目录

Chapter 1

代数基本概念

1.1 代数运算

定义 1.1.1 (代数运算). 设 A 是一个非空集合, 任意一个由 $A \times A \longrightarrow A$ 的映射就称为定义在 A 上的代数运算.

1.2 群的定义和简单性质

定义 1.2.1 (群). 设 G 是一个非空集合, 在 G 上定义了一个称之为乘法的代数运算, 记作 ab, 若该代数运算满足如下性质, 就称 G 为一个群

$$[\text{结合律}](1)(ab)c = a(bc);$$

$$[\text{左幺元}](2)\exists e \in G \quad \text{s.t.} \quad \forall a \in G, \text{有} ea = a;$$

$$[\text{左逆元}](3)\forall a \in G, \exists b \in G \quad \text{s.t.} \quad ba = e.$$

1. 若 $ba = e$, 则 $ab = e$.

证. 任取 $b \in G$, 存在 $c \in G$, 使得 $cb = e$, 于是

$$a = ea = (cb)a = c(ba) = ce, \tag{1.2.1}$$

在等式(1.2.1)两侧同时右乘 b, 就有

$$ab = (ce)b = c(eb) = cb = e,$$

问题证毕. □

2. 若对所有的 $a \in G$, 有 $ea = a$, 那么也有 $ae = a$, 对所有的 $a \in G$.

证. 取 $b \in G$, 使得 $ba = e$, 同时 $ab = e$, 于是

$$ae = a(ba) = (ab)a = ea = a,$$

问题证毕. □

3. 群 G 中有惟一的元素 e 具有性质

$$\forall a \in G, ea = ae = a.$$

证. 假设 G 中有元素 e_1, e_2 满足此性质, 则

$$e_1 = e_1 e_2 = e_2,$$

可见惟一性得证. □

4. 对群 G 中任意元素 a, 有惟一元素 b, 使 $ab = ba = e$.

证. 假设在 G 中还有元素 c 满足 $ac = ca = e$, 则

$$c = ec = ce = c(ab) = (ca)b = eb = b,$$

这就证明了惟一性. □

5. 对于群 G 中任意元素 a, b, 方程

$$ax = b$$

在 G 中有惟一解.

证. 在题设方程两侧同时左乘 $a^{-1} \in G$, 有

$$(a^{-1}a)x = a^{-1}b$$

亦即 $x = a^{-1}b \in G$, 解的存在性得证.

假设还有元素 $c \in G$ 满足 $ac = b$, 则

$$ax = b = ac, \tag{1.2.2}$$

在等式(1.2.2)两侧同时左乘 a^{-1}, 就有

$$(a^{-1}a)x = (a^{-1}a)c \iff x = c,$$

解的惟一性得证.

综上所述, 问题得证. □

定义 1.2.2 (Abel 群 (或交换群)). *若群 G 的运算适合交换律, 则称群 G 为 Abel 群 (或交换群).*

定义 1.2.3 (阶). *群 G 中所含元素的个数称为群 G 的阶, 记作 $|G|$.*

定义 1.2.4 (有限群与无限群). *若 $|G|$ 是一个有限数 (无限数), 则称群 G 为有限群 (无限群).*

1.3 群的例子

本节将不加证明地给出一些常见的群的例子和性质.

定义 1.3.1 (图形 F 对称群, 二面体群). 已知 F 是平面上的一个图形. 令 G_F 为全体保持 F 不变的平面正交变换所成的集合, 则 G_F 在变换的称发下成群, 称为图形 F 的对称群.

若用 T 表示绕 O 旋转 $90°$,S 表示对于直线 l 的镜面反射, 则不难看出

$$G_F = \left\{T, T^2, T^3, T^4, ST, ST^2, ST^3, ST^4\right\},$$

其中 $T^4 = I, S^2 = I, ST = T^{-1}S$($I$ 表示恒等映射).

类似地, 若 F 是平面上正 n 边形, 则 F 的对称群 G_F 由 $2n$ 个元素组成. 令 T 为绕中心转 $\frac{2\pi}{n}$,S 为对于某一对称轴的镜面反射, 则有

$$G_F = \left\{T, T^2, \cdots, T^n, ST, ST^2, \cdots, ST^n\right\},$$

其中 $T^n = I, S^2 = I, ST = T^{-1}S$. 称这些群为二面体群记作 D_n.

定义 1.3.2 (对称群 S_n 集合 M 全变换群,n 置换,n 对称群, 不相交的). 若 M 为非空集合, 则 M 到自身的全体可逆变换关于变换的乘法成群, 称该群为集合 M 的全变换群, 记作 $S(M)$. 当 M 是无限集,$S(M)$ 为无限群.

当 M 含有 n 个元素时,M 的可逆变换称为 M 的 n 元置换,$S(M)$ 称为 n 元对称群, 简记为 S_n.

若 M 中的元素用 $1, 2, \cdots, n$ 编号后, 则 S 中的元素表示为

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

其中 $\alpha_i = \sigma(i), i = 1, 2, \cdots, n$. 易见 n 元置换与 n 阶排列之间存在一一对应, 亦即 $|S| = n!$.

若一个 n 元置换 σ 将 $1, 2, \cdots, n$ 中某 m 个数 $\alpha_1, \cdots, \alpha_m$ 轮换, 即

$$\sigma(\alpha_1) = \alpha_2, \sigma(\alpha_2) = \alpha_3, \cdots$$
$$\sigma(\alpha_{m-1}) = \alpha_m, \sigma(\alpha_m) = \alpha_1,$$

其余的数保持不变, 则称 σ 为轮换, 表示为

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

当 $m = 2$ 时, 也称 σ 为对换.

若 S_n 中的两个轮换 $(\alpha_1\alpha_2\cdots\alpha_m)$ 与 $\beta_1\beta_2\beta_l$ 满足

$$\alpha_i \neq \beta_j, i = 1, 2, \cdots, m, j = 1, 2, \cdots, l,$$

则称这两个对换为不相交的.

命题 1.3.1. *非单位的置换能惟一地表成一些不相交的轮换的乘积.* □

1.4 子群, 陪集

定义 1.4.1 (子群)**.** *若群 G 的非空子集合 H 对 G 的运算也成群, 则称群 H 是群 G 的子群, 记作 $H < G$.*

定理 1.4.1. *群 G 的非空子集合 H 是群 G 的子群的充分必要条件是*

$$\forall a, b \in H \Longrightarrow ab^{-1} \in H.$$

证. 必要性显然, 接下来证明充分性.
(1) 结合律: 显然满足;
(2) 幺元的存在性:$\forall a \in H$, 取 $b = a$, 则 $e = aa^{-1} \in H$;
(3) 逆元的存在性:$\forall b \in H$, 取 $a = e$, 则 $b^{-1} = eb^{-1} \in H$.
结合 (1),(2),(3) 可得 H 成为群, 进而是群 G 的子群. □

定义 1.4.2 (左陪集, 右陪集)**.** *设群 H 是群 G 的一个子群, 对 G 中的任意一个元素 a, 称 $aH = \{ah : h \in H\}$ 是 H 的一个左陪集; 称 $Ha = \{ha : h \in H\}$ 是 H 的一个右陪集.*

定义 1.4.3 (基数)**.** *若两集合之前存在一个一一对应, 则称这两个集合有相同的基数. 对任意集合 X, 记 X 的基数为 $|X|$.*

当 X 为无限集时, 记 $|X| = \infty$; 当 X 为有限集时, 记 $|X|$ 为 X 所含元素的个数.

定义 1.4.4 (商集, 指数)**.** *称群 G 关于子群 H 的所有左陪集 (或右陪集) 组成的集合为群 G 关于子群 H 的左商集 (或右商集), 称它的基数为 H 在 G 中的指数, 记作 $[G : H]$.*

定理 1.4.2. *设 G 是群,$H < G$, 则 H 的任意一个左陪集 gH 与 H 含有同样多的元素. 该定理对于右陪集同样成立.*

证. 易见 $h \mapsto ah$ 是子群 H 到左陪集 aH 的一个一一对应,$h \mapsto ha$ 是子群 H 到右陪集 Ha 的一个一一对应, 因此定理得证. □

定理 1.4.3. *设群 H 是群 G 的子群.H 的任意两个左 (右) 陪集要么相等, 要么无公共元素. 群 G 可以表示为若干个不相交的左 (右) 陪集之并.*

证. 利用相互包含证明第一个论断: 取 H 的两个左陪集 aH,bH 并假设它们有公共元素, 即有 $ah_1 \in aH, bh_2 \in bH$ 满足

$$ah_1 = bh_2, \tag{1.4.3}$$

等式(1.4.3)两端同时右乘 h_1^{-1}, 有

$$a = bh_2h_1^{-1} \in bH,$$

可见 $aH \subset bH$. 同理可证 $aH \supset bH$, 进而 $aH = bH$. 第一个论断证毕.

第二个论断的证明: 由于 $a \in aH$, 所以

$$G = \bigcup_{a\in G} aH,$$

去掉其中的重复项, 就有

$$G = \bigcup_{\alpha} a_\alpha H,$$

其中 $a_\alpha H$ 两两无交. □

推论 1.4.1 (Lagrange 定理)**.** *设 G 是有限群,H 是它的子群, 则 $|H|$ 是 $|G|$ 的因子.*

证. 设 $|G|=n, |H|=t$, 由定理1.4.3可得

$$G = a_1 H \cup a_2 H \cup \cdots \cup a_r h, \tag{1.4.4}$$

其中 $a_i H \cap a_j H = \varnothing (i,j=1,2,\cdots,r且i \neq j)$, 在等式(1.4.4)两侧同时取因子, 并利用定理1.4.2就有

$$|G| = r|H|,$$

从而 $|H|$ 是 $|G|$ 的因子. □

定义 1.4.5 (由 a 生成的子群)**.** *在群 G 中, 任意一个元素 a 的全体方幂组成的集合 $\{a^m : m \in \mathbb{Z}\}$ 显然成 G 的子群, 称为由 a 生成的子群.*

注 1.4.1. *(1) 元素 a 的方幂要么两两不同要么存在 $l \in \mathbb{Z}_+$ 使得 $a^l = e$;*

(2) 在 (1) 的后一种情形中, 一定有最小的正整数 d 满足 $a^d = e$. 此时将 d 称为元素 a 的阶.

推论 1.4.2. *设 G 为一有限群, 则 G 中每一个元素的阶一定是 $|G|$ 的因子.*

证. 设 H 是由 G 中的元素 a 生成的子群, 则

$$\text{(i)}|a| = |<a>| = |H|;$$
$$\text{(ii)}H是G的子群 \Longrightarrow |H|整除|G|,$$

可见 G 中每一个元素的阶一定是 G 的因子. □

1.5 群的同构

定义 1.5.1 (群的同构)**.** 若 G, G' 是两个群,$\varphi : g \mapsto g', G \longrightarrow G'$ 是一一对应, 并且满足 $\forall g_1, g_2 \in G$

$$\varphi(g_1 g_2) = \varphi(g_1')\varphi(g_2'), \tag{1.5.5}$$

则称群 G 同构于群 G', 记作 $G \cong G'$. 适合等式(1.5.5)的一一对应称为同构映射, 简称同构.

引理 1.5.1. 任意非空集合上的全体可逆变换构成的集合关于变换的乘法成群. □

定理 1.5.1 (Cayley 定理)**.** 任何一个群都同构于某一集合上的变换群.

证. 设 G 是群. 对每一个 $a \in G$, 定义 G 上的变换 φ_a 如下

$$\varphi_a(x) = ax, x \in G,$$

可见 $\forall x \in G$

$$\text{(i)}\varphi_{a^{-1}}\varphi_a(x) = \varphi_{a^{-1}}(ax) = a^{-1}ax = x;$$
$$\text{(ii)}\varphi_a\varphi_{a^{-1}}(x) = \varphi_a(a^{-1}x) = aa^{-1}x = x,$$

可见 $\forall a \in G, \varphi_a$ 均是可逆变换. 记 $G_l = \{\varphi_a : a \in G\}$, 于是 $\forall a, b \in G_l$

$$\varphi_a\varphi_{b^{-1}}(x) = \varphi_a(b^{-1}x) = ab^{-1}x = \varphi_{ab^{-1}}(x),$$

即 $\varphi_a\varphi_{b^{-1}} = \varphi_{ab^{-1}} \in G_l$, 根据引理1.5.1与定理1.4.1可得 G_l 成群, 亦即 G_l 是一变换群.

根据 G_l 定义易知映射 $a \mapsto \varphi_a$ 为满映射.

由于

$$\varphi_a(e) = a,$$

所以当 $a \neq b$ 时,$\varphi_a \neq \varphi_b$, 亦即映射 $a \mapsto \varphi_a$ 是单映射. 进而映射 $a \mapsto \varphi_a$ 是一一对应. 再由 $\varphi_a\varphi_b = \varphi_{ab}$ 可知所述映射为同构映射, 从而 $G \cong G_l$, 定理得证. □

1.6 同构, 正规子群

定义 1.6.1 (同态映射). 若 φ 是群 G 到群 G' 的映射, 满足 $\forall g_1, g_2 \in G$

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

则称 φ 是群 G 到 G' 的同态映射, 或同态.

注 1.6.1. 在同态映射的定义中, 既不要求它是映上的, 也不要求它是单射.

当 φ 是 G 到 G' 的同态映射时, 常常简记为

$$\varphi : G \mapsto G'.$$

定义 1.6.2 (象). 若 $\varphi : G \mapsto G'$, 定义

$$\varphi G = \{\varphi(a) : a \in G\}$$

为同态映射 φ 的象.

注 1.6.2. *(1)* 易见 φG 是 G' 的子群;

(2) 若 φ 是映上的, 即 $\varphi G = G'$, 称 φ 为满同态;

(3) 若 φ 是单射, 即 G 与 φG 同构, 亦即 G 与 G' 的一个子群同构, 则称 φ 为单一同态, 或嵌入映射.

定义 1.6.3 (完全反象, 核). 对于同态映射 $\varphi : G \mapsto G'$, 定义

$$\varphi^{-1}(a') = \{a : \varphi(a) = a'\}$$

为元素 a' 的完全反象. 特别地, 定义 $\varphi^{-1}(e')$ 为同态映射 φ 的核, 记作 $\ker \varphi$.

命题 1.6.1. 记 $\varphi(a) = a'$, 则 $\varphi^{-1}(a') = \begin{cases} a \ker(\varphi); \\ \ker(\varphi) a. \end{cases}$

证. (1) 任取 $h \in \ker\varphi$, 有

$$\varphi(ah) \xlongequal{\text{同态映射}} \varphi(a)\varphi(h) = a'e' = a',$$

这说明 $a\ker\varphi$ 中的元素在映射 φ 下的象均为 a', 亦即 $a\ker\varphi \subset \varphi^{-1}(a')$;

(2) 反之, 任取 $a \in \varphi^{-1}(a')$, 即 $\varphi(a) = a'$. 又 $e \in \ker\varphi$, 从而

$$a = ae \in a\ker\varphi,$$

这说明在映射 φ 下的象为 a' 的元素在 $a\ker\varphi$ 中, 亦即 $a\ker \supset \varphi^{-1}(a')$.

由 (1),(2) 可知 $\varphi^{-1}(a) = a\ker(\varphi)$.

同理可证 $\varphi^{-1}(a') = \ker(\varphi)a$. □

定义 1.6.4 (正规子群)**.** *设群 H 是群 G 的子群, 若对任意 $g \in G$, 都有 $gH = Hg$, 则称 H 是 G 的正规子群, 记作 $H \lhd G$.*

注 1.6.3. *(1) 由命题1.6.1可知, 同态的核都是正规子群;*

(2) 正规子群的定义可以改写为

$$\forall g \in G, gHg^{-1} = H.$$

正规子群的定义换个说法就是子群 H 的左右陪集相等;

(3) 在 Abel 群中, 每个子群都正规.

1.7 商群

定义 1.7.1 (群的子集合的运算)**.**

1. 定义

$$AB = \{ab|a \in A, b \in B\},$$

子集乘积满足结合律:$(AB)C = A(BC)$;

2. 定义

$$A^{-1} = \left\{a^{-1}|a \in A\right\}.$$

利用集合运算, 定理1.4.1可改写为

$$\text{群 } G \text{ 的非空子集合 } H \text{ 是子群 } \Longleftrightarrow HH^{-1} \subset H.$$

定理 1.7.1. *设 H 是群 G 的一个子群.H 是正规子群 $\Longleftrightarrow$ H 的任意两个左 (右陪集) 之积还是左 (右陪集).*

证. (1) 必要性

任取正规子群 H 的两个左陪集 aH 与 bH, 有

$$(aH)(bH) = a(Hb)H = a(bH)H = (ab)(HH) = abH,$$

必要性得证;

(2) 充分性

任取 H 的两个左陪集 aH 与 bH, 根据已知条件可设 $(aH)(bH) = cH$, 由于 $ab \in (aH)(bH)$, 所以 $ab \in cH$, 再由 $ab \in abH$ 与定理1.4.3可得

$$abH = cH = (aH)(bH), \tag{1.7.6}$$

等式两端同时左乘 a^{-1}, 有

$$bH = HbH \supset Hbe = Hb,$$

由于 b 具有任意性, 故可以将其改成 b^{-1}, 得到

$$b^{-1}H \supset Hb^{-1},$$

等式两边同时左乘 b, 右乘 b, 得到

$$Hb \supset bH,$$

亦即 $bH = Hb$, 可见 H 是正规子群. □

令 G/H 代表正规子群 H 的全部不同的右陪集组成的集合.

命题 1.7.1. *G/H 在陪集的运算下成群.*

证. (1) 结合律

由 $(Ha)(Hb) = Hab$ 可见, 陪集之间的乘法可归结为陪集代表的乘法, 故结合律显然成立;

(2) 左幺元

$\forall Ha \in G/H$, 有

$$H \cdot Ha = Ha,$$

可见左幺元存在, 为 H;

(3) 左逆元

$\forall Ha \in G/H$, 有

$$(Ha^{-1})(Ha) = H(a^{-1}H)a = H(Ha^{-1})a = (HH)(a^{-1}a) = H,$$

可见 G/H 中的任一元都有左逆元.

(1),(2),(3) 说明 G/H 成群, 问题得证. □

定义 1.7.2 (商群). *G/H 在陪集的乘法下所成的群称为群 G 对正规子群 H 的商群, 仍记作 G/H.*

命题 1.7.2. *设群 H 是群 G 的正规子群, 定义映射*

$$\begin{aligned} \varphi : G \to & G/H \\ g \mapsto & Hg, \end{aligned}$$

则 φ 是满同态且 $\ker\varphi = H$.

证. (1)$\forall a, b \in G$, 有

$$\begin{aligned} & \varphi(ab) \\ = & Hab \\ = & HabH \end{aligned}$$

$$
\begin{aligned}
&= Ha(bH)\\
&= Ha(Hb)\\
&= HaHb\\
&= \varphi(a)\varphi(b)\\
\Longrightarrow &\varphi\text{是同态映射;}
\end{aligned}
$$

(2) 根据商群的定义,φ 显然是映上的;

(3) 对 $\forall h \in H$, 注意到

$$
\begin{aligned}
&\varphi(h)\\
=&hH\\
=&H\\
=&eH,
\end{aligned}
$$

可见 $h \in H$, 于是 $\ker\varphi \supset H$. 同时对 $\forall k \in \ker\varphi$, 有

$$
\begin{aligned}
\varphi(k) =&kH\\
=&H,
\end{aligned}
$$

所以对任意 $h \in H$, 都有 $kh \in H$, 现取 $h = e$, 所以

$$k = ke \in H,$$

即 $k \in H$, 所以 $\ker\varphi \subset H$.

(1),(2) 说明 $\varphi : G \to G/H$ 为满同态;(3) 说明 $\ker\varphi = H$. □

注 1.7.1. *由于 $H \lhd G$, 所以若定义*

$$
\begin{aligned}
\varphi : G \to& G/H\\
g \mapsto& gH,
\end{aligned}
$$

则命题1.7.2也成立.

定义 1.7.3 (自然同态)**.** *称命题1.7.2中的 φ 为 $G \to G/H$ 的自然同态.*

注 1.7.2. *由命题1.6.1可知, 同态的核都是正规子群; 自然同态的构造说明每个正规子群也都是某一同态的核.*

引理 1.7.1. *若 H 为群 G 的子群,$a, b \in G$, 则*

$$b^{-1}a \in H \iff aH = bH;$$
$$ab^{-1} \in H \iff Ha = Hb.$$

证. 只要证明第一条即可, 第二条同理可证.

(1) 必要性

可设 $h \in H$ 满足 $b^{-1}a = h$, 从而 $a = bh \in bH$, 又 $e \in H$ 且 $a = ae$, 故

$$a = ae \in aH$$
$$a \in bH,$$

可见 $aH \cap bH \neq \varnothing$, 进而 $aH = bH$, 必要性得证;

(2) 充分性

等式 $aH = bH$ 两端同时左乘 b^{-1} 有

$$b^{-1}aH = H \Longrightarrow b^{-1}a \cdot e \in H \iff b^{-1}a \in H,$$

充分性得证. □

定理 1.7.2 (群同态基本定理)**.** *若 $\sigma : G \to G'$, 则 $G/\ker\sigma \cong \operatorname{im}\sigma$. 进一步, 若 σ 是满同态, 则 $G/\ker\sigma \cong G'$.*

证. 设 $\varphi : G \to G/\ker\sigma$ 是自然同态, 则得到两个满同态 σ 和 φ, 交换图如下:

$$\begin{tikzcd} G \arrow[rr, "\sigma"] \arrow[d, "\varphi"'] & & \operatorname{im}\sigma \\ G/\ker\sigma \arrow[urr, dashed, "\psi"'] & & \end{tikzcd}$$

其中虚线部分的 ψ 表示我们要找的同构. 定义映射

$$\psi_0(\ker\sigma\cdot a)=\sigma(a),$$

显然 ψ_0 是良定义的.

由于

$$\psi_0(\ker\sigma\cdot a\ker\sigma\cdot b)\xlongequal{\ker\sigma\text{是正规子群}}\psi_0(\ker\sigma\cdot ab)=\sigma(ab)=\sigma(a)\sigma(b),$$

所以 ψ_0 是同态映射.

当 $\sigma(a)=\sigma(b)$ 时, 有

$$\begin{aligned}\sigma(a)(\sigma(b))^{-1}=&e'\\ \sigma(ab^{-1})=&e',\end{aligned}$$

根据引理1.7.1,

$$ab^{-1}\in\ker\sigma\iff b^{-1}\ker\sigma=a^{-1}\ker\sigma,$$

即 $a\ker\sigma=b\ker\sigma$, 亦即 $\ker\sigma\cdot a=\ker\sigma\cdot b$. 可见 ψ_0 为单射.

显然 ψ_0 是满射.

综上所述,ψ_0 是同构映射. 取 $\psi=\psi_0$ 即证明了 $G/\ker\sigma\cong\in\sigma$.

进一步, 若 σ 是满同态, 则 $G'\cong\operatorname{im}\sigma$, 从而 $G/\ker\sigma\cong G'$. □

1.8 环, 子环

定义 1.8.1 (环). *设 L 是一个非空集合, 在 L 上定义了两个代数运算, 一个叫加法, 记为 $a+b$, 一个叫乘法, 记为 ab. 若这两种运算具有性质*

(1)L *对于加法构成 Abel 群;*

(2)L *对于乘法满足结合律;*

(3)L *满足乘法对加法的分配律,*

则称 L 为环.

定义 1.8.2 (子环)**.** 设 S 是环 L 的非空子集合, 若 S 对于 L 的两种运算也成环, 则称环 S 是环 L 的子环.

命题 1.8.1. 环 L 的非空子集合 S 成环的充分必要条件为 S 对于加法是子群且对于乘法封闭.

证. 必要性是显然的, 下面证明充分性.

(1)S 对于加法构成 Abel 群: 任取 $a, b \in S$, 于是 $a, b \in L$, 所以

$$ab \xlongequal{L\text{对于乘法构成 Abel 群}} ba,$$

可见 S 关于加法构成的子群满足交换律, 所以 S 为 Abel 群;

(2)S 对于乘法满足结合律: 任取 $a, b, c \in S$, 有 $a, b, c \in L$, 所以

$$a(bc) = (ab)c = abc \in S,$$

可见 S 对于乘法满足结合律;

(3)S 满足乘法对于加法的分配律: 任取 $a, b, c \in S$, 有 $a, b, c \in L$, 所以

$$a(b+c) \xlongequal{L\text{满足乘法对加法的分配律}} ab + ac \in S,$$

可见 S 满足乘法对于加法的分配律. □

定义 1.8.3 (同构映射)**.** 设 L 与 L' 是两个环, 若有 L 到 L' 的一一对应 σ 满足如下性质

$$(1)\sigma(a+b) = \sigma(a) + \sigma(b);$$
$$(2)\sigma(ab) = \sigma(a)\sigma(b),$$

其中 $a, b \in L$, 则称 L 与 L' 同构, 称具有以上性质的 σ 为一个同构映射 (简称同构).

1.9 各种特殊类型的环

命题 1.9.1.

$$\begin{tikzcd}
 & & 环 \arrow[dll, "乘法可交换"'] \arrow[d, dashed, "存在幺元"] \arrow[drr, "无零因子"] & & \\
交换环 \arrow[dr] \arrow[dddrr] & & 幺环 \arrow[dr] & & 无零因子环 \arrow[dl] \\
 & 交换整环 & & 整环 \arrow[ll] \arrow[d, dashed, "非零元可逆"] & \\
 & & & 体 \arrow[d] & \\
 & & & 域 &
\end{tikzcd}$$

注 1.9.1. 幺元*:* 设 L 是环. 若 $e \in L$ 满足

$$\forall a \in L, ae = ea = a,$$

则称 e 为环 L 的幺元 (幺元), 简记为 1;

用 0 表示环中加法群的幺元 (即零元素);

零因子*:* 设 L 是环. 若有 $0 \neq a \in L, 0 \neq b \in L$ 满足 $ab = 0$, 则称 a 为一个左零因子, 称 b 为一个右零因子.

引理 1.9.1. 非零元可逆 $\underset{\not\Leftarrow}{\Rightarrow}$ 无零因子.

证. (1) 非零元可逆 $\Rightarrow$ 无零因子:

设 L 是环且非零元可逆. 假设 $a \in L$ 是 L 的左零因子 (右零因子同理), 则有

$$ab = 0 且 a \neq 0, b \neq 0.$$

设 $c \in L$ 是 a 的逆元, 即

$$ac = ca = 1,$$

于是

$$
\begin{aligned}
&(ca)b = c(ab)\\
&(ca)b = 1b = b \neq 0\\
&c(ab) = c0 = 0,
\end{aligned}
$$

得到矛盾, 从而 L 无零因子, 问题得证.

(2) 无零因子 $\not\Rightarrow$ 非零元可逆:

如整数环. □

定义 1.9.1 (子域)**.** *若域 F 的子环 S 是域, 则称 S 是域 F 的子域.*

1.10 环的同态, 理想

定义 1.10.1 (同态)**.** *设 L, L' 是两个环,σ 是 L 到 L' 的映射. 若对 $\forall a, b \in L, \sigma$ 具有性质*

$$
\begin{aligned}
&(1)\sigma(a+b) = \sigma(a) + \sigma(b);\\
&(2)\sigma(ab) = \sigma(a)\sigma(b),
\end{aligned}
$$

就称 σ 为环 L 到环 L' 的一个同态映射 (简称同态), 简记为 $\sigma : L \to L'$.

注 1.10.1. *(1) 由同态的定义可以看出 $\sigma(L)$ 是 L' 的子环;*

(2) 若 $\sigma(L) = \{0\}$, 称 σ 为零同态;

(3) 若 $\sigma(L) = L'$, 称 σ 为满同态, 称 L' 为 L 的同态象.

定义 1.10.2 (理想)**.** *设 L 成环,$I \subset L$ 为 L 的一个加法子群. 若 $\forall r \in L, \forall a \in L$, 都有*

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

就称 I 是 L 的理想 (或双边理想). 若只满足 $ra \in I$(或$ar \in I$), 则称 I 是 L 的右 (或左) 理想.

注 1.10.2. *显然 $\{0\}$ 与 L 都是 L 的理想, 称它们为平凡的理想.*

1.11 商环

定义 1.11.1 (陪集)**.** *设环 I 是环 L 的理想,I 作为 L 的加法群的子群, 按如下方式定义陪集*

$$r+I(\forall r\in L)\text{为左陪集};\qquad I+r(\forall r\in L)\text{为右陪集},$$

按如下方式定义陪集的加法与乘法

$$\begin{aligned}(r_1+I)+(r_2+I)&=r_1+r_2+I &&(\forall r_1,r_2\in L);\\(r_1+I)(r_2+I)&=r_1r_2+I &&(\forall r_1,r_2\in L),\end{aligned}$$

全体陪集所成的集合在这样规定的运算下成环.

定义 1.11.2 (商环)**.** *设环 I 是环 L 的理想.L 对于 I 的陪集在定义1.11.1的运算下所成的环称为 L 对于 I 的商环, 记作 L/I.*

设环 I 是环 L 的理想. 不难发现 $\sigma(a)=a+I, a\in L$ 是环 L 到商环 L/I 的满同态, 且该同态的核为理想 I. 可见每个理想都是某一同态的核.

引理 1.11.1. *设 $\sigma: L\to L'$, 则 $\ker\sigma$ 是 L 的理想.*

证. 对 $\forall a\in\ker\sigma,\forall b\in L$, 有

$$\begin{aligned}\sigma(ab)&\xlongequal{\sigma\text{是同态}}\sigma(a)\sigma(b)=0\sigma(b)=0\Longrightarrow ab\in\ker\sigma;\\\sigma(ba)&\xlongequal{\sigma\text{是同态}}\sigma(b)\sigma(a)=\sigma(b)0=0\Longrightarrow ba\in\ker\sigma,\end{aligned}$$

可见 $\ker\sigma$ 是 L 的理想. □

定理 1.11.1 (环同态基本定理)**.** *若 $\sigma: L\to L'$, 则 $L/\ker\sigma\cong\operatorname{im}\sigma$. 进一步, 若 σ 是满同态, 则 $L/\ker\sigma\cong L'$.*

证. 设 $\varphi: L\to L/\ker\sigma$ 是自然同态, 则得到两个满同态 σ 和 φ, 交换图如下:

$$\begin{tikzcd}
L \arrow[rr, "\sigma"] \arrow[d, "\varphi"'] & & \operatorname{im}\sigma \\
L/\ker\sigma \arrow[urr, dashed, "\psi"'] & &
\end{tikzcd}$$

其中虚线部分的 ψ 表示我们要找的同构. 定义映射

$$\psi_0(\ker\sigma + a) = \sigma(a),$$

显然 ψ_0 是良定义的.

对 $\forall a, b \in L$, 有

$$\begin{aligned}
\psi_0[(\ker\sigma + a) + (\ker\sigma + b)] \xlongequal{\ker\sigma\text{是理想}} & \psi_0(\ker\sigma + a + b) \\
= & \sigma(a + b) \\
\xlongequal{\sigma\text{是同态}} & \sigma(a) + \sigma(b) \\
= & \psi_0(\ker\sigma + a) + \psi_0(\ker\sigma + b),
\end{aligned}$$

由此可见 ψ_0 保持加法;

$$\begin{aligned}
\psi_0[(\ker\sigma + a)(\ker\sigma + b)] \xlongequal{\ker\sigma\text{是理想}} & \psi_0(\ker + ab) \\
= & \sigma(ab) \\
\xlongequal{\sigma\text{是同态}} & \sigma(a)\sigma(b) \\
= & \psi_0(\ker\sigma + a)\psi_0(\ker\sigma + b),
\end{aligned}$$

由此可见 ψ_0 保持乘法, 于是 $\psi_0 : L/\ker\sigma \to \operatorname{im}\sigma$.

对 $\forall \sigma(a) = \sigma(b)$, 有

$$\begin{aligned}
& \sigma(a) - \sigma(b) = 0 \\
\overset{\sigma\text{是同态}}{\Longrightarrow} & \sigma(a - b) = 0 \\
\Longrightarrow & a - b \in \ker\sigma \\
\overset{\text{引理1.7.1}}{\Longrightarrow} & \ker\sigma + a = \ker\sigma + b
\end{aligned}$$

$$\Longrightarrow \psi_0\text{是单射}.$$

ψ_0 显然是满射.

综上所述,ψ_0 是同构映射. 取 $\psi = \psi_0$ 即证明了 $L/\ker\sigma \cong \operatorname{im}\sigma$.

进一步, 若 σ 是满同态, 则 $L' \cong \operatorname{im}\sigma$, 从而 $L/\ker I \cong L'$. □

1.12 特征

设 F 是域,e 是 F 中的幺元. 若 e 是有限阶元素, 即存在正整数 m 使得 $me = 0$, 则将 m 定义为 F 的幺元在 F 的加法群中的阶. 显然 m 一定是素数.

定义 1.12.1 (特征)**.** *设 F 是域. 若 F 的幺元 e 在 F 的加法群中是有限阶元素, 阶为 p, 就称域 F 的特征为 pl 若幺元是无限阶元素, 就称域 F 的特征为 0. 域 F 的特征记为 $\chi(F)$.*

命题 1.12.1. *在域的加法群中, 任一非零元素都与幺元有相同的阶.*

证. 设 a 是域 F 的任一非零元, 由

$$ma = mae \xlongequal{ae\text{乘法可交换}} a(me)$$

可知,$ma = 0$ 当且仅当 $me = 0$, 问题得证. □

定理 1.12.1. *设 F 为域. 若 $\chi(F) = p \neq 0$, 则 F 包含与 Z/pZ 同构的子域; 若 $\chi(F) = 0$, 则 F 包含与有理数域同构的子域.*

证. 首先按如下方式定义整数环到 F 的映射 σ

$$\sigma(n) = ne.$$

注意到 $\forall n, m \in \mathbb{Z}$

$$\sigma(n+m) = (n+m)e = ne + me;$$

$$\sigma(nm) = (nm)e = (ne)(me) = \sigma(n)\sigma(m),$$

于是 $\sigma : \mathbb{Z} \to F$.

(1) 若 $\chi(F) = p \neq 0$, 令 $\sigma(n) = 0$, 有

$$0 = \sigma(n) = ne \iff n \in p\mathbb{Z},$$

可见 $\ker\sigma = p\mathbb{Z}$. 易见

$$\operatorname{im}\sigma = \{e, 2e, \cdots, (p-1)e, 0\} \subset F,$$

不难验证 $\operatorname{im}\sigma$ 构成域 F 的子域. 根据环同态基本定理 (定理1.11.1), 有

$$F/p\mathbb{Z} \cong \operatorname{im}\sigma.$$

(2) 若 $\chi(F) = 0$, 令 $\sigma(n) = e$ 可推出 $n = 0$, 即 $\ker\sigma = \{0\}$, 所以 σ 是单射. 易见

$$\operatorname{im}\sigma = \{ne |\, n \in \mathbb{Z}\}$$

与整数环 $\mathbb{Z}$ 同构. 按如下方式扩充 σ 的定义

$$\sigma\left(\frac{m}{n}\right) = (ne)^{-1}(me),$$

由于当 $\dfrac{m}{n} = \dfrac{m'}{n'}$ 时

$$(ne)^{-1}(me)^{-1} = (n'e)^{-1}(m'e)^{-1} \iff \sigma\left(\frac{m}{n}\right) = \sigma\left(\frac{m'}{n}\right),$$

所以这是良定义的. 易见

$$\operatorname{im}\sigma = \left\{(ne)^{-1}me : n \in \mathbb{Z}\text{且}n \neq 0; m \in \mathbb{Z}\right\} \subset F$$

构成 F 的子域, 而 $\operatorname{im}\sigma \cong \mathbb{Q}$, 亦即 F 有一个同构于有理数域 $\mathbb{Q}$ 的子域.

综上所述, 问题得证. $\square$

1.13 CHAPTER1 习题

问题 1.1 (P54T7)**.** *设 G 是群,$a, b \in G$. 若 $a^{-1}ba = b^r (r \in \mathbb{N}_+)$, 证明 $a^{-i}ba^i = b^{r^i}(1, 2, \cdots)$.*

证. 使用数学归纳法.

(1) 题设条件已经说明, 当 $i = 1$ 时结论成立;

(2) 假设当 $i = n$ 时结论成立即 $a^{-n}ba^n = b^{r^n}$, 于是

$$\begin{aligned} a^{-(n+1)}ba^{n+1} =& a^{-1}(a^{-n}ba^n)a \\ =& a^{-1}b^{r^n}a \\ =& (a^{-1}ba)^{r^n} \\ =& (b^r)^{r^n} \\ =& b^{r^{n+1}}, \end{aligned}$$

可见当 $i = n + 1$ 时结论也成立.

综上所述, 问题得证. □

问题 1.2 (P54T8)**.** *证明: 群 G 为交换群 $\iff$ 映射 $x \mapsto x^{-1}$ 为同构映射.*

证. 设 $\varphi : G \to G', x \mapsto x^{-1}$, 不难发现 $G = G'$.

(1) 必要性:

令 $\varphi(x) = e$, 有 $x^{-1} = e \Longrightarrow x = e \Longrightarrow \ker\varphi = \{e\}$, 可见 φ 是单射;

$\forall x \in G' = G$,$\exists x^{-1} \in G$ 满足 $\varphi(x^{-1}) = x$, 可见 φ 是满射;

$\forall x, y \in G$, 有

$$\begin{aligned} \varphi(xy) = (xy)^{-1} =& y^{-1}x^{-1} \\ \xlongequal{G\text{是交换群}}& x^{-1}y^{-1} \\ =& \varphi(x)\varphi(y), \end{aligned}$$

于是 φ 是同态.

必要性得证.

(2) 充分性:

$\forall x, y \in G$, 有 $x^{-1}, y^{-1} \in G$, 并且

$$\begin{aligned}\varphi(x^{-1}y^{-1}) &\xlongequal{\varphi\text{是同态}} \varphi(x^{-1})\varphi(y^{-1}) \\ \Longrightarrow & yx = xy \\ \Longrightarrow & G\text{是交换群}.\end{aligned}$$

充分性得证.

综上所述, 问题得证. □

问题 1.3 (P54T9)**.** *设 S 为群 G 的非空子集合, 在 G 中定义关系 $a \sim b$ 当且仅当 $ab^{-1} \in S$. 证明这是等价关系的充要条件为 S 为 G 的子群.*

证. 先给出等价关系的定义.

称满足如下三条性质的关系 $\sim$ 为等价关系

$$\begin{gathered}\text{(i)反身性:} a \sim a; \\ \text{(ii)对称性: 若 } a \sim b, \text{ 则 } b \sim a; \\ \text{(iii)传递性: 若 } a \sim b, b \sim c, \text{ 则 } a \sim c.\end{gathered}$$

(1) 必要性:

对 $\forall a, b \in S$ 亦即 $ae^{-1}, be^{-1} \in S$, 有

$$ae^{-1}(be^{-1})^{-1} \in S,$$

即 $ab^{-1} \in S$, 可见 $S < G$.

必要性得证.

(2) 充分性:

由于 S 非空, 所以 $\forall s \in S$, 有

$$ss^{-1} \in S,$$

即 $s \sim s$, 反身性得证;

任取 $a \in S$, 由于 S 成群, 所以 $a^{-1} \in S$, 进而若 $a \sim b$ 即 $ab^{-1} \in S$ 即 $a \sim b$, 有

$$ba^{-1} = (ab^{-1})^{-1} \in S,$$

即 $b \sim a$, 对称性得证;

设 $a \sim b, b \sim c$ 即 $ab^{-1} \in S, bc^{-1} \in S$, 由 S 成群可知

$$(ab^{-1})(bc^{-1}) \in S,$$

即 $a \sim c$, 传递性得证.

充分性得证.

综上所述, 问题证毕. □

问题 1.4 (P55T20)**.** *设群 H, K 为群 G 的子群, 证明 HK 为 G 的子群当且仅当 $HK = KH$.*

证. (1) 必要性

按以下方式定义从 HK 到 HK 的一一对应 φ_1

$$\varphi_1(hk) = (hk)^{-1}, \forall hk \in HK.$$

注意到 $\operatorname{im}\varphi_1 = HK$, 并且

$$(hk)^{-1} = k^{-1}h^{-1} \in KH,$$

即 $HK = \operatorname{im}\varphi_1 \subset KH$. 同理, 按以下方式定义 KH 到 KH 的一一对应 φ_2 可证 $KH \subset HK$

$$\varphi_2(kh) = k^{-1}h^{-1}, \forall kh \in KH.$$

由 $HK \subset KH$ 及 $KH \subset HK$ 可得 $HK = KH$, 必要性得证.

(2) 充分性

对任意 $h_1k_1, h_2k_2 \in HK$, 有

$$\begin{aligned} h_1k_1(h_2k_2)^{-1} =& h_1k_1k_2^{-1}h_2^{-1} \\ =& h_1(k_1k_2^{-1}h_2^{-1}), \end{aligned}$$

而

$$k_1k_2^{-1}h_2^{-1} \in KH = HK,$$

所以 $h_1k_1(h_2k_2)^{-1} \in HK$, 亦即

$$\forall a, b \in HK \Longrightarrow ab^{-1} \in HK,$$

可见 $HK < G$, 充分性得证.

综上所述, 问题证毕. □

问题 1.5 (P56T28). *在整数集 $\mathbb{Z}$ 上重新定义加法与乘法为*

$$a \oplus b = ab, \qquad a \odot b = a + b.$$

试问 $\mathbb{Z}$ 在新定义的运算下是否成环.

解. 不能成环, 理由如下.

假设 $\mathbb{Z}$ 在新定义的运算下成环, 则 $\mathbb{Z}$ 关于加法成交换群. 对 $\forall n \in \mathbb{Z}$

$$1 \oplus n = 1 \cdot n = n,$$

所以 $\mathbb{Z}$ 在新定义的运算下, 关于加法的所成的交换群中的幺元是 1. 注意到 $\forall m \in \mathbb{Z}$

$$0 \oplus m = 0 \cdot m = 0 \neq 1,$$

所以在此加法群中,0 无逆元, 这与 $\mathbb{Z}$ 关于加法成交换群矛盾, 所以 $\mathbb{Z}$ 在新定义的运算下不成环. □

问题 1.6 (P56T29). 设 L 为有幺元的交换环, 在 L 中定义

$$a \oplus b = a + b - 1,$$
$$a \odot b = a + b - ab.$$

证明在新定义的运算下,L 仍为有幺元的交换环, 并且与原来的环同构.

证. (1) 对任意 $a, b, c \in L$

$$\begin{aligned}
&(a \oplus b) \oplus c \\
=&(a + b - 1) \oplus c \\
=&(a + b - 1) + c - 1 \\
=&a + b + c - 2 \\
=&a + (b + c - 1) - 1 \\
=&a + (b \oplus c) - 1 \\
=&a \oplus (b \oplus c),
\end{aligned}$$

L 关于 $\oplus$ 满足结合律;

(2) 对任意 $a \in L$

$$\begin{aligned}
&1 \oplus a \\
=&1 + a - 1 \\
=&a,
\end{aligned}$$

L 关于 $\oplus$ 有幺元;

(3) 对任意 $a \in L$

$$\begin{aligned}
&(-a) \oplus a \\
=&-a + a - 1 \\
=&1,
\end{aligned}$$

L 中的元素关于 $\oplus$ 有逆元;

(4) 对任意 $a, b \in L$

$$\begin{aligned}&a \oplus b\\=&a+b-1\\=&b+a-1\\=&b \oplus a,\end{aligned}$$

L 关于 $\oplus$ 可交换;

(5) 对任意 $a, b, c \in L$

$$\begin{aligned}&(a \oplus b) \odot c\\=&(a+b-1) \odot c\\=&(a+b-1)+c-(a+b-1)c\\=&a+b+2c-ac-bc-1,\end{aligned}$$

$$\begin{aligned}&(a \odot c) \oplus (b \odot c)\\=&(a \odot c)+(b \odot c)-1\\=&(a+c-ac)+(b+c-bc)-1\\=&a+b+2c-ac-bc-1,\end{aligned}$$

L 满足 $\odot$ 对于 $\oplus$ 的分配律;

(6) 对任意 $a, b \in L$

$$\begin{aligned}&a \odot b\\=&a+b-ab\\=&b+a-ba\\=&b \odot a,\end{aligned}$$

L 关于 $\odot$ 满足交换律;

(7) 对任意 $a \in L$, 存在 $0 \in L$ 满足

$$\begin{aligned}
&0 \odot a \\
=&0 + a - 0a \\
=&a,
\end{aligned}$$

L 关于 $\odot$ 有幺元.

(1)~(7) 说明 L 成有幺元的交换环, 其中零元为 1, 幺元为 0.

定义 φ 为 $(L;+,\cdot) \to (L;\oplus,\odot)$ 的映射

$$\varphi(x) = 1 - x,$$

显然 φ 为双射.

注意到

$$\begin{aligned}
\varphi(x+y) =&1 - x - y, \\
\varphi(x) \oplus \varphi(y) =&(1-x) \oplus (1-y) \\
=&(1-x) + (1-y) - 1 = 1 - x - y,
\end{aligned}$$

即 $\varphi(x+y) = \varphi(x) \oplus \varphi(y)$;

$$\begin{aligned}
\varphi(xy) =&1 - xy, \\
\varphi(x) \odot \varphi(y) =&(1-x) \odot (1-y) \\
=&(1-x) + (1-y) - (1-x)(1-y) \\
=&2 - x - y - (1 - y - x + xy) \\
=&1 - xy,
\end{aligned}$$

即 $\varphi(xy) = \varphi(x) \odot \varphi(y)$. 可见 φ 是同态映射.

综上所述,$\varphi : (L;+,\cdot) \to (L;\oplus,\odot)$ 为同构映射, 问题得证. $\square$

问题 1.7 (P56T30). *给环出 L 与它的子环 S 的例子, 它们分别具有下列性质*

(1)L 有幺元,S 无幺元;

(2)L 无幺元,S 有幺元;

(3)L, S 均有幺元, 但不相同;

(4)L 不交换,S 交换.

解. (1)$L = (\mathbb{Z}; +, \cdot), S = (2\mathbb{Z}; +, \cdot)$.
(1.1) 对于 L:

(1.1.1)$\forall a, b, c \in \mathbb{Z}$

$$(a + b) + c = a + b + c = a + (b + c),$$

可见 $(\mathbb{Z}; +)$ 满足结合律;

(1.1.2)$\forall a \in \mathbb{Z}, \exists 0 \in \mathbb{Z}$ 满足

$$0 + a = a,$$

可见 $(\mathbb{Z}; +)$ 存在左幺元;

(1.1.3)$\forall a \in \mathbb{Z}, \exists -a \in \mathbb{Z}$ 满足

$$-a + a = 0,$$

可见 $(\mathbb{Z}; +)$ 中的任意元素都有左逆元;

(1.1.4)$\forall a, b \in \mathbb{Z}$, 有

$$a + b = b + a \in \mathbb{Z},$$

可见 $(\mathbb{Z}; +)$ 满足交换律;

(1.1.5)$\forall a, b, c \in \mathbb{Z}$, 有

$$a(b + c) = ab + ac,$$

可见 $(\mathbb{Z};+,\cdot)$ 满足乘法对于加法的分配律.
(1.1.1)~(1.1.5) 说明 $(\mathbb{Z};+,\cdot)$ 成环. 注意到 $\forall a\in\mathbb{Z}$, 有 $1\in\mathbb{Z}$ 满足

$$1\cdot a=a,$$

所以 $(\mathbb{Z};+,\cdot)$ 有幺元 1.
(1.2) 对于 S:

同理可证 S 成环. 假设 S 有幺元 e, 则 $\forall s\in S$

$$es=s,$$

现取 $n\in\mathbb{Z}$ 且 $m\neq 0$, 则 $2n\in 2\mathbb{Z}$ 且

$$e(2n)=2n\overset{\text{等式两端同时除以 }2n}{\Longrightarrow}e=1\notin 2\mathbb{Z},$$

这与 $e\in S$ 矛盾, 所以 S 没有幺元.

(2)

$$L=\left(\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}:a,b\in\mathbb{R}\right\};+,\cdot\right),S=\left(\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix}:a\in\mathbb{R}\right\};+\cdot\right).$$

(2.1) 对于 L:

(2.1) 容易验证 L 成环. 令 $e=\begin{pmatrix}x_1&x_2\\x_3&x_4\end{pmatrix}$ 满足

$$\begin{cases}e\begin{pmatrix}a&b\\0&0\end{pmatrix}=\begin{pmatrix}x_1&x_2\\x_3&x_4\end{pmatrix}\begin{pmatrix}a&b\\0&0\end{pmatrix}=\begin{pmatrix}a&b\\0&0\end{pmatrix}\\\begin{pmatrix}a&b\\0&0\end{pmatrix}e=\begin{pmatrix}a&b\\0&0\end{pmatrix}\begin{pmatrix}x_1&x_2\\x_3&x_4\end{pmatrix}=\begin{pmatrix}a&b\\0&0\end{pmatrix}\end{cases}\text{对任意 }a,b\in\mathbb{R}\text{ 均成立}$$

$$\iff \begin{cases} ax_1 = a \\ bx_1 = b \\ ax_3 = 0 \\ bx_4 = 0 \\ ax_1 + bx_3 = a \\ ax_2 + bx_4 = b \\ ax_3 = 0 \\ bx_3 = 0 \end{cases} \quad \text{对任意 } a, b \in \mathbb{R} \text{ 均成立},$$

解之可得

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin L,$$

亦即 L 没有幺元.

容易验证 S 成环. 注意到 $\forall s = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in S, \exists e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in S$ 满足

$$es = se = s,$$

所以 S 有幺元 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

(3)

$$L = \left(\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R} \right\}; +, \cdot \right), S = \left(\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}; +, \cdot \right).$$

取 $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, e_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ 验证它们分别是 L 与 S 中的幺元即可.

(4)

$$L = \left(\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}; +, \cdot \right), S = \left(\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}; +, \cdot \right).$$

(4.1) 对于 L:

令 $l_1 = \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}, l_2 = \begin{pmatrix} 3 & 0 \\ 4 & 0 \end{pmatrix} \in L$, 易见

$$l_1 l_2 = \begin{pmatrix} 3 & 0 \\ 6 & 0 \end{pmatrix} \neq \begin{pmatrix} 3 & 0 \\ 4 & 0 \end{pmatrix} = l_2 l_1,$$

于是 L 不交换.

(4.2) 对于 S:

任取 $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in S$, 注意到

$$\begin{aligned} & \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \\ = & \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \\ = & \begin{pmatrix} ba & 0 \\ 0 & 0 \end{pmatrix} \\ = & \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \end{aligned}$$

所以 S 交换. □

问题 1.8 (P56T31). *环 L 中元素 e_L 称为左幺元, 若对 $\forall a \in L$*

$$e_L a = a;$$

元素 e_R 称为右幺元, 若对 $\forall a \in L$

$$e_R a = a;$$

证明

(1) 若 L 既有左单位又有右单位, 则 L 有幺元;

(2) 若 L 有左单位, 无零因子, 则 L 有幺元;

(3) 若 L 有左单位, 无右单位, 则 L 至少有两个左单位.

证. (1) 由

$$e_Le_R = \begin{cases} e_R(e_L \text{ 是左幺元}); \\ e_L(e_R \text{ 是右幺元}) \end{cases}$$

可知 $e_L = e_R$, 所以 L 有幺元;

(2) 在等式 $e_La = a$ 两端同时左乘 a 可得

$$\begin{aligned} &ae_La = a^2 \\ \Longrightarrow &(ae_L - a)a = 0 \\ \Longrightarrow &ae_L - a = 0 \\ \Longrightarrow &ae_L = a, \end{aligned}$$

可见 L 有幺元;

(3) 设 e_L 为 L 的一个左单位, 由于 L 无右单位, 所以 $\exists x \in L$, 满足

$$\begin{aligned} &xe_L \neq x \\ \Longrightarrow &xe_L - x + e_L \neq e_L. \end{aligned}$$

注意到 $\forall a \in L$

$$(xe_L - x + e_L)a = a,$$

所以 $xe_L - x + e_L$ 是异于 e_L 的左单位, 所以 L 至少有两个左单位. □

问题 1.9 (P56T32)**.** *设 F 为域. 证明 F 无非平凡的理想.*

证. 设 $I \neq \varnothing$ 是 F 的理想. 首先证明 I 一定含有零元.

对 $\forall a \in I$, 若 a 是零元, 则显然 I 含有零元; 若 a 不是零元, 由

$$a \in I \subset F$$

可知 a 在 F 中存在逆元 $-a$, 于是由理想的定义可知

$$0 = a + (-a) \in I,$$

所以 I 有零元.

由理想的定义有 $\forall f \in F$

$$f = 0 + f \in I,$$

所以 $F \subset I$, 从而 $F = I$. 可见域 F 没有非平凡的理想. □

问题 1.10 (P57T35)**.** *设 L 为有幺元的交换环. 若 L 无非平凡的理想, 则 L 为域.*

证. 由命题1.9.1与引理1.9.1可知, 若能证明 L 的非零元可逆, 便能推出 L 为域.

任取 $0 \neq a \in L$, 令

$$La = \{la : l \in L\},$$

首先证明 La 是 L 的加法子群.

对 $\forall l_1 a, l_2 a \in La$, 有

$$l_1 a - l_2 a = (l_1 - l_2)a,$$

注意到 $l_1 - l_2 \in L$, 于是

$$(l_1 - l_2)a \in La \Longrightarrow l_1 a - l_2 a \in La,$$

所以 La 是 L 的加法子群.

然后证明 La 是 L 的理想. 对 $\forall la \in La, b \in L$, 注意到 $bl, lb \in L, ab = ba$, 所以

$$\begin{aligned} &lab = l(ab) = l(ba) = lba \in La \\ &bla \in La, \end{aligned}$$

所以 La 是 L 的理想. 因为 $La \neq \varnothing$ 且 L 没有非平凡的理想, 所以 $La = L$.

最后证明 L 即 La 是域. 由于 $1 \in L = La$, 所以

$$\exists b \in L \ \text{ s.t. } \ ba = 1,$$

所以 a 有逆元 b, 亦即 L 的非零元均有逆元, 从而 L 是域. 问题证毕. $\square$

Chapter 2

群

2.1 群的同态定理

定理 2.1.1 (群的第一同构定理)**.** *设 G 是群,$H < G, N \lhd G$, 则*

$$(1) HN < G$$

$$(2) H \cap N \lhd H \text{且} H/H \cap N \cong HN/N.$$

证. (1) 的证明

$HN < G \iff$

$$\text{(i)} HN\text{非空}$$

$$\text{(ii)} \forall a, b \in HN \Longrightarrow ab^{-1} \in HN.$$

HN 显然非空. 对任意 $h_1n_1, h_2n_2 \in HN$ 注意到

$$\begin{aligned} & h_1n_1(h_2n_2)^{-1} \\ =& h_1n_1n_2^{-1}h_2^{-1} \\ =& h_1h_2^{-1}(h_2n_1n_2^{-1}h_2^{-1}). \end{aligned}$$

由于 $N \lhd G$, 所以 $\forall g \in G, gNg^{-1} \in N$, 又 $h_2 \in H \subset G$, 所以

$$h_1 h_2^{-1}(h_2 n_1 n_2^{-1} h_2^{-1}) \in N,$$

从而

$$h_1 n_1 (h_2 n_2)^{-1} \in N,$$

于是 $HN < G$.

(2) 的证明

定义映射

$$\begin{aligned} \varphi : H &\to HN/N \\ h &\mapsto hN, \end{aligned}$$

显然这是良定义的. 对 $\forall h_1, h_2 \in H$

$$\begin{aligned} \varphi(h_1 h_2) &= h_1 h_2 N \\ &= h_1 N h_2 N \\ &= \varphi(h_1)\varphi(h_2), \end{aligned}$$

可见 φ 是同态映射, 所以由群同态基本定理 (定理1.7.2)

$$H/\ker\varphi \cong \operatorname{im}\varphi.$$

注意到

$$\begin{aligned} & h \in \ker\varphi \\ \Longleftrightarrow\ & hN = N \\ \Longleftrightarrow\ & h \in N \\ \overset{h\in H}{\Longleftrightarrow}\ & h \in H \cap N, \end{aligned}$$

所以 $\ker\varphi = H\cap N$, 从而

$$H\cap N \lhd H$$
$$H/H\cap N \cong \operatorname{im}\varphi.$$

对 $\forall hnN \in HN/N$, 有

$$hnN = hN,$$

所以 $\exists h\in H$ s.t.

$$\varphi(h) = hN,$$

所以 φ 是满同态, 从而

$$\operatorname{im}\varphi = HN/N,$$

所以

$$H/H\cap N \cong HN/N.$$

$\square$

注 2.1.1. *类似可以证明: 若 $H<G, N\lhd G$, 有*

$$(1) NH < G$$
$$(2) H\cap N \lhd H \text{且} H/H\cap N \cong NH/N.$$

定理 2.1.2 (群的第二同构定理)**.** *设 G 是群. 若 $N\lhd G, H\lhd G$ 并且 $N\subset H$, 则*

$$(1) H/N \lhd G/N$$
$$(2) (G/N)/(H/N) \cong G/H.$$

证. (1) 的证明

定义映射

$$\begin{aligned}\varphi : G/N &\to G/H\\ gN &\mapsto gH,\end{aligned}$$

显然 φ 是良定义的. 对 $\forall g_1, g_2 \in G$

$$\begin{aligned}&\varphi(g_1Ng_2N)\\ \xlongequal{N\lhd G}&\varphi(g_1g_2N)\\ =&g_1g_2H\\ \xlongequal{H\lhd G}&g_1Hg_2H\\ =&\varphi(g_1N)\varphi(g_2N),\end{aligned}$$

可见 φ 是同态映射, 所以由群同态基本定理 (定理1.7.2)

$$(G/N)/\ker\varphi \cong \operatorname{im}\varphi.$$

注意到

$$\begin{aligned}&gN \in \ker\varphi\\ \iff& gH = H\\ \iff& g \in H\\ \iff& gN \in H/N,\end{aligned}$$

可见 $\ker\varphi = H/N$, 所以

$$\begin{aligned}&H/N \lhd G/N\\ &(G/N)/(H/N) \cong \operatorname{im}\varphi.\end{aligned}$$

(2) 的证明

对 $\forall gH \in G/H, \exists g \in G$ s.t.

$$\varphi(gN) = gH,$$

可见 φ 是满同态, 进而

$$\operatorname{im}\varphi = G/H,$$

所以

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

$\square$

注 2.1.2. *习惯上将群同态基本定理 (定理1.7.2), 群的第一同构定理 (定理2.1.1), 群的第二同构定理 (定理2.1.2) 统称为群的同态定理.*

定理 2.1.3. *若 G 是群,$N \lhd G$, 则 G 的所有包含 N 的子群与 G/N 的所有子群之间存在一一对应.*

证. 取自然同态

$$\begin{aligned} \pi : G \to & G/N \\ g \mapsto & gN, \end{aligned}$$

则问题转化为证明在集合 A 与 B 之间存在一一对应, 其中

$$\begin{aligned} A &= \{H : H < G, H \supset \ker\pi\} \\ B &= \{H' : H' < \operatorname{im}\pi\}. \end{aligned}$$

设 $H \in A, \pi_H$ 为映射 π 在子群 H 上的限制, 容易验证 $\operatorname{im}\pi_H \in B$. 定义映射

$$\varphi : A \to B$$

$$H \mapsto \operatorname{im} \pi_H,$$

容易验证 φ 是良定义. 若能证明 φ 是一一对应, 则问题证毕.

(1)φ 是满射

$\forall H' < \operatorname{im} \pi$ 即

$$H' = \{\pi(k) : k \in K \subset G\}.$$

注意到

$$\begin{aligned}
& H'\text{成群} \\
\Longleftrightarrow & \forall \pi(k_1), \pi(k_2) \in H' \Longrightarrow \pi(k_1)[\pi(k_2)]^{-1} \in H' \\
\Longleftrightarrow & \forall \pi(k_1), \pi(k_2) \in H' \Longrightarrow \pi(k_1 k_2^{-1}) \in H' \\
\Longleftrightarrow & \forall k_1, k_2 \in K \Longrightarrow k_1 k_2^{-1} \in K \\
\Longleftrightarrow & K < G,
\end{aligned}$$

所以

$$H' = \{\pi(k) : k \in K < G\}. \tag{2.1.1}$$

注意到

$$\forall t \in \ker \pi \Longrightarrow \pi(t) = e \in H',$$

因此不妨让式(2.1.1)中的 K 包含 $\ker \pi$, 即

$$\begin{aligned}
H' &= \{\pi(k) : k \in K < G, K \supset \ker \pi\} \\
&= \operatorname{im} \pi_K (K < G, K \supset \ker \pi),
\end{aligned}$$

所以

$$\begin{aligned}
B &= \{\operatorname{im} \pi_K : K < G, K \supset \ker \pi\} \\
&= \{\operatorname{im} \pi_H : H < G, H \supset \ker \pi\}
\end{aligned}$$

$$= \{ \operatorname{im} \pi_H : H \in A \} ,$$

由此可见 $\operatorname{im} \varphi = B$, 即 φ 是满同态;

(2)φ 是单射

$$\begin{aligned}
&\Longleftrightarrow \forall x_1, x_2 \in A, \text{若} x_1 \neq x_2, \text{则} \varphi(x_1) \neq \varphi(x_2) \\
&\Longleftrightarrow |\{x \in A : \varphi(x) = \varphi(x_0), x_0 \in A\}| = 1 \\
&\Longleftrightarrow |\{H \supset N : \operatorname{im} \pi|_H = \operatorname{im} \pi|_{H_0}, H_0 \supset A\}| = 1 \\
&\Longleftrightarrow \{H \supset N : \operatorname{im} \pi|_H = \operatorname{im} \pi|_{H_0}, H_0 \supset A\} = \{H_0\} \\
&\Longleftrightarrow \text{若 } H_0 \supset N, H \supset N \text{ 且 } \operatorname{im} \pi|_H = \operatorname{im} \pi|_{H_0}, \text{则 } H = H_0,
\end{aligned} \tag{2.1.2}$$

注意到在(2.1.2)的题设条件下, 显然有 $H \supset H_0$, 故只需证明 $H \subset H_0$ 便可得到 $H = H_0$.

在(2.1.2)的题设条件下

$$\begin{aligned}
&\forall h \in H, \exists h_0 \in H_0 \ \text{ s.t. } \ \pi(h) = \pi(h_0) \\
\Longleftrightarrow &\forall h \in H, \exists h_0 \in H_0 \ \text{ s.t. } \ hN = h_0 N \\
\Longleftrightarrow &\forall h \in H, \exists h_0 \in H_0 \ \text{ s.t. } \ h \in h_0 N \subset H_0 \\
\Longrightarrow &H \subset H_0.
\end{aligned}$$

所以 φ 是单射.

由 (1),(2) 便知

$$\begin{aligned}
\varphi : A &\to B \\
H &\mapsto \operatorname{im} \pi_H
\end{aligned}$$

为一一对应, 问题得证. □

定义 2.1.1 (由 S 生成的群)**.** 设 G 是群,S 是 G 的非空子集合.G 的包含 S 的最小的子群, 称为由 S 生成的群, 记作 $< S >$, 即

$$< S > = \bigcap_{S \subset H < G} H.$$

命题 2.1.1. 设 $(G,\cdot)$ 是群. 若 S 是 G 的非空子集合, 则

$$< S >= \left(\left\{ \prod_{k=1}^{m} x_k : x_1, \cdots, x_m \in S \cup S^{-1}, m \in \mathbb{N}_+ \right\}, \cdot \right),$$

即集合 $S \cup S^{-1}$ 中任意多个元素的乘积组成的集合关于 $\cdot$ 构成 $< S >$.

证. 容易验证群 G 的子集合 $\left\{ \prod_{k=1}^{m} x_k : x_1, \cdots, x_m \in S \cup S^{-1}, m \in \mathbb{N}_+ \right\}$ 关于群 G 的乘法成群, 记此群为 A. 注意到 A 包含 S, 所以 A 包含: 包含 S 的最小的子群, 即 $A \supset < S >$.

反之, 对 $\forall a \in A$ 有

$$a = \left(\prod_{\alpha \in \Lambda_1} s_\alpha \right) \cdot \left(\prod_{\beta \in \Lambda_2} s_\beta \right),$$

其中

$$\begin{aligned} & s_\alpha \in S \subset < S >, \alpha \in \Lambda_1 \\ & s_\beta \in S^{-1}, \beta \in \Lambda_2, \end{aligned}$$

注意到 $s_\beta^{-1} \in S \subset < S >, \beta \in \Lambda_2$, 而 $< S >$ 成群, 从而

$$\begin{aligned} & s_\beta = \left(s_\beta^{-1} \right)^{-1} \in < S >, \beta \in \Lambda_2 \\ \Longrightarrow & a = \left(\prod_{\alpha \in \Lambda_1} s_\alpha \right) \cdot \left(\prod_{\beta \in \Lambda_2} s_\beta \right), \end{aligned}$$

可见 $A \subset < S >$.

综上,$A =< S >$, 即

$$< S >= \left(\left\{ \prod_{k=1}^{m} x_k : x_1, \cdots, x_m \in S \cup S^{-1}, m \in \mathbb{N}_+ \right\}, \cdot \right).$$

□

定义 2.1.2 (有限生成的, 循环群)**.** 设 G 是群. 若 $< S >= G$, 则称 S 为 G 的一组生成元. 若 G 中存在一有限集合 S 使得 $< S >= G$, 则称 G 为有限生成的. 由一个元素生成的群称为循环群.

命题 2.1.2. *有限群一定是有限生成的, 反之未必成立.*

证. 设 G 是有限群,$m = |G| \in \mathbb{N}_+$, 则 G 所含元素的个数为 m. 取

$$S = \{g_1, g_2, \cdots, g_m : g_k \text{ 是 } G \text{ 中两两不同的元素}, k = 1, 2, \cdots, m\},$$

则

$$G =< S >,$$

第一个论断证毕;

注意到

$$|(\mathbb{Z}, +)| = \infty$$
$$(\mathbb{Z}, +) =< \{1\} >,$$

所以第二个论断证必. □

定义 2.1.3 (换位子, 换位子群)**.** 对 $\forall a, b \in G$, 元素 $a^{-1}b^{-1}ab$ 称为群 G 中元素 a, b 的换位子, 简记为 $[a, b]$. 由所有换位子生成的群称为 G 的换位子群, 记作 $G^{(1)}$.

命题 2.1.3. *已知 $\varphi : G \to G'$ 是同态映射, 有以下结论成立*
(1) 若 G 是 Abel 群, 则 $\mathrm{im}\,\varphi$ 是 Abel 群;
(2) 虽 $\mathrm{im}\,\varphi$ 是 Abel 群, 但 G 未必是 Abel 群;
(3)$\mathrm{im}\,\varphi$ 是 Abel 群 $\iff G^{(1)} \subset \ker\varphi$.

证. (1)
对 $\forall g_1, g_2 \in G$

$$\varphi(g_1)\varphi(g_2)$$

$$
\begin{aligned}
&\xlongequal{\varphi\text{是同态映射}}\varphi(g_1g_2)\\
&\xlongequal{G\text{是 Abel 群}}\varphi(g_2g_1)\\
&=\varphi(g_2)\varphi(g_1),
\end{aligned}
$$

可见 $\operatorname{im}\varphi$ 是 Abel 群.

(2)

令

$$
G=\left(\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}: a,b,c,d\in\mathbb{R}\text{且}\begin{vmatrix}a & b\\ c & d\end{vmatrix}\neq 0\right\},\cdot\right)
$$

$$
\begin{aligned}
\varphi: G &\to G'\\
\begin{pmatrix}a & b\\ c & d\end{pmatrix} &\mapsto \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},
\end{aligned}
$$

不难得到上述定义的 G 与 φ 证明了 (2).

(3)

$$
\begin{aligned}
&\operatorname{im}\varphi\text{是 Abel 群}\\
\Longleftrightarrow\ &\forall g_1,g_2\in G,\varphi(g_1)\varphi(g_2)=\varphi(g_2)\varphi(g_1)\\
\Longleftrightarrow\ &\forall g_1,g_2\in G,[\varphi(g_2)\varphi(g_1)]^{-1}\varphi(g_1)\varphi(g_2)=e\\
\Longleftrightarrow\ &\forall g_1,g_2\in G,\varphi(g_1^{-1}g_2^{-1}g_1g_2)=e\\
\Longleftrightarrow\ &\forall g_1,g_2\in G,g_1^{-1}g_2^{-1}g_1g_2\in\ker\varphi\\
\Longleftrightarrow\ &G^{(1)}\subset\ker\varphi,
\end{aligned}
$$

问题得证. □

2.2 循环群

循环群的定义见定义2.1.2.

定理 2.2.1. 整数加群 $\mathbb{Z}$ 的子群都是由某一非负整数 m 生成的循环群. 且 $\forall m,n\in\mathbb{N}_+$

$$n\mathbb{Z}\supset m\mathbb{Z} \iff n|m.$$

证. 设 H 是 $(\mathbb{Z},+)$ 的一个子群.

(1)(i) 若 $H=(\{0\},+)$, 取 $m=0$ 即可.

(ii) 若 $H\neq(\{0\},+)$, 则 H 中含有非零数, 因而含有正整数. 设 m 是 H 中最小的正整数, 我们来证明 $H=m\mathbb{Z}$. 任取 $x\in H$, 由整数的除法算式有

$$x=qm+r, \text{其中 } q,r\in\mathbb{Z}, 0\leqslant r<m,$$

从而

$$r=x-qm\in H.$$

若 $r\neq 0$, 则 r 是 H 中小于 m 的正整数, 矛盾, 所以 $r=0$, 即

$$x=qm,$$

这说明 H 中的任意元素都是 m 的倍数. 反之, 由群对运算的封闭性不难得到 m 的倍数也在 H 中. 综上可得

$$H=m\mathbb{Z},$$

第一个论断证毕.

(2) 由 $n\mathbb{Z}\supset m\mathbb{Z}$ 可知 $m\in n\mathbb{Z}$, 所以 $n|m$;

由 $n|m$ 可知,m 的倍数都是 n 的倍数, 所以 $n\mathbb{Z}\supset m\mathbb{Z}$.

综上可得

$$n\mathbb{Z}\supset m\mathbb{Z} \iff n|m,$$

第二个论断证毕. □

定义 2.2.1 (无限循环群)**.** *设群 $G=< g >$, 若 G 是无限群, 则称 G 为无限循环群, 此时记 $|G|=\infty$.*

定理 2.2.2. *已知群 $G=< g >, |G|=m$, 则有以下结论成立*

(1) 若 $m=\infty$, 则 $G\cong\mathbb{Z}$, 它的子群与非负整数成一一对应 (见定理2.2.1);

(2) 若 $m\in\mathbb{N}_+$, 则 $G\cong\mathbb{Z}/m\mathbb{Z}$, 它的子群与 m 的因子一一对应.

证. 定义映射

$$\begin{aligned}\varphi:\mathbb{Z}&\to G\\ n&\mapsto g^n,\end{aligned}$$

显然 φ 是良定义的满同态.

(1) 若 $m=\infty$, 则

$$\begin{aligned}&\forall n,m\in\mathbb{N}_+, n\neq m, \Longrightarrow g^n\neq g^m\\ \Longleftrightarrow\ &\varphi\text{是单射}\\ \Longleftrightarrow\ &\varphi\text{是同构映射}\\ \Longleftrightarrow\ &G\cong\mathbb{Z}.\end{aligned}$$

****

(2) 若 $m\in\mathbb{N}_+$, 不难得到

$$\ker\varphi=m\mathbb{Z},$$

于是根据群同态基本定理 (定理1.7.2) 有

$$G=\operatorname{im}\varphi\cong\mathbb{Z}/k\mathbb{Z}.$$

*** □

引理 2.2.1. *设交换群 G 中元素 g,h 的阶为 m,n 且 $(m,n)=1$, 则元素 gh 的阶为 mn.*

证. ** □

定理 2.2.3. *若 G 是有限交换群, 则在 G 中存在一个元素, 它的阶是 G 中所有元素阶的倍数.*

证. ** □

定理 2.2.4. *若 G 是有限交换群, 则 G 是循环群的充分必要条件是对 $\forall m \in \mathbb{N}_+$, 在 G 中适合方程 $x^m = e$ 的元素的个数不超过 m.*

证. ** □

2.3 单群与 A_n 单性

定义 2.3.1 (单群)**.** *若群 G 没有非平凡的子群, 则称群 G 为单群.*

定理 2.3.1. *设 G 为交换群,$G \neq \{e\}$, 则 G 为单群的充分必要条件是 G 为素数阶的循环群.*

证. ** □

定义 2.3.2 (置换)**.** *设 Ω 为有限集合, 由 Ω 到自身的一个双射叫作 Ω 的一个置换.*

定义 2.3.3 (轮换)**.** *若一个 n 元置换 σ 把 i_1 映成 i_2, 把 i_2 映成 i_3,$\cdots$, 把 i_{r-1} 映成 i_r, 把 i_r 映成 i_1, 其余的元素保持不变, 则称 σ 为一个 r-轮换, 简称轮换.2-轮换也称为对换.*

引理 2.3.1. *每个置换都可以表示成一些对换的乘积; 每个偶置换 (置换 σ 为偶置换当且仅当 σ 的对换分解式中对换的个数为偶数) 都可以表示成一些长度为 3 的轮换 (简称 3-轮换) 的乘积.*

证. ** □

定义 2.3.4 (全变换群)**.** 非空集合 Ω 到自身的所有双射组成的集合, 对于映射的乘法成群, 称它为集合 Ω 的全变换群, 记作 S_n.

定义 2.3.5 (n 元交错群)**.** S_n 中所有偶置换组成的集合, 对于映射的乘法成群, 称它为 n 元交错群, 记作 A_n.

定理 2.3.2. 交错群 $A_n, n \geqslant 5$ 是单群.

证. ** □

2.4 可解群

对任意群 G 而言, 它的换位子群 $G^{(1)}$ 是 G 的正规子群, 即

$$G^{(1)} \lhd G,$$

再做 $G^{(1)}$ 的换位子群 $\left(G^{(1)}\right)^{(1)}$, 记作 $G^{(2)}$, 就有

$$G^{(2)} \lhd G^{(1)} \lhd G,$$

以此类推可得

$$\cdots \lhd G^{(k)} \lhd G^{(k-1)} \lhd \cdots \lhd G^{(2)} \lhd G^{(1)} \lhd G.$$

若 G 是有限群, 这样的群列只有以下两种可能

$$\begin{aligned}&(1)\exists k \in \mathbb{N}_+ \ \text{ s.t. } \ G^{(k)} = G^{(k+1)} = \cdots \neq \{e\}\\ &(2)\exists k \in \mathbb{N}_+ \ \text{ s.t. } \ G^{(k)} = \{e\}.\end{aligned}$$

定义 2.4.1 (可解群)**.** 设 G 是群. 若

$$\exists k \in \mathbb{N}_+ \ \text{ s.t. } \ G^{(k)} = \{e\},$$

则称 G 为可解群.

定理 2.4.1. *群 G 是可解的当且仅当存在一递降的子群列*

$$G = G_0 > G_1 > \cdots > G_s = \{e\},$$

其中每个 G_i 是前一个 G_{i-1} 的正规子群，且商群 G_{i-1}/G_i 交换 $(i = 1, \cdots, s)$.

证. *** □

由群的第二同构定理 (定理2.1.2) 可知, 当群 N 是群 G 的正规子群时, 商群 G/N 的正规子群与 G 中包含 N 的正规子群是一一对应的. 因此, 商群 G/N 是单群的充要条件为正规子群 N 不包含在另一个非平凡的正规子群中, 即不存在 G 的正规子群 $N_1, N_1 \neq G, N_1 \neq N$, 且

$$N < N_1 \lhd G,$$

具有此性质的正规子群 N 称为极大的.

定理 2.4.2. *有限群 G 是可解的的充分必要条件为存在递降的子群列*

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_t = \{e\},$$

其中商群 $H_{i-1}/H_i (i = 1, \cdots, t)$ 都是素数阶的循环群.

证. *** □

2.5 群的自同构群

定义 2.5.1 (自同构与自同构群)**.** *一个群到它自身的同构映射称为自同构映射，简称为自同构. 群的全部自同构在变换下的乘法下成群，称为自同构群. 群 G 的自同构群记作 $\mathrm{Aut}\,(G)$.*

设 G 为群,$a \in G$ 为固定元素. 定义

$$\sigma_a : G \to G$$

$$g \mapsto aga^{-1},$$

不难验证 $\sigma_a \in \mathrm{Aut}\,(G)$.

定义 2.5.2 (内自同构与内自同构群)**.** 称 σ_a 这种由 G 中元素引起的自同构为内自同构.$a \mapsto \sigma_a$ 给出了群 G 到 $\mathrm{Aut}\,(G)$ 的同态,G 的同态像就是 G 的全体内自同构, 它们组成 $\mathrm{Aut}\,(G)$ 的子群, 记作 $\mathrm{In}\,(G)$, 称为 G 的内自同构群.

定义 2.5.3 (中心)**.** 对任意群 G, 与 G 的全体元素可交换的元素组成的集合称为 G 的中心, 记作 $Z(G)$.

定理 2.5.1. 定义映射

$$\begin{aligned} f :&G \to \mathrm{In}\,(G) \\ &a \mapsto \sigma_a, \end{aligned}$$

则

$$\begin{aligned} \ker f &= Z(G) \\ G/Z(G) &\cong \mathrm{In}\,(G). \end{aligned}$$

证. ** □

定理 2.5.2. 对任意群 G, 有

$$\mathrm{In}\,(G) \lhd \mathrm{Aut}\,(G).$$

证. ** □

定义 2.5.4 (外自同构群)**.** 对任意群 G, 称自同构群对于内自同构群的商群

$$\mathrm{Aut}\,(G)/\mathrm{In}\,(G)$$

为 G 的外自同构群.

定理 2.5.3. 对任意群 G, 若 $Z(G)=\{e\}$, 则

$$G \cong \mathrm{In}\,(G).$$

此时我们可以认为 $G < \mathrm{In}\,(G)$.

证. ** □

定义 2.5.5 (完全群)**.** 一个中心为单位且自同构全是内自同构的群称为完全群.

2.6 群作用

定义 2.6.1 (群 G 在集合 X 上的作用)**.** 设 G 是群,X 是非空集合. 若映射 $f: G\times X \to X$ 适合以下条件

$$\begin{aligned}\forall g_1, g_2 \in G, & x\in X:\\ &(1) f(e,x)=x\\ &(2) f(g_1g_2,x)=f(g_1,f(g_2,x)),\end{aligned}$$

就称 f 决定了群 G 在集合 X 上的作用.

注 2.6.1. 在不需要明确指出映射 f 情况下, 通常把 $f(g,x)$ 简写成 $g(x)$. 按此写法, 定义2.6.1中的条件就可以写成

$$\begin{aligned}&(1) e(x)=x\\ &(2) g_1(g_2(x))=g_1g_2(x).\end{aligned}$$

例 2.6.1. 设 G 是群, 取 $X=G$. 定义

$$g(x)=gx, \quad 对 g,x\in G.$$

这就给出了一个群在集合 G 上的作用. 此即以前所谓的左平移.

例 2.6.2 (共轭变换)**.** *设 G 是群, 取 $X = G$. 定义*

$$g(x) = gxg^{-1}, \quad \text{对} g, x \in G.$$

此即群 G 上的共轭变换. 称元素 x 与元素 gxg^{-1} 共轭; 称子群 H 与子群 gHg^{-1} 共轭, 它们都是等价关系; 称群 G 共轭作用在集合 G 上.

例 2.6.3. *设 G 是群,$H < G$, 令 $X = \{xH : x \in G\}$, 定义*

$$g(xH) = gxH, \quad g, x \in G.$$

这就决定了群 G 在集合 X 上的左右.

定义 2.6.2 (齐性空间)**.** *设 G 是群,$H < G$, 称*

$$X = \{xH : x \in G\}$$

是群 G 的一个齐性空间.

当群 G 作用在集合 X 上时, 有可能 G 中的不同的元素在 X 上引起相同的映射, 亦即 $g \mapsto \sigma_g$ 不一定是单射. 比如在例2.6.2中,$Z(G)$ 中的元素都对应 G 上的恒同映射.

定义 2.6.3 (如实的)**.** *若映射*

$$\begin{aligned} f : & G \to \mathrm{In}\,(G) \\ & a \mapsto \sigma_a \end{aligned}$$

是单射, 就称群 G 在集合 X 上的作用是如实的, 或称群 G 如实地作用在集合 X 上. 其中

$$\begin{aligned} \sigma_a : & G \to G \\ & g \mapsto aga^{-1}. \end{aligned}$$

注 2.6.2. *例2.6.1中的作用是如实的; 例2.6.2, 例2.6.3不一定是如实的.*

定义 2.6.4 (等价的)**.** 设 G 是群,X 与 X' 是非空集合,G 作用在 X 与 X' 上. 若有一个一一对应 $\varphi: X \to X'$ 使得

$$\varphi\left(g(x)\right) = g\left(\varphi(x)\right),$$

则称 G 在集合 X 与 X' 上的作用是等价的.

从抽象的观点来看, 两个等价的作用可以不加区别.

定义 2.6.5 (集合 X 上的等价关系)**.** 对 $\forall x, y \in X$, 若

$$\exists g \in G \ \ \text{s.t.} \ \ y = g(x),$$

则称 x 等价于 y, 记作 $x \sim y$.

注 2.6.3. *定义2.6.5中的关系 $\sim$ 是等价关系的证明如下.*

证. ** □

定义 2.6.6 (G-轨道)**.** *在定义2.6.5中的等价关系下, 集合 X 中的元素被分成等价类, 称这样分成的等价类为 x 的 G-轨道, 简称轨道, 记作 O_x. 称 x 为该轨道的代表.*

注 2.6.4. 由于轨道就是等价类, 所以任意两条轨道要么相等, 要么无交, 即

$$X = \bigcup_{i \in I} O_{x_i},$$

其中当 $x_i \neq x_j$ 时 $O_{x_i} \cap O_{x_j} = \varnothing$. 进而

$$|X| = \sum_{i \in I} |O_{x_i}|.$$

定义 2.6.7 (完全代表系)**.** 称集合

$$\{x_i : i \in I\}$$

为 x 的 G-轨道的完全代表系.

定义 2.6.8 (不动元素). 当轨道 O_x 只含有一个元素 x 即

$$\forall g \in G, g(x) = x$$

时, 称 x 为 G 的不动元素.

在例2.6.2中, 若 $x \in Z(G)$, 则显然 $O_x = \{x\}$; 反之, 由 $O_x = \{x\}$ 可知 $x \in Z(G)$.

定义 2.6.9 (传递的). 设群 G 作用在集合 X 上, 当 X 是一个轨道即

$$\forall x, y \in X, \exists g \in G \quad \text{s.t.} \quad g(x) = g(y)$$

时, 称群 G 在集合 X 上的作用是传递的.

不难发现, 例2.6.1与例2.6.3都是传递的的情形.

定义 2.6.10 (稳定子与稳定子群). 设群 G 作用在集合 X 上, 对 $\forall x \in X$, 称集合

$$H_x = \{g \in G : g(x) = x\}$$

是 x 的稳定子. 容易验证,H_x 是 G 的子群, 因此也称为元素 x 的稳定子群.

当群 G 在集合 G 上的作用是共轭作用 (参考例2.6.2) 时

$$\begin{aligned} H_x &= \left\{g \in G : gxg^{-1} = x\right\} \\ &= \left\{g \in G : gx = xg\right\}. \end{aligned} \tag{2.6.3}$$

定义 2.6.11 (中心化子). 称等式(2.6.3)右端的集合为 x 在 G 里的中心化子, 记作 $Z(x)$, 它就是在群 G 的共轭作用下 x 的稳定子群 H_x.

定理 2.6.1 (轨道-稳定子定理). 设群 G 作用在集合 X 上,$x \in X, O_x$ 是包含 x 的轨道,H_x 是 x 的稳定子群, 则群 G 在集合 O_x 上的作用与群 G 在齐性空间 G/H_x 上的作用等价, 也可写作

$$|O_x| = [G : H_x],$$

即 x 的轨道的长度 *(x 的轨道所含元素的个数)* 等于 x 的稳定子在 G 中的指数.

证. ** □

推论 2.6.1. 设群 G 在集合 X 上的作用是传递的,$x \in X, H_x$ 是元素 x 的稳定子群. 则 G 在 X 上的作用与 G 在齐性空间 G/H_x 上的作用等价.

证. ** □

推论 2.6.2. 设有限群 G 作用在集合 X 上. 则任意一个轨道 O_x 包含有限多个元素, 并且包含的元素的个数是 $|G|$ 的因子.

证. ** □

定义 2.6.12 (p-群)**.** 设 G 是有限群, 若 $|G|$ 是素数 p 的方幂, 即

$$|G| = p^k, \quad k \geqslant 1,$$

则称 G 为 p-群 *(p 是素数)*.

推论 2.6.3. 设有限群 G 作用在有限集合 X 上. 若 G 是 p-群,$|X| = n, (n,p) = 1$, 则 X 中一定有不动元素.

证. ** □

推论 2.6.4. 设 p-群作用在有限集合 X 上,$|X| = n$. 若 t 为 X 中不动元素的个数, 则

$$t \equiv n \mod p.$$

证. ** □

推论 2.6.5. p-群有非平凡的中心.

证. ** □

定义 2.6.13 (共轭类)**.** *当群 G 在集合 G 上的作用是共轭变换 (例2.6.2) 时, 称轨道 O_x 为 x 所在的共轭类, 记作 $C(x)$.*

定理 2.6.2. *设群 G 作用在集合 X 上,$x, y \in X$. 若存在 $g_0 \in G$ 使得 $y = g_0 x$, 则 $H_y = g_0 H_x g_0^{-1}$.*

证. ** □

2.7 Sylow 定理

Lagrange 定理 (推论1.4.1) 指出, 有限群 G 的任意子群的阶是 $|G|$ 的因子. 反之, 对于 $|G|$ 的任意正因子 d, 是否存在一个 d 阶子群? 本节介绍的 Sylow 定理将回答这一问题.

在此之前我们需要以下引理.

引理 2.7.1. *若 $n = p^l m, (p, m) = 1, k \leqslant l, C_n^{p^k}$ 是组合数, 则*

$$p^{l-k} | C_n^{p^k}, p^{l-k+1} \nmid C_n^{p^k}.$$

证. ** □

定理 2.7.1 (Sylow 第一定理)**.** *若群 G 的阶为 $n = p^l m$, 其中 p 为素数,$(p, m) = 1, l \geqslant 1$, 则对于 $0 \leqslant k \leqslant l$,$G$ 有 p^k 阶子群. 特别地, 称 p^l 阶子群为 G 的 Sylow p-子群.*

证. 令

$$X = \left\{ A : A \subset G, |A| = p^k \right\},$$

易见 $|X| = C_n^{p^k}$. 对 $\forall A \in X$, 对 $\forall g \in G$ 定义映射

$$\begin{aligned} g : & X \to X \\ & A \mapsto gA, \end{aligned}$$

不难验证这是良定义的. 该映射给出了群 G 在集合 X 上的作用.

由注2.6.4可知

$$|X| = \sum_{i \in I} |O_{A_i}|.$$

由引理2.7.1可知

$$p^{l-k+1} \nmid C_n^{p^k} = |X|,$$

所以至少有一个轨道, 不妨设为 O_{A_j}, 满足

$$p^{l-k+1} \nmid |O_{A_j}|,$$

此即 $|O_{A_j}|$ 含有的 p 因子至多为 p^{l-k}.

对于 A_j 的稳定子群 H_{A_j}, 由轨道-稳定子定理 (定理2.6.1) 可知

$$|O_{A_j}| = [G : H_{A_j}] = \frac{|G|}{|H_{A_j}|},$$

注意到

$$\begin{aligned} &|G| \text{ 含有的 } p \text{ 因子恰好为 } p^l \\ &|O_{A_j}| \text{ 含有的 } p \text{ 因子至多为 } p^{l-k}, \end{aligned}$$

所以

$$H_{A_j} \text{ 含有的 } p \text{ 因子至少为 } p^k,$$

亦即

$$\exists q \in \mathbb{N}_+ \quad \text{s.t.} \quad |H_{A_j}| = p^k q,$$

可见

$$|H_{A_j}| \geqslant p^k. \tag{2.7.4}$$

反之, 对 $\forall g \in H_{A_j}$, 有 $g(A_j)=A_j$, 所以对 $\forall a \in A_j$, 有 $ga \in A_j$, 从而

$$H_{A_j}a=\left\{ga : g \in H_{A_j}\right\} \subset A_j,$$

于是

$$|H_{A_j}| = \left|H_{A_j}a\right| \leqslant |A_j| = p^k. \tag{2.7.5}$$

由式(2.7.4)与式(2.7.5)可知,H_{A_j} 是 G 的 p^k 阶子群. 定理得证. □

定理 2.7.2 (Sylow 第二定理)**.** *若有限群 G 的阶为 $p^l m$, 其中 p 为素数且 $(p,m)=1$, 记 P 为 G 的 Sylow p-子群. 则 G 的任意一个阶为 $p^k(k \leqslant l)$ 的子群 H 包含在一个与 P 共轭的 Sylow p-子群中.*

证. 令

$$X=\{gP : g \in G\},$$

对 $\forall h \in H$, 定义映射

$$\begin{aligned} h : X &\to X \\ gP &\mapsto hgP, \end{aligned}$$

容易验证该定义是良定义的,h 确定了群 H 在集合 X 上的作用. 由 Lagrange 定理 (推论1.4.1) 的证明过程可知

$$|G|=|X|\cdot|P|,$$

所以 $|X|=m$. 注意到有限 p-群 H 作用在集合 X 上, 并且 $(p,m)=1$, 所以由推论2.6.3可知 X 有不动元素, 不妨设其中的一个为 g_jP, 即

$$\begin{aligned} &\forall h \in H, hg_jP=g_jP \\ \Longleftrightarrow\ &\forall h \in H, g_j^{-1}hg_jP=P \\ \Longleftrightarrow\ &\forall h \in H, g_j^{-1}hg_j \in P \end{aligned}$$

$$\begin{aligned}&\iff \forall h \in H, h \in g_j P g_j^{-1}\\&\iff H \subset g_j P g_j^{-1},\end{aligned}$$

注意到 H, P 均成群, 所以 $H < g_j P g_j^{-1}$, 即 H 包含在一个与 P 共轭的 Sylow p- 子群中, 定理得证. □

推论 2.7.1. *对有限群而言, 任意两个 Sylow p- 子群都互相共轭.*

证. ** □

推论 2.7.2. *有限群 G 的 Sylow p- 子群是惟一的当且仅当 G 的 Sylow p- 子群是正规子群.*

证. G 的子群 P 是正规子群即 P 的所有共轭子群都等与 P 自身.

任取 G 的两个 Sylow p- 子群 P_0, P, 由推论2.7.1可知 P_0, P 互相共轭, 又由于 P_0, P 互相共轭可知 $P_0 = P$, 推论得证. □

定义 2.7.1 (正规化子)**.** *对群 G 的任意子群 H, 定义*

$$N(H) = \left\{g \in G : gHg^{-1} = H\right\},$$

则 $N(H) < G$ 且 $H \subset N(H)$. 称 $N(H)$ 为子群 H 的正规化子.

由定义2.7.1可立即推出 $H \lhd N(H)$.

推论 2.7.3. *若 G 是有限群,P 是 G 的 Sylow p- 子群, 则*

$$\begin{aligned}&(1) N(N(P)) = N(P)\\&(2) N(P) \text{ 不包含 } G \text{ 的另一个 Sylow } p\text{- 子群.}\end{aligned}$$

证. ** □

推论 2.7.4. *若 G 是有限群,p 是素数且 $p \Big| |G|$, 则 G 的 Sylow p- 子群的个数是 $|G|$ 的因子.*

证. ** □

定理 2.7.3 (Sylow 第三定理)**.** 若 $|G|=p^lm, p$ 是素数且 $(p,m)=1, l\geqslant 1$, 记 G 的 Sylow p- 子群的个数为 k, 则 $k\equiv 1 \mod p$.

分析. *注意到该定理的结论与推论2.6.4十分相似, 这引诱我们构造某 p-群 P, 使其作用在某 k 元集合 X 后所得不动元素的个数为 1.*

证. 令

$$X=\left\{P:P<G,|P|=p^l\right\},$$

于是 $|X|=k$.

任取 $P\in X$, 考虑 P 在 X 上的共轭作用. 对 $\forall a\in P$, 定义映射

$$\begin{aligned} a:X &\to X \\ Q &\mapsto aQa^{-1}, \end{aligned}$$

容易验证这是良定义的,a 给出了群 P 在集合 X 上的作用. 设 X_0 为 P 作用在 X 上的不动点集, 即

$$X_0=\{Q\in X:a(Q)=Q\},$$

则

$$\begin{aligned} Q\in X_0 &\iff \forall a\in P, a(Q)=Q \\ &\iff \forall a\in P, aQa^{-1}=Q \\ &\iff \forall a\in P, a\in N(Q) \\ &\iff P\subset N(Q), \end{aligned}$$

又 $Q\subset N(Q)$ 且 P,Q 都是 G 的 Sylow p- 子群, 所以由推论2.7.3可知 $P=Q$, 进而 $|X_0|=1$. 由推论2.6.4可知

$$|X_0|\equiv|X| \mod p,$$

即

$$
\begin{aligned}
& 1 \equiv k \mod p \\
\Longleftrightarrow & k \equiv 1 \mod p,
\end{aligned}
$$

定理得证. □

推论 2.7.5. *若群 G 的阶为 $p^l m$, 其中 p 是素数且 $(p,m)=1$, 则 G 的 Sylow p- 子群的个数是 m 的因子.*

证. 设 G 的 Sylow p- 子群的个数为 k.
由推论2.7.4可知 $k\Big||G|$, 由 $|G|=p^l m$,p 是素数且 $(p,m)=1$

$$k|p\text{或}k|m. \tag{2.7.6}$$

由 Sylow 第三定理 (定理2.7.3) 可知

$$k \nmid p. \tag{2.7.7}$$

由式(2.7.6)与(2.7.7)可知 $k|m$, 推论得证. □

作为本节的结束, 我们来看一个例子来说明如何利用上面的结果来解决群论的问题.

例 2.7.1. *已知有限群 G 的阶为 72, 证明 G 不是单群.*

证. 注意到

$$72 = 2^3 \cdot 3^2,$$

所以利用 Sylow 第三定理 (定理2.7.3), 可设 G 的 Sylow 3-子群的个数为

$$1+3t, t \in \mathbb{N},$$

再利用推论2.7.5可知

$$(1+3t)|2^3,$$

所以 $t=0$ 或 $t=1$.

(1) 若 $t=0$, 即 G 有惟一的 Sylow 3-子群, 设为 P, 由推论2.7.2可知

$$P \lhd G,$$

所以此时 G 有非平凡的正规子群 P, 从而不是单群.

(2) 若 $t=1$, 即 G 有 4 个 Sylow 3-子群, 设为 P_1, P_2, P_3, P_4. 考虑 G 在集合

$$X = \{P_1, P_2, P_3, P_4\}$$

上的共轭变换 (例2.6.2). 由推论2.7.1可知 G 任意两个 Sylow 3-子群都互相共轭, 所以 G 的每个元素都在 X 上诱导出一个 4 次置换, 从而诱导出同态

$$\varphi : G \to S_4,$$

由群同态基本定理 (定理1.7.2) 可知

$$G/\ker\varphi \cong \operatorname{im}\varphi,$$

所以

$$\begin{aligned} |\ker\varphi| &= \frac{|G|}{|\operatorname{im}\varphi|} \geqslant \frac{|G|}{|S_4|} = 3 \\ \Longrightarrow \ker\varphi &\neq \{e\}. \end{aligned} \tag{2.7.8}$$

由 G 的 Sylow 3-子群不惟一可知

$$\begin{aligned} &\operatorname{im}\varphi > 1 \\ \Longrightarrow &\ker\varphi \neq \{e\} \\ \Longrightarrow &\ker\varphi \neq G. \end{aligned} \tag{2.7.9}$$

由式(2.7.8)与(2.7.9)可知, 此时 $\ker\varphi$ 是 G 的非平凡的正规子群.

综上,G 不是单群. □

注 2.7.1. *在证明例2.7.1时所构造的群同态 φ 是十分重要的, 通常将其称为传递置换表示, 下面严格地给出它的定义.*

定义 2.7.2 (传递置换表示)**.** *若 H 是群 G 的子群,H 的全体左陪集构成集合*

$$P = \{a_iH : a_i \in G, i = 1, \cdots, r\},$$

则称群作用

$$\begin{aligned} g : P &\to P \\ a_iH &\mapsto ga_iH \end{aligned}$$

所诱导出的群同态

$$\varphi : G \to S_r$$

为群 G 在子群 H 上的传递置换表示.

2.8 群的直和

现在来介绍一种由已知群来构造新群的方法. 先看两个群的情形.

设 G_1, G_2 成群, 考虑集合

$$G_1 \times G_2,$$

对 $\forall G_1 \times G_2$ 中的两个元素 $(a_1, b_1), (a_2, b_2)$, 定义乘法为

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2), \tag{2.8.10}$$

其中第一个分量为作 G_1 的乘法, 第二个分量为作 G_2 的乘法.

若 e_1, e_2 分别为 G_1, G_2 中的幺元, 则可验证 $G_1 \times G_2$ 在新定义的乘法下成群, 幺元为 (e_1, e_2).

定义 2.8.1 (群的直和)**.** 已知 G_1, G_2 成群, 则将集合 $G_1 \times G_2$ 在乘法(2.8.10)下所成的群称为 G_1 与 G_2 的直和, 记作

$$G_1 \oplus G_2.$$

容易验证有以下 3 个命题成立.

命题 2.8.1. 当群 G_1, G_2 是有限群时,$G_1 \oplus G_2$ 也是有限群, 并且

$$|G_1 \times G_2| = |G_1| \cdot |G_2|.$$

$\square$

命题 2.8.2. 在 $G_1 \oplus G_2$ 中令

$$\overline{G_1} = \{a, e_2 : a \in G_1\}, \quad \text{其中 } e_2 \text{ 为 } G_2 \text{ 中的幺元}$$
$$\overline{G_2} = \{e_1, b : b \in G_2\}, \quad \text{其中 } e_1 \text{ 为 } G_1 \text{ 中的幺元},$$

则

$$\overline{G_1} \lhd G_1 \times G_2, \overline{G_2} \lhd G_1 \times G_2$$
$$\overline{G_1} \cong G_1, \overline{G_2} \cong G_2.$$

$\square$

命题 2.8.3. $G_1 \oplus G_2$ 中的每个元素都可以分解成 $\overline{G_1}$ 与 $\overline{G_2}$ 中的元素的乘积, 并且该分解是唯一的. $\square$

定义2.8.1与命题2.8.1,2.8.2,2.8.3均可以推广到多个群的情形.

经过上述讨论我们已经知道, 直和 $\bigoplus\limits_{i=1}^{s} G_i$ 的结构完全被群 G_i 的结构决定. 因此如果一个群能够分解成一些群的直和, 那么该群的研究就可以归结为另一些群 (一般比原来的群简单) 的研究. 下面将讨论在什么情况下, 一个群能够分解成一些群的直和.

定理 2.8.1. 设群 N_i 是群 G 的正规子群,$i=1,\cdots,s$, 若

(1) $G=\prod_{i=1}^{s} N_i$

(2) 对 $\forall g\in G$, 表示式 $g=\prod_{i=1}^{s} g_i$, 是唯一的, 其中 $g_i\in N_i$,

则

$$G\cong\bigoplus_{i=1}^{s} N_i.$$

证. 由表示式 $g=\prod_{i=1}^{s}$ 的唯一性可知映射

$$\varphi: G\to\prod_{i=1}^{s}$$
$$g_1g_2\cdots g_s\mapsto(g_1,g_2,\cdots,g_s)$$

是一一对应. 若能证明 φ 是同态映射, 便能得到 φ 是同构映射, 进而 $G\cong\prod_{i=1}^{s} N_s$.

注意到

$$\begin{aligned}
&\varphi \text{ 是同态映射}\\
\Longleftrightarrow\ &\forall x,y\in G,\varphi(xy)=\varphi(x)\varphi(y)\\
\Longleftrightarrow\ &\forall\prod_{i=1}^{s}x_i,\prod_{i=1}^{s}y_i\in G,\varphi\left[\left(\prod_{i=1}^{s}x_i\right)\cdot\left(\prod_{i=1}^{s}y_i\right)\right]=\varphi\left(\prod_{i=1}^{s}x_i\right)\cdot\varphi\left(\prod_{i=1}^{s}y_i\right)\\
\Longleftrightarrow\ &\forall\prod_{i=1}^{s}x_i,\prod_{i=1}^{s}y_i\in G,\varphi\left[(x_1x_2)\cdots(x_sy_1)\cdots(y_{s-1}y_s)\right]=\\
&\varphi\left(\prod_{i=1}^{s}x_i\right)\cdot\varphi\left(\prod_{i=1}^{s}y_i\right)
\end{aligned}$$

$$\begin{aligned}
&\Longleftrightarrow \forall \prod_{i=1}^{s} x_i, \prod_{i=1}^{s} y_i \in G, (x_1x_2, \cdots, x_sy_1, \cdots x_sy_s) = (x_1, \cdots x_s)(y_1, \cdots y_s) \\
&\Longleftrightarrow \forall \prod_{i=1}^{s} x_i, \prod_{i=1}^{s} y_i \in G, (x_1x_2, \cdots, x_sy_1, \cdots x_sy_s) = (x_1y_1, \cdots, x_sy_s) \\
&\Longleftrightarrow \forall \prod_{i=1}^{s} x_i, \prod_{i=1}^{s} y_i \in G, x_1x_2 \cdots x_sy_1 \cdots y_{s-1}y_s = x_1y_1 \cdots x_sy_s \\
&\Longleftrightarrow \forall g_i, g_j \in G, g_ig_j = g_jg_i, \qquad (2.8.11)
\end{aligned}$$

可见, 问题转化成了证明(2.8.11).

对 $\forall g \in N_i \cap N_j, i \neq j$, 假设 $g \neq e$, 则 g 有两种不同的表示方式

$$g = e \cdots e\underset{\substack{\uparrow \\ \text{第 } i \text{ 位}}}{g}e \cdots e = e \cdots e\underset{\substack{\uparrow \\ \text{第 } j \text{ 位}}}{g}e \cdots e$$

亦即 G 中的元素 g 有两种不同的分解方式, 这与题设条件 (2) 矛盾, 所以假设不成立, 即

$$N_i \cap N_j = \{e\}, i \neq j.$$

对 $\forall g_i \in N_i, g_j \in N_j \lhd G, i \neq j$

$$N_i\text{成群} \Longrightarrow g_i^{-1} \in N_i$$

$$g_i^{-1} \in N_i \lhd G, g_j \in N_j \lhd G \overset{\text{定义1.6.4}}{\Longrightarrow} g_jg_i^{-1}g_j^{-1} \in N_i,$$

从而

$$g_ig_jg_i^{-1}g_j^{-1} \in N_i, \qquad (2.8.12)$$

同理可证

$$g_ig_jg_i^{-1}g_j^{-1} \in N_j. \qquad (2.8.13)$$

由(2.8.12)与(2.8.13)可知

$$
\begin{aligned}
& g_i g_j g_i^{-1} g_j^{-1} \in N_i \cap N_j = \{e\} \\
\Longleftrightarrow\ & g_i g_j g_i^{-1} g_j^{-1} = e. \qquad (2.8.14)
\end{aligned}
$$

注意到当 $i = j$ 时(2.8.14)也成立, 从而 $\forall g_i, g_j \in G$

$$
\begin{aligned}
& g_i g_j g_i^{-1} g_j^{-1} = e \\
\Longleftrightarrow\ & g_i g_j = g_j g_i,
\end{aligned}
$$

可见(2.8.11)成立, 从而定理得证. □

定义 2.8.2 (内直和)**.** *若群 G 同构于其正规子群 $N_1, \cdots, N_s$ 的直和, 则称群 G 分解成正规子群 $N_1, \cdots, N_s$ 的直和, 也称 G 等于 $N_1, \cdots, N_s$ 的内直和.*

命题 2.8.4. *与线性空间分解成子空间的直和的情况类似, 不难证明定理2.8.1的条件 (2) 有以下两种等价描述*

(2') 幺元的表示方式唯一, 即

$$
\text{若 } e = \prod_{i=1}^{s} x_i, \text{ 则 } x_i = e
$$

(2")

$$
N_j \bigcap \prod_{i=1, i \neq j}^{s} N_i = \{e\}.
$$

定义 2.8.3 (不可分解的)**.** *若群 G 不能被分解成两个非平凡的正规子群的直和, 则称 G 是不可分解的.*

事实上, 任意一个有限群总能分解成一些不可分解的群的直和. 群的直和是群论中的重要问题, 这里不再细说.

下面给出一个例子, 来看看有限交换群的分解.

例 2.8.1. 有限交换群能被分解成 p-群的直和.

证. 设 G 是有限交换群,$|G| = n$ 的标准分解式为

$$n = \prod_{i=1}^{r} p_i^{r_s},$$

其中 p_i 是不同的素数,$r_i > 0$.

由 Sylow 第一定理 (定理2.7.1) 可知 G 存在 Sylow p_i-子群, 记为 G_i. 注意到 G 是交换群, 所以 G_i 是正规的, 从而由推论2.7.2可知 G_i 是 G 的惟一一个 Sylow p_i 子群, 结合2.7.1不难看出 G_i 恰由 G 中所有阶为 p_i 的幂的元素组成.

令 $H = \prod_{i=1}^{s} G_i$, 由

G_i 中的元素的阶为 p_i 的方幂

子群 $\prod_{i=1, i\neq j}^{s} G_i$ 元素的阶为 $\prod_{i=1, i\neq j}^{s} p_i^{r_i}$ 的因子 (引理2.2.1),

可知

$$G_j \cap \prod_{i=1, i\neq j}^{s} G_i = \{e\},$$

结合定理2.8.1与命题2.8.4可得

$$H \cong \bigoplus_{i=1}^{s} G_i.$$

由上述讨论可知

$$H < G$$
$$|H| = |G|,$$

所以 $H = G$, 进而

$$G \cong \bigoplus_{i=1}^{s} G_i,$$

问题得证. □

注 2.8.1. *有时交换 p-群还能被分解. 以后将证明 p-群不能被分解的充要条件为它是循环群.*

2.9 Jordan-Hölder定理

本节将指出, 递降子群列也是刻画一般有限群结构的重要工具.

定义 2.9.1 (次正规子群列, 因子群组, 合成群列, 长度)**.** *若群 G 的递降子群列*

$$G = G_0 > G_1 > \cdots > G_r = \{e\} \tag{2.9.15}$$

满足 $G_{i-1} \rhd G_i$, 则称(2.9.15)为 G 的次正规子群列.

称(2.9.15)的商群组

$$G_0/G_1, G_1/G_2, \cdots, G_{r-1}/G_r \tag{2.9.16}$$

为(2.9.15)的因子群组.

若(2.9.15)的因子群组(2.9.16)都是单群, 则称(2.9.15)为合成群列.

在(2.9.15)中可能有重复项出现, 即在(2.9.16)中可能有单位群 $\{e\}$ 出现. 称(2.9.16)中非单位群的因子群的个数为(2.9.15)的长度.

注 2.9.1. *由于 $G_{i-1} \rhd G_i \nRightarrow G_{i-1} \rhd G$, 所以叫'次'正规.*

群的次正规子群列不惟一, 群的递降子群列的长度惟一.

命题 2.9.1. *有限群有合成群列.*

证. ** □

在上述证明过程中可知, 只要某一因子群 G_i/G_{i+1} 不是单群, 则可在 G_i 与 G_{i+1} 之间插入一个子群 H 使次正规子群列的长度增加. 亦即合成群列是不能再插入任何一项的次正规子群列.

无限群而言不一定有合成群列, 如整数加法群. 为了确保无限群存在合成群列, 必须添加适当的条件, 本书不作讨论.

在2.4节中已经得到以下两条结论

1) 每个有限可解群 G 有一个合成群列

$$G = G_0 \triangleright G_1 \cdots \triangleright G_r = \{e\},$$

使得每个因子群 G_i/G_{i+1} 都是素数阶循环群. 反之也成立.

2) 有限可解群 G 的任一合成群列 (无重复项)$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = \{e\}$ 的因子群组

$$G_0/G_1, G_1/G_2, \cdots, G_r{-}1/G_r$$

不及次序地由 G 惟一决定, 与合成群列的选取无关.

第一条是有限可解群的特性, 用它可以判别一个有限群是不是可解的. 第二条则不是有限群的特性, 它是一般有限群类的共性, 这表现在下述定理中

定理 2.9.1 (Jordan-Hölder定理). *有限群的无重复项的合成群列有相同的长度, 并且它们的因子群组在同构意义下不计次序地一一相等.*

证. ** □

Jordan-Hölder定理 (定理2.9.1) 指出, 给定的有限群的全体合成群列的因子群组是相同的, 由一组非平凡的单群构成, 因此也称其为该有限群的因子群组. 反之, 任给一组有限单群

$$S = \{S_1, \cdots, S_r\},$$

以 S 为因子群组的有限群有多少种不同构的类型? 一般来说, 它可以归结为以下问题

问题. *对任意群 H, N, 试构造出所有不同构的群 G_i 使得*

$$\begin{aligned} N &\lhd G_i \\ G_i/H &\cong H. \end{aligned}$$

这就是所谓的群扩张问题. 群扩张是群论中的重要理论, 这里不作讨论.

2.10 幺半群

****

2.11 CHAPTER2 习题

问题 2.1 (P97T1)**.** *已知 G 是有限群,$N \lhd G$,$(|N|, [G:N]) = 1$. 证明: 若元素 a 的阶整除 $|N|$, 则 $a \in N$.*

证. 考虑自然同态

$$\begin{aligned} \pi : G \to& G/N \\ g \mapsto& gN, \end{aligned}$$

于是

$$\begin{aligned} [\pi(a)]^{o(a)} =& (aN)^{o(a)} \\ \xlongequal{N \lhd G}& a^{o(a)} N^{o(a)} \\ =& N, \end{aligned}$$

又 N 是 G/N 的幺元, 所以

$$|\pi(a)| \,\Big|\, |o(a)| \,\Big|\, |N| \,. \tag{2.11.17}$$

注意到

$$aN \in G/N,$$

所以

$$|aN| \,\Big|\, [G:N],$$

即

$$|\pi(a)| \,\Big|\, [G:N]. \tag{2.11.18}$$

由式(2.11.17)与(2.11.18)结合 $(|N|, [G:N]) = 1$ 可知

$$\begin{aligned} & |\pi(a)| = 1 \\ \Longrightarrow & \pi(a) = N \\ \Longrightarrow & aN = N \\ \Longrightarrow & a \in N, \end{aligned}$$

问题得证. □

问题 2.2 (P97T2)**.** 设 c 是群 G 中阶为 rs 的元素, 其中 $(r,s)=1$. 证明 c 可以表示成 $c=ab$, 其中 a 的阶为 r, b 的阶为 s, 且 a,b 都是 c 的方幂.

证. 由 $(r,s)=1$ 可知

$$\exists u, v \in \mathbb{Z} \ \text{ s.t. } \ ur + vs = 1,$$

不难验证

$$\begin{aligned} a &= c^{vs} \\ b &= c^{ur} \end{aligned}$$

满足题设要求. □

问题 2.3 (P97T3)**.** 已知群 G 中元素 a 的阶与正整数 k 互素, 证明方程 $x^k = a$ 在 $< a >$ 内恰有一解.

证. 由 $(o(a), k) = 1$ 可知

$$\exists u, v \in \mathbb{Z} \ \text{ s.t. } \ uo(a) + vk = 1,$$

所以

$$a^{uo(a)+vk} = a,$$

即

$$a^{vk} = a,$$

由此可见 $x = a^v$ 是 $x^k = a$ 在 $< a >$ 内的解.

现设 $x = a_0^v$ 也是 $x^k = a$ 在 $< a >$ 内的解, 其中 $0 \leqslant v - v_0 \leqslant o(a) - 1$, 于是

$$a^{vk} = a$$
$$a^{v_0 k} = a,$$

即

$$vk \equiv 1 \mod o(a)$$
$$v_0 k \equiv 1 \mod o(a),$$

所以

$$o(a) | (v - v_0)k,$$

由此可见 $v - v_0 = 0$ 即 $v = v_0$.

综上, 问题证毕. □

问题 2.4 (P97T4)**.** 证明在群中,ab 与 ba 有相同的阶.

证. 注意到 $ab = b^{-1} \cdot ba \cdot b$, 所以

$$\begin{aligned} & ab = e \\ \Longleftrightarrow\ & b^{-1} \cdot ba \cdot b = e \\ \Longleftrightarrow\ & ba = e, \end{aligned}$$

可见问题得证. □

问题 2.5 (P97T10). 证明 S_n 中的任意一个置换能由 $n-1$ 个对换 $(12), (13), \cdots, (1n)$ 生成, 也能由 $n-1$ 个对换 $(12), (23), \cdots, (n-1\ n)$ 生成.

证. 由引理2.3.1可知 S_n 中的任意一个置换都可以拆成若干个对换 (ij) 的复合, 注意到

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

所以任意一个置换都能由 $(n-1)$ 个对换

$$(12), (13), \cdots, (1n)$$

生成, 第一个论断证毕.

注意到

$$(1i)(i\ i+1)(1i) = (1\ i+1),$$

故可用归纳法证明

$$(12), (23), \cdots, (n-1\ n)$$

能生成

$$(12)(13), \cdots, (1n),$$

再结合第一个论断可知它能生成 S_n 中的任意一个置换, 第二个论断证毕. □

问题 2.6 (P97T16). 设 H_1, H_2 是群 G 的两个子群, 证明 $H_1 \cap H_2$ 的任一左陪集是 H_1 的一个左陪集与 H_2 的一个左陪集的交.

证. 若能证明对 $\forall g \in G$ 都有 $g(H_1 \cap H_2) = gH_1 \cap gH_2$, 则问题得证. 证明思路为两者互相包含.

(1) 对 $\forall$ 给定的 $g \in G$, 在 $g(H_1 \cap H_2)$ 中任取 gh_0, 有

$$
\begin{aligned}
& h_0 \in H_1 \cap H_2 \\
\Longrightarrow & gh_0 \in gH_1, gh_0 \in gH_2 \\
\Longrightarrow & gh_0 \in gH_1 \cap gH_2 \\
\Longrightarrow & g(H_1 \cap H_2) \subset gH_1 \cap gH_2.
\end{aligned}
$$

(2) 反之, 对任意给定的 $g \in G$, 在 $gH_1 \cap gH_2$ 中任取 gh_0, 有

$$
\begin{aligned}
& gh_0 \in gH_1, gh_0 \in gH_2 \\
\stackrel{g\text{的任意性}}{\Longrightarrow} & h_0 \in H_1, h_0 \in H_2 \\
\Longrightarrow & h_0 \in H_1 \cap H_2 \\
\Longrightarrow & gh_0 \in g(H_1 \cap H_2) \\
\Longrightarrow & gH_1 \cap gH_2 \subset g(H_1 \cap H_2).
\end{aligned}
$$

由 (1),(2) 便知 $g(H_1 \cap H_2) = gH_1 \cap gH_2$, 综上, 问题得证. □

问题 2.7 (P98T18). 设 G 为有限群,$H < G$ 且 $[G : H] = n > 1$. 证明 G 或者含有指数能整除 $n!$ 的非平凡正规子群, 或者 G 同构于 S_n 的一个子群.

证. 设群 G 在子群 H 上的传递置换表示 (定义2.7.2) 为

$$\varphi : G \to S_n.$$

由 $[G : H] > 1$ 可知

$$\operatorname{im} \varphi > 1$$

$$\begin{aligned} &\Longrightarrow \operatorname{im}\varphi \neq \{e\} \\ &\Longrightarrow \ker\varphi \neq G. \end{aligned} \tag{2.11.19}$$

(1) 若 $\ker\varphi \neq \{e\}$, 结合(2.11.19)可知

$$\ker\varphi \text{ 是 } G \text{ 的非平凡正规子群.} \tag{2.11.20}$$

注意到

$$|\ker\varphi| \Big| [G:H] \xlongequal{\text{群同态基本定理 (定理1.7.2)}} |\operatorname{im}\varphi| \Big| |S_n| = n!, \tag{2.11.21}$$

所以由(2.11.20)与(2.11.21)可知 $\ker\varphi$ 是 G 的指数能够整除 $n!$ 的非平凡的正规子群.

(2) 若 $\ker\varphi = \{e\}$, 则

$$\begin{aligned} &G/\ker\varphi \cong \operatorname{im}\varphi \\ \Longleftrightarrow\ &G \cong \operatorname{im}\varphi < S_n, \end{aligned}$$

即 G 同构于 S_n 的子群 $\operatorname{im}\varphi$.

由 (1),(2) 便知问题证毕. □

问题 2.8 (P98T19). *设 G 为有限群,p 是 $|G|$ 的最小素因子. 证明指数 (定义1.4.4) 为 p 的子群 (若存在) 必正规.*

证. 设 H 是群 G 的指数为 p 的子群, 即 $[G:H]=p$,φ 是 G 在 H 上的传递置换表示 (定义2.7.2).

(1) 若 $\ker\varphi = \{e\}$, 则由群同态基本定理 (定理1.7.2) 可知

$$\begin{aligned} &G/\ker\varphi \cong \operatorname{im}\varphi \\ \Longleftrightarrow\ &G \cong \operatorname{im}\varphi < S_p, \end{aligned}$$

于是

$$|G| = |\operatorname{im}\varphi| \Big| |S_p| = p!,$$

结合 p 是 $|G|$ 的最小素因子便知 $|G|=p$, 于是

$$\begin{aligned}
&|H|=\frac{|G|}{[G:H]}=\frac{p}{p}=1\\
\iff &H=\{e\}\\
\implies &H\text{是 } G \text{ 的正规子群.}
\end{aligned}$$

(2) 若 $\ker\varphi\neq\{e\}$, 则

$$\begin{aligned}
&g\in\ker\varphi\\
\iff &\forall a_i\in G, ga_iH=a_iH\\
\xRightarrow{\text{当 } a_i=e \text{ 时}} &gH=H\\
\iff &g\in H,
\end{aligned}$$

由此可见 $\ker\varphi\subset H$, 从而 $\ker\varphi\lhd H$. 注意到

$$\begin{aligned}
&[G:\ker\varphi]=|\operatorname{im}\varphi|\Big||S_p|=p!\\
\xRightarrow{p \text{ 是 } |G| \text{ 的最小素因子}} &[G:\ker\varphi]=p\\
\xRightarrow{\ker\varphi\lhd H,[G:H]=p} &H=\ker\varphi \text{ 是 } G \text{ 的指数为 } p \text{ 的正规子群.}
\end{aligned}$$

由 (1),(2) 可知问题证毕. □

问题 2.9 (P98T21)**.** *证明任一非交换的 6 阶群同构于 S_3.*

证. ** □

问题 2.10 (P98T29)**.** *设 G 为有限群,A,B 是 G 的两个非空子集. 若 $|A|+|B|>|G|$, 则 $AB=G$.*

证. ** □

问题 2.11 (P98T33)**.** *设 G 是有限群,$N\lhd G,P$ 为 N 的一个 Sylow 子群,T 为 P 在 G 中的正规化子. 证明 $G=NT$.*

证. *** □

问题 2.12 (P98T35)**.** 设 G 为有限群,$H < G, P$ 是 G 的 Sylow p- 子群,$N \lhd G$. 证明 $P \cap N$ 是 N 的一个 Sylow p- 子群, 同时 PN/N 是 G/N 的一个 Sylow p- 子群.

证. *** □