群论基础

呜哩天才琪露诺

日期：2024 年 7 月

目录

1 引论 **1**

1.1 等价关系，商集 1

1.2 环，域，群 2

1.3 环的同构，Euler 函数 3

1.4 域的特征 3

2 群的定义，子群 **4**

3 循环群 **5**

4 群的同态与同构 **5**

5 陪集分解 **6**

6 拉格朗日定理 **7**

7 正规子群与商群 **8**

8 同构定理 **9**

9 群的直积 **10**

1 引论

1.1 等价关系，商集

非空集合 S 上的二元关系 $\mathcal{R}$ 是 $S \times S$ 的一个子集，若 $(a, b) \in \mathcal{R}$，则称 a 与 b 满足关系 $\mathcal{R}$，记作 $a\mathcal{R}b$；否则，称 a 与 b 不满足关系 $\mathcal{R}$. S 上的二元关系 $\sim$ 称为等价关系，若它满足：

1. 反身性：$a \sim a$；
2. 对称性：$a \sim b$ 则 $b \sim a$；
3. 传递性：$a \sim b$，$b \sim c$，则 $a \sim c$.

$\sim$ 是 S 上的等价关系，对 $a \in S$，令

$$\overline{a} = \{x \in S \mid x \sim a\}$$

称为 $\overline{a}$ 是 a 关于 $\sim$ 的等价类，把 a 称为等价类 $\overline{a}$ 的一个代表. 注意，等价类的代表不是唯一的.

容易证明，$\overline{a}=\overline{b}$ 与 $a\sim b$ 等价，且不相等的两个等价类的交集一定为空. 由此可知，若集合 S 上有等价关系 $\sim$，则 S 可以表示为一组等价类的无交并，即：

$$S=\bigsqcup_{a\in S}\overline{a}$$

$\sim$ 是 S 上的等价关系，则所有等价类组成的集合称为 S 对 $\sim$ 的商集，记作 $S/\sim$.

同余是极为重要的一种等价关系. 对大于 1 的整数 m，称整数 a 与整数 b 模 m 同余，若 $m\mid(a-b)$，记作 $a\equiv b \mod m$. 容易验证，模 m 同余是 $\mathbb{Z}$ 上的等价关系，共有 m 个等价类 $\overline{i}=\{x\in\mathbb{Z}\mid x\equiv i \mod m\}$ $(i=1,2,\cdots,m-1)$，称为模 m 剩余类. $\mathbb{Z}$ 对模 m 同余关系的商集 $\mathbb{Z}_m=\{\overline{0},\overline{1},\cdots,\overline{m-1}\}$.

1.2 环，域，群

集合 S 上的二元运算 $\circ$ 是指映射 $S\times S\to S,(a,b)\mapsto a\circ b$.

环是一个非空集合 R，其上定义了二元运算加法 $+$ 和乘法 $\cdot$，且加法满足交换律、结合律、零元存在、负元存在；乘法满足结合律；加法和乘法一起满足左分配律和右分配律.

模 m 同余有如下性质：若 $a\equiv b \mod m$ 且 $c\equiv d \mod m$，则 $a+b\equiv b+d \mod m$ 及 $ab\equiv bd \mod m$. 由此，我们可以按 $\overline{a}+\overline{b}\triangleq\overline{a+b}$ 及 $\overline{a}\cdot\overline{b}\triangleq\overline{ab}$ 定义模 m 剩余类的加法和乘法. 验证可知 $\mathbb{Z}_m$ 对这样定义的加法和乘法构成一个环，称为模 m 剩余类环. 环的零元为 $\overline{0}$，$\overline{a}$ 的负元为 $\overline{-a}$. 此外，模 m 剩余类环的乘法还有幺元 $\overline{1}$.

环的定义不要求乘法满足交换律. 例如，n 阶矩阵的集合 M_n 对一般定义的矩阵加法和乘法构成环，但矩阵乘法是不满足交换律的. 若环 R 的乘法满足交换律，则称 R 为交换环. 由于乘法不一定具有交换律，所以左分配律和右分配律是互相独立的.

环的定义也不要求幺元存在. 偶数的集合 $2\mathbb{Z}$ 对一般的加法和乘法构成环，但整数乘法的幺元是 1，显然不在 $2\mathbb{Z}$ 中，故 $2\mathbb{Z}$ 无幺元. 若环有幺元，则幺元必唯一.

对有幺元 e 的环 R，$a\in R$，若存在 $b\in R$ 使得 $a\cdot b=b\cdot a=e$，则称 a 是可逆元，称 b 为 a 的逆元，记作 a^{-1}. 可以证明，逆元存在必唯一.

设环 R 的零元为 0，由环的分配律可以证明 $a\cdot 0=0\cdot a=0$. 我们熟悉的实数乘法中，若 $a,b\neq 0$，则 $a\cdot b\neq 0$，但在一般的环上，这一点是不一定成立的. 例如，考虑模 4 剩余类环 $\mathbb{Z}_4=\{\overline{0},\overline{1},\overline{3},\overline{4}\}$，则有 $\overline{2}\cdot\overline{2}=\overline{2\cdot 2}=\overline{4}=\overline{0}$. 对 $a\in R$，若存在非零的 $c\in R$ 使得 $a\cdot c=0$（或 $c\cdot a=0$），则称 a 为 R 的左零因子（或右零因子）. 左零因子和右零因子统称零因子. 若 R 是有幺元的环，则 R 的零因子不是可逆元，反之，R 的可逆元不是零因子.

设 F 是一个有幺元 e 的环，若 F 中的任意一个非零元都是可逆元，则称 F 为域. 最为常见的域是数域，如有理数域 $\mathbb{Q}$，实数域 $\mathbb{R}$ 和复数域 $\mathbb{C}$.

对 $\mathbb{Z}_m$，若 m 是合数，则 $\mathbb{Z}_m$ 不是域. 这是因为，m 可以分解为两较小正整数的积 m_1m_2，$\bar{m}_1$ 和 $\bar{m}_2$ 都非零，而 $\bar{m}_1\cdot\bar{m}_2=\overline{m_1m_2}=\overline{m}=\overline{0}$.

在 $\mathbb{Z}_m$ 中，$\bar{a}$ 是可逆元当且仅当 a 与 m 互素. 证明如下.

证明.（充分性）设 a 与 m 互素，由 Bezout 定理，存在整数 x,y 使得

$$xa+ym=\gcd(a,m)=1$$

于是在 $\mathbb{Z}_m$ 中

$$\overline{1}=\overline{xa+ym}=\bar{x}\cdot\bar{a}+\bar{y}\cdot\bar{m}=\bar{x}\cdot\bar{a}$$

从而 $\bar{a}$ 是可逆元.

（必要性）设 $\bar{a}$ 是可逆元，而 a 与 m 不互素，则 $\gcd(a,m)=d\neq 1$，存在两个整数 a_1 和 m_1 使得

$$a=a_1d, m=m_1d$$

从而

$$am_1=a_1dm_1=a_1m$$

因此 $\bar{a}\cdot\bar{m_1}=\bar{a_1}\cdot\bar{m}=\bar{0}$，$\bar{m_1}\neq 0$，故 $\bar{a}$ 是左零因子，从而不是可逆元，矛盾！ □

由此可见，$\mathbb{Z}_m$ 的每个元素要么是可逆元，要么是零因子，且二者不能同时成立. 这一点对数域亦成立，但对一般的域并不成立. 例如，定义在 $[-1,1]$ 上的连续函数的集合对函数的加法和乘法构成域，考虑 $f:x\mapsto x^2$，则 f 既不是可逆元，也不是零因子.

对素数 p，$\mathbb{Z}_p$ 都是一个域. 这是因为，对任意比 p 小的正整数 k，k 与 p 互素，故 $\bar{k}$ 是可逆元. 于是 $\mathbb{Z}_p$ 的非零元都是可逆元.

设 G 是一个非空集合，在上面定义了乘法 $\cdot$，且满足结合律、幺元存在以及逆元存在，则称 G 为一个群. 若乘法还满足交换律，则称 G 为 Abel 群.

$\mathbb{Z}_m$ 的所有可逆元的集合记作 $\mathbb{Z}_m^*$. $\mathbb{Z}_m^*$ 对 $\mathbb{Z}_m$ 的加法不封闭，比如对 $\mathbb{Z}_{12}^*=\{\bar{1},\bar{5},\bar{7},\bar{11}\}$ 有 $\bar{1}+\bar{5}=\bar{6}\notin\mathbb{Z}_{12}^*$. 但 $\mathbb{Z}_m^*$ 对 $\mathbb{Z}_m$ 的乘法是封闭的，且对它构成一个群，称为 $\mathbb{Z}_m$ 的单位群.

1.3 环的同构，Euler 函数

若环 R 到环 R' 有双射 σ，且 σ 保持加法和乘法运算，则称 σ 是 R 到 R' 的同构映射，称 R 与 R' 是同构的，记作 $R\cong R'$.

R 的可逆元对应到 R' 的可逆元，论证如下：

a 是 R 的可逆元 $\Leftrightarrow$ 存在 $b\in R$ 使得 $a\cdot b=e\Leftrightarrow$ 存在 $b\in R$ 使得 $\sigma(a\cdot b)=\sigma(e)\Leftrightarrow$ 存在 $\sigma(b)\in R'$ 使得 $\sigma(a)\cdot\sigma(b)=\sigma(e)=e'\Leftrightarrow\sigma(a)$ 是 R' 的可逆元

作为一个应用，我们研究 Euler 函数 $\varphi(m)$，它代表 $\{1,2,\cdots,m\}$ 中与 m 互素的整数的个数. 立刻可知 $\varphi(m)=|\mathbb{Z}_m^*|$.

任意整数都可以唯一分解为 $2^{r_1}3^{r_2}\cdots p_i^{r_i}\cdots$ 的形式，其中 p_i 表示第 i 个素数. 于是我们只需要研究素数的幂的 Euler 函数，再研究 $\varphi(m)$ 与 $\varphi(m_1)$ 和 $\varphi(m_2)$（其中 m_1,m_2 互素，$m=m_1m_2$）的关系即可. 对前一个问题，我们直接给出结论：$\varphi(p^r)=p^{r-1}(p-1)$.

对后一个问题，考虑 Descartes 积 $\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}$，并按 $(a,a')+(b,b')=(a+b,a'+b')$ 和 $(a,a')\cdot(b,b')=(a\cdot b,a'\cdot b')$ 定义其加法和乘法. 容易验证 $\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}$ 构成有幺元 $(1,1')$ 的交换环，叫做 $\mathbb{Z}_{m_1}$ 与 $\mathbb{Z}_{m_2}$ 的直和，记作 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$. 验证可知，$(a,a')$ 是 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$ 的可逆元等价于 a 和 a' 分别是 $\mathbb{Z}_{m_1}$ 和 $\mathbb{Z}_{m_2}$ 的可逆元，于是 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$ 的可逆元个数为 $\varphi(m_1)\varphi(m_2)$. 构造映射 $\sigma:\mathbb{Z}_m\to\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2},\bar{x}\mapsto(\bar{x}_{m_1},\bar{x}_{m_2})$，可以验证 σ 是一个环同构映射，则 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}\cong\mathbb{Z}_m$，则 $\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}$ 的可逆元个数为 $\varphi(m)$. 于是：

$$\varphi(m)=\varphi(m_1)\varphi(m_2)$$

近世代数的思路就是，选取合适的代数系统，利用其结构或态射解决问题.

1.4 域的特征

设 R 是一个环，对 $a\in R$，规定 m 个 a 之和为 a 的 m 倍，记作 ma，显然有：

$$(m+n)a=ma+na$$

$$(mn)a = m(na)$$

$$m(a+b) = ma + mb$$

$$m(a \cdot b) = (ma) \cdot b = a \cdot (mb)$$

对数域，是有 $n1 \neq (\forall n)$. 对模 p 剩余类 $\mathbb{Z}_p$，$p\bar{1} = \bar{p} = \bar{0}$ 而 $l\bar{1} = \bar{l} \neq \bar{0}(0 < l < p)$. 对任意的域 F，其单位元为 e，则要么 $ne \neq (\forall n)$，要么存在素数 p 使得 $pe = 0$ 而 $le \neq 0(0 < l < p)$. 证明如下.

证明. 若存在正整数 n 使得 $ne = 0$. 由良序定理，有一个最小正整数 n_0 使得 $n_0 e = 0$. 设 n_0 不是素数，$n_0 = n_1 n_2$，则：

$$(n_1 e)(n_2 e) = n_1[e(n_2 e)] = n_1[n_2(ee)] = n_1(n_2 e) = (n_1 n_2)e = ne = 0$$

而 $n_1 e \neq 0, n_2 e \neq 0$，这与 F 是域矛盾! □

对第一种情况，我们称域 F 的特征为 0，对后一种情况，我们称 F 的特征为 p. 域的特征记为 char$F$.

2 群的定义，子群

定义 2.1. 群 在集合 G 上定义了二元运算 $\cdot$，$(G, \cdot)$ 称为群，若满足

1.（结合律）对任意的 $a, b, c \in G$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \tag{1}$$

2. 存在单位元 $1 \in G$，使得对任意 $a \in G$ 有

$$a \cdot 1 = 1 \cdot a = a \tag{2}$$

3. 对任意 $a \in G$，存在 a 的逆元 a^{-1} 使得

$$a \cdot a^{-1} = a^{-1} \cdot a = 1 \tag{3}$$

若 1 和 $1'$ 都是群 G 的单位元，则 $1 = 1 \cdot 1' = 1'$，可见群的单位元是唯一的. 还可以证明，群中元素 a 的逆元也是唯一的. 另外一个重要的性质是乘法的消去律，即若 $ab = ac$ 则 $b = c$，若 $ba = ca$ 则 $b = c$，这可以通过在等式两边同时左乘或右乘 a 的逆元得到.

定义 2.2. 元素个数有限的群称为有限群，其元素个数称为它的阶. 元素个数无限的群称为无限群，规定其阶为 ∞.

定义 2.3. 若 G 上的乘法还满足交换律，即任意的 $a, b \in G$ 有

$$a \cdot b = b \cdot a \tag{4}$$

则称 G 为交换群或 Abelian 群

定义 2.4. 子群 设 G 为群，$H \subseteq G$，若 H 对 G 的乘法构成群，则称 H 为 G 的子群，记为 $H \leq G$. 若 $H \neq G$，则称 H 为 G 的真子群，记作 $H < G$.

要验证 H 是 G 的子群，我们首先需要验证乘法 $\cdot$ 仍是 H 上的二元运算. 这要求 $\cdot$ 在 H 上封闭，即对任意的 $a, b \in H$，需要 $a \cdot b \in H$. 然后，我们需要验证 H 对 $\cdot$ 构成群，结合律由运算本身的结构保证，我们只需要验证单位元 1 在 H 中，以及 H 中任意元素 a 的逆元仍在 H 中即可.

3 循环群

定义 3.1. 设 G 是群而 g 是 G 中的元素，g 生成的子群是指包含 g 的最小子群，记为 $\langle g\rangle$.

由群的定义，$\langle g\rangle$ 必然包含下面三类元素

1. $g^0 \equiv 1$;
2. $g^k \equiv \underbrace{g\cdot g\cdots g}_{k个}$;
3. $g^{-k} \equiv \underbrace{g^{-1}\cdot g^{-1}\cdots g^{-1}}_{k个}$.

而由这三类元素构成的集合正是 G 的子群，故

$$\langle g\rangle = \{g^k \mid k\in\mathbb{Z}\} \tag{5}$$

定义 3.2. 元素的阶 设 g 是群 G 的元素，它的阶是指满足 $g^k = 1$ 的最小正整数. 若这样的 k 不存在，则称 g 为无限阶元.

定理 3.1. *若 g 为 k 阶元，则 $g^n = 1$ 当且仅当*

$$n \equiv 0 \mod k \tag{6}$$

而 $g^i = g^j$ 当且仅当

$$i \equiv j \mod k \tag{7}$$

若 g 为无限阶元，则对任意的 $i\neq j$，$g^i \neq g^j$.

证明. 若 g 为 k 阶元，设 $n = kq+r, 0\le r<k$. 若 $r\neq 0$，因为 k 是使 $g^k = 1$ 的最小正整数，所以 $g^r\neq 1$，故 $g^n = g^{kq+r} = (g^k)^q\cdot g^r \neq 1$，矛盾！故 $r = 0$. 若 $r = 0$，则 $g^n = (g^k)^q = 1$. 于是 $g^n = 1$ 的充要条件为 $n\equiv 0 \mod k$. 而 $g^i = g^j$ 等价于 $g^{i-j} = 1$，自然也等价于 $i-j\equiv 0 \mod k$，即 $i\equiv j \mod k$.

若 g 为无限阶元，则 $g^i = g^j$ 等价于 $g^{i-j} = 1$，等价于 $i-j = 0$，即 $i = j$. □

于是，g 为 k 阶元时，g 生成的子群为 k 阶有限群

$$\langle g\rangle = \{1, g, \cdots g^{k-1}\} \tag{8}$$

4 群的同态与同构

定义 4.1. 群同态 设 G 和 G' 为群，则同态是映射 $\varphi: G\to G'$，使得对任意的 $a,b\in G$ 有

$$\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b) \tag{9}$$

等式左右两端的乘法 $\cdot$ 分别是在 G 和 G' 中定义的，这里用了相同的记号，注意加以区分.

定理 4.1. *若 $\varphi: G\to G'$ 是群同态，则：*

1. 同态把单位元映为单位元

$$\varphi(1_G) = 1_{G'} \tag{10}$$

2. 同态把逆元映为逆元，即对任意的 $a\in G$

$$\varphi(a^{-1}) = [\varphi(a)]^{-1} \tag{11}$$

定义 4.2. 设 φ 是群同态，若 φ 是单射，则称 φ 为单同态. 若 φ 是满射，则称 φ 为满同态. 若 φ 是双射，则称 φ 为同构，称 G_1 与 G_2 同构，记作 $G_1 \cong G_2$.

定义 4.3. 设 $\varphi : G \to G'$ 是群同态，则

$$\varphi(G) \equiv \{x \in G' \mid \exists a \in G, x = \varphi(a)\} \tag{12}$$

称为 φ 的像.

$$\ker \varphi \equiv \{a \in G \mid \varphi(a) = 1\} \tag{13}$$

称为 φ 的核.

定理 4.2. 设 $\varphi : G \to G'$ 为群同态，$a, b \in G$，φ 的核为 K，则

$$\varphi(a) = \varphi(b) \Leftrightarrow a^{-1}b \in K \tag{14}$$

定理 4.3. 同构映射的逆映射仍为同构映射.

5 陪集分解

定义 5.1. 设 H 是 G 的子群，对于 $a \in G$，集合

$$aH \equiv \{ah \mid h \in H\} \tag{15}$$

称为 G 关于 H 的左陪集. 集合

$$Ha \equiv \{ha \mid h \in H\} \tag{16}$$

称为 G 关于 H 的右陪集.

因为左陪集和右陪集是完全类似的，下面的讨论只涉及左陪集.

定理 5.1. 陪集 $aH = bH$ 要么不交，要么重合，且 $aH = bH$ 当且仅当 $b^{-1}a \in H$.

证明. 若 $aH \cap bH \neq \emptyset$，令 $ah_1 = bh_2$，则 $b^{-1}a = h_2 h_1^{-1} \in H$. 此时

$$\begin{aligned} ah &= ah_1(h_1^{-1}h) = bh_2(h_1^{-1}h) \in bH \\ bh &= bh_2(h_2^{-1}h) = ah_1(h_2^{-1}h) \in aH \end{aligned} \tag{17}$$

故 $aH = bH$. □

这个定理也可以从以下角度说明. 构造同余关系 $\sim$

$$a \sim b \Leftrightarrow \exists h \in H \, s.t. \, b = ah \tag{18}$$

容易验证 $\sim$ 是 H 上的等价关系，且 aH 是 a 关于 $\sim$ 的等价类，由等价类的性质即得.

于是，群 G 可以划分为其关于 H 的左陪集的不交并

$$G = \bigsqcup_{i \in I} a_i H \tag{19}$$

其中 $\{a_i H \mid i \in I\}$ 是 G 关于 H 的所有左陪集的集合. 一般称 $\{a_i \mid i \in I\}$ 为 G 的左陪集代表元系，即我们可以从每个陪集中选取一个元素，代表这个陪集.

用陪集的语言，我们可以把定理 3 重写为

定理 5.2. 设 $\varphi : G \to G'$ 是群同态，$a, b \in G$，φ 的核为 K，则

$$\varphi(a) = \varphi(b) \Leftrightarrow aK = bK \tag{20}$$

6 拉格朗日定理

定义 6.1. 指数 群 G 关于子群 H 的指数，记为 $(G:H)$，是指 G 关于 H 的陪集代表元的个数. 若陪集代表元的个数无限，则规定 $(G:H)=\infty$.

定理 6.1. 拉格朗日定理 对群 G 和它的子群 H，有

$$|G| = |H| \cdot (G:H) \tag{21}$$

证明. G 为无限群时显然成立.

G 为有限群时，由 (1.19) 得

$$|G| = \sum_{i\in I} |a_i H| = \sum_{i\in I} |H| = |H| \cdot |I| = |H| \cdot (G:H) \tag{22}$$

□

拉格朗日定理有很多重要推论

定理 6.2. 设 G 为有限群，$x \in G$，则 $x^{|G|} = 1$. 即元素 x 的阶总是群 G 的阶的因子.

定理 6.3. 素数阶群都是循环群.

定理 6.4. 设 $G = \langle x \rangle$ 为 n 阶循环群，则对于 n 的正因子 d，G 中有唯一 d 阶子群

$$\{1, x^{\frac{n}{d}}, \cdots, x^{\frac{n}{d}(d-1)}\} \tag{23}$$

此子群也是循环群.

证明. 容易验证 $\{1, x^{\frac{n}{d}}, \cdots, x^{\frac{n}{d}(d-1)}\}$ 是 G 的 d 阶循环子群. 设 H 也是 G 的 d 阶子群，$y = x^a \in H$，因为 y 的阶数必然整除 d，$y^d = x^{ad} = 1$，所以 $ad = kn$，$y = x^{\frac{n}{d}k}$. □

下面我们对拉格朗日定理进行推广.

定理 6.5. 设群 $K \le H \le G$，且 $(G:K)$ 有限，则

$$(G:K) = (G:H) \cdot (H:K) \tag{24}$$

证明. 设 G 关于 H 以及 H 关于 K 的陪集分解分别为

$$G = \bigsqcup_{i\in I} g_i H,\ H = \bigsqcup_{j\in J} h_j K \tag{25}$$

则

$$G = \bigcup_{(i,j)\in I\times J} g_i h_j K \tag{26}$$

若 $g_i h_j K = g_{i'} h_{j'} K$，则 $g_i H \cap g_{i'} H \neq \emptyset$，所以 $i = i'$，故 $h_j K = h_{j'} K$，所以 $j = j'$，故

$$G = \bigsqcup_{(i,j)\in I\times J} g_i h_j K \tag{27}$$

故 $\{g_i h_j \mid i \in I, j \in J\}$ 为 G 关于 K 的左陪集代表元系，故

$$(G:K) = (G:H) \cdot (H:K) \tag{28}$$

□

7 正规子群与商群

我们考虑

$$G/H \equiv \{aH \mid a \in G\} \tag{29}$$

如果我们希望 G/H 也具有群结构，那就需要在 G/H 上定义乘法，一个自然的想法是规定

$$(aH)\cdot(bH) = abH \tag{30}$$

这自然要求 $aH = a'H, bH = b'H$ 时 $abH = a'b'H$. 也就是说，对 $(a')^{-1}a \in H$ 和 $(b')^{-1}b \in H$ 有

$$(a'b')^{-1}(ab) = (b')^{-1}(a')^{-1}ab = (b')^{-1}(a')^{-1}ab \in H \tag{31}$$

因为 $b^{-1}b' = [(b')^{-1}b]^{-1} \in H$，故 (1.31) 等价于

$$b^{-1}[(a')^{-1}a]b \in H \tag{32}$$

其中 $(a')^{-1}a$ 是 H 中任意的元素，而 b 是 G 中任意的元素. 于是，可以在 G/H 上自然地定义乘法的条件是，对于任意的 $b \in G$ 和 $a \in H$ 有 $b^{-1}ab \in H$ 成立. 我们引入下面的定义.

定义 7.1. 共轭 设 x 是群 G 中的元素. 对任意 $g \in G$，$x' = gxg^{-1}$ 称为 x 的共轭元，称 x' 与 x 共轭.

定义 7.2. 正规子群 子群 N 称为 G 的正规子群，若对所有的 $g \in G$ 有 $g^{-1}Ng = N$. 即对任意的 $g \in G$ 和 $a \in N$ 有

$$g^{-1}ag \in N \tag{33}$$

记作 $N \lhd G$.

定理 7.1. *$\varphi : G \to H$ 为群同态，则 $\ker\varphi$ 是 G 的正规子群，$im\varphi$ 是 H 的子群.*

证明. 设 $a, b \in \ker\varphi$，则

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)[\varphi(b)]^{-1} = 1$$

故 $a^{-1}b \in \ker\varphi$，$\ker\varphi$ 是 G 的子群.

设 $g \in G, a \in \ker\varphi$，则

$$\varphi(g^{-1}ag) = [\varphi(g)]^{-1}\varphi(a)\varphi(g) = [\varphi(g)]^{-1}\varphi(g) = 1 \tag{34}$$

所以 $g^{-1}ag \in \ker\varphi$，故 $\ker\varphi$ 是 G 的正规子群.

设 $h_1, h_2 \in \mathrm{i}\varphi$，令 $\varphi(g_1) = h_1, \varphi(g_2) = h_2$，则

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)[\varphi(g_2)]^{-1} = h_1 h_2^{-1}$$

所以 $h_1 h_2^{-1} \in \mathrm{i}\varphi$，$\mathrm{i}\varphi$ 是 H 的子群. □

对 $g \in G$ 和 G 的子群 H，我们引入记号

$$gHg^{-1} \equiv \{ghg \mid h \in H\} \tag{35}$$

则

定理 7.2. *$H \lhd G$ 和以下条件等价*

1. *对任意的 $g \in G$ 有 $gHg^{-1} = H$;*
2. *对任意的 $g \in G$ 有 $gH = Hg$;*
3. *G 对 H 的任意左陪集同时也是右陪集.*

由此可以推出

定理 7.3. *如果群 G 的 r 阶子群只有 H，则 $H \lhd G$.*

证明. 对任意的 $g \in G$，显然 gHg^{-1} 的阶数也是 r，由假设可知 $gHg^{-1} = H$，由定理 9 得 $H \lhd G$. □

设 $N \lhd G$，则 G/N 在 (1.30) 所定义的乘法下构成群. 称 G 关于 N 的商群. 考虑

$$\pi : G \to G/N, a \mapsto aN \tag{36}$$

则 π 是 G 与 G/N 之间的满同态，且 $\ker \pi = N$.

8 同构定理

定理 8.1. *同态基本定理 设 $\varphi : G \to H$ 为群同态，则 φ 诱导的同态*

$$\bar{\varphi} : G/\ker\varphi \to \mathrm{i}\varphi, g\ker\varphi \mapsto \varphi(g) \tag{37}$$

为群同构.

证明. 首先证明 $\bar{\varphi}$ 是良定义的. 若 $g\ker\varphi = g'\varphi$，则存在 $a \in \ker\varphi$ 使得 $g' = ga$，所以 $\varphi(g') = \varphi(ga) = \varphi(g)$.

证明 $\bar{\varphi}$ 确为同态. 若 $g_1\ker\varphi, g_2\ker\varphi \in G/\ker\varphi$，则

$$\bar{\varphi}(g_1g_2\ker\varphi) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \bar{\varphi}(g_1\ker\varphi)\bar{\varphi}(g_2\ker\varphi) \tag{38}$$

$\bar{\varphi}$ 显然是满同态.

证明 $\bar{\varphi}$ 是单同态. 若 $\bar{\varphi}(g_1) = \bar{\varphi}(g_2)$，则 $\varphi(g_1) = \varphi(g_2)$，故 $g_2 = g_1(g_1^{-1}g_2) \in g_1\ker\varphi$，即 $g_2\ker\varphi = g_1\ker\varphi$. □

由此可以推出

定理 8.2. *设群同态 $\varphi : G \to G'$.φ 是单同态当且仅当它的核 K 是 $\{1\}$.φ 是满同态当且仅当 $G/\ker\varphi \cong H$*

从同态基本定理可以延伸出以下重要定理

定理 8.3. *第二同构定理 如果 $N \lhd G, H \leq G$，则*

$$(H \cap N) \lhd H, N \lhd NH \leq G \tag{39}$$

以及

$$NH/H \cong H/H \cap N \tag{40}$$

证明. 对任意 $a_1h_1, a_2h_2 \in NH$ 有

$$a_1h_1(a_2h_2)^{-1} = a_1h_1h_2^{-1}a_2^{-1} = a_1(h_1h_2^{-1})a_2^{-1}(h_2h_1^{-1})(h_1h_2^{-1}) \tag{41}$$

因为 $N \lhd H, (h_1h_2^{-1})a_2^{-1}(h_1h_2^{-1})^{-1} \in N$, 故 $a_1(h_1h_2^{-1})a_2^{-1}(h_1h_2^{-1})^{-1} \in N$, 从而 $a_1(h_1h_2^{-1})a_2^{-1}(h_2h_1^{-1})(h_1h_2^{-1}) \in NH$，故 $NH \leq G$.

对任意 $a \in N, a'h \in NH$，$(a'h)a(a'h)^{-1} = a'(hah^{-1})(a')^{-1}$. 由 $N \lhd G$ 可知 $hah^{-1} \in N$，从而 $a'(hah^{-1})(a')^{-1} \in N$. 于是 $N \lhd NH$.

定义同态

$$\varphi : H \to NH/N, h \mapsto hN \tag{42}$$

则 φ 为满同态，且

$$\ker\varphi = \{h \mid \varphi(h) = 1\} = \{h \mid h \in N\} = H \cap N \tag{43}$$

由同态基本定理

$$(H \cap N) \lhd H \tag{44}$$

且

$$NH/N \cong H/H \cap N \tag{45}$$

□

定理 8.4. *第三同构定理 如果 $N \lhd G, M \lhd G$ 且 $N \leq M$，则*

$$G/M \cong \frac{G/N}{M/N} \tag{46}$$

证明. 定义同态

$$\varphi : G/N \to G/M, gN \mapsto gM \tag{47}$$

由 $N \leq M$ 可知 φ 为满同态，且

$$\ker\varphi = \{gN \mid gM = M\} = \{gN \mid g \in M\} = M/N \tag{48}$$

由同态基本定理

$$G/M \cong \frac{G/N}{M/N} \tag{49}$$

□

9 群的直积

定义 9.1. 群的直积 设 G 和 G' 是两个群，在 $G \times G'$ 上定义乘法

$$(g_1, g_1') \cdot (g_2, g_2') = (g_1 g_2, g_1' g_2') \tag{50}$$

则 $(G \times G', \cdot)$ 构成一个群，称为 G 和 G' 的直积，仍记作 $G \times G'$.

容易证明，$G \times G' \cong G' \times G$，同构映射为 $(g, g') \mapsto (g', g)$.$G \times \{e'\} \cong G$，同构映射为 $(g, e') \mapsto g$.

定理 9.1. *设 $H \leq G, K \leq G$，则 $H \times K \cong G$ 当且仅当以下条件成立*

1. $H \cap K = \{1\}$;
2. $HK \equiv \{hk \mid h \in H, k \in K\} = G$;
3. $H \lhd G, K \lhd G$. *且同构映射为*

$$f : H \times K \to G, (h, k) \mapsto hk \tag{51}$$

证明. 首先，显然 f 为满射当且仅当 $HK = G$.

其次，f 是单射等价于

$$f(h_1, k_1) = f(h_2, k_2) \Rightarrow (h_1, k_1) = (h_2, k_2) \tag{52}$$

等价于

$$h_1 k_1 = h_2 k_2 \Rightarrow h_1 = h_2, k_1 = k_2 \tag{53}$$

等价于

$$h_2^{-1} h_1 = k_2^{-1} k_1 \Rightarrow h_1 = h_2, k_1 = k_2 \tag{54}$$

也就是 $H \cap K = \{1\}$

然后，对任意的 $(h_1, k_1), (h_2, k_2) \in K \times H$，

$$f[(h_1, k_1) \cdot (h_2, k_2)] = f(h_1, k_1) f(h_2, k_2) \tag{55}$$

等价于 $(h_1 h_2)(k_1 k_2) = (h_1 k_1)(h_2 k_2)$，这等价于 H 中的元素和 K 中的每个元素都可交换.

若 H 和 K 满足定理条件，则 f 既单又满，f 为双射. 考虑对易子 $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. 因为 $K \lhd G$，等式左边属于 H，因为 $H \lhd G$，等式右边属于 H. 因为 $H \cap K = \{1\}$，$hkh^{-1}k^{-1} = 1$，故 $hk = kh$，H 中的元素和 K 中的每个元素都可交换，f 为同态，故 f 为同构，充分性得证. 反过来容易证明必要性. □