群的概念

定义 1 (半群)**.** 设集合 S 带有二元运算“$\circ$”，若对任意 $a,b,c\in S$，有 $(a\circ b)\circ c=a\circ(b\circ c)$，则称 $(S,\circ)$ 是**半群**.

定义 2 (幺半群)**.** 设半群 $(M,\circ)$，若存在 $e\in M$，对任意 $a\in M$，有 $e\circ a=a\circ e=a$，则称 $(M,\circ)$ 为**幺半群**，e 称为 $(M,\circ)$ 的**幺元**.

定义 3 (群)**.** 设集合 G 带有二元运算“$\circ$”，满足以下条件：

1. 对任意 $a,b,c\in G$，有 $(a\circ b)\circ c=a\circ(b\circ c)$;
2. 存在 $e\in G$，对任意 $a\in G$，有 $e\circ a=a\circ e=a$;
3. 对任意 $a\in G$，存在 $a^{-1}\in G$，使得 $a\circ a^{-1}=a^{-1}\circ a=e$,

则称 $(G,\circ)$ 是一个**群**.

注. 在不引起歧义的情况下，可以说“设 G 是一个群”，而将运算“$\circ$”看作广义上的“乘法”而省略，即“$a\circ b$”记作“ab”.

注. 称“a^{-1}”为 a 的**逆元**.

定义 4 (交换群)**.** 若 G 中任意元素 a,b 满足 $ab=ba$，则称 G 是**交换群**或 **Abel 群**.

定理 1. 群 G 的幺元是唯一的.

证明. 设 $e,e'\in G$ 都是幺元，则 $e=ee'=e'$. □

定理 2. 群 G 的逆元是唯一的.

证明. 对任意 $a\in G$，设 $b,c\in G$ 是 a 的逆元，则 $b=b(ac)=(ba)c=c$. □

由于结合律成立，则 $a^n=\underbrace{a\circ a\circ\cdots\circ a}_{n\text{个}}$ 是良定义的. 同时有 $a^m a^n=a^{m+n}$，$(a^s)^t=a^{st}$.

定理 3 (消去律)**.** 设 $a,b,c\in G$，若 $ab=ac$，则 $b=c$；若 $ba=ca$，则 $b=c$.

证明. $ab=ac\Rightarrow a^{-1}ab=a^{-1}ac\Rightarrow b=c$，类似地 $ba=ca\Rightarrow baa^{-1}=caa^{-1}\Rightarrow b=c$. □

定义 5 (群的阶)**.** 群 G 中元素的个数称为群的**阶**，记作 $|G|$. 当 $|G|$ 有限时，称 G 为**有限群**，否则称 G 为**无限群**.

定义 6 (群中元素的阶)**.** 设 G 为一个群，$a \in G$，若存在正整数 k 使得 $a^k = e$，则最小的正整数 k 称为 a 的**阶**，记作 $|a|$. 即 $|a| = \min\left\{k \in \mathbb{N}^+ | a^k = e\right\}$. 若不存在这样的 k，则称 a 的阶为无穷.

定理 4. $|a| = \infty \iff \forall m, n \in \mathbb{N}^+, m \neq n, a^m \neq a^n$.

证明. 设 $m.n.k \in \mathbb{N}^+$ 且 $m = n + k$. 则 $|a| = \infty \iff \forall k \in \mathbb{N}^+$，$a^k \neq e \iff a^{m-n} \neq e \iff a^m \neq a^n$. □

定理 5. 设 $|a| = d$，则 $\forall h \in \mathbb{Z}$，$a^h = e \iff d|h$.

证明. 充分性：$d|h$，则存在 $k \in \mathbb{Z}$ 使得 $h = kd$，则 $a^h = a^{kd} = (a^d)^k = e$.

必要性：设 $h = qd + r$，$0 \leqslant r < d$，则 $a^{qd+r} = a^{qd}a^r = a^r = e$，则 $r = 0$. □

推论 1. 对任意 $m, n \in \mathbb{Z}$，$a^m = a^n \iff d|m - n \iff m \equiv n \pmod d$.

定理 6. 设 $|a| = d$，$k \in \mathbb{N}^+$，则 $|a^k| = \dfrac{d}{(d, k)}$.

证明. 设 $|a^k| = h$，则 $a^{kh} = e$. 而 $|a| = d$，则 $d|kh$.

设 $d = d_1(d, k)$，$k = k_1(d, k)$，则 $(d_1, k_1) = 1$，$d_1|k_1h$，则 $d_1|h$.

$(a^k)^{d_1} = a^{kd_1} = a^{dk_1} = e$，故 $h|d_1$. 于是 $|a^k| = h = d_1 = \dfrac{d}{(d, k)}$. □

推论 2. $|a^k| = d \iff (d, k) = 1$.

定理 7. 设 $a, b \in G$，$|a| = m$，$|b| = n$，$ab = ba$，$(m, n) = 1$，则 $|ab| = mn$.

证明. 设 $|ab| = d$，而 $(ab)^{mn} = (a^m)^n(b^n)^m = e$，于是 $d|mn$;

又 $(ab)^{md} = a^{md}b^{md} = b^{md} = e$，故 $n|md$，而 $(m, n) = 1$，于是 $n|d$. 同理 $m|d$，于是 $mn|d$，故 $mn = d$. □