1 运算及其性质

【定义1.1】（运算）对于集合 A，称函数 $f: A^n \to A$ 为集合 A 上的一个 n 元运算。

【定义1.2】（函数封闭）对于函数 $f: A^n \to B$，如果 $B \subseteq A$，称 f 在 A 上封闭。

运算的表示：①算符，包括 $*, \cdot, \star, \oplus, \otimes, \circ$ 等等；②运算表，表示**有穷集**上的一元和二元运算。

运算的性质

【定义1.3】（交换律）已知 $\langle A, * \rangle$，若 $\forall x, y \in A$，有 $x * y = y * x$，称 $*$ 在 A 上可交换。

【定义1.4】（结合律）已知 $\langle A, * \rangle$，若 $\forall x, y, z \in A$，有 $x * (y * z) = (x * y) * z$，称 $*$ 在 A 上可结合。

【结论】（广义结合律）对于可结合的二元运算 $*$，有

$$a_1 * a_2 * \ldots * a_n = (a_1 * a_2 * \ldots * a_i) * (a_{i+1} * a_{i+2} * \ldots * a_j) * (a_{j+1} * a_{j+2} * \ldots * a_n)$$

即只要元素相对顺序不变，可以随意添加括号。

进一步地，若 $*$ 含具有可交换性，那么可以随意交换位置。

【定义1.5】（幂等律）已知 $\langle A, * \rangle$，若 $\forall x \in A$，有 $x * x = x$，则称 $*$ 在 A 上满足幂等律。

【定义1.6】（分配律）已知 $\langle A, *, \oplus \rangle$，若 $\forall x, y, z \in A$，有 $x * (y \oplus z) = (x * y) \oplus (x * z)$（左分配律）和 $(y \oplus z) * x = (y * x) \oplus (z * x)$（右分配律），则称运算 $*$ 对于运算 $\oplus$ 是可分配的。

【定义1.7】（吸收律）已知 $\langle A, *, \oplus \rangle$，运算 $*$ 与 $\oplus$ 均为可交换的，若 $\forall x, y \in A$，有 $x * (x \oplus y) = x$ 且 $x \oplus (x * y) = x$，则称运算 $*$ 和 $\oplus$ 满足吸收律。例：幂集 $P(S)$ 上的运算 $\cap, \cup$ 满足吸收律。

单位元相关

【定义1.8】（单位元）已知 $\langle A, * \rangle$，$e_l, e_r, e \in A$。若有 $\forall x, e_l * x = x$，则称 e_l 为 $*$ 的左单位元；若有 $\forall x, x * e_r = x$，则称 e_r 为 $*$ 的右单位元。若 e 既是左单位元，又是右单位元，称 e 为 $*$ 的单位元，即$\forall x, x * e = e * x = x$。

【定理1.1】（左右单位元相等）设 $*$ 是在 A 上的二元运算，具有左单位元 e_l，右单位元 e_r，则 $e_l = e_r = e$。

证明：$e_l = e_l * e_r = e_r$，证毕。

【推论1.1】（单位元的唯一性）二元运算的单位元若存在则唯一。

证明：反证，设有单位元 e, e' 且 $e \neq e'$。又 $e = e * e' = e'$，矛盾。原命题得证。

零元相关

【定义1.9】（零元）已知 $\langle A, * \rangle$，$\theta_l, \theta_r, \theta \in A$。若有 $\forall x, \theta_l * x = \theta_l$，则称 θ_l 为 $*$ 的左零元；若有 $\forall x, x * \theta_r = \theta_r$，则称 θ_r 为 $*$ 的右零元。若 θ 既是左零元又是右零元，则称 θ 为 $*$ 的零元，即 $\forall x, \theta * x = x * \theta = \theta$。

【定理1.2】（左右零元相等）设 $*$ 是在 A 上的二元运算，具有左零元 θ_l，右零元 θ_r，则 $\theta_l = \theta_r = \theta$。

【推论1.2】（零元的唯一性）二元运算的零元若存在则必唯一。

定理1.2和推论1.2的证明与定理1.1、推论1.1相似。

逆元相关

【定义1.10】（逆元）已知 $\langle A,*\rangle$，e 为 $*$ 单位元。若 $x*y=e$，则对于 $*$，x 是 y 的左逆元，y 是 x 的右逆元，若 $x*y=y*x=e$，称 x 是 y 的逆元，记作 $x=y^{-1}$。存在逆元（左逆元，右逆元）的元素称为可逆的（左可逆的，右可逆的）。

【定理1.3】（左右逆元相等）对于可结合运算 $*$，如果 x 有左逆元 y，右逆元 z，则 $y=z=x^{-1}$。

证明：$z=e*z=(y*x)*z=y*(x*z)=y*e=y$，证毕。

【推论1.3】（逆元唯一）对于可结合运算 $*$，逆元若存在则必唯一。

证明：若对 x 存在逆元 y,z，则 $z=e*z=(y*x)*z=y*(x*z)=y*e=y$，矛盾。原命题得证。

消去律

【定义1.11】（消去律）已知 $\langle A,*\rangle$，若 $\forall x,y,z\in A$，有

- 若 $x*y=x*z$ 且 $x\neq\theta$，则 $y=z$（左消去律）；
- 若 $y*x=z*x$ 且 $x\neq\theta$，则 $y=z$（右消去律）；

则称 $*$ 满足消去律。

2 代数系统及同态

【定义2.1】（代数系统）设 A 为非空集合，Ω 为 A 上运算的集合，称 $\langle A,\Omega\rangle$ 为一个代数系统。

- 当 $\Omega=\{f_1,f_2,\ldots,f_n\}$ 有限时，代数系统也记为 $\langle A,f_1,f_2,\ldots,f_n\rangle$。
- 当 A 有限时，称 $\langle A,\Omega\rangle$ 为有限代数系统。

代数系统还可以表示为 $\langle A,\Omega,c_1,c_2,\ldots\rangle$，其中，$c_1,c_2,\ldots$ 为代数常数，如单位元等。

【定义2.2】（同类型的代数系统）如果两个代数系统运算个数相同，对应运算元数相同，且代数常数个数相同，则称他们为同类型代数系统。

【定义2.3】（子代数系统）设 $V=\langle S,f_1,f_2,\ldots,f_k\rangle$ 是代数系统，对于 $\emptyset\neq B\subseteq S$，如果 B 对于 $f_1,f_2,\ldots,f_k$ 是封闭的，且 B 和 S 含有相同的代数常数，则称 $\langle B,f_1,f_2,\ldots,f_k\rangle$ 是 V 的子代数系统，简称子代数。

- 最大的子代数是 V 本身；最小的子代数是由 V 中所有代数常数构成的集合 B' 进行延拓使其满足封闭性所得到的集合 B 构成的代数系统 $\langle B,f_1,f_2,\ldots,f_k\rangle$。
- 最大的子代数和最小的子代数统称为平凡的子代数。
- 若 B 是 S 的真子集，则 B 构成的子代数称为 V 的真子代数。

【定义2.4】（积代数）设 $V_1=\langle A,\circ\rangle,V_2=\langle B,*\rangle$ 是同类型的代数系统，$\circ$ 和 $*$ 为二元运算，在集合 $A\times B$ 上如下定义二元运算 $\oplus$：

$$\forall(a_1,b_1),(a_2,b_2)\in A\times B,\quad (a_1,b_1)\oplus(a_2,b_2)=(a_1\circ a_2,b_1*b_2)$$

则称 $V=\langle A\times B,\oplus\rangle$ 为 V_1 和 V_2 的积代数，记作 $V_1\times V_2$，此时也称 V_1,V_2 是 V 的因子代数。

【定理2.1】设 $V_1=\langle A_1,\circ\rangle,V_2=\langle B,*\rangle$ 是同类型的代数系统，$\circ$ 和 $*$ 为二元运算，$V=\langle A\times B,\oplus\rangle$ 为 V_1 和 V_2 的积代数，则

- 如果 $\circ$ 和 $*$ 是可交换（可结合、幂等）的，则 $\oplus$ 也是可交换（可结合、幂等）的。
- 如果 e_1,e_2（θ_1,θ_2）分别为 $\circ$ 和 $*$ 的单位元（零元），则 $\langle e_1,e_2\rangle$（$\langle\theta_1,\theta_2\rangle$）也是 $\oplus$ 的单位元（零元）。
- 如果 x 和 y 分别为 $\circ$ 和 $*$ 的可逆元素，则 $\langle x,y\rangle$ 也是 $\oplus$ 运算的可逆元素，其逆为 $\langle x^{-1},y^{-1}\rangle$。

证明：利用定义容易得到。

【定义2.5】（同态映射）设 $V_1=\langle A,\circ\rangle, V_2=\langle B,*\rangle$ 是同类型的代数系统，$f:A\to B$，对 $\forall x,y\in A$ 有 $f(x\circ y)=f(x)*f(y)$，则称 f 是 V_1 到 V_2 的同态映射。

- f 如果是单射，称为单同态；
- f 如果是满射，称为满同态，此时称 V_2 是 V_1 的同态像，记作 $V_1\sim V_2$ 或 $A\sim B$；
- f 如果是双射，称为同构，也称 V_1 同构于 V_2，记作 $V_1\cong V_2$ 或 $A\cong B$；
- 如果 $V_1=V_2$ 称为自同态（注意是 $V_1=V_2$，也即 $A=B$ 且运算相同）。

3 半群

【定义3.1】（半群）一个代数系统 $\langle A,*\rangle$，其中 A 为非空集合，$*$ 是定义在集合 A 上的二元运算。如果 $*$ 是封闭的，而且是可结合的，那么该代数系统被称为半群。

- 半群中不一定存在单位元，如 $\langle\mathbb{Z}_+,+\rangle$。

【定理3.1】若 $\langle A,*\rangle$ 是一个半群，且 A 为有限集，那么 A 中必然存在等幂元，即 $\exists a\in A, a=a*a$ 。

证明：因为 A 是一个半群，任选 $a\in A$，则由于封闭性，$a^2=a*a\in A$，$a^3=a*a^2\in A$，……，$a^n\in A\quad(n\in\mathbb{N}_+)$。

又因为 A 为有限集，则必然存在 $i<j$，使得 $a^i=a^j$。设 $k=j-i$，则有 $a^j=a^k*a^i=a^i$，从而

$$\forall m>i, a^{k+m}=a^m$$

必定存在 $n\geq 1$ 使得 $kn\geq i$，从而，

$$a^{kn}=a^{k+kn}=a^{k+(k+kn)}=\ldots=a^{nk+nk}=a^{nk}*a^{nk}$$

即存在等幂元。

【定义3.2】（独异点）若半群 $\langle A,*\rangle$ 中有单位元 e 存在，则称 $\langle A,*\rangle$ 是一个独异点（含幺半群）。也用三元组 $\langle A,*,e\rangle$ 表示。

【定理3.2】设 $\langle A,*,e\rangle$ 为一个含幺半群，运算 $*$ 的运算表中的任意两行或两列均不相同。

证明：对于任意两行或两列，必然存在一个位置为和 e 进行运算，此时对 $a\neq b$，有 $a*e=a\neq b=b*e$，$e*a=a\neq b=e*b$，故不存在完全相同的两行或两列，得证。

4 群、子群、群元素的阶

【定义4.1】（群）一个代数系统 $\langle G,*\rangle$，其中 G 为非空集合，$*$ 是定义在 G 上的二元运算。如果该代数系统是半群，且满足如下性质：

- 存在单位元 e；
- 每个元素均存在逆元，即 $\forall a\in G,\exists a^{-1}$。

则称 $\langle G,*\rangle$ 是一个群。也即群是所有元素都可逆的含幺半群。

【定义4.2】（群的阶）设 $\langle G,*\rangle$ 为一个群，若 G 是有限集合，则称该群为有限群，集合 G 的大小称为该群的阶，记作 $|G|$；如果 G 为无限集合，称该群为无限群。

【定理4.1】（群的性质）设 $\langle G,*\rangle$ 是群，则满足如下性质：

- 阶数大于 1 的群必不含有零元；（零元不存在逆元）
- $\forall a,b\in G$，存在唯一的 $x\in G$，使得 $a*x=b$；（$x=a^{-1}*b$，且逆元唯一）
- $\forall a,b,c\in G$，若 $a*b=a*c$，则 $b=c$，即群满足**消去律**；（两边同左乘 a^{-1}）
- 其运算表中每一行（每一列）都是 G 元素的一个置换，且每个置换彼此不同；

证明：反证，若不是一个置换则存在 $b \neq c$ 但是有 $a * b = a * c$，根据消去律即可推得矛盾；置换彼此不同在【定理3.2】中已经证明。

- 除单位元 e 之外，不可能存在等幂元。

  证明：反证，若存在 $a \neq e$ 且 $a * a = a = a * e$，根据消去律可以推得矛盾。

【定义4.3】（群的等价定义1）设 $\langle G, * \rangle$ 是一个半群，且存在左单位元 e，任一元素 $a \in G$，都有左逆元 a^{-1} 满足 $a^{-1} * a = e$，则 $\langle G, * \rangle$ 是一个群。（注：左、右单位元 / 逆元任选其一即可）

证明（等价定义1和原定义等价）：

- 一方面，

  (1) $\langle G, * \rangle$ 是一个半群，封闭性和可结合性成立。

  (2) 左单位元 e 同时是右单位元，进而根据【推论1.1】是单位元。

$$\begin{gathered} a * e = e * a * e = ((a^{-1})^{-1} * a^{-1}) * a * (a^{-1} * a) \\ \Longrightarrow a * e = (a^{-1})^{-1} * (a^{-1} * a) * a^{-1} * a = ((a^{-1})^{-1} * a^{-1}) * a = a \end{gathered}$$

  (3) 左逆元 a^{-1} 同时是右逆元，进而根据【推论1.3】是逆元。

  $a * a^{-1} = e * a * a^{-1} = (a^{-1})^{-1} * a^{-1} * a * a^{-1} = (a^{-1})^{-1} * (a^{-1} * a) * a^{-1} = (a^{-1})^{-1} * a^{-1} = e$

- 另一方面，群显然满足此定义中的条件。

【推论4.1】群内元素的左逆元即为逆元；群的左单位元即为单位元。

【定义4.4】（群的等价定义2）设 $\langle G, * \rangle$ 是一个半群，$\forall a, b \in G$，若一元一次方程 $a * x = b$ 和 $y * a = b$ 在集合 G 中有解，则 $\langle G, * \rangle$ 是一个群。

证明（等价定义2和等价定义1等价）：

- 一方面，根据等价定义1，只需要证明存在左单位元和左逆元即可。

  任取 $a = b \in G$，有 $y * b = b$ 有解 $y = e$ ，从而 $eb = b$;

  又 $\forall a \in G, bx = a$ 有解 $x = c$，从而 $e * a = e * (b * c) = (e * b) * c = b * c = a$，即存在左单位元。

  取 $b = e$，则 $y * a = e$，解得 $y = a^{-1}$ 为左逆元。

- 另一方面，根据【推论4.1】，左右逆元均存在且相等，因此上述两方程有解（作用逆元即可）。

【定义4.5】（**有限**群的等价定义3）设 $\langle G, * \rangle$ 为一个**有限**半群，$\forall a, b, c \in G$，若 $a * b = a * c$ 有 $b = c$；若 $b * a = c * a$ 有 $b = c$，则 $\langle G, * \rangle$ 是一个群。

证明：设 $G = \{a_1, a_2, \ldots, a_n\}$。一方面，从运算表的角度，根据【定理4.1】其运算表每一行每一列均为一个置换，且不相同，因此$\forall a, b$，$a * x = b$ 和 $y * a = b$ 必然有解。进而由【定义4.4】知是一个群；另一方面，从【定义4.2】除法，由【定理4.1】容易知道满足消去率。

无限群的反例：$\langle \mathbb{Z}_+, + \rangle$ 为半群，且满足消去律。但是其不含有单位元，不是群。

【引理4.1】子群 $\langle H, * \rangle$ 中的单位元即为原群 $\langle G, * \rangle$ 的单位元。

证明：设 e_H 为子群的单位元，e 为原群的单位元，则 $e_H, e \in G$。

$$e_H * e = e_H = e_H * e_H$$

在群 G 中应用消去律，有 $e = e_H$。证毕。

【定理4.2】（群元素的性质）设 $\langle G, * \rangle$ 是一个群，$\forall a, b \in G$，有

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

  证明：$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * b = e$，根据【推论4.1】即为逆元。

- $a^{m+n} = a^m * a^n$

- $(a^m)^n = a^{mn}$

【定义4.6】（子群）设 $\langle G, *\rangle$ 是一个群，$\emptyset \neq H \subseteq G$，如果 H 在 $*$ 下也构成群，则 $\langle H, *\rangle$ 被称为 $\langle G, *\rangle$ 子群，简写为 $H \leq G$。

- $\langle G, *\rangle$，$\langle \{e\}, *\rangle$ 都是 $\langle G, *\rangle$ 的平凡子群。
- 若 H 是 G 的真子集，称 $\langle H, *\rangle$ 为 $\langle G, *\rangle$ 的真子群。

【定理4.3】（子群判定定理）设 $\langle G, *\rangle$ 是一个群，集合 H 是 G 的非空子集。则 $\langle H, *\rangle$ 是 $\langle G, *\rangle$ 的子群等价于下列之一：

- 判定定理 1：对于 H 中任意元素 a 和 b，都有 $a * b^{-1} \in H$；
- 判定定理 2：任意 $a, b \in H$，$a * b \in H$；任意 $a \in H$，$a^{-1} \in H$。（简写为 $H * H \subseteq H, H^{-1} \subseteq H$）
- 判定定理 2.5：如果 H 是有限群，判定定理 2 只需要保留前半部分 $H * H \subseteq H$。

证明：注意，下面证明中基于 G 中已经含有单位元 e，事实上，由【引理4.1】其即为 H 单位元。

- 先证明判定定理 1：

  (1) 运算 $*$ 满足可结合性；(2) 令 $a = b$，则有 $a * a^{-1} = e \in H$，原群单位元 e 在子群中，子群单位元存在；

  (3) 令 $a = e$，则可知，$\forall b \in H, e * b^{-1} = b^{-1} \in H$，逆元存在；

  (4) $\forall a, b \in H, a * (b^{-1})^{-1} = a * b \in H$，满足封闭性。

- 再证明判定定理 2：

  (1) 运算 $*$ 满足可结合性；(2) 条件满足封闭性；(3) 条件满足逆元存在；

  (4) 令 $b = a^{-1}$，则 $a * b = a * a^{-1} = e \in H$，原群单位元 e 在子群中，子群单位元存在；

- 判定定理 2.5 的证明：

  (1) 运算 $*$ 满足可结合性；(2) 条件满足封闭性；

  任取 $a \in H$，

  (3) 由封闭性 $a, a^2, a^3, \ldots, a^n, \ldots \in H$，因而必然存在 $i < j$，$a^i = a^j$，从而 $e = a^{-i} * a^i = a^{j-i}$，即 a^{j-i} 即为原群单位元，且一定在子群中；

  (4) $j - i \geq 1$，分类讨论。若 $j - i = 1$，则 $e = a$，单位元的逆元即为其本身；若 $j - i > 1$，则 $e = a^{j-i} = a^{j-i-1} * a$ 即可知逆元为 a^{j-i-1}。

  注：可能有很多不同类的元素，每类元素需要找出其的单位元，进而求出其逆元。

【定义4.7】（子群的交、并、复合）设 $\langle G, *\rangle$ 有子群 $\langle H_1, *\rangle$，$\langle H_2, *\rangle$，则

- $\langle H_1 \cap H_2, *\rangle$ 称为子群的交，其是原群的子群。证明显然。
- $\langle H_1 \cup H_2, *\rangle$ 称为子群的并，其不一定是原群的子群。可以寻找两个集合的对称差部分。
- $\langle H_1 H_2, *\rangle$ 称为子群的复合，其中 $H_1 H_2 = \{h_1 * h_2 \mid h_1 \in H_1, h_2 \in H_2\}$，其不一定是原群的子群。

【定义4.8】（群中集合生成的子群）设 $\langle G, *\rangle$ 是一个群，集合 S 是 G 的非空子集。记 $\left\langle \cap_{S \subseteq H, \langle H, *\rangle \leq \langle G, *\rangle} H, * \right\rangle$ 是 S 所生成的子群，记为 $\langle (S), *\rangle$。

【推论4.2】由定义自然有，$S \subseteq (S)$，$\langle (S), *\rangle$ 是 $\langle G, *\rangle$ 的子群且 (S) 为包含了 S 的能够构成群的最小集合。

【定义4.9】（群元素的阶）设 $\langle G, *\rangle$ 是一个群，单位元为 e，任意元素 $a \in G$，定义集合 $S = \{n \in \mathbb{Z}^+ : a^n = e\}$。

- 若 $S = \emptyset$，则称 a 的阶为 ∞，记作 $|a| = \infty$，并称 a 为无限元；
- 若 $S \neq \emptyset$，则称 S 中的最小数 n 为 a 的阶，记作 $|a| = n$，并称 a 为 n 阶元。

【定理4.4】（群元素阶的性质定理1）设 $\langle G, *\rangle$ 是一个群，单位元为 e。对任意元素 $a \in G$，若 $|a| = k \in \mathbb{N}$，且若存在 $n \in \mathbb{N}$ 使得 $a^n = e$，则有 $k \mid n$。

证明：反证。设 $n = qk + r$，其中 $q \in \mathbb{N}, 0 < r < k$，则

$$e = a^n = a^{qk+r} = (a^k)^q * a^r = e^q * a^r = a^r$$

故 $|a| = r < k$ 与 $|a| = k$ 矛盾。故原命题成立，$k|n$。

【定理4.5】（群元素阶的性质定理2）设 $\langle G, *\rangle$ 是一个群，单位元为 e。对任意元素 $a \in G$，若 $|a| = n \in \mathbb{N}$，且对任意的 $k \in \mathbb{Z}^+$，a^k 的阶为 $\frac{n}{(n,k)}$。

证明：设 $|a^k| = m$，则 $a^{km} = e$，由【定理4.4】有 $n \mid km$，故 $\frac{n}{(n,k)} \mid \frac{k}{(n,k)}m$，由 $\left(\frac{n}{(n,k)}, \frac{k}{(n,k)}\right) = 1$ 则 $\frac{n}{(n,k)} \mid m$。

另一方面，$(a^k)^{\frac{n}{(k,n)}} = (a^n)^{\frac{k}{(n,k)}} = e$，由【定理4.4】有 $m \mid \frac{n}{(n,k)}$。

综上，$|a^k| = m = \frac{n}{(n,k)}$。

5 Abelian 群和循环群

【定义5.1】（Abelian群）满足交换律的群被称为 Abelian 群。

【定义5.2】（元素的幂次）对于群 $\langle G, *\rangle$，元素 a 的 i 次整数幂完整定义为：

$$a_0 = e, \quad a^i = a * a * \ldots * a, \quad a^{-i} = a^{-1} * a^{-1} * \ldots * a^{-1}$$

其中，e 也可记为 1。

【定义5.3】（循环群）设 $\langle G, *\rangle$ 为群，若 G 中存在元素 a，使得 G 的任意元素都由 a 的幂次组成，则称该群为循环群，有时也记作 $\langle (a), *\rangle$，a 称为群 $\langle G, *\rangle$ 的生成元。

- 循环群一定是 Abelian 群；是最简单的群，仅由一个元素生成；
- 分为有限群换群和无限循环群。

【定理5.1】（循环群的形状）若 $\langle G, *\rangle$ 为一个循环群，则其必有如下形状：

- $G = \{\ldots, a^{-n}, \ldots, a^{-2}, a^{-1}, e = a^0, a, a, a^2, \ldots, a^n, \ldots\} = \{a^n \mid n \in \mathbb{N}\}$ 为无限循环群，群的阶为 ∞；
- $G = \{e = a^0, a^1, a^2, \ldots, a^{n-1}\}$，其中 $a^n = e$，而且对于 $0 \le s, t < n$, $a^s = a^t \iff s = t$。则其为有限循环群，群的阶为 n。

【推论5.1】（循环群的阶和生成元的阶）循环群的阶和生成元的阶相等。

证明：分类讨论为有限循环群或无限循环群，利用【定理5.2】即证。

【定理5.2】 设 $\langle G, *\rangle$ 为阶为 n 的有限循环群，$a \in G$ 是生成元。对任意整数 m，若有 $a^m = e$，则必有 $n|m$。

证明：反证。设$m = qn + r$，其中 $q \in \mathbb{N}, 0 < r < n$。

$$e = a^m = a^{qn+r} = a^{qn} * a^r = (a^n)^q * a^r = e * a^r = a^r$$

从而 $a^r = a^0 = e$，矛盾。故原命题成立，即 $n \mid m$。

【定理5.3】 设 $\langle G, *\rangle$ 为无限循环群，则若 $|G| = \infty$，则 G 中仅有两个生成元 a, a^{-1}。

证明：若 $|G| = \infty$ 且 a 为生成元，则任意 $b = a^k \in G$，有$b = (a^{-1})^{-i}$，从而 a^{-1} 也是生成元。

若 G 中还有其他生成元 $b = a^m$，则必然存在 n 使得 $a = b^n = (a^m)^n = a^{mn}$，从而 $a^{mn-1} = e$。

由于 $\langle G,*\rangle$ 为无限群，则只可能 $mn-1=0$，即 $m=1,n=1$，$b=a$，故生成元唯一。

【引理5.1】（裴蜀定理）$as+bt=m$ 有整数解 (s,t) 当且仅当 $(s,t)\mid m$。

【定理5.4】 设 $\langle G,*\rangle$ 为循环群，若 $|G|=n\in\mathbb{N}$，则 G 内有 $\varphi(n)$ 个生成元。

证明：设 a 是一个生成元，则其他生成元一定能表示为 a 的幂次，设生成元 $b=a^r$，则 $\exists t, b^t=(a^r)^t=a^{rt}=a$，从而$a^{rt-1}=e$，则必有 $n\mid(rt-1)$。即 $\exists q, rt+qn=1$，由裴蜀定理，$(r,n)=1$，从而生成元的个数为 $\varphi(n)$。证毕。

【定理5.5】（循环群的子群）设 $\langle G,*\rangle$ 为一个循环群，则

- 其子群一定是循环群；
- 若 $\langle G,*\rangle$ 是无限循环群，则除平凡子群 $\langle\{e\},*\rangle$ 外，其他子群也是无限群；
- 若 $\langle G,*\rangle$ 为有限循环群且生成元为 a，阶为 n，若其子群 $\langle H,*\rangle$ 中元素最小正整数幂为 a^k，则 $|H|=\frac{n}{k}$。

证明：

- 设其子群 $\langle H,*\rangle$ 内元素最小正整数幂为 a^k，则由封闭性、逆元存在性，$a^{sk}\in H(s\in\mathbb{Z})$ 。如果说明了对于任意 $b=a^n\in H(n\geq k)$ 都有 $k\mid n$ 即可说明 $\langle H,*\rangle$ 为循环群。反证，设存在 $n=qk+r$，其中 $q\in\mathbb{N},0<r<k$，则 $b=a^n=a^{qk+r}=a^{qk}*a^r$，进而 $a^r=a^{n-qk}=a^n*a^{-qk}$，由于 $a^{-qk}\in H, a^n\in H$ 故 $a^r\in H$，与假设（最小正整数幂）矛盾。原命题得证明，即子群 $\langle H,*\rangle$ 一定是由 a^k 为生成元的循环群。
- 由上条，子群一定是循环群。反证，若某以 a^k 为生成元的子群为有限群，则必定存在 n，$(a^k)^n=e$，即 $a^{kn}=e$，从而群 $\langle G,*\rangle$ 不是无限循环群，矛盾。原命题成立，即无限循环群的子群是无限循环群。
- 设 $|H|=d$。上上条已证，a^k 为子群生成元。首先说明 $k\mid n$。反证，若$k\nmid n$，首先有 $n\leq kd$，则$\exists m, mk<n\leq(m+1)k$，从而$a^{(m+1)k-n}=a^{(m+1)k}\in H$ 且 $(m+1)k-n<k$，与 H 中元素最小正整数幂是 k 矛盾。一方面，$(a^k)^{n/k}=a^n=e$，则 $d\mid\frac{n}{k}$；另一方面，由于 $(a^k)^d=e$ ，因此由【定理5.2】有 $n\mid kd$，从而 $\frac{n}{k}\mid d$。进而$|H|=d=\frac{n}{k}$。

【推论5.2】 若 $\langle G,*\rangle$ 为有限循环群且生成元为 a，阶为 n，若其子群 $\langle H,*\rangle$ 中元素最小正整数幂为 a^k，则 a^k 为子群 $\langle H,*\rangle$ 生成元且 $k\mid n$。

证明见【定理5.5】证明第1、3条。

【定理5.6】 设 $\langle G,*\rangle$ 是 n 阶循环群，则对于 n 的每一个正因子 d，$\langle G,*\rangle$ 有且仅有一个 d 阶子群。

证明：设 $n/d=k$。则首先，令 $H=\{(a^k)^m|m\in\mathbb{Z}\}\subseteq G$，则 H 为 a^k 生成的集合，下面证明 $\langle H,*\rangle$ 是一个群。可结合性、封闭性满足，单位元逆元显然存在；且由于 $|G|=n$，因此容易说明 $|H|=d$。其次，若有两个 d 阶子群 $\langle H,*\rangle,\langle H',*\rangle$，且后者的最小正幂次元素为 $a^{k'}$，则有 $n\mid k'd\Longrightarrow k'd=qn\Longrightarrow k'=\frac{qn}{d}=kq$，因此 $H'\subseteq H$，又 $|H'|=|H|$，故 $H'=H$，唯一性得证。

【推论5.3】 对于有限循环群，子群个数就等于群的阶的正因子个数。

【推论5.4】 对于 n 阶循环群，$\langle(a),*\rangle$，若 $\left\langle(a^k),*\right\rangle$ 为子群，则必然有 $k\mid n$，且 $|(a^k)|=n/k=d$ 。

6 陪集与指数

【定义6.1】（陪集）设 $\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的一个子群，$a\in G$，则集合 $aH=\{a*h|h\in H\}$ （或集合 $Ha=\{h*a|h\in H\}$）被称为 H 在 G 中的左陪集（右陪集）。

【定理6.1】（陪集的性质）设 $\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的一个子群，$a,b\in G$，则 $\langle H,*\rangle$ 的左陪集具有如下性质:

- $H = eH, a \in aH$;
- $|aH| = |H|$;
- $a \in H \Longleftrightarrow aH = H$;
- $\forall x \in aH, aH = xH$;
- $\forall a, b \in G$，要么 $aH = bH$，要么 $aH \cap bH = \emptyset$。

证明:

- $\forall x \in H \subseteq G, e * x = x$，从而 $H = eH$；又由于 $e \in H$，所以 $a * e = a \in aH$。
- 首先，$|aH| \le |H|$。反证，若 $|aH| < |H|$，则 $\exists h_1, h_2 \in H (h_1 \ne h_2), a * h_1 = a * h_2$，根据消去律，有 $h_1 = h_2$，矛盾。因此 $|aH| = |H|$。
- 充分性：由于 $aH = H$，则 $\forall h \in H, a * h = h' \in H$，从而 $a = h' * h^{-1} \in H$（根据群的性质）。必要性：$a \in H$，则 $\forall a * h \in aH, a * h \in H$，即 $aH \subseteq H$；同时 $\forall h \in H, a^{-1} * h \in H$，从而 $a * a^{-1} * h = h \in aH$，即 $H \subseteq aH$；综上，$H = aH$。
- $\forall x = a * h' \in aH$，一方面 $\forall x * h \in xH, x * h = a * h' * h = a * (h' * h) \in aH$，从而 $xH \subseteq aH$；另一方面 $\forall a * h \in aH, a * h = x * h'^{-1} * h = x * (h'^{-1} * h) \in xH$，从而 $aH \subseteq xH$，即 $aH = xH$。
- 若 $aH \cap bH \ne \emptyset$，即 $\exists g \in aH \cap bH$，$\exists h_1, h_2 \in H, a * h_1 = b * h_2$，从而 $\forall a * h \in aH$，有 $a * h = a * h_1 * h_1^{-1} * h = b * (h_2 * h_1^{-1} * h) \in bH$，即 $aH \subseteq bH$，同理 $bH \subseteq aH$，则 $bH = aH$。

  【注】上述过程可以简写为 $aH = a(h_1H) = (ah_1)H = (bh_2)H = b(h_2H) = bH$。

【定理6.2】 设 $\langle G, * \rangle$ 是一个群，且有子群为 $\langle H, * \rangle$。$a, b \in G$，则左陪集 $aH = bH$ 等价于 $a^{-1} * b \in H$ 或 $b^{-1} * a \in H$；类似的，右陪集 $Ha = Hb$ 等价于 $b * a^{-1} \in H$，或 $a * b^{-1} \in H$。

证明：下面仅证明 $aH = bH \Longleftrightarrow a^{-1} * b \in H$，其余同理可证。必要性：因为 $aH = bH$，则 $\exists h_1, h_2 \in H$，$a * h_1 = b * h_2$，即$a^{-1} * b = h_1 * h_2^{-1} \in H$；充分性：$a^{-1} * b = h \in H$，则 $b = ah \in aH$，即 $b \in aH$，根据【定理6.1】有，$aH = bH$。

【定义6.2】 群 $\langle G, * \rangle$ 有子群 $\langle H, * \rangle$，定义 $S_L = \{G\text{关于}H\text{的所有左陪集}\}, S_R = \{G\text{关于}H\text{的所有右陪集}\}$，则 H 在 G 中的指数 $[G:H]$ 定义为 S_L（S_R）的势。当集合 S_L（S_R）是有限集时，H 在 G 中的指数 $[G:H]$ 就等于 G 关于 H 的左（右）陪集个数。

【定理6.3】（Lagrange 定理）设 $\langle G, * \rangle$ 是有限群，$\langle H, * \rangle$ 是它的子群，则 $|H| \mid |G|$，即

$$|G| = [G:1] = [G:H] \times [H:1] = [G:H] \times |H|$$

注：这里将子群 $\langle \{e\}, * \rangle$ 中的 $\{e\}$ 简写为 1。

【定理6.4】 设 $\langle G, * \rangle$ 是 n 阶群，则 $\langle G, * \rangle$ 中任意元素 a 的阶都是 n 的因子，且有 $a^n = e$。

证明：由于 $\langle (a), * \rangle$ 是 $\langle G, * \rangle$ 的子群，且是以 a 为生成元的循环群，设这个子循环群的阶为 m，则 $|a| = |(a)| = m$，由 Lagrange 定理有 $|(a)| \mid |G|$ 即 $m|n$，从而任意元素 a 的阶都是 n 的因子。同时，有 $n = km$，从而 $a^n = a^km = (a^m)^k = e^k = e$。

【例6.1】 阶为素数的 p 群一定是循环群。

证明：从群中任取一个非单位元元素 a 构成循环群，则 a 生成的子群一定是循环群且该子群的阶 n 一定满足 $n|p$，由于 $a \ne e$，从而 $n \ne 1$，从而 $n = p$，即原群一定是循环群。

【例6.2】 阶数为 4 的群 $\langle G, * \rangle$ 要么是循环群，要么是 Klein 四元群。

证明：若该四元群中存在阶数为 4 的元素 a，那么 a 是生成元，原群是循环群。否则由【定理6.4】，G 中只有阶数为 1 或 2 的元素，阶数为 1 的元素只有 e，那么其余三个元素 a, b, c 阶数均为2，所以 $a^2 = b^2 = c^2 = e$。考虑 $a * b$，显然 $a * b \ne a, a * b \ne b$（若等则消去律后 $a = e$ 或 $b = e$），$a * b \ne e$（若等则 $a = b$），所以 $a * b = c$，所得到的运算表即 Klein 四元群的运算表

【**定理6.5**】设 A, B 是群 $\langle G, *\rangle$ 的两个有限子群，那么有 $|AB| = \frac{|A|\times|B|}{|A\cap B|}$，其中

$$AB = \{a * b | a \in A, b \in B\} = \cup_{a\in A} aB$$

证明：令 $A \cap B = C$，则 C 是 A 的子群。令

$$S_1 = AB = \cup_{a\in A} aB, \quad S_2 = AC = \cup_{a\in A} aC, \quad T_1 = \{aB|a \in A\}, \quad T_2 = \{aC|a \in A\}$$

那么 $|S_1| = |AB|$，$|S_2| = |A|$。定义映射 $f : aB \to aC$，则满射显然，下面证明其为单射：（反证）若有 $a, a' \in A(aB \neq a'B)$，$f(aB) = aC = a'C = f(a'B)$，则由【定理6.2】，$a^{-1} * a' \in C = A \cap B$，故 $a^{-1} * a' \in B$，从而 $aB = a'B$，矛盾。从而 f 为双射，即 $|T_1| = |T_2|$。

由于 $|AB| = |S_1| = |T_1| \times |B|$，$|A| = |S_2| = |T_2| \times |C| = |T_2| \times |A \cap B|$，从而联立有 $|AB| = \frac{|A|\times|B|}{|A\cap B|}$。

【**引理6.1**】若群 $\langle G, *\rangle$ 中只有一阶、二阶元，则 $\langle G, *\rangle$ 为交换群。

证明：一阶元 e 和任何元素运算显然满足可交换，对于任意二阶元 a, b，有 $a * a = e, b * b = e$，且 $a * b \in G$，满足 $(a * b) * (a * b) = e$，从而 $b^{-1} * a^{-1} * a * b * a * b = b^{-1} * a^{-1} \Longrightarrow a * b = b * a$。综上群满足可交换。

【**例6.3**】证明6阶群中有且仅有一个3阶子群。

证明：设6阶群为 $\langle G, *\rangle$，选择任意元素 $a \in G$，则 $|a| \mid |G| = 6$，从而 $|a| = 1, 2, 3, 6$。

- 先证明存在3阶子群。反证，若不存在3阶子群，则同时也不存在6阶子群（若有6阶子群即为循环群 G，设其生成元 b，则 b^2 必然可以生成三阶子群）。因此 G 中只有一阶、二阶元，则 $\langle G, *\rangle$ 可交换。设 $G = \{e, a_1, a_2, a_3, a_4, a_5\}$，则 a_1, a_2, a_3, a_4, a_5 都是二阶元，考察 $a_1 * a_2$，则和【例6.3】类似，$a_1 * a_2 \neq e, a_1 * a_2 \neq a_1, a_1 * a_2 \neq a_2$，故 $a_1 * a_2 = a_3$或a_4或a_5，从而 $\langle \{e, a_1, a_2, a_1 * a_2\}, *\rangle$ 形成了一个群，同时也是 $\langle G, *\rangle$ 的子群，该子群的阶是4而原群阶为6，不满足 Lagrange 定理，因此存在3阶子群。
- 再证明唯一性，设 $\langle G, *\rangle$ 中有两个三阶子群 $\langle A, *\rangle, \langle B, *\rangle$，令 $K = A \cap B$，则 $\langle K, *\rangle$ 是 $\langle A, *\rangle, \langle B, *\rangle$ 的子群，根据 Lagrange 定理，$|K| \mid |A| = |B| = 3$，从而 $|K| = 1$或3。若 $K = 1$，则 $K = A \cap B = \{e\}$，那么根据【定理6.5】，$|AB| = \frac{|A|\times|B|}{|A\cap B|} = \frac{3\times3}{1} = 9$，但是 $AB \subseteq G$ 从而 $|AB| \leq |G| = 6$，矛盾，从而 $K = 3$。于是 $|A| = |B| = |A \cap B|$，故 $A = B$，唯一性得证。

7 正规子群与商群

【**定义7.1**】设 $\langle G, *\rangle$ 是群，$H \leq G$。若 $\forall a \in G, aH = Ha$，则称 $\langle H, *\rangle$ 是 $\langle G, *\rangle$ 的正规子群（不变子群），记作 $H \lhd G$。

【**定理7.1**】（正规子群的判定）设有群 $\langle G, *\rangle$，$H \leq G$，则下面四个说法等价：

- $H \lhd G$
- $\forall a \in G, aHa^{-1} = H$
- $\forall a \in G, aHa^{-1} \subseteq H$
- $\forall a \in G, h \in H, aha^{-1} \in H$

证明：

- ①→②：$aH = Ha$，则 $aHa^{-1} = H$；
- ②→③：$aHa^{-1} = H$，则 $aHa^{-1} \subseteq H$；
- ③→④：$aHa^{-1} \subseteq H$，则 $\forall aha^{-1} \in aHa^{-1}, aha^{-1} \in H$。
- ④→①：一方面，$\forall a \in G, h \in H, \exists h' \in H, aha^{-1} = h'$，从而 $ah = h'a \in Ha$，故 $aH \subseteq Ha$；另一方面，$\forall a \in G(a^{-1} \in G), h \in H, \exists h' \in H, a^{-1}ha = h'$，从而 $ha = ah' \in aH$，故 $Ha \subseteq aH$。故$aH = Ha$。

【定理7.2】 设 $\langle G, *\rangle$ 是群，且 $H \leq G$，H 的任意两个左陪集的乘积仍然为左陪集，则 $H \lhd G$。

证明：$\forall a, b \in G, \exists c \in G, aHbH = cH$，则首先有 $ab = (ae)(be) \in aHbH = cH$，由【定理6.1】，$abH = cH$，故 $aHbH = abH$。从而 $\forall h \in H, a \in G$，有 $aha^{-1}h \in aHa^{-1}H = aa^{-1}H = H$。所以 $aha^{-1} \in H$，从而由【定理7.1】有，$H \lhd G$。

【定理7.3】 设 $\langle G, *\rangle$ 是群，且 $H \lhd G, H' \leq G$，则 $H \cdot H' \leq G, H' \cdot H \leq G$。

证明：本定理是【引理8.1】直接推论。

【例7.1】 设 $\langle G, *\rangle$ 是群，$H \leq G$，且 $[G : H] = 2$，证明 $H \lhd G$。

证明：任取 $a \notin H$，则 $G = H \cup aH$；同理 $G = H \cup Ha$，而且 $H \cap Ha = H \cap aH = \emptyset$，从而 $Ha = aH$，即 $H \lhd G$。

【定理7.4】 设 $\langle G, *\rangle$ 是群，且 $H \lhd G$，则 H 的任意两个左陪集的乘积仍然为左陪集。

证明：$\forall a, b \in G, h, h' \in H$，有$ahbh' \in aHbH$，又 $ahbh' = a(hb)h' \in a(Hb)H = a(bH)H = abH$，证毕。

【定义7.2】（正规子群定义陪集之间的代数结构：商群）设 $\langle G, *\rangle$ 是群，$H \lhd G$，形成 G 陪集的集合（划分）

$$\{aH | a \in G\} = G/H$$

定义集合之间的运算 $aH \cdot bH$ （简写为 $aHbH$）为$aH \cdot bH = abH$。

则该运算在 G/H 上满足：

- 封闭性
- 可结合性（$aHbHcH = abcH = aH(bHcH)$）
- 单位元存在（$H = eH$）
- 逆元存在（$(aH)^{-1} = a^{-1}H$）

故 $\langle G/H, \cdot\rangle$ 是群，称为商群。

注：$H \lhd G$ 是定义商群的必要前提。

【定理7.5】 商群 $\langle G/H, \cdot\rangle$ 的阶是 $|G/H| = [G : H] = \frac{|G|}{|H|}$ 。

8 同态与同构、群同态、群同态基本定理

【定理8.1】 若两个代数系统 $\langle A_1, *\rangle$ 和 $\langle A_2, \circ\rangle$ 之间存在满同态映射 $f : A_1 \to A_2$，则有如下性质：

- 若 $\langle A_1, *\rangle$ 满足交换律或结合律，则 $\langle A_2, \circ\rangle$ 也满足交换律或结合律。
- 若 $\langle A_1, *\rangle$ 中有单位元 e，则 $\langle A_2, \circ\rangle$ 也有单位元 $f(e)$。
- 若 $\langle A_1, *\rangle$ 中任意元素 $a \in A_1$ 存在逆元 a^{-1}，则 $\langle A_2, \circ\rangle$ 中 $f(a)$ 一定存在逆元 $f(a^{-1})$。

证明：首先，根据条件，$\forall a, b \in A_1, f(a * b) = f(a) \circ f(b)$。$f(x)(x \in A_1)$ 取遍 A_2。

- 若 $\forall a, b \in A_1$，$f(a) \circ f(b) = f(a * b) = f(b * a) = f(b) \circ f(a)$；

  若 $\forall a, b, c \in A_1$，$f(a) \circ f(b) \circ f(c) = f(a * b * c) = f(a * (b * c)) = f(a) \circ (f(b) \circ f(c))$。
- 若 $\forall a \in A_1, a = e * a$，则 $f(a) = f(e * a) = f(e) \circ f(a)$，即 $f(e)$ 为单位元。
- 若 $\forall a \in A_1, a^{-1} * a = e$，则 $f(e) = f(a^{-1} * a) = f(a^{-1}) \circ f(a)$，从而 $f(a^{-1})$ 为 $f(a)$ 逆元。

注：性质3对于非满同态也成立。对于满同态可以强化为：只要 A_1 中的任意元素有逆元，A_2 中的任意元素就有逆元。

【例8.1】 试证明：任意无限循环群都与 $\langle \mathbb{Z}, +\rangle$ 同构。

证明：设无限循环群 $\langle(a),*\rangle$，则定义映射 $f(a^k)=k$，显然 $f:(a)\to\mathbb{Z}$。首先，因为 $\langle(a),*\rangle$ 是无限循环群，所以必不存在 $i\neq j,a^i=a^j$，从而 f 是单射；又因为 $\forall k\in\mathbb{Z},\exists a^k\in(a),f(a^k)=k$，所以 f 是满射；综上 f 是双射。最后，$f(a^i*a^j)=f(a^{i+j})=i+j=f(a^i)+f(a^j)$。证毕。

【定理8.2】 若给出了群 $\langle G,*\rangle$ 到群 $\langle G',\circ\rangle$ 的同态映射 f，则

- 若 $H\leq G$，则 $f(H)\leq G'$；特别地，$f(G)\leq G'$。
- 若 $H'\leq G'$，（f 为单射），则 $f^{-1}(H')=\{a|a\in G,f(a)\in H'\}\leq G$ 。

证明：

- $\forall f(a),f(b)\in f(H)$，即 $a,b\in H$，有 $f(a)\circ(f(b))^{-1}=f(a)\circ f(b^{-1})=f(a*b^{-1})\in f(H)$，根据【定理4.3】，又因为 $f:G\to G'$，则 $f(H)\subseteq G$，从而 $f(H)\leq G'$。
- $\forall a,b\in f^{-1}(H')$，即 $f(a),f(b)\in H'$，从而 $f(a*b^{-1})=f(a)\circ f(b^{-1})=f(a)\circ(f(b))^{-1}\in H'$，从而 $a*b^{-1}\in f^{-1}(H')$

【定义8.1】（零同态）设 $\langle G,*\rangle,\langle G',\circ\rangle$ 是两个群，定义映射 $f:x\to e'$，其中 $x\in G$，e' 是 G' 中单位元，则 $f(x*y)=e'$，因此 f 是 $\langle G,*\rangle$ 到 $\langle G',\circ\rangle$ 的一个同态，称为**零同态**。零同态存在于任意两个群中。

【定理8.3】 群同态的复合仍然是群同态，群同构的逆仍是群同构。

证明：

- 设群 $\langle G,*\rangle,\langle G',\circ\rangle$ 间存在同态映射 f，$\langle G',\circ\rangle,\langle G'',\oplus\rangle$ 中存在同态映射 g，则

  $\forall a,b\in G,(g\circ f)(a*b)=g(f(a)\circ f(b))=g(f(a))\oplus g(f(b))$

  因此群同态的复合仍是群同态。

- 设 $\langle G,*\rangle\cong\langle G',\circ\rangle$，同构映射为 f。则 $\forall b,b'\in G'$，设 $f^{-1}(b)=a,f^{-1}(b')=a'$，从而 $f^{-1}(b\circ b')=f^{-1}(f(a)\circ f(a'))=f^{-1}(f(a*a'))=a*a'=f^{-1}(b)*f^{-1}(b')$，由于 f 是双射，所以 f^{-1} 是双射，从而 $\langle G',\circ\rangle\cong\langle G,*\rangle$。

【注】 为方便，在下面的内容中，在运算不重要时默认依次为 $*,\circ$，此时将群 $\langle G,*\rangle$ 简单记为 G。

【定义8.2】（自然同态）若 $N\lhd G$，则定义 G 到商群 G/N 的映射 $h:h(x)=xN$。则 h 是从 G 到商群 G/N 的同态映射，称为自然同态。

【定义8.3】（同态核）若 $f:G\to G'$ 为群同态，e,e' 分别为 G,G' 单位元，则同态核定义为 $\ker f\overset{def}{=}\{x|x\in G,f(x)=e'\}$ 。

【定理8.4】 $\ker f\lhd G$ 。

证明：

- 首先有 $e\in\ker f$，则 $\ker f\neq\emptyset$。
- $\forall a,b\in\ker f,f(a*b^{-1})=f(a)\circ f(b^{-1})=f(a)\circ(f(b))^{-1}=e'\circ(e')^{-1}=e'$，同时 $\ker f\subseteq G$，从而 $\ker f$ 是 G 的子群。
- $\forall a\in G,a'\in\ker f,f(a*a'*a^{-1})=f(a)\circ f(a')\circ(f(a))^{-1}=f(a)\circ e'\circ(f(a))^{-1}=e'$ 。从而有 $a*a'*a^{-1}\in\ker f$，由【定理7.1】，$\ker f\lhd G$。

【定理8.5】 若有群同态 $f:G\to G'$，则 f 是单射 $\Longleftrightarrow\ker f=\{e\}$。

证明：

- $e\in\ker f$，f 是单射，则任意 $x\in G,x\neq e$，有 $f(x)\neq f(e)=e'$，从而 $\ker f=\{e\}$。
- 若 $\ker f=e$，且有 $x,y\in G,f(x)=f(y)$，则 $e'=f(x)\circ(f(y))^{-1}=f(x*y^{-1})$，从而 $x*y^{-1}\in e$，从而 $x*y^{-1}=e$，从而 $x=y$。故 f 是单射。

【定理8.6】（同态基本定理）设 $f:G\to G'$，令 $N=\ker f$，则有 $G/N\cong f(G)$。

证明：记 $N=\ker f$，则由 Kernel 的定义，N 一定是 G 的正规子群。定义 $\delta:G/N\to f(G)$ 为 $\delta(aN)=f(a)$。下面证明 δ 为同构映射。

- $\forall aN,bN\in G/N,\delta(aN\cdot bN)=\delta(abN)=f(a*b)=f(a)\circ f(b)=\delta(aN)\circ\delta(bN)$。
- 对于 $aN=bN$，有 $a*b^{-1}\in N$，从而$e'=f(a*b^{-1})=f(a)\circ(f(b))^{-1}$，即 $f(a)=f(b)$，故 $\delta(aN)=f(a)=f(b)=\delta(bN)$，从而 δ 是映射。
- 由上条知，最多有 $|G/N|$ 个不同 $f(\cdot)$ 取值，且对于任意取值 $f(a')=b$，$\exists a$，使得 $aN=a'N$ 且 $aN\in G/N$，使得 $\delta(aN)=\delta(a'N)=f(a')=f(a)$，从而 δ 是满射。
- 若由 $aN\neq bN$ 但 $\delta(aN)=f(a)=f(b)=\delta(bN)$，则 $e'=f(a)\circ(f(b))^{-1}=f(a*b^{-1})$，从而 $a*b^{-1}\in\ker f=N$，所以 $aN=bN$，矛盾，从而 δ 是单射。

综上，δ 为同构映射，从而 $G/N\cong f(G)$。

【引理8.1】 若 A,B 是 G 的子群且满足 $AB=BA$，则 AB 也是 G 的子群。

证明：$\forall a_1*b_1,a_2*b_2\in AB$，由
$(a_1*b_1)*(a_2*b_2)^{-1}=a_1*b_1*b_2^{-1}*a_2^{-1}\in ABA=AAB=AB$ 及 $AB\subseteq G$，根据【定理4.3】，$AB\leq G$。

【定理8.7】（第一同构定理）若 A 和 B 都是群 G 的子群，且 $B\lhd G$，则 $AB/B\cong A/(A\cap B)$。

证明：

- 根据【定理7.3】，$AB\leq G$ 是群；同时 $A\cap B$ 显然是群。
- $B\lhd G$，$B\subseteq AB\subseteq G$，从而根据定义可知 $B\lhd AB$。
- $\forall b\in A\cap B$，有 $b\in A$ 且 $b\in B$；$\forall a\in A$，$a*b*a^{-1}\in A$，同时由于 $B\lhd G$，且 $A\subseteq G$，根据【定理7.1】，$a\in A\subseteq G$，从而 $a*b*a^{-1}\in B$。综上 $a*b*a^{-1}\in A\cap B$，即 $A\cap B\lhd A$。
- 定义映射 $\delta:A\to AB/B$ 为 $\delta(a)=aB$，首先 δ 是一个同态，$\delta(a*b)=abB=aB\cdot bB=\delta(a)\cdot\delta(b)$；其次 δ 是一个满同态（满同态是为了说明 $\delta(A)=AB/B$）。同时 $\ker\delta=\{a|a\in A,\delta(a)=aB=B\}$，根据陪集的性质【定理6.1】有 $\ker\delta=\{a|a\in A,a\in B\}=A\cap B$，从而由同态基本定理，有
$$A/(A\cap B)=A/\ker\delta\cong\delta(A)=AB/B\Longrightarrow AB/B\cong A/(A\cap B)$$

【引理8.2】（第二同构定理引理）已知群 G,G' 中存在满同态映射 f，且 $H'\lhd G'$，$H=f^{-1}(H')$，则有 $H\lhd G$ 且 $G/H\cong G'/H'$。

证明：

- 根据【定理8.2】，$H\leq G$。此外，$\forall h\in H,g\in G$，$f(g*h*g^{-1})=f(g)\circ f(h)\circ(f(g))^{-1}$，由于 $H'\lhd G'$，从而 $f(g*h*g^{-1})\in H'$，从而 $g*h*g^{-1}\in H$。即 $H\lhd G$。
- 构造映射 $\phi:G'\to G'/H'$ 为自然同态，显然自然同态为满同态，则 $\phi\circ f:G\to G'/H'$ 为满同态。
$\ker\phi\circ f=\{x|x\in G,\phi(f(x))=H'\}=\{x|x\in G,f(x)H'=H'\}=\{x|x\in G,f(x)\in H'\}=|H|$，从而由同态基本定理，$G/\ker\phi\circ f\cong G'/H'$，即 $G/H\cong G'/H'$。

【定理8.8】（第二同构定理）若 $N\lhd G,H\lhd G$，且 $H\subseteq N$，则 $G/N\cong(G/H)/(N/H)$。

证明：首先显然有 $H\lhd N$。

- $N/H\leq G/H$；由于 $N\lhd G$，有 $gng^{-1}\in N$，从而 $gH\cdot nH\cdot g^{-1}H=(gng^{-1})H\in N/H$，从而 $N/H\lhd G/H$。
- 映射 $f:G\to G/H$ 为自然满同态。则 $f^{-1}(N/H)=N$，利用【引理8.2】得 $G/N\cong(G/H)/(N/H)$。

9 群的直积

【定义9.1】（两个群的直积）若 $\langle G_1,*\rangle,\langle G_2,\circ\rangle$ 为两个群，在这两个集合的笛卡尔积上定义二元运算 $(a_1,b_1)\cdot(a_2,b_2)=(a_1*a_2,b_1\circ b_2)$。则 $\langle G_1\times G_2,\cdot\rangle$ 形成群，称为 G_1 和 G_2 的直积，简记为 $G_1\times G_2$。

【定理9.1】 $\langle G_1,*\rangle,\langle G_2,\circ\rangle$ 为两个群，则

- 若 G_1 单位元 e_1，G_2 单位元 e_2，则 $G_1\times G_2$ 有单位元 (e_1,e_2)；
- 若 $(a,b)\in G_1\times G_2$，则 $(a,b)^{-1}=(a^{-1},b^{-1})$；
- 若 G_1,G_2 有限群，则 $G_1\times G_2$ 也是有限群，且 $|G_1\times G_2|=|G_1||G_2|$；
- 若 G_1,G_2 是交换群，则 $G_1\times G_2$ 也是交换群。

证明：(3) 显然；(1) (2) (4) 见【定理2.1】。

【例9.1】用 C_n 表示 n 阶循环群，$(n,s)=1$，证明：$C_n\times C_s\cong C_{ns}$。

证明：$C_n=(a),|a|=n,C_s=(b),|b|=s$，则 $((a,b))$ 为 $C_n\times C_s$ 子群，设 $|(a,b)|=d$ 且单位元 (e_a,e_b)，由于 $(a,b)^{ns}=(a^{ns},b^{ns})=(e,e')$，所以 $d|ns$。又因为 $(e,e')=(a,b)^d=(a^d,b^d)$，所以 $n|d,s|d$。又因为 $(n,s)=1$，所以 $ns|d$。因此 $ns=d$，即 $|((a,b))|=ns$，从而 $((a,b))=C_n\times C_s$，所以 $C_n\times C_s$ 为 ns 阶循环子群，显然 $C_n\times C_s\cong C_{ns}$。

【定义9.2】给定群 G 的 $k(k\geq 2)$ 个子集 $S_1,S_2,\ldots,S_k$，如果 $\forall a\in G$，都存在 $a_i\in S_i(i=1,2,\ldots,k)$，使得 $a=a_1*a_2*\ldots*a_k$，则称 G 中元素可以表示为 $S_1,S_2,\ldots,S_k$ 中元素之积。又若 $\forall a\in G$，若 $a_1*a_2*\ldots*a_k=a=b_1*b_2*\ldots*b_k$ 则有 $a_i=b_i(i=1,2,\ldots,k)$，则称 G 中元素可以唯一表示为 $S_1,S_2,\ldots,S_k$ 中元素之积。

【定理9.2】若 $G_1\leq G,G_2\leq G$，且 G 中元素可表示成 G_1,G_2 元素乘积，则该表示是唯一的，当且仅当

- $G_1\cap G_2=\{e\}$；
- 或 G 的单位元 e 可以唯一的表示成 G_1,G_2 元素乘积。

证明：

- 先证必要性，显然 $e\in G_1,e\in G_2$，从而 $e\in G_1\cap G_2$。若 $\exists a\in G_1\cap G_2$，则 $a^{-1}\in G_1\cap G_2$。则 $e=a*a^{-1}=e*e$，因为表示唯一，所以 $a=a^{-1}=e$，从而 $G_1\cap G_2=\{e\}$。
- 再证充分性，若 $\exists g_1,g_1'\in G_1,g_2,g_2'\in G_2$，使得 $a=g_1*g_2=g_1'*g_2'$，则 $g_1^{-1}*g_1'=g_2\times g_2'^{-1}=t$，从而 $t\in G_1\cap G_2$，则 $t=e$，从而 $g_1=g_1',g_2=g_2'$，即表示唯一。
- 条件二和条件一等价。证明显然。

【定理9.3】若$G_1\leq G,G_2\leq G$，且 G 中的元素可以唯一表示为 G_1,G_2 中元素的乘积，则 $G_1\lhd G,G_2\lhd G$ 等价于 $\forall a\in G_1,b\in G_2,a*b=b*a$。

证明：由【定理9.2】知 $G_1\cap G_2=\{e\}$。

- 若 $G_1\lhd G,G_2\lhd G$，则 $\forall a\in G_1,b\in G_2$，$b^{-1}*a*b\in G_1,a*b*a^{-1}\in G_2$，从而 $(b^{-1}*a*b)*a^{-1}\in G_1$ 同时 $b^{-1}*(a*b*a^{-1})\in G_2$，则 $b^{-1}*a*b*a^{-1}\in G_1\cap G_2$，即 $b^{-1}*a*b*a^{-1}=e$，即 $a*b=b*a$。
- $\forall a\in G_1,t\in G$，有 $t=a'*b$，从而 $t*a*t^{-1}=a'*b*a*b^{-1}*a'^{-1}=a\in G_1$，所以 $G_1\lhd G$。同理 $G_2\lhd G$。

【定义9.3】（内部直积）若 $G_1\lhd G,G_2\lhd G$，且 G 中元素可以唯一表示为 G_1,G_2 中元素的乘积，则称 G 为 G_1,G_2 的内部直积，记作 $G=G_1\times G_2$。

【定理9.4】若 $G=G_1\times G_2$，则 $G\cong G_1\times G_2$。

定义映射 $f:G_1\times G_2\to G$ 为 $f((a,b))=a*b$，则

- $f((a,b)\cdot(c,d))=f(a*c,b*d)=a*c*b*d=a*c*b*d=a*b*c*d=f((a,b))*f((c,d))$

（由【定理9.3】），所以 f 是同态。
- 显然 f 是双射。

综上，$G \cong G_1 \times G_2$。

【定理9.5】 若 $A \lhd G, B \lhd G$ 且 $G = A \times B$，$N \lhd A$，则有 $N \lhd G$ 且 $G/N \cong (A/N) \times B$。

证明：

- $\forall n \in N, x \in G, \exists a \in A, b \in B$，满足 $x = a * b$，从而 $x * n * x^{-1} = a * b * n * b^{-1} * a^{-1} = a * n * a^{-1}$ （运用【定理9.3】），又根据 $N \lhd A$，$x * n * x^{-1} = a * n * a^{-1} \in N$，从而 $N \lhd G$。
- 对任意 $x \in G$，若 $x = a * b(a \in A, b \in B)$，则定义 $f : G \to (A/N) \times B$，令 $f(x) = (aN, b)$，则 $f(x * y) = f(a_1 * b_1 * a_2 * b_2) = f(a_1 * a_2 * b_1 * b_2) = ((a_1 * a_2)N, b_1 * b_2) = (a_1N, b_1) \cdot (a_2N, b_2)$，从而 $f(x * y) = f(x) \cdot f(y)$，因此 f 是同态。又 $\ker f = \{g | g = a * b \in G, a \in A, b \in B, (aN, b) = (N, e)\}$，从而 $\ker f = \{g | g = a * b \in G, a \in A, b \in B, a \in N, b = e\} = N$，显然 f 是满射，由【定理8.6】同态基本定理有 $G/N \cong (A/N) \times B$。

【定义9.4】（有限个群的直积）设 $G_1, G_2, \ldots, G_n$ 为 n 个群，则 $G_1 \times G_2 \times \ldots \times G_n$ 关于 $\cdot$ 运算 $(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \oplus_1 b_1, a_2 \oplus_2 b_2, \ldots, a_n \oplus_n b_n)$ 形成了一个群，称为 $G_1, G_2, \ldots, G_n$的直积，记作 $G_1 \times G_2 \times \ldots \times G_n$。

【定理9.6】（有限个群的直积的性质）类似【定理9.1】，对有限个群的直积也有：

- 若对 $i = 1, 2, \ldots, n$，G_i 单位元 e_i，则 $G_1 \times G_2 \times \ldots \times G_n$ 有单位元 $(e_1, e_2, \ldots, e_n)$；
- 若 $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \ldots \times G_n$，则 $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$；
- 若 $G_i(i = 1, 2, \ldots, n)$ 有限群，则 $G_1 \times G_2 \times \ldots \times G_n$ 是有限群，且 $|G_1 \times G_2 \times \ldots \times G_n| = \prod_{i=1}^{n} |G_i|$；
- 若 $G_i(i = 1, 2, \ldots, n)$ 交换群，则 $G_1 \times G_2 \times \ldots \times G_n$ 是交换群。

证明：和【定理9.1】完全类似。

【定理9.7】 若 G 是其正规子群 $G_1, G_2, \ldots, G_n$ 的内部直积，有 $G \cong G_1 \times G_2 \times \ldots \times G_n$。

证明：和【定理9.4】完全类似。