶为 $4>1$.

9. 设 G 是群，$N\trianglelefteq G$，$|N|=m$，$(m,n)=1$. 证明：若 $|a|=n$，则 aN 在商群 G/N 中的阶也是 n；反之，若 aN 的阶是 n，则在 G 中有 n 阶元素 b 使

$$bN=aN.$$

证 因为 $|a|=n$，故

$$(aN)^n=a^nN=eN=N.$$

又设 $(aN)^r=N$，则 $a^rN=N$，$a^r\in N$. 但是 $|N|=m$，故

$$a^{rm}=e.$$

由 $|a|=n$ 知，$n|rm$. 但由题设 $(m,n)=1$，故 $n|r$，即在商群 G/N 中元素 aN 的阶也是 n.

反之，若 aN 的阶是 n，由于 $(m,n)=1$，故存在整数 s,t 使

$$ms+nt=1. \tag{1}$$

令

$$b=a^{ms}=a^{1-nt}=a\cdot a^{-nt}. \tag{2}$$

由于 aN 的阶是 n，故

$$(aN)^n=a^nN=N,\quad a^n\in N.$$

从而由(2)知

$$a^{-1}b=a^{-nt}=(a^n)^{-t}\in N,\quad bN=aN.$$

又因为 $|N|=m$，$a^n\in N$，故 $(a^n)^m=e$. 从而

$$b^n=(a^{ms})^n=e.$$

又若 $b^r=a^{msr}=e$，则

$$(aN)^{msr}=eN=N.$$

但 aN 的阶是 n，故 $n|msr$. 又由(1)知 $(n,ms)=1$，故 $n|r$. 从而 b 的阶是 n.

10.

证 1) 设 φ 是群 G 的任一自同态，于是对 G 中任二元素 a,b 有

$$\varphi(a\circ b)=\varphi(a^{-1}b^{-1}ab)=\varphi(a^{-1})\varphi(b^{-1})\varphi(a)\varphi(b)$$
$$=\varphi(a)^{-1}\varphi(b)^{-1}\varphi(a)\varphi(b)=\varphi(a)\circ\varphi(b).$$

任取 $x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}\in K$，即其中 $x_1,\cdots,x_k$ 都是 G 的换位元，而 $m_1,m_2,\cdots,m_k$ 为整数，则由上面知，$\varphi(x_1),\cdots,\varphi(x_k)$ 均仍为换位元，故

$$\varphi(x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k})=\varphi(x_1)^{m_1}\varphi(x_2)^{m_2}\cdots\varphi(x_k)^{m_k}\in K,$$

即 $\varphi(K)\subseteq K$. 因此，K 是 G 的一个全特征子群. 从而 K 是 G 的一个正规子群.

2) 任取 $a,b\in G$，则由于 $ab=ba(a\circ b)$，故

$$aK\cdot bK=(ab)K=(ba)(a\circ b)K=baK=bK\cdot aK,$$

即 G/K 是交换群.

3) 因为 G/N 是交换群，则对任意 $a,b\in G$，有

$$aN\cdot bN=bN\cdot aN,\quad (ab)N=(ba)N,$$

从而 $a\circ b=a^{-1}b^{-1}ab\in N$. 即 G 中任二元素的换位元都属于 N，因此 $K\subseteq N$.

注 一般称 K 为群 G 的换位子群或导群，并用 G' 表示. 另外由以上证明可知，G' 不仅是群 G 的正规子群，而且还是 G 的一个全特征子群.

11.

证 因为 $H\cap K\leqslant H$, $H\cap K\leqslant K$, 而 H 与 K 又都是有限子群, 故

$$|H\cap K|\,\big|\,|H|,\quad |H\cap K|\,\big|\,|K|,$$

从而 $|H\cap K|\,\big|\,(|H|,|K|)$. 但由题设 $(|H|,|K|)=1$, 故

$$|H\cap K|=1,\quad H\cap K=\{e\}.$$

任取 $a,b\in G$, 则由于商群 G/H 和 G/K 都是交换群, 故

$$abH=baH,\quad abK=baK.$$

即 $a^{-1}b^{-1}ab\in H$, $a^{-1}b^{-1}ab\in K$, 从而

$$a^{-1}b^{-1}ab\in H\cap K=\{e\},\ a^{-1}b^{-1}ab=e,\ ab=ba.$$

即 G 是交换群.

12. 设 k 是一个奇数. 证明: $2k$ 阶群 G 必有一个 k 阶子群.

证 由 Cayley 定理知, $2k$ 阶群 G 与 G 上的一个 $2k$ 阶 $2k$ 次置换群 $\overline{G}$ 同构.

由于 G 是偶数阶群, G 必含有 2 阶元, 令 a 是 G 的任意一个 2 阶元. 再任取 $x_1\in G$, 于是易知

$$x_1\neq ax_1.$$

再从 G 中取 $x_2\notin\{x_1,ax_1\}$, 则由于 $a^{-1}=a$, 故易知

$$ax_2\neq x_2,\ ax_2\neq x_1,\ ax_2\neq ax_1;$$

如此下去, 由于 $|G|=2k$, 故可得

$$G=\{x_1,x_2,\cdots,x_k,ax_1,ax_2,\cdots,ax_k\}.$$

又由于

$$a^2=e,\ a(ax_i)=a^2x_i=x_i\quad (i=1,2,\cdots,k),$$

故

$$\tau_a=\begin{pmatrix}x_1 & x_2 & \cdots & x_k & ax_1 & ax_2 & \cdots & ax_k\\ ax_1 & ax_2 & \cdots & ax_k & x_1 & x_2 & \cdots & x_k\end{pmatrix}$$

$$=(x_1,ax_1)(x_2,ax_2)\cdots(x_k,ax_k)\in\overline{G}.$$

但 k 是奇数, 于是 $\overline{G}$ 含有奇置换. 从而由第二章 §6 例 3 知, $\overline{G}$ 中奇偶置换各半. 又因 $|\overline{G}|=2k$, 故其 k 个偶置换作成 G 的一个子群, 即 $\overline{G}$ 有 k 阶子群, 从而 G 也有 k 阶子群.

13.

证 设 $|G|=p^m$. 将 G 分解为共轭元素类的并:

$$G=G_1\cup G_2\cup\cdots\cup G_r,\quad G_i\cap G_j=\varnothing(i\neq j).$$

其中 $G_1=\{e\}$. 由于每个 $|G_i|$ 都是 p^m 的因数，因此每个 $|G_i|$ 必是 1 或素数 p 的方幂. 但是

$$|G_1|+|G_2|+\cdots+|G_r|=|G|=p^m,$$

且 $|G_1|=1$，故至少还有一个 r 使 $|G_r|=1$. 于是 G_r 只含有一个元素 $a\neq e$，从而 $a\in C$. 因此，$|C|>1$.

14. 证明：p^2 阶群必是交换群，其中 p 是一个素数.

证 设 G 是一个阶为 p^2 的群，C 是 G 的中心，则 C 是 G 的正规子群，因此 $|C|\mid p^2$. 但由上题知 $|C|>1$，故必

$$|C|=p \text{ 或 } p^2.$$

若 $|C|=p$，则商群 G/C 的阶为素数 p，从而是循环群. 于是由习题 3.2 第 6 题知，G 是交换群. 因此 $C=G$，这与 G 是 p^2 阶群矛盾. 故 $|C|=p^2$，即 $G=C$ 是交换群.

15. 证明：群 G 的子集 S 的中心化子 $C(S)$ 等于 S 中各元素的正规化子的交.

证 由于

$$C(S)=\{x\in G\mid x\text{ 与 }S\text{ 中每个元素可换}\},$$
$$N(a)=\{y\in G\mid ya=ay\},\ a\in S,$$

故可知

$$\bigcap_{a\in S}N(a)=\{z\mid z\in G,\text{对 }\forall a\in S\text{ 都有 }az=za\},$$

从而

$$\bigcap_{a\in S}N(a)\subseteq C(S).$$

又任取 $x\in C(S)$，当然 $x\in\bigcap_{a\in S}N(a)$，故

$$C(S)\subseteq\bigcap_{a\in S}N(a).$$

因此

$$C(S)=\bigcap_{a\in S}N(a).$$

16.

证 设 $|G|=p^n$，并对 n 用数学归纳法.

当 $n=1$ 时结论显然. 假定对 $k<n$ 时结论成立，下证对 $|G|=p^n$ 时结论成立.

设 C 是 G 的中心，由第 13 题知 $|C|>1$，故 $|G/C|<p^n$. 而由题设 G 只有一个指数为 p 的子群 H，再由于易知

$$(G/C:H/C)=p\Longleftrightarrow(G:H)=p,$$

从而商群 G/C 只能有一个指数为 p 的子群. 于是由归纳假设，G/C 是循环群. 从而由习题 3.2 第 6 题知，G 是交换群.

因此，G 是有限交换 p-群，根据基本定理，设

$$G=\langle a_1\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle,$$

其中 $|a_i|=p^{k_i}(i=1,2,\cdots,s)$. 如果 $s>1$，则 $\langle a_1\rangle$ 与 $\langle a_2\rangle$ 均有惟一的指数为 p 的子群 $\langle a_1^p\rangle$ 与 $\langle a_2^p\rangle$. 于是

$$\langle a_1^p\rangle\times\langle a_2\rangle\times\cdots\times\langle a_s\rangle\quad\text{与}\quad\langle a_1\rangle\times\langle a_2^p\rangle\times\langle a_3\rangle\times\cdots\times\langle a_s\rangle$$

便是 G 的两个指数为 p 的子群，与题设矛盾. 故必 $s=1$，即 G 为循环群.

17.

证　设 G 是一个 n 阶群，且 $G=\{e,a_2,\cdots,a_n\}$.

任取$\sigma\in \mathrm{Aut}\,G$，因为 $\sigma(e)=e$，又 σ 为双射，故 σ 在集合

$$S=\{a_2,a_3,\cdots,a_n\}$$

上的限制 $\sigma|_S$ 是 S 上的一个置换，从而

$$\sigma|_S\in S_{n-1},$$

其中 S_{n-1} 为集合 S 上的 $n-1$ 次对称群. 又易知

$$\varphi:\sigma\longrightarrow\sigma|_S$$

是 G 的自同构群 $\mathrm{Aut}\,G$ 到 S_{n-1} 的一个单射.

又任取 $\sigma,\tau\in \mathrm{Aut}\,G, x\in G$，由于 $\sigma|_S$ 与 σ 对于 G 中元素 x 的象是一致的，即 $\sigma|_S(x)=\sigma(x)$，故易知 φ 是一个同态映射. 从而 φ 是 $\mathrm{Aut}\,G$ 到 S_{n-1} 的一个单同态映射. 因此

$$\mathrm{Aut}\,G\cong\varphi(\mathrm{Aut}\,G)\leqslant S_{n-1}.$$

于是由 Lagrange 定理知，$|\mathrm{Aut}\,G|$ 是 $|S_{n-1}|=(n-1)!$ 的一个因数.

18. 设 G_1,G_2 是两个群. 证明：若 $G_1\cong G_2$，则

$$\mathrm{Aut}\,G_1\cong\mathrm{Aut}\,G_2.$$

再举例指出反之不成立.

证　由题设：$G_1\cong G_2$，且设 φ 为其一个同构映射. 任取 $\sigma_1\in\mathrm{Aut}\,G_1$，下证：

$$\sigma_2:\varphi(x_1)\longrightarrow\varphi(\sigma_1(x_1))\quad(x_1\in G_1)$$

是 G_2 的一个自同构.

事实上，任取 $x_2\in G_2$，令 $\varphi(x_1)=x_2$，则 $\varphi(\sigma_1(x_1))$ 是由 x_2 完全确定的 G_2 中的一个元素. 反之，任取 $y_2\in G_2$，令

$$\varphi(y_1)=y_2,\ y_1\in G_1,\ \sigma_1(x_1)=y_1,$$

于是 $\varphi(x_1)\in G_2$，且

$$\sigma_2(\varphi(x_1))=\varphi(\sigma_1(x_1))=\varphi(y_1)=y_2,$$

即 σ_2 是 G_2 到 G_2 的一个满射.

类似可证 σ_2 是单射，从而为双射.

最后，由于对 G_1 中任意元素 x_1,y_1 有

$$\begin{aligned}&\sigma_2[\varphi(x_1)\varphi(y_1)]=\sigma_2[\varphi(x_1y_1)]\\&=\varphi[\sigma_1(x_1y_1)]=\varphi[\sigma_1(x_1)\sigma_1(y_1)]\\&=\varphi[\sigma_1(x_1)]\cdot\varphi[\sigma_1(y_1)]=\sigma_2[\varphi(x_1)]\cdot\sigma_2[\varphi(y_1)],\end{aligned}$$

故 σ_2 是群 G_2 的一个自同构，即 $\sigma_2\in\mathrm{Aut}\,G_2$.

易知 $\Psi:\sigma_1\longrightarrow\sigma_2$ 是 $\mathrm{Aut}\,G_1$ 到 $\mathrm{Aut}\,G_2$ 的一个映射. 又任取 $\tau_2\in\mathrm{Aut}\,G_2$，令

$$\tau_1:x_1\longrightarrow\varphi^{-1}[\tau_2(\varphi(x_1))].$$

则可证 $\tau_1\in\mathrm{Aut}\,G_1$，且对任意 $x_2\in G_2$，令 $\varphi(x_1)=x_2$，有

$$\varphi[\tau_1(x_1)]=\varphi\varphi^{-1}[\tau_2(x_2)]=\tau_2(x_2)=\tau_2[\varphi(x_1)],$$

即在 Ψ 之下，τ_1 是 τ_2 的逆象，故 Ψ 为满射.

类似可证 Ψ 为单射，从而为双射.

又对 $\sigma_1,\tau_1\in \mathrm{Aut}\,G_1$，令

$$\sigma_2:\varphi(x_1)\longrightarrow\varphi[\sigma_1(x_1)],\quad \tau_2:\varphi(x_1)\longrightarrow\varphi[\tau_1(x_1)].$$

于是

$$\sigma_2\tau_2(\varphi(x_1))=\sigma_2[\varphi(\tau_1(x_1))]$$
$$=\varphi[\sigma_1(\tau_1(x_1))]=\varphi[(\sigma_1\tau_1)(x_1)],$$

即 Ψ 是 $\mathrm{Aut}\,G_1$ 与 $\mathrm{Aut}\,G_2$ 的一个同构映射，故

$$\mathrm{Aut}\,G_1\cong\mathrm{Aut}\,G_2.$$

反之，若 $\mathrm{Aut}\,G_1\cong\mathrm{Aut}\,G_2$，则不一定有 $G_1\cong G_2$. 这由 §5 推论 2 可知.

19.

证 1) 令 $P_1=P\cap N$，则 P_1 显然是 p-子群. 若能证明 P_1 在 N 中的指数不含因子 p，则 P_1 便是 N 的 Sylow p-子群. 为此，下面来考察 $(N:P_1)$.

因为由群同构定理知，$N/(P\cap N)\cong PN/N$，故

$$(N:P_1)=(N:P\cap N)=(PN:P),\qquad (1)$$
$$(G:P)=(G:PN)(PN:P).\qquad (2)$$

而 P 是 G 的 Sylow p-子群，故 $(G:P)$ 不含因子 p. 从而由(2)知，$(PN:P)$ 也不含因子 p. 从而再由(1)知，$(N:P_1)$ 不含因子 p. 得证.

2) 设 $|G|=p^nst$，$|N|=p^mt$，$(p,st)=1$，则 $|P|=p^n$，$|P\cap N|=p^r$，$r\leqslant m$.

由群的同构定理知：

$$|PN/N|=|P/(P\cap N)|=p^{n-r},\quad n-r\geqslant n-m.\ (1)$$

但 $|G/N|=p^{n-m}$，$|PN/N|\mid|G/N|$，故

$$|PN/N|\leqslant p^{n-m},\ \text{即}\ n-r\leqslant n-m.$$

从而由(1)知，$n-r=n-m$，即 $|PN/N|=p^{n-m}$，亦即 PN/N 是 G/N 的 Sylow p-子群.

20.

证 S_3 共有三个 2 阶子群：

$$H_1=\{(1),(12)\},\quad H_2=\{(1),(13)\},\quad H_3=\{(1),(23)\}.$$

令 $M'=\{H_1,H_2,H_3\}$，且 S_3' 为 M' 上的三次对称群. 则易知

$$\varphi:\tau\longrightarrow\begin{pmatrix}H_1 & H_2 & H_3\\ \tau(H_1) & \tau(H_2) & \tau(H_3)\end{pmatrix}\quad(\forall\,\tau\in\mathrm{Aut}\,S_3)$$

是 $\mathrm{Aut}\,S_3$ 到 S_3' 的一个同态映射. 又易知

$$\tau\in\mathrm{Ker}\,\varphi\Longleftrightarrow\tau\ \text{在}\ S'\ \text{上引出恒等置换},$$

即 $\tau(H_i)=H_i(i=1,2,3)$，亦即 τ 把(12)，(13)，(23)分别变为自身. 但因

$$S_3=\langle(12),(13),(23)\rangle,$$

故 τ 是 S_3 的恒等自同构. 因此 φ 是单射.

又由 $|C(S_3)|=1$，$\mathrm{Inn}\,S_3\cong S_3/C(S_3)\cong S_3$，得

$$|\mathrm{Aut}\,S_3|\geqslant|\mathrm{Inn}\,S_3|=|S_3|=6.$$

于是 φ 满同态，从而 φ 是同构映射，$\mathrm{Aut}\,S_3\cong S_3'\cong S_3$.

注 更一般地，当 $n\geqslant3$，但 $n\neq6$ 时，S_n 的自同构都是内自同构，而且

$$\mathrm{Aut}\,S_n\cong S_n.$$

21.

证 设 G 有 k_p 个 Sylow p-子群，有 k_q 个 Sylow q-子群，则由 Sylow 定理可知：$k_p \mid q, k_q \mid p^2$. 但 p, q 是互异素数，故

$$k_p = 1 \text{ 或 } q; \quad k_q = 1, p, p^2.$$

1) 若 $k_p = 1$，则 G 有惟一的 Sylow p-子群，它是 G 的非平凡正规子群，故此时 G 不是单群.

2) 若 $k_p = q$，则由于 $k_p \equiv 1 \pmod{p}$，故 $p \mid q-1$，$p < q$.

若 $k_q = p$，则因 $k_q \equiv 1 \pmod{q}$，故 $q \mid p-1$. 这与 $p < q$ 矛盾；若 $k_q = p^2$，则由于 $|G| = p^2 q$ 即 G 的 Sylow q-子群都是 q 阶元生成的循环群，而任二这种互异子群的交为 $\{e\}$，从而 G 共有

$$k_q(q-1) = p^2(q-1) = p^2 q - p^2$$

个 q 阶元. 于是，G 的非 q 阶元共有 p^2 个. 设 P 是 G 的一个 Sylow p-子群，则 $|P| = p^2$ 且 P 中元素都不是 q 阶的. 于是 P 是 G 的惟一的 Sylow p-子群，这与 $k_p = q$ 也矛盾.

因此只有 $k_q = 1$，即 G 有惟一的 Sylow q-子群，它是 G 的非平凡正规子群. 从而 G 不是单群.

22. 设 G 是有限群，且 $|G| = pqr$，其中 p, q, r 是互异素数. 证明：G 不是单群.

证 不妨设 $p > q > r$，且 G 有 k_p 个 Sylow p-子群，k_q 个 Sylow q-子群，k_r 个 Sylow r-子群. 若 $k_p > 1, k_q > 1, k_r > 1$，则由于任二不同的 Sylow p-子群的交是 $\{e\}$，因此 k_p 个 Sylow p-子群共含 $k_p(p-1)$ 个 p 阶元. 同理，有 $k_q(q-1)$ 个 q 阶元，有 $k_r(r-1)$ 个 r 阶元. 于是

$$|G| = pqr \geqslant 1 + k_p(p-1) + k_q(q-1) + k_r(r-1). \quad (1)$$

但是由 Sylow 定理知，$k_p \mid qr$. 由于 p, q, r 是互异素数，且 $k_p > 1$，故只有

$$k_p = q, \ r, \ qr.$$

若 $k_p = q$，则由于 $p \mid k_p - 1$，故 $p \mid q-1$，这与 $p > q$ 矛盾；若 $k_p = r$，则同样有 $p \mid r-1$，这与 $p > r$ 矛盾. 故只有

$$k_p = qr. \quad (2)$$

又因 $k_q \mid pr, q \mid k_q - 1, k_q > 1, q > r$，所以 $k_q \geqslant p$.

同理，$k_r \geqslant q$. 于是由(1)及(2)知：

$$pqr \geqslant 1 + qr(p-1) + p(q-1) + q(r-1).$$

从而得 $0 \geqslant (p-1)(q-1)$，矛盾. 故 k_p, k_q, k_r 中至少有一个为 1，从而 G 至少有一个非平凡正规子群，G 不是单群.

23. 证明：不存在 56 阶单群.

证 设 G 是任意一个 56 阶群. 因为 $56 = 2^3 \cdot 7$，于是由 Sylow

定理知，G 的 Sylow 7 -子群的个数 $k_7 \mid 56$ 且

$$k_7 \equiv 1 \pmod 7.$$

据此可得

$$k_7 = 1 \text{ 或 } 8.$$

若 $k_7 = 1$，则这惟一的 Sylow 7 -子群是 G 的正规子群，且是非平凡的，从而 G 不是单群.

若 $k_7 = 8$，因为 G 的 Sylow 7 -子群是 7 阶群，所以它们为循环群且任二个不同的 Sylow 7 -子群之交只含有单位元，因此，这 8 个 Sylow 7 -子群共占去 G 的 49 个元素，而 Sylow 7 -子群与 Sylow 2 -子群的交只含有单位元，故 G 只有一个 Sylow 2 -子群. 因而它就是 G 的正规子群，故 G 不是单群.

总之，不存在 56 阶单群.

24. 证明：凡 455 阶群必为循环群.

证 设 G 是一个 455 阶群. 因为 $455 = 5 \cdot 7 \cdot 13$，所以由Sylow 定理知，G 有阶是 5，7，13 的元素. 设 G 的 Sylow 7 -子群有 k_7 个，于是由 Sylow 定理知：

$$k_7 \mid 455 = 5 \cdot 7 \cdot 13, \text{ 且 } k_7 \equiv 1 \pmod 7.$$

据此可知必 $k_7 = 1$. 即 G 的 Sylow 7 -子群只有一个，用 P_7 表示，它是 G 的一个正规子群.

同理，G 的 Sylow 13 -子群也只有一个，用 P_{13} 表示，它也是 G 的一个正规子群. 从而 $P_7 P_{13}$ 是 G 的 91 阶正规子群.

又同理，根据 Sylow 定理，G 的 Sylow 5 -子群的个数为 1 或 91. 如果有 91 个 Sylow 5 -子群，则 G 共有 $91 \times 4 = 364$ 个 5 阶元素，而 $P_7 P_{13}$ 中包含 91 个阶与 5 互素的元，这两种元素共有 455 个，即 G 的全部元素. 任取一个 Sylow 5 -子群 P_5，则 $P = P_5 P_7$ 是 G 的一个 35 阶子群. 因为

$$P_5 \lhd P, \quad P_7 \lhd P, \quad P_5 \cap P_7 = \{e\},$$

故 $P = P_5 \times P_7$. 因此，P 是一个 35 阶循环群. 从而 G 包含一个 35 阶元. 但 G 的前面所有元中没有 35 阶元，矛盾. 因此，G 只有一个 Sylow 5 -子群 P_5.

又因为 P_5，P_7，P_{13} 都是 G 的互异的素幂阶循环群，故由上面第 6 题知，

$$G = P_5 \times P_7 \times P_{13}$$

是一个循环群.

25.

证 令 P 是 G 的一个 Sylow p-子群. 若 $|G|=p^m$，则根据群的类等式可知，G 的中心 C 的阶必大于 1. 又因 G 不可换，故 $C\neq G$，即 C 是 G 的非平凡正规子群，这与 G 是单群矛盾.

因此，$|G|$ 至少有两个不同的素因子. 于是

$$\{e\}\subset P\subset G.$$

这样，如果 P 是 G 的惟一的 Sylow p-子群，则 P 便是 G 的一个非平凡的正规子群，这与 G 是单群矛盾. 故 G 的 Sylow p-子群的个数 $k>1$.

26. 设 G 是一个有限群，$H\lhd G$，$K\lhd G$，又 P 是 G 的一个 Sylow p-子群. 证明：

1) $|P\cap HK|=\dfrac{|P\cap H|\cdot|P\cap K|}{|P\cap H\cap K|}$；

2) $P(H\cap K)=PH\cap PK$.

证 1) 设 $|G|=p^sm$，$p\nmid m$，其中 p 是素数，则 $|P|=p^s$. 另设

$$|H|=p^\alpha a,\ |K|=p^\beta b,\ |H\cap K|=p^\gamma c, \tag{1}$$

其中 $p\nmid a$，$p\nmid b$，$p\nmid c$. 由于 $H\lhd G$，$K\lhd G$，故

$$H\cap K\lhd G,\ HK\lhd G,$$

且由第 19 题知，$P\cap H$、$P\cap K$、$P\cap H\cap K$ 分别为 H、K、$H\cap K$ 的 Sylow p-子群. 于是由(1)知：

$$|P\cap H|=p^\alpha,\ |P\cap K|=p^\beta,\ |P\cap H\cap K|=p^\gamma,$$

$$|HK|=\frac{|H|\cdot|K|}{|H\cap K|}=p^{\alpha+\beta-\gamma}\cdot d. \tag{2}$$

其中 $d=\dfrac{ab}{c}$ 为正整数，且 $p\nmid d$.

又因 $P\cap HK$ 也是 HK 的 Sylow p-子群，故由(2)知

$$|P\cap HK|=p^{\alpha+\beta-\gamma}=\frac{|P\cap K|\cdot|P\cap K|}{|P\cap H\cap K|}. \tag{3}$$

2) 再根据

$$|PHK|=\frac{|P|\cdot|HK|}{|P\cap HK|},\ |P(H\cap K)|=\frac{|P|\cdot|H\cap K|}{|P\cap H\cap K|}$$

以及(3)可得

$$|PH\cap PK|=\frac{|PH|\cdot|PK|}{|PHK|}=\frac{|P|\cdot|H\cap K|}{|P\cap H\cap K|}$$

$$=|P(H\cap K)|.$$

但由于 G 是有限群，且显然

$$P(H\cap K)\subseteq PH\cap PK,$$

因此，

$$P(H\cap K)=PH\cap PK.$$

27.

证 $n=3$ 时，结论显然成立. 因此下设 $n>3$.

由于 A_n 中每个元素都可表为偶数个对换之积，从而也就是一些形如

$$(ab)(cd) \text{ 或 } (ab)(ac)$$

的项之积. 其中 a,b,c,d 是 $\{1,2,\cdots,n\}$ 中互异的元素. 但由于

$$(ab)(cd)=(abc)(bcd),\quad (ab)(ac)=(acb),$$

故 A_n 中的每个元素又都是一些 3 -循环之积，即 A_n 由全体 3 -循环生成.

28.

证 设 $\{(1)\}\neq N\trianglelefteq A_n$. 在 N 中任取元素 $\tau\neq(1)$，且 τ 是 N 中变动数码最多的一个置换.

1) 若 τ 恰变动 4 个数码，这时 τ 必为二对换之积，因为恰变动 4 个数码的偶置换，别的可能性是不存在的. 现在不妨设

$$\tau=(12)(34).$$

因为 $n>4$，$N\trianglelefteq A_n$，取 $\sigma=(345)$，则易知

$$\tau_1=\sigma\tau\tau^{-1}=(12)(45)\in N,\quad \tau^{-1}\tau_1=(345)\in N.$$

这与 τ 是 N 中变动数码最多的置换矛盾.

2) 设 τ 所变动的数码多于 4 个. 此时可分以下三种情形并取 $\sigma=(234)$ 可得：

① $\tau=(1234\cdots)\cdots$，$\tau_1=\sigma\tau\sigma^{-1}=(1342\cdots)\cdots\in N$；

② $\tau=(123)(4a\cdots)\cdots$，$\tau_1=\sigma\tau\sigma^{-1}=(134)(2\cdots)\cdots\in N$；

③ $\tau=(12)(34\cdots)\cdots$，$\tau_1=\sigma\tau\sigma^{-1}=(13)(42)(56)\cdots\in N$.

其中显然 $\tau_1\neq\tau$，故 $\tau^{-1}\tau_1\neq(1)$. 在①与③情形下，由于对所有数码 $k>4$ 均有 $\tau^{-1}\tau_1(k)=k$，这与 τ 的取法矛盾；在②的情形下，$\tau^{-1}\tau_1$ 除 $1,2,3,4,a$ 之外使其余数码都不变，即 $\tau^{-1}\tau_1$ 只变动五个数码，而此时 τ 所变动的数码多于 5 个，这与 τ 的取法也矛盾.

因此由 1)与 2)知，τ 只能变动三个数码，即 τ 是一个 3 -循环，故由上题知，$N=A_n$.

29. 证明：当 $n\geqslant5$ 时，n 次对称群 S_n 不是可解群.

证 见习题 3.2 第 8 题.

30.

证 设 σ 与 τ 共轭，即存在 n 次置换 α 使

$$\sigma=\alpha\tau\alpha^{-1}.$$

设 $\tau=(i_1i_2\cdots i_s)(j_1j_2\cdots j_t)\cdots(k_1k_2\cdots k_m)$ 是不相连的循环之积（每个字母都出现）. 则由第二章 §6 定理 5 知，

$$\sigma=\alpha\tau\alpha^{-1}=(\alpha(i_1)\cdots\alpha(i_s))(\alpha(j_1)\cdots\alpha(j_t))\cdots(\alpha(k_1)\cdots\alpha(k_m))$$

显然仍为不相连的循环之积，即 σ 与 τ 有相同的循环结构.

反之，设 σ 与 τ 有相同的循环结构，且

$$\sigma=(i_1)(i_2)\cdots(i_s)\cdots(j_1j_2\cdots j_t)\cdots,$$
$$\tau=(i'_1)(i'_2)\cdots(i'_s)\cdots(j'_1j'_2\cdots j'_t)\cdots.$$

令

$$\alpha=\begin{pmatrix} i_1 & i_2 & \cdots & i_s & \cdots & j_1 & j_2 & \cdots & j_t & \cdots \\ i'_1 & i'_2 & \cdots & i'_s & \cdots & j'_1 & j'_2 & \cdots & j'_t & \cdots \end{pmatrix},$$

则

$$\alpha(i_1)=i'_1,\cdots,\alpha(i_s)=i'_s,\cdots,\alpha(j_1)=j'_1,\cdots,\alpha(j_t)=j'_t,\cdots$$

于是

$$\begin{aligned}\alpha\tau\alpha^{-1}&=(\alpha(i_1))\cdots(\alpha(i_s))\cdots(\alpha(j_1)\cdots\alpha(j_t))\cdots\\&=(i'_1)\cdots(i'_s)\cdots(j'_1j'_2\cdots j'_t)\cdots=\sigma.\end{aligned}$$

即 σ 与 τ 共轭.

31. 设 a 是群 G 中一个阶为 $m_1m_2\cdots m_n$ 的元素. 证明：若正整数 $m_1,m_2,\cdots,m_n$ 两两互素，则 a 可惟一表示为

$$a=a_1a_2\cdots a_n,$$

其中 a_i 都是 a 的方幂（从而可两两互换）且

$$|a_i|=m_i\quad(i=1,2,\cdots,n).$$

证 对 n 用数学归纳法.

1) 存在性

当 $n=1$ 时显然，假设对 $n-1$ 成立，下证对 n 成立.

令 $k=m_1m_2\cdots m_{n-1}$，则由于 $m_1,m_2,\cdots,m_n$ 两两互素，故

$$(k,m_n)=1,$$

于是存在整数 s,t 使 $ks+m_nt=1$. 由此可得

$$a=a^{m_nt}\cdot a^{ks}=a'\cdot a_n,\qquad(1)$$

其中 $a'=a^{m_nt}$，$a_n=a^{ks}$. 且易知

$$|a'|=m_1m_2\cdots m_{n-1},\quad |a_n|=m_n.$$

于是由归纳假设，有

$$a'=a_1a_2\cdots a_{n-1},\qquad(2)$$

其中 $|a_i|=m_i$，且 a_i 都是 a' 的方幂从而也是 a 的方幂（$i=1,2,\cdots,n-1$）.

将(2)式代入(1)式，得

$$a=a_1a_2\cdots a_{n-1}a_n.$$

其中 $|a_i|=m_i$，且每个 a_i 都是 a 的方幂（$i=1,2,\cdots,n$）.

2) 惟一性

当 $n=1$ 时显然. 假定对 $n-1$ 成立，下证对 n 成立. 令

$$a=a_1a_2\cdots a_{n-1}a_n=b_1b_2\cdots b_{n-1}b_n,$$

其中 $|a_i|=|b_i|=m_i$，且 a_i 与 b_i 都是 a 的方幂（$i=1,2,\cdots,n$）. 再令

$$a'=a_1a_2\cdots a_{n-1},\quad b'=b_1b_2\cdots b_{n-1},$$

则由于 $m_1,m_2,\cdots,m_{n-1}$ 两两互素，且 a_i 与 b_i 都是 a 的方幂，从而可换，故

$$|a'|=|b'|=k=m_1m_2\cdots m_{n-1}.$$

令

$$b'a'^{-1}=a_nb_n^{-1}=c\qquad(3)$$

于是有

$$c^k=(b'a'^{-1})^k=e,\quad c^{m_n}=(a_nb_n^{-1})^{m_n}=e.$$

但由于 $m_1,m_2,\cdots,m_{n-1},m_n$ 两两互素，故 $(k,m_n)=1$. 从而由此易知 $c=e$ 是群 G 的单位元. 于是由(3)知

$$a'=b',\quad a_n=b_n.$$

即 $a'=a_1a_2\cdots a_{n-1}=b_1b_2\cdots b_{n-1}$，$a_n=b_n$. 因此由归纳假设知

$$a_i=b_i\quad(i=1,2,\cdots,n).$$

第四章　环与域

§1　环的定义

一、主要内容

1．环与子环的定义和例子。在例子中，持别重要的是效域上的多项式环、n阶全阵环和线性变换环，以及集M的幂集环.

2．环中元素的运算规则和环的非空子集S作成子环的充要条件：

$$a,b\in S \Longrightarrow a-b\in S,$$

$$a,b\in S \Longrightarrow ab\in S.$$

3．循环环的定义和性质.

加群是循环群的环称为循环环.其性质在本节内的主要有：

1）循环环必为交换环；

2）循环环的子环也是循环环；

3）循环环的子加群必为子环；

4）pq（p,q是互异素数）阶环必为循环环.

二、释疑解难

1．设R是一个关于

代数运算十，•作成的环．应注意两个代数运算的地位是不平等的，是要讲究次序的．所以有时把这个环记为$(R,十,•)$(或者就直接说“R对十，•作成一个环”)．但不能记为$R,•,十$)．因为这涉及对两个代数运算所要求满足条件的不同．我们知道，环的代数运算符号只是一种记号．如果集合只有二代数运算记为$\circ$，$\oplus$，又R对$\circ$作成一个交换群，对$\oplus$满足结合律且$\oplus$对$\circ$满足左、右分配律，即

$$a\oplus(b\circ c)=(a\oplus b)\circ(a\oplus c),\quad (a\circ b)\oplus c=(a\oplus c)\circ(b\oplus c),$$

则就只能说R对“$\circ,\oplus$”作成一个环，或记为$(R,\circ,\oplus)$.

就是说，在环的定义里要留意两个代数运算的顺序.

2．设R对二代数运算十，•作成一个环．那么，R对“十”作成一个加群，这个加群记为$(R,十)$；又R对“•”作成一个半群，这个乍群记为$(R,•)$．再用左、右分配律把二者联系起来就得环$(R,十.•)$.

现在问：环R中的这个半群$(R,•)$是否也有可能作成一个群呢？回答是否定的，除非$|R|=1$．因若$|R|>1$，则对R中任意元素$a\neq 0$总有

$$0\cdot a=a\cdot 0=0,$$

这说明0不是$(R,•)$的单位元，而且0在$(R,•)$中也没有逆元.因此，$(R,•)$只能作成半群而不能作成群.

进一步，如果去掉0，那么R的全体非零元素对乘法是否作成群呢？这是可能的.例如任何数域就属于这种情形.当然，R的全体非零元也有不能作成群的，如偶数环和整数环，等等.

3．由于在环R中有：$a\cdot 0=0\cdot a=0$，故

e是R的左（右、双边）单位元$\Longleftrightarrow$

e是半群$(R,•)$的左（右、双边）单位元.

4．n阶循环环的幂等元和其有单位元的条件.

设$R=\langle a\rangle=\{0,a,2a,\cdots,(n-1)a\}$为一个$n$阶循环环，且$a^2=ka$.以下三例阐明$R$有单位元的条件和其幂等元的情况.

以下三例均假定$R=\langle a\rangle$为n阶循环环，且$a^2=ka$

$(0\leqslant k<n)$.

例 1 R 有单位元 $\Longleftrightarrow (k,n)=1$.

证 设 $(k,n)=1$，则有整数 u,v 使

$$ku+nv=1.$$

于是对 R 中任意元素 sa 有

$$(sa)(ua)=(suk)a=s(1-nv)a=sa,$$

由于 R 是可换环，故 ua 是 R 的单位元.

反之，设 R 有单位元 $e=ta$，则

$$ae=a,\quad a(ta)=(tk)a=a,\quad (tk-1)a=0,$$

于是 $n\mid tk-1$. 设 $tk-1=nq$，则

$$tk+n(-q)=1,\quad \text{故}(k,n)=1.$$

例 2 ta 是 R 的幂等元 $\Longleftrightarrow n\mid kt^2-t$.

证 设 ta 是环 R 的幂等元，则

$$(ta)^2=t^2a^2=t^2ka=ta,\quad (kt^2-t)a=0.$$

但由于 a 是 R 的加群的 n 阶元素，故 $n\mid kt^2-t$.

反之，设 $n\mid kt^2-t$，则因 $na=0$，故 $(kt^2-t)a=0$ 且

$$ta=kt^2a=t^2\cdot ka=t^2a^2=(ta)^2.$$

即 ta 是 R 的幂等元.

例 3 环 R 有 $2^{\varphi(n)-\varphi(k,n)}$ 个幂等元，其中 $\varphi(n)$ 为 n 的不同素因数的个数，$\varphi(k,n)$ 为 k 与 n 的最大公因数 (k,n) 的不同素因数的个数.

证 设 $n=p_1^{r_1}p_2^{r_2}\cdots p_m^{r_m}$ 是 n 的标准分解式，由上例知，R 中幂等元的个数就是同余式

$$kx^2-x\equiv 0\pmod n \tag{1}$$

的解的个数，而这个同余式的解的个数等于 m 个同余式

$$kx^2-x\equiv 0\pmod{p_i^{r_i}}\quad (i=1,2,\cdots,m) \tag{2}$$

的解的个数的乘积. 但易知，对一个固定 i，当 $p_i\mid k$ 时，方程(2)只有解 0；当 $p_i\nmid k$ 时，由于 $(p_i^{r_i},k)=1$，故有整数 u,v 使

$$p_i^{r_i}u+kv=1.$$

于是 $p_i\nmid v$，$p_i^{r_i}\mid kv-1$，$p_i^{r_i}\mid v(kv-1)=kv^2-v$.

故 v 是方程(2)的一个非零解；又 0 显然为其一解，而且方程(2)没有别的解，即此时方程(2)只有两个解. 于是同余式(1)有 $2^{\varphi(n)-\varphi(k,n)}$ 个解，即 R 有 $2^{\varphi(n)-\varphi(k,n)}$ 个幂等元.

三、习题 4.1 解答

1.

解 虽然易知乘法$\circ$满足结合律，又$\circ$对$+$也满足左分配律，但是右分配律不满足. 例如易知：

$$(1+(-1))\circ 2=0,\quad (1\circ 2)+((-1)\circ 2)=4,$$

即 $(1+(-1))\circ 2\neq(1\circ 2)+((-1)\circ 2)$，故 $\mathbf{R}$ 对$+$，$\circ$不作成环.

2.

解 F 上一切方阵 $\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}$ 显然作成环，但不可换，因为

例如

$$\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}=\begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix},\quad \begin{pmatrix}3 & 4\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}=\begin{pmatrix}3 & 6\\ 0 & 0\end{pmatrix},$$

二者不相等. 又显然一切方阵 $\begin{pmatrix}1 & b\\ 0 & 0\end{pmatrix}$ $(\forall b\in F)$ 都是此环的左单位元，但无右单位元. 从而此环无单位元.

3.

解 R 对所给加法与乘法作成一个有单位元的交换环. 单位元是$(1,1)$. 又当 $a_1a_2\neq 0$ 时(a_1,a_2)有逆元(a_1^{-1},a_2^{-1}). 而当$a_1a_2=0$时(a_1,a_2)没有逆元.

4.

证 设 R 是布尔环,则对 R 中任意元素 a,b 有

$$a+b=(a+b)^2=a^2+ab+ba+b^2=a+ab+ba+b,$$

故

$$ab+ba=0. \tag{1}$$

在上式中取 $b=a$,则由于 R 中元素都是幂等元,故有

$$a^2+a^2=0, \quad \text{即 } a+a=0;$$

再由 $a+a=0$ 得 $a=-a$. 从而由(1)式得

$$ab=-ba=ba.$$

即布尔环 R 为交换环.

5.

证 设 G 的全体自同态映射作成的集合为 R,则 R 一定包含 G 的零同态 θ,故 $R\neq\varnothing$.

又任取 $\sigma,\tau,\gamma\in R,a\in G$,则

$$(\theta+\sigma)a=\theta a+\sigma a=\sigma a, \quad (-\sigma+\sigma)a=-\sigma a+\sigma a=0,$$

$$[(\sigma+\tau)+\gamma]a=(\sigma+\tau)a+\gamma a=(\sigma a+\tau a)+\gamma a$$

$$=\sigma a+(\tau a+\gamma a)=\sigma a+(\tau+\gamma)a=[\sigma+(\tau+\gamma)]a,$$

$$(\sigma+\tau)a=\sigma a+\tau a=\tau a+\sigma a=(\tau+\sigma)a,$$

由于 a 的任意性,故由上诸式得

$$\theta+\sigma=\sigma, \quad -\sigma+\sigma=\theta,$$

$$(\sigma+\tau)+\gamma=\sigma+(\tau+\gamma),$$

$$\sigma+\tau=\tau+\sigma,$$

即 R 对所给加法来说,θ 为零元,$-\sigma$ 为 σ 的负元,且加法满足结合律、交换律,故 R 作成加群. 又

$$[(\sigma\tau)\gamma]a=(\sigma\tau)(\gamma a)=\sigma[\tau(\gamma a)]$$

$$=\sigma[(\tau\gamma)a]=[\sigma(\tau\gamma)]a,$$

$$[\sigma(\tau+\gamma)]a=\sigma[(\tau+\gamma)a]=\sigma(\tau a+\gamma a)$$

$$=\sigma(\tau a)+\sigma(\gamma a)=(\sigma\tau)a+(\sigma\gamma)a,$$

故 $\sigma(\tau+\gamma)=\sigma\tau+\sigma\gamma$. 类似地有

$$(\tau+\gamma)\sigma=\tau\sigma+\gamma\sigma.$$

即乘法满足结合律,乘法对加法满足分配律,故 R 对所给加法和乘法作成环.

又显然 G 的恒等自同构是这个环的单位元.

6.

证 设 e 是环 R 的单位元,$a,b\in R$,则

$$(a+b)-(b+a)=(a+b)-e(b+a)$$

$$=(a+b)+(-e)(b+a)=(a+b)+(-e)b+(-e)a$$

$$=ea+eb+(-e)b+(-e)a=ea+[e+(-e)]b+(-e)a$$

$$=ea+0+(-e)a=[e+(-e)]a=0,$$

故 $a+b=b+a$,即 R 中的加法满足交换律.

7.

证 因为 $a+b=ab$，故有

$$(1-a)(1-b)=1-(a+b)+ab=1.$$

又因为 $1-a$ 可逆，故 $1-b=(1-a)^{-1}$. 从而

$$1=(1-b)(1-a)=1-(a+b)+ba=1-ab+ba.$$

因此 $$ab=ba.$$

8. 证明：循环环必是交换环，并且其子环也是循环环.

证 设 $R=\{\cdots,-2a,-a,0,a,2a,\cdots\}$ 为循环环，且 $a^2=ka$.

则任取 $x,y\in R$，令

$$x=sa,\quad y=ta.\quad \text{则 } xy=yx=stka.$$

故 R 可换.

又由于循环群的子群仍为循环群，故循环环的子环仍为循环环.

§4.2 环的零因子和特征

一、主要内容

1. 环的左、右零因子和特征的定义与例子.

2. 若环 R 无零因子且阶大于 1，则 R 中所有非零元素对加法有相同的阶. 而且这个相同的阶不是无限就是一个素数.

这就是说，阶大于 1 且无零因子的环的特征不是无限就是一个素数.

有单位元的环的特征就是单位元在加群中的阶.

3. 整环(无零因子的交换环)的定义和例子.

二、释疑解难

1. 由教材关于零因子定义直接可知，如果环有左零因子，则 R 也必然有右零因子. 反之亦然.

但是应注意，环中一个元素如果是一个左零因子，则它不一定是一个右零因子. 例如，教材例 1 中的元素 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ 就是一个例子. 反之，一个右零因子也不一定是一个左零因子. 例如，设置为由一切方阵

$$\begin{pmatrix}x&y\\0&0\end{pmatrix}\qquad(\forall x,y\in Q)$$

对方阵普通加法与乘法作成的环. 则易知 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ 是 R 的一个右零因子，但它却不是 R 的左零因子.

2. 关于零因子的定义.

关于零因子的定义，不同的书往往稍有差异，关键在于是否把环中的零元也算作零因子. 本教材不把零元算作零因子，而有的书也把零元算作零因子. 但把非牢的零因子称做真零因子. 这种不算太大的差异，读者看参考书时请留意.

3. 关于整环的定义.

整环的定义在不同的书中也常有差异. 大致有以下 4 种定义方法：

定义 1 无零因子的交换环称为整环(这是本教材的定义方法).

定义 2 阶大于 1 且无零因子的交换环，称为整环.

定义 3 有单位元且无零因子的交换环，称为整环.

定义 4 阶大于 1、有单位元且无零因子的交换环，称为整环.

以上 4 种定义中，要求整环无零因子、交换是共同的，区别就在于是否要求有单位元和阶大于 1. 不同的定义方法各有利弊，不宜绝对肯定哪种定义方法好或不好. 这种情况也许到某

个时期会得到统一．但无论如何现在看不同参考书时应留意这种差异．

本教材采用定义 1 的方法也有很多原因，现举一例。本章§8 定理 1：设 P 是交换环 R 的一个理想．则

P 是 R 的素理想 $\Leftrightarrow$ R / P 是整环．

这样看起来本定理表述显得干净利索．但若整环按定义 2(或定义 3、4)要求，那么以上定理表述就需变动．究竟要怎样变动，作为练习请读者自己给出．　　。’

三、习题 4．2 解答

1．

证　1) 设 S 是由环 R 的全体正则元作成的集合．并令 $a,b\in S$，且 $(ab)c=0$．于是得

$$a(bc)=0.$$

但 a 是正则元，故 $bc=0$．又因 b 是正则元，故 $c=0$．

同理，由 $c(ab)=0$ 可得 $c=0$．因此，ab 也是正则元，即 $ab\in S$．从而 S 作成半群．

2) 设 $a\neq 0$ 是环 R 的正则元，且 $axa=0$．于是 $a(xa)=0$．从而

$$xa=0.\quad \text{故 } x=0.$$

反之，设元素 a 满足条件，且 $ab=0$，则便有

$$aba=0.\quad \text{从而 } b=0.$$

同理，若 $ba=0$ 便有 $aba=0$，从而 $b=0$．即 a 不是零因子，从而是正则元．

2．

证　由题设，对任意 $x\in R$ 有 $ex=x$，从而由 $R\neq\{0\}$ 知 $e\neq 0$．又因为

$$(xe-x)e=0,$$

而 R 无右零因子，故 $xe-x=0$，$xe=x$．从而 e 是 R 的单位元．

3．

证　用 $M_n(F)$ 表示数域 F 上的 n 阶全阵环．任取 $\boldsymbol{O}\neq\boldsymbol{A}\in M_n(F)$，如果 $|\boldsymbol{A}|\neq 0$，则 $\boldsymbol{A}$ 有逆方阵 $\boldsymbol{A}^{-1}$，从而 $\boldsymbol{A}$ 是全阵环 $M_n(F)$ 的可逆元．

如果 $|\boldsymbol{A}|=0$，则齐次线性方程组 $\boldsymbol{AX}=\boldsymbol{0}$ 有非零解．任取其一非零解 $b_1,b_2,\cdots,b_n$，则以此非零解为任一列，而其余列全是零的 n 阶方阵 $\boldsymbol{B}\neq\boldsymbol{O}$，则有 $\boldsymbol{AB}=\boldsymbol{O}$，即 $\boldsymbol{A}$ 是全阵环 $M_n(F)$ 的零因子．

4．

证 设 R 是一个交换环，其全体幂零元作成的集合为 S. 任取 $a,b\in S$，令

$$a^m=0,\qquad b^n=0,$$

其中 m,n 为正整数，则由 R 可换知：

$$(ab)^m=(a^m)^n(b^n)^m=0;$$

$$\begin{aligned}(a-b)^{m+n}=&a^{m+n}-C_{m+n}^1a^{m+n-1}b+\cdots+\\&(-1)^{n-1}C_{m+n}^{n-1}a^{m+1}b^{n-1}+(-1)^nC_{m+n}^na^mb^n+\\&(-1)^{n+1}C_{m+n}^{n+1}a^{m-1}b^{n+1}+\cdots+(-1)^{m+n}b^{m+n}\\=&a^ma^n-C_{m+n}^1a^ma^{n-1}b+\cdots+(-1)^{n-1}C_{m+n}^{n-1}a^mab^{n-1}+\\&(-1)^nC_{m+n}^na^mb^n+(-1)^{n+1}C_{m+n}^{n+1}a^{m-1}b^nb+\cdots+\\&(-1)b^nb^m=0.\end{aligned}$$

故 $ab,a-b\in S$. 从而 $S\leqslant R$.

5.

证 设 m 是最小正整数使 $a^m=0$. 如果 $1<n<m$，令

$$m=nq_1+r_1\quad(0\leqslant r_1<n).$$

则由 $a^n=a$ 可得

$$0=a^m=a^{nq_1}\cdot a^{r_1}=a^{q_1+r_1}.$$

但是 $0<q_1+r_1<m$，这与 m 的最小性矛盾.

因此，$n\geqslant m$. 再设

$$n=mq+r\quad(0\leqslant r<m).$$

于是有：

$$a=a^n=a^{mq+r}.$$

若 $r=0$，则 $a=a^{mq}=0$；若 $r>0$，则 $a=a^{mq}\cdot a^r=0$. 总之，$a=0$.

6.

解 例如，1) 所有 $\begin{pmatrix}x&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&0\end{pmatrix}$ 及所有 $\begin{pmatrix}x_1&0&\cdots&0\\0&x_2&\cdots&0\\\vdots&\vdots&&\vdots\\0&0&\cdots&x_n\end{pmatrix}$；

2）所有$\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & x & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & x \end{pmatrix}$及所有$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & x_n \end{pmatrix}$；

3）所有$\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$及所有$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ x_n & 0 & \cdots & 0 \end{pmatrix}$；

4）所有$\begin{pmatrix} 2x_1 & 0 & \cdots & 0 \\ 0 & 2x_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 2x_n \end{pmatrix}$及所有$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & x_n \end{pmatrix}$；

5）所有$\begin{pmatrix} 2x_1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$及所有$\begin{pmatrix} 2x_1 & 0 & \cdots & 0 \\ 0 & 2x_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 2x_n \end{pmatrix}$.

7．设 R 是一个无零因子的环．证明：若 $|R|$ 偶数，则 R 的特征必为 2.

证 设 R_+ 是 R 的加群，则根据习题 2.2 第 4 题知，R_+ 必有 2 阶元．又 R_+ 为交换群，故 2 整除 R_+ 中最大阶元的阶，即 $2 \mid \operatorname{char} R$.

另一方面，由于 R 是有限的无零因子环，因此，$\operatorname{char} R$ 一定是素数，再由 $2 \mid \operatorname{char} R$ 知，必

$$\operatorname{char} R = 2.$$

8．证明：P—环无非零幂零元.

证 设 R 是一个 p -环，且 a 是 R 的一个幂零元，故可设 n 是使 $a^n=0$ 的最小正整数.

若 $n>p$，令 $n=pq+r$，$(0\leqslant r<p)$，则因 $a^p=a$，故当 $r>0$ 时，

$$a^n=a^{pq+r}=(a^p)^q a^r=a^q \cdot a^r=a^{q+r}=0;$$

当 $r=0$ 时，有

$$a^n=a^{pq}=(a^p)^q=a^q=0,$$

即 $a^{q+r}=0$，但是 $n=pq+r>q+r$，这与 n 的最小性矛盾．故 $n\leqslant p$.

若 $n=p$，则由于 $a^n=0$，而 $a^p=0$，故 $a=0$；

若 $n<p$，令 $p=n+(p-n)$，则

$$a=a^p=a^{n+(p-n)}=a^n a^{p-n}=0.$$

总之，$a=0$．即 R 无非零幂零元.

§4.3 除环和域

一、主要内容

1．除环和域的定义及例子．四元数除环.

2．有限环若有非零元素不是零因子，则必有单位元，且每个非零又非零因子的元素都是可

逆元.

3. 有单位元环的乘群(单位群)的定义和例子.

有单位元的环的全体可逆元作成的群，称为该环的乘群或单位群.

除环或域的乘群为其全体非零元作成的群；整数环 Z 的乘群为

$$Z^* = \{1, -1\};$$

数域上 n 阶全阵环的乘群为全体 n 阶可逆方阵对乘法作成的群；Gaus s 整环的乘群为

$$U(Z[i]) = \{1, -1, i, -i\}.$$

二、释疑解难

1. 阶大于 1 的有限环可分为两类： ”

1) 一类是有零因子的有限环. 例如，有限集 $M(|M|>1)$ 上的幂集环 $P(M)$，不仅是个有零因子的有限环，而且除单位元 M 外其余每个非零元素都是零因子；后面§5所讲的以合数 n 为模的剩余类环 Zn 也是一个有零因子的有限环.

2) 另一类就是无零因子的有限环. 实际上根据本节推论和魏得邦定理可知，这种有限环就是有限域. 例如，以素数 p 为模的剩余类环 Z_p 以及教材第六章所介绍的伽罗瓦域都属于这种情形.

这就是说，阶大子 1 的有限环或者有零因子或者无零因子，从而为域.

2. 教材定理 3 指出：

阶大于 1 的环 R 是除环 $\Longleftrightarrow$ 对 R 中任意元素 $a\neq 0, b$，方程

$$ax=b \quad (\text{或 } ya=b)$$

在 R 中有解.

与群定义中要求两个方程 $ax=b$ 与 $ya=b$ 都有解不同，这里仅要求方程 $ax=b$ 或 $ya=b$ ($\forall 0\neq a, b\in R$) 中有一个在 R 中有解即可. 教材中利用方程 $ax=b$ 有解得到 R 的全体非零元有右单位元且每个非零元素都有右逆元，从而得到 R 是除环.

如果利用方程 $ya=b$ 在 R 中有解，则将得到 R 的全体非零元有左单位元且每个非零元都有左逆元，从而也得到只是除环.

3. 关于有单位元环的单位群.

设 R 是阶大于 1 的有单位元的环. 则显然

$$R\text{是除环}\Leftrightarrow R\text{的单位群是 } R-\{0\};$$

$$R\text{是域}\Leftrightarrow R-\{0\}\text{是交换群.}$$

显然，除环或域有“最大’’的单位群. 又显然幂集环 $P(M)$ 的单位群只有单位元(因其他元素那是零因子)，它是“最小”的单位群.

三、习题 4. 3 解答

1. 证略.

2. 证略.

3. 证明：域和其子域有相同的单位元.

证 设 F_1 是域 F 的子域，1 是 F 的单位元，$1'$ 是 F_1 的单位元. 则任取 $a\in F_1$，且 $a\neq 0$，由 F_1 是域知，$a^{-1}\in F_1$，且 $aa^{-1}=1'$；但 $a, a^{-1}\in F$，$aa^{-1}=1$，故

$$1'=aa^{-1}=1,$$

即 F 与 F_1 有相同的单位元. (也可由 F^* 与 F_1^* 有相同单位元直接得出)

4.

证 令$\alpha=a_0+a_1i+a_2j+a_3k$，

$\beta=b_0+b_1i+b_2j+b_3k$（其中a_i,b_i为实数）.

则直接根据四元数乘法可得：

$$\alpha\beta-\beta\alpha=2(a_2b_3-a_3b_2)i+$$
$$2(a_3b_1-a_1b_3)j+2(a_1b_2-a_2b_1)k.$$

又易知当$\delta=x_1i+x_2j+x_3k$时，$\delta^2=-x_1^2-x_2^2-x_3^2$是实数，它同任意四元数均可换. 因此，$(\alpha\beta-\beta\alpha)^2$是实数，它同任意四元数可换，即有

$$(\alpha\beta-\beta\alpha)^2\gamma=\gamma(\alpha\beta-\beta\alpha)^2.$$

5.

解 1) 易知R作成一个有单位元的交换环，但不一定作成域.

例如，当F为实数域时，方阵

$$\boldsymbol{A}=\begin{pmatrix}\sqrt{2} & 2\\ 1 & \sqrt{2}\end{pmatrix}\neq\boldsymbol{O}$$

属于R，但$|\boldsymbol{A}|=0$，故$\boldsymbol{A}$在R中没有逆元，从而此时R不能作成域. 又此时R的单位群是：

$$R^*=\left\{\begin{pmatrix}a & 2b\\ b & a\end{pmatrix}\middle|\,a^2\neq2b^2\right\}.$$

2) 但是，当F为有理数域时，R能作成域.

事实上，设

$$\boldsymbol{A}=\begin{pmatrix}a & 2b\\ b & a\end{pmatrix}\neq\boldsymbol{O}$$

为R中任一非零方阵（即a,b是不全为0的有理数），则

$$|\boldsymbol{A}|=a^2-2b^2\neq0.$$

因若不然，设$|\boldsymbol{A}|=0$，则有$a^2=2b^2$. 于是必然$b\neq0$，且

$$\left(\frac{a}{b}\right)^2=2,$$

这是不可能的. 故$|\boldsymbol{A}|\neq0$，从而A有逆方阵，且

$$\boldsymbol{A}^{-1}=\frac{1}{|\boldsymbol{A}|}\begin{pmatrix}a & -2b\\ -b & a\end{pmatrix}\in R,$$

即A在R中有逆元，从而此时R作成域.

6.

证 1) 设域F的特征是素数p，则F中每个非零元素的阶（作为加群）都是p. 但$|F|=4$，故$p|4$，从而$p=2$. 即

$$\mathrm{char}\ F=2.$$

2) 设 $F=\{0,1,a,b\}$，则

$$G=\{1,a,b\}$$

对 F 的乘法作成一个群，即域 F 的乘群. 由于 a,b 在 G 中的阶整除 $|G|=3$，故 a,b 的阶只能是 3. 令 x 是 a,b 中的任一个，则 $x^3=1$ 且

$$x^3-1=(x-1)(x^2+x+1)=0.$$

但 $x\neq 1$，且域无零因子，故

$$x^2+x+1=0 \text{ 或 } x^2=-x-1.$$

又因 char $F=2$，故 $x=-x,1=-1$，从而有 $x^2=x+1$.

§4 环的同态与同构

一、主要内容

1. 环的同态映射和同构映射的定义和例子
2. 环同态映射的简单性质.

设 φ 是环 R 到环豆 $\overline{R}$ 的同态满射，则

1) $\varphi(0)$ 是 $\overline{R}$ 的零元，$\varphi(-a)=-\varphi(a)$ $(\forall a\in R)$ ；

2) 当 R 是交换环时，$\overline{R}$ 也是交换环；

3) 当 R 有单位元时，$\overline{R}$ 也有；并且 R 的单位元的象是 $\overline{R}$ 的单位元.

3. 在环同态映射下，是否有零因子不会传递. 即若环 $R\sim\overline{R}$，则当 R 有零因子时，$\overline{R}$ 可能没有，当 R 无零因子时，$\overline{R}$ 却可能有.

二、释疑解难

1. 在 §1 已经强调过，对于环的两个代数运算一定要区分前后顺序. 同样，对于环的同态映射，也要注意其保持运算必须是：加法对加法，乘法对乘法. 即

$$\varphi(a+b)=\varphi(a)+\varphi(b),$$

$$\varphi(ab)=\varphi(a)\varphi(b).$$

第一式中等号左边的加号“+”是环 R 的加法，而等号右边的加号“+”是环 R 的代数运算. 二者虽然都用同一符号，但在实际例子中这两个代数运算却可能点很大差异，根本不是一回事.

对上述第二个式子中等号两端的乘法完全类似，不再赘述.

2. 由于零因子在环同态映射下不具有传递性，因此，若环 $R\sim\overline{R}$，则当 R 为整环时，$\overline{R}$ 不一定是整环；又当 R 不是整环时，$\overline{R}$ 却可能是整环. 教材中的例 1 和例 2 说明了这一点.

3. 关于环的挖补定理，

设 R 是环，$S\leqslant R$，又 $S\cong\overline{S}$ 且 $\overline{S}\cap(R-S)=\varnothing$. 挖补是说，可在环 R 中把子环 S“挖”出来把 $\overline{S}$“补”进去，从而可把 $\overline{S}$ 看作 R 的子环(在同构意义下).

其实，挖补定理对群也成立. 不再赘述.

三、习题 4. 4 解答

1. 证 略.

2.

证 设 σ 是有理数域 Q 的一个自同构. 由于在同构映射下，单位元与单位元对应，负元与负元对应，逆元与逆元对应，故

$$\sigma(1)=1,\quad \sigma(2)=\sigma(1+1)=\sigma(1)+\sigma(1)=2.$$

一般地，$\sigma(m)=m,\sigma(-m)=-m$，其中 m 为正整数. 又易知

$$\sigma(m^{-1})=m^{-1},\quad \sigma(n/m)=n/m\quad (m\neq 0).$$

即 σ 为 Q 的恒等自同构. 从而有理数域只有恒等自同构.

3.

证 恒等变换和 $\sigma:a+bi\longrightarrow a-bi$ 显然是数域 $Q(\mathrm{i})$ 的两个自同构.

现在设 τ 也是 $Q(\mathrm{i})$ 的一个自同构，则由上题知，对任意有理数 a，有 $\tau(a)=a$. 另外，设 $\tau(\mathrm{i})=c+d\mathrm{i},d\neq 0$，则

$$-1=\tau(\mathrm{i}^2)=(c+d\mathrm{i})^2=c^2-d^2+2cd\mathrm{i}.$$

这只有 $c=0,d=\pm 1$. 但当 $d=1$ 时，由

$$\tau(a)=a,\quad \tau(\mathrm{i})=\mathrm{i}$$

可得 $\tau(a+b\mathrm{i})=a+b\mathrm{i}$，即 τ 为恒等自同构；当 $d=-1$ 时，又得 $\tau(a+b\mathrm{i})=a-b\mathrm{i}$，即 $\tau=\sigma$.

故 $Q(\mathrm{i})$ 有且只有两个自同构.

4.

证 $Q(\mathrm{i})$ 与 $Q(\sqrt{2})$ 不同构. 因若同构，设 σ 是 $Q(\sqrt{2})$ 到 $Q(\mathrm{i})$ 的一个同构映射，则 $\sigma(1)=1$，从而 $\sigma(4)=4$.

令 $\sigma(\sqrt{2})=x\in Q(\mathrm{i})$，则

$$\sigma(2\sqrt{2})=\sigma(\sqrt{2}+\sqrt{2})=\sigma(\sqrt{2})+\sigma(\sqrt{2})=2x.$$

于是，一方面 $\sigma(\sqrt{2}\cdot 2\sqrt{2})=\sigma(4)=4$；而另一方面有

$$\sigma(\sqrt{2}\cdot 2\sqrt{2})=\sigma(\sqrt{2})\sigma(2\sqrt{2})=x\cdot 2x=2x^2,$$

故 $4=2x^2,x^2=2$. 但易知 $Q(\mathrm{i})$ 中不存在这样的 x，从而这与 σ 是从 $Q(\sqrt{2})$ 到 $Q(\mathrm{i})$ 的同构映射矛盾. 故域 $Q(\mathrm{i})$ 与 $Q(\sqrt{2})$ 不同构.

5.

证 令 K 及其二运算如教材中本题提示所示. 则可验算出 K 对此二运算作成一个有单位元的环，其单位元是 $(0,1)$.

再令 $$R_0=\{(a,0)\mid a\in R\}.$$

则易知 $\varphi:a\longrightarrow(a,0)$ $(\forall a\in R)$ 是 R 到 R_0 的一个环同构映射. 因此，

$$R\cong R_0.$$

于是若规定 $(a,0)=a$，则 $R\leqslant K$. 即无单位元环 R 被包含在有单位元的环 K 中.

6.

证 显然，R 对所规定的新运算$\oplus$，$\circ$是封闭的. 令 R 对新运算作成的集合记为 $R(\oplus,\circ)$. 下面在 R 与 $R(\oplus,\circ)$之间建立映射：

$$\varphi: x \longrightarrow x+u \quad (x\in R).$$

易知这是 R 到 $R(\oplus,\circ)$的双射，即 R 的双射变换.

又
$$\begin{aligned}\varphi(a+b)&=(a+b)+u=(a+u)+(b+u)-u\\&=\varphi(a)+\varphi(b)-u=\varphi(a)\ominus\varphi(b),\end{aligned}$$

$$\begin{aligned}\varphi(a)\circ\varphi(b)&=(a+u)\circ(b+u)\\&=(a+u)(b+u)-(a+u)u-u(b+u)+u^2+u\\&=ab+au+ub+u^2-au-u^2-ub-u^2+u^2+u\\&=ab+u=\varphi(ab),\end{aligned}$$

因此，φ 是 R 到 $R(\oplus,\circ)$的同构映射. 由于 R 是环，故 $R(\oplus,\circ)$也是环且与 R 同构.

7.

证 设 τ 是实数域 R 的任一自同构，于是由第 2 题知，

$$\tau(n/m)=n/m.$$

又设 a 为实数，且 $a>0$，则必 $\tau(a)>0$；因为设 $a=b^2$，则 $\tau(a)=\tau(b^2)=\tau(b)^2>0$.

又若 $a>c$，则由于 $a-c>0$，故

$$\tau(a-c)=\tau(a)-\tau(c)>0,$$

从而 $\tau(a)>\tau(c)$.

现在设 a 为任一实数，则存在有理数 r,s 使 $r<a<s$. 于是由上面所证知：

$$\tau(r)<\tau(a)<\tau(s), \quad \text{即 } r<\tau(a)<s.$$

这就是说，对满足 $r<a<s$ 的任何有理数 r,s 必有

$$r<\tau(a)<s.$$

因此必 $\tau(a)=a$，即 τ 是 R 的恒等自同构.

§4. 5 模 n 剩余类环

一、主要内容

1. 以正整数 n 为模的 n 个同余类 $\bar{0},\bar{1},\cdots,\overline{n-1}$ 关于同余类的加法与乘法，作成一个有单位元的 n 阶交换环，记为 Z_n，称为模 n 剩余类环.

若 $n=1$，则 $Z_n=\{\bar{0}\}$. 因此，以下假设 $n>1$.

环 Z_n 有以下性质：

1) 若 $(m,n)=1$，则 $\bar{m}$ 为 Z_n 中可逆元，从而 Z_n 中有 $\varphi(n)$个可逆元；若 $(m,n)\neq 1$，则 $\bar{m}$ 是环 Z_n 的零因子.

2) Z_n 的特征是 n. 又 Z_p（p 为素数）是域；又当 n 为合数时，Z_n 有零因子，从而不是域.

3) $Z_m\sim Z_n \iff n\mid m$.

2. 循环环定义、例子和简单性质.

1) 整数环及其子环以及剩余类环及其子环都是循环环. 而且在同构意义下这也是全部的循环环.

2) 循环环是交换环，但不一定有单位元. 而且这种环的子加群同子环、理想三者是一回事. 因此，n 阶循环环有且只有 $T(n)$（n 的正因数个数）个子环（理想）.

二、释疑解难

1．剩余类环是一类很重要的有限环，因为这种环是一种具体的环，特别是它的特征、子环(理想)、零因子、可逆元和单位群等都很清楚．因此，在环的讨论里常常以它作为例子来加以利用，并说明问题．

2．整数环的任二不同的非零子环，作为加群，它们显然是同构的(因为它们都是无限循环群)．但是，作为环，它们并不同构．因为，例如设

$$\langle s\rangle=\{\cdots,-s,0,s,2s,\cdots\},\quad \langle t\rangle=\{\cdots,-t,0,t,2t,\cdots\}.$$

其中整数 $s\neq\pm t$，且 $st\neq0$．若 $\langle s\rangle\cong\langle t\rangle$，且 φ 为其一同构映射，令

$$\varphi(s)=kt,\quad \varphi(rs)=t.$$

于是由 $\varphi(s)=kt$ 又得 $\varphi(rs)=rkt$．从而

$$rkt=t,\quad rk=1,\quad k=\pm1.$$

若 $k=1$，则 $\varphi(s)=t$．于是 $\varphi(s^2)=t^2=st$，从而 $s=t$，矛盾；

若 $k=-1$，则 $\varphi(s)=-t$．于是 $\varphi(s^2)=(-t)^2=-st$，从而 $s=-t$，矛盾．

因此，$\langle S\rangle$ 与 $\langle T\rangle$ 不能同构．

3．剩余类环 Z_n 中任二不同的子环也不能同构．

事实上，Z_n 的任二不同阶的子环当然不能同构．又设置为 Z_n 的任意 k 阶子环，则 $k|n$．但由于 $(Z_n,+)$ 是 n 阶循环群，从而对 n 的每个正因数 k，$(Z_n,+)$ 有且只有一个 k 阶子群，于是环 Z_n 有且仅有一个 k 阶子环．因此，Z_n 的任二不同的于环当然不同构．

4．但是，有有限环存在，其有二不同子环是同构的．例如：令 R 是 Z_2 上的 2 阶全阵环，则 $|R|=16$，且易知

$$R_1=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\},$$

$$R_2=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}1&1\\0&0\end{pmatrix}\right\}$$

都是 R 的 4 阶子环，而且易知 R_1 还是一个域．但是，R_2 无单位元(且不可换，又非零元都是零因子)，因此，R_1 与 R_2 不能同构．

此外易知：

$$R_3=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix}\right\},$$

$$R_4=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$$

也都是环 R 的 4 阶子环，而且 R_1，R_2，R_3，R_4 都是互不同构的．对此不再详述，兹留给读者作为练习．

有文献已经证明，互不同构的 4 阶环共有 11 个．对此不再赘述．

三、习题 4．5 解答

1. 证明：同余类的乘法是 Z_n 的一个代数运算．

证 设 $\overline{i}=\overline{s}$，$\overline{j}=\overline{t}$ (i,j,s,t 均为整数)，则

$$n|i-s,\quad n|j-t.$$

于是 n 整除

$$i(j-t)+(i-s)t=ij-st.$$

从而

$$\overline{ij}=\overline{st}.$$

即同余类的乘法是 Z_n 的一个代数运算.

2. 试指出环 Z_8 中的可逆元和零因子，再给出它的所有子环.

解 易知，Z_8 的全部可逆元为：

$$\overline{1},\overline{3},\overline{5},\overline{7}.$$

而 Z_8 的全部零因子为：$\overline{2},\overline{4},\overline{6}$.

又由于 Z_8 是循环环，其子加群就是子环(也是理想)，故可知其全部子环有 $T(8)=4$ 个，它们是

$$\{\overline{0}\},\ \{\overline{0},\overline{4}\},\ \{\overline{0},\overline{2},\overline{4},\overline{6}\},\ Z_8$$

3. 试给出 Z_{10} 的所有子环，并指出它们各自的特征.

解 Z_{10} 有 $T(10)=4$ 个子环. 这 4 个子环是

$$\{\overline{0}\},\ \{\overline{0},\overline{5}\},\ \{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8}\},\ Z_{10}.$$

而且它们的特征依次是 1,2,5,10.

4.

证 由于 Z_n 中的元素 $\overline{k}$ 是可逆元当且仅当$(k,n)=1$，但小于 n 且与 n 互素的正整数有 $\varphi(n)$ 个，于是 Z_n 中的全体可逆元对乘法作成一个 $\varphi(n)$ 阶交换群. 由于$(a,n)=1$，故 $\overline{a}$ 是这个群中的元素. 于是由 Lagrange 定理可知，$\overline{a}$ 在这个群中的阶整除这个群的阶 $\varphi(n)$，从而 $\overline{a}^{\varphi(n)}=\overline{1}$，即

$$a^{\varphi(n)}\equiv 1 \pmod{n}.$$

注 1640 年费马提出，若$(a,p)=1$ (p 是素数)时，有

$$a^{p-1}\equiv 1 \pmod{p}.$$

此称为费马小定理，被欧拉于 1736 年证明. 后于 1760 年被欧拉证明了更一般情形，即本题结论，故常称其为欧拉定理.

5.

证 设 $g(x)=a_0+a_1x+\cdots+a_nx^n$. 由于 Z_p 与多项式环 $Z_p[x]$ 的特征均为 p，且对任意 $a\in Z_p$ 有 $a^p=a$，故

$$\begin{aligned}[g(x)]^p&=(a_0+a_1x+\cdots+a_nx^n)^p\\&=a_0^p+a_1^px^p+\cdots+a_n^p(x^p)^n\\&=a_0+a_1x^p+\cdots+a_n(x^p)^n=g(x^p),\end{aligned}$$

即

$$[g(x)]^p=g(x^p).$$

6.

证　任取环 Z_n 的一个幂零元 $\bar{a}$，则存在正整数 s 使 $\bar{a}^s=\bar{0}$，亦即

$$n\mid a^s,\quad p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}\mid a^s.$$

从而 $p_i\mid a$ $(i=1,\cdots,m)$. 但由于 $p_1,p_2,\cdots,p_m$ 是互异的素数，故 $p_1p_2\cdots p_m\mid a$，从而 $\bar{a}\in\langle\overline{p_1p_2\cdots p_m}\rangle$.

反之，若 $\bar{a}\in\langle\overline{p_1p_2\cdots p_m}\rangle$，即，$p_i\mid a$，令

$$s=\max(k_1,k_2,\cdots,k_m),\ \text{则}(p_1p_2\cdots p_m)^s\mid a^s.$$

但是 $n=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}\mid(p_1p_2\cdots p_m)^s$，故 $n\mid a^s$. 因此，

$$\bar{a}^s=\overline{a^s}=\bar{0},$$

即 $\langle\overline{p_1p_2\cdots p_m}\rangle$ 是 Z_n 的全体幂零元作成的集合（实际是由 $\overline{p_1p_2\cdots p_m}$ 生成的 Z_n 的子环）.

又由于 $\langle\overline{p_1p_2\cdots p_m}\rangle$ 仅由以下元素构成：

$$\overline{p_1p_2\cdots p_m},\ 2\,\overline{p_1p_2\cdots p_m},\ \cdots,\ (p_1^{k_1-1}p_2^{k_2-1}\cdots p_m^{k_m-1})\,\overline{p_1p_2\cdots p_m},$$

故 Z_n 有 $p_1^{k_1-1}p_2^{k_2-1}\cdots p_m^{k_m-1}$ 个幂零元.

7. 证明：整数环的不同子环不同构，　证：见上面“释疑解难”部分中的 2.

8.

证　设 $R\cong\overline{R}$，且 $R=\langle a\rangle$，$a^2=ka$，$0\leqslant k<n$. 则由于在同构映射下生成元与生成元相对应，故 R 的生成元 a 的象，记为 $\bar{a}$，也是 $\overline{R}$ 的一个生成元. 而且也有

$$\bar{a}^2=k\bar{a}\quad(0\leqslant k<n).$$

反之，设 a 与 $\bar{a}$ 分别为 R 与 $\overline{R}$ 的生成元，且

$$a^2=ka,\quad \bar{a}^2=k\bar{a}\quad(0\leqslant k<n).$$

则易知 $\varphi(ma)=m\bar{a}$（m 为非负整数）是环 R 与 $\overline{R}$ 的一个同构映射. 故 $R\cong\overline{R}$.

§4.6 理　想

一、主要内容

1. 左、右理想、理想的定义和例子.

2. 单环的定义以及单环的一个重要性质.

设环 R 有单位元，则 R 上全阵环 $R_{n\times n}$ 的理想都是 R 中某个理想上的全阵环. 由此可知：

$$R_{n\times n}\text{是单环}\Leftrightarrow R\text{是单环}.$$

特别，除环和域上的全阵环都是单环.

3. 由环中元素山 a_1，a_2，…，a_m 生成的理想 $\langle a_1,a_2,\cdots,a_m\rangle$. 特别，由一个元素 a 生成的主理想 $\langle a\rangle$.

在一般情况下，主理想 $\langle a\rangle$ 中元素的表达形式. 在特殊环（交换环和有单位元的环）中 $\langle a\rangle$ 的元素表达形式如下：

1）在有单位元的环 R 中：

$$\langle a\rangle=\left\{\sum_{i=1}^{m}x_iay_i \mid x_i,y_i\in R,m\text{为正整数}\right\}.$$

2）在交换环 R 中：

$$\langle a\rangle=\{ra+na\mid r\in R,n\in\mathbf{Z}\}.$$

3）在有单位元的交换环 R 中：

$$\langle a\rangle=\{ra\mid r\in R\}.$$

4．理想的和与积仍为理想．

二、释疑解难

1．关于理想的乘法．

我们知道，如果 A，B 是群 G 的二子集或(正规)子群，则 A 与 B 的乘积是如下规定的：

$$AB=\{ab\mid a\in A,,\ b\in B\}.$$

但当 A，B 是环 R 的理想时，如果仍按以上规定相乘，则一般而言其乘积 AB 不再是理想．由于这个原因，环中理想的乘法规定为

$$AB=\{\text{有限和}\sum a_ib_i\mid a_i\in A,,\ b_i\in B\}.$$

易证明，此时 $AB\trianglelefteqslant R$.

2．对任意环 R，则 R 至少有平凡理想｛0｝和 R．通常把 R 本身叫做 R 的单位理想，这是由于以下原因：对 R 的任意理想 N，显然都有

$$RN\subseteq N,\qquad NR\subseteq N.$$

但当 R 有单位元时，则显然又有 $RN\subseteq N$，　　$NR\subseteq N$．从而有

$$RN=NR=N.$$

这就是说，此时 R 在理想乘法中的作用类似于数 1 在数的乘法中的作用．

3．设 R 为任意环，$a\in R$．则易知

$$\mathrm{N}=\{ra\mid r\in R\}$$

是 R 的一个左理想．若 R 是交换环，则当然 $N\trianglelefteqslant R$．但是应注意，由于 R 不一定有单位元，故不一定有 $a\in N$．从而也不能说 N 是由 a 生成的理想．

例 1　设 R 为偶数环，$a=4$，则

$$N=\{ra\mid r\in R\}=\{\cdots,-16,-8,0,8,16,\cdots\},$$

且 $4\notin N$．而且实际上 N 是偶数环中由 8 生成的主理想，即

$$N=\{4r\mid r\in R\}$$
$$=\langle 8\rangle=\{8r+8n\mid r\in R,n\in\mathbf{Z}\}=\{8n\mid n\in\mathbf{Z}\}.$$

但是 $\langle 4\rangle=\{4r+4n\mid r\in R,n\in\mathbf{Z}\}=\{4n\mid n\in\mathbf{Z}\}=\{\cdots-8,-4,0,4,8,\cdots\}$．因此，$N\neq\langle 4\rangle$．实际上是 $N=\langle 8\rangle\subset\langle 4\rangle$．

在一般环中，$N=\{ra\mid r\in R\}\subseteq\langle a\rangle$．当然，如果环 R 有单位元时，则显然

$$N=\{ra\mid r\in R\}=\langle a\rangle.$$

4．教材中只介绍了由一个元素生成的主理想$\langle a\rangle$和由有限个元素生成的理想$\langle a_1,a_2,\cdots,a_m\rangle$．其实这一概念也可以推广．

设 S 为环 R 的任一非空子集，则 R 中所有包含 S 的理想的交记为 $\langle S\rangle$，它是 R 中包含 S 的最小理想，并称其为 R 中由 S 生成的理想. 当 S 只包含一个元素或有限个元素时，$\langle S\rangle$ 就是我们上面所说的理想.

5. n 阶循环环的有单位元的理想(子环).

例 2 设 $R=\langle a\rangle$ 为 n 阶循环环，且 $a^2=ka$. 则 R 的 $T(n)$ 个子环(理想)中有 $2^{\Psi(n)-\Psi(k,n)}$(参考前面 §1 释疑解难中的例 3)个有单位元的子环，它们正好都是由幂等生成元生成的子环.

证 设 e 是环 R 的一个幂等元，则由 e 生成的子环(亦即子加群)$\langle e\rangle$ 中，任取一个元素 x，令 $x=re$，则

$$ex=e(re)=re^2=re=x,$$

故 e 是子环 $\langle e\rangle$ 的单位元.

其次，设 e 和 e' 都是环 R 的幂等元，且 $\langle e\rangle=\langle e'\rangle$，则由上面知，$e$ 和 e' 是一子环的单位元，故 $e'=e$. 即不同的幂等元生成不同的有单位元的子环.

最后，设 $N\leqslant R$，且 N 有单位元 e，则 $\langle e\rangle\subseteq N$. 另一方面，任取 $x\in N$，则 $xe=x$. 但 $\langle e\rangle$ 是子环，从而也是理想，故 $xe\in\langle e\rangle$，因此 $N\subseteq\langle e\rangle$，$N=\langle e\rangle$. 得证.

三、习题 4. 6 解答

1. 证 略.

2. 证 1) 略. 2) 由于

$$ar_1b-ar_2b=a(r_1-r_2)b,\quad ar_1b\cdot ar_2b=a(r_1bar_2)b,$$

其中 $r_1,r_2\in R$，故得 $aRb\leqslant R$.

注 一般 aRb 不是环 R 的理想.

3.

证 用 S_l 表示 S 的全体左零化子作成的集合，显然 $0\in S_l$. 又若 $a,b\in S_l$，即 $aS=0$，$bS=0$. 于是对任意 $x\in S$ 及 $r\in R$ 有

$$(a-b)x=ax-bx=0,\ (ra)x=r(ax)=0.$$

即 $a-b,ra\in S_l$. 因此，S_l 是 R 的一个左理想.

类似有 S 的右零化子和 S 的右零化理想.

4. 证 参考上面“释疑解难”部分 3.

5.

证 1) Z 是有单位元的交换环，又 $a\in N$. 故 $\langle a\rangle\subseteq N$.

又任取 $b\in N$，并令

$$b=aq+r\quad(0\leqslant r<a).$$

则 $r=b-aq\in N$. 再由 a 的最小性知，$r=0$. 从而

$$b=aq\in\langle a\rangle,$$

故 $N\subseteq\langle a\rangle$. 因此，$N=\langle a\rangle$.

2) 任取 $a\in\langle a_1,a_2,\cdots,a_m\rangle$，并令

$$a=k_1a_1+k_2a_2+\cdots+k_ma_m\quad(k_i\in Z).$$

由于 $d\mid a_i$，故 $d\mid a$. 从而 $a\in\langle d\rangle$，$\langle a_1,a_2,\cdots,a_m\rangle\subseteq\langle d\rangle$.

反之，由于 $(a_1,a_2,\cdots,a_m)=d$，故存在整数 $t_1,t_2,\cdots,t_m$ 使

$$d=t_1a_1-t_2a_2+\cdots+t_ma_m\in\langle a_1,a_2,\cdots,a_m\rangle,$$

故 $\langle d\rangle\subseteq\langle a_1,a_2,\cdots,a_m\rangle$. 从而得证.

由于 $d\mid a_i$，故 $d\mid a$. 从而 $a\in\langle d\rangle$，$\langle a_1,a_2,\cdots,a_m\rangle\subseteq\langle d\rangle$.

反之，由于 $(a_1,a_2,\cdots,a_m)=d$，故存在整数 $t_1,t_2,\cdots,t_m$ 使

$$d=t_1a_1-t_2a_2+\cdots+t_ma_m\in\langle a_1,a_2,\cdots,a_m\rangle,$$

故 $\langle d\rangle\subseteq\langle a_1,a_2,\cdots,a_m\rangle$. 从而得证.

6. 证明：域 F 上多项式环 $F[x]$ 的每个理想都是主理想.

证　设 $N\trianglelefteqslant F[x]$. 若 $N=\{0\}$，则 $N=\langle 0\rangle$；若 $N\neq\{0\}$，则 N 中存在次数最小的多项式 $m(x)$. 任取 $f(x)\in N$，令

$$f(x)=q(x)m(x)+r(x),$$

其中 $r(x)=0$ 或 $r(x)$ 的次数小于 $m(x)$ 的次数.

因为 $m(x)\in N\trianglelefteqslant F[x]$，故 $q(x)m(x)\in N$，从而

$$r(x)=f(x)-q(x)m(x)\in N.$$

但 $m(x)$ 是 N 中次数最小的多项式，故 $r(x)=0$. 即

$$f(x)=q(x)m(x),\quad N\subseteq\langle m(x)\rangle.$$

又 $\langle m(x)\rangle\subseteq N$，故 $N=\langle m(x)\rangle$.

7. 举例指出，环 R 的中心不一定是 R 的理想.

解　例如，有理数域 Q 上 $n(n>1)$ 阶全阵环 $Q_{n\times n}$ 的中心为 $C=\{aE\mid a\in Q\}$，它不是 $Q_{n\times n}$ 的理想，因为易知存在 $A\in Q_{n\times n}$ 使 $aE\cdot A=aA\notin C$，其中 $a\neq 0$.

又例如，设 R 为数域 F 上的 2 阶全阵环，其中心 C 为 F 上一切纯量方阵 aE（$a\in F$，E 为 2 阶单位矩阵）作成的子环. 但 C 不是 R 的理想：因为例如

$$\begin{pmatrix}1&1\\1&1\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\begin{pmatrix}1&1\\1&1\end{pmatrix}\notin C.$$

8. 8. 证明：§4 中例 3 中的环 F_N，当 N 为降秩方阵时，不是单环.

证　设 $r(N)=r$. 因 N 为降秩方阵，故 $0\leqslant r<n$. 而且线性方程组

$$NX=0\quad 与\quad YN=0$$

均有非零解. 各取其一非零解，设分别为 $(a_1,a_2,\cdots,a_n)^{\mathrm{T}}$ 及

$(b_1,b_2,\cdots,b_n)^{\mathrm{T}}$. 现令 A 是第一列元素为 $a_1,a_2,\cdots,a_n$，其余各列元素全为 0 的 n 阶方阵，而 B 是第一行元素为 $b_1,b_2,\cdots,b_n$，其余各行元素全为 0 的 n 阶方阵. 显然 $AB\neq 0$ 而且

$$NA=BN=0.$$

由此可知，对任意 $C\in F_N$ 都有

$$C\circ(AXB)=(AXB)\circ C=0 \quad (\forall X\in F_N).$$

故易知

$$W=\{AXB\mid X\in F_N\}\trianglelefteqslant F_N.$$

又显然任何满秩方阵都不属于 W，故 $W\lhd F_N$.

再因为 $AB\neq 0$，而 $AB=AEB\in W$，从而 $W\neq 0$. 即 W 是环 F_N 的一个非平凡理想，故 F_N 不是单环.

注 W 显然是一个零乘环.

§4.7 商环与环同态基本定理

一、主要内容

1. 设 $N\trianglelefteqslant R$，则所有(关于加法的)陪集 $x+N(\forall x\in R)$ 对于陪集的加法与乘法

$$(a+N)+(b+N)=(a+b)+N, \qquad (a+N)(b+N)=ab+N$$

作成一个环，称为 R 关于理想 N 的商环，记为 R/N.

$R\sim R/N$ $(x\longrightarrow x+N)$. 反之，若环 $R\sim\overline{R}$，且核为 N，则

$$N\trianglelefteqslant R, \quad 且 \quad R/N\cong\overline{R}.$$

即在同构意义下，任何环能而且只能与其商环同态. 此称为环同态基本定理或环的第一同构定理.

2. 环的第二同构定理. 设 $H\leqslant R, N\trianglelefteqslant R$. 则

1) $H\cap N\trianglelefteqslant H, N\trianglelefteqslant(H+N)$;

2) $H/(H\cap N)\cong(H+N)/N$.

3. 环的第三同构定理. 设 $A\trianglelefteqslant R, B\trianglelefteqslant R, A\leqslant B$. 则

$$B/A\trianglelefteqslant R/A, \quad (R/A)/(B/A)\cong R/B.$$

二、释疑解难

1. 环同态基本定理有的书包括："$N\trianglelefteqslant R\Rightarrow R\sim R/N$"，但有的书不包括这一结论，而只指出：

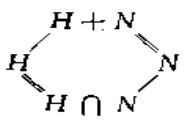
$$R\sim\overline{R},\ N\text{为核}\Rightarrow R/N\cong\overline{R}.$$

也有书称此为"环的第一同态定理"或"环的第一同构定理". 甚至也有的书虽有此定理，但却未给予任何名称. 不过多数的书均明示"环同态基本定理"且指出

$$"R\sim\overline{R},\ N\text{为核}\Rightarrow R/N\cong\overline{R}".$$

当然，这些问题是非本质的，只是在看参考书时留意其差异即可.

2. 环的第二同构定理与群的第二同构定理很类似. 不仅定理的条件和结论类似，而且其证明方法也基本相同. 区别只在于把原来群中的子群 H 和正规子群 N 的乘积 HN 现在换为 $H+N$(现在 H 是子环，N 是理想). 由此可同样画出此同构定理的示意图如右图.



3. 环的第三同构定理与群的第三同构定理也基本类似，只是其中有一部分转移到本节习题中去了.

以上环的三个同构定理，从叙述(条件和结论)和证明方法应多与群的三个同构定理作比较，这样不仅可以加深理解而且可以增强记忆.

三、习题 4. 7 解答

1.

证　必要性显然. 现设 $\operatorname{Ker}\varphi = N = \{0\}$，且

$$\varphi(a) = \varphi(b) \quad (a, b \in R).$$

则 $\varphi(a-b) = \bar{0}$. 于是 $a-b \in N = \{0\}$，$a-b = 0$，$a = b$. 即 φ 又是单射. 从而 φ 是同构映射.

2.

证　1) 因为 $\operatorname{char} R = \infty$，则易知

$$\varphi: n \longrightarrow ne \quad (\forall n \in N, e \text{ 是 } R \text{ 的单位元})$$

是整数环 Z 到环 R 的单同态. 从而 $Z \cong \varphi(Z) \leqslant R$.

2) 因为 $\operatorname{char} R = p$，同理易知

$$\tau: ne \longrightarrow \bar{n}$$

是 R 的子环 $R_1 = \{0, e, 2e, \cdots, (p-1)e\}$ 到 $Z_p = \{\bar{0}, \bar{1}, \cdots, \overline{p-1}\}$ 的同构映射，故 $R_1 \cong Z_p$.

3.

证　设 $\varphi(N) = \bar{N}$，则显然 $N \subseteq \varphi^{-1}(\bar{N})$.

任取 $a \in \varphi^{-1}(\bar{N})$，设 $\varphi(a) = \bar{n} \in \bar{N}$，则存在 $n \in N$ 使 $\varphi(n) = \bar{n} = \varphi(a)$. 从而

$$\varphi(a-n) = \varphi(a) - \varphi(n) = \bar{0},$$

即 $a-n \in K \subseteq N$. 令 $a-n = n_1 \in N$，则

$$a = n + n_1 \in N.$$

因此，$\varphi^{-1}(\bar{N}) \subseteq N$. 再由 $N \subseteq \varphi^{-1}(\bar{N})$ 可知：

$$N = \varphi^{-1}(\bar{N}).$$

4.

证　易知

$$\varphi: a+bi \longrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

是环 R 到 $\bar{R}$ 的一个双射. 又由于

$$\begin{aligned}
\varphi[(a+bi)+(c+di)] &= \varphi[(a+c)+(b+d)i] \\
&= \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\
&= \varphi(a+bi) + \varphi(c+di), \\
\varphi[(a+bi)(c+di)] &= \varphi[(ac-bd)+(ad+bc)i] \\
&= \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\
&= \varphi(a+bi)\varphi(c+di),
\end{aligned}$$

故 φ 是同构映射，从而 $R \cong \bar{R}$.

5. 设 R 为环，$N \lhd R$. 证明：

1) R/N 中的理想都具有形状 K/N，其中 K 是 R 的含 N 的理想；

2) 在自然同态 $R \sim R/N$ 之下，R 的理想 H 的象为

$$(H+N)/N.$$

证 1) 设 $\overline{K}\trianglelefteqslant R/N$，且 $K=\{k\mid k+N\in\overline{K},k\in R\}$，则任取 k_1，$k_2\in K,r\in R$，有 $k_1+N,k_2+N\in\overline{K}$，且

$$(k_1+N)-(k_2+N)=(k_1-k_2)+N\in\overline{K},$$

$$(r+N)(k_1+N)=rk_1+N\in\overline{K},$$

$$(k_1+N)(r+N)=k_1r+N\in\overline{K},$$

即 $k_1-k_2,rk_1,k_1r\in K$. 从而 $K\trianglelefteqslant R$，且 $\overline{K}=K/N$.

2) 因为 $H\trianglelefteqslant R$，且在自然同态下 H 的象为 K/N，则任取 $k+N\in K/N$，存在 $h\in H$，使 $h+N=k+N$. 即 $k-h\in N$. 令 $k-h=n$，则

$$k=h+n\in H+N,\quad K\subseteq H+N.$$

又任取 $h+n\in H+N,h\in H,n\in N$，则 $h+n$ 在自然同态之下的象为

$$h+n+N=h+N\in K/N.$$

故 $h+n\in K$，$H+N\subseteq K$. 因此 $K=H+N$，即 H 的象为 $(H+N)/N$.

§4．8 素理想和极大理想

一、主要内容

1．素理想和极大理想的定义和例子.

整数环 Z 的素理想为 $\{0\}$、Z 以及由任意素数 p 生成的理想 $<p>$，而且 $<p>$（p 为任意素数）还是 Z 的全部极大理想.

$<x>$，$<y>$，$<x,y>$ 以及 $<x,y,2>$ 都是环 $Z[x,y]$ 的素理想，而且 $<x,y,2>$ 还是 $Z[x,y]$ 的一个极大理想.

2．交换环 R 中，理想 P 是素理想 $\Leftrightarrow R/P$ 是整环.

在一般环 R 中，理想 N 是极大理想 $\Leftrightarrow R/N$ 是单环.

3．有单位元的可换单环必为域.

1) 设 R 是有单位元的交换环，$N\trianglelefteqslant R$. 则 R/N 是域 $\Longleftrightarrow$ N 是极大理想.

2) 有单位元的交换环中极大理想必为素理想.

二、释疑解难

1．关于素理想的定义.

多数的书都是在交换环中定义素理想. 但 1949 年麦珂(N. H. McCOY)推广为在任意环中定义素理想.

定义 设 P 是环 R(不一定可换)的一个理想. 若对 R 的任意理想 A,B 有

$$AB\subseteq P\Longrightarrow A\subseteq P\text{ 或 }B\subseteq P,$$

则称 P 为环 R 的一个素理想.

若 P 是现在意义下的素理想，则当 R 为交换环时 P 必为教材中所定义的素理想(即：$ab\in P\Longrightarrow a\in P$ 或 $b\in P$). 其证明留给读者作为练习

2. 在无单位元的环中，极大理想不一定是素理想.

例如在偶数环 R 中，

$$\langle 4\rangle=\{4r+4n\mid r\in R,n\in \mathbf{Z}\}=\{4n\mid n\in \mathbf{Z}\}$$
$$=\{\cdots,-12,-8,-4,0,4,8,12,\cdots\}$$

是极大理想：因为若有

$$\langle 4\rangle\subset N\trianglelefteq R,$$

则必有 $a\in N$，而 $a\notin\langle 4\rangle$. 从而可设 $a=2t$，其中 t 为奇数. 令 $t=2s+1$，则

$$a=2(2s+1)=4s+2,\quad 2=a-4s\in N.$$

从而 $N=R$.

但是，由于 $2\cdot 2=4\in\langle 4\rangle$，但 $2\notin\langle 4\rangle$，即 $\langle 4\rangle$ 不是 R 的素理想.

故极大理想 $\langle 4\rangle$ 不是素理想.

3. 素理想和极大理想的意义和作用.

由教材定理 1 可知，若 P 是交换环 R 的素理想，则 R/P 是整环；由定理 3、定理 4 和推论 1 可知，若 N 是有单位元的交换环 R 的极大理想，则 R/N 是一个域. 商环与原环关系密切，又整环特别是域更是性质较好的特殊环类. 这就是说，利用素理想和极大理想可得到一个与原环关系密切且性质又好的环，这对于研究原环 R 是非常重要和有利的. 这就是研究素理想和极大理想的意义和作用.

三、习题 4. 8 解答 1.

解 $\langle x\rangle$ 不是 $Z[x]$ 的极大理想，因为有

$\langle x\rangle=\{xf(x)\mid f(x)\in Z[x]\}\subset\{$常数项为偶数的整系数多项式$\}\lhd Z[x]$.

但是，$\langle x\rangle$ 是有理数域上多项式环 $Q[x]$ 的极大理想：因若

$$\langle x\rangle\subset N\trianglelefteq Q[x],$$

则有 $f(x)=xf_1(x)+a\in N$ $(0\neq a\in Q)$. 于是 $a\in N$，$N=Q[x]$，即 $\langle x\rangle$ 是 $Q[x]$ 的极大理想.

2. 证明：$\langle 4\rangle$ 是偶数环 R 的极大理想，但 $R/\langle 4\rangle$ 不是域.

证 $\langle 4\rangle$ 是 R 的极大理想，见上面“释疑解难”部分中的 2.

又易证商环

$$R/N=\{2k+\langle 4\rangle\mid k\in \mathbf{Z}\}$$

中没有单位元，从而不是域.

3.

解 1) 先证$\langle 2p\rangle$是 R 的极大理想：设若

$$\langle 2p\rangle \subset N \trianglelefteqslant R,$$

则有 $2k\in N$，但 $2k\notin\langle 2p\rangle$. 从而 $p\nmid k$，$(p,k)=1$. 故有

$$ps+kt=1 \quad (s,t\in \mathbf{Z}).$$

对 R 中任意偶数 $2m$，有

$$2m=2(ps+kt)m=2psm+2ktm\in N,$$

故 $N=R$.

反之，若$\langle 2m\rangle$是 R 的一个极大理想，则 m 必为素数. 因若 m 为合数，设

$$m=m_1m_2 \quad (1<m_i<m).$$

则$\langle 2m\rangle\subset\langle 2m_1\rangle\subset R$. 这与$\langle 2m\rangle$是极大理想矛盾.

因此，$\langle 2p\rangle$（p 为任意素数）是偶数环的全部极大理想.

2) 偶数环的全部素理想是：$\{0\}$，R 以及所有$\langle 2p\rangle$，其中 p 为任意奇素数.

教材本节例 2 已证明$\langle 2p\rangle$为素理想（p 为奇素数），而$\langle 4\rangle$不是素理想. 由于偶数环的理想均为主理想，下证当 m 为合数时$\langle 2m\rangle$不是素理想：设

$$m=m_1m_2 \quad (1<m_i<m). \qquad (1)$$

则由于 $2m_1\cdot 2m_2=4m\in\langle 2m\rangle=\{\cdots-2m,0,2m,4m,\cdots\}$，但是

$$2m_1,2m_2\notin\langle 2m\rangle.$$

因若 $2m_1\in\langle 2m\rangle$，设 $2m_1=2mk(k\in\mathbf{Z})$，得 $1=m_2k$，与(1)矛盾.

注 本题题目本身问法不合适，特别对理想$\langle 4\rangle$.

4.

解 1) 因为剩余类环是循环环，而循环环的子加群、子环和理想是一回事，因此 Z_6 的全部理想有 4 个，它们是：

$$R_1=\{\bar{0}\},\ R_2=\{\bar{0},\bar{3}\},\ R_3=\{\bar{0},\bar{2},\bar{4}\},\ Z_6.$$

由于 Z_6 有零因子，故 R_1 不是素理想，当然也不是极大理想. 再由 Lagrange 定理知，R_2 与 R_3 都是 Z_6 的极大理想，从而由推论 2 知，它们也是 Z_6 的素理想.

2) 理由同上，Z_{10}的素理想和极大理想都是

$$\{\bar{0},\bar{5}\},\quad \{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\}.$$

5.

证 设 R/N 是域，从而是单环. 于是由定理 3 知，N 是 R 的极大理想.

其次，设 $a\in R$ 且 $a^2\in N$，则在域 R/N 中有

$$\overline{a^2}=\overline{a}^2=\overline{0}.$$

从而必 $\overline{a}=\overline{0}$，即 $a\in N$.

反之，设 N 是 R 的极大理想且对 R 中任意 a 有 $a^2\in N$ 必有 $a\in N$. 令

$$N'=\{b+ar\mid b\in N, r\in R\},\ \text{且}\ a\notin N.$$

则易知 $N\subseteq N'\leqslant R$. 由于显然 $a^2\in N'$，但 $a^2\notin N$（否则将有 $a\in N$），故 $N\subset N'$. 但 N 是 R 的极大理想，故必 $N'=R$，于是对任 $c\in R$，总存在 $b\in N, r\in R$ 使

$$c=b+ar.$$

由此对于环 R/N 有 $\overline{c}=\overline{a}\,\overline{r}$. 即方程 $\overline{a}x=\overline{c}$ $(\overline{a}\neq\overline{0})$ 在 R/N 中有

解. 又由于 R 可换，从而 R/N' 可换. 故 R/N 是域.

§4. 9 环与域上的多项式环

一、主要内容

1. 有单位元环 R 上多项式环 $R[x]$ 的性质.

1) $R[x]$ 是整环 $\Leftrightarrow$ R 是整环.

2) $R[x]$ 中多项式的除法——左、右商及左、右余式.

2. 域 F 上多项式的根.

1) F 上 n 次多项式在扩域内根的个数 $\leqslant n$;

2) F 上多项式 $f(x)$ 在扩域内无重根 $\Leftrightarrow (f(x),\ f'(x))=1$.

二、释疑解难

1. 本节均假定环 R 有单位元，但并未假定 R 可换. 因此，在对 R 上的多项式在进行除法时，必须分左、右商和左、右余式. 从本节习题中可知，一般说左右商不一定相等，左右余式也不一定相等. 当然，如果 R 是交换环，它们则分别相等，就不必再分左与右了.

2. 域上多项式的根的状况同我们所熟知的数域上多项式的情况一致. 但是，环上多项式根的状况，由例子可知，就很不一样. 例如，环 R 上一个 n 次多项式在 R 内可能无根（这种情况并不奇怪，因为例如有理数域上多项式在有理数域内也不一定有根），也可能有多于 n 个的根（这种情况在数域或域上多项式不会发生）. 不过，教材中除下一章惟一分解整环的多项式扩张外. 主要用到场上的多项式. 例如教材第六章中的最小多项式和多项式的分裂域就属于这种情况.

三、习题 4. 9 解答

1.

证 令 φ: $f(x)\longrightarrow f(a)$ $(\forall f(x)\in R[x])$. 则易知 φ 是环 $R[x]$ 到 $R[a]$ 的一个同态满射，故

$$R[x]\sim R[a].$$

2.

解 例如，环 $Z_6[x]$ 中多项式

$$f(x)=\overline{2}x^3+x^2-\overline{3}x+\overline{5}\quad 与\quad g(x)=\overline{3}x^2+\overline{1}$$

的乘积 $f(x)g(x)=\overline{3}x^4-x^3+\overline{4}x^2-\overline{3}x+\overline{5}$ 就不是 3+2 次多项式.

3. 解　经验算得知，$f(x)$在Z_5上无根.

4.

解　经验算得知，Z_3上的2次不可约多项式有三个，它们是：

$$x^2+\bar{1},\quad x^2+x-\bar{1},\quad x^2-x-\bar{1}.$$

5.

证　设G是F^*的一个n阶子群. 现取G的一个最大阶元a，并设$|a|=m$. 由于G是交换群，故G中每个元素都满足方程

$$x^m-1=0.$$

但域上m次方程在F中最多有m个根，故$n\leqslant m$. 而由 Lagrange 定理知，$m|n$. 从而$m=n$且$G=\langle a\rangle$.

6.

解　右商和右余式分别为：

$$q_1(x)=\begin{pmatrix}0 & 0\\ 2 & 1\end{pmatrix}x+\begin{pmatrix}1 & 1\\ -2 & -1\end{pmatrix},\quad r_1=\begin{pmatrix}2 & 0\\ 1 & 1\end{pmatrix};$$

左商和左余式分别为：

$$q_2(x)=\begin{pmatrix}1 & -2\\ 0 & 0\end{pmatrix}x+\begin{pmatrix}1 & -1\\ 0 & -1\end{pmatrix},\quad r_2=\begin{pmatrix}1 & 0\\ 1 & 2\end{pmatrix}.$$

* §10　分　式　域

一、主要内容

1. 设R是个阶大于1的整环，则在同构意义下由定理2可知，包含R的域总是存在的. 那么在这个域中一切元素

$$\frac{b}{a}=a^{-1}b\quad(a,b\in R,a\neq 0)$$

作成一个包含R为其子环的域，即所谓R的分式域.

2. 同构的整环其分式域也同构. 因此，在同构意义下整环的分式域不仅存在，而且是惟一的.

二、释疑解难

1. 定理1不仅给出了分式域的定义，而且启发我们如何寻找构造分式域的方法.

2. 定理2不仅指出了整环的分式域一定存在，而且指出了分式域的具体构造方法.

按照定理2所指出的方法，用$\frac{b}{a}$表示

$$M=\{(x,y)\mid x,y\in R,x\neq 0\}$$

中元素(a,b)所在的等价类. 而令

$$F=\left\{\frac{b}{a}\,\middle|\,a,b\in R,a\neq 0\right\}.$$

则 F 对于普通分式的加法与乘法作成一个域. 这就是整环 R 的分式域.

整环 R 的分式域就是包含 R 的最小域. 也就是说，包含 R 的任意一个域必包含 R 的分式域.

3. 按照定理 2 的证明，在映射 $\varphi:a\longrightarrow\frac{ab}{b}$ （$\forall a,b\in R$，但 $b\neq 0$）之下，

$$R\cong S=\left\{\frac{ab}{b}\,\middle|\,a\in R,b\neq 0\right\}.$$

这样，根据挖补定理，把 R 中元素 a 与 F 中元素$\frac{ab}{b}$等同起来，即规定

$$a=\frac{ab}{b},$$

于是 $F\supseteq R$，且 R 是分式域 F 的子环，通常把这个事实称之为“把环 R 同构嵌入到域 F 中”.

4. 整环（可换且无零因子）可以同构嵌入到一个域中. 那么一个无零因子的非交换环（因为非交换，当然不能同构嵌入到域中）是否可以同构嵌入到一个除环中呢？也就是是否可以被包含在一个除环中呢？在近世代数中，有时举一个反例并不容易，甚至是很困难的. 到 1936 年才由苏联数学家马尔采夫（A. Malcev，1909—1967）发表论文给出一个无零因子非交换环不被除环包含的例子.

5. 更一般的，设 R 是一个交换环（有无零因子不限制），S 是 R 中所有非零因子作成的集合. 显然 S 对 R 的乘法作成一个半群. 同定理 2 类似，R 可以同构嵌入到环

$$\overline{R}=\left\{\frac{b}{a}\,\middle|\,b\in R,a\in S\right\}$$

中. 这个环 $\overline{R}$ 称为 R 的分式环. 它显然是分式域概念的推广.

三、习题 4.10 解答

1. 证明：域 F 的分式域就是自身.

证 因为 F 是域，故对 F 中任意元素 $a\neq 0,b$ 有

$$\frac{b}{a}=a^{-1}b\in F,\quad \text{即得.}$$

2. 证明定理 2 中集合 M 的元素间的关系

$$(a,b)\sim(c,d)\Longleftrightarrow ad=bc$$

是一个等价关系.

证 反身性和对称性显然. 下证满足传递性.

设$(a,b)\sim(c,d)$，$(c,d)\sim(s,t)$，其中 $acs\neq 0$. 则

$$ad=bc,\quad ct=ds. \tag{1}$$

从而 $adct=bcds$. 但 R 是整环，消去律成立，又 $c\neq 0$，故

$$adt=bds. \tag{2}$$

若 $d=0$，则由(1)可知 $b=t=0$，从而 $at=bs$；若 $d\neq 0$，从(2)中消去 d，亦得 $at=bs$. 因此，$(a,b)\sim(s,t)$.

3. 证明定理 2 中的 φ 是 R 到 S 的一个同构映射.

证 φ 是满射显然. 又若

$$\frac{ab}{b}=\frac{cb}{b},\quad \text{即 } ab^2=cb^2.$$

则因 R 是整环，消去律成立，又 $b^2\neq 0$，故 $a=c$，即 φ 是单射，从而 φ 是双射. 又

$$\varphi(a+c)=\frac{(a+c)b}{b}=\frac{ab}{b}+\frac{cb}{b}=\varphi(a)+\varphi(c),$$

$$\varphi(ac)=\frac{ac\cdot b}{b}=\frac{ab}{b}\cdot\frac{cb}{b}=\varphi(a)\varphi(c),$$

故 φ 是 R 到 S 的同构映射.

4. 问：Gauss 整环 $Z[i]$ 的分式域为何？

解 由于 $Z[i]$ 包含整数环 Z，并包含元素 i，因此，$Z[i]$ 的分式

域为：

$$Q(i)=\{a+bi\mid a,b\in Q\}.$$

5. 设 p 是一个素数. 证明：

$$R=\left\{\frac{m}{n}\mid m,n\in Z,(n,p)=1\right\}$$

是一个整环，并求其分式域.

证 R 是整环显然. 又其分式域为有理数域 Q.

* §11 环的直和

一、主要内容

1. 环的外直和与内直和的定义和例子
2. 环是其子环的直和的充要条件.

设 R 为环，$R_i\lhd R(i=1,2,\cdots,n)$. 又 $R=R_1+R_2+\cdots+R_n$. 则

$$R=R_1\oplus R_2\oplus\cdots\oplus R_n\Longleftrightarrow \text{零元素表示法惟一}$$

$$\Longleftrightarrow R_i\cap\sum_{j\neq i}R_j=\{0\}(i=1,2,\cdots,n).$$

3. 直和的性质.

1) 直和项的理想也是原环的理想；

2) 设环 $R=\sum_{i=1}^{m}\oplus R_i$，若 $N_i\lhd R_i(i=1,2,\cdots,m)$，则

$$\sum_{i=1}^{m}\oplus N_i\lhd R.$$

反之，若 $N\lhd R$，则当 R 有单位元时有 $N_i\lhd R$，使

$$N=N_1\oplus N_2\oplus\cdots\oplus N_m.$$

3) 环的直和的特征：若 $\text{char } R=n=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$（$p_1,p_2,\cdots,p_m$ 为互异素数，$k_i\geqslant 1$），则有

$$R=R_1\oplus R_2\oplus\cdots\oplus R_m,$$

其中 $\text{char } R_i=p_i^{k_i}(i=1,2,\cdots,m)$.

二、释疑解难

1. 定理 1 指出，理想的和 $R=\sum_{i=1}^{n}R_i$ 是直和$\Longleftrightarrow$零元素表示法惟一.

其实，“零元素表示法惟一”也可改为“R 中任意一个固定元素表示法惟一”. 证明如下：

任取 $a\in R$，令

$$a=a_1+a_2+\cdots+a_n\quad(a_i\in R_i),\tag{1}$$

并假定 a 的表示法惟一. 又任取 $x\in R$，设

$$x=x_1+x_2+\cdots+x_n=y_1+y_2+\cdots+y_n,$$

其中 $x_i,y_i\in R_i$. 则

$$0=(x_1-y_1)+(x_2-y_2)+\cdots+(x_n-y_n).$$

于是由(1)得

$$a=(a_1+x_1-y_1)+(a_2+x_2-y_2)+\cdots+(a_n+x_n-y_n).\tag{2}$$

由于 a 的表示法惟一，(1)与(2)两式比较得

$$x_1=y_1,\ x_2=y_2,\ \cdots,\ x_n=y_n.$$

即 R 中每个元素表示法惟一.

2. 关于环按特征的分解.

教材中定理 5 和定理 6 可以合并为以下更一般的定理：设环 R 的特征是 $n=n_1n_2\cdots n_s$. 若正整数 $n_1,n_2,\cdots,n_s$ 两两互素，则 R 有理想 $R_1,R_2,\cdots,R_s$ 使

$$R=R_1\oplus R_2\oplus\cdots\oplus R_s,$$

而且其中 $\text{char } R_i=n_i\ (i=1,2,\cdots,s)$.

这个定理的证明可对 s 用数学归纳法，留给读者作为练习.

3. 直和的重要意义.

1) 若 $R=R_1\oplus R_2\oplus\cdots\oplus R_n$，则 R 的运算决定于每个环 $R_i(R$

的理想)的运算;R 是否有单位元或可换,决定于每个 R_i 是否有单位元或可换.或者说,R 的结构决定于每个 R_i 的结构.而一般来说,R_i 的构造相对简单,从而可利用 R_i 来讨论 R.

2) 从理想来说,教材定理 3 和定理 4 说明,每个 R_i 的理想与其直和 R 的理想关系密切.而且在一定条件下 R 的理想也决定于每个 R_i 的理想.

3) 定理 5 与定理 6 指明环的特征与直和的关系.就是说讨论特征为 n 的环,可转化为讨论特征是素数幂的环.

三、习题 4.11 解答

1. 设环 $R=R_1\oplus R_2\oplus\cdots\oplus R_n$.证明:环 R 有单位元当且仅当每个理想 R_i 有单位元.并且

$$1=1_1+1_2+\cdots+1_n,$$

其中 1 是 R 的单位元,1_i 是 R_i 的单位元.

证 设 R 有单位元,用 1 表示.由于

$$R=R_1\oplus R_2\oplus\cdots\oplus R_n,$$

故可设

$$1=1_1+1_2+\cdots+1_n,\quad 1_i\in R_i$$

任取 $x_i\in R_i$,则

$$x_i=1x_i=(1_1+1_2+\cdots+1_n)x_i=1_ix_i.$$

同理有 $x_i=x_i1_i$.因此,1_i 为 R_i 的单位元.

反之,设 1_i 是 R_i 的单位元,且

$$e=1_1+1_2+\cdots+1_n,$$

则对任意 $r\in R$,令

$$r=r_1+\cdots+r_i+\cdots+r_n,$$

有
$$\begin{aligned}re&=(r_1+\cdots+r_i+\cdots+r_n)(1_1+\cdots+1_i+\cdots+1_n)\\&=r_11_1+\cdots+r_i1_i+\cdots+r_n1_n\\&=r_1+\cdots+r_i+\cdots+r_n=r.\end{aligned}$$

同理有 $er=r$.即 $e=1$ 是 R 的单位元.

注 在题设条件下,当 R 有单位元(用 1 表示)时,还可证明

$$R_i=R1_i=1_iR\quad(i=1,2,\cdots,n).$$

事实上,因为 $1_i\in R_i\leqslant R$,故

$$R1_i\subseteq R_i,\quad 1_iR\subseteq R_i.$$

又任取 $x_i\in R_i$,则由于

$$x_i=1_ix_i\in 1_iR,\quad x_i=x_i1_i\in R1_i,$$

故 $R_i\subseteq 1_iR$,$R_i\subseteq R1_i$.从而

$$R_i=R1_i=1_iR,\quad(i=1,2,\cdots,n).$$

2. 设 $Z_2=\{0,1\}$,且

$$R=\{(a_1,a_2,\cdots,a_n)\mid a_i\in Z_2\}.$$

即 R 是 n 个环 Z_2 的外直和.证明:R 是一个布尔环.又 R 的特征为何?

证 因为 $a_i\in Z_2$,故 $a_i^2=a_i$.从而

$$(a_1,a_2,\cdots,a_n)^2=(a_1,a_2,\cdots,a_n),$$

即 R 是布尔环.又明显 R 的特征是 2.

3. 设环 R 是环 $R_1,R_2,\cdots,R_n$ 的直和,即

$$R=R_1\oplus R_2\oplus\cdots\oplus R_n.$$

证明:$\varphi_i:\ a_1+\cdots+a_i+\cdots+a_n\longrightarrow a_i$ 是 R 到 R_i 的同态满射(称为正则投射),且

1) $\varphi_i\varphi_j=\begin{cases}\varphi_i, & i=j\\ 0, & i\neq j;\end{cases}$ 2) $\varphi_1+\varphi_2+\cdots+\varphi_n=\varepsilon.$

其中 0 是零同态,ε 是 R 的恒等变换.

证 显然 φ_i 是满射.又在 R 中任取

$$a=a_1+\cdots+a_i+\cdots+a_n,\quad b=b_1+\cdots+b_i+\cdots+b_n,$$

有

$$ab=a_1b_1+\cdots+a_ib_i+\cdots+a_nb_n,$$

$$a+b=(a_1+b_1)+\cdots+(a_i+b_i)+\cdots+(a_n+b_n).$$

即 $\varphi_i(ab)=\varphi_i(a)\varphi_i(b)$,$\varphi_i(a+b)=\varphi_i(a)+\varphi_i(b)$.

所以 φ_i 是同态满射.

由上又可知，

$$\varphi_i^2(a)=\varphi_i(a_i)=a_i,\quad \varphi_i\varphi_j(a)=\varphi_i(a_j)=0\ (i\neq j).$$

因此，$\varphi_i^2=\varphi_i$，$\varphi_i\varphi_j=0\ (i\neq j)$，即 1)成立.

又$(\varphi_1+\varphi_2+\cdots+\varphi_n)(a)=\varphi_1(a)+\cdots+\varphi_n(a)$

$$=a_1+\cdots+a_n=a,$$

故 $\varphi_1+\varphi_2+\cdots+\varphi_n=\varepsilon$，即 2)成立.

4. 设 N 是环 R 的一个理想. 证明：如果 N 有单位元，则 N 是 R 的一个直和项，即存在 R 的理想 N' 使

$$R=N\oplus N'.$$

证　用 e 表示理想 N 的单位元，并令

$$N'=\{x\mid x\in R, xe=ex=0\}.$$

显然 $0\in N'$，故 N' 非空. 又设 $x,y\in N'$，则

$$xe=ex=0,\quad ye=ey=0,$$

于是

$$(x-y)e=e(x-y)=0,\quad x-y\in N'.$$

又对任意 $r\in R$，由于 e 是 N 的单位元，故 $re\in N$，从而

$$re=e(re).$$

再根据 $xe=ex=0$，得

$$(xr)e=x(re)=x(ere)=xe(re)=0,$$

$$e(xr)=(ex)r=0,\quad \text{于是}(xr)e=e(xr)=0.$$

故 $xr\in N'$.

同理有 $rx\in N'$. 因此 $N'\trianglelefteqslant R$.

又设 $x\in N\cap N'$，则 $x\in N$，$xe=x$. 但 $x\in N'$，故 $xe=0$，从而 $x=0$. 所以 $N\cap N'=\{0\}$.

任取 $r\in R$，则 $re=a\in N$，且

$$ae=(re)e=re,\quad (r-a)e=0.$$

同理，由于 $er\in N$，e 是 N 的单位元，故 $er=ere$，从而 $e(r-a)=0$，于是

$$r-a=b\in N',\quad r=a+b\in N\oplus N'.$$

所以 $R=N\oplus N'$.

5.

证　令

$$\varphi:\bar{x}\longrightarrow(\bar{x},\bar{x},\cdots,\bar{x}),$$

其中箭号左边的 $\bar{x}\in Z_{n_1n_2\cdots n_s}$，而$(\bar{x},\bar{x},\cdots,\bar{x})$中第 1 个 $\bar{x}\in Z_{n_1}$，第 2 个 $\bar{x}\in Z_{n_2}$，…，第 s 个 $\bar{x}\in Z_{n_s}$. 就是说，同一个符号 $\bar{x}$ 由于所在位置不同，其所表示的元素也不一样.

若$(\bar{x},\bar{x},\cdots,\bar{x})=(\bar{y},\bar{y},\cdots,\bar{y})$，则

$$n_i\mid x-y\quad (i=1,2,\cdots,s).$$

但 $n_1,n_2,\cdots,n_s$ 两两互素，故

$$n_1n_2\cdots n_s\mid x-y.$$

从而在环 $Z_{n_1n_2\cdots n_s}$ 中，$\bar{x}=\bar{y}$，即 φ 为单射. 又由于 $Z_{n_1n_2\cdots n_s}$ 的阶与直和 $Z_{n_1}\oplus Z_{n_2}\oplus\cdots\oplus Z_{n_s}$ 的阶相同，都是 $n_1n_2\cdots n_s$，因此 φ 是双射. 又显然 φ 保持加法与乘法运算，因此 φ 是同构映射. 从而得证.

6. 证　1)　在 R 中任取元素 r_1,r_2,r. 由于

$$(r_1-r_1e)-(r_2-r_2e)=(r_1-r_2)-(r_1-r_2)e,$$

$$r_1(r-re)=r_1r-r_1re,$$

故 $R(1-e)$是环 R 的左理想.

同理,$(1-e)R$ 是环 R 的右理想.

2) 因为 $er_1e\cdot er_2e=e(r_1er_2)e$,并且

$$er_1e-er_2e=e(r_1-r_2)e,$$

故 $eRe\leqslant R$. 同理,由于 e 是 R 的幂等元,故

$$(er_1-er_1e)(er_2-er_2e)$$

$$=er_1er_2-er_1er_2-er_1er_2e+er_1er_2e=0.$$

从而 $eR(1-e)$是 R 的子环且为零乘环.

$(1-e)Re$ 也是 R 的零乘子环.

3) 任取 $r\in R$,则有

$$r=re+(r-re)\in Re+R(1-e),$$

故 $R=Re+R(1-e)$.

又任取 $x\in Re\cap R(1-e)$,令

$$x=r_1e=r_2-r_2e\quad(r_1,r_2\in R).\tag{2}$$

由于 $e^2=e$,故由(2)知:

$$x=r_1e=r_1e^2=(r_1e)e=(r_2-r_2e)e=0.$$

因此,$Re\cap R(1-e)=\{0\}$. 从而 $R=Re\oplus R(1-e)$.

同理,$R=eR\oplus(1-e)R$.

最后,任取 $r\in R$,则显然有

$$r=ere+(er-ere)+(re-ere)+(r-er-re+ere),$$

故 $R=eRe+eR(1-e)+(1-e)Re+(1-e)R(1-e)$.

又若

$$0=er_1e+(er_2-er_2e)+(r_3e-er_3e)+$$

$$(r_4-er_4-r_4e+er_4e),\tag{3}$$

左右两端乘 e,得 $er_1e=0$;然后(3)式左乘 e 可得

$$er_2-er_2e=0;$$

而后再用 e 右乘(3)式两端,可得 $r_3e-er_3e=0$. 从而又有

$$r_4-er_4-r_4e+er_4e=0.$$

即 0 表示法惟一,故为直和. 即(1)式成立.

* §12 非交换环

一、主要内容

1. 对任意整数 $n>1$,构造 n^2 阶非交换环的方法.

令 $R=(Z_n,+)\oplus(Z_n,+)$. 加法如常,乘法规定如下:

$$(x_1,y_1)(x_2,y_2)=(x_2+y_2)(x_1,y_1).$$

则 R 就是一个 n^2 阶非交换环.

2. 对任意素数 p 与任意整数 $n>1$,构造 p^s 阶非交换环的方法. 其中 $s=\dfrac{n(n+1)}{2}$.

域 Z_p 上一切 n 阶上三角矩阵关于矩阵的普通加法与乘法,作成一个 p^s 阶的非交换环.

3. 存在 n 阶非交换环的充要条件.

对整数 $n>1$,存在 n 阶非交换环 $\Longleftrightarrow$ n 有平方因子.

二、释疑解难

1. 非交换环是一类重要的环,它也是环论中重要的研究对象之一. 本节利用环的直和与有限交换群基本定理,对于非交换环的讨论虽然是初步的,但也比较完整. 它指出一个根本问题,即对于什么样的正整数 n 才能有 n 阶非交换环.

2. 另外,定理 1、2、3 证明本身也同时给出了 n(有平方因子)阶非交换环的构造方法.

通过这些讨论,也进一步看出环的直和的重要作用.

三、习题 4.12 解答

1. 验算 §12 定理 1 证明中给出的环 R 的结合律(对乘法)

成立.

解 因为易知

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

都等于$(x_2+y_2)(x_3+y_3)(x_1,y_1)$，故 R 对乘法满足结合律.

2. 问：§12 定理 1 给出的环 R 是否有单位元？为什么？

解 R 没有单位元. 因若不然，设(a,b)是 R 的单位元，则

$$(a,b)(1,0)=(a,b)=(1,0),$$

$$(a,b)(0,1)=(a,b)=(0,1).$$

于是 $n|a-1, n|a$. 这与 $n>1$ 矛盾.

3. 给出 §12 例 1 中 4 阶非交换环 R_1 的乘法表，并证明环 R_1 与环 R_2 不同构.

证 用 $0,x,y,z$ 依次表示环 R_2 中的 4 个元素(即 Z_2 上的 4 个 2 阶方阵)，则非交换环 R_1 与 R_2 的乘法表分别为：

·	0	a	b	c
0	0	0	0	0
a	0	a	a	0
b	0	b	b	0
c	0	c	c	0

·	0	x	y	z
0	0	0	0	0
x	0	x	y	z
y	0	x	y	z
z	0	0	0	0

反证法. 设若 $R_1\cong R_2$，且 φ 为其一同构映射，则除 $\varphi(0)=0$ 外，设

1) $\varphi(a)=x, \varphi(b)=y$. 则必 $\varphi(ab)=\varphi(a)\varphi(b)$. 则由乘法表知，即

$$\varphi(a)=xy=y, \quad \text{矛盾；}$$

若 $\varphi(b)=z$，则由 $\varphi(ab)=\varphi(a)\varphi(b)$，得

$$\varphi(a)=xz=z, \quad \text{也矛盾.}$$

2) $\varphi(a)=y, \varphi(b)=x$，则同样由 $\varphi(ab)=\varphi(a)\varphi(b)$，得

$$\varphi(a)=yx=x, \quad \text{矛盾；}$$

若 $\varphi(b)=z$. 则由 $\varphi(ab)=\varphi(a)\varphi(b)$ 得 $\varphi(a)=yz=z$，矛盾.

3) $\varphi(a)=z, \varphi(b)=x$，则由 $\varphi(ab)=\varphi(a)\varphi(b)$ 得

$$\varphi(a)=zx=0, \quad \text{矛盾；}$$

若 $\varphi(b)=y$，则由 $\varphi(ab)=\varphi(a)\varphi(b)$ 得 $\varphi(a)=zy=0$，矛盾. 因此，R_1 与 R_2 不能同构.

4. 令 R_1' 为由 Z_2 上 4 个二阶方阵

$$\begin{pmatrix}0&0\\0&0\end{pmatrix}, \quad \begin{pmatrix}0&0\\0&1\end{pmatrix}, \quad \begin{pmatrix}0&1\\0&1\end{pmatrix}, \quad \begin{pmatrix}0&1\\0&0\end{pmatrix}$$

关于方阵的普通加法与乘法作成的环. 证明：§12 例 1 中的环 R_1 与这个环 R_1' 同构.

证 显然，R_1 与 R_1' 对加法都作成一个 Klein 四元群.

再列出 R_1' 的乘法表，并令(参考上题)

$$\varphi: \quad 0\longrightarrow\begin{pmatrix}0&0\\0&0\end{pmatrix}, \quad a\longrightarrow\begin{pmatrix}0&0\\0&1\end{pmatrix},$$

$$b\longrightarrow\begin{pmatrix}0&1\\0&1\end{pmatrix}, \quad c\longrightarrow\begin{pmatrix}0&1\\0&0\end{pmatrix}.$$

从而可知 φ 是环 R 到 R_1' 的同构映射. 故 $R_1\cong R_1'$.

5. 给出两个不同构的 12 阶非交换环.

解 令 R_2 为上面第 3 题中所说的非交换环，即由 Z_2 上 4 个 2 阶方阵

$$\begin{pmatrix}0&0\\0&0\end{pmatrix}, \quad \begin{pmatrix}1&0\\0&0\end{pmatrix}, \quad \begin{pmatrix}1&1\\0&0\end{pmatrix}, \quad \begin{pmatrix}0&1\\0&0\end{pmatrix}$$

关于方阵普通加法与乘法作成的环. 则例 2 中的环

$$R=R_1\oplus Z_3$$

与环的直和 $R'=R_2\oplus Z_3$ 都是 12 阶非交换环. 但它们不同构：

因若 $R\cong R'$，则由于

$$R_1\cong R/Z_3\cong R'/Z_3\cong R_2,$$

从而 $R_1\cong R_2$. 这与第 3 题的结论矛盾.

6. 给出两个不同构的无限非交换环.

解 令 F 是整数环 Z 上的 2 阶全阵环，又 Z_2 是模 2 剩余类环，则 F 与 $F\oplus Z_2$ 都是无限非交换环，但二者不能同构，因为直和 $F\oplus Z_2$ 有 2 阶子环，但 F 显然没有 2 阶子环.

7. 证明：若 e 是环 R 的惟一的左单位元，则 e 必是 R 的单位元.

证 任取 $a,b\in R$，则因 e 是 R 的左单位元，故

$$(ae-a+e)b=a(eb)-ab+eb=ab-ab+b=b,$$

即 $ae-a+e$ 也是 R 的左单位元. 于是由题设得

$$ae-a+e=e,\quad \text{故 } ae=a.$$

即 e 是 R 的单位元.

8. 设 R 是一个有单位元(用 1 表示)的环，$a,b\in R$. 证明：如果 $1+ab$ 在 R 中有逆元，则 $1+ba$ 在 R 中也有逆元.

证 令 c 是 $1+ab$ 的逆元，即有

$$c(1+ab)=(1+ab)c=1,$$

或 $c-1+cab=c-1+abc=0$. 于是有

$$\begin{aligned}(1-bca)(1+ba)&=1-bca+ba-bcaba\\&=1-b[c-1+cab]a=1,\\(1+ba)(1-bca)&=1+ba-bca-babca\\&=1-b[c-1+abc]a=1.\end{aligned}$$

即 $1-bca$ 是 $1+ba$ 的逆元.

9. 设 R 是一个有单位元的环. 如果 R 中元素 a,b 有 $ab=1$，则称 b 是 a 的一个右逆元，而称 a 是 b 的一个左逆元. 证明卡普兰斯基(I. Kaplansky)定理：设 R 是一个有单位元(用 1 表示)的环，如果 R 中元素 a 有一个以上的右逆元，则 a 必有无限多个右逆元.

证法 I 设 a 只有有限个右逆元，它们是 $a_1,a_2,\cdots,a_m$. 则由题设 $m\geqslant 2$，且

$$aa_1=1,\quad aa_2=1,\quad \cdots,\quad aa_m=1. \tag{1}$$

由此可得

$$a(1-a_ia+a_i)=1\quad (i=1,2,\cdots,m).$$

又当 $i\neq j$ 时，$1-a_ia+a_i\neq 1-a_ja+a_j$：因若

$$1-a_ia+a_i=1-a_ja+a_j,$$

则有 $a_ia=a_ja$. 两边右乘 a_i 得 $a_i=a_j$，矛盾. 这就是说

$$1-a_ia+a_i\quad (i=1,2,\cdots,m)$$

是 a 的全部右逆元，故必存在 k，使

$$a_1=1-a_ka+a_1,$$

从而

$$a_ka=1. \tag{2}$$

又因 $m\geqslant 2$，故有 $s\neq k$，$1\leqslant s,k\leqslant m$. 用 a_s 右乘(2)式两端并根据(1)可得

$$a_kaa_s=a_s,\quad a_k=a_s.$$

这与 $a_1,a_2,\cdots,a_m$ 是 a 的互不相同的右逆元相矛盾，从而 a 必有无限多个右逆元.

证法 II 令 $S=\{x\mid x\in R,ax=1\}$，$T=\{xa-1+s\mid x\in S\}$，其中 s 是 S 中一个固定元素. 显然

$$\varphi:\quad x\longrightarrow xa-1+s\quad (\forall\, x\in S)$$

是 S 到 T 的一个满射. 又若

$$xa-1+s=ya-1+s\quad (x,y\in S)$$

则有

$$xa=ya,\quad xax=yax,\quad x=y.$$

即 φ 也是单射，从而为双射. 因此，$|T|=|S|$.

如果 S 有限，则由于显然 $T\subseteq S$，故 $T=S$ 且

$$s\in S=T,\quad s=xa-1+s,\quad xa=1.$$

这与 a 有一个以上右逆元(即 $|S|\geqslant 2$)矛盾. 故必 S 无限，即 a 有无限个右逆元.

10. 设 R 是一个有单位元的环，a 与 b 是 R 的单位(即可逆元). 证明：若有二互素的整数 m 和 n 使

$$a^m=b^m,\quad a^n=b^n,$$

则必 $a=b$.

证 因为$(m,n)=1$,故有整数 s,t 使 $ms+nt=1$. 于是

$$a=a^{ms+nt}=a^{ms}a^{nt}=(a^m)^s(a^n)^t,$$

$$b=b^{ms+nt}=b^{ms}b^{nt}=(b^m)^s(b^n)^t.$$

但是 $a^m=b^m$,$a^n=b^n$,故 $a=b$.

11. 设 R 为布尔环,即环 R 中每个元素 x 都有 $x^2=x$. 证明:若$|R|\geqslant 3$,则 R 不是整环.

证 反证法. 假设 R 是整环,则 R 无零因子.

因为$|R|\geqslant 3$,故 R 中有互异的元素 $a\neq 0,b\neq 0$. 由 $a^2=a$ 得

$$(a^2-a)b=a(ab-b)=0.$$

因 R 是整环,无零因子,$a\neq 0$,于是由上得

$$ab-b=0,\quad ab-b^2=0,\quad (a-b)b=0.$$

但 $b\neq 0$,于是又得 $a=b$,矛盾. 因此,R 不是整环.

12. 设 R 是一个 Jacobson 环,即对 R 中每个元素 a 都有与 a 有关的整数 $n>1$ 使 $a^n=a$. 证明:R 的幂等元都是中心元.

证 设 $a^2=a$,则易知$(axa-ax)^2=(axa-xa)^2=0$. 于是由习题 4.2 第 5 题知:$axa-ax=axa-xa=0$. 从而

$$axa=ax=xa\quad(\forall x\in R).$$

即 a 是 R 的中心元.

13. 设 R 是一个有单位元(用 1 表示)的有限环. 证明:如果 $ab=1$,则 $ba=1$.

证 因为 $ab=1$,故若 $bx=0$ $(x\in R)$,则

$$x=(ab)x=a(bx)=a\cdot 0=0,$$

即 b 不是左零因子.

于是,对 $x,y\in R$,$x\neq y$ 有 $bx\neq by$. 这样,因为 R 是有限环,令 $R=\{a_1,a_2,\cdots,a_n\}$,则便有

$$R=\{ba_1,ba_2,\cdots,ba_n\}.$$

由于 $1\in R$,故存在 $a_i\in R$,使 $ba_i=1$. 两边左乘 a,由 $ab=1$ 得

$$a(ba_i)=(ab)a_i=a_i.$$

又因为 $a(ba_i)=a\cdot 1=a$,故 $a_i=a$,从而得 $ba=1$.

14. 若对环 R 中每个元素 a 都有 $a'\in R$(a' 与 a 相关)使 $a=aa'a$,则称 R 为正则环. 证明:

1) p -环是正则环. 但反之不成立;

2) 再指出正则环的子环不一定是正则环;

3) 对正则环 R 中任二元素 a,b,都有 R 中幂等元 e_1,e_2 使

$$Ra=Re_1,\quad Ra+Rb=Re_2.$$

证 1) 设 R 是一个 p -环,若 $p=2$,则由于 $a^2=a$,从而有 $a^3=a$,即方程

$$axa=a$$

在 R 中有解 $x=a$,因此 R 是正则环.

若 $p>2$,则因 $a^p=a$,故 a^{p-2} 满足 $axa=a$,从而 R 是正则环.

又除环和域显然都是正则环. 但由 §2 知,p -环是可换环,因而是非可换除环,例如四元数除环是正则环,但非 p -环.

2) 例如,有理数域是正则环,但其子环整数环显然不是正则环.

3) 因 R 是正则环,故存在 $x\in R$ 使 $axa=a$.

令 $e_1=xa$,则 $e_1^2=e_1$. 显然 $Re_1\subseteq Ra$;又因 $a=ae_1$,故

$$Ra=Rae_1\subseteq Re_1,\quad Ra=Re_1.$$

又因为 $Ra=Re_1$,$e_1=xa$,且易知

$$Rb\subseteq Rbe_1+R(b-be_1),$$

故

$$Ra+Rb=Re_1+R(b-be_1).\tag{1}$$

由(1)设 $R(b-be_1)=Re$,其中 $e=e^2\in Re$,故

$$e\in R(b-be_1).$$

令 $e=r(b-be_1)$,由此可知 $ee_1=0$. 再令 $e_3=e-e_1e$,得

$$ee_3=e,\quad e_3^2=e_3e=e_3,\quad e_1e_3=e_3e_1=0.\tag{2}$$

又因 $e_3\in Re$,$e\in Re_3$,故 $Re=Re_3$. 从而由(1)得

$$Ra+Rb=Re_1+Re_3.\tag{3}$$

最后令 $e_2=e_1+e_3$,则由(2)知 $e_2^2=e_2$,且

$$r_1e_1+r_2e_3=(r_1e_1+r_2e_3)(e_1+e_3)\in Re_2,$$

故 $Re_1+Re_3=Re_2$. 从而由(3)知

$$Ra+Rb=Re_2.$$

15. 设 R 是一个正则环. 证明：若 R 中元素 a 对 R 中任意元素 x 都存在 $b\in R$ 使

$$ax+b+axb=0,$$

则 $a=0$.

证 因为 R 是正则环，故存在 $c\in R$，使 $aca=a$. 又由假设，对元素 $(-c)$ 存在 $b\in R$，使

$$a(-c)+b+a(-c)b=0. \tag{1}$$

用 ac 从左边乘(1)式两端，得

$$-acac+acb-acacb=0. \tag{2}$$

但是 $aca=a$，故由(2)式可得：$-ac-acb-acb=0$. 从而

$$-ac=0,\quad ac=0,\quad a=aca=0\cdot a=0.$$

16. 设 $C_n=\langle a\rangle$ 为 n 阶循环群，Z_n^* 为模 n 剩余类环 Z_n 的单位群. 证明：

$$\mathrm{Aut}C_n\cong Z_n^*;$$

再由此利用数论结论证明：

$\mathrm{Aut}C_n$ 是循环群 $\Longleftrightarrow$ n 为 $2,4,p^k,2p^k$（p 为奇素数）.

证 由于 $|Z_n^*|=\varphi(n)$，又 C_n 的自同构把生成元 a 仍变为生成元 a^m，从而 $(m,n)=1$，且

$$|\mathrm{Aut}C_n|=\varphi(n),$$

因此易知

$$\psi:\sigma\longrightarrow m\quad(\sigma(a)=a^m)$$

是 $\mathrm{Aut}C_n$ 到 Z_n^* 的一个同构映射，故 $\mathrm{Aut}C_n\cong Z_n^*$.

但由数论（参考华罗庚“数论导引”$P.56$ 定理 1 或熊全淹“初等整数论”$P.168$ 定理 4）知，Z_n^* 是循环群（即 Z_n^* 有 $\varphi(n)$ 阶元或称 n 有原根）的充要条件是，n 为整数 $2,4,p^k,2p^k$（其中 p 为任意奇素数）. 因此，这也就是 $\mathrm{Aut}C_n$ 为循环群的充要条件.

17. 如果一个环的特征是素数，问：这个环是否一定无零因子？

解 不一定. 例如模 p（素数）剩余类域 Z_p 上的 $n>1$ 阶全阵环，其特征为素数 p，但却有零因子.

18. 证明：若加群 G 为可分解群，则其自同态环 $\mathrm{End}\,G$ 不是域.

证 设 $G=H\oplus K$，其中 $H,K<G$. 则易知

$$\sigma:h+k\longrightarrow h\quad 与\quad \tau:h+k\longrightarrow k\quad(\forall\, h\in H,k\in K)$$

是 G 的两个自同态，即 $\sigma,\tau\in\mathrm{End}\,G$. 但显然 $\sigma\tau(h+k)=0$，即 $\sigma\tau=0$. 亦即 $\mathrm{End}G$ 有零因子，从而不是域.

19. 证明：有理数域 Q 的加群 $(Q,+)$ 的自同态环与 Q 同构.

证 用 $\mathrm{End}(Q,+)$ 表示加群 $(Q,+)$ 的自同态环. 任取 $\tau\in\mathrm{End}(Q,+)$. 并令 $\tau(1)=a$. 则由此可得，对任意有理数 $\frac{n}{m}$ 有

$$\tau\left(\frac{n}{m}\right)=\frac{n}{m}a.$$

这就是说，$\tau(1)$ 完全决定了 $(Q,+)$ 的自同态 τ. 于是令

$$\varphi:\ \tau\longrightarrow\tau(1)\quad(\forall\,\tau\in\mathrm{End}(Q,+)).$$

易知 φ 是 $\mathrm{End}(Q,+)$ 到 Q 的一个双射. 又对 $\mathrm{End}(Q,+)$ 中任意 σ,τ，由于

$$\begin{aligned}\varphi(\sigma+\tau)&=(\sigma+\tau)(1)=\sigma(1)+\tau(1)=\varphi(\sigma)+\varphi(\tau),\\ \varphi(\sigma\tau)&=\sigma\tau(1)=\sigma(\tau(1))=\sigma(a)\\ &=a\sigma(1)=\tau(1)\sigma(1)=\sigma(1)\tau(1)\\ &=\varphi(\sigma)\varphi(\tau),\end{aligned}$$

故 φ 是同构映射，因此，$\mathrm{End}(Q,+)\cong Q$.

20. 在所有 n 阶循环环中，有且只有 $T(n)$ 个是互不同构的. 其中 $T(n)$ 表示 n 的正因数的个数.

证 1) 设 $R=\langle a\rangle$ 是由元素 a 生成的任意一个 n 阶循环环，并且

$$a^2=ka\quad(1\leqslant k\leqslant n).$$

则 R 的全体生成元可设为

$$r_1a,\ r_2a,\ \cdots,\ r_ma\ (m=\varphi(n)),$$

其中 $r_1=1$，$1\leqslant r_i<n$，$(r_i,n)=1$ $(i=1,2,\cdots,m)$.

再设 $(k,n)=d$. 则由数论可知，存在整数 r_t $(1\leqslant t\leqslant m)$，$s$ 使

$$kr_t+ns=d,$$

这样，根据此等式以及 $a^2=ka$ 便得

$$\begin{aligned}(r_ta)^2&=(kr_t)(r_ta)\\&=(d-ns)(r_ta)=d(r_ta),\end{aligned}$$

这表明，n 阶循环环 R 总存在生成元及 n 的正因数 d 使上式成立. 因此由习题 4.5 第 8 题知，互不同构的 n 阶循环环不超过 $T(n)$ 个.

2) 设 $R=\langle a\rangle$ 与 $\overline{R}=\langle b\rangle$ 是两个 n 阶循环环，且

$$a^2=ka\quad(1\leqslant k\leqslant n);\quad b^2=hb\quad(1\leqslant h\leqslant n),$$

并根据以上证明还令 $k\mid n$，$h\mid n$ 且 $k\neq h$.

下证环 R 与 $\overline{R}$ 不同构. 根据习题 4.5 第 8 题，就是要证明二整数组

$$kr_1,kr_2,\cdots,kr_m\quad 与\quad hr_1,hr_2,\cdots,hr_m$$

中对模 n 没有同余的. 若不然，设 kr_i 与 hr_j 对模 n 同余，则

$$n\mid kr_i-hr_j,$$

于是由 $h\mid n$ 可知，$h\mid kr_i$. 但 $(h,r_i)=1$，故 $h\mid k$.

同理有 $k\mid h$. 因此 $h=k$，矛盾.

由上面的 1)与 2)可知，在所有 n 阶循环环中，有且只有 $T(n)$ 个是互不同构的.

注 此原题与习题 4.5 第 8 题重复现改为此题.

21. 设 $Z[\mathrm{i}]$ 是 Gauss 整环，即

$$Z[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in Z\},$$

其中 Z 是整数环，问：商环 $Z[\mathrm{i}]/\langle 1+\mathrm{i}\rangle$ 有多少个元素？是否为域？

证 1) 易知整数 k,l 有相同奇偶性$\Longleftrightarrow$存在整数 x,y 满足

$$k=x-y,\quad l=x+y.$$

2) 因为 $Z[\mathrm{i}]$ 是有单位元的交换环，所以

$$\begin{aligned}\langle 1+\mathrm{i}\rangle&=\{(x+y\mathrm{i})(1+\mathrm{i})\mid x+y\mathrm{i}\in Z[\mathrm{i}]\}\\&=\{(x-y)+(x+y)\mathrm{i}\mid x,y\in Z\}.\end{aligned}$$

于是，由 1)知，对于 $k+l\mathrm{i}\in Z[\mathrm{i}]$，有

$$k+l\mathrm{i}\in\langle 1+\mathrm{i}\rangle\Longleftrightarrow k\text{ 与 }l\text{ 有相同奇偶性.}$$

3) 由上面知，$1\in Z[\mathrm{i}]$，但 $1\notin\langle 1+\mathrm{i}\rangle$.

再任取 $m+n\mathrm{i}\in Z[\mathrm{i}]$，若 $m+n\mathrm{i}\notin\langle 1+\mathrm{i}\rangle$，即 m 与 n 有相反的奇偶性，则 $m-1$ 与 n 就有相同的奇偶性，从而

$$m+n\mathrm{i}-1=(m-1)+n\mathrm{i}\in\langle 1+\mathrm{i}\rangle,$$

即 $m+n\mathrm{i}+\langle 1+\mathrm{i}\rangle=1+\langle 1+\mathrm{i}\rangle$. 故 $Z[\mathrm{i}]/\langle 1+\mathrm{i}\rangle$ 共有两个元素：

$$\langle 1+\mathrm{i}\rangle,\quad 1+\langle 1+\mathrm{i}\rangle;$$

而且显然作成一个 2 元域.

22. 设环 R 的元素有一个分类，包含元素 x 的类用 $[x]$ 表示，而 S 是所有这些类作成的集合. 证明：如果

$$[x]+[y]=[x+y]\quad 及\quad [x][y]=[xy]$$

是 S 的两个代数运算，则 $[0]$ 是环 R 的一个理想，且所给的每一个类恰好是关于理想 $[0]$ 的一个陪集.

证 1) 先证 $[0]\trianglelefteqslant R$.

1° 任取 $a,b\in[0]$，则 $[a]=[b]=[0]$，于是

$$\begin{aligned}a-b&=a+(-b)\in[a]+[-b]=[b]+[-b]\\&=[b-b]=[0];\end{aligned}$$

即 $a-b\in[0]$.

2° 任取 $a\in[0]$，$r\in R$，则 $[a]=[0]$，且

$$[ra]=[r][a]=[r][0]=[r0]=[0].$$

故 $ra\in[0]$.

同理有 $ar\in[0]$，故 $[0]\trianglelefteqslant R$.

2) 再证 $[x]=x+[0]$，即每个类都是一个关于理想 $[0]$ 的陪集.

首先，$x+[0]\subseteq[x]+[0]=[x+0]=[x]$；其次，任取

$y\in[x]$，则

$$y-x=y+(-x)\in[x]+[-x]=[0],\quad y\in x+[0].$$

于是又有$[x]\subseteq x+[0]$，从而$[x]=x+[0]$.

23. 令R是一个有单位元的交换环，N是R的全体幂零元作成的集合. 证明：$N\trianglelefteqslant R$且商环R/N不含非零幂零元.

证　1) N显然非空. 又若$a,b\in N$，且

$$a^m=0,\quad b^n=0,$$

则由于R是交换环，故

$$(a-b)^{m+n}=a^{m+n}-C_{m+n}^1a^{m+n-1}b+\cdots+C_{m+n}^na^m(-b)^n+$$
$$C_{m+n}^{n+1}a^{m-1}(-b)^{n+1}+\cdots+(-b)^{m+n}=0.$$

从而$a-b\in N$.

又对R中任意元素r，由于$a^m=0$，故

$$(ar)^m=(ra)^m=a^mr^m=0,$$

从而$ra,ar\in N$. 故$N\trianglelefteqslant R$.

2) 设aN是商环R/N的幂零元，且

$$(aN)^n=\bar{0},\quad 即\ a^nN=\bar{0},$$

则$a^n\in N$. 但N中元素都是R的幂零元，故有正整数n使

$$a^{nn}=(a^n)^n=0,$$

即a为R的幂零元，$a\in N$. 从而$aN=\bar{0}$. 故商环R/N无非零幂零元.

24. 设N_1,N_2是环R的两个理想，规定

$$N_1N_2=\{\text{有限和}\sum a_ib_i\mid a_i\in N_1,b_i\in N_2\}.$$

证明：$N_1N_2\trianglelefteqslant R$，且$N_1N_2\subseteq N_1\cap N_2$.

证　由于有限和的差仍为有限和以及$N_i\trianglelefteqslant R$，故

$$N_1N_2\trianglelefteqslant R.$$

又由于$N_1\trianglelefteqslant R$，故$N_1N_2\subseteq N_1$；又$N_2\trianglelefteqslant R$，故$N_1N_2\subseteq N_2$. 从而

$$N_1N_2\subseteq N_1\cap N_2.$$

25. 证明：n阶循环环R是域的充要条件是，n为素数且R不是零乘环.

证　设循环环$R=\langle a\rangle=\{0,a,2a,\cdots,(n-1)a\}$，且

$$|a|=n,\quad a^2=ka\quad(0\leqslant k<n).\qquad(1)$$

若R是域，则R当然不能是零乘环. 又若n是合数，令

$$n=n_1n_2\quad(1\leqslant n_i<n,\ i=1,2).$$

则$n_1a\neq0,n_2a\neq0$. 但是$n_1a\cdot n_2a=na^2=0$. 这同R是域矛盾，故n必为素数.

反之，若R不是零乘环且$n=p$为素数，则由(1)知$k\neq0$. 于是若

$$sa\cdot ta=sta^2=(stk)a=0,$$

则因$|a|=p$，故$p\mid stk$. 但由(1)知$(k,p)=1$，故

$$p\mid s\quad 或\quad p\mid t.$$

从而有$sa=0$或$ta=0$. 即R无零因子. 于是由教材§3可知，R是一个除环. 再由于R可换，从而R是域.

26. 如果环R是单环或者R的所有非平凡理想都是域，则称R为NF-环. 证明：若环R的阶为pq（p,q为互异素数），则

$$R\text{是NF-环}\iff R\text{有单位元}.$$

证　因为$|R|=pq$，故可知R有p阶元知q阶元(对加法). 但因p与q是互异素数，故R有pq阶元(对加法)，从而R是pq阶循环环. 设

$$R=\langle a\rangle=\{0,a,\cdots,(pq-1)a\}.$$

1) 若R有单位元，则易知R有$T(pq)=4$个子环，且这4个子环都是有单位元的循环环，其阶分别为$1,p,q,pq$. 设两个非平凡子环为

$$S_1=\{0,e_1,2e_1,\cdots,(p-1)e_1\},$$
$$S_2=\{0,e_2,2e_2,\cdots,(q-1)e_2\},$$

其中e_i是S_i的单位元. 由上题知，S_1与S_2都是域. 因此，R是NF-环.

2) 反之，设 R 是 NF-环，且 $a^2=ka$ $(1\leqslant k<pq)$. 若 R 无单位元，则由本书本章 §1 释疑解难例 1 知，k 与 pq 不互素，不妨设 $k=p$，则 $\psi(pq)=2$，$\psi(k,pq)=1$. 于是由本书本章 §6 释疑解难例 2 知，R 有

$$2^{\psi(pq)\cdot\psi(k,pq)}=2^{2\cdot 1}=2$$

个子环有单位元. 但 R 共有 4 个子环，从而 R 有非平凡子环无单位元，当然就不能是域. 这与 R 是 NF-环矛盾.

因此，R 必有单位元.

27. 设 R 是一个 p^2 (p 为素数)阶环，证明：

$$R \text{ 是 NF-环} \Longleftrightarrow R \text{ 是域或 } R\cong Z_p\oplus Z_p.$$

证 充分性显然. 下证必要性.

设 R 是 NF-环，则首先 R 中不能有 p^2 阶元素：因若不然，设 $a\in R$ 且 $|a|=p^2$，则

$$\langle pa\rangle=\{0,pa,2pa,\cdots,(p-1)pa\}$$

是 R 的一个 p 阶子环，而且是零乘环. 这与 R 是 NF-环矛盾. 因此，R 中所有非零元素的阶只能都是 p.

若 R 不是域，则由教材 §3 定理 2 知，R 必有零因子：$x\neq 0$，$y\neq 0$，$xy=0$. 于是 $|x|=|y|=p$. 令

$$S_1=\{0,x,2x,\cdots,(p-1)x\},\quad S_2=\{0,y,2y,\cdots,(p-1)y\}.$$

若 $x^2=0$，则 S_1 是 p 阶零乘环，这与 R 是 NF-环矛盾. 故 $x^2\neq 0$. 从而 $|x^2|=p$. 任取 $b\in S_1\cap S_2$，令

$$b=sx=ty\quad (0\leqslant s<p,0\leqslant t<p),$$

则 $sx^2=x(ty)=t(xy)=0$，故 $p\mid s$. 从而 $s=0$，$b=0$. 因此

$$S_1\cap S_2=\{0\},\quad R=S_1\oplus S_2 \text{(作为加群)}.$$

由于 $x^2\in R$，故可令

$$x^2=k_1x+k_2y\quad (0\leqslant k_i<p). \tag{1}$$

于是 $x^2y=k_1xy+k_2y^2$. 但 $xy=0$，故 $k_2y^2=0$.

同上理，$y^2\neq 0$，从而 $|y^2|=p$. 于是 $p\mid k_2$，$k_2=0$. 因此由(1)得

$$x^2=k_1x\in S_1\quad (1\leqslant k_1<p).$$

这说明 S_1 是 R 的一个 p 阶子环，但 R 是 NF-环，故 S_1 是 p 阶域，从而 $S_1\cong Z_p$.

同理，$S_2\cong Z_p$. 因此，$R\cong Z_p\oplus Z_p$.

28. 证明本章 §2 引理.

证 1) 必要性 设 $AZ=0$ 在 R 中有非零解：

$$x_1=k_1,\ x_2=k_2,\ \cdots,\ x_n=k_n.$$

不妨设 $k_1\neq 0$. 当 $m<n$ 时，显然 $r(A)<n$，故下设 $m\geqslant n$.

令 D 是 A 的一个 n 阶子式，例如设

$$D=\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & \vdots & & \vdots\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{vmatrix}.$$

则用 D 的第 1 列诸元素的代数余子式 A_{11}，A_{21}，$\cdots$，A_{n1} 依次分别乘以下诸等式两端：

$$\begin{aligned} &a_{11}k_1+a_{12}k_2+\cdots+a_{1n}k_n=0,\\ &a_{21}k_1+a_{22}k_2+\cdots+a_{2n}k_n=0,\\ &\cdots\cdots\cdots\cdots\\ &a_{n1}k_1+a_{n2}k_2+\cdots+a_{nn}k_n=0,\end{aligned}$$

然后左右两端再分别相加，类似普通行列式性质，可得

$$D\cdot k_1+0\cdot k_2+\cdots+0\cdot k_n=0,$$

即 $k_1D=0$.

同理对 A 的其他 n 阶子式 M_n 均有 $k_1M_n=0$.

因此，k_1 是 S_n (A 的所有 n 阶子式作成的集合)的一个真零化子. 故由 §2 定义 6 知，$r(A)<n$.

2) 充分性. 设 $r(A)=r<n$.

若 $r=m$，则可用系数和常数项全是 0 的方程加以补充，使得方程组中方程的个数大于秩 r. 因此可设 $r<m$.

因为 $r(A)=r$，故 S_{r+1} 有真零化子 k，于是对 A 的任意 $r+1$ 阶子式 M_{r+1} 均有 $kM_{r+1}=0$ $(k\neq 0)$.

若 $r=0$，则 k 零化 A 中每个元素，从而

$$x_1=x_2=\cdots=x_n=k$$

显然是 $AX=0$ 的一个非零解.

若 $r>0$，则由于 S_r 无真零化子，从而必有 A 的某 r 阶子式 M_r 使 $kM_r\neq 0$. 现在不妨设 M_r 位于 A 的左上角，且 M_{r+1} 是 A 的左上角的 $r+1$ 阶子式. 再设 $d_1,d_2,\cdots,d_r,d_{r+1}$ 是 M_{r+1} 的最后一行诸元素的代数余子式，从而 $d_{r+1}=M_r$. 下证

$$x_1=kd_1,\ \cdots,\ x_r=kd_r,\ x_{r+1}=kd_{r+1},$$

$$x_{r+2}=\cdots=x_n=0 \qquad (3)$$

是 $AX=0$ 的一个非零解.

非零显然，因为 $x_{r+1}=kd_{r+1}=kM_r\neq 0$.

又因为当 $i=1,2,\cdots,r$ 时有

$$\begin{aligned}a_{i1}(kd_1)+\cdots+a_{i,r+1}(kd_{r+1})&=k(a_{i1}d_1+\cdots+a_{i,r+1}d_{r+1})\\&=k\cdot 0=0,\end{aligned}$$

即(3)满足 $AX=0$ 的前 r 个方程.

其次，再取 A 的 $r+1$ 阶子式

$$D_{r+1}=\begin{vmatrix} & & a_{1,r+1}\\ & M_r & \vdots\\ & & a_{r,r+1}\\ a_{j1} & \cdots & a_{j,r+1}\end{vmatrix}\quad (r<j\leqslant m),$$

按最后一行展开，得 $D_{r+1}=a_{j1}d_1+\cdots+a_{j,r+1}d_{r+1}$. 于是

$$\begin{aligned}&a_{j1}(kd_1)+\cdots+a_{j,r+1}(kd_{r+1})\\&=k(a_{j1}d_1+\cdots+a_{j,r+1}d_{r+1})=kD_{r+1}=0.\end{aligned}$$

即(3)也满足 $AX=0$ 的后 $m-r$ 个方程.

因此，$AX=0$ 有非零解.

29. 设 R 是一个有单位元的交换环. 证明：

$0\neq f(x)$ 是 $R[x]$ 的零因子 $\Longleftrightarrow$ 有 $0\neq c\in R$ 使 $cf(x)=0$.

证 充分性显然，下证必要性.

设 $f(x)$ 是 $R[x]$ 的零因子. 若 $f(x)\in R$，则结论显然. 故下设 $f(x)$ 的次数 $\geqslant 1$，且

$$f(x)=a_0+a_1x+\cdots+a_{m-1}x^{m-1}+a_mx^m.$$

由于 $f(x)$ 是 $R[x]$ 的零因子，故存在 R 上多项式

$$g(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}+b_nx^n\neq 0,$$

使 $g(x)f(x)=0$，其中 $0\neq b_n\in R$.

显然只需证明必有次数小于 n 的多项式与 $f(x)$ 之积仍为 0 即可.

由于 $g(x)f(x)=0$，故由上知：

$$a_mb_n=0, \qquad (1)$$

但是 $a_mg(x)f(x)=0$，而

$$\begin{aligned}a_mg(x)&=a_m(b_0+b_1x+\cdots+b_{n-1}x^{n-1}+b_nx^n)\\&=a_m(b_0+b_1x+\cdots+b_{n-1}x^{n-1}),\end{aligned}$$

因此，若 $a_mg(x)\neq 0$，则其次数小于 n，便已得证. 若 $a_mg(x)=0$，则由上知：

$$a_mb_0=a_mb_1=\cdots=a_mb_{n-1}=0,$$

从而有

$$\begin{aligned}g(x)f(x)=&(b_0+b_1x+\cdots+b_nx^n)\cdot\\&(a_0+a_1x+\cdots+a_{m-1}x^{m-1})=0,\end{aligned}$$

由此又得

$$a_{m-1}b_n=0, \qquad (2)$$

于是有

$$a_{m-1}g(x)f(x)=a_{m-1}(b_0+b_1x+\cdots+b_{n-1}x^{n-1})f(x)=0.$$

若 $a_{m-1}g(x)\neq 0$，则其次数小于 n，也已得证. 若 $a_{m-1}g(x)=0$，则有

$$\begin{aligned}g(x)f(x)=&(b_0+b_1x+\cdots+b_nx^n)\cdot\\&(a_0+a_1x+\cdots+a_{m-2}x^{m-2})=0,\end{aligned}$$

由此又得

$$a_{m-2}b_n=0. \qquad (3)$$

如此继续下去，或者有次数小于 n 的多项式与 $f(x)$ 之积为 0，

或者有

$$g(x)f(x)=g(x)a_0=0,$$

即有 $a_m g(x)=a_{m-1}g(x)=\cdots=a_1 g(x)=a_0 g(x)=0$. 于是由(1),(2),(3),…,有

$$a_m b_n=a_{m-1}b_n=\cdots=a_0 b_n=0.$$

从而 $b_n f(x)=0$,其中 $0\neq b_n\in R$.

30. 设 Z_n^* 为模 n 剩余类环 Z_n 的单位群. 证明:Z_n^* 中每个元素都满足 $x^2=1$ 的充要条件是,n 为以下整数:

$$2,3,4,6,8,12,24. \qquad (1)$$

证 可直接验算,当 n 为(1)中 7 个整数中的任一个时,Z_n^* 中每个元素都满足 $x^2=1$.

下证:当 n 不是(1)中的 7 个正整数时,Z_n^* 中有元素不满足 $x^2=1$.

1) $n=2^s\cdot 3^t$,$s\geqslant 4$,$t=0$ 或 1.

若 $t=0$,则 $n=2^s$. 由于 $3\in Z_n^*$(这里将 $\bar{3}$ 简记为 3,下同),$s\geqslant 4$,故

$$3^2=9<2^4\leqslant 2^s.$$

因此,$3^2=9\neq 1$.

若 $t=1$,则 $n=2^s\cdot 3$. 由于 $5\in Z_n^*$,$s\geqslant 4$,故

$$5^2=25<2^4\cdot 3\leqslant 2^s\cdot 3.$$

因此,$5^2=25\neq 1$.

2) $n=2^s\cdot 3^t$,$s\geqslant 0$,$t\geqslant 2$.

若 $s=0$,则 $n=3^t$. 由于 $2\in Z_n^*$,$t\geqslant 2$,于是

$$2^2=4<3^2\leqslant 3^t.$$

因此,$2^2=4\neq 1$.

若 $s=1$,$t=2$,则 $n=2\cdot 3^2$. 但由于 $5\in Z_n^*$,故

$$5^2=25=7\neq 1.$$

若 $s=1$,$t>2$,则 $n=2\cdot 3^t$. 但由于 $5\in Z_n^*$,且

$$5^2=25<2\cdot 3^3\leqslant 2\cdot 3^t,$$

因此,$5^2=25\neq 1$.

3) $n=p^k$,$k\geqslant 1$,而 p 是大于 3 的素数. 因为

$$2\in Z_n^*,\quad 2^2=4<5\leqslant p^k,$$

故 $2^2=4\neq 1$.

4) $n=2^s\cdot p^t$,$s\geqslant 1$,$t\geqslant 1$,p 是大于 3 的素数.

由于 $3\in Z_n^*$,且 $3^2=9<2\cdot 5\leqslant 2^s\cdot p^t$,因此

$$3^2=9\neq 1.$$

5) $n=2^s\cdot p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m}$,$s\geqslant 0$,$m\geqslant 2$,$t_i\geqslant 1$,且 $p_1,p_2,\cdots,p_m$ 为互异的奇素数.

因为 Z_n^* 是 $\varphi(n)$ 阶群,要证明 Z_n^* 中有元素不满足方程 $x^2=1$ 仅需指出同余方程

$$x^2\equiv 1\pmod{n} \qquad (2)$$

的解的个数小于 $\varphi(n)$ 即可.

当 $s=0$ 或 1 时,由于每个同余方程

$$x^2\equiv 1\pmod{p_i^{t_i}}\quad (i=1,\cdots,m)$$

都有两个解,因此同余方程(2)有 2^m 个解. 但因 $m\geqslant 2$,故

$$2^m<p_1^{t_1-1}p_2^{t_2-1}\cdots p_m^{t_m-1}(p_1-1)(p_2-1)\cdots(p_m-1)=\varphi(n);$$

当 $s=2$ 时,$n=2^2\cdot p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m}$. 由于 $x^2\equiv 1\pmod 4$ 有 2 个解,从而(2)有 2^{m+1} 个解. 再由 $m\geqslant 2$,得

$$2^{m+1}<2p_1^{t_1-1}p_2^{t_2-1}\cdots p_m^{t_m-1}(p_1-1)(p_2-1)\cdots(p_m-1)=\varphi(n);$$

当 $s>2$ 时,由于同余方程

$$x^2\equiv 1\pmod{2^s}$$

有 4 个解,故同余方程(2)有 2^{m+2} 个解. 但 $m\geqslant 2$,故

$$2^{m+2}<2^{s-1}p_1^{t_1-1}p_2^{t_2-1}\cdots p_m^{t_m-1}(p_1-1)\cdots(p_m-1)=\varphi(n).$$

综合以上可知,得证.