0.1 子群与商群

定义 0.1

设 A, B 是群 G 的两个子集, 约定

$$AB = \{ab|a \in A, b \in B\}, A^{-1} = \{a^{-1}|a \in A\}.$$

特别地, 当 $A = \{a\}$ 为单点集时, 记 $AB = aB, BA = Ba$. 当然这些符号对半群与幺半群可同样使用.

定义 0.2

群 G 的非空子集 H 若对 G 的运算也构成一个群, 则称为 G 的**子群**, 记作 $H < G$.

注 显然, $H = \{1\}$(1 为 G 的幺元) 与 $H = G$ 均为 G 的子群, 称为 G 的**平凡子群**, 其他的子群称为**非平凡子群**.

定理 0.1

设 H 是群 G 的非空子集, 则下列条件等价:

(1) H 是 G 的子群;

(2) $1 \in H$; $a \in H$, 则 $a^{-1} \in H$; $a, b \in H$, 则 $ab \in H$;

(3) $a, b \in H$, 则 $ab \in H, a^{-1} \in H$;

(4) $a, b \in H$, 则 $ab^{-1} \in H$.

证明 (1) $\Rightarrow$ (2). 由 H 对 G 的乘法构成群知 $a, b \in H$, 则 $ab \in H$. 又 H 有幺元 $1'$, 即有 $1' \cdot 1' = 1'$. 设 $1'$ 在 G 中的逆元为 $1'^{-1}$, 则有

$$1 = 1' \cdot 1'^{-1} = (1' \cdot 1') \cdot 1'^{-1} = 1',$$

故 $1 \in H$. 设 a 在 H 中的逆元为 a', 于是 $aa' = 1' = 1$, 即 $a' = a^{-1}$, 故 $a^{-1} \in H$. 由此知 (2) 成立, 而且 H 的幺元是 G 的幺元. $a \in H$, a 在 H 中的逆元与在 G 中的逆元一致.

(2) $\Rightarrow$ (3). 这是显然的.

(3) $\Rightarrow$ (4). 若 $a, b \in H$, 故 $a, b^{-1} \in H$, 故 $ab^{-1} \in H$.

(4) $\Rightarrow$ (1). 由 $H \neq \varnothing$ 知 $\exists a \in H$, 因而 $1 = aa^{-1} \in H$. 又由 $1, a \in H$ 知 $a^{-1} = 1 \cdot a^{-1} \in H$. 又若 $a, b \in H$, 由 $b^{-1} \in H$ 得 $ab = a(b^{-1})^{-1} \in H$. 由此可知 G 的乘法也是 H 的乘法. 对 H 而言有幺元 1; 对 $a \in H$ 有逆元 a^{-1}; 结合律显然成立. 故 H 是 G 的子群. □

推论 0.1

设 H 是群 G 的非空子集, 则下列条件等价:

(1) H 是 G 的子群;

(2) $HH = H, H^{-1} = H$;

(3) $H^{-1}H = H$.

证明

□

推论 0.2

1. 若 H_1, H_2 是群 G 的子群, 则 $H_1 \cap H_2$ 也是 G 的子群.
2. 若 G 是一个群, 则 G 的任意子群的交 $\bigcap\limits_{H<G} H$ 也是 G 的子群.

证明

□

例题 0.1

1. 设 V 是数域 $\mathbf{P}$ 上的 n 维线性空间.S_V 为 V 上的全变换群, $GL(V)$ 表示 V 上所有可逆线性变换的集合, 则 $GL(V)$ 为 S_V 的子群, 称为线性空间 V 的**一般线性群**.
   又设 $SL(V)$ 为 V 上所有行列式等于 1 的线性变换的集合, 则 $SL(V)$ 是 $GL(V)$(同时也是 S_V) 的子群, 称为**特殊线性群**.
2. 设 V 是 n 维 Euclid 空间. 以 $O(V)$ 表示 V 上所有正交变换的集合, $SO(V)$ 表示所有行列式等于 1 的正交变换的集合, 则 $O(V)$ 是 $GL(V)$ 的子群, $SO(V)$ 是 $O(V)$ 的子群. $O(V)$ 称为 V 的**正交变换群**, 简称**正交群**, $SO(V)$ 称为**转动群** (或**特殊正交变换群**、**特殊正交群**).

注 将上述 S_V 换成数域 $\mathbf{P}$ 上的全体方阵构成的乘法群, 线性变换换成方阵, 结论也成立.

证明

□

例题 0.2 设 $m \in \mathbf{Z}$, 则 $m\mathbf{Z} = \{mx|x \in \mathbf{Z}\}$ 是整数加法群 $\mathbf{Z}$ 的子群. 并且 $\mathbf{Z}$ 的任何子群都是这样的子群.

证明

□

例题 0.3 先考虑 n 个不定元 $x_1, x_2, \cdots, x_n$ 的多项式

$$A = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) \in \mathbf{C}[x_1, x_2, \cdots, x_n].$$

对于 $\sigma \in S_n$, 令

$$A_\sigma = \prod_{1 \leqslant i < j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)}),$$

则 $A_\sigma = \pm A$. 若 $A_\sigma = A$, 则称 σ 为**偶置换**, 并记 $\mathrm{sgn}\sigma = 1$; 若 $A_\sigma = -A$, 则称 σ 为**奇置换**, 并记 $\mathrm{sgn}\sigma = -1$, $\mathrm{sgn}\sigma$ 称为 σ 的**符号**. 故有

$$A_\sigma = \mathrm{sgn}\sigma A.$$

令 A_n 为 S_n 中偶置换集合, 即

$$A_n = \{\sigma \in S_n | \mathrm{sgn}\sigma = 1\},$$

则 A_n 为 S_n 的子群.A_n 称为 n 个文字的**交错群**.

证明 先证明 $A_\sigma = \pm A$. 注意到 A 中没有 $x_i - x_j$ 的重因式, 因而只需说明 A_σ 中没有重因式即可. 设有 $\{\sigma(i), \sigma(j)\} = \{\sigma(k), \sigma(l)\}$, 则有如下两种可能:

(1) $\sigma(i) = \sigma(k), \sigma(j) = \sigma(l)$, 则有 $i = k, j = l$;

(2) $\sigma(i) = \sigma(l), \sigma(j) = \sigma(k)$, 则有 $i = l, j = k$,

因而都有 $\{i, j\} = \{k, l\}$, 由此知 $A_\sigma = \pm A$.

事实上, 若 $\tau, \sigma \in S_n$, 则有

$$A_{\sigma\tau} = \prod_{1 \leqslant i < j \leqslant n} (x_{\sigma\tau(i)} - x_{\sigma\tau(j)}).$$

将 $A_{\sigma\tau}$ 与 A_σ 进行比较. 若 $\tau(i) < \tau(j)$, 则 $x_{\sigma\tau(i)} - x_{\sigma\tau(j)}$ 仍是 A_σ 中一个因子; 若 $\tau(i) > \tau(j)$, 则 $x_{\sigma\tau(j)} - x_{\sigma\tau(i)} = -(x_{\sigma\tau(i)} - x_{\sigma\tau(j)})$ 为 A_σ 中一因子, 因而将 A_σ 变成 $A_{\sigma\tau}$ 时改变因子符号的次数与将 A 变成 A_τ 时改变因子符号的次数相同, 因而有

$$A_{\sigma\tau} = \mathrm{sgn}\tau \cdot \prod_{1 \leqslant i < j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)}) = \mathrm{sgn}\sigma\mathrm{sgn}\tau A.$$

于是

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}\sigma\mathrm{sgn}\tau, \quad \forall \sigma, \tau \in S_n.$$

又注意到 $\mathrm{sgn}\tau^{-1} = \mathrm{sgn}\tau, \forall \tau \in S_n$, 故

$$\mathrm{sgn}(\sigma\tau^{-1}) = \mathrm{sgn}\sigma\mathrm{sgn}\tau^{-1} = \mathrm{sgn}\sigma\mathrm{sgn}\tau = 1 \Longrightarrow \sigma\tau^{-1} \in A_n, \quad \forall \sigma, \tau \in A_n.$$

由此知 A_n 为 S_n 的子群. □

定义 0.3

设 H 是群 G 的子群, 又 $a \in G$. 集合 aH 与 Ha 分别称为以 a 为代表的 H 的**左陪集**与**右陪集**. ♣

定理 0.2

设 H 是群 G 的子群, 则由

$$aRb, \text{ 若 } a^{-1}b \in H$$

所确定的 G 中的关系 R 是一个等价关系, 并且 a 所在的等价类为 $aH : a \in G$, 故 H 的左陪集族 $\{aH : a \in G\}$(集合无相同元素) 是 G 的一个分划. ♡

证明 由 $a^{-1}a \in H$ 知 $aRa(\forall a \in G)$. 又设 aRb, 即 $a^{-1}b \in H$, 故 $(a^{-1}b)^{-1} = b^{-1}a \in H$, 即 bRa. 再设 aRb, cRb, 即 $a^{-1}b, b^{-1}c \in H$, 故 $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, 即 aRc. 这样知 R 是等价关系. 又由 $b = a(a^{-1}b)$ 知

$$aRb \iff a^{-1}b \in H \iff b \in aH,$$

故 a 所在的等价类为 aH. 由定理**??**知 $\{aH : a \in G\}$ 为 G 的一个分划. □

推论 0.3

设 H 是群 G 的子群, 则下列条件等价:

(1) $aH \cap bH \neq \varnothing$;

(2) $aH = bH$;

(3) $a^{-1}b \in H$,

而且 $G = \bigcup\limits_{a \in G} aH$ 为不相交的并. ♡

证明

□

定义 0.4

设 H 是群 G 的子群, 由定理 0.2定义 G 中的等价关系 R 为

$$aRb, \text{ 若 } a^{-1}b \in H.$$

将 G 对等价关系 R 的商集合, 即以左陪集 aH, $a \in G$ 为元素的集合记为 $G/H = \{aH : a \in G\}$, 称为 G 对 H 的**左陪集空间**. G/H 中元素个数 $|G/H|$ 称为 H 在 G 中的**指数**, 记为 $[G : H]$. 相应可定义**右陪集空间**. ♣

注 $\{1\}$ 作为 G 的子群, 在 G 中指数显然为 $|G|$. 故也记 $|G| = [G : 1]$.

例题 0.4 设 V 是数域 $\mathbf{P}$ 上的 n 维线性空间, $GL(V)$ 有子群 $SL(V)$. 在 V 中取定一组基, 任何一个线性变换由它在这组基下的矩阵完全确定, 可把它们等同起来.$\forall \lambda \in \mathbf{P}, \lambda \neq 0$, 令 $D(\lambda) = \mathrm{diag}(\lambda, 1, \cdots, 1)$, 于是 $D(\lambda) \in GL(V)$, 对于 $A \in GL(V)$ 有

$$ASL(V) = D(\lambda)SL(V) \iff \det A = \lambda.$$

于是

$$GL(V) = \bigcup_{\lambda \neq 0} D(\lambda)SL(V),$$

因而

$$[GL(V) : SL(V)] = +\infty.$$

证明

□

例题 0.5 设 V 是 n 维 Euclid 空间. 由 $A\in O(V)$ 有 $\det A=\pm1$, 令 $D(\lambda)=\mathrm{diag}(\lambda,1,\cdots,1)$, 于是

$$O(V)=SO(V)\bigcup D(-1)SO(V),\quad [O(V):SO(V)]=2.$$

证明

□

例题 0.6 设 $m>0, m\mathbf{Z}$ 为 $\mathbf{Z}$ 的子群, 则有

$$\mathbf{Z}=\bigcup_{k=0}^{m-1}(k+m\mathbf{Z}),\quad [\mathbf{Z}:m\mathbf{Z}]=m.$$

证明

□

例题 0.7 设 σ 是 S_n 中任一奇置换, 则有 $S_n=A_n\cup\sigma A_n$, 故 $[S_n:A_n]=2$.

证明

□

定理 0.3 (Lagrange 定理)

设 H 是有限群 G 的子群, 则有

$$[G:1]=[G:H][H:1] \tag{1}$$

因而子群 H 的阶是群 G 的阶的因子.

注 这个结论对无限群 G 也正确, 此时等式两边都是 $+\infty$.

证明 设 $a\in G$. 显然, 映射 $h\to ah$ 是 H 到 aH 上的一一对应, 因而 $|aH|=|H|=[H:1]$. 又由推论 0.3知 $G=\bigcup\limits_{a\in G}aH$ 为不相交的并, $\{aH\}$ 的不同左陪集个数为 $[G:H]$, 故式 (1) 成立. □

推论 0.4

有限群 G 的任一元素 a 的阶是 G 的阶的因子.

证明 令 $\langle a\rangle=\{a^n|n\in\mathbf{Z}\}$, 容易验证这是 G 的一个子群. 又由于 G 有限, 故 $\langle a\rangle$ 有限, 因而 a 是有限阶的, 设为 d. 对 $n\in\mathbf{Z}$ 有 t_n 与 r_n $(0\leqslant r_n<d)$, 使 $n=t_nd+r_n$, 于是 $a^n=a^{r_n}$. 因此 $\langle a\rangle$ 中至多只有 d 个元素 $1,a,\cdots,a^{d-1}$.

又对 $\forall r_1,r_2\in\mathbf{N}$, 且 $r_1\neq r_2, 0\leqslant r_1,r_2<d$, 则 $|r_1-r_2|<d$, 从而 $a^{r_1-r_2}\neq1$, 进而 $a^{r_1}\neq a^{r_2}$. 故 $1,a,\cdots,a^{d-1}$ 互不相同. 由此知 $\langle a\rangle=\{1,a,\cdots,a^{d-1}\}$, 即 $\langle a\rangle$ 是 d 阶群. 故由Lagrange 定理知 d 为 $[G:1]$ 的因子. □

定义 0.5 (循环群)

我们称

$$\langle a\rangle=\{a^n|n\in\mathbf{Z}\}$$

是由 a 生成的 G 的子群, 如果在一个群 G 中存在一个元素 a, 使得 $G=\langle a\rangle$, 即 G 由 a 生成, 则称 G 是**循环群**, a 为 G 的一个**生成元**.

定理 0.4

设 H 是群 G 的子群, 则 G 中由

$$aRb,\ \text{当}\ a^{-1}b\in H$$

所定义的关系 R 为同余关系的充分必要条件是

$$ghg^{-1}\in H,\quad \forall g\in G,h\in H.$$

此时称 H 为 G 的**正规子群**, 记为 $H \lhd G$. 同时, 商集合 G/H 对同余关系 R 导出的运算

$$aH \cdot bH = abH, \quad \forall a, b \in G$$

也构成一个群, 称为 G 对 H 的**商群**. 商群 G/H 的幺元为 $1 \cdot H = H$.

证明 设 R 为同余关系. 又 $g \in G, h \in H$, 于是有

$$gRgh, \quad g^{-1}Rg^{-1},$$

因而 $gg^{-1}R(ghg^{-1})$, 即 $1Rghg^{-1}$, 亦即 $ghg^{-1} \in H$.

反之, 设 $\forall g \in G, h \in H$ 有 $ghg^{-1} \in H$. 设 aRb, cRd, 则 $a^{-1}b, c^{-1}d \in H$, 即 $\exists h_1, h_2 \in H$, 使 $b = ah_1, d = ch_2$, 从而 $c^{-1} = h_2 d^{-1}$. 因而 $(ac)^{-1}(bd) = c^{-1}a^{-1}ah_1 d = h_2\left(d^{-1}h_1 d\right) \in H$, 则有 $(ac)R(bd)$, 即 R 为同余关系.

设 R 为同余关系. 因 a 所在等价类为 aH, 由定理**??** 知 G/H 中的乘法为

$$aH \cdot bH = abH, \quad \forall a, b \in G. \tag{2}$$

显然有 $(aH \cdot bH)cH = abcH = aH(bH \cdot cH)$, $1H \cdot aH = aH$, $a^{-1}H \cdot aH = 1 \cdot H$, 故 G/H 为群. □

推论 0.5

若 G 为有限群, $H \lhd G$, 商群 G/H 的阶 $[G/H : H] = [G : H] = \dfrac{[G:1]}{[H:1]}$.

证明 这是Lagrange 定理的直接推论. 当 G 为无限群时, $[G/H : H] = [G : H]$ 仍然成立. □

定理 0.5

设 H 是群 G 的子群, 则下列条件等价:

(1) $H \lhd G$;

(2) $gHg^{-1} = H, \forall g \in G$;

(3) $gH = Hg, \forall g \in G$;

(4) $g_1Hg_2H = g_1g_2H, \forall g_1, g_2 \in G$.

证明 (1) $\Rightarrow$ (2). $g \in G, h \in H$, 则由 $H \lhd G$ 有 $ghg^{-1} \in H$, 又 $h = g(g^{-1}hg)g^{-1} \in gHg^{-1}$, 故有 $gHg^{-1} = H$.

(2) $\Rightarrow$ (3). $\forall g \in G, h \in H$ 有 $gh = ghg^{-1}g \in Hg$, $hg = gg^{-1}hg \in gH$, 故 $gH = Hg$.

(3) $\Rightarrow$ (4). 设 $g_1, g_2 \in G, h_1, h_2, h \in H$. 由条件 (3) 成立知 $\exists h_1', h' \in H$, 使 $h_1g_2 = g_2h_1'$, $g_2h = h'g_2$. 于是 $g_1h_1g_2h_2 = g_1g_2h_1'h_2 \in g_1g_2H$, $g_1g_2h = g_1h'g_2 \cdot 1 \in g_1H \cdot g_2H$, 故 $g_1H \cdot g_2H = g_1g_2H$.

(4) $\Rightarrow$ (1). 设 $g \in G, h \in H$, 故有 $ghg^{-1} \in gHg^{-1}H = gg^{-1}H = H$, 则 $H \lhd G$. □

命题 0.1

Abel 群 G 的任一子群 H 都是正规子群, 商群 G/H 也是 Abel 群.

证明

□

例题 0.8 为方便计, 将商群 G/H 中元素记为 $\bar{g} = gH$, 则

(1) $SL(V) \lhd GL(V)$, $GL(V)/SL(V) = \{\overline{D(\lambda)} | \lambda \neq 0\}$ 且 $\overline{D(\lambda)D(\mu)} = \overline{D(\lambda\mu)}$;

(2) $SO(V) \lhd O(V)$, $O(V)/SO(V) = \{\overline{D(1)}, \overline{D(-1)}\}$;

(3) $m\mathbf{Z} \lhd \mathbf{Z}$, $\mathbf{Z}/m\mathbf{Z} = \mathbf{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$;

(4) $A_n \lhd S_n$, $S_n/A_n = \{\bar{1}, \bar{\sigma} | \sigma$ 奇置换$\}$ 且

$$\bar{1} \cdot \bar{\sigma} = \bar{\sigma} \cdot \bar{1} = \bar{\sigma}, \quad \bar{\sigma} \cdot \bar{\sigma} = \bar{1} \cdot \bar{1} = \bar{1}.$$

定义 0.6

若半群 S 的非空子集 S_1 对 S 的运算也是半群, 则称 S_1 为 S 的**子半群**.

若幺半群 M 的子集 Q 对 M 的运算也是幺半群且 M 的幺元 $1 \in Q$, 则称 Q 为 M 的**子幺半群**.

如果关系 $\sim$ 是幺半群 (或半群) 中的同余关系, 那么商集合对导出的运算也是幺半群 (或半群), 称之为**商幺半群** (或**商半群**).

♣