Contents

1

集合与关系

在了解群之前，引入一些基本的定义，尽管它们非常简单，但对于后续严谨的表达必不可少.

1.1 关系

Definition 1.1

若 A, B 为两个集合，则集合 $A \times B = \{(a, b) | a \in A \text{ and } b \in B\}$ 是 A 和 B 的**笛卡尔积** (Cartesian product).

Example 1.2

若集合 $A = \{1, 2\}, B = \{3, 4\}$，则 $AB = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$. n 维实数坐标可以表示为 $\mathbb{R}^n$ 的元素.

Definition 1.3

集合 A 和 B 的**关系** (relation) 是 $A \times B$ 的一个子集 R . 我们将 $(a, b) \in R$ 读作 a 与 b 相关，记作 aRb.

Example 1.4

恒等关系　集合 S 上的恒等关系 (equality relation) 定义为

$$\{(x, x) | x \in S\} \subset S \times S.$$

对于一个关系 R ，若它是集合 S 和它自身的笛卡尔积 $S \times S$ 的子集，则称其为一个 S **上的关系**.

Example 1.5

函数 $f(x) = x^3 (x \in \mathbb{R})$ ，可以写作集合 $\{(x, x^3) | x \in \mathbb{R}\}$ ，它是笛卡尔积 $\mathbb{R} \times \mathbb{R}$ 的子集，因此是 $\mathbb{R}$ 上的一个关系.
这说明，实函数 $y = f(x)$ 可以被简单地描述为 $\mathbb{R} \times \mathbb{R}$ 的一类子集，也即 $\mathbb{R}$ 上的一类关系，并且容易将 $\mathbb{R}$ 拓展到任意两个集合 X 和 Y .

Definition 1.6

从 X 到 Y 的**函数** ϕ 是 X 和 Y 之间的一个关系，其性质是每个 $x \in X$，恰好是一个有序对 (x, y) 的第一个成员. 这样的函数也称为 X 到 Y 的一个**映射**，记作 $\phi : X \to Y$. X 称作 ϕ 的定义域 (Domain)，Y 称作 ϕ 的陪域 (Codomain). X 的值域 (Range) 为 $\phi[X] = \{\phi(x) | x \in X\}$.

Example 1.7

可以将加法运算看作一个映射 $\phi : \mathbb{R}^2 \to \mathbb{R}$，对于一个加法等式 $a + b = c$，可以记作 $\phi((a, b)) = c$，或 $((a, b), c) \in \phi$，它们分别从映射和关系的角度描述.

Definition 1.8

集合 X 的**基数** (cardinality) 指 X 内元素的个数，记作 $|X|$.

Definition 1.9

对于函数 $\phi : X \to Y$，若 $\phi(x_1) = \phi(x_2)$ 当且仅当 $x_1 = x_2$，则称其为单射 (one to one)；若 ϕ 的值域等于陪域，则称其为满射 (onto)；若 ϕ 同时具有上述两条性质，则 ϕ 是一个双射，也称为一一对应 (one-to-one correspondence).

Example 1.10

若两个集合之间存在一一对应，则基数相等. 设函数 $f : \mathbb{R} \Rightarrow \mathbb{R}$，其中 $f(x) = x^2$，则 f 不是一个一一对应，因为 $f(2) = f(-2) = 4$，而 $2 \neq -2$. 同时它也不是一个满射，因为其值域是陪域的真子集. 设函数 $g : \mathbb{R} \Rightarrow \mathbb{R}$，其中 $g(x) = x^3$，则 g 既是一一对应也是满射.

1.2 等价关系

当关系具有某些特性时，我们称其为等价关系，这些特性可以从“相似”中抽象得到.

Definition 1.11

如果一个非空集合 S 上的一个关系 R 满足下列三条:

1. 自反性. 所有 $a \in S$ 都满足 aRa；
2. 对称性. 若 aRb，则 bRa；
3. 传递性. 若 aRb 且 bRc，则 aRc；

则称 R 是 S 的一个等价关系，通常记为“$\sim$”.

在等价关系的基础上，我们可以将集合中的元素进行分类. 对于每个 $a \in S$，定义

集合

$$S_a = \{x \in S \mid x \sim a\},$$

则 S_a 称为 S 中 a 的**等价类**.

Definition 1.12

集合 X 的**划分** (partial) 是 X 的非空子集的集合，使得每个 X 的元素 x 都只包含在这些子集的其中一个内.

Proposition 1.13

对于 $a, b \in S$，等价类 S_a 和 S_b 要么完全一样，要么没有交集. 去掉 $\{S_a \mid a \in S\}$ 中重复的集合，即可得到 S 的一组划分. 同时 S 的每一个划分都对应了一个 S 上的等价关系，其中 $a \sim b$ 当且仅当 a 和 b 属于该划分中的同一个单元.

Proof. 假设 $S_a \cap S_b \neq \varnothing$，则考虑元素 $c \in S_a \cap S_b$，对于任意的 $a \in S_a$ 和 $b \in S_b$，都有 $a \sim c$ 且 $c \sim b$. 根据传递性有 $a \sim b$，因此 $S_a = S_b$.

同样地，对于任意一个划分，定义关系 R，使得 aRb 当且仅当 a 和 b 属于划分中的同一个单元，很容易验证 R 满足等价关系的三条性质.

□

2

群与子群

2.1 二元运算

Definition 2.1

集合上的**二元运算** (binary operation) $*$ 是一个从 $S \times S$ 映射到 S 的函数. 对于每个 $(a,b) \in S \times S$，记 S 中的元素 $*((a,b))$ 为 $a * b$.

Definition 2.2

设 $H \subset S$，$*$ 为 S 上的一个二元运算，若对于任意 $a,b \in H$，都有 $a * b \in H$，则称子集 H 对于 $*$ **封闭**.

根据上述定义，S 自身一定是对二元运算 $*$ 封闭的，但子集 H 不一定.

Definition 2.3

$*$ 满足**交换律**当且仅当任意 $a,b \in S$，都有 $a * b = b * a$；满足**结合律**当且仅当任意 $a,b,c \in S$，都有 $(a * b) * c = a * (b * c)$.

2.2 群

Definition 2.4

一个群 $\langle G, * \rangle$ 是一个在二元运算 $*$ 下封闭的集合，且满足以下性质:

1. 对于任意 $a,b,c \in G$，都有 $(a * b) * c = a * (b * c)$, 即 $*$ 满足结合律.
2. 存在元素 $e \in G$，使得任意 $x \in G$ 满足

$$e * x = x * e = x.$$

   e 称为群 G 的单位元 (identity element).

3. 对任意 $a \in G$，都存在 $a' \in G$, 使得

$$a' * a = a * a' = e.$$

Definition 2.5

群中的元素个数称为群的阶 (order)，记作 $|G|$.

为方便起见，后面将省略二元运算的符号. 容易证明群中的单位元有且仅有一个: 设 e 和 e' 都是群 G 的单位元，$e \neq e'$，则 $ee' = e = e'$，矛盾.

Definition 2.6

若二元运算满足交换律，则 G 为阿贝尔群 (abelian group).

Example 2.7

所有整数 $\mathbb{Z}$ 在加法运算下构成群. 若 n 为任意整数，所有整除 n 的整数也构成群，记作 $n\mathbb{Z}$. $\mathbb{Z}$ 和 $n\mathbb{Z}$ 都是阿贝尔群.

Example 2.8

非零实数乘法群是所有非零实数在乘法运算下构成的群，即 $\mathbb{R}\backslash 0$. 所有正实数在乘法运算下也构成群，即 $\mathbb{R}^+$.

Theorem 2.9

G 上的二元运算满足左右消去律. 即对于任意 $a, b, c \in G$，若 $ab = ac$，则 $b = c$; 若 $ba = ca$，则 $b = c$.

Proof. 设 $ab = ac$ 且 $b \neq c$，则在等式两边左乘 a 的逆元 a'，得到

$$a'(ab) = a'(ac),$$

根据结合律以及单位元的性质，

$$(a'a)b = (a'a)c \Rightarrow eb = ec \Rightarrow b = c.$$

右消去律同理.

□

Theorem 2.10

对于任意 $a, b \in G$，等式 $ax = b$ 和 $xa = b$ 存在唯一解.

Proof. 设 a' 为 a 的逆元，注意到，$a(a'b) = (aa')b = eb = b$，因此 $a'b$ 是 $ax = b$ 的一个解. 若 $ax = b$ 存在两个不同的解 x_1 和 x_2，则 $ax_1 = ax_2 = b$，由 2.9 可得 $x_1 = x_2$，因此解唯一. 等式 $xa = b$ 同理. □

基于上述讨论，不难证明群中每个元素都存在唯一一个逆元. 由此唯一性，可得下述推论.

Corollary 2.11

在群 G 中，对任意的 $a, b \in G$，都有 $(ab)' = b'a'$.

我们可以将群的定义进一步弱化为单边定义，只定义左单位元和左逆. 将三条性质重新描述如下:

1. 对于任意 $a,b,c \in G$，都有 $(a*b)*c = a*(b*c)$，即 $*$ 满足结合律.
2. 存在元素 $e \in G$，使得任意 $x \in G$ 满足 $e*x = x$.
3. 对任意 $a \in G$，都存在 $a' \in G$，使得 $a'*a = e$.

下面证明该描述和定义 2.4 是等价的.

Proof. 对于任意 $x \in G$，有 $ex = x$ 以及 $x'x = e$，因此

$$x'x = x'(ex) = (x'e)x = e.$$

从等式中观察到

$$(x'e)x = x'x,$$

根据消去律，得到 $x'e = x'$，因此 e 也是右单位元.

因为 $x'x = e$，两边左乘一个 x，得到

$$x(x'x) = (xx')x = x = ex.$$

同样根据消去律，得到 $xx' = e$. 因此左逆也是右逆. □

2.3 子群

Definition 2.12

若 H 为群 G 的子集，对 G 的二元运算下封闭，且在群诱导的运算下构成一个群，则 H 为 G 的子群，记作 $H \leq G$. 若 $H \neq G$，则记作 $H < G$.

显然 $\{e\}$ 和 G 都是 G 的子群，它们被称为平凡子群. 子群的交仍然是子群，但子群的并不一定. 我们可以通过下述性质来判断子群.

Theorem 2.13

群 G 的子集 H 是子群当且仅当

1. H 在 G 的二元运算下封闭.
2. 单位元 $e \in H$.
3. 对于任意 $a \in H$，$a^{-1} \in H$.

上述三条直接使 H 满足了群的三条性质. 但实际上有更简单的判断方式.

Theorem 2.14

群 G 的子集 H 是子群当且仅当任意 $a,b \in H$，都有 $ab^{-1} \in H$.

Proof. 分配律始终成立. 考虑群的第二条性质，取 $a \in H$，则 $aa^{-1} = e \in H$，因此 H 包含单位元; 取 $ea^{-1} = a^{-1} \in H$，任意元素的逆元也在 H 中，即得证. □

子群中有一类特殊的子群，它可以由一个元素的幂次来生成，称做循环子群 (cyclic subgroups)，下面给出其定义.

Theorem 2.15

设 a 是群 G 中一元素，则

$$H = \{a^n | n \in \mathbb{Z}\}$$

是 G 的子群，并且是包含 a 的最小子群，即任何包含 a 的子群都包含 H.

Proof. 借助定理 2.14，对于任意 $a^m, a^n \in H$，都有 $a^m \left(a^n\right)^{-1} = a^{m-n} \in H$，因此 H 是 G 的子群.

对于任意包含 a 的子群，由子群运算的封闭性，必然包含 $a^n (n \in \mathbb{Z})$，即包含 H. 因此 H 是最小的包含 a 的子群. □

Definition 2.16

设 a 为群 G 中的元素，则 G 的子群 $\{a^n | n \in \mathbb{Z}\}$ 称为由 a 生成的 G 的循环子群，或简称 a 的 **生成群**，记作 $\langle a \rangle$. 若 $\langle a \rangle = G$，则称 a 为 G 的**生成元**，G 为 **循环群**.

2.4 群的例子

2.4.1 线性群

Example 2.17

所有实数的 $n \times n$ 可逆矩阵在矩阵乘法运算下构成一个群.

Solution. 记 $n \times n$ 可逆矩阵集合为 S，矩阵乘法结合律; 单位阵可逆，因此 S 包含单位元; 设 $A, B \in S$，则 A^{-1} 和 B^{-1} 也为可逆矩阵，满足群的第三条性质. 容易验证封闭性:

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = I_n.$$

■

上述集合 S 称为 **一般线性群**，通常记作 $GL(n, \mathbb{R})$. 其中行列式为 1 的矩阵也构成一个群，称为**特殊线性群**，通常记作 $SL(n, \mathbb{R})$. 因此 $SL(n, \mathbb{R})$ 是 $GL(n, \mathbb{R})$ 的子群.

$GL(n, \mathbb{R})$ 中的正交矩阵构成正交群，记作 $O(n, \mathbb{R})$. 正交群中行列式为 1 的矩阵构成特殊正交群，记作 $SO(n, \mathbb{R})$. 为我们所熟知的三维旋转矩阵，其构成的群就是 $SO(3)$. 由群的性质，旋转矩阵的叠加仍为旋转矩阵.

2.4.2 对称群

Definition 2.18

设 M 为非空集合，则 M 到自身的全部可逆变换构成的集合显然对于变换乘法构成一个群，这个群称为集合 M 的全变换群，可以写作

$$S(M)=\{\phi: M \to M \mid \phi\text{为双射}\}.$$

若 M 中有 n 个元素，则将 $S(M)$ 记为 S_n，称作 n 元**对称群**，其中元素称作**置换**.

对 M 中元素用 $1,2,\cdots,n$ 编号，则置换可以写作

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \alpha_1 & \alpha_2 & \cdots & \alpha_n\end{pmatrix},$$

表示 $\sigma(i)=\alpha_i$. 不难发现，S_n 实际上就是 n 个元素的全排列，因此 $\left|S_n\right|=n!$. 我们也容易得到置换的乘积

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

也就是从右往左执行置换操作，从而得到一个新的置换. 如果一个置换将 $1,2,\cdots,n$ 中的 m 个元素 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 按顺序变换，即

$$\sigma(\alpha_1)=\alpha_2,\sigma(\alpha_2)=\alpha_3,\cdots,\sigma(\alpha_m)=\sigma(\alpha_1).$$

而保持其余的元素不变，则 σ 称为一个**轮换**，可将其简写为

$$\sigma=(\alpha_1\alpha_2\cdots\alpha_m).$$

当 $m=2$ 时，σ 仅将两个元素交换，这样的轮换称为**对换**. 若两个轮换之间没有公共元素，则称其为不相交轮换. 不相交轮换的乘法运算显然是可以交换的.

Theorem 2.19

任意一个非单位的置换都能表示成一些不相交轮换的乘积，而且该表示是唯一的.

Proof. 设 σ 为一 n 元置换，在 $1,2,\cdots,n$ 中任取一个元素 α_1，则能够得到序列 $\{\alpha_i\}$，其中

$$\alpha_2=\sigma(\alpha_1),\alpha_3=\sigma(\alpha_2),\cdots,$$

由于元素个数有限，序列中一定会出现重复元素. 令 α_j 为第一个与它前面某个元素相同的元素，令该元素为 $\alpha_i(i<j)$，不难发现，若 $i\neq 1$，则

$$\sigma^{j-1}(\alpha_1)=\sigma^{i-1}(\alpha_1)=\alpha_j=\alpha_i.$$

因为 $\alpha_{i-1}\neq\alpha_{j-1}$，而 σ 是一个双射，因此上式不成立，i 只能为 1. 这表明 σ 在 $\alpha_1,\alpha_2,\cdots,\alpha_j$ 上构成一轮换. 重复上述操作，由于元素个数有限，σ 最终可以被分解为有限多个不相交轮换的乘积.

若存在两种不同的分解，则必有元素同时存在于两个不同的轮换中，这会导致 σ 不再是单射. 因此该分解具有唯一性. □

Proposition 2.20

设 $\sigma \in S_n$ 为一置换，$(\alpha_1\alpha_2\cdots\alpha_m)$ 为一轮换，则有

$$\sigma(\alpha_1\alpha_2\cdots\alpha_m)\sigma^{-1} = (\sigma(\alpha_1)\sigma(\alpha_2)\cdots\sigma(\alpha_m)).$$

Proof. 考虑 $\sigma(\alpha_i)$，首先通过变换 σ^{-1} 变为 α_i，然后通过轮换变为 α_{i+1}，最后通过 σ 变为 $\sigma(\alpha_{i+1})$. 以此类推，得到上述轮换. 若 $j \notin \{\sigma(\alpha_1), \sigma(\alpha_2), \cdots, \sigma(\alpha_m)\}$，容易验证其不发生变化. □

Proposition 2.21

轮换可分解为对换的乘积，即

$$(\alpha_1\alpha_2\cdots\alpha_m) = (\alpha_1\alpha_m)(\alpha_1\alpha_{m-1})\cdots(\alpha_1\alpha_2).$$

Proof. 若 $m = 2$，等式成立; 若 $m = k-1$ 成立，则

$$(\alpha_1\alpha_2\cdots\alpha_{k-1}) = (\alpha_1\alpha_{k-1})(\alpha_1\alpha_{k-2})\cdots(\alpha_1\alpha_2).$$

注意到

$$(\alpha_1\alpha_2\cdots\alpha_k) = (\alpha_1\alpha_k)(\alpha_1\alpha_2\cdots\alpha_{k-1}) = (\alpha_1\alpha_k)(\alpha_1\alpha_{k-1})(\alpha_1\alpha_{k-2})\cdots(\alpha_1\alpha_2).$$

结论得证. □

若置换可以被分解为偶数个对换，则称其为**偶置换**，反之为**奇置换**. 对换是奇置换，而包含奇数个元素的轮换是偶置换. S_n 中所有的偶置换构成群，记作 A_n.

置换的奇偶性能够在一个简单而有趣的例子上发挥作用. 设定一个类似于华容道的游戏: 每一次只能移动 16，使其和相邻方块交换位置，能否将下面中的 14 和 15 互换位置而 16 保持不变?

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	16

$\Rightarrow$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

从变换的结果来看是一个对换 $(14, 15)$，因此是奇置换. 但因为每个置换都包含 16，奇数次置换后 16 不可能回到原位置，因此该操作不可能实现.

Definition 2.22

二面体群是正 n 边形的对称群，通常记作 D_n.

D_n 可以看作对正 n 边形的翻折和旋转. 设 $T: P_n \to P_n$ 表示顺时针旋转 $2\pi/n$，$S: P_n \to P_n$ 表示某个翻折，则可以写出 D_n 中的所有元素.

$$D_n = \left\{I, T, \cdots, T^{n-1}, S, ST, \cdots .ST^{n-1}\right\}.$$

从中我们不难发现一些性质. 例如对于任意翻折 S，执行两次将使图形保持不变，即

$$SS = I \Rightarrow S = S^{-1}.$$

由于 T^iS 也是一个翻折，因此

$$T^iS = (T^iS)^{-1} = S^{-1}(T^i)^{-1} = ST^{-i}.$$

基于该结论，可以表示任意两个翻折的乘积

$$(ST^i)(ST^j) = S(T^iS)T^j = S(ST^{-i})T^j = T^{j-i}.$$

2.4.3 循环群

由定义 2.16，循环群是一类可由单个元素生成的群，并且显然是阿贝尔群. 若 G 为有限循环群，则定义其生成元 a 的阶[1]是包含 a 的循环子群的阶，即 $|\langle a\rangle|$. 若 G 为无限群，则 a 的阶无限.

由于整除的性质，循环群在整数数论中时常出现，下面给出几个定理.

Theorem 2.23

设 m 为正整数，n 为任意整数，存在唯一的整数 q 和 r 使得

$$n = mq + r(0 \le r < m).$$

Proof. 若 $n > 0$，则依次检验 $n-m, n-2m, \cdots, n-km$，若 $n-km$ 是第一个小于 0 的，则 $q = k-1, r = n-qm$. $n < 0$ 同理.

下面证明唯一性. 若存在两组不同的整数，使得

$$n = mq_1 + r_1,$$
$$n = mq_2 + r_2,$$

则两式相减，得到

$$m(q_1 - q_2) = r_2 - r_1.$$

因为 $q_1 - q_2 \neq 0$，所以 $m \mid m(q_1 - q_2)$，即 $m \mid (r_2 - r_1)$. 由于 $0 \le r1, r2 < m$，所以 $0 < |r_2 - r_1| < m$，不可能被 m 整除. 唯一性得证. □

[1] 元素的阶和群的阶定义并不相同，但它们共享一个名称.

在除法运算中，q 称为商 (quotient)，r 称为余数 (remainder).

Theorem 2.24

循环群的子群一定是循环群.

Proof. 设 G 为循环群，$H < G$. 若 H 为平凡子群，则为循环群. 若 H 非平凡，设 a 为 G 的生成元，则 H 中的元素都可以记作 $a^n (n \in \mathbb{Z})$. 设 m 是使 $a^m \in H$ 的最小正整数，则对于任意 $a^n \in H$，由定理 2.23 可知，存在唯一的整数 q 和 r 使得

$$n = mq + r (0 \leq r < m).$$

因此 $a^n = a^{mq+r}$. 可得

$$a^r = a^{n-mq} = \left(a^m\right)^{-q} a^n.$$

因为 $a^m, a^n \in H$ ，可知 $a^r \in H$. 若 $0 < r < m$，意味着 m 不是最小的正整数，与假设矛盾，因此 r 只能为 0，即 $n = qm$.

综上，H 中的任意元素都可以表示为 a^m 的幂次，因此 $H = \langle a^m \rangle$ 为循环群. □

Theorem 2.25

加法群 $\mathbb{Z}$ 的子群一定是 $n\mathbb{Z}$.

Proof. $\mathbb{Z}$ 显然是循环群，其中 $1, -1$ 都是生成元. 由定理 2.24 ，$\mathbb{Z}$ 的子群仍为循环群，且由其中最小的正整数生成. 因此 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的全部子群. □

这一定理使得我们可以优雅地定义**最大公约数** (greatest common divisor) .

Definition 2.26

设 r, s 为正整数，则循环群

$$H = \{nr + ms | n, m \in \mathbb{Z}\}$$

的正生成元 d 是 r 和 s 的最大公约数，记作 $d = \gcd(r, s)$.

容易证明 H 构成群，且 $H \subset \mathbb{Z}$，因此 H 是一个循环群. 对于 H 的正生成元 d ，因为 $r, s \in H$ ，所以 d 是 r 和 s 的公因子. 又因为 $d \in H$ ，可以将其写作

$$d = nr + ms (n, m \in \mathbb{Z}).$$

假设 c 也是 r 和 s 的公因子，c 一定整除 $nr + ms = d$. 因此 $c \leq d$ ，d 为最大公约数. 换言之，所有公因子中只有最大公约数可以被写成上式的形式.

从中也可以发现，当我们想要求得 $d = \gcd(r, s)$ 时，可以将其中一个数减去另一个数的倍数，其最大公约数不变. 设 $t = s - kr > 0$，则 $d = nr + ms = nr + m(t + kr) = (n + mk)r + mt$，因此 $\gcd(r, s) = \gcd(r, t)$，这就是**辗转相除法**.

此外，若两个数的最大公约数为 1，则称它们互素，因此有结论如下:

Corollary 2.27

若 r 和 s 互素，则存在整数 n 和 m，使得 $nr + ms = 1$.

Lemma 2.28

若 r 和 s 互素，且 $r \mid sm$，则 $r \mid m$.

Proof. 因为 r 和 s 互素，则存在整数 a 和 b，使得 $ar + bs = 1$. 等式两边同乘 m，得

$$mar + mbs = m,$$

因为 r 同时整除 mar 和 mbs，因此 $r \mid m$. □

Lemma 2.29

设 $G = \langle a \rangle$ 为有限循环群，则 $|G| = d$ 当且仅当 d 是最小的正整数使得 $a^d = e$.

Proof. 因为 $G = \langle a \rangle = \left\{a, a^2, \cdots, a^d\right\}$，其中包含单位元. 设 $1 \leq k < d$，使得 $a^k = e$，则

$$\langle a \rangle = \left\{a, a^2, \cdots, a^k\right\} \subsetneq G.$$

推出矛盾，因此 $a^d = e$. □

Theorem 2.30

设 G 为有限循环群，$|G| = n$，a 是 G 的一个生成元. 令 $b = a^s \in G$，b 的生成群 $H = \langle b \rangle \leq G$，设 $|H| = m$，则有

$$m = \frac{n}{\gcd(n, s)}.$$

Proof. 由引理，$|H| = m$ 当且仅当 m 是最小的正整数使得 $\left(a^s\right)^m = e$，即 $n \mid sm$. 设 $d = \gcd(n, s)$，则有

$$d = an + bs.$$

其中 $a, b \in \mathbb{Z}$. 两边同除以 d，得到

$$1 = a(n/d) + b(s/d).$$

因为 n/d 和 s/d 均为正整数，可知它们互素. 问题转化为找到最小的 m 使得

$$\frac{ms}{n} = \frac{m(s/d)}{(n/d)}$$

为整数. 由引理 2.28 可知，$(n/d) \mid m$，因此 $m = n/d$. □

由此我们可以很容易得到推论:

Corollary 2.31

设 G 为有限循环群，$|G| = n$，a 是 G 的一个生成元. 则 a^r 也为生成元当且仅当 r 和 n 互素.

2.5 陪集

Theorem 2.32

令 H 为 G 的子群，定义等价关系 $\sim_L$ 和 $\sim_R$，$a \sim_L b$ 当且仅当 $a^{-1}b \in H$，$a \sim_R b$ 当且仅当 $ab^{-1} \in H$. 则 $\sim_L$ 和 $\sim_R$ 都是 G 上的等价关系.

Proof. 给出 $\sim_L$ 是等价关系的证明.

自反性 设 $a \in G$，则 $a^{-1}a = e \in H$，因此 $a \sim_L a$.

对称性 设 $a \sim_L b$，则 $a^{-1}b \in H$，且 $\left(a^{-1}b\right)^{-1} = b^{-1}a$ 也在 H 中. 因此 $b \sim_L a$.

传递性 设 $a \sim_L b, b \sim_L c$，则 $a^{-1}b, b^{-1}c \in H$，$\left(a^{-1}b\right)\left(b^{-1}c\right) = a^{-1}\left(bb^{-1}\right)c = a^{-1}c \in H$，则 $a \sim_L c$. □

由定理 2.32，$\sim_L$ 定义了 G 的一个划分. 设 $a \in G$，则 a 的等价类可写作

$$G_a = \{x \in G \mid a \sim_L x\}.$$

设 $a^{-1}x \in H$，则存在 $h \in H$，使得 $a^{-1}x = h$，即 $x = ah$. 因此 $G_a = \{ah | h \in H\}$. 我们将它记作 aH . 同样地，对于等价关系 $\sim_R$，可以说明 a 的等价类表示为 $Ha = \{ha | h \in H\}$. 由此引入陪集的定义.

Definition 2.33

设 $H < G$，则 G 的子集 $aH = \{ah | h \in H\}$ 称为 H 包含 a 的**左陪集** (left coset)，$Ha = \{ha | h \in H\}$ 称为 H 包含 a 的**右陪集** (right coset).

根据等价关系的性质，H 的左陪集构成了 G 的一个划分，因此 H 的左陪集之间要么相等，要么不相交. 右陪集同理. 基于这一观察，可以得到**拉格朗日定理** (Theorem of Lagrange).

Theorem 2.34

设 H 是有限群 G 的子群，则 $|H|$ 是 $|G|$ 的因子.

Proof. 设 $|G| = n, |H| = m$，考虑 H 的左陪集 aH. 构建映射 $\phi : H \to aH$，其中 $\phi(h) = ah$，下面证明 ϕ 是一个双射.

假设 $\phi(h_1) = \phi(h_2)$，则 $gh_1 = gh_2$. 由消去律，可得 $h_1 = h_2$. 因此 ϕ 为单射. 同时由陪集定义，ϕ 为满射，因此 ϕ 构建了 H 到 aH 的一一对应，即陪集的元素个数和子群的元素个数相等.

又因为陪集定义了 G 的划分，设陪集中不重复的个数最多有 r 个，则 $n = rm$，即 $m \mid n$. □

Definition 2.35

设 H 是有限群 G 的子群，则 H 的左 (右) 陪集个数称做 H 在 G 中的指数 (index)，记作 $[G : H]$.

Corollary 2.36

素数阶群一定是循环群.

Proof. 设该素数阶群为 G，$|G| = p$. 由拉格朗日定理，G 的子群的阶只能是 1 或 p. 设 $a \in G$，则 a 的生成群 $\langle a \rangle$ 是 G 的子群. 若 $\langle a \rangle$ 的阶为 1，则 $a^2 = a = ae$, a 为单位元. 若 $\langle a \rangle$ 的阶为 p，则 $G = \langle a \rangle$ 为循环群. □

2.6 群的同构

同构是分析群的重要手段. 当群之间的映射能够保持运算“不变”，说明这一映射没有改变群的结构. 这是笼统的解释，下面给出同构的具体定义.

Definition 2.37

设 G 和 G' 为两个群，若存在一个从 G 到 G' 的一一对应 φ，使得所有的 $x, y \in G$ 都有

$$\varphi(xy) = \varphi(x)\varphi(y),$$

则称 G 和 G' **同构** (isomorphism)，记作 $G \cong G'$.

若一个映射 $f : X \to Y$ 具有性质 $f(xy) = f(x)f(y)$，则称映射 f **保持运算**.

Example 2.38

设 $\mathbb{R}^+$ 是全体正实数对乘法组成的群，$\mathbb{R}$ 是全体实数对加法组成的群，则映射 $\varphi : \mathbb{R}^+ \to \mathbb{R}$ 使得

$$\varphi(x) = \ln(x)$$

是一个一一对应，这是由函数 $\ln(x)$ 的单调性以及值域 $(-\infty, \infty)$ 保证的. 验证它保持运算：

$$\varphi(xy) = \ln(xy) = \ln(x)\ln(y) = \varphi(x)\varphi(y).$$

因此 φ 是一个同构，并且我们看到 $\mathbb{R}$ 和 $\mathbb{R}^+$ 上具有不同的二元运算.

显然，群的同构是一个等价关系，因此群可以通过同构加以分类，我们也可以通过同构来研究群的内部结构.

Theorem 2.39: 凯莱定理

任何一个群都同构与其上的变换群.

Proof. 设 G 是一个群，对于任意一个元素 $a \in G$，可以定义一个 G 上的变换 σ_a，使得

$$\sigma_a(x) = ax, x \in G.$$

因此我们得到 $|G|$ 个变换构成的集合 G_l，下面证明它构成群. 不难发现，σ_a 是一个双射. 首先对于任意 $x, y \in G$，由消去律可知，$ax = ay \Leftrightarrow x = y$，因此 σ_a 为单射. 同时对于任意 $x \in G$，都存在 y 使得 $ay = x$，因此 $aG = G$，σ_a 为双射.

双射是可逆的. 由

$$\sigma_{a^{-1}}\sigma_a(x) = a^{-1}ax = x.$$

$$\sigma_a\sigma_{a^{-1}}(x) = aa^{-1}x = x.$$

可知 σ_a 的逆变换为 $\sigma_{a^{-1}}$，仍在 G_l 中. 又有

$$\sigma_e\sigma_a = \sigma_a\sigma_e = \sigma_a,$$

其中 e 为群 G 的单位元，可知 G_l 是一个变换群，单位变换为 σ_e.

自然地，我们构造映射 $\varphi : G \to G_l$，使得

$$\varphi(a) = \sigma_a.$$

因为 $\sigma_a(e) = a$，因此 $\sigma_a = \sigma_b$ 当且仅当 $a = b$，可知 φ 为单射. 满射显然，因此 φ 是一个一一对应. 只需再验证运算保持：

$$\varphi(ab) = \sigma_{ab} = \sigma_a\sigma_b.$$

综上，G 和 G_l 同构. □

这样，我们就得到了一个群和其自身的变换群的同构. 请注意，这个变换群并不是全变换群，它的元素个数和群本身相同，因此是全变换群 $S_{|G|}$ 的子集. 凯莱定理有一个推论，在此之前先证明一个引理.

Lemma 2.40

偶数阶群一定有二阶元.

Proof. 设群 G 的阶为 $2m$，其中没有二阶元，即对于任意 $a \in G$，都有 $a \neq a^{-1}$. 从 G 中取一个元素 a_1，则有对应的逆元 a_1^{-1}，将这两个元素去掉. 重复这一操作，可以将 G 记作 m 对互为逆元的元素. 但观察这一表示，会发现 G 中没有单位元，不符合群的定义. 由此得证. 不难发现，二阶元不仅存在，而且一定有奇数个. □

Corollary 2.41

若 G 的阶为 $2m$，且 $2 \nmid m$，则 G 中存在一个子群 H，使得 $[G:H]=2$，即 $|H|=m$.

Proof. 由凯莱定理，G 同构于变换群 G_l，因此只要找到 G_l 的 m 阶子群，将其逆映射回去即可. 考察 G_l 中置换的奇偶性：σ_a 可以被写作不相交轮换的乘积. 假设 a 的阶为 d，即 d 是使得 $a^d=e$ 的最小正整数，则对于任意元素 $x\in G$，

$$\begin{pmatrix} x & ax & a^2x & \cdots & a^{d-1}x \end{pmatrix}$$

构成一个轮换，并且是 σ_a 的分解. 由此可知 σ_a 分解的轮换一定都包含 d 个元素，且轮换的个数为 $\left[G:\langle a\rangle\right]$，因此其奇偶性为

$$\left((-1)^{d-1}\right)^{2m/d}=(-1)^{2m(d-1)/d}.$$

根据引理，我们取出 G 中的二阶元 g，则 σ_g 为奇置换. 因此对于 G_l 中任意一个偶置换 σ，都有与之对应的奇置换 $\sigma_g\sigma$，因此 G_l 中奇偶置换个数相等. 不难证明其中所有偶置换构成一个子群. 即 $\left(G_l\cap A_{2m}\right)<G_l$，它的阶为 m. □

3

同态与商群

同态和同构类似，但不要求映射为双射，因此同构都是同态. 在后面我们会看到同态和同构如何彼此联系，并发挥它们的作用.

Definition 3.1

设 G 和 G' 为两个群，若存在一个从 G 到 G' 的映射 φ，使得所有的 $x, y \in G$ 都有

$$\varphi(xy) = \varphi(x)\varphi(y),$$

则称 φ 为 G 和 G' 的一个**同态** (isomophism)，记作 $G \simeq G'$.

Remark

设函数 $f : A \to B$，H 为 A 的子集，则 H 在 f 下的像 (image) 记作

$$f[H] = \{f(h) \mid h \in H\}.$$

Theorem 3.2

同态映射 $\phi : G \to G'$ 为单射应当且仅当 $\ker(\phi) = \{e\}$，e 为群 G 的单位元.

Proof. ($\Rightarrow$) 设 $x \in \ker(\phi)$，有 $\phi(x) = e'$. 则对于任意 $a \in G$，都有

$$\phi(ax) = \phi(a)\phi(x) = \phi(a)e' = \phi(a).$$

由 ϕ 为单射可得 $ax = a$，因此 $x = e$ 为 G 的单位元，即 $\ker(\phi) = \{e\}$. 另一端的证明同理. □

4

环与域

4.1 环

为了理解整数、实数的性质，研究包含多个二元运算的结构是必要的，因此引入了环和域.

Definition 4.1

环 $\langle R, +, \cdot \rangle$ [a] 是同时包含加法和乘法两个二元运算的集合 R，并满足以下性质:

1. $\langle R, + \rangle$ 是一个阿贝尔群.
2. 乘法满足结合律.
3. 对于任意的 $a, b, c \in R$，左右分配律成立，即

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$
$$(b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

[a] 通常来说，环中的乘法符号可以省略.

Example 4.2

任意复数的子集，若其加法构成群，且对乘法封闭，则一定构成环，因为加法的交换律、乘法的结合律以及分配律都是一定满足的. 如 $\langle \mathbb{Z}, +, \cdot \rangle$,$\langle \mathbb{Q}, +, \cdot \rangle$,$\langle \mathbb{R}, +, \cdot \rangle$ 和 $\langle \mathbb{C}, +, \cdot \rangle$ 都是环.

Example 4.3

考虑循环群 $n\mathbb{Z}$，对于任意两个元素 nr, ns，都有

$$nrns = n(nrs),$$

因此对乘法封闭. 并且整数满足乘法的分配律和结合律，因此 $\langle n\mathbb{Z}, +, \cdot \rangle$ 是一个环.

Example 4.4

设 F 是所有函数 $f:\mathbb{R}\Rightarrow\mathbb{R}$ 构成的集合，则 $\langle F,+\rangle$ 在下述函数加法的定义下为阿贝尔群.

$$(f+g)(x)=f(x)+g(x).$$

为了使其成为环，可定义乘法

$$(fg)(x)=f(x)g(x).$$

验证乘法交换律：

$$(f(gh))(x)=f(x)gh(x)=f(x)g(x)h(x)=((fg)h)(x).$$

验证乘法结合律：

$$\begin{aligned}(f(g+h))(x)&=f(x)(g+h)(x)=f(x)g(x)+f(x)h(x)\\&=(fg)(x)+(fh)(x)=(fg+fh)(x).\end{aligned}$$

因此 F 在上述加法和乘法定义下构成环.

Example 4.5

若 $R_1,R_2,\cdots,R_n$ 均为环，我们能够得到集合 $R_1\times R_2\times\cdots\times R_n$，其元素为所有有序 n 元组 $(r_1,r_2,\cdots,r_n)$，其中 $r_i\in R_i$. 我们可以定义元素间的加法和乘法为逐元素的加法和乘法，即

$$\begin{aligned}(a_1,a_2,\cdots,a_n)+(b_1,b_2,\cdots,b_n)&=(a_1+b_1,a_2+b_2,\cdots,a_n+b_n),\\(a_1,a_2,\cdots,a_n)\cdot(b_1,b_2,\cdots,b_n)&=(a_1b_1,a_2b_2,\cdots,a_nb_n).\end{aligned}$$

容易验证该集合构成一个环. $R_1\times R_2\times\cdots\times R_n$ 称为环 R_i 的**直积** (direct product).

通常来说，我们将环的加法群中的单位元记作 0, 即对于任意 $a\in R$，都有 $0+a=a+0=a$. a 在加法群中的逆元记作 $-a$. 需要注意的是，对于 n 个 a 相加，一般记作 $n\cdot a$，使用 $\cdot$ 来区分环内部的乘法. 同时定义 $0\cdot a=0$. 等式左边的 0 是数字 0，而等式右边表示加法群的单位元. 不仅如此，我们可以证明在环中，$0a=a0=0$.

Theorem 4.6

若 R 为环，加法单位元为 0，则对于任意 $a,b\in R$，我们有

1. $0a=a0=0$,
2. $a(-b)=(-a)b=-(ab)$.
3. $(-a)(-b)=ab$.

Proof. 根据分配律，可知

$$a0 + a0 = a(0 + 0) = a0 = 0 + a0,$$

由消去律，两边同时去掉 $a0$，可得 $a0 = 0$. 另一侧同理.

对于第二条性质，因为 $-(ab)$ 是 (ab) 的逆元，因此 $-(ab) + (ab) = 0$, 而根据结合律，

$$ab + a(-b) = a(b + -b) = a0 = 0,$$

由消去律，得到 $a(-b) = -(ab)$. 另一侧同理.

对于第三条性质，因为 $-(ab) + ab = 0$，且

$$-(ab) + (-a)(-b) = (-a)(-b) + (-a)b = (-a)(-b + b) = (-a)0 = 0.$$

同样由消去律得证. □

4.2 域

在我们提到的许多环中，都存在乘法单位元 1，例如 $\mathbb{Z}$, $\mathbb{Q}$ 和 $\mathbb{R}$. 然而，$2\mathbb{Z}$ 没有乘法单位元. 同时需要注意，环中的乘法不一定交换.

考虑只有一个元素的环 $\{0\}$ ，其中 $0 + 0 = 0, (0)(0) = 0$ ，因此 0 在该环中同时是加法和乘法单位元，该环称为**零环**. 根据定理 4.6 有 $0a = 0$，而 0 为乘法单位元要求 $0a = a$ ，因此只有零环能够满足，**在其它任何环中，加法单位元和乘法单位元都不相同**. 类比群的结论，乘法单位元是唯一的. 通常来说我们将其记为 1.

Definition 4.7

乘法可交换的环称为**交换环**. 有乘法单位元的环称为**幺环** (ring with unity).
幺环中的分配律说明

$$\underbrace{(1 + 1 + \cdots + 1)}_{n\text{个}}\underbrace{(1 + 1 + \cdots + 1)}_{m\text{个}} = \underbrace{(1 + 1 + \cdots + 1)}_{nm\text{个}}.$$

即 $(n \cdot 1)(m \cdot 1) = (nm \cdot 1)$. 下面是这一观察的一个应用.

Example 4.8

设整数 r,s 互素，即 $\gcd(r,s)=1$，可以得到环 $\mathbb{Z}_{rs}$ 和 $\mathbb{Z}_r\times\mathbb{Z}_s$ 同构. 首先它们都是阶为 rs 的循环阿贝尔群，生成元分别为 1 和 $(1,1)$. 因此仅通过定义 $\phi:\mathbb{Z}_{rs}\to\mathbb{Z}_r\times\mathbb{Z}_s$ 为 $\phi(n\cdot 1)=n\cdot\phi(1)=n\cdot(1,1)$，就可以说明 ϕ 为加法群同态，因为任意 $a,b\in\mathbb{Z}_{rs}$ ，都有

$$\begin{aligned}\phi(a)+\phi(b)&=\phi(a\cdot 1)+\phi(b\cdot 1)\\&=a\cdot(1,1)+b\cdot(1,1)=(a+b)\cdot(1,1)=\phi(a+b).\end{aligned}$$

对于乘法，我们运用上面的观察，可以很容易得到

$$\phi(nm)=(nm)\cdot(1,1)=[n\cdot(1,1)][m\cdot(1.1)]=\phi(n)\phi(m).$$

接下来证明双射. 由于两边的元素个数相等，因此只需证明单射即可. 因为 $\ker(\phi)$ 中的元素 x 同时模 r 和 s 余 1，且 $\gcd(r,s)=1$，易得 x 模 rs 余 1，即 $x=1$ 为单位元，单射得证.

容易发现，环直积为交换环或包含幺元当且仅当每个环都为交换环或都包含幺元.

若幺环 R 中 $0\neq 1$ ，去掉 0 得到集合 R^* ，若 R^* 在环的乘法下封闭且乘法逆元存在，则构成乘法群. 对于 $a\in R$ ，其乘法逆元为 $a^{-1}\in R$ 使得 $aa^{-1}=a^{-1}a=1$. 由群中的结论，每个元素的逆元是唯一的. 之所以去掉 0 ，是因为 0 显然没有逆元，不可能出现在乘法群中，除非是零环. 接下来我们讨论幺环中非零元素是否存在逆元，这也将会带来更多定义.

Definition 4.9

设幺环 R 中 $0\neq 1$. 若 R 中元素 u 有乘法逆元，则称 u 是 R 的一个**单元** (unit)[a] ，也叫可逆元素. 如果 R 中任意非零元素都是单元，则 R 为**除环** (division ring) ，也叫**斜域** (skew field). 交换除环称为**域** (field)，非交换除环称为**严格斜域** (strictly skew field).

[a]注意区分 unit 和 unity，unity 是乘法单位元.

Example 4.10

找一找 $\mathbb{Z}_{14}$ 中的单元. 显然 1 和 $-1=13$ 都是. $(3)(5)=1$，因此 3 和 5 也为单元，同理 $-3,-5,11,9$ 也是. 因此我们得到 $2,4,6,7,8,10$ 都不是单元. 这些数都是 2 或 7 的倍数. 我们可以归纳得到结论，$\mathbb{Z}_n$ 中的单元 m 一定满足 $\gcd(m,n)=1$. 这一结论很容易得证明. 假设 $0\le a,b<n$ 且 a,b 互为逆元，则

$$ab=kn+1\Rightarrow ab-kn=1.$$

由推论 2.27，可知 a,b 都与 n 互素.

显然环中所有可逆元素构成一个乘法群. 简单地给出子环和子域的定义. **子环**是环的子集，且在环诱导的运算下构成一个环. **子域**是域的子集，且在域诱导的运算下构成一个域. 根据定义容易得到子环的判断方法.

Theorem 4.11

设 S 为 R 的一个非空子集，则 S 是 R 的子环当且仅当 S 是加法子群且对于乘法封闭.

4.3 整环

Definition 4.12

设环 R 中元素 a，存在元素 $b\in R$ 使得 $ab=0$，则元素 a 称为**左零因子**，元素 b 称为**右零因子**.

Example 4.13

环 $M_n(\mathbb{R})$ 有零因子，而环 $\mathbb{Z}$ 没有.

Theorem 4.14

若环 R 无零因子，则在 R 中消去律成立.

Proof. 设 $ab=ac$，其中 $a,b,c\in R,a\neq 0$. 由分配律得

$$ab-ac=a(b-c)=0.$$

因为环中没有零因子，因此只能是 $b-c=0$. 得证. □

对比群论，可以看到群中消去律成立的关键在于每个元素都可逆. 而环中的零元一定不可逆，这是根本的不同.

Definition 4.15: 整环

若环 R 为交换幺环，其中 $1\neq 0$，且无零因子，则 R 称为整环.

回顾域的定义：交换除环且 $1\neq 0$. 则域 F 中每个非零元素都是单元. 若 $a,b\in F$ 且 $ab=0,a\neq 0$，则存在 a^{-1}，使得

$$a^{-1}(ab)=b=0.$$

因此域 F 中无零因子，从而说明**域一定是整环**. 然而整环 $\mathbb{Z}$ 不是域 (没有逆元), 表明**整环不一定是域**.

Theorem 4.16

有限整环是域.

Proof. 设 R 为整环，$|R| = n$，其元素为

$$a_1, a_2, \cdots, a_n,$$

其中 $a_1 = 1$. 取 F 中任意非零元素 a，和所有元素相乘得

$$aa_1, aa_2, \cdots, aa_n,$$

整环无零因子，因此满足消去律，可知 $aa_i \neq aa_j$ 当且仅当 $i \neq j$. 因此 $aa_i (i = 1, 2, \cdots, n)$ 就是 R 中所有元素，其中必有 1. 换言之，存在 $aa_k = 1$. 因此对于任意非零元素 a 都有逆元存在，得证. □

Definition 4.17: 体

若环 R 为幺环，其中 $1 \neq 0$，且所有非零元素均为单元，则 R 称为**体**.

不要求乘法交换的域就是体，因此所有的域都是体.

Example 4.18: 四元数体

设 $\mathbb{C}$ 为复数域，令 H 为 $M_2(\mathbb{C})$ 中全体形为

$$\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}, \alpha, \beta \in \mathbb{C}$$

的矩阵所组成的集合，其中 $\overline{\alpha}$ 表示 α 的复共轭. H 形成一个体，通常称为**四元数体**.

Proof. H 对加法显然构成阿贝尔群. 考虑乘法的封闭性：

$$\begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} \begin{bmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{bmatrix}$$
$$= \begin{bmatrix} \alpha\gamma - \beta\overline{\delta} & \alpha\delta + \beta\overline{\gamma} \\ -\alpha\overline{\delta} - \overline{\beta}\gamma & \overline{\alpha\gamma} - \overline{\beta}\delta \end{bmatrix}$$

令 $a = \alpha\gamma - \beta\overline{\delta}, b = \alpha\delta + \beta\overline{\gamma}$，由共轭的性质可得

$$-\alpha\overline{\delta} - \overline{\beta}\gamma = -\overline{b},$$
$$\overline{\alpha\gamma} - \overline{\beta}\delta = \overline{a},$$
$$\Rightarrow \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix} \begin{bmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{bmatrix} = \begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix} \in H.$$

因此 H 对乘法封闭，构成一个环. 显然 H 中单位元为

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

因此 H 为幺环. 同时对于任意非零元素

$$X = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix},$$

都可以求得其逆元

$$X^{-1} = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}^{-1} = \frac{1}{|\alpha|^2 + |\beta|^2} \begin{bmatrix} \overline{\alpha} & -\overline{\beta} \\ \beta & \alpha \end{bmatrix} \in H.$$

因此 H 是一个体. H 中元素还有一个优雅的表示：令 $\alpha = a + b\boldsymbol{i}, \beta = c + d\boldsymbol{i}$, 则

$$\begin{aligned} \begin{bmatrix} a + b\boldsymbol{i} & c + d\boldsymbol{i} \\ -c + d\boldsymbol{i} & a - b\boldsymbol{i} \end{bmatrix} &= a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} \boldsymbol{i} & 0 \\ 0 & -\boldsymbol{i} \end{bmatrix} + c \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d \begin{bmatrix} 0 & \boldsymbol{i} \\ -\boldsymbol{i} & 0 \end{bmatrix} \\ &= a + bI + cJ + dK. \end{aligned}$$

其中 I, J, K 具备一些良好的运算性质，例如

$$\begin{cases} I^2 = J^2 = K^2 = -1, \\ IJ = K = -JI, \\ JK = I = -KJ, \\ KI = J = -IK. \end{cases}$$

显然，H 不符合乘法交换律，构成一个体而非域. □

4.4 费马定理与欧拉定理

4.4.1 费马小定理

我们知道在加法群中，$\mathbb{Z}_n$ 与 $\mathbb{Z}/n\mathbb{Z}$ 是自然同构，只需将陪集 $a + n\mathbb{Z}$ 映射到 $a \in \mathbb{Z}_n$ 即可. 此外，陪集的加法可以简化为代表元的加法，然后找到代表元之和所在的陪集.

类似地，我们定义陪集的乘法为代表元的乘法，从而使 $\mathbb{Z}/n\mathbb{Z}$ 形成一个环. 考虑分别从陪集 $a + n\mathbb{Z}$ 和 $b + n\mathbb{Z}$ 取出元素 $a + rn$ 和 $b + sn$, 则有

$$(a + rn)(b + sn) = ab + (as + br + rsn)n \in ab + \mathbb{Z}.$$

说明代表元的乘法是良定义的. 至此我们得到了环 $\mathbb{Z}_n$ 和 $\mathbb{Z}/n\mathbb{Z}$. 它们依然同构.

Lemma 4.19

对于任意一个域，其非零元素在域的乘法下构成一个交换群.

Proof. 域中的元素可逆，且存在幺元，同时分配律在环的定义中得到满足. □

根据推论 2.27，当 p 为素数时，$\mathbb{Z}/p$ 中所有非零元均可逆，因此 $\mathbb{Z}_p$ 为域. 则非零元素

$$1, 2, 3, \cdots, p-1$$

构成一个模 p 的乘法交换群. 由于元素的阶一定整除群的阶，因此对于 $\mathbb{Z}_p$ 中任意非零元素 b，都有

$$b^{p-1} = 1.$$

又因为 $\mathbb{Z}_p$ 与 $\mathbb{Z}/p\mathbb{Z}$ 同构，对于 $\mathbb{Z}/p\mathbb{Z}$ 中任意不属于 $0 + p\mathbb{Z}$ 的元素，都有

$$a^{p-1} \equiv 1 \pmod{p}.$$

这就是著名的费马小定理.

Theorem 4.20: 费马小定理

设 $a \in \mathbb{Z}$，p 为一素数，且 $a \nmid p$，则 p 整除 a^{p-1}，即 $a^{p-1} \equiv 1 \pmod{p}$.

Corollary 4.21

设 $a \in \mathbb{Z}$，则对于任意素数 p 都有 $a^p \equiv a \pmod{p}$ 成立.

Proof. 若 $a \not\equiv 0 \pmod{p}$，则根据费马小定理 $a^{p-1} \equiv \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$. 若 $a \equiv 0 \pmod{p}$，则显然 $a^p \equiv a \equiv 0 \pmod{p}$. □

Example 4.22

证明 $2^{11213} - 1$ 不能被 11 整除.

Proof. 由费马小定理，$2^{10} \equiv 1 \pmod{11}$. 因此

$$2^{11213} - 1 \equiv (2^{10})^{1121} \cdot 2^3 - 1 \equiv 8 - 1 \equiv 7 \pmod{11}.$$

因此余数为 7. 这里 11213 是素数，而 $2^{11213} - 1$ 也是素数. 此类形如 $2^p - 1$ 的素数 (p 为素数) 被称为**梅森素数** *(Mersenne primes)*. □

Example 4.23

证明对于任意整数 n，$n^{33} - n$ 都能被 15 整除.

Proof. 注意到 $15 = 3 \cdot 5$，只需分别说明 $n^{33} - n$ 能够被 3 和 5 整除.

若 $3 \mid n$，自然有 $3 \mid (n^{33} - n)$. 若 $3 \nmid n$，则有 $n^2 \equiv 1 \pmod{3}$, 因此

$$n^{33} - n \equiv n(n^{32} - 1) \equiv n((n^2)^{16} - 1) \equiv n(1^{16} - 1) \equiv 0 \pmod{3}.$$

上述讨论表明 $n^{33} - n$ 总是能被 3 整除. 对于 5 的情况方法相同. □

4.4.2 欧拉定理

欧拉给出了费马小定理的一般形式.

Theorem 4.24

$\mathbb{Z}_n$ 中非零且不能整除 0 的元素构成一个乘法群 G_n.

Proof. 首先证明乘法的封闭性. 对于 $a, b \in G_n$，假设 $ab \notin G_n$，则存在 $c \in \mathbb{Z}_n (c \neq 0)$，使得

$$(ab)c = 0.$$

注意到结合律成立，因此 $a(bc) = 0$. 因为 $b \in G_n$，所以 $bc \neq 0$. 又因为 $a \in G_n$，则 $a(bc) \neq 0$. 推出矛盾，因此 $ab \in G_n$.

下面证明 G_n 构成群. 乘法结合律显然成立，且单位元一定在 G_n 中. 只需证明每个元素都存在逆元. 设 G_n 中元素为

$$1, a_1, \cdots, a_r.$$

则元素

$$a1, aa_1, \cdots, aa_r$$

两两不相等. 若 $aa_i = aa_j$，则 $a(a_i - a_j) = 0$，由 G_n 的性质，$a_i = a_j$. 因此要么 $a1 = 0$，要么存在 $i \leq r$ 使得 $aa_i = 1$. 任意元素存在乘法逆元得证.

这一证明手法类似于定理 4.16，通常被称为**计数** *(counting)*. 它虽然简单，但往往能应对有限集合相关的问题，因此也是理解“有限”的一种角度. □

令 n 为正整数，定义 $\varphi(n)$ 为所有小于等于 n 的正整数中，与 n 互素的个数. 规定 $\varphi(1) = 1$. 事实上，$\varphi(n)$ 就是 $\mathbb{Z}_n$ 中非零且不能整除 0 的元素个数，也就是群 G_n 的阶. 函数 $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ 称为 **欧拉 φ 函数** (Euler phi-function). 它能够将费马小定理推广到更一般的形式.

Theorem 4.25: 欧拉定理

设 a 与 n 互素，则 $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. 对于任意整数 a，一定存在 $b < n$ 使得 b 与 n 互素，且 $a \equiv b \pmod{n}$. 即

$$a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod{n}.$$

根据定理 4.24，可知 $b \in G_n$，且在 G_n 中单位元为 1，因此

$$b^{|G|} = b^{\varphi(n)} = 1.$$

定理得证. □

5

理想与商环

5.1 同态与同构

在群同态的基础上，很容易定义环同态，即同时保持加法和乘法不变.

Definition 5.1: 环同态

对于环 R 和 R'，若映射 $\phi: R \to R'$ 满足

1. $\phi(a+b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$.

则称 ϕ 为一环同态.

同样地，我们给出环同构的定义.

Definition 5.2: 环同构

对于环 R 和 R'，若映射 $\phi: R \to R'$ 是一个同态且为双射，则称 ϕ 为同构映射，环 R 和 R' **同构**.

由于 ϕ 也是加法群的群同态，因此群同态中的结论对环同态依然适用. 例如根据定理 3.2 , ϕ 是一个单射当且仅当它的核 $\ker(\phi) = \{a \in R | \phi(a) = 0'\}$ 恰为 $\{0\}$.

Example 5.3

对于 4.4 所定义的实函数集合 F，我们知道 F 是一个环. 定义映射 $\phi_a: F \to \mathbb{R}$，其中 $\phi(f) = f(a)$. 考虑加法，

$$\phi(f+g) = (f+g)(a) = f(a) + g(a) = \phi(f) + \phi(g),$$

考虑乘法，

$$\phi(fg) = (fg)(a) = f(a)g(a) = \phi(f)\phi(g).$$

因此 ϕ 为同态，一般称为**运算同态**.

Example 5.4

由例子 4.5 可知，环 R 的 n 次直积 R^n 构成一环. 定义映射 $\phi : R^n \to R$，其中

$$\phi((a_1, a_2, \cdots, a_n)) = a_1,$$

则 ϕ 显然为一满同态.

Example 5.5

在 $M_4(\mathbb{Q})$ 中全体形为

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}, A, B, C \in M_2(\mathbb{Q})$$

的矩阵构成一环，记为 R. 定义映射

$$\phi\left(\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}\right) = A,$$

则 ϕ 为环 R 到环 $M_2(\mathbb{Q})$ 的满同态.

5.2 环的理想

Theorem 5.6

环同态的核是子环.

Proof. 设同态 $\phi : R \to R'$ 的核为

$$\ker(\phi) = \{a \in R \,|\, \phi(a) = 0'\},$$

因为环同态也是加法群的同态，因此环同态的核与加法群同态的核一致. 若 $a, b \in \ker(\phi)$，则

$$\phi(ab) = \phi(a)\phi(b) = 0.$$

即 $ab \in \ker(\phi)$. 因此 $\ker(\phi)$ 对乘法封闭，构成一个子环. □

从中可以发现，要使 $\phi(ab) = 0$，只需 a 和 b 其中一个属于 $\ker(\phi)$ 即可. 设 $a \in \ker(\phi)$，则对于任意的 $r \in R$，都有

$$\phi(ra) = \phi(r)\phi(a) = 0,$$
$$\phi(ar) = \phi(a)\phi(r) = 0.$$

基于上述观察，我们将具有此类性质的子环定义为理想.

Definition 5.7: 理想

设 R 为一环，$I \subset R$ 是 R 的一个加法子群. 如果对于任意 $r \in R, a \in I$，都有

$$ra \in I,\ ar \in I,$$

则 I 称为 R 的一个**双边理想**. 如果只满足 $ra \in I$ 或 $ar \in I$，则称为**左理想**或**右理想**.

Example 5.8

在整数环 $\mathbb{Z}$ 中，子环 $m\mathbb{Z}(m > 0)$ 是一个理想.

Example 5.9

在 5.3 中我们定义了运算同态. 设所有以 a 为零点的函数构成的集合为

$$\{f(x) \in F \,|\, f(a) = 0\}.$$

能够证明该子集是一个理想，并且它也是同态的核.

显然，$\{0\}$ 和 R 都是 R 的理想，它们称为 **平凡理想**. 若 R 为幺环，且理想 I 中含有单位元素，则意味着所有元素都在理想中，即 $I = R$.

Lemma 5.10

域只有平凡理想.

Proof. 设 R 为域，表明 R 中每个非零元都有逆元. 设 I 是 R 的非零理想，对于任意 $a \in I$，都有 $a^{-1} \in R$. 由理想的性质，$a^{-1}a = 1 \in I$，即理想包含单位元，因此 $I = R$. □

5.3 商环

同态的核是一个理想，那是否环的每个理想都是某一同态的核？我们引入商环的概念，来为每一个理想构造一个同态.

设 I 是环 R 的一个理想. I 作为加法子群，可以将 R 划分为一系列陪集

$$r + I,\ r \in L.$$

因为加法群是交换的，可以定义陪集间的加法运算：

$$(r_1 + I) + (r_2 + I) = r_1 + r_2 + I + I = r_1 + r_2 + I.$$

接下来证明任意两个陪集之积还是陪集. 设

$$x = r_1 + a \in r_1 + I,\ a \in I,$$
$$y = r_2 + b \in r_2 + I,\ b \in I,$$

则根据理想的性质，

$$\begin{aligned} xy &= (r_1 + a)(r_2 + b) \\ &= r_1 r_2 + r_1 b + a r_2 + ab \in r_1 r_2 + I. \end{aligned}$$

因此我们定义陪集的乘法运算为

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I.$$

因为陪集间运算都是陪集代表的运算，不难验证分配律和结合律. 因此，全体陪集构成的集合为一环.

Definition 5.11: 商环

设 I 是环 R 的一个理想，R 对于 I 的陪集在上述定义的运算下构成的环称为 R 对于 I 的商环，记作 R/I.

定义映射 $\phi(a) = a + I, a \in R$，则 ϕ 是 R 到 R/I 的一个自然同态，且 $\ker(\phi) = I$.

Example 5.12

$\mathbb{Z}/n\mathbb{Z}$ 是一个环. 我们已经知道 $n\mathbb{Z}$ 是环 $\mathbb{Z}$ 的一个理想，因此 $\mathbb{Z}/n\mathbb{Z}$ 是也是一个环，即 $\mathbb{Z}_n$. 根据 4.10 中的讨论，当且仅当 n 为素数时，$\mathbb{Z}_n$ 中所有非零元素都有逆元，此时 $\mathbb{Z}_n$ 为域. 它是一个**有限域**的例子，而我们熟悉的数域都是无限的.

类似于群同态，我们给出环同态基本定理.

Theorem 5.13

如果 $\phi : R \to R'$ 是满同态，I 是 ϕ 的核，则商环 R/I 与 R' 同构.

证明过程和群同态相似. 只需定义 $\phi : R/I \to R'$，其中 $\phi(a + I) = \sigma(a)$，显然 ϕ 为满射，且保留加法和乘法运算. 容易证明 $\ker(\phi)$ 的核为 I，则可知 ϕ 为单射. 同构得证.

5.4 环的同构定理

下面给出环的同构定理，它们和群的同构定理是平行的.

Theorem 5.14

设 $\phi : R \to R'$ 是一个环的满同态，N 为 ϕ 的核. ϕ 诱导出 R 的所有包含 N 的子环的集合到 R' 的所有子环的集合的一个一一对应. 而且在这个对应中，理想与理想对应.

5.5 特征

Theorem 5.15

设 F 是一个域，考虑 F 中单位元素在 F 的加法群中的阶. 如果 e 为有限阶元素，则阶一定是素数.

Proof. 设 m 为最小的正整数使得 $m \cdot e = 0$，即 e 的阶为 m. 若 m 不为素数，则有 $m = m_1 m_2 (1 < m_1, m_2 < m)$，于是

$$m \cdot e = (m_1 \cdot e)(m_2 \cdot e) = 0.$$

因为 $m_1 \cdot e, m_2 \cdot e$ 均为非零元素，且域 F 中无零因子，因此该式不成立，m 为素数. □

Definition 5.16: 特征

设 F 为一域，如果 F 的单位元素 e 在 F 的加法群中是有限阶元素，阶为 p，则称域 F 的**特征**为 p. 如果单位元素是无限阶元素，则域 F 的特征为 0. 域的特征通常记作 $\mathrm{char}(F)$.

Theorem 5.17

在域的加法群中，任意非零元素都与单位元素有相同的阶.

Proof. 数域的特征为 0，而有限域 $\mathbb{Z}_p$ 的特征为 p. 设 a 为域 F 中一非零元素，m 为正整数，由

$$m \cdot a = m \cdot ae = a(m \cdot e)$$

可知，$m \cdot a = 0$ 当且仅当 $(m \cdot e) = 0$. 即 a 的阶等于 e 的阶，定理得证. □

设 $\mathrm{char}(F) = 0$，n 为正整数，考虑方程 $n \cdot x = b$ 的解. 由

$$n \cdot x = (n \cdot e)x, n \cdot e \neq 0$$

可知，$n \cdot e$ 存在逆元，因此 $(n \cdot e)^{-1} b$ 是方程的解. 域中无零因子，满足消去律，所以该解是唯一解. 通常我们将其记作

$$\frac{1}{n} b.$$

而对于特征不等于 0 的域，上述讨论不成立. 我们引出一个重要的定理.

Theorem 5.18

设 F 为一域，如果 $\mathrm{char}(F) = 0$，则 F 包含一子域与有理数域 $\mathbb{Q}$ 同构；如果 $\mathrm{char}(F) = p \neq 0$，则 F 包含一子域与 $\mathbb{Z}/p\mathbb{Z}$ 同构.

Proof. 若 F 的特征为 p，定义映射 $\phi : \mathbb{Z} \to F$ 使得 $\phi(n) = n \cdot e$. 容易验证 ϕ 为同态映射，且 $\ker(\phi) = p\mathbb{Z}$. 同态的像为

$$F_p = \{e, \cdots, (p-1)e, 0\}.$$

由同态基本定理，F_p 与 $\mathbb{Z}/p\mathbb{Z}$ 同构.

若 F 的特征为 0，可将 ϕ 扩充到有理数域. 定义

$$\phi\left(\frac{m}{n}\right) = (n\cdot e)^{-1}(m\cdot e).$$

容易验证 ϕ 依然为同态映射，且同态核 $\ker(\phi) = 0$. 而同态的像

$$F_0 = \left\{(n\cdot e)^{-1}(me)\middle| n, m \in \mathbb{Z}, n \neq 0\right\}$$

显然是域 F 的子域. 所以 F_0 和商环 $Q/\{0\}$ 同构，也即与 Q 同构. □

由此可以认为有理数域 $\mathbb{Q}$ 和整数模 p 的域 $\mathbb{Z}_p$ 是一些最小的域，它们统称为**素域**.

Corollary 5.19

设有限域 F 的特征为 p，则 F 的阶一定为 p 的幂次，即 $|F| = p^n (n \in \mathbb{Z}^+)$.

Proof. 由定理 5.18 可知，有限域 F 包含一个子域和 $\mathbb{Z}/p\mathbb{Z}$ 同构. 由向量空间的定义，可以将 F 定义为该子域上的向量空间. 若 F 向量空间的维数为 n，即 F 的生成元的最小个数为 n，可知 F 中元素个数为 p^n. □

5.6 理想的运算

设 H, N 为环 R 的子环，则它们的**交** $H\cap N$ 为 R 的子环，因为 $H\cap N$ 首先是加法子群，其次对乘法封闭，这很容易验证. 进一步假设 H 和 N 都为 R 的理想，则 $H\cap N$ 是 R 的理想. 因为若 $a \in H\cap N$，则对于任意 $r \in R$，都有 $ra, ar \in N$ 且 $ra, ar \in H$.

定义环的和为

$$H + N = \{a + b | a \in H, b \in N\}.$$

Theorem 5.20

子环的和 $H+N$ 是环 R 的一个加法子群，但不一定是子环. 若 N 为理想，则 $H+N$ 为子环.

Proof. $H + N$ 显然是加法子群. 对于 $a_1, a_2 \in H, b_1, b_2 \in N$, 则

$$(a_1 + b_1)(a_2 + b_2) = a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2.$$

乘法有可能不封闭. 但如果 N 为理想，则

$$a_1a_2 \in H,\ a_1b_2 + b_1a_2 + b_1b_2 \in N,$$

表明乘法封闭，即 $H + N$ 为子环. 因此子环与理想的和是子环. □

此外，若 H 和 N 都为环 R 的理想，则**理想的积**定义为理想元素的积的有限和，即

$$HN = \left\{ \sum a_i b_i \middle| a_i \in H, b_i \in N \right\}.$$

容易验证 HN 仍为理想. 且显然理想的加法和乘法满足分配律，设 K 也为 R 的理想，则

$$H(N+K) = HN + HK,$$
$$(N+K)H = BH + NK.$$

Definition 5.21

若幺环 R 的理想 H, N 满足 $H + N = R$，则称 H 和 N **互素**.

类比整数中的互素，若 a, b 互素，则存在正整数 r, s 使得 $ra + sb = 1$. 因此任意整数 x 都可以写作 $(rx)a + (sx)b$，可得 $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. 理想的互素是整数互素进一步的抽象化.

Lemma 5.22

设 H, N, K 为幺环 R 的理想，则有结论

1. 若 R 为交换环且 $H + N = R$，则 $HN = H \cap N$.
2. 若 H, K 都与 N 互素，则 HK 也与 N 互素.

Proof. 由理想的性质，易知 $HN \subset H \cap N$，因为 HN 中任意元素都同时在 H 和 N 中. 下面只需证明 $H \cap N \subset HN$. 设 $c \in H \cap N$. 因为 $H + N = R$，可知存在 $a \in H, b \in N$，使得 $a + b = 1$. 因此

$$c = ca + cb = ac + cb \in HN.$$

结论 1 得证.

结论 2 可以表述为

$$H + N = R, K + N = R \Rightarrow HK + N = R.$$

对 R 中任意元素 r，都存在 $a \in H, b, c \in N, d \in K$，使得

$$a + c = b + d = 1.$$

相乘得

$$1 = (a+c)(b+d) = ab + ad + cb + cd.$$

其中 $ad \in HK, ab, cb, cd \in N$，即 $1 \in HK + N$，因此 $HK + N = R$. □

这也提供了一个思路：证明两个理想互素只需证明单位元包含在理想的和中.

5.7 中国剩余定理

在《孙子算经》中，古人首次提出了同余方程组问题及其解法，其描述如下：

有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二. 问物几何？

即求解一个模三余二、模五余三、模七余二的整数. 设该数为 x，则方程组可写为

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

我们希望将三个方程独立看待，因此可以将 x 表示为三个数 x_1, x_2, x_3 之和，每个数分别满足一个方程. 但考虑到它们的和不一定同时满足整个方程组，我们要求

$$\begin{cases} 5 \times 7 \mid x_1, \\ 3 \times 7 \mid x_2, \\ 3 \times 5 \mid x_3. \end{cases}$$

此时 $x = x_1 + x_2 + x_3$ 就是方程组的解. 这就是中国剩余定理的一般求解思路. 需要思考的是：同余方程组是否一定有解？回顾这一思路，有解的必要条件是能够找到一个整数 x_1，使得 $35x_1 \equiv 2 \pmod 3$. 结合推论 2.27，不难发现这等同于要求 35 和 3 互素. 因为只要存在模 3 余 1 的数，其它数就一定有解. 拓展到 n 个数，就意味着这 n 个数需要**两两互素**.

前面提到了理想的互素，下面将中国剩余定理推广到环中.

Theorem 5.23: 中国剩余定理

设幺环 R 的理想 $I_1, I_2, \cdots, I_n$ 两两互素，则

$$R/(I_1 \cap I_2 \cap \cdots \cap I_n) \cong (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n).$$

Proof. 类似于前面的构造方式，令 $M_i = I_1 \cdots I_{i-1} I_{i+1} \cdots I_n, i = 1, \cdots, n$，即去掉 I_i 的其它理想的积. 则有

$$M_1 + M_2 = (I_2 + I_1)(I_3 \cdots I_n).$$

因为 $I_1 + I_2 = R$，且理想的积还是理想，可得

$$M_1 + M_2 = I_3 \cdots I_n.$$

同理，推出 $M_1 + M_2 + M_3 = (I_3 + I_1 I_2)(I_4 \cdots I_n)$，由引理 5.22，可得 $M_1 + M_2 + M_3 = I_4 \cdots I_n$. 以此类推，

$$\sum_{i=1}^{n} M_i = R.$$

因此存在 $e_i \in M_i (i = 1, \cdots, n)$，使得 $\sum_{i=1}^{n} e_i = 1$. 设 $i \neq j; i, j = 1, 2, \cdots, n$，则

$$\begin{cases} e_j \in I_i \\ e_j \in 1 + I_j \end{cases}$$

显然成立，接下来构造同态映射. 同样类似于整数，导出每个理想的自然同态 $\varphi_i : R \to R/I_i, i = 1, \cdots, n$ ，则有映射 $\varphi : R \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$ ，使得

$$\varphi(x) = (\varphi_1(x), \varphi_2(x), \cdots, \varphi_n(x)).$$

显然 φ 也是一个同态. 对于任意元素 $(x_1 + I, x_2 + I, \cdots, x_n + I)$, 都有 $x = \sum_{i=1}^{n} x_i e_i$ ，则

$$\varphi_j(x) = \sum_{i=1}^{n} \varphi_j(x_i)\varphi_j(e_i) = \varphi_j(x_j)\varphi_j(e_j) = x_j + I_j = \varphi(x_j).$$

因此

$$\varphi(x) = (\varphi(x_1), \cdots, \varphi(x_n)).$$

ϕ 为满射. 且 $\ker(\varphi) = \{x \mid \varphi_i(x) = I_i (i = 1, 2, \cdots, n)\} = I_1 \cap I_2 \cap \cdots \cap I_n$, 根据同态基本定理，

$$R/(I_1 \cap I_2 \cap \cdots \cap I_n) \cong (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n). \qquad \square$$

我们再一次看到了单位元的力量，它的确是证明理想相关问题的好帮手.

5.8 素理想与极大理想

在上一节我们几乎只讨论幺环，因为理想相关的结论通常依赖于单位元. 在这一节，所有的环都是交换幺环，并引入素理想与极大理想，它们和整环、域紧密联系，是非常重要的概念.

Definition 5.24: 极大理想

设 R 为交换幺环，R 的理想 $M \neq R$ ，且不存在理想 N 使得 $M \subsetneq N \subsetneq R$ ，则 M 是 R 的一个**极大理想**.

Example 5.25

设 p 为素数，则 $p\mathbb{Z}$ 是整数环 $\mathbb{Z}$ 的理想. 若存在 $\mathbb{Z}$ 的理想 $q\mathbb{Z}$ 包含 $p\mathbb{Z}$ ，则表明 $q \mid p$ ，即 $q = 1$ 或 p. 由此可见，$p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想.

接下来探讨极大理想的性质. 由环的第一同构定理，若 $\varphi : R \to R'$ 是满同态，则 φ 诱导出 R 中包含 $N = \ker(\varphi)$ 的理想与 R' 的理想的一一对应. 若 I, J 是 R 中包含 N 的理想，则 $I \subset J$ 当且仅当 $\varphi(I) \subset \varphi(J)$. 因此 φ 诱导出 R 中包含 $N = \ker(\varphi)$ 的极大理想与 R' 的极大理想的一一对应.

Theorem 5.26

设 R 为交换幺环，则 R 为域的充要条件是零理想为极大理想.

Proof. *(⇒)* 由引理 5.10，若 R 为域，则 R 的理想只有零理想和它本身. 由极大理想的定义，零理想为极大理想.

(⇐) 若零理想为极大理想，我们要证明 R 为域. 设 $a \in R$ 为非零元，则构造 R 的子集

$$Ra = \{xa | x \in R\},$$

不难发现 Ra 是 R 的一个理想. 因为 $Ra \neq 0$，可知 $Ra = R$，表明存在 $b \in R$ 使得 $ba = 1$，即 a 可逆，R 为域得证. □

Theorem 5.27

设 R 为交换幺环，则 M 为 R 的极大理想的充要条件是 R/M 为域.

Proof. *(⇒)* 考虑自然同态 $\varphi : R \to R/M$，则 R 中包含 M 的极大理想和 R/M 的极大理想一一对应. 因为 M 已经是极大理想，$\varphi(M) = 0 + M$ 是 R/M 的极大理想. 根据定理 5.26，R/M 为域.

(⇐) 若 R/M 为域，则 $0+M$ 是 R/M 的极大理想. 同样根据一一对应，$\ker(\varphi) = M$ 是 R 的极大理想. □

素理想的概念可从素数中抽象而来，但理想并没有所谓的整除或分解. 素数的另一个性质是：若 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$. 据此定义素理想.

Definition 5.28: 素理想

设 R 为交换幺环，R 的理想 $P \neq R$，且对于任意 $a, b \in R$，$ab \in P$ 蕴含 $a \in P$ 或 $b \in P$，则 P 是 R 的一个素理想.

Theorem 5.29

设 R 为交换幺环，则 R 的理想 $M \neq R$ 为素理想的充要条件是 R/M 为整环.

Proof. *(⇒)* 依然考虑自然同态 $\varphi : R \to R/M$，设 $a, b \in R$ 则

$$\varphi(ab) = ab + M = \varphi(a)\varphi(b) = (a + M)(b + M).$$

由素理想的定义，若 $ab + M = M$ 则必有 $a + M = M$ 或 $b + M = M$，这表明 R/M 中任意两个非零元相乘都不为零，因此 R/M 为整环.

(⇐) 若 R/M 为整环，则 $ab + M = M$ 蕴含了 $a + M = M$ 或 $b + M = M$，即 $ab \in M$ 必有 $a \in M$ 或 $b \in M$，因此 M 为素理想. □

Theorem 5.30

设 R 为交换幺环，则 R 为整环的充要条件是零理想为素理想.

Proof. *(⇒)* R 为整环，即 $ab = 0$ 必有 $a = 0$ 或 $b = 0$，易得零理想为素理想.

(⇐) 反面同样显然. □

是否类似于极大理想，素理想之间也有一一对应呢？这是成立的，但看起来不那么明显. 设 $\varphi : R \to R'$ 为满射，$\ker(\varphi) = N$ ，P 为 R 中包含 N 的素理想，则对于 $\varphi(a)\varphi(b) \in \varphi(P)$，可知 $\varphi(ab) \in \varphi(P)$ ，即

$$ab \in \varphi^{-1}(\varphi(P)).$$

由对应定理，$\varphi^{-1}(\varphi(P)) = P$ ，则 $a \in P$ 或 $b \in P$, 推出 $\varphi(a) \in P$ 或 $\varphi(b) \in P$. 因此 $\varphi(P)$ 为素理想，且和 P 一一对应.