Chapter 4

群、环、域简介

这一章我们介绍抽象代数的基本概念：群、环和域。它们都是带有特定运算结构的集合，我们的目的是研究这些结构的性质，并将其应用到具体的数学对象上。这种思路也是代数学的基本想法之一。初学者面对这一章的内容或许会感到难以理解，但实际上这一章的内容大部分是很具体的 (甚至是可以“计算”的)，读者可以结合例子来慢慢理解这些代数学对象的“实在性”。

4.1 二元运算

定义 4.1.1 设 S 是非空集合，我们称映射 $S\times S\to S$ 是一个二元运算，简称运算。对任意 $x,y\in S$，我们也把 $f(x,y)$ 简记为 xfy。

例 4.1.1 (i) $+:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\ (a,b)\mapsto a+b$ 是 $\mathbb{Z}$ 上的二元运算。

(ii) $\cdot:M_n(\mathbb{R})\times M_n(\mathbb{R}),\ (A,B)\mapsto AB$ 是 $M_n(\mathbb{R})$ 上的二元运算。

(iii) 记 $*:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\ (x,y)\mapsto|x-y|$，则 $*$ 也是 $\mathbb{Z}$ 上的二元运算。

定义 4.1.2 若二元运算 f 满足 $\forall x,y\in S,\ f(x,y)=f(y,x)$，则我们称 f 满足交换律；若二元运算 f 满足 $\forall x,y,z\in S,\ f(f(x,y),z)=f(x,f(y,z))$，则我们称 f 满足结合律。

当然，一个运算满足交换律和满足结合律之间没有必然关系，例如例 4.1.1 中 (ii) 是结合但不交换的，(iii) 是交换但不结合的，验证留作练习。

定理 4.1.1 (**广义结合律**) 设 $*$ 是集合 S 上的一个满足结合律的二元运算，$x_1,\dots,x_n\in S,\ n\geqslant 2$，归纳定义

$$x_1*x_2*\cdots*x_n=(x_1*\cdots*x_{n-1})*x_n\quad\text{(左正规化)}$$

则对任意 $\forall k\in\{1,\dots,n-1\}$，有

$$x_1*x_2*\cdots*x_n=(x_1*\cdots*x_i)*(x_{i+1}*\cdots*x_n).$$

证明: $n=1,2$ 时定理显然成立。当 $n=3$，由结合律，我们有

$$x_1*x_2*x_3=(x_1*x_2)*x_3=x_1*(x_2*x_3).$$

对 n 用数学归纳法。假设定理对 "$< n$" 的所有正整数都成立，即括号的位置与二元运算无关。则对 n 个元素的二元运算，当 $i = n-1$ 时，即是定义。不妨设 $1 \leqslant i < n-1$, 我们有：

$$\begin{aligned}
& x_1 * \cdots * x_i * x_{i+1} * \cdots * x_n \\
=\ & (x_1 * \cdots * x_{n-1}) * x_n && \text{(定义)} \\
=\ & [(x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_{n-1})] * x_n) && \text{(归纳假设)} \\
=\ & (x_1 * \cdots * x_i) * [(x_{i+1} * \cdots * x_{n-1}) * x_n)] && \text{(结合律)} \\
=\ & (x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_n) && \text{(定义)}
\end{aligned}$$

即定理对 n 的情形也对，这样我们就完成了证明。 □

有了广义结合律，我们就可以对一个结合的二元运算 $*$ 定义**方幂**：设 $n \in \mathbb{Z}^+$，记 $\underbrace{x * \cdots * x}_{\text{n 个}} = x^n$，则对 $\forall m, n \in \mathbb{Z}^+$，方幂满足性质：$(x^n) * (x^m) = x^{n+m}$，$(x^n)^m = x^{mn}$。

定义 4.1.3 设 $*$ 是集合 S 上的一个二元运算，$e \in S$，如果 $\forall x \in S, x * e = e * x = x$，则称 e 是 S 上关于 $*$ 的单位元或幺元 (identity)。

例 4.1.2 显然 0 是 $\mathbb{Z}$ 上关于加法"+" 的单位元；E_n 是 $M_n(\mathbb{R})$ 上关于矩阵乘法的单位元。

命题 4.1.1 设 $*$ 是集合 S 上的二元运算，若 e, e' 都是 S 上关于 $*$ 的单位元，则 $e = e'$。即单位元若存在则必唯一。

由 $e = ee' = e'$ 立刻得证。

定义 4.1.4 设 $*$ 是 S 上的二元运算，e 是 S 中关于 $*$ 的单位元，$x \in S$。如果存在 $y \in S$ 使得 $x * y = y * x = e$，则我们称 x 是 S 中关于 $*$ 的可逆元，并称 y 是 x 的逆。

例 4.1.3 显然 $\mathbb{Z}$ 中任意元素都关于 "$+$" 可逆，且 x 的逆就是 $-x$；在 $M_n(\mathbb{R})$ 中，关于矩阵乘法可逆的元素是所有满秩矩阵，并且逆是逆矩阵。

下面我们正式引入一个在代数和数论中都十分重要的研究对象：剩余类。在第一章中，我们定义了 $\mathbb{Z}$ 上的同余关系，

$$\forall a, b \in \mathbb{Z}, n \in \mathbb{Z}^+, a \equiv_n b \iff n | (a-b)$$

同余关系是一个等价关系。有时也记作 $a \equiv b \mod n$. 下面我们考虑 $\mathbb{Z}$ 在 $\equiv_n$ 关系下的分割. $\forall a \in \mathbb{Z}$，作带余除法 $a = qn + r$, $r \in \{0, 1, \ldots, n-1\}$，则 $a \equiv_n r$。于是 $\equiv_n$ 关系下有且只有 n 个等价类 $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$，其中 $\overline{i} = \{i + kn \mid k \in \mathbb{Z}\}$, $i = 0, \ldots, n-1$。于是，我们有 $\mathbb{Z}/\equiv_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$。我们以后将 $\mathbb{Z}/\equiv_n$ 也记作 $\mathbb{Z}_n$ 或 $\mathbb{Z}/n\mathbb{Z}$，称之为 $\mathbb{Z}$ 模 n 的剩余类。我们在剩余类集合上可以定义运算加法 "$+$" 和乘法 "$\cdot$"[1]如下：

$$\begin{aligned}
+ : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} & \qquad \cdot : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\
(\overline{a}, \overline{b}) &\longmapsto \overline{a+b} & (\overline{a}, \overline{b}) &\longmapsto \overline{ab}
\end{aligned}$$

首先，这两个运算都是良定义的。我们只验证乘法 "$\cdot$" 的良定义性，加法 "$+$" 的验证留作练习。设 $\overline{a} = \overline{a'}$, $\overline{b} = \overline{b'}$，则 $n \mid a - a'$, $n \mid b - b'$，于是 $n \mid (a-a')(b-b') + a'(b-b') + b'(a-a')$，即 $n \mid ab - a'b'$，所以 $\overline{ab} = \overline{a'b'}$。此即 "$\cdot$" 良定义。

下面考察剩余类上加法和乘法满足的运算律。$\mathbb{Z}_n$ 上的加法满足：

[1]以后我们经常将 "$\cdot$" 省略。

(1) 交换律 $\overline{a}+\overline{b}=\overline{b}+\overline{a}$;

(2) 结合律 $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$;

(3) 加法单位元 $\overline{0}$: $\overline{0}+\overline{a}=\overline{a}+\overline{0}=\overline{a}$;

(4) 每个元素加法可逆: $\overline{a}+\overline{-a}=\overline{-a}+\overline{a}=\overline{0}$。

$\mathbb{Z}_n$ 上的乘法满足:

(1) 交换律 $\overline{a}\overline{b}=\overline{b}\overline{a}$;

(2) 结合律 $(\overline{a}\overline{b})\overline{c}=\overline{a}(\overline{b}\overline{c})$;

(3) 单位元 $\overline{1}$: $\overline{1}\cdot\overline{a}=\overline{a}\cdot\overline{1}=\overline{a}$。

下面考虑 $\mathbb{Z}_n\setminus\{\overline{0}\}$ 上关于乘法可逆的元素 (显然 $\overline{0}$ 关于乘法不可逆), 我们有以下的命题:

命题 4.1.2 设 $\overline{m}\in\mathbb{Z}_n$, 则 $\overline{m}$ 在 $\mathbb{Z}_n$ 中关于乘法可逆 $\Longleftrightarrow\gcd(m,n)=1$。

证明: ($\Longleftarrow$) 由 Bezout 关系, $\gcd(m,n)=1\Longrightarrow\exists a,b\in\mathbb{Z}$ 使得 $am+bn=1$, 则 $am\equiv 1 \mod n$, 即 $\overline{a}\cdot\overline{m}=\overline{1}$, 于是 $\overline{m}$ 乘法可逆 $\overline{a}$ 是 $\overline{m}$ 的乘法逆。
($\Longrightarrow$) 由 $\overline{m}$ 乘法可逆得存在 $\overline{a}\in\mathbb{Z}_n$ 使得 $\overline{a}\cdot\overline{m}=\overline{1}$, 即 $am\equiv 1 \mod n$, 所以存在 $b\in\mathbb{Z}$ 使得 $am+bn=1$, 即 $\gcd(m,n)=1$。 □

马上我们就会知道, $\mathbb{Z}_n$ 是一个交换环, 我们把 $\mathbb{Z}_n$ 中关于乘法可逆的元素放在一起做成一个集合, 记作 $\mathbb{Z}_n^\times$。$\mathbb{Z}_n^\times$ 中的元素称为 (乘法) 可逆元或者单位 (unit)。

4.2 群

定义 4.2.1 (**半群**) 设 $*$ 是集合 S 上的一个二元运算，若 $*$ 满足结合律，则称 $(S,*)$ 是半群 (semigroup)(当运算已经明确时常常省略，即称 S 是半群)。特别地，若半群 $(S,*)$ 中有单位元 e，则称 $(S,*,e)$ 是幺半群 (monoid)；若半群 $(S,*)$ 中 $*$ 还满足交换律，则称 $(S,*)$ 是交换 (commutative or abeliean) 半群。

例 4.2.1 $(\mathbb{Z}_n,\cdot,\overline{1})$ 是幺半群；$(M_n(\mathbb{R}),\cdot,E_n)$ 也是幺半群。

下面的命题表明，幺半群中一个元素若可逆，则逆必然唯一。

命题 4.2.1 设 $(S,*,e)$ 是幺半群，$x\in S$ 可逆，则 $\exists!y\in S$ 使得 $xy=yx=e$。

证明: 由于 $xy=yx=e$, $xz=zx=e$，因此 $y=ey=(zx)y=z(xy)=ze=z$。 □

于是我们可以定义群了。

定义 4.2.2 设 $(G,*,e)$ 是幺半群，如果 $\forall g\in G$，g 都可逆，则称 $(G,*,e)$ 是群 (group)。

当一个群的运算明确时，我们常常省略群运算和单位元，而直接称 G 是群。下面是一些常见的群的例子。

例 4.2.2 (1)$(\mathbb{Z},+,0)$ 和 $(\mathbb{Z}_n,+,\overline{0})$ 都是群，$(\mathbb{Q},+,0)$, $(\mathbb{R},+,0)$, $(\mathbb{C},+,0)$ 也都是群；
(2)$(M_n(\mathbb{R}),+,O_{n\times n})$ 是群；记 $\mathrm{GL}_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \mathrm{rank}(A)=n\}$，则 $(\mathrm{GL}_n(\mathbb{R}),\cdot,E_n)$ 是群，称为一般 (实) 线性群 (general linear group)；记 $\mathrm{SL}_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \det(A)=1\}$，则 $(\mathrm{SL}_n(\mathbb{R}),\cdot,E_n)$ 是群，称为特殊 (实) 线性群 (special linear group)；
(3) 设 X 是非空集合，记 $T_X=\{f:X\to X\mid f\text{是双射}\}$，则 $(T_X,\circ,\mathrm{id}_X)$ 是群，称为 X 的变换群。特别地，当 $X=\{1,2,\ldots,n\}$ 时，即 $T_X=S_n$，我们称 $(S_n,\circ,e)$ 是 n 元置换群。

命题 4.2.2 记 $\mathbb{Z}_n^*=\mathbb{Z}_n\setminus\{\overline{0}\}$，则 $(\mathbb{Z}_n^*,\cdot,\overline{1})$ 是群 $\Longleftrightarrow$ n 是素数。

证明: 由命题 4.1.2 立刻可证。 □

定义 4.2.3 设 $(G,*,e)$ 是群，如果 $*$ 满足交换律，则称 G 是交换群或阿贝尔群 (abeliean group)，否则称为非交换群。

例 4.2.3 在例 4.2.1 中，(1) 中的群和 (2) 中的 $(M_n(\mathbb{R}),+,O_{n\times n})$ 是交换群，其余例子都是非交换群。例如，S_3 中 (1 2)(2 3) = (3 1 2), (2 3)(1 2) = (1 3 2) 不相等。

当 G 是交换群时，我们经常称群 G 的运算为加法。

定义 4.2.4 如果群 G 中只有有限个元素，则称 G 为有限群 (finite group)，否则称为无限群 (infinite group)。当 G 是有限群时，我们把 G 中元素的个数称为群 G 的阶 (order)，记为 $|G|$。

例 4.2.4 $(\mathbb{Z}_n,+,\overline{0}),(S_n,\circ,e)$ 都是有限群，而 $(\mathrm{GL}_n(\mathbb{R}),\cdot,E_n),(\mathrm{SL}_n(\mathbb{R}),\cdot,E_n)$ 都是无限群。

我们引入群的平移变换的概念，并证明一个引理。

引理 4.2.1 设 G 是群，$a\in G$，则映射 $L_a:G\to G$, $g\mapsto ag$ 和 $R_a:G\to G$, $g\mapsto ga$ 都是双射，分别称为 G 关于 a 的左 (右) 平移变换。

证明: 由于 a 可逆，故可构造映射 $L_{a^{-1}}: G \to G,\ g \mapsto a^{-1}g$，则对 $\forall g \in G$，有

$$L_a \circ L_{a^{-1}}(g) = L_a(a^{-1}g) = aa^{-1}g = g$$

即 $L_a \circ L_{a^{-1}} = \mathrm{id}_G$。同理可以验证 $L_{a^{-1}} \circ L_a = \mathrm{id}_G$。于是 L_a 是双射。R_a 是双射可以用同样的方法证明。 □

有限群的构造可以用乘法表 (Cayley 表) 来表示。设群 $G = \{g_1, \ldots, g_n\}$，运算为乘法 $*$，则下表完全给出了 G 的结构:

$*$	g_1	g_2	$\cdots$	g_j	$\cdots$	g_n
g_1	g_1^2	g_1g_2	$\cdots$	g_1g_j	$\cdots$	g_1g_n
$\vdots$	$\vdots$					$\vdots$
g_i	g_ig_1	g_ig_2	$\cdots$	g_ig_j	$\cdots$	g_ig_n
$\vdots$	$\vdots$					$\vdots$
g_n	g_ng_1	g_ng_2	$\cdots$	g_ng_j	$\cdots$	g_n^2

由引理 4.2.1 知，Caylay 表的每一行，每一列的元素都互不相同，是 $g_1, \ldots, g_n$ 的一个重新排列。下面我们考虑一些低阶群的结构。

例 4.2.5 1. $|G| = 1$: 即群 G 中只有一个单位元，记为 e;

2. $|G| = 2$: 即群 G 中只有单位元 e 和一个非单位元 a，此时乘法表为:

$*$	e	a
e	e	a
a	a	e

   $G = \{e, a\}$ 满足 $a^2 = e$。例如群 $(\mathbb{Z}_2, +, 0)$, $(S_2, \circ, e)$.

3. $|G| = 3$: 即群 G 中只有单位元 e 和两个非单位元 a, b，此时乘法表为:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

   $G = \{e, a, b\}$ 满足 $b = a^2, b^2 = a, ab = ba = e$。例如群 $(\mathbb{Z}_3, +, 0)$,

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\cos(2\pi/3) & -\sin(2\pi/3)\\ \sin(2\pi/3) & \cos(2\pi/3)\end{pmatrix}, \begin{pmatrix}\cos(4\pi/3) & -\sin(4\pi/3)\\ \sin(4\pi/3) & \cos(4\pi/3)\end{pmatrix}\right\}$$

4. $|G| = 4$, 此时群 G 有两种结构，一是 $G = \{e, a, a^2, a^3\}$, 满足 $a^4 = e$; 另一种是 $G = \{e, a, b, ab\}$, 满足 $a^2 = b^2 = (ab)^2 = e$, 可以证明 4 阶群只有这两种结构，并且这两种结构是“不同”的! 我们很快就会证明这一点。

有了群的概念以后，一个必然的问题是考虑不同的群之间的关系，这就是我们下面讨论的群的同态与同构。

定义 4.2.5 设 $(G,*,e)$, $(H,\cdot,\varepsilon)$ 是两个群，我们称 $\varphi: G\to H$ 是 G 到 H 的同态映射 (homomorphism)，如果 φ 满足：$\forall g_1,g_2\in G$，有 $\varphi(g_1*g_2)=\varphi(g_1)\cdot\varphi(g_2)$。特别地，若 φ 是单射，则称 φ 是单同态 (injective homomorphism)；若 φ 是满射，则称 φ 是满同态 (surjective homomorphism)；若 φ 是双射，则称 φ 是同构 (isomorphism)。如果两个群 G,H 之间存在同构映射，则称 G 与 H 同构，记作 $G\simeq H$。

引理 4.2.2 设 φ 是群 $(G,*,e)\to(H,\cdot,\varepsilon)$ 的同态，则：
(1)$\varphi(e)=\varepsilon$;
(2)$\forall g\in G$, $\varphi(g^{-1})=[\varphi(g)]^{-1}$;
(3) 若 φ 是同构，则逆映射 φ^{-1} 也是同构;
(4) 若 G 是交换群，H 是非交换群，则 φ 不是同构。

证明: (1) 首先我们有

$$\varphi(e)=\varphi(e*e)=\varphi(e)\cdot\varphi(e).$$

于是

$$\begin{aligned}\varepsilon&=\varphi(e)\cdot[\varphi(e)]^{-1}\\&=\varphi(e)\cdot\varphi(e)\cdot[\varphi(e)]^{-1}\\&=\varphi(e)\cdot\varepsilon\\&=\varphi(e).\end{aligned}$$

(2) 对 $\forall g\in G$，注意到 $\varepsilon=\varphi(e)=\varphi(g*g^{-1})=\varphi(g)\cdot\varphi(g^{-1})$，即 $\varphi(g^{-1})=[\varphi(g)]^{-1}$。
(3)φ 是双射推出 φ^{-1} 也是双射，于是我们只需证明 φ^{-1} 也是同态。对 $\forall h_1,h_2\in H$, $\exists!\ g_1,g_2\in G$ 使得 $\varphi(g_1)=h_1$, $\varphi(g_2)=h_2$，又因为 $\varphi(g_1*g_2)=\varphi(g_1)\cdot\varphi(g_2)=h_1\cdot h_2$，于是 $\varphi^{-1}(h_1\cdot h_2)=g_1*g_2=\varphi^{-1}(h_1)*\varphi^{-1}(h_2)$，即 φ^{-1} 是同态。
(4) 用反证法，设 φ 是同构。由于 G 是交换群，即任意 $a,b\in G$ 都有 $a*b=b*a$，用 φ 作用上去以后得到 $\varphi(a)\cdot\varphi(b)=\varphi(b)\cdot\varphi(a)$，又因为 φ 是双射，所以 $\varphi(a),\varphi(b)$ 可以取遍 H 中的所有元素，故 H 是交换群，这与 H 是非交换群矛盾！这样我们就完成了证明。 □

下面是一些同态的例子。

例 4.2.6 $\Pi_n:\mathbb{Z}\to\mathbb{Z}_n$, $a\mapsto\overline{a}$ 是群 $(\mathbb{Z},+,0)$ 到 $(\mathbb{Z}_n,+,\overline{0})$ 的同态；$\det:\mathrm{GL}_n(\mathbb{R})\to\mathbb{R}^*$, $A\to\det(A)$ 是群 $(\mathrm{GL}_n(\mathbb{R}),\cdot,E)$ 到 $(\mathbb{R}^*,\cdot,1)$ [1]的同态。验证留作练习。

引理 4.2.3 设 G,H,K 是三个群，$\varphi:G\to H$, $\psi:H\to K$ 是群同态，则 $\psi\circ\varphi:G\to K$ 也是群同态。

证明可以由交换图 $\begin{array}{ccc}G&\xrightarrow{\varphi}&H\\&\searrow^{\psi\circ\varphi}&\downarrow\psi\\&&K\end{array}$ 表示，细节留作练习。

用上面的引理我们很容易证明群的同构是一个等价关系，细节留作练习。

例 4.2.7 求证群 $(\mathbb{Z}_4,+,\overline{0})$ 与群 $(\mathbb{Z}_2\times\mathbb{Z}_2,+,(\overline{0},\overline{0}))$ 不同构。[2]

[1] $\mathbb{R}^*=\mathbb{R}\setminus\{0\}$

[2] 这里 $+$ 是指坐标分量对应相加。

证明: 用反证法，假设存在 $\varphi:\mathbb{Z}_4\to\mathbb{Z}_2\times\mathbb{Z}_2$ 是同构，则 $\varphi(\bar{0})=(\bar{0},\bar{0})$，注意到 $\forall y\in\mathbb{Z}_2\times\mathbb{Z}_2$，$y+y=(\bar{0},\bar{0})$，于是不管 $\varphi(\bar{1})$ 是 $\mathbb{Z}_2\times\mathbb{Z}_2$ 中的哪个元素，都有 $\varphi(\bar{2})=\varphi(\bar{1})+\varphi(\bar{1})=(\bar{0},\bar{0})$，这与 φ 是双射矛盾！ □

群论的一个基本问题就是给定一类群，寻找同构关系下的等价类，即对一类群按照同构进行分类。其中，一个基本的类型是对有限单群 [1] 进行分类。有限单群分类是 20 世纪最伟大的数学成就之一，相关的结果有上万页之多，即使简化后仍有数千页的证明，至今简化整理的工作尚未完成。

下面是一些小阶数群的分类。

表：阶数 $\leqslant 15$ 的群[2]

$\lvert G\rvert$	G	
	交换群	非交换群
1	$\{e\}$	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4,\mathbb{Z}_2\times\mathbb{Z}_2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	$S_3\simeq D_3$
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8,\mathbb{Z}_2\times\mathbb{Z}_4,\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$	D_4,Q_8
9	$\mathbb{Z}_9,\mathbb{Z}_3\times\mathbb{Z}_3$	
10	$\mathbb{Z}_{10}$	D_5
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12},\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3$	D_6,A_4,T
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14}$	D_7
15	$\mathbb{Z}_{15}$	

其中，$D_n=\{\sigma^i\tau^j\mid\sigma^n=\tau^2=e,\ (\tau\sigma)^2=e;\ i=0,1,\dots n-1;\ j=0,1\}$ 是 $2n$ 阶群，被称为二面体群；S_n 是 n 元置换群；A_n 是全体 n 元偶置换在映射复合下形成的群；$Q_8=\{\sigma^i\tau^j\mid\sigma^4=e,\tau^2=\sigma^2,\tau\sigma=\sigma^3\tau;\ i=0,1,2,3;\ j=0,1\}$；$T=\{\sigma^i\tau^j\mid\sigma^6=1,\tau^2=\sigma^3,\tau\sigma=\sigma^5\tau;\ i=0,1,\dots,5;\ j=0,1\}$。其中素数阶群和 $\leqslant 6$ 阶群的结构要求大家掌握，其余内容会在后续抽象代数课程中学习。

特别地，我们注意 D_3 的几何意义。考虑平面上的一个正三角形，对它进行变换，则保持这个三角形与原来重合的变换有且只有 6 个 (旋转 $0,\frac{2\pi}{3},\frac{4\pi}{3}$ 角以及分别沿三条对称轴翻转)，它们在映射复合下构成的群称为 D_3。这样我们很容易看到 $D_3\simeq S_3$。我们可以类似地定义 D_n 是保持正 n 边形与原来重合的变换构成的群。

下面我们开始介绍子群的概念。

定义 4.2.6 设 $(G,*,e)$ 是群，$H\subset G$ 且 $e\in H$，如果 $(H,*,e)$ 也是群，则称 H 是 G 的子群 (subgroup)，记作 $H<G$。特别地，$\{e\}$ 和 G 本身都是 G 的子群，称为 G 的平凡子群 (trivial subgroup)；其余的 G 的子群称为 G 的真子群 (proper subgroup)。

[1] 我们会在抽象代数中介绍单群的概念，不过本讲义中不会出现了。

[2] 引自《近世代数引论》，冯克勤、李尚志、章璞著，中国科学技术大学出版社

引理 4.2.4 设 $(G,*,e)$ 是群，H 是 G 的非空子集，则 H 是 G 的子群 $\Longleftrightarrow \forall h_1,h_2\in H,\ h_1h_2^{-1}\in H$。

证明: ($\Longrightarrow$) 由 H 是群，$h_2\in H$ 可知 $h_2^{-1}\in H$，又 $h_1\in H$，所以由群对乘法封闭可得 $h_1h_2^{-1}\in H$。($\Longleftarrow$) 首先，任取 $h\in H$ 则 $e=hh^{-1}\in H$，于是 $h^{-1}=eh^{-1}\in H$，即 H 对求逆封闭。下证 H 对乘法封闭。$\forall h_1,h_2\in H$，由上面的证明知 $h_2^{-1}\in H$，于是 $h_1h_2=h_1(h_2^{-1})^{-1}\in H$。即得结论。 □

引理 4.2.5 设 H,K 是 G 的子群，则 $H\cap K$ 是 G 的子群。

用定义直接验证即可，留作练习。

需要注意的是，子群的积不一定是子群，即 $H<G,\ K<G\nRightarrow HK=\{hk\mid h\in H,\ k\in K\}<G$。反例取 S_3 的两个子群 $H=\{e,\ (1\ 2)\},\ K=\{e,\ (1\ 3)\}$ 即可验证。

例 4.2.8 所有 n 元偶置换的集合 A_n 是 S_n 的子群。这是因为偶置换的积显然是偶置换，由引理 1.5.6 可知偶置换的逆也是偶置换，即 A_n 对乘法和求逆封闭，所以 $A_n<S_n$。

定义 4.2.7 设 G 是群，$H<G$，任取 $g\in G$，称集合 $gH=\{gh\mid h\in H\}$ 为 H 的一个左陪集 (coset)。

类似地我们也可以定义右陪集的概念，事实上，H 的所有左陪集 (或右陪集) 构成了 G 的一个分割 [1](1.4.5 小节)，我们会在下面 Lagrange 定理的证明中顺便证明这一点。此外，注意到 $gH=L_g(H)$，而 L_g 是双射，因此 $\forall g\in G,\ |gH|=|H|$。

定理 4.2.1 (Lagrange **定理**) 设 G 是有限群，$H<G$，则 $|H|\ \Big|\ |G|$。

证明: 我们先证明如下的结论：如果子群 H 的两个左陪集 g_1H,g_2H 不相等，则 $g_1H\cap g_2H=\emptyset$。用反证法，假设存在 $a\in g_1H\cap g_2H$，则存在 $h_1,h_2\in H$ 使得 $a=g_1h_1=g_2h_2$，于是 $g_2=g_1(h_1h_2^{-1})\in g_1H$，那么 $\forall x\in g_2H$，都存在 $h\in H$ 使得 $x=g_2h=g_1(h_1h_2^{-1})h$，即 $x\in g_1H$，所以 $g_2H\subset g_1H$。同理可证 $g_1H\subset g_2H$，于是 $g_1H=g_2H$，这与 g_1H,g_2H 不相等矛盾！

下面我们证明原命题。H 是平凡子群时结论显然成立。下面考虑 H 是 G 的真子群的情形。令 $g_1=e$，取 $g_2\in G\setminus H$，如果 $g_1H\cup g_2H=G$，则由 $|gH|=|H|$ 可知 $2|H|=|G|$，命题成立；否则可取

$g_3\in G\setminus(g_1H\cup g_2H)$，如果 $G=g_1H\cup g_2H\cup g_3H$ 则命题成立；否则可以继续取 g_4 重复上述操作 $\cdots\cdots$。这一过程必然在有限步内终止，否则 $|G|=\infty$ 与 $|G|$ 是有限群矛盾！即 $\exists k\in\mathbb{N}^+$ 使得 $G=g_1H\cup\cdots\cup g_kH$ 是不交并，并且每个左陪集的元素个数都等于 $|H|$，所以 $|H|\ \Big|\ |G|$。 □

实际上，G 的全体左陪集只有上面的 $g_1H,\ldots,g_kH$。这是因为 $\forall g\in G$，一定存在 $i\in\{1,\ldots,k\}$ 使得 $g\in g_iH$，即 $g=g_ih,\ h\in H$。于是 $g\in gH\cap g_iH\neq\emptyset$，故由上面的证明过程可知 $gH=g_iH$。

此外，若 $H<G$，则我们称 $|G|/|H|$ 为子群 H 在 G 中的指数，记作 $[G:H]$。

例 4.2.9 由 Lagrange 定理立刻可以得到：如果 $|G|$ 是素数，则群 G 没有非平凡的子群。

下面我们考虑一类最简单的群：循环群。首先，在群 G 中我们可以将元素 x 的方幂推广到整数次方：记 $x^0=e,\ x^{-n}=(x^{-1})^n,\ n\in\mathbb{Z}^+$。容易验证推广后的方幂仍然满足：$(x^n)(x^m)=x^{n+m},\ (x^n)^m=x^{mn}$(留作练习)。

定义 4.2.8 设 G 是群，若存在 $a\in G$ 使得 $\forall g\in G$，存在 $n\in\mathbb{Z}$ 使得 $g=a^n$，则称 G 是由元素 a 生成的循环群，记为 $G=<a>$；a 称为 G 的生成元。

[1]从而我们可以定义商群了，这会在抽象代数中学习。

显然 $< a >= \{a^m \mid m \in \mathbb{Z}\}$(重复的只保留一个代表)。注意循环群的生成元不一定是唯一的，因为 a 是生成元 $\iff$ a^{-1} 也是生成元。

例 4.2.10 容易验证 $(\mathbb{Z}, +, 0)$, $(S_2, \circ, e)$ 都是循环群，它们的生成元分别是 1(或-1) 和 (1 2) (注意 $(1\ 2)^{-1} = (1\ 2)$)。

我们引入群元素的阶的概念。

定义 4.2.9 设 G 是群，$a \in G$，如果不存在 $n \in \mathbb{Z}$ 使得 $z^n = e$，则称 a 是无穷阶元素，记为 $\mathrm{ord}(a) = \infty$；否则，一定存在一个最小的**正整数** k 使得 $a^k = e$，此时称 a 的阶是 k，记作 $\mathrm{ord}(a) = k$。

例 4.2.11 (1) S_3 中 (1 2) 的阶是 2，(1 2 3) 的阶是 3；

(2) $\mathbb{Z}$ 中任意元素的阶都是 ∞；

(3) $\mathbb{Z}_{10}$ 中 $\mathrm{ord}(\overline{2}) = 5$。

我们先证明下面两个引理。

引理 4.2.6 设 G 是群，$g \in G$ 并且 $\mathrm{ord}(g) = k < \infty$，则 $g^n = e \iff k \mid n$。

证明: ($\Longrightarrow$) 作带余除法 $n = qk + r$，其中 $r \in \{0, 1, \ldots, k-1\}$，则 $g^{qk} = e^q = e$，于是 $g^n = g^{qk} g^r = g^r$，于是由 k 的最小性得 $r = 0$。
($\Longleftarrow$) $n = kq \Longrightarrow g^n = (g^k)^q = e^q = e$。

引理 4.2.7 设 G 是群，$g \in G$。
(1) 若 $\mathrm{ord}(g) = \infty$，则 $\forall i, j \in \mathbb{Z}$，都有 $g^i \neq g^j$；
(2) 若 $\mathrm{ord}(g) = k \in \mathbb{Z}^+$，则 $k = |< g >|$ 并且 $< g >= \{e, g, \ldots, g^{k-1}\}$。

证明: (1) 用反证法。如果 $\exists i, j$ 使得 $g^i = g^j$，不妨设 $i > j$，则 $g^{i-j} = e$，与 $\mathrm{ord}(g) = \infty$ 矛盾!
(2)$< g >= \{g^n \mid n \in \mathbb{Z}\}$。而对每个 $n \in \mathbb{Z}$，都可以作带余除法 $n = qk + r$, $r \in \{0, \ldots, k-1\}$，此时 $g^n = g^{qk} g^r = g^r \in \{e, g, \ldots, g^{k-1}\}$。而 $\forall i, j \in \{0, 1, \ldots, k-1\}, i \neq j$，有 $g^i \neq g^j$(否则不妨设 $i > j$，则 $g^{i-j} = e$，而 $i - j < k$，这与 k 的最小性矛盾!)。此即我们所需要的结论。 □

推论 4.2.1 设 G 是有限群，$g \in G$，则 $\mathrm{ord}(g) \,\big|\, |G|$。

这是 Lagrange 定理的直接推论。
下面我们可以对循环群的结构进行讨论了。

定理 4.2.2 设 G 是循环群，若 $|G| = \infty$，则 $G \simeq (\mathbb{Z}, +, 0)$；若 $|G| = n$, $n \in \mathbb{Z}^+$，则 $G \simeq (\mathbb{Z}_n, +, \overline{0})$。

证明: (1) 设 $G =< g >$，如果 $\mathrm{ord}(g) = \infty$，则可以作映射:

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z} \\ g^n &\longmapsto n. \end{aligned}$$

由引理 4.2.7(1) 易证 φ 是双射，并且 $\varphi(g^m g^n) = \varphi(g^{m+n}) = m+n = \varphi(g^m) + \varphi(g^n)$，即 φ 是同构。
(2)G 是循环群且 $|G| = n$，那么 G 的生成元 (不妨记作 a) 一定是 n 阶元。由引理 4.2.7(2) 知 $G =< a >= \{e, a, \ldots, a^{n-1}\}$，于是可以作映射：

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z}_n \\ a^j &\longmapsto \bar{j}. \end{aligned}$$

容易验证 φ 是良定义的双射并且是同态，于是 φ 是同构。 □

例 4.2.12 G 是群且 $|G| = 4$，则必有 $G \simeq \mathbb{Z}_4$ 或 $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$。

证明: 由 Lagrange 定理，G 中元素的阶只可能是 1，2，4。(1) 如果 G 中有一个 4 阶元 g，则容易作同构 $G \to \mathbb{Z}_4$，$g \mapsto \bar{1}$(验证留作练习)。
(2) 若 G 中只有单位元 e 和三个二阶元 a, b, c，则作映射

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \\ e &\longmapsto (\bar{0}, \bar{0}) \\ a &\longmapsto (\bar{1}, \bar{0}) \\ b &\longmapsto (\bar{0}, \bar{1}) \\ c &\longmapsto (\bar{1}, \bar{1}). \end{aligned}$$

容易验证这是一个同构。 □

命题 4.2.3 (1) 循环群都是交换群，并且其任何子群都是循环群；
(2) 无限循环群 G 的子群必然同构于 $(m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}, +, 0)$；
(3)G 是 n 阶循环群，则对每个 $m \mid n$，存在 G 的唯一 m 阶子群。[1]

证明留作练习。

由一个元素生成的群是循环群，我们已经讲的比较清楚了。我们可以进一步考虑由一些元素生成的群，这就需要生成组的概念。

定义 4.2.10 (**生成组**) 设 G 是群，$S \subset G$ 是非空子集，如果包含 S 的 G 的子群只有 G 本身，则称 S 是 G 的生成组。

我们也可以这样来看待这个定义：将所有包含 S 的 G 的子群作交集，得到的还是一个子群 (引理 4.2.5 推广到任意交也成立，用定义即可证明)，记其为 $< S >$。即 $< S >$ 是 G 中包含 S 的最小的子群。如果 $< S >= G$，则 S 是 G 的生成组。此外，我们还可以从元素运算的角度定义生成组：记 $S^{-1} = \{a^{-1} \mid a \in S\}$，则

$$< S >= \{x_1 \cdots x_m \mid m \in \mathbb{Z}^+,\ x_i \in S \cup S^{-1}, i = 1,\ \ldots, m\}$$

可以证明这两个定义是一致的 (留作习题)。

例 4.2.13 $\mathrm{GL}_n(\mathbb{R})$ 的生成组是 $\mathbb{R}$ 上所有 n 阶初等矩阵的集合；S_n 的生成组是全体对换或全体循环。

[1]这个结论可以推广到：G 是 n 阶群，则 G 是循环群 $\iff$ 对每个 $m \mid n$，存在唯一 G 的 m 阶子群。证明较难，可以参考《抽象代数学习辅导》孟道骥等著，科学出版社 P47。

当生成组 S 是有限集时我们称群 G 是**有限生成**的，显然有限群必然是有限生成的，但有限生成的群可以是无限群，例如 $(\mathbb{Z},+,0)=<1>$ 就是有限生成的。

接下来我们更深入地讨论群同态和同构的一些性质。

定义 4.2.11 设 $f:(G,*,e)\to(H,\cdot,\varepsilon)$ 是群同态，我们定义同态核 $\ker(f)=\{x\in G\mid f(x)=\varepsilon\}$，同态像 $\mathrm{im}(f)=\{y\in H\mid \exists x\in G\text{使得}y=f(x)\}$。

容易验证 $\ker(f)$ 和 $\mathrm{im}(f)$ 分别是 G 和 H 的子群。我们验证 $\ker(f)$ 是 G 的子群，另一个验证留作练习。设 $a,b\in\ker(f)$，即 $f(a)=f(b)=\varepsilon$ 则 $f(ab^{-1})=f(a)[f(b)]^{-1}=\varepsilon$，所以 $ab^{-1}\in\ker(f)$。由引理 4.2.4 即得结论。

我们有更进一步的结论：$\ker(f)$ 是 G 的正规子群[1]，并且 G 的每个正规子群都是 G 到某个群的同态核。我们会在抽象代数课程中证明这一点。

例 4.2.14 (1) 令 $\varphi:S_n\to(\{\pm1,\times,1\})$, $\sigma\mapsto\varepsilon_\sigma$，则 $\ker(f)=A_n$。

(2) 令 $\varphi:S_n\to\mathrm{GL}_n(\mathbb{R})$, $\sigma\mapsto A=(a_{ij})_{n\times n}$，其中 $a_{ij}=\begin{cases}1, & i=\sigma(j);\\ 0, & i\neq\sigma(j).\end{cases}$ 则 $\ker(\varphi)=\{e\}$。

引理 4.2.8 设 $f:(G,*,e)\to(H,\cdot,\varepsilon)$ 是群同态，则 f 是单同态 $\iff\ker(f)=\{e\}$；f 是满同态 $\iff\mathrm{im}(f)=H$。

直接按照单同态和满同态的定义即可证明。

下面的定理表明了变换群在群论中的重要作用。

定理 4.2.3 (Cayley **定理**) 任何一个群 G 都同构于 G 到自身的变换群 T_G(定义于例 4.2.2(3)) 的某一个子群。

证明: 作映射 $\varphi:G\to T_G$, $g\mapsto L_g$，其中 L_g 是引理 4.2.1 中定义的左平移变换 (显然 $L_g\in T_G$)。首先，φ 是同态，这是因为任取 $g_1,g_2\in G$ 及 $x\in G$，有 $L_{g_1g_2}(x)=g_1g_2x=L_{g_1}\circ L_{g_2}(x)$，从而

$$\varphi(g_1g_2)=L_{g_1g_2}=L_{g_1}\circ L_{g_2}=\varphi(g_1)\circ\varphi(g_2).$$

其次 φ 是单射，这是因为：如果 $\varphi(g_1)=\varphi(g_2)$，即 $L_{g_1}=L_{g_2}$，则 $L_{g_1}(e)=L_{g_2}(e)$，即 $g_1e=g_2e$，$g_1=g_2$。于是 $\mathrm{im}(\varphi)$ 作为 T_G 的子群与 G 同构。 □

推论 4.2.2 设 G 是 n 阶群，则 G 同构于 S_n 的某一个子群。

证明留作练习。

需要注意的是，无限群可以同构于自身的一个真子群，例如 $m\mathbb{Z}<\mathbb{Z}$，但 $\mathbb{Z}\to m\mathbb{Z}:n\mapsto mn$ 就是一个同构。

最后，我们考虑群到自身的同态 (或同构) 映射，称为群的**自同态** (**或自同构**)。

命题 4.2.4 群 G 到自身的所有同态的集合 (记作 $\mathrm{Hom}(G)$) 在映射复合下构成了一个幺半群；G 到自身的所有同构的集合 (记作 $\mathrm{Aut}(G)$) 在映射复合下构成群。

证明留作练习。

[1] 即 $\forall g\in G$, $a\in\ker(f)$，有 $gag^{-1}\in\ker(f)$。

定义 4.2.12 我们称形容：$I_a : G \to G,\ g \mapsto aga^{-1}$ 的 G 的自同构 (验证这是同构留作练习) 为群 G 的内自同构映射。容易验证 G 的所有内自同构映射构成一个群 (练习)，称为 G 的内自同构群，记作 $\mathrm{Inn}(G)$。

可以证明 $\mathrm{Inn}(G)$ 是 $\mathrm{Aut}(G)$ 的一个正规子群，并且 G 是交换群 $\iff$ $\mathrm{Inn}(G)$ 是平凡群 $\{\mathrm{id}\}$。

例 4.2.15 设 G 是有限群，设 $\varphi \in \mathrm{Aut}(G), \varphi^2 = \mathrm{id}_G$，并且若 $a \neq e$ 则一定有 $\varphi(a) \neq a$，则：
(1)G 是交换群；
(2)$|G|$ 是奇数。

证明: 首先，任取 $a \in G$，令 $g = \varphi(a)a^{-1}$，则

$$\varphi(g) = \varphi^2(a)[\varphi(a)]^{-1} = a[\varphi(a)]^{-1} = [\varphi(a)a^{-1}]^{-1} = g^{-1}.$$

下面说明 g 能取遍 G。注意到如果 $\varphi(a)a^{-1} = \varphi(b)b^{-1}$，则

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

于是 $b^{-1}a = e$，即 $a = b$。这说明 $\psi : a \to \varphi(a)a^{-1}$ 是单射。由定理 1.3.3 知 ψ 是双射，即当 a 取遍 G 时 g 可以取遍 G。

那么 φ 就是映射 $G \to G,\ g \mapsto g^{-1}$。于是：
(1)$\forall a, b \in G,\ ab = \varphi(a^{-1})\varphi(b^{-1}) = \varphi((ba)^{-1}) = ba$。即 G 是交换群。
(2) 先证明：如果 $g_i \neq g_j$且$g_i \neq g_j^{-1}$，则 $\{g_i, g_i^{-1}\} \cap \{g_j, g_j^{-1}\} = \emptyset$。这只需证明 $g_j \neq g_i^{-1}$(思考之)。用反证法。如果 $g_j = g_i^{-1}$，则 $g_j = \varphi(g_i)$，即 $g_j^{-1} = \varphi(g_j) = \varphi^2(g_i) = g_i$，这与 $g_i \neq g_j^{-1}$ 矛盾!

于是 G 由 e 与成对的 $\{g_i, g_i^{-1}\},\ i = 1, \ldots, k$ 组成，不同的 i 对应的对交为空集。所以 $|G|$ 是奇数。 □

4.3 环

上一节我们介绍了群的概念和简单性质。然而，群中只有一种运算，而我们常见的数学结构中往往有两种或更多的运算，并且运算之间有联系。这时，我们就需要更多的工具来研究问题，例如本节的环。

定义 4.3.1 设 $(R,'+','0')$ 是一个交换群，如果 R 上还有另一种运算“乘法” $'\cdot'$，并且 $(R,'\cdot')$ 构成乘法半群 (即 $'\cdot'$ 满足结合律)，如果乘法对加法“+”还满足左右分配律，即 $\forall x,y,z\in R$:

$$(x+y)\cdot z = x\cdot z + y\cdot z;\ x\cdot(y+z) = x\cdot z + y\cdot z.$$

则称 $(R,'+','\cdot')$ 是一个环。

注 4.3.1 (1) 一般地，我们研究的环都要求乘法构成一个幺半群，即乘法有单位元 $'1'$，称为幺环。以后，如果我们不作特别说明的话，我们所说的环都是幺环，同时标明乘法单位元。
(2) 以后，在不引起歧义的情况下，我们经常将乘法的“$\cdot$”省略。

例 4.3.1 (1)$(\mathbb{Z},+,0,\cdot,1)$, $(\mathbb{Q},+,0,\cdot,1)$, $(\mathbb{R},+,0,\cdot,1)$, $(\mathbb{C},+,0,\cdot,1)$ 都是环。
(2) 由 4.1 节最后的大段论述可知，$(\mathbb{Z}_n,+,\overline{0},\cdot,\overline{1})$ 是环，称为模 n 的剩余类环。
(3) 所有 n 阶方阵的集合在矩阵的加法和乘法下构成环，称 $(M_n(\mathbb{R}),+,O_{n\times n},\cdot,E_n)$ 为 n 阶矩阵环。
(4) 设 X 是集合，R 是环，我们将所有 $X\to R$ 的函数放在一起做成一个集合，记为 R^X，在 R^X 上定义加法和乘法如下：$\forall f,g: X\to R$，定义：

$$\begin{aligned} f+g: X &\longrightarrow R & \qquad f\cdot g: X &\longrightarrow R \\ x &\longmapsto f(x)+g(x) & x &\longmapsto f(x)\cdot g(x) \end{aligned}$$

容易验证 (验证留作练习) 这是一个环，0 函数和 1 函数分别是其加法单位元和乘法单位元，称为 X 到 R 的函数环。
(5) 设 $(A,+,0)$ 是一个加法交换群，在 A 上定义乘法：$\forall x,y\in A$，定义 $x\cdot y=0$，则 A 关于这个乘法是一个半群 (但不是幺半群！)，我们称 $(A,+,0,'\cdot')$ 是 A 的零乘法环 (不是幺环)。

以后，我们将 R 对于加法做成的群的单位元 0 为 R 的零元，乘法幺半群的的单位元 1 称为幺元。设 $a\in R$，我们将 a 在加法运算下的逆记为 $-a$，称为 a 的负元。将 $m(\in\mathbb{Z}^+)$ 个 a 连加得到的结果记为 ma，并规定 $0a=0$, $(-n)a=-(na)$。此外，将 m 个 a 连乘得到的结果记为 a^m。此外，将 $a+(-b)$ 简记为 $a-b$。

命题 4.3.1 (1) 对 $\forall a,b\in R$ 和 $m,n\in\mathbb{Z}$，我们有 $(m+n)a=ma+na$, $m(-a)=-(ma)$, $(mn)a=m(na)$, $m(a+b)=ma+mb$[1];

(2) 对 $\forall a\in R$, $m,n\in\mathbb{Z}^+$，有 $a^{m+n}=a^ma^n$, $a^{mn}=(a^m)^n$;

(3) 广义分配律：$a_1,\dots,a_n,b_1,\dots,b_m\in R$，则 $(\sum_{i=1}^n a_i)(\sum_{j=1}^m b_j)=\sum_{i=1}^n\sum_{j=1}^m a_ib_j$;

(4) $\forall a,b\in R$，有 $a0=0a=0$(这里 0 是 R 的零元) 以及 $(-a)b=a(-b)=-(ab)$，$(-a)(-b)=ab$。

[1]即任何一个环的加法结构可以视作整数环 $\mathbb{Z}$ 上的左模。实际上交换群即可满足这些性质，为此，我们可以使用主理想整环上的有限生成模结构定理来给出有限生成交换群的分类，我们会在抽象代数中学习。

证明: (1)(2) 的证明比较简单，留作练习。(3) 只需对 m,n 分别做数学归纳法即可。
对于 (4)，首先 $a0 = a(0+0) = a0 + a0$，于是 $0 = a0$(加法成群，因此有消去律)。$0a = 0$ 同理可证。其次，注意到 $a(b+(-b)) = a0 = 0$，用分配律展开得 $ab + a(-b) = 0$，而 ab 的负元为 $-(ab)$，所以 $a(-b) = -ab$。$(-a)b = -(ab)$ 同理。最后，$(-a)(-b) = -(a(-b)) = -(-ab) = ab$。 □

推论 4.3.1 (**二项式定理**) 设 R 是环，$a,b \in R$ 且 $ab = ba$，$n \in \mathbb{Z}$，则

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

证明是简单的，留作练习。

一个平凡的情形是，如果一个环 R 中 $0 = 1$，那么 R 中只有一个元素 0。这是因为 $\forall a \in \mathbb{R}$，有 $a = a\cdot 1 = a\cdot 0 = 0$。零环的结构简单，没有研究价值，因此下面我们只要不特别声明，均要求环 R 中 $0 \neq 1$。

定义 4.3.2 设 R 是环，$a \in R\setminus\{0\}$，如果 $\exists b \in R\setminus\{0\}$ 使得 $ab = 0$，则称 a 为 R 中的左零因子；反过来，$b \in R\setminus\{0\}$，如果 $\exists a \in R\setminus\{0\}$ 使得 $ab = 0$，则称 b 为 R 中的右零因子。左零因子和右零因子统称为零因子。如果 R 中乘法是交换的，则不区分左零因子和右零因子。

例 4.3.2 (1)$(\mathbb{Z},+,0,\cdot,1)$ 中没有零因子。
(2)$(M_n(\mathbb{R}),+,O_{n\times n},\cdot,E_n)$ 中，矩阵 A 是零因子 $\iff \operatorname{rank}(A) < n$。
这是因为：如果存在非零矩阵 B 使得 $AB = O_{n\times n}$ 或 $BA = O_{n\times n}$，则由 Sylvester 不等式易得 $\operatorname{rank}(A) < n$；反之，$\operatorname{rank}(A) < n$ 可知 $A\mathbf{x} = \mathbf{0}$ 的解空间 V_A 不是零子空间，设 $\mathbf{v} \in V_A$，令 $B = (\mathbf{v},\mathbf{0},\cdots,\mathbf{0})$ 即有 $AB = O_{n\times n}$。

命题 4.3.2 R 是无零因子环 $\iff$ R 满足左右消去律 (即 $x \neq 0$，则 $xy = xz$ 或 $yx = zx$ 都可以得到 $y = z$)。

这个命题在群当中是显然的，因为我们可以左乘 (或右乘)x^{-1} 直接得到结论。但在环中，由于元素关于乘法不一定可逆，因此我们需要借助加法。

证明: ($\Longrightarrow$) 由 R 中无零因子，故 $xy = xz \Rightarrow x(y-z) = 0 \Rightarrow y - z = 0$，即 $y = z$。右消去律同理。
($\Longleftarrow$) 设环 R 满足左右消去律，则若 $ax = 0$，即 $ax = a0$，由左消去律得 $x = 0$，即 R 没有右零因子；同理可证 R 没有左零因子。 □

下面我们定义一些特殊的环。

交换环 (abelian ring)	R 上的乘法满足交换律
整环 (integral domain)	无零因子交换幺环
除环 (体，斜域，division ring)	$R\setminus\{0\}$ 关于乘法成群，即非零元关于乘法都可逆
域 (field)	交换的除环，即可以进行“通常”的加减乘除的结构

定义 4.3.3 设 R 是环，$a \in R$，如果存在 $b \in R$ 使得 $ba = 1$，则称 a 右可逆；同理可以定义左可逆。如果 a 既是左可逆的又是右可逆的，则称 a 是 R 中的 (乘法) 可逆元或者单位 (unit)。如果 a 可逆，则逆一定唯一，证明方法类似于逆矩阵的唯一性。显然 R 中的所有单位关于 R 上的乘法构成群 (验证留作练习)，称为 R 的单位群 (unit group)，记作 $R^\times$ 或 U_R。

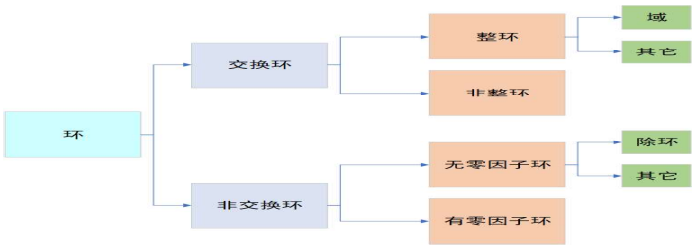

图 4.1: 环

首先，零因子一定不会是单位，这是因为如果环 R 中 $ab=0$, $a,b\neq 0$，那么如果 $ac=ca=1$，就有 $a(c+b)=1$，那么 $c+b=ca(c+b)=c$，即 $b=0$，矛盾！

例 4.3.3 矩阵环 $M_n(\mathbb{R})$ 中的所有单位是 $\mathrm{GL}_n(\mathbb{R})$。

命题 4.3.3 在剩余类环 $\mathbb{Z}_n$ 中：
(1)$\overline{m}$ 是单位 $\iff \gcd(m,n)=1$；
(2)$\overline{m}$ 是零因子 $\iff \gcd(m,n)>1$ 且 $n\nmid m$。

证明: 命题的前一部分已经在命题 4.1.2 中证明过了，下面证明后一部分。
($\Longrightarrow$) 由 $\overline{m}$ 是零因子，即 $\overline{m}\neq\overline{0}$ 且 $\overline{m}$ 不可逆，即 $n\nmid m$ 且 $\gcd(m,n)>1$。
($\Longleftarrow$) 设 $g=\gcd(m,n)$，由 $g>1$，$n\nmid m$ 可知 $\exists k,l\in\mathbb{Z}$ 使得 $m=kg$，$n=lg$ 并且 $\overline{l}\neq\overline{0}$，于是 $lm=lkg=kn$，即 $\overline{lm}=\overline{lm}=\overline{0}$。 □

于是 $\mathbb{Z}_n$ 的单位群 $\mathbb{Z}_n^\times$ 中有 $\varphi(n)$ 个元素 ($\varphi(n)$ 是欧拉函数，表示小于 n 并且与 n 互素的正整数个数)。特别地，当 p 是素数时，$|\mathbb{Z}_p^\times|=p-1$。于是我们有下面的定理。

定理 4.3.1 (Euler **定理**) 对 $\forall a\in\mathbb{Z}$, $n\in\mathbb{Z}^+$，假设 $\gcd(a,n)=1$，则有 $a^{\varphi(n)}\equiv 1 \mod n$，其中 φ 是欧拉函数。特别地，若 p 是素数，则 $a^{p-1}\equiv 1 \mod p$(Fermat 小定理)。

证明: 由于 $\gcd(a,n)=1$，故可以任取 $\overline{a}\in\mathbb{Z}_n^\times$，由于 $\mathbb{Z}_n^\times$ 关于剩余类的乘法是群，故可以考虑 $\overline{a}$ 在这个群中的阶 $\mathrm{ord}(\overline{a})$。由推论 4.2.1，我们有 $\mathrm{ord}(\overline{a})\mid|\mathbb{Z}_n^\times|$，又由上面的论证知 $|\mathbb{Z}_n^\times|=\varphi(n)$，即 $\overline{a}^{\varphi(n)}=\overline{1}$，也即 $a^{\varphi(n)}\equiv 1 \mod n$。特别地，当 p 是素数时，$\varphi(p)=p-1$，即得到 Fermat 小定理。
□

类似于群的同态和同构，我们可以定义环的同态和同构。

定义 4.3.4 设 $(R,+,0_R,\cdot,1_R)$ 和 $(S,+,0_S,\cdot,1_S)$ 是两个环，$\varphi: R\to S$。如果对 $\forall z,y\in R$，有 $\varphi(x+y)=\varphi(x)+\varphi(y)$, $\varphi(xy)=\varphi(x)\varphi(y)$ 成立，则我们称 φ 是环同态。类似地我们可以定义单同态、满同态和同构的概念。

例 4.3.4 $\pi_n:\mathbb{Z}\to\mathbb{Z}_n$, $a\mapsto\overline{a}$ 是环同态，验证留作练习。

定义 4.3.5 设 $\varphi:R\to S$ 是环同态，我们同样可以定义同态核：$\ker(\varphi)=\{r\in R\mid\varphi(r)=0_S\}$ 和同态像：$\mathrm{im}(\varphi)=\{s\in S\mid\exists r\in R\text{使得}\varphi(r)=s\}$。

命题 4.3.4 设 $\varphi:R\to S$ 是环同态，则 φ 是单同态 $\iff \ker(\varphi)=\{0_R\}$。

直接利用定义即可证明。

命题 4.3.5 设 R,S 是环，S 无零因子。如果环同态 $\varphi: R \to S$ 不是零同态 (即 $\forall x \in R,\ \varphi(r) = 0_S$)，那么 $\varphi(1_R) = \varphi(1_S)$。

证明: 注意到 $\varphi(1_R)\varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R)$，即 $\varphi(1_R)(\varphi(1_R) - 1_S) = 0_S$，由 S 无零因子，故 $\varphi(1_R) = 0_S$ 或 $\varphi(1_R) = 1_S$。前者表明 $\forall r \in R,\ \varphi(r) = \varphi(1_R)\varphi(r) = 0_S$，即零同态；后者即我们所需要的结论。 □

下面我们考虑一个重要的定义：环的**特征** (characteristic)，它反映了环的加法性质。

定义 4.3.6 设 R 为环。如果 1 在加法群 $(R,+,0)$ 中是无穷阶的，则称 R 的特征为 0；反之，如果 1 在 $(R,+,0)$ 中是 $n(\in \mathbb{Z}^+)$ 阶的，则称 R 的特征为 n。我们将环 R 的特征记为 $\mathrm{char}(R)$。

例 4.3.5 $\mathrm{char}(\mathbb{Z}) = 0,\ \mathrm{char}(\mathbb{Z}_n) = n.$

命题 4.3.6 如果环 R 的特征 $\mathrm{char}(R) = m > 0$，$n \in \mathbb{Z}$ 且 $m \mid n$，则任意 $r \in R$，有 $nr = 0$。

证明: 设 $n = km$，则 $nr = kmr = k(\underbrace{1 + \cdots + 1}_{\text{m 个}})r = k(0r) = 0$(这里 $1 \in R$)。 □

命题 4.3.7 设 R 为无零因子环，令 $R^* = R \setminus \{0\}$, 则 R^* 中的元素对于 R 的加法具有相同的阶，且当这一共同的阶有限时，必为素数。

证明: 首先，如果 R^* 中的所有元素关于加法都是无穷阶的，那么命题显然成立。

其次，如果存在 $a \in R^*$ 使得 a 关于加法的阶是一个有限的正整数 n，那么，对任意的 $b \in R^*$，我们需要证明 b 的加法阶也是 n。由于 $na = 0$，注意到 $0 = 0b = (na)b = a(nb)$，而 R 是无零因子环，且 $a \neq 0$，于是 $nb = 0$，即 b 的加法阶整除 n。设 b 的加法阶为 m，反过来对 a 进行上述讨论可得 $n \mid m$，所以 $n = m$，由 b 的任意性可知 R^* 中所有元素的加法阶都相同。

最后，如果 R^* 中元素的加法阶是 $n \in \mathbb{Z}^+$，我们需要证明 n 是素数。用反证法，如果存在 $k,l \in \{2,3,\ldots,n-1\}$ 使得 $n = kl$，则对 $a \in R^*$，有 $(ka)(la) = na^2 = (na)a = 0$，但由加法阶的定义可知 $ka \neq 0,\ la \neq 0$，于是 $ka,\ la$ 是零因子，这与 R 是无零因子环矛盾！这样我们完成了证明。□

上面的命题告诉我们无零因子环的特征必定为素数。反过来，如果环的特征是合数，则必有零因子 (证明留作练习)。

命题 4.3.8 设 R 为整环，其特征为素数 p，则对任何 $a,b \in R$，有

$$(a+b)^p = a^p + b^p, \quad (a-b)^p = a^p - b^p.$$

利用二项式定理及 $p \mid \binom{p}{k}$ (例 1.6.3) 即可证明。

类似于子群的概念，我们也可以定义子环：

定义 4.3.7 设 $(R,+,0,\cdot,1)$ 是环，如果 $S \subset R$，且 $(S,+,0,\cdot)$ 也是环 (这里有时并不要求 S 里有 1)，则称 S 是 R 的子环 (subring)。

利用定义我们很容易得到判断子环的充要条件：

命题 4.3.9 S 是环 R 的子环 $\iff \forall a,b \in S$，有 $a-b \in S,\ ab \in S$。

由此容易证明，环 R 的子环的子环还是 R 的子环，留作练习。

例 4.3.6 (1)$\mathbb{Z}$ 是 $\mathbb{Q}$ 的子环，任意 $m \in \mathbb{Z}$，$m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$ 是 $\mathbb{Z}$ 的子环。实际上，$\mathbb{Z}$ 的子环一定是 $m\mathbb{Z}$ 的形式 (验证之)。
(2) 设 R 是环，我们记 $C_R = \{c \in R \mid \forall r \in R,\ rc = cr\}$，称 C_R 为环 R 的中心，容易验证 C_R 是 R 的子环 (留作练习)。
(3) 设 $\varphi : R \to S$ 是环同态，容易验证 $\ker(\varphi)$ 和 $\mathrm{im}(\varphi)$ 分别是 R 和 S 的子环。
(4) 我们考虑闭区间 $[0,1] \to \mathbb{R}$ 的函数环 $\mathbb{R}^{[0,1]}$。作嵌入映射 $\varphi : \mathbb{R} \to \mathbb{R}^{[0,1]},\ x \mapsto 1_x$(其中 1_x 表示常值映射，它把 $[0,1]$ 闭区间上的数都映到 x)，则容易验证 φ 是单同态，于是我们可以将 $\mathbb{R}$ 视作 $\mathbb{R}^{[0,1]}$ 的子环 (确切地说是 $\mathrm{im}(\varphi) = \{1_x \mid x \in \mathbb{R}\}$ 是 $\mathbb{R}^{[0,1]}$ 的子环)。此外，容易验证 $[0,1]$ 上的所有有界函数、连续函数、可微函数构成的环 (分别记作 $\mathbb{R}_b^{[0,1]}, \mathbb{R}_c^{[0,1]}, \mathbb{R}_d^{[0,1]}$) 都是 $\mathbb{R}^{[0,1]}$ 的子环。

子环的性质还不够好，我们以后经常研究满足以下条件 (乘法吸收性) 的子环，即理想。

定义 4.3.8 设 I 为环 R 的子环，如果 $\forall a \in I, x \in R$，都有 $xa \in I$，则称 I 为 R 的左理想；如果 $\forall a \in I, x \in R$，都有 $ax \in I$，则称 I 为 R 的右理想。若子环 I 既是左理想，又是右理想，则称 I 为双边理想，简称理想 (ideal)。

显然 $\{0\}$ 和 R 本身是 R 的理想，称为平凡理想；再例如，$m\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想。有了理想的概念，我们就可以作商环了。我们将在抽象代数课程中学习后续的内容。

下面我们讨论一个特殊的例子：四元数除环 (四元数体)。它是由英国数学家 Hamilton 发现的，在代数学和微分几何上都有重要的作用。

首先，中学时我们就知道，每个复数 $a + b\sqrt{-1}$ 都可以看成一个实数对 (a,b). 而将复数看成实数对后, 加法和乘法可以表示为

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1)(a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$$

那么，按这个思路, 我们可以将每个四元数可以看成一个实数四元组, 然后再定义合理的加法和乘法，使得这个四元组能进行加减乘除运算 (只不过乘法不满足交换律)。不过这种做法似乎不够自然。下面我们利用矩阵将“虚”的部分实体化, 这样就可以更加自然地定义四元数的概念。首先注意到，如果将复数 $a + b\sqrt{-1}$ 写成一个矩阵

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

则所有复数的集合对应于 $M_2(\mathbb{R})$ 的一个子集

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

而且复数的加法和乘法恰好对应矩阵的加法和乘法。按照这个思路，我们考虑 $M_2(\mathbb{C})$ 中的子集

$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\beta & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$$

容易验证 $\mathbb{H}$ 是 $(M_2(\mathbb{C}), +, O_{2\times 2}, \cdot, E_2)$ 的一个子环。下面考虑 $\mathbb{H}$ 的性质。容易看出：

(1) $\mathbb{H}$ 中包含幺元 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$。

(2) 令

$$\mathbf{i}=\begin{pmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{pmatrix},\quad \mathbf{j}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\quad \mathbf{k}=\begin{pmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{pmatrix}.$$

则 $\mathbf{jk}=\mathbf{i}$, $\mathbf{kj}=-\mathbf{i}$，即 $\mathbb{H}$ 不是交换环。

(3) 如果

$$A=\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\neq O_{2\times 2}$$

则 A 可逆，而且

$$A^{-1}=\frac{1}{|\alpha|^2+|\beta|^2}\begin{pmatrix}\overline{\alpha} & -\beta\\ \overline{\beta} & \alpha\end{pmatrix}.$$

综上所述，$\mathbb{H}$ 是非交换的除环，这就是四元数除环。

现在我们回到最初的问题：将四元数写成实数四元组并定义加法和乘法。利用上面定义的 $\mathbf{i},\mathbf{j},\mathbf{k}$ 容易验证，对于 $\alpha=a+b\sqrt{-1},\beta=c+d\sqrt{-1}$，其中 $a,b,c,d\in\mathbb{R}$，有

$$\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}=\begin{pmatrix}a+b\sqrt{-1} & c+d\sqrt{-1}\\ -c+d\sqrt{-1} & a-b\sqrt{-1}\end{pmatrix}=a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}.$$

其中 $\mathbf{1}$ 是单位矩阵. 这样我们就可以将四元数看成四元实数组了，而四元实数组的加法就是对应的分量相加。对于乘法，$\mathbf{1}$ 是么元，而 $\mathbf{i},\mathbf{j},\mathbf{k}$ 满足

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-\mathbf{1},\ \mathbf{ij}=-\mathbf{ji}=\mathbf{k},\ \mathbf{jk}=-\mathbf{kj}=\mathbf{i},\ \mathbf{ki}=-\mathbf{ik}=\mathbf{j}.$$

将上述公式线性扩充到任何两个四元实数组, 即可得到乘法规则。

以后我们会知道，$\mathbb{R},\mathbb{C},\mathbb{H}$ 都可以视作 $\mathbb{R}$ 上的向量空间，并且这个向量空间中可以定义满足结合律的线性的乘法，而且非零元素对乘法都可逆。这种结构称为 $\mathbb{R}$ 上的可除代数 (division algebra)。Frobenius 证明了 $\mathbb{R}$ 上的可除代数必然同构于 $\mathbb{R},\mathbb{C}$ 或 $\mathbb{H}$ 中的一种，感兴趣的读者可以参考 Algebra, Thomas.W.Hungerford,GTM73 的 §9.6。

4.4 域

上一节中我们已经定义了域，这一节我们来讨论域的更多性质。以下我们默认域中 $0 \neq 1$。

定义 4.4.1 设 $(\mathbb{F}, +, 0, \cdot, 1)$ 是交换环，$0 \neq 1$，如果 $\mathbb{F} \setminus \{0\}$ 中的每个元素都是乘法可逆元，则称 $\mathbb{F}$ 是域。

显然 $\mathbb{F}$ 是域 $\iff \mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ 是乘法群。域一定是整环。

例 4.4.1 $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$($p$ 是素数) 都是域。

下面我们考虑如何从一个整环构造一个域，这个过程实际上是一个局部化 (localization) 的过程。关于一般的局部化，我们会在抽象代数中学习。

设 D 是整环，记 $D^* = D \setminus \{0\}$，则 D^* 满足：

(1)$1 \in D^*$;

(2) 若 $a, b \in D^*$，则 $ab \in D^*$. [1]

于是我们可以在 $D \times D^*$ 上定义如下的等价关系：设 $(a, b), (c, d) \in D \times D^*$，我们定义

$$(a, b) \sim (c, d) \iff ad = bc$$

下面我们验证 $\sim$ 确实是一个等价关系。

(1) 自反性：设 $(a, b) \in D \times D^*$，则由 $ab = ba$ 显然有 $(a, b) \sim (a, b)$;

(2) 对称性：设 $(a, b) \sim (c, d)$，即 $ad = bc$，所以 $bc = ad$，即 $(c, d) \sim (a, b)$;

(3) 传递性：如果 $(a_1, b_1) \sim (a_2, b_2)$, $(a_2, b_2) \sim (a_3, b_3)$，则 $a_1 b_2 = a_2 b_1$, $a_2 b_3 = a_3 b_2$，于是 $a_1 a_2 b_2 b_3 = a_2 a_3 b_1 b_2$，即 $(a_1 b_3 - a_3 b_1)(a_2 b_2) = 0$，由 $b_2 \neq 0$，于是 $a_1 b_3 - a_3 b_1 = 0$ 或 $a_2 = 0$，前者直接说明 $(a_1, b_1) \sim (a_3, b_3)$，后者表明 $a_1 b_2 = 0$, $a_3 b_2 = 0$ ，即 $a_1 = a_3 = 0$，所以 $a_1 b_3 = a_3 b_1 = 0$，即 $(a_1, b_1) \sim (a_3, b_3)$。

有了这个等价关系，我们可以定义商集 $F = D \times D^* / \sim$，为了书写简便，我们将 (a, b) 的等价类 $\overline{(a, b)} \in F$ 记作 $\dfrac{a}{b}$。下面我们在 F 上定义合适的加法和乘法运算使得 F 成为一个域。

令

$$\begin{aligned} +: F \times F &\longrightarrow F & \times: F \times F &\longrightarrow F \\ (\frac{a}{b}, \frac{c}{d}) &\longmapsto \frac{ad + bc}{bd} & (\frac{a}{b}, \frac{c}{d}) &\longmapsto \frac{ac}{bd} \end{aligned}$$

首先，我们定义的加法和乘法是良定义的，这只需用定义验证 (留作练习)：如果 $\dfrac{a}{b} = \dfrac{a'}{b'}$, $\dfrac{c}{d} = \dfrac{c'}{d'}$，则 $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a'}{b'} + \dfrac{c'}{d'}$ 及 $\dfrac{a}{b} \times \dfrac{c}{d} = \dfrac{a'}{b'} \times \dfrac{c'}{d'}$。

其次，容易验证 F 在这样定义的加法和乘法之下仍然是整环 (验证环，乘法交换，无零因子，细节留作练习)，其中，F 关于加法的零元是 $\dfrac{0}{1}$，乘法的幺元是 $\dfrac{1}{1}$，$\dfrac{a}{b}$ 关于加法的负元是 $\dfrac{-a}{b}$。

最后，若 $\dfrac{a}{b} \in F^*$(即 $\dfrac{a}{b} \neq \dfrac{0}{1}$)，则 $\dfrac{a}{b}$ 关于乘法的逆元是 $\dfrac{b}{a}$。

综上所述，F 是域，称为整环 D 的**分式域**。

注 4.4.1 我们可以将 D 嵌入到 F 中 $a \mapsto \dfrac{a}{1}$(这是一个单同态)，于是我们将 $\dfrac{a}{1}$ 也简记为 a。

由前面命题 4.3.3的讨论立刻有下面的定理：

[1] 以后我们会知道，满足这两条性质的环的非空子集称为乘性子集，我们可以在乘性子集上进行类似的操作，而不是仅限于 D^*。

定理 4.4.1 剩余类环 $\mathbb{Z}_n$ 是域 $\Longleftrightarrow$ n 是素数。

下面我们考虑域的同态。

定义 4.4.2 设 $\mathbb{F},\mathbb{K}$ 是两个域，如果 $\varphi:\mathbb{F}\to\mathbb{K}$ 是环同态，则称 φ 是域同态。如果 φ 是双射则称为域同构。

命题 4.4.1 设 $\varphi:\mathbb{F}\to\mathbb{K}$ 是非零的域同态，则 φ 必是单射。

证明: 只需证明 $\ker(\varphi)=\{0_{\mathbb{F}}\}$。用反证法。如果 $\exists a\in\mathbb{F}\setminus\{0_{\mathbb{F}}\}$ 使得 $\varphi(a)=0_{\mathbb{K}}$，则由命题 4.3.5有 $1_{\mathbb{K}}=\varphi(1_{\mathbb{F}})=\varphi(a^{-1}a)=\varphi(a^{-1})0_{\mathbb{K}}=0_{\mathbb{K}}$，即 $1_{\mathbb{K}}=0_{\mathbb{K}}$，矛盾! □

于是，我们在考虑域的同态时，只需要考虑单同态的情形，即我们只需要考虑把一个域嵌入到一个更大的域中。等价地有如下定义：

定义 4.4.3 设 P 是域，且 P 是域 $\mathbb{F}$ 的子环，则称 P 是 $\mathbb{F}$ 的子域，$\mathbb{F}$ 是 P 的扩域 (field extension)。

例 4.4.2 (1)$\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$，前者是后者的子域；
(2) 固定一个 $p\in\mathbb{Z}^+$ 是非平方数，则 $\mathbb{Q}(\sqrt{p})=\{a+b\sqrt{p}\mid a,b\in\mathbb{Q}\}$ 是 $\mathbb{Q}$ 的扩域 (验证留作练习)。

用定义容易验证，域 $\mathbb{F}$ 的任意多个子域的交也是 $\mathbb{F}$ 的子域。

定义 4.4.4 一个域如果不包含任何真子域，则称为素域。

为了研究素域的性质，我们需要将环的特征的概念应用到域上。设 $\mathbb{F}$ 是域，由于域是无零因子环，故 $\mathrm{char}(\mathbb{F})=0$ 或 $\mathrm{char}(\mathbb{F})=p$，$p$ 为素数。更进一步地，我们有

定理 4.4.2 (1) 有理数域 $\mathbb{Q}$ 和素数阶的剩余类域 $\mathbb{Z}_p$ 都是素域；
(2) 如果 $\mathbb{F}$ 是素域，则 $\mathbb{F}$ 必同构于 $\mathbb{Q}$ 或 $\mathbb{Z}_p$。

证明: (1) 设 P 是 $\mathbb{Q}$ 的子域，由于 $1\in P$，P 对加减法封闭，故 $\mathbb{Z}=<1>\subset P$，即 $\forall m,n\in\mathbb{Z}$，$m,n\in P$，又 P 中非零元都关于乘法可逆，即 $n\neq 0\Rightarrow n^{-1}\in P$，于是由乘法封闭知 $mn^{-1}\in P$，即 $\mathbb{Q}\subseteq P$。于是 $P=\mathbb{Q}$，即 $\mathbb{Q}$ 是素域。

同样地，设 p 是素数，L 是 $\mathbb{Z}_p$ 的子域，则 $\overline{1}\in L$，于是 L 包含 $\overline{1}$ 生成的加法子群 $<\overline{1}>$，但 $<\overline{1}>=\mathbb{Z}_p$，于是 $\mathbb{Z}_p\subseteq L\subseteq\mathbb{Z}_p$，所以 $L=\mathbb{Z}_p$，即 $\mathbb{Z}_p$ 是素域。

(2) 设 $\mathbb{F}$ 是素域，e 是其乘法幺元，$H=<e>$ 是 e 生成的加法子群。由于 $(me)(ne)=(mn)e$，$m,n\in\mathbb{Z}$，故 H 是 $\mathbb{F}$ 的子环，且 H 是整环 (域的子环一定是整环)。

(i) $\mathrm{char}(\mathbb{F})=0$，即 H 是无限阶循环群，则容易验证 $\varphi:H\to\mathbb{Z}$，$ne\mapsto n$ 是一个环同构 (双射显然，$\varphi((me)(ne))=\varphi((mn)e)=mn=\varphi(me)\varphi(ne)$)。作 H 的分式域 $\mathbb{K}$，我们可以将 φ 扩张成

$$\begin{aligned}\varphi':&\mathbb{K}\longrightarrow\mathbb{Q}\\&(me)(se)^{-1}\longmapsto ms^{-1}\end{aligned}$$

用定义容易验证 φ' 是域同构，注意到 $\mathbb{K}$ 是 $\mathbb{F}$ 的子域，而 $\mathbb{F}$ 是素域，故 $\mathbb{F}=\mathbb{K}$，即此时 $\mathbb{F}\simeq\mathbb{Q}$。

(ii) $\mathrm{char}(\mathbb{F})=p$，即 H 是 p 阶循环群 (p 为素数)，即 $H=\{0,e,\dots,(p-1)e\}$，满足 $pe=0$。容易验证 H 是域 (对于 $me\in H$，$m\in\{0,\dots,p-1\}$，由 m,p 互素可知存在 $s,t\in\mathbb{Z}$ 使得 $sm+tp=1$，做带余除法 $s=up+r$，$r\in\{0,1,\dots,p-1\}$，则可以验证 $(me)^{-1}=re$)。作映射 $\varphi:H\to\mathbb{Z}_p$，$me\mapsto\overline{m}$，容易验证这是一个域同构。而由 $\mathbb{F}$ 是素域可知 $H=\mathbb{F}$，即此时 $\mathbb{F}\simeq\mathbb{Z}_p$。 □

域扩张和域的自同构群的理论是伽罗瓦理论的基础，我们会在抽象代数中进一步学习。

最后我们简单讨论一下一般域上的线性代数，更详细的讨论会在下册抽象向量空间中进行。

设 $\mathbb{F}$ 是域，我们考虑坐标空间 $\mathbb{F}^n = \{(x_1, \cdots, x_n)^t \mid x_i \in \mathbb{F}\}$，则仿照 $\mathbb{R}^n$，在 $\mathbb{F}^n$ 上可以自然地定义加法和 “数乘 (域上的元素乘以向量)”。容易验证 $\mathbb{F}^n$ 也满足 2.1.1 小节中的运算律。同理我们也可以定义 $\mathbb{F}$ 上的矩阵空间 $\mathbb{F}^{m\times n}$ 和 $M_n(\mathbb{F})$，它们和 $\mathbb{R}$ 上的矩阵满足相同的运算律和性质 (验证之)。

例 4.4.3 设 $A = \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{2} & \overline{4} \\ \overline{1} & \overline{4} & \overline{2} \end{pmatrix} \in M_3(\mathbb{Z}_5)$，试计算 V_A 的维数和一组基。

解: 对 A 作如下的初等行变换:

$$A \xrightarrow{r_3 - r_1} \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{2} & \overline{4} \\ \overline{0} & \overline{2} & \overline{4} \end{pmatrix} \xrightarrow{r_3 - r_2} \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{2} & \overline{4} \\ \overline{0} & \overline{0} & \overline{0} \end{pmatrix}$$

即 $\mathrm{rank}(A) = 2$, 所以 $\dim(V_A) = 1$。在 $\mathbb{Z}_5$ 上解齐次线性方程组 $\begin{cases} x_1 + \overline{2}x_2 + \overline{3}x_3 = \overline{0} \\ \overline{2}x_2 + \overline{4}x_3 = \overline{0} \end{cases}$, 可得 $\begin{cases} x_1 = \overline{1}x_3 \\ x_2 = \overline{3}x_3 \end{cases}$。

取 $x_3 = \overline{1}$ 即有 $V_A =< (\overline{1}, \overline{3}, \overline{1})^t >$。

设 $\mathbb{F}$ 是域，我们同样可以定义 $M_n(\mathbb{F})$ 上的行列式，它满足如下性质:

命题 4.4.2 设 $\mathbb{F}, \mathbb{K}$ 是域，R 是 $\mathbb{F}$ 的子环，$\varphi : R \to \mathbb{K}$ 是环同态，令 $A = (a_{ij})_{n\times n} \in M_n(R)$，将 φ 扩张到矩阵上: $\varphi : M_n(R) \to M_n(\mathbb{K})$, $A \mapsto \varphi(A) = (\varphi(a_{ij}))_{n\times n}$，则 $\varphi(\det(A)) = \det(\varphi(A))$。

证明: 利用行列式的完全展开定义有:

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon_\sigma a_{\sigma(1)1} \cdots a_{\sigma(n)n}$$

由于 φ 是环同态，所以

$$\varphi(\det(A)) = \sum_{\sigma \in S_n} \varepsilon_\sigma \varphi(a_{\sigma(1)1}) \cdots \varphi(a_{\sigma(n)n}) = \det(\varphi(A))$$

即得结论。 □

推论 4.4.1 条件同上面的命题。若 $\varphi(A)$ 满秩，则必有 A 满秩。

利用 $\det(\varphi(A)) \neq 0 \Rightarrow \varphi(\det(A)) \neq 0 \Rightarrow \det(A) \neq 0$ 即可证明。需要注意的是，推论的逆命题不一定成立，反例的构造留作思考。

例 4.4.4 判断矩阵 $A = \begin{pmatrix} 2 & 7 & 6 & 4 \\ 5 & 8 & 11 & 9 \\ 3 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in M_4(\mathbb{Z})$ 是否满秩。

解: 作同态 $\pi_2 : \mathbb{Z} \to \mathbb{Z}_2$，$a \mapsto \overline{a}$，则

$$\pi_2(A) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{1} \\ \overline{1} & \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} & \overline{1} \end{pmatrix}$$

计算得 $\det(\pi_2(A)) = \overline{1} \neq \overline{0}$，于是 $\operatorname{rank}(A) = 4$，即 A 满秩。

本章的内容只是对抽象代数的一个浅显的介绍，更加深入的内容读者可以参考抽象代数的标准教材。