代　　数（二）

School of Computer
Wuhan University

代数（二）内容

1. 群的性质
   - 群的性质
   - 元素的阶
2. 陪集和拉格朗日定理
   - 陪集的定义和性质
   - 拉格朗日定理
   - 陪集关系

群的性质

群

- 群是半群、含幺半群且每个元素都有逆元;
- 半群、含幺半群的所有性质在群中全部成立。

群的性质

群

- 群是半群、含幺半群且每个元素都有逆元;
- 半群、含幺半群的所有性质在群中全部成立。

群的性质（一）

逆元

- 若群$< G, * >$的单位元为e，$\forall a, b \in G$,

① $(a^{-1})^{-1} = a$

② $(a * b)^{-1} = b^{-1} * a^{-1}$

证明：

① $\because a * a^{-1} = e, a^{-1} * a = e,$,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1} = a$;

② $\because (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e$,

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

$\therefore b^{-1} * a^{-1}$是$a * b$的左、右逆元，$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

群的性质（一）

逆元

- 若群$< G, * >$的单位元为e，$\forall a, b \in G$,

① $(a^{-1})^{-1} = a$

② $(a * b)^{-1} = b^{-1} * a^{-1}$

证明：

① $\because a * a^{-1} = e, a^{-1} * a = e,$,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1} = a$;

② $\because (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e$,

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

$\therefore b^{-1} * a^{-1}$是$a * b$的左、右逆元，$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

群的性质（一）

逆元

- 若群$< G, * >$的单位元为e，$\forall a, b \in G$，

① $(a^{-1})^{-1} = a$

② $(a * b)^{-1} = b^{-1} * a^{-1}$

证明：

① $\because a * a^{-1} = e, a^{-1} * a = e$,,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1} = a$;

② $\because (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e$,

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

$\therefore b^{-1} * a^{-1}$是$a * b$的左、右逆元，$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

群的性质（一）

逆元

- 若群$< G, * >$的单位元为e，$\forall a, b \in G$,

① $(a^{-1})^{-1} = a$

② $(a * b)^{-1} = b^{-1} * a^{-1}$

证明：

① $\because a * a^{-1} = e, a^{-1} * a = e,$,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1} = a$;

② $\because (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e,$

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

$\therefore b^{-1} * a^{-1}$是$a * b$的左、右逆元，$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

群的性质（一）

逆元

- 若群$< G, * >$的单位元为e，$\forall a, b \in G$,

① $(a^{-1})^{-1} = a$

② $(a * b)^{-1} = b^{-1} * a^{-1}$

证明：

① $\because a * a^{-1} = e, a^{-1} * a = e,$,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1} = a$;

② $\because (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e,$

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

$\therefore b^{-1} * a^{-1}$是$a * b$的左、右逆元，$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

群的性质（一）

逆元

- 若群$< G, * >$的单位元为e，$\forall a, b \in G$,

① $(a^{-1})^{-1} = a$

② $(a * b)^{-1} = b^{-1} * a^{-1}$

证明：

① $\because a * a^{-1} = e, a^{-1} * a = e,$,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1} = a;$

② $\because (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e,$

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

$\therefore b^{-1} * a^{-1}$是$a * b$的左、右逆元，$\therefore (a * b)^{-1} = b^{-1} * a^{-1}.$

群的性质（一）

逆元

- 若群$<G,*>$的单位元为e，$\forall a,b\in G$,

① $(a^{-1})^{-1}=a$

② $(a*b)^{-1}=b^{-1}*a^{-1}$

证明：

① $\because a*a^{-1}=e, a^{-1}*a=e,$,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1}=a;$

② $\because (a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=a*e*a^{-1}=e,$

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

$\therefore b^{-1}*a^{-1}$是$a*b$的左、右逆元，$\therefore (a*b)^{-1}=b^{-1}*a^{-1}.$

群的性质（一）

逆元

- 若群$< G, * >$的单位元为e，$\forall a, b \in G$,

① $(a^{-1})^{-1} = a$

② $(a * b)^{-1} = b^{-1} * a^{-1}$

证明：

① $\because a * a^{-1} = e, a^{-1} * a = e,$,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1} = a;$

② $\because (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e,$

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

$\therefore b^{-1} * a^{-1}$是$a * b$的左、右逆元，$\therefore (a * b)^{-1} = b^{-1} * a^{-1}$.

群的性质（一）

逆元

- 若群$< G, * >$的单位元为e，$\forall a, b \in G$,

① $(a^{-1})^{-1} = a$

② $(a*b)^{-1} = b^{-1} * a^{-1}$

证明：

① $\because a * a^{-1} = e, a^{-1} * a = e,$,

$\therefore a$是a^{-1}的左、右逆元，$\therefore (a^{-1})^{-1} = a$;

② $\because (a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$

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

$\therefore b^{-1}*a^{-1}$是$a*b$的左、右逆元，$\therefore (a*b)^{-1} = b^{-1}*a^{-1}$.

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明：

① 存在性：令$x = a^{-1} * b$，则
$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$,

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明：

① 存在性：令$x = a^{-1} * b$，则

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

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明:

① 存在性：令$x = a^{-1} * b$，则

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

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明：

① 存在性：令$x = a^{-1} * b$，则

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

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明：

① 存在性：令$x = a^{-1} * b$，则
$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$,

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明：

① 存在性：令$x = a^{-1} * b$，则

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

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明：

① 存在性：令$x = a^{-1} * b$，则
$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$,

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明：

① 存在性：令$x = a^{-1} * b$，则

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

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（二）

方程的解

- 若$< G, * >$是群，则$\forall a, b \in G$,

① 存在惟一的x，使得$a * x = b$;

② 存在惟一的y，使得$y * a = b$;

证明：

① 存在性：令$x = a^{-1} * b$，则
$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$,

惟一性：若$a * x = b$,

则$a^{-1} * (a * x) = a^{-1} * b$,

$\therefore (a^{-1} * a) * x = a^{-1} * b$, 即$x = a^{-1} * b$.

② 同理可证。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元；

  ② 若$|G| > 1$, 且群G中有零元θ,

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元；

  ② 若$|G| > 1$, 且群G中有零元θ，

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元；

  ② 若$|G| > 1$, 且群G中有零元θ，

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元；

  ② 若$|G| > 1$, 且群G中有零元θ,

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元;

  ② 若$|G| > 1$, 且群G中有零元θ,

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元;

  ② 若$|G| > 1$, 且群G中有零元θ,

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。
- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$
- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元；

  ② 若$|G| > 1$, 且群G中有零元θ,

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元；

  ② 若$|G| > 1$, 且群G中有零元θ，

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元；

  ② 若$|G| > 1$, 且群G中有零元θ,

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（三）

性质

- 群中消去律成立。

  证：群的每个元素都可逆，则每个元素都可约，所以消去律成立。

- 单位元是群中唯一的幂等元。

  证：若x是幂等元，则，$x = x * x$

  $$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

- 群中不可能有零元。

  证：① 若$|G| = 1$, 则唯一的元素视为单位元；

  ② 若$|G| > 1$, 且群G中有零元θ，

  则$\forall x \in G, x * \theta = \theta * x = \theta \neq e$,

  所以θ无逆元，与G是群矛盾。

群的性质（四）

性质

- 有限群$< G, * >$的运算表中的每一行（列）是G中元素的一个置换。(有限集合S到S的一个双射，称为S的一个置换。)

证：

① 先证：群G中的任一元素在运算表中的每一行（列）中均出现（满射)：考虑运算表中对应于元素a的那一行，

$\forall b \in G$, 则$b = a * (a^{-1} * b)$, $\therefore$ b出现在a的那一行。

由a, b的任意性，得证；

② 再证：一个元素在运算表中的每一行（列）中不能出现两次(单射)：假设元素k在a的那一行出现两次，

即$k = a * b_1 = a * b_2$, 且$b_1 \neq b_2$, 但与群的可约性矛盾。

③ 因群G中有单位元，$\therefore$任两行（列）均不相同。

群的性质（四）

性质

- 有限群$< G, * >$的运算表中的每一行（列）是G中元素的一个置换。(有限集合S到S的一个双射，称为S的一个置换。)

证：

① 先证：群G中的任一元素在运算表中的每一行（列）中均出现（满射)：考虑运算表中对应于元素a的那一行，

$\forall b \in G$, 则$b = a * (a^{-1} * b)$, $\therefore$ b出现在a的那一行。

由a, b的任意性，得证；

② 再证：一个元素在运算表中的每一行（列）中不能出现两次(单射)：假设元素k在a的那一行出现两次，

即$k = a * b_1 = a * b_2$, 且$b_1 \neq b_2$, 但与群的可约性矛盾。

③ 因群G中有单位元，$\therefore$任两行（列）均不相同。

群的性质（四）

性质

- 有限群$< G, * >$的运算表中的每一行（列）是G中元素的一个置换。（有限集合S到S的一个双射，称为S的一个置换。）

证：

① 先证：群G中的任一元素在运算表中的每一行（列）中均出现（满射）：考虑运算表中对应于元素a的那一行，

$\forall b \in G$, 则$b = a * (a^{-1} * b), \therefore b$出现在$a$的那一行。

由a, b的任意性，得证；

② 再证：一个元素在运算表中的每一行（列）中不能出现两次（单射）：假设元素k在a的那一行出现两次，

即$k = a * b_1 = a * b_2$, 且$b_1 \neq b_2$, 但与群的可约性矛盾。

③ 因群G中有单位元，$\therefore$任两行（列）均不相同。

群的性质（四）

性质

- 有限群$< G, * >$的运算表中的每一行（列）是G中元素的一个置换。(有限集合S到S的一个双射，称为S的一个置换。)

证：

① 先证：群G中的任一元素在运算表中的每一行（列）中均出现（满射)：考虑运算表中对应于元素a的那一行，

$\forall b \in G$, 则$b = a * (a^{-1} * b), \therefore b$出现在$a$的那一行。

由a, b的任意性，得证；

② 再证：一个元素在运算表中的每一行（列）中不能出现两次(单射)：假设元素k在a的那一行出现两次，

即$k = a * b_1 = a * b_2$, 且$b_1 \neq b_2$, 但与群的可约性矛盾。

③ 因群G中有单位元，$\therefore$任两行（列）均不相同。

群的性质（四）

性质

- 有限群$< G, * >$的运算表中的每一行（列）是G中元素的一个置换。(有限集合S到S的一个双射，称为S的一个置换。)

证：

① 先证：群G中的任一元素在运算表中的每一行（列）中均出现（满射）：考虑运算表中对应于元素a的那一行，

$\forall b \in G$, 则$b = a * (a^{-1} * b)$, $\therefore$ b出现在a的那一行。

由a, b的任意性，得证；

② 再证：一个元素在运算表中的每一行（列）中不能出现两次(单射)：假设元素k在a的那一行出现两次，

即$k = a * b_1 = a * b_2$, 且$b_1 \neq b_2$, 但与群的可约性矛盾。

③ 因群G中有单位元，$\therefore$任两行（列）均不相同。

群的性质（四）

性质

- 有限群$< G, * >$的运算表中的每一行（列）是G中元素的一个置换。(有限集合S到S的一个双射，称为S的一个置换。)

证：

① 先证：群G中的任一元素在运算表中的每一行（列）中均出现（满射)：考虑运算表中对应于元素a的那一行，

$\forall b \in G$, 则$b = a * (a^{-1} * b), \therefore b$出现在$a$的那一行。

由a, b的任意性，得证；

② 再证：一个元素在运算表中的每一行（列）中不能出现两次(单射)：假设元素k在a的那一行出现两次，

即$k = a * b_1 = a * b_2$, 且$b_1 \neq b_2$, 但与群的可约性矛盾。

③ 因群G中有单位元，$\therefore$任两行（列）均不相同。

群的性质（四）

性质

- 有限群$< G, * >$的运算表中的每一行（列）是G中元素的一个置换。(有限集合S到S的一个双射，称为S的一个置换。)

证：

① 先证：群G中的任一元素在运算表中的每一行（列）中均出现（满射)：考虑运算表中对应于元素a的那一行，

$\forall b \in G$, 则$b = a * (a^{-1} * b), \therefore b$出现在$a$的那一行。

由a, b的任意性，得证；

② 再证：一个元素在运算表中的每一行（列）中不能出现两次(单射)：假设元素k在a的那一行出现两次，

即$k = a * b_1 = a * b_2$, 且$b_1 \neq b_2$, 但与群的可约性矛盾。

③ 因群G中有单位元，$\therefore$任两行（列）均不相同。

群的性质（四）

性质

- 有限群$< G, * >$的运算表中的每一行（列）是G中元素的一个置换。(有限集合S到S的一个双射，称为S的一个置换。)

证：

① 先证：群G中的任一元素在运算表中的每一行（列）中均出现（满射)：考虑运算表中对应于元素a的那一行，

$\forall b \in G$, 则$b = a * (a^{-1} * b), \therefore b$出现在$a$的那一行。

由a, b的任意性，得证；

② 再证：一个元素在运算表中的每一行（列）中不能出现两次(单射)：假设元素k在a的那一行出现两次，

即$k = a * b_1 = a * b_2$, 且$b_1 \neq b_2$, 但与群的可约性矛盾。

③ 因群G中有单位元，$\therefore$任两行（列）均不相同。

有限群例子

Table：一阶群

$*$	e
e	e

Table：二阶群

$*$	e	a
e	e	a
a	a	e

Table：三阶群

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Table：四阶群(1)

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table：四阶群(2)

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

群的性质（四）

定理

- 群 $< G, * >$，$\forall a \in G$，定义函数 $f_a : G \longrightarrow G$，$x \longmapsto a * x$，则 f_a 是双射。
- 证：

$$
\begin{aligned}
& f_a \circ f_{a^{-1}}(x) \\
= & f_a(f_{a^{-1}}(x)) \\
= & f_a(a^{-1} * x) \\
= & a * a^{-1} * x = x
\end{aligned}
$$

$\therefore$ $f_a \circ f_{a^{-1}} = \mathbb{I}_G$，同理，$f_{a^{-1}} \circ f_a = \mathbb{I}_G$，

$\therefore$ f_a 是双射。

群的性质（四）

定理

- 群$< G, * >$，$\forall a \in G$，定义函数$f_a : G \longrightarrow G$，$x \longmapsto a * x$，则$f_a$是双射。
- 证：

$$
\begin{aligned}
& f_a \circ f_{a^{-1}}(x) \\
=& f_a(f_{a^{-1}}(x)) \\
=& f_a(a^{-1} * x) \\
=& a * a^{-1} * x = x
\end{aligned}
$$

$\therefore$ $f_a \circ f_{a^{-1}} = \mathbb{I}_G$，同理，$f_{a^{-1}} \circ f_a = \mathbb{I}_G$，

$\therefore$ f_a是双射。

群的性质（四）

定理

- 群$< G, * >$，$\forall a \in G$，定义函数$f_a : G \longrightarrow G$，$x \longmapsto a * x$，则$f_a$是双射。
- 证：

$$
\begin{aligned}
& f_a \circ f_{a^{-1}}(x) \\
=& f_a(f_{a^{-1}}(x)) \\
=& f_a(a^{-1} * x) \\
=& a * a^{-1} * x = x
\end{aligned}
$$

$\therefore$ $f_a \circ f_{a^{-1}} = \mathbb{I}_G$，同理，$f_{a^{-1}} \circ f_a = \mathbb{I}_G$，

$\therefore$ f_a是双射。

群的性质（四）

定理

- 群$< G, * >$，$\forall a \in G$，定义函数$f_a : G \longrightarrow G$，$x \longmapsto a * x$，则$f_a$是双射。
- 证：

$$
\begin{aligned}
& f_a \circ f_{a^{-1}}(x) \\
= & f_a(f_{a^{-1}}(x)) \\
= & f_a(a^{-1} * x) \\
= & a * a^{-1} * x = x
\end{aligned}
$$

$\therefore$ $f_a \circ f_{a^{-1}} = \mathbb{I}_G$，同理，$f_{a^{-1}} \circ f_a = \mathbb{I}_G$，

$\therefore$ f_a是双射。

群的性质（四）

定理

- 群$< G, * >$，$\forall a \in G$，定义函数$f_a : G \longrightarrow G$，$x \longmapsto a * x$，则$f_a$是双射。
- 证：

$$
\begin{aligned}
& f_a \circ f_{a^{-1}}(x) \\
= & f_a(f_{a^{-1}}(x)) \\
= & f_a(a^{-1} * x) \\
= & a * a^{-1} * x = x
\end{aligned}
$$

$\therefore\ f_a \circ f_{a^{-1}} = \mathbb{I}_G$，同理，$f_{a^{-1}} \circ f_a = \mathbb{I}_G$，

$\therefore\ f_a$是双射。

例题

例

- 群$< G, * >$是可交换群，iff，
  $\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b)$.
- 证：

  $\Longleftarrow$

  若$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b)$,

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

  $\therefore$由结合律，$b*a = a*b$，群$< G, * >$是可交换群；

  $\Longrightarrow$

  若群$< G, * >$是可交换群，则$\forall a, b \in G, a*b = b*a$,

  $\therefore a*(a*b)*b = a*(b*a)*b$

  $\therefore (a*a)*(b*b) = (a*b)*(a*b)$

例题

例

- 群 $< G, * >$ 是可交换群，iff，$\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$.
- 证：

$\Longleftarrow$

若 $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$,

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

$\therefore$ 由结合律，$b * a = a * b$，群 $< G, * >$ 是可交换群；

$\Longrightarrow$

若群 $< G, * >$ 是可交换群，则 $\forall a, b \in G, a * b = b * a$,

$\therefore a * (a * b) * b = a * (b * a) * b$

$\therefore (a * a) * (b * b) = (a * b) * (a * b)$

例题

例

- 群$< G, * >$是可交换群，iff，
  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$.
- 证：

  $\Longleftarrow$

  若$\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$,

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

  $\therefore$由结合律，$b * a = a * b$，群$< G, * >$是可交换群；

  $\Longrightarrow$

  若群$< G, * >$是可交换群，则$\forall a, b \in G, a * b = b * a$,

  $\therefore a * (a * b) * b = a * (b * a) * b$

  $\therefore (a * a) * (b * b) = (a * b) * (a * b)$

例题

例

- 群$< G, * >$是可交换群，iff，$\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$.
- 证：

$\Longleftarrow$

若$\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$,

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

$\therefore$由结合律，$b * a = a * b$，群$< G, * >$是可交换群；

$\Longrightarrow$

若群$< G, * >$是可交换群，则$\forall a, b \in G, a * b = b * a$,

$\therefore a * (a * b) * b = a * (b * a) * b$

$\therefore (a * a) * (b * b) = (a * b) * (a * b)$

例题

例

- 群 $< G, * >$ 是可交换群，iff，
  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$.
- 证：

  $\Longleftarrow$

  若 $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$,

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

  $\therefore$ 由结合律，$b * a = a * b$，群 $< G, * >$ 是可交换群；

  $\Longrightarrow$

  若群 $< G, * >$ 是可交换群，则 $\forall a, b \in G, a * b = b * a$,

  $\therefore a * (a * b) * b = a * (b * a) * b$

  $\therefore (a * a) * (b * b) = (a * b) * (a * b)$

例题

例

- 群$< G, * >$是可交换群，iff，
  $\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b)$.
- 证：

  $\Longleftarrow$

  若$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b)$,
  $\therefore \; a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1}$,
  $\therefore$由结合律，$b*a = a*b$，群$< G, * >$是可交换群；

  $\Longrightarrow$

  若群$< G, * >$是可交换群，则$\forall a, b \in G, a*b = b*a$,
  $\therefore a*(a*b)*b = a*(b*a)*b$
  $\therefore (a*a)*(b*b) = (a*b)*(a*b)$

例题

例

- 群$< G, * >$是可交换群，iff，
  $\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b)$.
- 证：

  $\Longleftarrow$

  若$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b)$,

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

  $\therefore$由结合律，$b*a = a*b$，群$< G, * >$是可交换群；

  $\Longrightarrow$

  若群$< G, * >$是可交换群，则$\forall a, b \in G, a*b = b*a$,

  $\therefore a*(a*b)*b = a*(b*a)*b$

  $\therefore (a*a)*(b*b) = (a*b)*(a*b)$

例题

例

- 群$< G, * >$是可交换群，iff，
  $\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b)$.
- 证：

$\Longleftarrow$

若$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b)$,

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

$\therefore$由结合律，$b*a = a*b$，群$< G, * >$是可交换群；

$\Longrightarrow$

若群$< G, * >$是可交换群，则$\forall a, b \in G, a*b = b*a$,

$\therefore a*(a*b)*b = a*(b*a)*b$

$\therefore (a*a)*(b*b) = (a*b)*(a*b)$

例题

例

- 群 $< G, * >$ 是可交换群，iff，
  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$.
- 证：

$\Longleftarrow$

若 $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$,

$\therefore \; a^{-1} * (a * b) * (a * b) * b^{-1} = a^{-1} * (a * a) * (b * b) * b^{-1}$,

$\therefore$ 由结合律，$b * a = a * b$，群 $< G, * >$ 是可交换群；

$\Longrightarrow$

若群 $< G, * >$ 是可交换群，则 $\forall a, b \in G, a * b = b * a$,

$\therefore a * (a * b) * b = a * (b * a) * b$

$\therefore (a * a) * (b * b) = (a * b) * (a * b)$

例题

例

- 群$< G, * >$是可交换群，iff，
  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证：

  $\Longleftarrow$

  若$\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b)$,

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

  $\therefore$由结合律，$b * a = a * b$，群$< G, * >$是可交换群；

  $\Longrightarrow$

  若群$< G, * >$是可交换群，则$\forall a, b \in G, a * b = b * a$,

  $\therefore a * (a * b) * b = a * (b * a) * b$

  $\therefore (a * a) * (b * b) = (a * b) * (a * b)$

元素的幂

定义-元素的幂

- 设群$< G, * >$，$\forall a \in G$，a的整数次幂可以归纳定义为：
  ① $a^0 = e$;
  ② $a^{n+1} = a^n * a, (n \in \mathbb{N})$;
  ③ $a^{-n} = a^{-1} * a^{-1} * \ldots * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质：
  ① $a^m * a^n = a^{m+n}$,
  ② $(a^m)^n = a^{mn}$,　$(m, n \in \mathbb{Z})$

元素的幂

定义-元素的幂

- 设群$< G, * >$，$\forall a \in G$，a的整数次幂可以归纳定义为：
  ① $a^0 = e$;
  ② $a^{n+1} = a^n * a, (n \in \mathbb{N})$;
  ③ $a^{-n} = a^{-1} * a^{-1} * \dots * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质：
  ① $a^m * a^n = a^{m+n}$,
  ② $(a^m)^n = a^{mn}, \quad (m, n \in \mathbb{Z})$

元素的幂

定义-元素的幂

- 设群$< G, * >$，$\forall a \in G$，a的整数次幂可以归纳定义为：
  ① $a^0 = e$;
  ② $a^{n+1} = a^n * a, (n \in \mathbb{N})$;
  ③ $a^{-n} = a^{-1} * a^{-1} * \ldots * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质：
  ① $a^m * a^n = a^{m+n}$,
  ② $(a^m)^n = a^{mn}$, $(m, n \in \mathbb{Z})$

元素的幂

定义-元素的幂

- 设群$< G, * >$，$\forall a \in G$，a的整数次幂可以归纳定义为：
  ① $a^0 = e$;
  ② $a^{n+1} = a^n * a, (n \in \mathbb{N})$;
  ③ $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质：
  ① $a^m * a^n = a^{m+n}$,
  ② $(a^m)^n = a^{mn}$,　$(m, n \in \mathbb{Z})$

元素的幂

定义-元素的幂

- 设群$< G, * >$，$\forall a \in G$，a的整数次幂可以归纳定义为：

  ① $a^0 = e$;

  ② $a^{n+1} = a^n * a, (n \in \mathbb{N})$;

  ③ $a^{-n} = a^{-1} * a^{-1} * \ldots * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$

- 性质：

  ① $a^m * a^n = a^{m+n}$,

  ② $(a^m)^n = a^{mn}, \quad (m, n \in \mathbb{Z})$

元素的幂

定义-元素的幂

- 设群$< G, * >$，$\forall a \in G$，a的整数次幂可以归纳定义为：

  ① $a^0 = e$;

  ② $a^{n+1} = a^n * a, (n \in \mathbb{N})$;

  ③ $a^{-n} = a^{-1} * a^{-1} * \ldots * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$

- 性质：

  ① $a^m * a^n = a^{m+n}$,

  ② $(a^m)^n = a^{mn}, \quad (m, n \in \mathbb{Z})$

元素的幂

定义-元素的幂

- 设群$< G, * >$，$\forall a \in G$，a的整数次幂可以归纳定义为：

  ① $a^0 = e$;

  ② $a^{n+1} = a^n * a, (n \in \mathbb{N})$;

  ③ $a^{-n} = a^{-1} * a^{-1} * \ldots * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$

- 性质：

  ① $a^m * a^n = a^{m+n}$,

  ② $(a^m)^n = a^{mn}, \quad (m, n \in \mathbb{Z})$

元素的阶

定义-元素的阶

- 设$< G, *, e >$是群，$a \in G$，若存在正整数n，使得$a^n = e$，满足上式的最小正整数n称为元素a的阶，并称元素a具有有限阶n，记为$|a| = n$.
- 若不存在这样的正整数n，则称元素a具有无限阶。

例

- 单位元e的阶为1，且单位元是阶为1的唯一元素。
- 群$< \mathbb{Z}, +, 0 >$中，除单位元0外，其余元素均为无限阶.
- $< \mathbb{N}_4, +_4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.$

元素的阶

定义-元素的阶

- 设$< G, *, e >$是群，$a \in G$，若存在正整数n，使得$a^n = e$，满足上式的最小正整数n称为元素a的阶，并称元素a具有有限阶n，记为$|a| = n$.
- 若不存在这样的正整数n，则称元素a具有无限阶。

例

- 单位元e的阶为1，且单位元是阶为1的唯一元素。
- 群$< \mathbb{Z}, +, 0 >$中，除单位元0外，其余元素均为无限阶.
- $< \mathbb{N}_4, +_4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.$

元素的阶

定义-元素的阶

- 设$< G, *, e >$是群，$a \in G$，若存在正整数n，使得$a^n = e$，满足上式的最小正整数n称为元素a的阶，并称元素a具有有限阶n，记为$|a| = n$.
- 若不存在这样的正整数n，则称元素a具有无限阶。

例

- 单位元e的阶为1，且单位元是阶为1的唯一元素。
- 群$< \mathbb{Z}, +, 0 >$中，除单位元0外，其余元素均为无限阶.
- $< \mathbb{N}_4, +_4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.$

元素的阶

定义-元素的阶

- 设$< G, *, e >$是群，$a \in G$，若存在正整数n，使得$a^n = e$，满足上式的最小正整数n称为元素a的阶，并称元素a具有有限阶n，记为$|a| = n$.
- 若不存在这样的正整数n，则称元素a具有无限阶。

例

- 单位元e的阶为1，且单位元是阶为1的唯一元素。
- 群$< \mathbb{Z}, +, 0 >$中，除单位元0外，其余元素均为无限阶.
- $< \mathbb{N}_4, +_4, 0 >$, $|0| = 1, |1| = 4, |2| = 2, |3| = 4$.

元素的阶

定义-元素的阶

- 设$< G, *, e >$是群，$a \in G$，若存在正整数n，使得$a^n = e$，满足上式的最小正整数n称为元素a的阶，并称元素a具有有限阶n，记为$|a| = n$.
- 若不存在这样的正整数n，则称元素a具有无限阶。

例

- 单位元e的阶为1，且单位元是阶为1的唯一元素。
- 群$< \mathbb{Z}, +, 0 >$中，除单位元0外，其余元素均为无限阶.
- $< \mathbb{N}_4, +_4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.$

元素阶的性质（一）

定理

- 群$< G, *, e >$中，$|a| = n$，则 $a^k = e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k = mn, m \in \mathbb{Z}$,
则$a^k = a^{mn} = (a^n)^m = e^m = e$.

$\Longrightarrow$

若$a^k = e$，设$k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$,
$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$.
$\because n$是使$a^n = e$的最小正整数，又$0 \leqslant t < n$,
$\therefore t = 0, k = mn$.

元素阶的性质（一）

定理

- 群 $< G, *, e >$ 中，$|a| = n$，则 $a^k = e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若 $n|k$，即 $k = mn, m \in \mathbb{Z}$,
则 $a^k = a^{mn} = (a^n)^m = e^m = e$.

$\Longrightarrow$

若 $a^k = e$，设 $k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$,
$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$.
$\because n$ 是使 $a^n = e$ 的最小正整数，又 $0 \leqslant t < n$,
$\therefore t = 0, k = mn$.

元素阶的性质（一）

定理

- 群$< G, *, e >$中，$|a| = n$，则 $a^k = e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k = mn, m \in \mathbb{Z}$,

则$a^k = a^{mn} = (a^n)^m = e^m = e$.

$\Longrightarrow$

若$a^k = e$，设$k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$,

$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$.

$\because n$是使$a^n = e$的最小正整数，又$0 \leqslant t < n$,

$\therefore t = 0, k = mn$.

元素阶的性质（一）

定理

- 群$< G, *, e >$中，$|a| = n$，则 $a^k = e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k = mn, m \in \mathbb{Z}$,

则$a^k = a^{mn} = (a^n)^m = e^m = e$.

$\Longrightarrow$

若$a^k = e$，设$k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$,

$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$.

$\because n$是使$a^n = e$的最小正整数，又$0 \leqslant t < n$,

$\therefore t = 0, k = mn$.

元素阶的性质（一）

定理

- 群$< G, *, e >$中，$|a| = n$，则 $a^k = e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k = mn, m \in \mathbb{Z}$,
则$a^k = a^{mn} = (a^n)^m = e^m = e$.

$\Longrightarrow$

若$a^k = e$，设$k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$,
$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$.
$\because n$是使$a^n = e$的最小正整数，又$0 \leqslant t < n$,
$\therefore t = 0, k = mn$.

元素阶的性质（一）

定理

- 群$< G, *, e >$中，$|a| = n$，则 $a^k = e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k = mn, m \in \mathbb{Z}$,

则$a^k = a^{mn} = (a^n)^m = e^m = e$.

$\Longrightarrow$

若$a^k = e$，设$k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$,

$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$.

$\because n$是使$a^n = e$的最小正整数，又$0 \leqslant t < n$,

$\therefore t = 0, k = mn$.

元素阶的性质（一）

定理

- 群$<G,*,e>$中，$|a|=n$，则 $a^k=e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k=mn, m\in\mathbb{Z}$,

则$a^k=a^{mn}=(a^n)^m=e^m=e$.

$\Longrightarrow$

若$a^k=e$，设$k=mn+t, 0\leqslant t<n, m\in\mathbb{Z}$,

$\therefore a^t=a^{k-mn}=a^k*(a^n)^{-m}=e*e^{-m}=e$.

$\because n$是使$a^n=e$的最小正整数，又$0\leqslant t<n$,

$\therefore t=0, k=mn$.

元素阶的性质（一）

定理

- 群$< G, *, e >$中，$|a| = n$，则 $a^k = e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k = mn, m \in \mathbb{Z}$,

则$a^k = a^{mn} = (a^n)^m = e^m = e$.

$\Longrightarrow$

若$a^k = e$，设$k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$,

$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$.

$\because n$是使$a^n = e$的最小正整数，又$0 \leqslant t < n$,

$\therefore t = 0, k = mn$.

元素阶的性质（一）

定理

- 群$<G,*,e>$中，$|a|=n$，则 $a^k=e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k=mn, m\in\mathbb{Z}$,

则$a^k=a^{mn}=(a^n)^m=e^m=e$.

$\Longrightarrow$

若$a^k=e$，设$k=mn+t, 0\leqslant t<n, m\in\mathbb{Z}$,

$\therefore a^t=a^{k-mn}=a^k*(a^n)^{-m}=e*e^{-m}=e$.

$\because n$是使$a^n=e$的最小正整数，又$0\leqslant t<n$,

$\therefore t=0, k=mn$.

元素阶的性质（一）

定理

- 群$<G,*,e>$中，$|a|=n$，则 $a^k=e$, **iff**, $n|k$.
- 证明：

$\Longleftarrow$

若$n|k$，即 $k=mn, m\in\mathbb{Z}$,

则$a^k=a^{mn}=(a^n)^m=e^m=e$.

$\Longrightarrow$

若$a^k=e$，设$k=mn+t, 0\leqslant t<n, m\in\mathbb{Z}$,

$\therefore a^t=a^{k-mn}=a^k*(a^n)^{-m}=e*e^{-m}=e$.

$\because n$是使$a^n=e$的最小正整数，又$0\leqslant t<n$,

$\therefore t=0, k=mn$.

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

  设群 $< G, *, e >$ 中，$a \in G$,

  ① 若元素 a 具有有限阶，设 $|a| = n$,

  $\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

  则 a^{-1} 也具有有限阶，设为 m，则 $m \leqslant n$,

  又 $\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

  所以 $m = n$;

  ② 若元素 a 具有无限阶，

  易证不存在正整数 m 使得 $(a^{-1})^m = e$，即 a^{-1} 也具有无限阶；

  所以，元素 a 和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

设群$< G, *, e >$中，$a \in G$,

① 若元素a具有有限阶，设$|a| = n$,

$\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

则a^{-1}也具有有限阶，设为m，则$m \leqslant n$,

又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

所以$m = n$;

② 若元素a具有无限阶，

易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

设群$< G, *, e >$中，$a \in G$,

① 若元素a具有有限阶，设$|a| = n$,

$\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

则a^{-1}也具有有限阶，设为m，则$m \leqslant n$,

又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

所以$m = n$;

② 若元素a具有无限阶，

易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

设群$< G, *, e >$中，$a \in G$,

① 若元素a具有有限阶，设$|a| = n$,

$\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

则a^{-1}也具有有限阶，设为m，则$m \leqslant n$,

又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

所以$m = n$;

② 若元素a具有无限阶，

易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

设群$< G, *, e >$中，$a \in G$，

① 若元素a具有有限阶，设$|a| = n$，

$\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$，

则a^{-1}也具有有限阶，设为m，则$m \leqslant n$，

又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$，

所以$m = n$；

② 若元素a具有无限阶，

易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

  设群$< G, *, e >$中，$a \in G$,

  ① 若元素a具有有限阶，设$|a| = n$,

  $\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

  则a^{-1}也具有有限阶，设为m，则$m \leqslant n$,

  又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

  所以$m = n$;

  ② 若元素a具有无限阶，

  易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

  所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

设群$< G, *, e >$中，$a \in G$,

① 若元素a具有有限阶，设$|a| = n$,

$\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

则a^{-1}也具有有限阶，设为m，则$m \leqslant n$,

又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

所以$m = n$;

② 若元素a具有无限阶，

易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

设群$< G, *, e >$中，$a \in G$,

① 若元素a具有有限阶，设$|a| = n$,

$\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

则a^{-1}也具有有限阶，设为m，则$m \leqslant n$,

又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

所以$m = n$;

② 若元素a具有无限阶，

易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

设群$< G, *, e >$中，$a \in G$,

① 若元素a具有有限阶，设$|a| = n$,

$\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

则a^{-1}也具有有限阶，设为m，则$m \leqslant n$,

又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

所以$m = n$;

② 若元素a具有无限阶，

易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

  设群$< G, *, e >$中，$a \in G$，

  ① 若元素a具有有限阶，设$|a| = n$，

  $\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$，

  则a^{-1}也具有有限阶，设为m，则$m \leqslant n$，

  又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$，

  所以$m = n$；

  ② 若元素a具有无限阶，

  易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

  所以，元素a和其逆元有相同的阶。

元素阶的性质（二）

定理

- 群中任一元素和其逆元具有相同的阶。
- 证明：

设群$< G, *, e >$中，$a \in G$,

① 若元素a具有有限阶，设$|a| = n$,

$\because (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$,

则a^{-1}也具有有限阶，设为m，则$m \leqslant n$,

又$\because a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, \therefore n \leqslant m$,

所以$m = n$;

② 若元素a具有无限阶，

易证不存在正整数m使得$(a^{-1})^m = e$，即a^{-1}也具有无限阶；

所以，元素a和其逆元有相同的阶。

元素阶的性质（三）

定理

- 在有限群$<G, *, e>$中，设$|G| = n$，则任一元素具有有限阶，且阶至多为n.
- 证明：

  $\forall a \in G$, 在序列$a, a^2, a^3, ..., a^{n+1}$中至少有两个元素相等，

  不妨设$a^r = a^s, 1 \leqslant r < s \leqslant n+1$,

  则 $a^{-r} = a^{-s}$,

  则 $a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$

  所以，元素a的阶至多为$s - r \leqslant n$.

元素阶的性质（三）

定理

- 在有限群$< G, *, e >$中，设$|G| = n$，则任一元素具有有限阶，且阶至多为n.
- 证明：

  $\forall a \in G$, 在序列$a, a^2, a^3, ..., a^{n+1}$中至少有两个元素相等，

  不妨设$a^r = a^s, 1 \leqslant r < s \leqslant n+1$,

  则 $a^{-r} = a^{-s}$,

  则 $a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$

  所以，元素a的阶至多为$s - r \leqslant n$.

元素阶的性质（三）

定理

- 在有限群$< G, *, e >$中，设$|G| = n$，则任一元素具有有限阶，且阶至多为n.
- 证明：

  $\forall a \in G$, 在序列$a, a^2, a^3, \ldots, a^{n+1}$中至少有两个元素相等，

  不妨设$a^r = a^s, 1 \leqslant r < s \leqslant n+1$,

  则 $a^{-r} = a^{-s}$,

  则 $a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$

  所以，元素a的阶至多为$s - r \leqslant n$.

元素阶的性质（三）

定理

- 在有限群$< G, *, e >$中，设$|G| = n$，则任一元素具有有限阶，且阶至多为n.
- 证明：

  $\forall a \in G$, 在序列$a, a^2, a^3, ..., a^{n+1}$中至少有两个元素相等，

  不妨设$a^r = a^s, 1 \leqslant r < s \leqslant n+1$,

  则 $a^{-r} = a^{-s}$,

  则 $a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$

  所以，元素a的阶至多为$s - r \leqslant n$.

元素阶的性质（三）

定理

- 在有限群$< G, *, e >$中，设$|G| = n$，则任一元素具有有限阶，且阶至多为n.
- 证明：

  $\forall a \in G$, 在序列$a, a^2, a^3, ..., a^{n+1}$中至少有两个元素相等，

  不妨设$a^r = a^s, 1 \leqslant r < s \leqslant n+1$,

  则 $a^{-r} = a^{-s}$,

  则 $a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$

  所以，元素a的阶至多为$s - r \leqslant n$.

元素阶的性质（三）

定理

- 在有限群$<G,*,e>$中，设$|G|=n$，则任一元素具有有限阶，且阶至多为n.
- 证明：

  $\forall a\in G$, 在序列$a,a^2,a^3,\dots,a^{n+1}$中至少有两个元素相等，

  不妨设$a^r=a^s, 1\leqslant r<s\leqslant n+1$,

  则 $a^{-r}=a^{-s}$,

  则 $a^{s-r}=a^s*a^{-r}=a^s*a^{-s}=e$

  所以，元素a的阶至多为$s-r\leqslant n$.

元素阶的性质（三）

定理

- 在有限群$< G, *, e >$中，设$|G| = n$，则任一元素具有有限阶，且阶至多为n.
- 证明：

  $\forall a \in G$, 在序列$a, a^2, a^3, ..., a^{n+1}$中至少有两个元素相等，

  不妨设$a^r = a^s, 1 \leqslant r < s \leqslant n+1$,

  则 $a^{-r} = a^{-s}$,

  则 $a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$

  所以，元素a的阶至多为$s - r \leqslant n$.

元素阶的性质（四）

定理

- 群$< G, *, e >$中，$a \in G$ $|a| = n$, 则$|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$. 特别的，$|a^{-1}| = |a|$.
- 证明：

  设$|a^k| = m$，则$a^{km} = e$,

  $\therefore n|km$，即$\frac{n}{(k,n)}|\frac{km}{(k,n)}$,

  而$\frac{n}{(k,n)}$与$\frac{k}{(k,n)}$互质，故$\frac{n}{(k,n)}|m$,

  又$\because (a^k)^{\frac{n}{(k,n)}} = (a^n)^{\frac{k}{(k,n)}} = e$,

  $\therefore m|\frac{n}{(k,n)}$

  又$m, \frac{n}{(k,n)} \in \mathbb{Z}_+, \therefore m = \frac{n}{(k,n)}$.

元素阶的性质（四）

定理

- 群$<G,*,e>$中，$a\in G$ $|a|=n$, 则$|a^k|=\frac{n}{(k,n)}, (k\in\mathbb{Z})$. 特别的，$|a^{-1}|=|a|$.
- 证明：

  设$|a^k|=m$，则$a^{km}=e$,

  $\therefore n|km$，即$\frac{n}{(k,n)}|\frac{km}{(k,n)}$,

  而$\frac{n}{(k,n)}$与$\frac{k}{(k,n)}$互质，故$\frac{n}{(k,n)}|m$,

  又$\because (a^k)^{\frac{n}{(k,n)}}=(a^n)^{\frac{k}{(k,n)}}=e$,

  $\therefore m|\frac{n}{(k,n)}$

  又$m,\frac{n}{(k,n)}\in\mathbb{Z}_+, \therefore m=\frac{n}{(k,n)}$.

元素阶的性质（四）

定理

- 群$< G, *, e >$中，$a \in G$ $|a| = n$, 则$|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$. 特别的，$|a^{-1}| = |a|$.
- 证明：

  设$|a^k| = m$，则$a^{km} = e$,

  $\therefore n | km$，即$\frac{n}{(k,n)} | \frac{km}{(k,n)}$,

  而$\frac{n}{(k,n)}$与$\frac{k}{(k,n)}$互质，故$\frac{n}{(k,n)} | m$,

  又$\because (a^k)^{\frac{n}{(k,n)}} = (a^n)^{\frac{k}{(k,n)}} = e$,

  $\therefore m | \frac{n}{(k,n)}$

  又$m, \frac{n}{(k,n)} \in \mathbb{Z}_+, \therefore m = \frac{n}{(k,n)}$.

元素阶的性质（四）

定理

- 群$< G, *, e >$中，$a \in G$ $|a| = n$, 则$|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$. 特别的，$|a^{-1}| = |a|$.
- 证明：

  设$|a^k| = m$，则$a^{km} = e$,

  $\therefore n | km$，即$\frac{n}{(k,n)} | \frac{km}{(k,n)}$,

  而$\frac{n}{(k,n)}$与$\frac{k}{(k,n)}$互质，故$\frac{n}{(k,n)} | m$,

  又$\because (a^k)^{\frac{n}{(k,n)}} = (a^n)^{\frac{k}{(k,n)}} = e$,

  $\therefore m | \frac{n}{(k,n)}$

  又$m, \frac{n}{(k,n)} \in \mathbb{Z}_+, \therefore m = \frac{n}{(k,n)}$.

元素阶的性质（四）

定理

- 群$<G,*,e>$中，$a\in G$ $|a|=n$, 则$|a^k|=\frac{n}{(k,n)}, (k\in\mathbb{Z})$. 特别的，$|a^{-1}|=|a|$.
- 证明：

  设$|a^k|=m$，则$a^{km}=e$,

  $\therefore n|km$，即$\frac{n}{(k,n)}|\frac{km}{(k,n)}$,

  而$\frac{n}{(k,n)}$与$\frac{k}{(k,n)}$互质，故$\frac{n}{(k,n)}|m$,

  又$\because (a^k)^{\frac{n}{(k,n)}}=(a^n)^{\frac{k}{(k,n)}}=e$,

  $\therefore m|\frac{n}{(k,n)}$

  又$m, \frac{n}{(k,n)}\in\mathbb{Z}_+, \therefore m=\frac{n}{(k,n)}$.

元素阶的性质（四）

定理

- 群$< G, *, e >$中，$a \in G$ $|a| = n$, 则$|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$. 特别的，$|a^{-1}| = |a|$.
- 证明：

  设$|a^k| = m$，则$a^{km} = e$,

  $\therefore n|km$，即$\frac{n}{(k,n)} | \frac{km}{(k,n)}$,

  而$\frac{n}{(k,n)}$与$\frac{k}{(k,n)}$互质，故$\frac{n}{(k,n)}|m$,

  又$\because (a^k)^{\frac{n}{(k,n)}} = (a^n)^{\frac{k}{(k,n)}} = e$,

  $\therefore m|\frac{n}{(k,n)}$

  又$m, \frac{n}{(k,n)} \in \mathbb{Z}_+, \therefore m = \frac{n}{(k,n)}$.

元素阶的性质（四）

定理

- 群$< G, *, e >$中，$a \in G$ $|a| = n$, 则$|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$. 特别的，$|a^{-1}| = |a|$.
- 证明：

  设$|a^k| = m$，则$a^{km} = e$,

  $\therefore n|km$，即$\frac{n}{(k,n)} | \frac{km}{(k,n)}$,

  而$\frac{n}{(k,n)}$与$\frac{k}{(k,n)}$互质，故$\frac{n}{(k,n)}|m$,

  又$\because (a^k)^{\frac{n}{(k,n)}} = (a^n)^{\frac{k}{(k,n)}} = e$,

  $\therefore m|\frac{n}{(k,n)}$

  又$m, \frac{n}{(k,n)} \in \mathbb{Z}_+, \therefore m = \frac{n}{(k,n)}$.

元素阶的性质（四）

定理

- 群$< G, *, e >$中，$a \in G$ $|a| = n$, 则$|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$. 特别的，$|a^{-1}| = |a|$.
- 证明：

  设$|a^k| = m$，则$a^{km} = e$,

  $\therefore n|km$，即$\frac{n}{(k,n)}|\frac{km}{(k,n)}$,

  而$\frac{n}{(k,n)}$与$\frac{k}{(k,n)}$互质，故$\frac{n}{(k,n)}|m$,

  又$\because (a^k)^{\frac{n}{(k,n)}} = (a^n)^{\frac{k}{(k,n)}} = e$,

  $\therefore m|\frac{n}{(k,n)}$

  又$m, \frac{n}{(k,n)} \in \mathbb{Z}_+, \therefore m = \frac{n}{(k,n)}$.

内容

陪集

定义-左陪集（右陪集）

- 设$< H, * >$是群$< G, * >$的子群，
- 集合$a * H \triangleq \{a * h | h \in H\}$为元素$a \in G$所确定的$H$的左陪集。左陪集$a * H$可简记为$aH$. 元素$a$为左陪集$aH$的表示元素.
- 集合$H * a \triangleq \{h * a | h \in H\}$为元素$a \in G$所确定的$H$的右陪集。右陪集$H * a$可简记为$Ha$. 元素$a$为右陪集$Ha$的表示元素.

陪集

定义-左陪集（右陪集）

- 设$< H, * >$是群$< G, * >$的子群，
- 集合$a * H \triangleq \{a * h | h \in H\}$为元素$a \in G$所确定的$H$的左陪集。左陪集$a * H$可简记为$aH$. 元素$a$为左陪集$aH$的表示元素.
- 集合$H * a \triangleq \{h * a | h \in H\}$为元素$a \in G$所确定的$H$的右陪集。右陪集$H * a$可简记为$Ha$. 元素$a$为右陪集$Ha$的表示元素.

陪集

定义-左陪集（右陪集）

- 设$< H, * >$是群$< G, * >$的子群，
- 集合$a * H \triangleq \{a * h | h \in H\}$为元素$a \in G$所确定的$H$的左陪集。左陪集$a * H$可简记为$aH$. 元素$a$为左陪集$aH$的表示元素.
- 集合$H * a \triangleq \{h * a | h \in H\}$为元素$a \in G$所确定的$H$的右陪集。右陪集$H * a$可简记为$Ha$. 元素$a$为右陪集$Ha$的表示元素.

3次对称群的子群、陪集（1/2）

例　S_3的左陪集

- $S_3 = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{(旋转)}\right.$
  $\left.\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{(翻转)}\right\}$
  $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$
- 3次对称群$< S_3, \circ >$，$H = \{\mathbb{I}, d\}$是群S_3的一个子群。

H的所有的左陪集为：

- $\mathbb{I}H = \{\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d\} = \{\mathbb{I}, d\}$　$dH = \{d \circ \mathbb{I}, d \circ d\} = \{d, \mathbb{I}\}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$　$aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$　$a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（1/2）

例　S_3的左陪集

- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{(旋转)} \right.$
  $\left. \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{(翻转)} \right\}$
  $\triangleq \{\mathbb{I}, a, a^2, b, c, d\}$;
- 3次对称群$< S_3, \circ >$，$H = \{\mathbb{I}, d\}$是群S_3的一个子群。

H的所有的左陪集为：

- $\mathbb{I}H = \{\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d\} = \{\mathbb{I}, d\}$　$dH = \{d \circ \mathbb{I}, d \circ d\} = \{d, \mathbb{I}\}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$　$aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$　$a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（1/2）

例 S_3的左陪集

- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{(旋转)} \right.$
  $\left. \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{(翻转)} \right\}$
  $\triangleq \{\mathbb{I}, a, a^2, b, c, d\}$;
- 3次对称群$< S_3, \circ >$，$H = \{\mathbb{I}, d\}$是群S_3的一个子群。

H的所有的左陪集为：

- $\mathbb{I}H = \{\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d\} = \{\mathbb{I}, d\}$ $\quad dH = \{d \circ \mathbb{I}, d \circ d\} = \{d, \mathbb{I}\}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$ $\quad aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$ $\quad a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（1/2）

例 S_3的左陪集

- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{(旋转)} \right.$ $\left. \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{(翻转)} \right\}$
  $\triangleq \{\mathbb{I}, a, a^2, b, c, d\}$;
- 3次对称群$< S_3, \circ >$，$H = \{\mathbb{I}, d\}$是群S_3的一个子群。

H的所有的左陪集为：

- $\mathbb{I}H = \{\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d\} = \{\mathbb{I}, d\}$ $dH = \{d \circ \mathbb{I}, d \circ d\} = \{d, \mathbb{I}\}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$ $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$ $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（1/2）

例　S_3的左陪集

- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{(旋转)} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{(翻转)} \right\}$
  $\triangleq \{\mathbb{I}, a, a^2, b, c, d\}$;
- 3次对称群$< S_3, \circ >$，$H = \{\mathbb{I}, d\}$是群S_3的一个子群。

H的所有的左陪集为：

- $\mathbb{I}H = \{\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d\} = \{\mathbb{I}, d\}$　$dH = \{d \circ \mathbb{I}, d \circ d\} = \{d, \mathbb{I}\}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$　$aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$　$a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（1/2）

例 S_3的左陪集

- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{(旋转)} \right.$
  $\left. \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{(翻转)} \right\}$
  $\triangleq \{\mathbb{I}, a, a^2, b, c, d\}$;
- 3次对称群$< S_3, \circ >$，$H = \{\mathbb{I}, d\}$是群S_3的一个子群。

H的所有的左陪集为：

- $\mathbb{I}H = \{\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d\} = \{\mathbb{I}, d\}$ $dH = \{d \circ \mathbb{I}, d \circ d\} = \{d, \mathbb{I}\}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$ $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$ $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（1/2）

例 S_3的左陪集

- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{(旋转)} \right.$
  $\left. \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{(翻转)} \right\}$
  $\triangleq \{\mathbb{I}, a, a^2, b, c, d\}$;
- 3次对称群$< S_3, \circ >$，$H = \{\mathbb{I}, d\}$是群S_3的一个子群。

H的所有的左陪集为：

- $\mathbb{I}H = \{\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d\} = \{\mathbb{I}, d\}$ $\quad dH = \{d \circ \mathbb{I}, d \circ d\} = \{d, \mathbb{I}\}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$ $\quad aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$ $\quad a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（1/2）

例 S_3的左陪集

- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{(旋转)} \right.$
  $\left. \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{(翻转)} \right\}$
  $\triangleq \{\mathbb{I}, a, a^2, b, c, d\}$;
- 3次对称群$< S_3, \circ >$，$H = \{\mathbb{I}, d\}$是群S_3的一个子群。

H的所有的左陪集为：

- $\mathbb{I}H = \{\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d\} = \{\mathbb{I}, d\}$ $\quad dH = \{d \circ \mathbb{I}, d \circ d\} = \{d, \mathbb{I}\}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$ $\quad aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$ $\quad a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（2/2）

H的所有的右陪集为：

- $H\mathbb{I} = \{\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}\} = \{\mathbb{I}, d\}$ $Hd = \{\mathbb{I} \circ d, d \circ d\} = \{d, \mathbb{I}\}$
- $Hc = \{\mathbb{I} \circ c, d \circ c\} = \{c, a^2\}$ $Ha^2 = \{\mathbb{I} \circ a^2, d \circ a^2\} = \{a^2, c\}$
- $Hb = \{\mathbb{I} \circ b, d \circ b\} = \{b, a\}$ $Ha = \{\mathbb{I} \circ a, d \circ a\} = \{a, b\}$

H的左、右陪集集合

- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（2/2）

H的所有的右陪集为：

- $H\mathbb{I} = \{\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}\} = \{\mathbb{I}, d\}$　$Hd = \{\mathbb{I} \circ d, d \circ d\} = \{d, \mathbb{I}\}$
- $Hc = \{\mathbb{I} \circ c, d \circ c\} = \{c, a^2\}$　$Ha^2 = \{\mathbb{I} \circ a^2, d \circ a^2\} = \{a^2, c\}$
- $Hb = \{\mathbb{I} \circ b, d \circ b\} = \{b, a\}$　$Ha = \{\mathbb{I} \circ a, d \circ a\} = \{a, b\}$

H的左、右陪集集合

- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（2/2）

H的所有的右陪集为：

- $H\mathbb{I} = \{\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}\} = \{\mathbb{I}, d\}$ $\quad Hd = \{\mathbb{I} \circ d, d \circ d\} = \{d, \mathbb{I}\}$
- $Hc = \{\mathbb{I} \circ c, d \circ c\} = \{c, a^2\}$ $\quad Ha^2 = \{\mathbb{I} \circ a^2, d \circ a^2\} = \{a^2, c\}$
- $Hb = \{\mathbb{I} \circ b, d \circ b\} = \{b, a\}$ $\quad Ha = \{\mathbb{I} \circ a, d \circ a\} = \{a, b\}$

H的左、右陪集集合

- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（2/2）

H的所有的右陪集为：

- $H\mathbb{I} = \{\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}\} = \{\mathbb{I}, d\}$ $\quad Hd = \{\mathbb{I} \circ d, d \circ d\} = \{d, \mathbb{I}\}$
- $Hc = \{\mathbb{I} \circ c, d \circ c\} = \{c, a^2\}$ $\quad Ha^2 = \{\mathbb{I} \circ a^2, d \circ a^2\} = \{a^2, c\}$
- $Hb = \{\mathbb{I} \circ b, d \circ b\} = \{b, a\}$ $\quad Ha = \{\mathbb{I} \circ a, d \circ a\} = \{a, b\}$

H的左、右陪集集合

- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

3次对称群的子群、陪集（2/2）

H的所有的右陪集为：

- $H\mathbb{I} = \{\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}\} = \{\mathbb{I}, d\}$　$Hd = \{\mathbb{I} \circ d, d \circ d\} = \{d, \mathbb{I}\}$
- $Hc = \{\mathbb{I} \circ c, d \circ c\} = \{c, a^2\}$　$Ha^2 = \{\mathbb{I} \circ a^2, d \circ a^2\} = \{a^2, c\}$
- $Hb = \{\mathbb{I} \circ b, d \circ b\} = \{b, a\}$　$Ha = \{\mathbb{I} \circ a, d \circ a\} = \{a, b\}$

H的左、右陪集集合

- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

$\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$

（证明$aH \subseteq bH$）

$\because \forall x \in aH, \exists h \in H,\ x = a * h,$，即$x = b * h_2 * h_1^{-1} * h,$

$\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$

同理可证，$bH \subseteq aH$，即$aH = bH.$

则$aH = bH$，或$aH \cap bH = \varnothing.$

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

$\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$

（证明$aH \subseteq bH$）

$\because \forall x \in aH, \exists h \in H$, $x = a * h$,，即$x = b * h_2 * h_1^{-1} * h$,

$\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH$.

同理可证，$bH \subseteq aH$，即$aH = bH$.

则$aH = bH$，或$aH \cap bH = \varnothing$.

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

  设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

  $\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$

  （证明$aH \subseteq bH$）

  $\because \forall x \in aH, \exists h \in H,\ x = a * h,$，即$x = b * h_2 * h_1^{-1} * h,$

  $\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$

  同理可证，$bH \subseteq aH$，即$aH = bH.$

  则$aH = bH$，或$aH \cap bH = \varnothing.$

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

  设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

  $\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$

  （证明$aH \subseteq bH$）

  $\because \forall x \in aH, \exists h \in H,\ x = a * h,$ ，即$x = b * h_2 * h_1^{-1} * h,$

  $\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$

  同理可证，$bH \subseteq aH$，即$aH = bH.$

  则$aH = bH$，或$aH \cap bH = \varnothing.$

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

  设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

  $\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2$, $\therefore a = b * h_2 * h_1^{-1}$

  （证明$aH \subseteq bH$）

  $\because \forall x \in aH, \exists h \in H,\ x = a * h$，即$x = b * h_2 * h_1^{-1} * h$,

  $\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH$.

  同理可证，$bH \subseteq aH$，即$aH = bH$.

  则$aH = bH$，或$aH \cap bH = \varnothing$.

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

  设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

  $\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$

  （证明$aH \subseteq bH$）

  $\because \forall x \in aH, \exists h \in H,\ x = a * h,$，即$x = b * h_2 * h_1^{-1} * h,$

  $\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$

  同理可证，$bH \subseteq aH$，即$aH = bH.$

  则$aH = bH$，或$aH \cap bH = \varnothing.$

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

  设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

  $\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$

  （证明$aH \subseteq bH$）

  $\because \forall x \in aH, \exists h \in H, \ x = a * h,$，即$x = b * h_2 * h_1^{-1} * h,$

  $\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$

  同理可证，$bH \subseteq aH$，即$aH = bH$.

  则$aH = bH$，或$aH \cap bH = \varnothing$.

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

  设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

  $\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$

  （证明$aH \subseteq bH$）

  $\because \forall x \in aH, \exists h \in H, \ x = a * h$，即$x = b * h_2 * h_1^{-1} * h$,

  $\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH$.

  同理可证，$bH \subseteq aH$，即$aH = bH$.

  则$aH = bH$，或$aH \cap bH = \varnothing$.

左（右）陪集性质（一）

定理

- 设$< H, * >$是群$< G, * >$的子群，aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- 证：

  设$aH \cap bH \neq \varnothing$，则$\exists f \in aH \cap bH$，

  $\therefore \exists h_1, h_2 \in H$,使得$f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$

  （证明$aH \subseteq bH$）

  $\because \forall x \in aH, \exists h \in H, \ x = a * h,$，即$x = b * h_2 * h_1^{-1} * h,$

  $\because H$是子群，$\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$

  同理可证，$bH \subseteq aH$，即$aH = bH$.

  则$aH = bH$，或$aH \cap bH = \varnothing$.

左（右）陪集性质（二）

定理

- 设$< H, * >$是群$< G, * >$的子群，则$G = \bigcup_{a \in G} aH$.

- 证：

  （1） $G \subseteq \bigcup_{a \in G} aH$

  $\because H \leqslant G, \therefore e \in H,$

  $\forall a \in G,\ a = a * e \in aH$，所以$G \subseteq \bigcup_{a \in G} aH;$

  （2） $\bigcup_{a \in G} aH \subseteq G$

  $\forall a \in G, \forall h \in H,\ a * h \in G,\ \therefore aH \subseteq G,$

  $\therefore \bigcup_{a \in G} aH \subseteq G$

左（右）陪集性质（二）

定理

- 设$< H, * >$是群$< G, * >$的子群，则$G = \bigcup_{a \in G} aH.$
- 证：

（1）$G \subseteq \bigcup_{a \in G} aH$

$\because H \leqslant G, \therefore e \in H,$

$\forall a \in G,\ a = a * e \in aH$，所以$G \subseteq \bigcup_{a \in G} aH;$

（2）$\bigcup_{a \in G} aH \subseteq G$

$\forall a \in G, \forall h \in H,\ a * h \in G,\ \therefore aH \subseteq G,$

$\therefore \bigcup_{a \in G} aH \subseteq G$

左（右）陪集性质（二）

定理

- 设$<H,*>$是群$<G,*>$的子群，则$G=\bigcup_{a\in G} aH$.
- 证：

(1) $G\subseteq \bigcup_{a\in G} aH$

$\because H\leqslant G, \therefore e\in H,$

$\forall a\in G,\ a=a*e\in aH$，所以$G\subseteq \bigcup_{a\in G} aH;$

(2) $\bigcup_{a\in G} aH\subseteq G$

$\forall a\in G, \forall h\in H,\ a*h\in G,\ \therefore aH\subseteq G,$

$\therefore \bigcup_{a\in G} aH\subseteq G$

左（右）陪集性质（二）

定理

- 设$<H,*>$是群$<G,*>$的子群，则$G=\bigcup_{a\in G} aH$.
- 证：

(1) $G\subseteq \bigcup_{a\in G} aH$

$\because H\leqslant G, \therefore e\in H,$

$\forall a\in G,\ a=a*e\in aH$，所以$G\subseteq \bigcup_{a\in G} aH;$

(2) $\bigcup_{a\in G} aH\subseteq G$

$\forall a\in G, \forall h\in H,\ a*h\in G,\ \therefore aH\subseteq G,$

$\therefore \bigcup_{a\in G} aH\subseteq G$

左（右）陪集性质（二）

定理

- 设$< H, * >$是群$< G, * >$的子群，则$G = \bigcup_{a \in G} aH$.
- 证：

  (1) $G \subseteq \bigcup_{a \in G} aH$

  $\because H \leqslant G, \therefore e \in H,$

  $\forall a \in G,\ a = a * e \in aH$，所以$G \subseteq \bigcup_{a \in G} aH;$

  (2) $\bigcup_{a \in G} aH \subseteq G$

  $\forall a \in G, \forall h \in H,\ a * h \in G,\ \therefore aH \subseteq G,$

  $\therefore \bigcup_{a \in G} aH \subseteq G$

左（右）陪集性质（二）

定理

- 设$<H,*>$是群$<G,*>$的子群，则$G=\bigcup_{a\in G} aH$.
- 证：

  （1） $G\subseteq\bigcup_{a\in G} aH$

  $\because H\leqslant G, \therefore e\in H,$

  $\forall a\in G,\ \ a=a*e\in aH$，所以$G\subseteq\bigcup_{a\in G} aH$;

  （2） $\bigcup_{a\in G} aH\subseteq G$

  $\forall a\in G, \forall h\in H,\ \ a*h\in G,\ \ \therefore aH\subseteq G,$

  $\therefore \bigcup_{a\in G} aH\subseteq G$

左（右）陪集性质（二）

定理

- 设$< H, * >$是群$< G, * >$的子群，则$G = \bigcup_{a \in G} aH$.
- 证：

（1） $G \subseteq \bigcup_{a \in G} aH$

$\because H \leqslant G, \therefore e \in H,$

$\forall a \in G,\ \ a = a * e \in aH$，所以$G \subseteq \bigcup_{a \in G} aH$;

（2） $\bigcup_{a \in G} aH \subseteq G$

$\forall a \in G, \forall h \in H,\ \ a * h \in G,\ \ \therefore aH \subseteq G,$

$\therefore \bigcup_{a \in G} aH \subseteq G$

左（右）陪集性质（二）

定理

- 设$< H, * >$是群$< G, * >$的子群，则$G = \bigcup\limits_{a \in G} aH.$

- 证：

  （1） $G \subseteq \bigcup\limits_{a \in G} aH$

  $\because H \leqslant G, \therefore e \in H,$

  $\forall a \in G,\ a = a * e \in aH$，所以$G \subseteq \bigcup\limits_{a \in G} aH;$

  （2） $\bigcup\limits_{a \in G} aH \subseteq G$

  $\forall a \in G, \forall h \in H,\ a * h \in G,\ \therefore aH \subseteq G,$

  $\therefore \bigcup\limits_{a \in G} aH \subseteq G$

左（右）陪集性质（三）

定理

- 设$< H, * >$是群$< G, * >$的子群，H的任意的陪集的大小（基数）是相等的。
- 证：

  设a是群G中的任一元素，h_1, h_2是子群H中的元素，

  若$h_1 \neq h_2$，则$a * h_1 \neq a * h_2$（消去律）。

  所以，aH中没有相同的元素，即aH和H的基数一样，且H的所有陪集基数相等。

  即$\forall a \in G, \ |aH| = |Ha| = |H|$.

左（右）陪集性质（三）

定理

- 设$< H, * >$是群$< G, * >$的子群，H的任意的陪集的大小（基数）是相等的。
- 证：

设a是群G中的任一元素，h_1, h_2是子群H中的元素，

若$h_1 \neq h_2$，则$a * h_1 \neq a * h_2$（消去律）。

所以，aH中没有相同的元素，即aH和H的基数一样，且H的所有陪集基数相等。

即$\forall a \in G$, $|aH| = |Ha| = |H|$.

左（右）陪集性质（三）

定理

- 设$< H, * >$是群$< G, * >$的子群，H的任意的陪集的大小（基数）是相等的。
- 证：

  设a是群G中的任一元素，h_1, h_2是子群H中的元素，

  若$h_1 \neq h_2$，则$a * h_1 \neq a * h_2$（消去律）。

  所以，aH中没有相同的元素，即aH和H的基数一样，且H的所有陪集基数相等。

  即$\forall a \in G$, $|aH| = |Ha| = |H|$.

左（右）陪集性质（三）

定理

- 设$< H, * >$是群$< G, * >$的子群，H的任意的陪集的大小（基数）是相等的。
- 证：

  设a是群G中的任一元素，h_1, h_2是子群H中的元素，

  若$h_1 \neq h_2$，则$a * h_1 \neq a * h_2$（消去律）。

  所以，aH中没有相同的元素，即aH和H的基数一样，且H的所有陪集基数相等。

  即$\forall a \in G$, $|aH| = |Ha| = |H|$.

左（右）陪集性质（三）

定理

- 设$< H, * >$是群$< G, * >$的子群，H的任意的陪集的大小（基数）是相等的。
- 证：

  设a是群G中的任一元素，h_1, h_2是子群H中的元素，

  若$h_1 \neq h_2$，则$a * h_1 \neq a * h_2$（消去律）。

  所以，aH中没有相同的元素，即aH和H的基数一样，且H的所有陪集基数相等。

  即$\forall a \in G$, $|aH| = |Ha| = |H|$.

左（右）陪集性质（三）

定理

- 设$< H, * >$是群$< G, * >$的子群，H的任意的陪集的大小（基数）是相等的。
- 证：

  设a是群G中的任一元素，h_1, h_2是子群H中的元素，

  若$h_1 \neq h_2$，则$a * h_1 \neq a * h_2$（消去律）。

  所以，aH中没有相同的元素，即aH和H的基数一样，且H的所有陪集基数相等。

  即$\forall a \in G,\ |aH| = |Ha| = |H|$.

陪集的性质

定理

设$< H, * >$是群$< G, * >$的子群，

- aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- $G = \bigcup_{a \in G} aH$.（所有左陪集的并集即为G）
- H的任意两个陪集的大小相等，都等于H的大小。
- H的左、右陪集的个数相等。(Th8. 5. 3)

定理

- H的所有左陪集集合，构成G的一个划分；
- 并且，划分中的块（即各个左陪集）的大小相等。
- 即：G的大小$=$左陪集的个数$\times H$的大小

陪集的性质

定理

设$< H, * >$是群$< G, * >$的子群，

- aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- $G = \bigcup\limits_{a \in G} aH$.（所有左陪集的并集即为$G$）
- H的任意两个陪集的大小相等，都等于H的大小。
- H的左、右陪集的个数相等。(Th8. 5. 3)

定理

- H的所有左陪集集合，构成G的一个划分；
- 并且，划分中的块（即各个左陪集）的大小相等。
- 即：G的大小$=$左陪集的个数$\times H$的大小

陪集的性质

定理

设$< H, * >$是群$< G, * >$的子群，

- aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- $G = \bigcup_{a \in G} aH$.（所有左陪集的并集即为G）
- H的任意两个陪集的大小相等，都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

定理

- H的所有左陪集集合，构成G的一个划分；
- 并且，划分中的块（即各个左陪集）的大小相等。
- 即：G的大小$=$左陪集的个数$\times H$的大小

陪集的性质

定理

设$< H, * >$是群$< G, * >$的子群，

- aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- $G = \bigcup_{a \in G} aH$. （所有左陪集的并集即为G）
- H的任意两个陪集的大小相等，都等于H的大小。
- H的左、右陪集的个数相等。(Th8. 5. 3)

定理

- H的所有左陪集集合，构成G的一个划分；
- 并且，划分中的块（即各个左陪集）的大小相等。
- 即：G的大小$=$左陪集的个数$\times H$的大小

陪集的性质

定理

设$< H, * >$是群$< G, * >$的子群，

- aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- $G = \bigcup_{a \in G} aH$.（所有左陪集的并集即为G）
- H的任意两个陪集的大小相等，都等于H的大小。
- H的左、右陪集的个数相等。(Th8. 5. 3)

定理

- H的所有左陪集集合，构成G的一个划分；
- 并且，划分中的块（即各个左陪集）的大小相等。
- 即：G的大小$=$左陪集的个数$\times H$的大小

陪集的性质

定理

设$< H, * >$是群$< G, * >$的子群，

- aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- $G = \bigcup_{a \in G} aH$.（所有左陪集的并集即为G）
- H的任意两个陪集的大小相等，都等于H的大小。
- H的左、右陪集的个数相等。(Th8. 5. 3)

定理

- H的所有左陪集集合，构成G的一个划分；
- 并且，划分中的块（即各个左陪集）的大小相等。
- 即：G的大小$=$左陪集的个数$\times H$的大小

陪集的性质

定理

设$< H, * >$是群$< G, * >$的子群，

- aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- $G = \bigcup_{a \in G} aH$.（所有左陪集的并集即为G）
- H的任意两个陪集的大小相等，都等于H的大小。
- H的左、右陪集的个数相等。(Th8. 5. 3)

定理

- H的所有左陪集集合，构成G的一个划分；
- 并且，划分中的块（即各个左陪集）的大小相等。
- 即：G的大小=左陪集的个数$\times$$H$的大小

陪集的性质

定理

设$< H, * >$是群$< G, * >$的子群，

- aH和bH是任意两个左陪集，则$aH = bH$，或$aH \cap bH = \varnothing$.
- $G = \bigcup_{a \in G} aH$. （所有左陪集的并集即为G）
- H的任意两个陪集的大小相等，都等于H的大小。
- H的左、右陪集的个数相等。(Th8. 5. 3)

定理

- H的所有左陪集集合，构成G的一个划分；
- 并且，划分中的块（即各个左陪集）的大小相等。
- 即：G的大小$=$左陪集的个数$\times H$的大小

Lagrange定理

定理

- 引入记号$[G:H]$：设$< H,* >$是群$< G,* >$的子群，称H的左（右）陪集的个数为H在G中的**指数**，记为$[G:H]$.
- **Lagrange定理** 设$< H,* >$是有限群$< G,* >$的子群，则$|H|$整除$|G|$，且$|G|=|H|\cdot[G:H]$

注意

- 注意：Lagrange定理的逆定理不成立。即，如果$|G|=n$，m整除n，则阶为m的子群未必存在。但是，对于循环群却成立。

Lagrange定理

定理

- 引入记号$[G:H]$：设$< H,* >$是群$< G,* >$的子群，称H的左（右）陪集的个数为H在G中的**指数**，记为$[G:H]$.
- **Lagrange定理** 设$< H,* >$是有限群$< G,* >$的子群，则$|H|$整除$|G|$，且$|G|=|H|\cdot[G:H]$

注意

- 注意：Lagrange定理的逆定理不成立。即，如果$|G|=n$，m整除n，则阶为m的子群未必存在。但是，对于循环群却成立。

Lagrange定理

定理

- 引入记号$[G:H]$：设$< H,*>$是群$< G,*>$的子群，称H的左（右）陪集的个数为H在G中的**指数**，记为$[G:H]$.
- **Lagrange定理** 设$< H,*>$是有限群$< G,*>$的子群，则$|H|$整除$|G|$，且$|G|=|H|\cdot[G:H]$

注意

- 注意：Lagrange定理的逆定理不成立。即，如果$|G|=n$，m整除n，则阶为m的子群未必存在。但是，对于循环群却成立。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

  证：设$a \in G$，$|a| = r$，则$a^r = e$.

  $< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

  即$< a > \leqslant G$，$\therefore$ $|< a >|$整除$|G|$，即$|a|$整除 $|G|$.

推论

- 质数阶段群必为循环群。

  证：设$|G| = p$，p是质数，$\forall a \in G$，$|a|$整除p，

  若$a \neq e$，则$|a| = p$，设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$，

  $< H, * >$构成群，则$H \leqslant G$，$|H| = p$，即$G = H =< a >$.

- 质数阶的群没有非平凡子群。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

  证：设$a \in G$, $|a| = r$, 则$a^r = e$.

  $< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

  即$< a > \leqslant G$, $\therefore$ $|< a >|$整除$|G|$，即$|a|$整除 $|G|$.

推论

- 质数阶段群必为循环群。

  证：设$|G| = p$, p是质数，$\forall a \in G$, $|a|$整除p,

  若$a \neq e$, 则$|a| = p$, 设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$，

  $< H, * >$构成群，则$H \leqslant G$, $|H| = p$, 即$G = H =< a >$.

- 质数阶的群没有非平凡子群。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

  证：设$a \in G$, $|a| = r$, 则$a^r = e$.

  $< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

  即$< a > \leqslant G$, $\therefore$ $|< a >|$整除$|G|$，即$|a|$整除$|G|$.

推论

- 质数阶段群必为循环群。

  证：设$|G| = p$, p是质数，$\forall a \in G$, $|a|$整除p,

  若$a \neq e$, 则$|a| = p$, 设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$,

  $< H, * >$构成群，则$H \leqslant G$, $|H| = p$, 即$G = H =< a >$.

- 质数阶的群没有非平凡子群。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

  证：设$a \in G$, $|a| = r$, 则$a^r = e$.

  $< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

  即$< a > \leqslant G$, $\therefore$ $|< a >|$整除$|G|$，即$|a|$整除 $|G|$.

推论

- 质数阶段群必为循环群。

  证：设$|G| = p$, p是质数，$\forall a \in G$, $|a|$整除p,

  若$a \neq e$, 则$|a| = p$, 设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$,

  $< H, * >$构成群，则$H \leqslant G$, $|H| = p$, 即$G = H =< a >$.

- 质数阶的群没有非平凡子群。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

证：设$a \in G$, $|a| = r$, 则$a^r = e$.

$< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

即$< a > \leqslant G$, $\therefore$ $| < a > |$整除$|G|$，即$|a|$整除 $|G|$.

推论

- 质数阶段群必为循环群。

证：设$|G| = p$, p是质数，$\forall a \in G$, $|a|$整除p,

若$a \neq e$, 则$|a| = p$, 设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$,

$< H, * >$构成群，则$H \leqslant G$, $|H| = p$, 即$G = H =< a >$.

- 质数阶的群没有非平凡子群。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

  证：设$a \in G$，$|a| = r$，则$a^r = e$.

  $< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

  即$< a > \leqslant G$，$\therefore$ $| < a > |$整除$|G|$，即$|a|$整除 $|G|$.

推论

- 质数阶段群必为循环群。

  证：设$|G| = p$，p是质数，$\forall a \in G$，$|a|$整除p，

  若$a \neq e$，则$|a| = p$，设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$，

  $< H, * >$构成群，则$H \leqslant G$，$|H| = p$，即$G = H = < a >$.

- 质数阶的群没有非平凡子群。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

  证：设$a \in G$, $|a| = r$, 则$a^r = e$.

  $< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

  即$< a > \leqslant G$, $\therefore$ $| < a > |$整除$|G|$，即$|a|$整除 $|G|$.

推论

- 质数阶段群必为循环群。

  证：设$|G| = p$, p是质数，$\forall a \in G$, $|a|$整除p,

  若$a \neq e$, 则$|a| = p$, 设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$，

  $< H, * >$构成群，则$H \leqslant G$, $|H| = p$, 即$G = H =< a >$.

- 质数阶的群没有非平凡子群。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

  证：设$a \in G$, $|a| = r$, 则$a^r = e$.

  $< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

  即$< a > \leqslant G$, $\therefore$ $|< a >|$整除$|G|$，即$|a|$整除 $|G|$.

推论

- 质数阶段群必为循环群。

  证：设$|G| = p$, p是质数，$\forall a \in G$, $|a|$整除p,

  若$a \neq e$, 则$|a| = p$, 设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$,

  $< H, * >$构成群，则$H \leqslant G$, $|H| = p$, 即$G = H =< a >$.

- 质数阶的群没有非平凡子群。

Lagrange定理的推论

推论

- 在有限群G中，每个元素的阶能整除$|G|$.

  证：设$a \in G$, $|a| = r$, 则$a^r = e$.

  $< \{e, a, a^2, a^3, \ldots\ldots, a^{r-1}\}, * >$是$< G, * >$的子群，

  即$< a > \leqslant G$, $\therefore$ $| < a > |$整除$|G|$，即$|a|$整除 $|G|$.

推论

- 质数阶段群必为循环群。

  证：设$|G| = p$, p是质数，$\forall a \in G$, $|a|$整除p,

  若$a \neq e$, 则$|a| = p$, 设$H = \{e, a, a^2, \ldots\ldots, a^{p-1}\}$，

  $< H, * >$构成群，则$H \leqslant G$, $|H| = p$, 即$G = H =< a >$.

- 质数阶的群没有非平凡子群。

左（右）陪集关系

陪集等价关系

设$< H, * >$是群$< G, * >$的子群，

- H的所有左（右）陪集的集合是G的一个划分；
- 由这个划分可以诱导出一个G上的等价关系，称之为子群H的左（右）陪集等价关系；
- 这个等价关系的每一个等价类就是H的一个左（右）陪集。

左（右）陪集关系

陪集等价关系

设$< H, * >$是群$< G, * >$的子群，

- H的所有左（右）陪集的集合是G的一个划分；
- 由这个划分可以诱导出一个G上的等价关系，称之为子群H的左（右）陪集等价关系；
- 这个等价关系的每一个等价类就是H的一个左（右）陪集。

左（右）陪集关系

陪集等价关系

设$< H, * >$是群$< G, * >$的子群，

- H的所有左（右）陪集的集合是G的一个划分；
- 由这个划分可以诱导出一个G上的等价关系，称之为子群H的左（右）陪集等价关系；
- 这个等价关系的每一个等价类就是H的一个左（右）陪集。

陪集关系的定义

左陪集关系

- 设$< H, * >$是群$< G, * >$的子群，则 $\forall x,\ x \in aH \iff a^{-1} * x \in H.$
- 证：$x \in aH \iff \exists h \in H,\ x = a * h \iff \exists h = a^{-1} * x \in H,$

  因此，$\forall x,\ x \in aH \iff a^{-1} * x \in H.$
- 描述了左陪集aH中的元素x。

右陪集关系

- 同理$\forall x,\ x \in Ha \iff x * a^{-1} \in H.$
- 描述右陪集Ha中的元素x。

陪集关系的定义

左陪集关系

- 设$< H, * >$是群$< G, * >$的子群，则 $\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H$.
- 证：$x \in aH \Longleftrightarrow \exists h \in H,\ x = a * h \Longleftrightarrow \exists h = a^{-1} * x \in H$,

  因此，$\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H$.
- 描述了左陪集aH中的元素x。

右陪集关系

- 同理$\forall x,\ x \in Ha \Longleftrightarrow x * a^{-1} \in H$.
- 描述右陪集Ha中的元素x。

陪集关系的定义

左陪集关系

- 设$< H, * >$是群$< G, * >$的子群，则 $\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H$.
- 证：$x \in aH \Longleftrightarrow \exists h \in H,\ x = a * h \Longleftrightarrow \exists h = a^{-1} * x \in H$,

  因此，$\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H$.
- 描述了左陪集aH中的元素x。

右陪集关系

- 同理$\forall x,\ x \in Ha \Longleftrightarrow x * a^{-1} \in H$.
- 描述右陪集Ha中的元素x。

陪集关系的定义

左陪集关系

- 设$< H, * >$是群$< G, * >$的子群，则
  $\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H$.
- 证：$x \in aH \Longleftrightarrow \exists h \in H,\ x = a * h \Longleftrightarrow \exists h = a^{-1} * x \in H$,

  因此，$\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H$.
- 描述了左陪集aH中的元素x。

右陪集关系

- 同理$\forall x,\ x \in Ha \Longleftrightarrow x * a^{-1} \in H$.
- 描述右陪集Ha中的元素x。

陪集关系的定义

左陪集关系

- 设$< H, * >$是群$< G, * >$的子群，则
  $\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H.$
- 证：$x \in aH \Longleftrightarrow \exists h \in H,\ x = a * h \Longleftrightarrow \exists h = a^{-1} * x \in H,$
  因此，$\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H.$
- 描述了左陪集aH中的元素x。

右陪集关系

- 同理$\forall x,\ x \in Ha \Longleftrightarrow x * a^{-1} \in H.$
- 描述右陪集Ha中的元素x。

陪集关系的定义

左陪集关系

- 设$< H, * >$是群$< G, * >$的子群，则 $\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H$.
- 证：$x \in aH \Longleftrightarrow \exists h \in H,\ x = a * h \Longleftrightarrow \exists h = a^{-1} * x \in H$,

  因此，$\forall x,\ x \in aH \Longleftrightarrow a^{-1} * x \in H$.
- 描述了左陪集aH中的元素x。

右陪集关系

- 同理$\forall x,\ x \in Ha \Longleftrightarrow x * a^{-1} \in H$.
- 描述右陪集Ha中的元素x。

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系$R: < a, b > \in R,\ iff,\ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa$;

  -对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$

  $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$

  $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H$,

  $\therefore x = a * (a^{-1} * x) \in aH$, $\therefore [a]_R \subseteq aH$;

  ②$aH \subseteq [a]_R$: $\forall x \in aH$, $\exists h \in H$, $x = a * h$,

  即$h = a^{-1} * x \in H$, $\therefore xRa$, $x \in [a]_R$, $aH \subseteq [a]_R$.

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系$R: < a, b > \in R,\ iff,\ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa;$

  -对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$

  $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$

  $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$

  $\therefore x = a * (a^{-1} * x) \in aH,\ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH,\ \exists h \in H,\ x = a * h,$

  即$h = a^{-1} * x \in H,\ \therefore xRa,\ x \in [a]_R,\ aH \subseteq [a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系$R: < a, b > \in R, \ iff, \ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa;$

  -对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$

  $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$

  $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$

  $\therefore x = a * (a^{-1} * x) \in aH, \ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH, \ \exists h \in H, \ x = a * h,$

  即$h = a^{-1} * x \in H, \ \therefore xRa, \ x \in [a]_R, \ aH \subseteq [a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系$R : < a, b > \in R,\ \ iff,\ \ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa;$

  -对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$

  $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$

  $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$

  $\therefore x = a * (a^{-1} * x) \in aH,\ \ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH,\ \ \exists h \in H,\ \ x = a * h,$

  即$h = a^{-1} * x \in H,\ \ \therefore xRa,\ \ x \in [a]_R,\ \ aH \subseteq [a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系$R: < a, b > \in R, \ iff, \ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa;$

  -对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$
  $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$
  $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$
  $\therefore x = a * (a^{-1} * x) \in aH, \ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH, \ \exists h \in H, \ x = a * h,$
  即$h = a^{-1} * x \in H, \ \therefore xRa, \ x \in [a]_R, \ aH \subseteq [a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系 $R: < a, b > \in R,\ iff,\ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性： $e = a^{-1} * a \in H \Longleftrightarrow aRa;$

  -对称性： $aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$
  $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性： $aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$
  $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$
  $\therefore x = a * (a^{-1} * x) \in aH,\ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH,\ \exists h \in H,\ x = a * h,$
  即$h = a^{-1} * x \in H,\ \therefore xRa,\ x \in [a]_R,\ aH \subseteq [a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$<H,*>$是群$<G,*>$的子群，定义G上的二元关系 $R: <a,b>\in R,\ iff,\ a^{-1}*b\in H$. 称$R$为$H$的**左陪集关系**。
- R是等价关系
  - 自反性：$e=a^{-1}*a\in H \Longleftrightarrow aRa;$
  - 对称性：$aRb \Longleftrightarrow a^{-1}*b\in H \Longleftrightarrow (a^{-1}*b)^{-1}\in H$ $\Longleftrightarrow b^{-1}*a\in H \Longleftrightarrow bRa$
  - 传递性：$aRb\wedge bRc \Longleftrightarrow a^{-1}*b\in H\wedge b^{-1}*c\in H$ $\Longrightarrow (a^{-1}*b)*(b^{-1}*c)=a^{-1}*c\in H \Longleftrightarrow aRc.$
- $[a]_R=aH$

  ①$[a]_R\subseteq aH$: $x\in[a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1}*x\in H,$

  $\therefore x=a*(a^{-1}*x)\in aH,\ \therefore [a]_R\subseteq aH;$

  ②$aH\subseteq[a]_R$: $\forall x\in aH,\ \exists h\in H,\ x=a*h,$

  即$h=a^{-1}*x\in H,\ \therefore xRa,\ x\in[a]_R,\ aH\subseteq[a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$<H,*>$是群$<G,*>$的子群，定义G上的二元关系 $R: <a,b>\in R,\ iff,\ a^{-1}*b\in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e=a^{-1}*a\in H \Longleftrightarrow aRa;$

  -对称性：$aRb \Longleftrightarrow a^{-1}*b\in H \Longleftrightarrow (a^{-1}*b)^{-1}\in H$
  $\Longleftrightarrow b^{-1}*a\in H \Longleftrightarrow bRa$

  -传递性：$aRb\wedge bRc \Longleftrightarrow a^{-1}*b\in H\wedge b^{-1}*c\in H$
  $\Longrightarrow (a^{-1}*b)*(b^{-1}*c)=a^{-1}*c\in H \Longleftrightarrow aRc.$
- $[a]_R=aH$

  ①$[a]_R\subseteq aH$: $x\in[a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1}*x\in H,$
  $\therefore x=a*(a^{-1}*x)\in aH,\ \therefore [a]_R\subseteq aH;$

  ②$aH\subseteq [a]_R$: $\forall x\in aH,\ \exists h\in H,\ x=a*h,$
  即$h=a^{-1}*x\in H,\ \therefore xRa,\ x\in[a]_R,\ aH\subseteq[a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系$R: < a, b > \in R,\ iff,\ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa;$

  -对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$

  $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$

  $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$

  $\therefore x = a * (a^{-1} * x) \in aH,\ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH,\ \exists h \in H,\ x = a * h,$

  即$h = a^{-1} * x \in H,\ \therefore xRa,\ x \in [a]_R,\ aH \subseteq [a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系$R: < a, b > \in R, \ iff, \ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa;$

  -对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H \Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H \Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$

  $\therefore x = a * (a^{-1} * x) \in aH, \ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH, \ \exists h \in H, \ x = a * h,$

  即$h = a^{-1} * x \in H, \ \therefore xRa, \ x \in [a]_R, \ aH \subseteq [a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系$R: < a, b > \in R,\ iff,\ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系

  -自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa;$

  -对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$
  $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$

  -传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$
  $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$
  $\therefore x = a * (a^{-1} * x) \in aH, \ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH, \ \exists h \in H, \ x = a * h,$
  即$h = a^{-1} * x \in H, \ \therefore xRa, \ x \in [a]_R, \ aH \subseteq [a]_R.$

左陪集等价关系

左陪集等价关系的定义

- 设$< H, * >$是群$< G, * >$的子群，定义G上的二元关系 $R: < a, b > \in R,\ iff,\ a^{-1} * b \in H$. 称$R$为$H$的左陪集关系。
- R是等价关系
  - 自反性：$e = a^{-1} * a \in H \Longleftrightarrow aRa;$
  - 对称性：$aRb \Longleftrightarrow a^{-1} * b \in H \Longleftrightarrow (a^{-1} * b)^{-1} \in H$
    $\Longleftrightarrow b^{-1} * a \in H \Longleftrightarrow bRa$
  - 传递性：$aRb \wedge bRc \Longleftrightarrow a^{-1} * b \in H \wedge b^{-1} * c \in H$
    $\Longrightarrow (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \Longleftrightarrow aRc.$
- $[a]_R = aH$

  ①$[a]_R \subseteq aH$: $x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$
  $\therefore x = a * (a^{-1} * x) \in aH,\ \therefore [a]_R \subseteq aH;$

  ②$aH \subseteq [a]_R$: $\forall x \in aH,\ \exists h \in H,\ x = a * h,$
  即$h = a^{-1} * x \in H,\ \therefore xRa,\ x \in [a]_R,\ aH \subseteq [a]_R.$

左陪集等价关系

小结

- 设$< H, * >$是群$< G, * >$的子群，则H可以诱导出一个由H的左（右）陪集集合构成的对G的划分；
- 由这个划分可以诱导出G的一个左（右）陪集等价关系；
- 左陪集等价关系：$\forall a, b$属于同一个左陪集$\Longleftrightarrow a, b$属于同一个左陪集等价关系的等价类$\Longleftrightarrow a^{-1} * b \in H$.
  - $\because\ a \in aH,\ b \in bH,$ 则 $aH = bH;$
  - 且，$a,\ b$有左陪集关系，即$a^{-1} * b \in H.$

例

Eg. $< \mathbb{Z},\ + >$的子群。

左陪集等价关系

小结

- 设$< H, * >$是群$< G, * >$的子群，则H可以诱导出一个由H的左（右）陪集集合构成的对G的划分；
- 由这个划分可以诱导出G的一个左（右）陪集等价关系；
- 左陪集等价关系：$\forall a, b$属于同一个左陪集$\Longleftrightarrow a, b$属于同一个左陪集等价关系的等价类$\Longleftrightarrow a^{-1} * b \in H$.
  - $\because\ a \in aH,\ b \in bH$, 则 $aH = bH$;
  - 且，$a,\ b$有左陪集关系，即$a^{-1} * b \in H$.

例

Eg. $<\mathbb{Z},\ + >$的子群。

左陪集等价关系

小结

- 设$< H, * >$是群$< G, * >$的子群，则H可以诱导出一个由H的左（右）陪集集合构成的对G的划分；
- 由这个划分可以诱导出G的一个左（右）陪集等价关系；
- 左陪集等价关系：$\forall a, b$属于同一个左陪集$\Longleftrightarrow a, b$属于同一个左陪集等价关系的等价类$\Longleftrightarrow a^{-1} * b \in H$.
  - $\because\ a \in aH,\ b \in bH$, 则 $aH = bH$;
  - 且，a, b有左陪集关系，即$a^{-1} * b \in H$.

例

Eg. $< \mathbb{Z},\ + >$的子群。

左陪集等价关系

小结

- 设$< H, * >$是群$< G, * >$的子群，则H可以诱导出一个由H的左（右）陪集集合构成的对G的划分；
- 由这个划分可以诱导出G的一个左（右）陪集等价关系；
- 左陪集等价关系：$\forall a, b$属于同一个左陪集$\Longleftrightarrow a, b$属于同一个左陪集等价关系的等价类$\Longleftrightarrow a^{-1} * b \in H$.

  ➪$\because$ $a \in aH$, $b \in bH$, 则 $aH = bH$;

  ➪且，a, b有左陪集关系，即$a^{-1} * b \in H$.

例

Eg. $< \mathbb{Z}, \ + >$的子群。

左陪集等价关系

小结

- 设$< H, * >$是群$< G, * >$的子群，则H可以诱导出一个由H的左（右）陪集集合构成的对G的划分;
- 由这个划分可以诱导出G的一个左（右）陪集等价关系;
- 左陪集等价关系：$\forall a, b$属于同一个左陪集$\Longleftrightarrow a, b$属于同一个左陪集等价关系的等价类$\Longleftrightarrow a^{-1} * b \in H$.
  - $\because\ a \in aH,\ b \in bH,$ 则 $aH = bH$;
  - 且，$a,\ b$有左陪集关系，即$a^{-1} * b \in H$.

例

Eg. $< \mathbb{Z},\ + >$的子群。

不变子群（正规子群）

3次对称群S_3

- 3次对称群$< S_3, \circ, \mathbb{I} >$，$S_3 = \{\mathbb{I}, a, a^2, b, c, d\}$,
- $H = \{\mathbb{I}, d\}$是群S_3的一个子群;
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$
- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

不变子群（正规子群）

3次对称群S_3

- 3次对称群$< S_3, \circ, \mathbb{I} >$，$S_3 = \{\mathbb{I}, a, a^2, b, c, d\}$,
- $H = \{\mathbb{I}, d\}$是群S_3的一个子群;
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$
- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

不变子群（正规子群）

3次对称群S_3

- 3次对称群$< S_3, \circ, \mathbb{I} >$，$S_3 = \{\mathbb{I}, a, a^2, b, c, d\}$，
- $H = \{\mathbb{I}, d\}$是群S_3的一个子群；
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$
- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

不变子群（正规子群）

3次对称群S_3

- 3次对称群$< S_3, \circ, \mathbb{I} >$，$S_3 = \{\mathbb{I}, a, a^2, b, c, d\}$,
- $H = \{\mathbb{I}, d\}$是群S_3的一个子群；
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$
- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

不变子群（正规子群）

3次对称群S_3

- 3次对称群$< S_3, \circ, \mathbb{I} >$，$S_3 = \{\mathbb{I}, a, a^2, b, c, d\}$,
- $H = \{\mathbb{I}, d\}$是群S_3的一个子群;
- H的所有左陪集组成的集合$\{\{\mathbb{I}, d\}, \{a, c\}, \{b, a^2\}\}$
- H的所有右陪集组成的集合$\{\{\mathbb{I}, d\}, \{c, a^2\}, \{a, b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

不变子群（正规子群）

定义-正规子群

- 设$< H, * >$是群$< G, * >$的子群，称H为G的不变子群（正规子群），iff, $\forall a \in G$, $aH = Ha$, 记为$H \lhd G$.
- 注：$\forall a \in G$, $aH = Ha \Longleftrightarrow$
  $\forall a \in G$, $\exists h_1, h_2 \in H$, $a * h_1 = h_2 * a$.
- 对于正规子群，左右陪集对应相等，$aH = Ha$，可简称为陪集。左右陪集关系相同，简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

不变子群（正规子群）

定义-正规子群

- 设$< H, * >$是群$< G, * >$的子群，称H为G的不变子群（正规子群），iff, $\forall a \in G,\ aH = Ha$，记为$H \lhd G$.
- 注：$\forall a \in G,\ aH = Ha \Longleftrightarrow$
  $\forall a \in G,\ \exists h_1, h_2 \in H,\ a * h_1 = h_2 * a.$
- 对于正规子群，左右陪集对应相等，$aH = Ha$，可简称为陪集。左右陪集关系相同，简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

不变子群（正规子群）

定义-正规子群

- 设$< H, * >$是群$< G, * >$的子群，称H为G的不变子群（正规子群），iff，$\forall a \in G$，$aH = Ha$，记为$H \lhd G$.
- 注：$\forall a \in G$，$aH = Ha \Longleftrightarrow$
  $\forall a \in G$，$\exists h_1, h_2 \in H$，$a * h_1 = h_2 * a$.
- 对于正规子群，左右陪集对应相等，$aH = Ha$，可简称为陪集。左右陪集关系相同，简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

不变子群（正规子群）

定义-正规子群

- 设$< H, * >$是群$< G, * >$的子群，称H为G的不变子群（正规子群），iff，$\forall a \in G$，$aH = Ha$，记为$H \lhd G$.
- 注：$\forall a \in G$，$aH = Ha \Longleftrightarrow$

  $\forall a \in G$，$\exists h_1, h_2 \in H$，$a * h_1 = h_2 * a$.
- 对于正规子群，左右陪集对应相等，$aH = Ha$，可简称为陪集。左右陪集关系相同，简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

不变子群（正规子群）

定义-正规子群

- 设$< H, * >$是群$< G, * >$的子群，称H为G的不变子群（正规子群），iff，$\forall a \in G$，$aH = Ha$，记为$H \lhd G$.
- 注：$\forall a \in G$，$aH = Ha \Longleftrightarrow$
  $\forall a \in G$，$\exists h_1, h_2 \in H$，$a * h_1 = h_2 * a$.
- 对于正规子群，左右陪集对应相等，$aH = Ha$，可简称为陪集。左右陪集关系相同，简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

不变子群（正规子群）

定义-正规子群

- 设$< H, * >$是群$< G, * >$的子群，称H为G的不变子群（正规子群），iff, $\forall a \in G$, $aH = Ha$, 记为$H \lhd G$.
- 注： $\forall a \in G$, $aH = Ha \Longleftrightarrow$

  $\forall a \in G$, $\exists h_1, h_2 \in H$, $a * h_1 = h_2 * a$.
- 对于正规子群，左右陪集对应相等，$aH = Ha$，可简称为陪集。左右陪集关系相同，简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

正规子群的性质

定理

设$H \leqslant G$，则下列条件相互等价:

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

正规子群的性质

定理

设$H \leqslant G$，则下列条件相互等价：

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

正规子群的性质

定理

设$H \leqslant G$，则下列条件相互等价:

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

正规子群的性质

定理

设$H \leqslant G$，则下列条件相互等价:

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

同余关系

定义-同余关系

- $< A, * >$是一个代数系统，R是A上的等价关系，称等价关系R在运算$*$下具有置换性质，iff,

  $$if\ \forall < a, b > \in R \wedge < c, d > \in R,\quad then\quad < a * c, b * d > \in R.$$

- 将一个运算数置换为等价类中的另一个元素，不会改变运算结果的等价类，即，等价关系R在运算$*$下仍然保持。
- 若等价关系R在运算$*$下具有置换性质，则称R为$< A, * >$上的同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2$，$h_1, h_2 \in H$,

$$
\begin{aligned}
a_1 * b_1 &= (a * h_1) * (b * h_2) \\
&= (a * h_1) * (h_3 * b) \\
&= a * h_4 * b \\
&= (a * b) * h_5 \qquad (h_i \in H)
\end{aligned}
$$

$\therefore\ \forall a_1 * b_1 \in (a * b)H.$

同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

a_1是aH中的任一元素，b_1是bH中的任一元素，

现证任意的$a_1 * b_1$都在H的同一陪集中。

设 $a_1 = a * h_1, b_1 = b * h_2$，$h_1, h_2 \in H$,

$$
\begin{aligned}
a_1 * b_1 &= (a * h_1) * (b * h_2) \\
&= (a * h_1) * (h_3 * b) \\
&= a * h_4 * b \\
&= (a * b) * h_5 \qquad (h_i \in H)
\end{aligned}
$$

$\therefore \ \forall a_1 * b_1 \in (a * b)H.$

同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2$，$h_1, h_2 \in H$,

$$
\begin{aligned}
a_1 * b_1 &= (a * h_1) * (b * h_2) \\
&= (a * h_1) * (h_3 * b) \\
&= a * h_4 * b \\
&= (a * b) * h_5 \qquad (h_i \in H)
\end{aligned}
$$

  $\therefore\ \forall a_1 * b_1 \in (a * b)H.$

  同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

设 $a_1 = a * h_1, b_1 = b * h_2$，$h_1, h_2 \in H$,

$$\begin{aligned} a_1 * b_1 &= (a * h_1) * (b * h_2) \\ &= (a * h_1) * (h_3 * b) \\ &= a * h_4 * b \\ &= (a * b) * h_5 \qquad (h_i \in H) \end{aligned}$$

$\therefore\ \forall a_1 * b_1 \in (a * b)H.$

同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2$，$h_1, h_2 \in H$,

  $$\begin{aligned} a_1 * b_1 &= (a * h_1) * (b * h_2) \\ &= (a * h_1) * (h_3 * b) \\ &= a * h_4 * b \\ &= (a * b) * h_5 \qquad (h_i \in H) \end{aligned}$$

  $\therefore\ \forall a_1 * b_1 \in (a * b)H.$

  同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2$, $h_1, h_2 \in H$,

  $$\begin{aligned} a_1 * b_1 &= (a * h_1) * (b * h_2) \\ &= (a * h_1) * (h_3 * b) \\ &= a * h_4 * b \\ &= (a * b) * h_5 \qquad (h_i \in H) \end{aligned}$$

  $\therefore\ \forall a_1 * b_1 \in (a * b)H.$

  同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2$，$h_1, h_2 \in H$,

$$
\begin{aligned}
a_1 * b_1 &= (a * h_1) * (b * h_2) \\
&= (a * h_1) * (h_3 * b) \\
&= a * h_4 * b \\
&= (a * b) * h_5 \qquad (h_i \in H)
\end{aligned}
$$

$\therefore\ \forall a_1 * b_1 \in (a * b)H.$

同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2$， $h_1, h_2 \in H$,

  $$\begin{aligned} a_1 * b_1 &= (a * h_1) * (b * h_2) \\ &= (a * h_1) * (h_3 * b) \\ &= a * h_4 * b \\ &= (a * b) * h_5 \qquad (h_i \in H) \end{aligned}$$

  $\therefore\ \forall a_1 * b_1 \in (a * b)H.$

  同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2,\ h_1, h_2 \in H,$

$$
\begin{aligned}
a_1 * b_1 &= (a * h_1) * (b * h_2) \\
&= (a * h_1) * (h_3 * b) \\
&= a * h_4 * b \\
&= (a * b) * h_5 \qquad (h_i \in H)
\end{aligned}
$$

  $\therefore\ \forall a_1 * b_1 \in (a * b)H.$

  同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2,\ h_1, h_2 \in H,$

$$
\begin{aligned}
a_1 * b_1 &= (a * h_1) * (b * h_2) \\
&= (a * h_1) * (h_3 * b) \\
&= a * h_4 * b \\
&= (a * b) * h_5 \qquad (h_i \in H)
\end{aligned}
$$

  $\therefore\ \forall a_1 * b_1 \in (a * b)H.$

  同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

正规子群和同余关系（一）

定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证：设aH和bH是群G的两个陪集，

  a_1是aH中的任一元素，b_1是bH中的任一元素，

  现证任意的$a_1 * b_1$都在H的同一陪集中。

  设 $a_1 = a * h_1, b_1 = b * h_2,\ h_1, h_2 \in H,$

$$
\begin{aligned}
a_1 * b_1 &= (a * h_1) * (b * h_2) \\
&= (a * h_1) * (h_3 * b) \\
&= a * h_4 * b \\
&= (a * b) * h_5 \qquad (h_i \in H)
\end{aligned}
$$

$$\therefore\ \forall a_1 * b_1 \in (a * b)H.$$

同时陪集关系是等价关系，所以由正规子群H诱导出的陪集关系是同余关系。

商群的定义

定义

- 设$< H, *, e >$是群$< G, *, e >$的正规子群。H的陪集关系R（是同余关系，具有置换性质），则$< G/H, \circledast, H >$是群，其中：

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

  $aH \circledast bH = (a * b)H$;

  $[aH]^{-1} = a^{-1}H$;

  H是单位元.

- R是H的陪集关系，习惯也记为$< G/R, \circledast, H >$，称为群G关于正规子群H的商群。

商群的定义

定义

- 设$< H, *, e >$是群$< G, *, e >$的正规子群。H的陪集关系R（是同余关系，具有置换性质），则$< G/H, \circledast, H >$是群，其中：

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

  $aH \circledast bH = (a * b)H$;

  $[aH]^{-1} = a^{-1}H$;

  H是单位元.

- R是H的陪集关系，习惯也记为$< G/R, \circledast, H >$，称为群G关于正规子群H的**商群**。

商群的定义

定义

- 设$< H, *, e >$是群$< G, *, e >$的正规子群。H的陪集关系R（是同余关系，具有置换性质），则$< G/H, \circledast, H >$是群，其中：

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

  $aH \circledast bH = (a * b)H$;

  $[aH]^{-1} = a^{-1}H$;

  H是单位元.

- R是H的陪集关系，习惯也记为$< G/R, \circledast, H >$，称为群G关于正规子群H的商群。

商群的定义

定义

- 设$< H, *, e >$是群$< G, *, e >$的正规子群。H的陪集关系R（是同余关系，具有置换性质），则$< G/H, \circledast, H >$是群，其中：

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

  $aH \circledast bH = (a * b)H$;

  $[aH]^{-1} = a^{-1}H$;

  H是单位元.

- R是H的陪集关系，习惯也记为$< G/R, \circledast, H >$，称为群G关于正规子群H的商群。

商群的定义

定义

- 设$< H, *, e >$是群$< G, *, e >$的正规子群。H的陪集关系R（是同余关系，具有置换性质），则$< G/H, \circledast, H >$是群，其中：

  $G/H = G/R = \{aH | a \in G\}$；

  $aH \circledast bH = (a * b)H$;

  $[aH]^{-1} = a^{-1}H$ ；

  H是单位元.

- R是H的陪集关系，习惯也记为$< G/R, \circledast, H >$，称为群G关于正规子群H的商群。

商群的定义

定义

- 设$< H, *, e >$是群$< G, *, e >$的正规子群。H的陪集关系R（是同余关系，具有置换性质），则$< G/H, \circledast, H >$是群，其中：

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

  $aH \circledast bH = (a * b)H$;

  $[aH]^{-1} = a^{-1}H$;

  H是单位元.
- R是H的陪集关系，习惯也记为$< G/R, \circledast, H >$，称为群G关于正规子群H的**商群**。

商群的例子

定义

- （有限群的）商群的阶等于群G的阶除以子群H的阶，即H在G中的指数。

例

- 群$<\mathbb{Z},+,0>$，$4\mathbb{Z}\lhd\mathbb{Z}$，商群为$<\{4\mathbb{Z},4\mathbb{Z}+1,4\mathbb{Z}+2,4\mathbb{Z}+3\},\ \oplus,\ 4\mathbb{Z}>$
- 群$<S_3,\circ,\mathbb{I}>$，$\{\mathbb{I},a,a^2\}\lhd S_3$，商群为$<\{\{\mathbb{I},a,a^2\},\ \{b,c,d\}\},\ \circledast,\ \{\mathbb{I},a,a^2\}>.$

商群的例子

定义

- （有限群的）商群的阶等于群G的阶除以子群H的阶，即H在G中的指数。

例

- 群$< \mathbb{Z}, +, 0 >$，$4\mathbb{Z} \lhd \mathbb{Z}$，商群为 $< \{4\mathbb{Z}, 4\mathbb{Z}+1, 4\mathbb{Z}+2, 4\mathbb{Z}+3\}$，$\oplus$，$4\mathbb{Z} >$
- 群$< S_3, \circ, \mathbb{I} >$，$\{\mathbb{I}, a, a^2\} \lhd S_3$，商群为 $< \{\{\mathbb{I}, a, a^2\}$，$\{b, c, d\}\}$，$\circledast$，$\{\mathbb{I}, a, a^2\} >$.

商群的例子

定义

- （有限群的）商群的阶等于群G的阶除以子群H的阶，即H在G中的指数。

例

- 群$< \mathbb{Z}, +, 0 >$，$4\mathbb{Z} \lhd \mathbb{Z}$，商群为$< \{4\mathbb{Z}, 4\mathbb{Z}+1, 4\mathbb{Z}+2, 4\mathbb{Z}+3\}, \oplus, 4\mathbb{Z} >$
- 群$< S_3, \circ, \mathbb{I} >$，$\{\mathbb{I}, a, a^2\} \lhd S_3$，商群为$< \{\{\mathbb{I}, a, a^2\}, \{b, c, d\}\}, \circledast, \{\mathbb{I}, a, a^2\} >$.

正规子群和同余关系（二）

定理

- 设R是群$< G, * >$上的同余关系，则$[e]_R \lhd G$，且R就是G关于正规子群$[e]_R$的陪集关系。
- 证：（略）

  （1）$[e]_R \leqslant G$;

  （2）$[e]_R \lhd G$;

  （3）$[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

正规子群和同余关系（二）

定理

- 设R是群$< G, * >$上的同余关系，则$[e]_R \lhd G$，且R就是G关于正规子群$[e]_R$的陪集关系。
- 证：（略）

  （1）$[e]_R \leqslant G$;

  （2）$[e]_R \lhd G$;

  （3）$[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

正规子群和同余关系（二）

定理

- 设R是群$< G, * >$上的同余关系，则$[e]_R \lhd G$，且R就是G关于正规子群$[e]_R$的陪集关系。
- 证：（略）

  （1）$[e]_R \leqslant G$;

  （2）$[e]_R \lhd G$;

  （3）$[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

正规子群和同余关系（二）

定理

- 设R是群$< G, * >$上的同余关系，则$[e]_R \lhd G$，且R就是G关于正规子群$[e]_R$的陪集关系。
- 证：（略）

  （1）$[e]_R \leqslant G$;

  （2）$[e]_R \lhd G$;

  （3）$[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

正规子群和同余关系（二）

定理

- 设R是群$< G, * >$上的同余关系，则$[e]_R \lhd G$，且R就是G关于正规子群$[e]_R$的陪集关系。
- 证：（略）

  （1）$[e]_R \leqslant G$;

  （2）$[e]_R \lhd G$;

  （3）$[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

正规子群和同余关系（二）

定理

- 设R是群$< G, * >$上的同余关系，则$[e]_R \lhd G$，且R就是G关于正规子群$[e]_R$的陪集关系。
- 证：（略）

  （1）$[e]_R \leqslant G$;

  （2）$[e]_R \lhd G$;

  （3）$[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

群同态基本定理

定理

- 设h是群$< G, *, e >$到群$< H, \circ, \mathbb{I} >$的同态，则：

  （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$

  （2）h的同态核K是$< G, *, e >$的正规子群，

  $K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$

  （3）K的陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。

群同态基本定理

定理

- 设h是群$< G, *, e >$到群$< H, \circ, \mathbb{I} >$的同态，则：

  （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G, \ a =_h b \Longleftrightarrow h(a) = h(b)$

  （2）h的同态核K是$< G, *, e >$的正规子群，

  $K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$

  （3）K的陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。

群同态基本定理

定理

- 设h是群$< G, *, e >$到群$< H, \circ, \mathbb{I} >$的同态，则：

  （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$

  （2）h的同态核K是$< G, *, e >$的正规子群，

  $K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$

  （3）K的陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。

群同态基本定理

定理

- 设h是群$< G, *, e >$到群$< H, \circ, \mathbb{I} >$的同态，则：

  （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$

  （2）h的同态核K是$< G, *, e >$的正规子群，

  $K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$

  （3）K的陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。

群同态基本定理

定理

- 设h是群$< G, *, e >$到群$< H, \circ, \mathbb{I} >$的同态，则：

  （1）h诱导的G上的等价关系$=_h$是同余关系，

  $$\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$$

  （2）h的同态核K是$< G, *, e >$的正规子群，

  $$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

  （3）K的陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。

群同态基本定理

定理

- 设h是群$< G, *, e >$到群$< H, \circ, \mathbb{I} >$的同态，则：

  （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$

  （2）h的同态核K是$< G, *, e >$的正规子群，

  $K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$

  （3）K的陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。

群同态基本定理（一）

Proof

- （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$

- 证：

  $\forall a, b, c, d$，若$a =_h b,\ \ c =_h d$，

  则$h(a) = h(b),\ \ h(c) = h(d)$，

  则$h(a * c) = h(a) \circ h(c) = h(b) \circ h(d) = h(b * d)$，

  即$a * c =_h b * d$.

  易证$=_h$是等价关系，所以$=_h$是同余关系。

群同态基本定理（一）

Proof

- （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$

- 证：

  $\forall a, b, c, d$，若$a =_h b$，$c =_h d$，

  则$h(a) = h(b)$，$h(c) = h(d)$，

  则$h(a * c) = h(a) \circ h(c) = h(b) \circ h(d) = h(b * d)$，

  即$a * c =_h b * d.$

  易证$=_h$是等价关系，所以$=_h$是同余关系。

群同态基本定理（一）

Proof

- （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ a =_h b \Longleftrightarrow h(a) = h(b)$
- 证：

  $\forall a, b, c, d$，若$a =_h b$，$c =_h d$，

  则$h(a) = h(b)$，$h(c) = h(d)$，

  则$h(a * c) = h(a) \circ h(c) = h(b) \circ h(d) = h(b * d)$，

  即$a * c =_h b * d$.

  易证$=_h$是等价关系，所以$=_h$是同余关系。

群同态基本定理（一）

Proof

- （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$

- 证：

  $\forall a, b, c, d$，若$a =_h b,\ \ c =_h d$,

  则$h(a) = h(b),\ \ h(c) = h(d)$,

  则$h(a * c) = h(a) \circ h(c) = h(b) \circ h(d) = h(b * d)$,

  即$a * c =_h b * d$.

  易证$=_h$是等价关系，所以$=_h$是同余关系。

群同态基本定理（一）

Proof

- （1）h诱导的G上的等价关系$=_h$是同余关系，

  $\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$

- 证：

  $\forall a, b, c, d$，若$a =_h b,\ \ c =_h d,$

  则$h(a) = h(b),\ \ h(c) = h(d),$

  则$h(a * c) = h(a) \circ h(c) = h(b) \circ h(d) = h(b * d),$

  即$a * c =_h b * d.$

  易证$=_h$是等价关系，所以$=_h$是同余关系。

群同态基本定理（一）

Proof

- （1）h诱导的G上的等价关系$=_h$是同余关系，

  $$\forall a, b \in G, \ a =_h b \Longleftrightarrow h(a) = h(b)$$

- 证：

  $\forall a, b, c, d$，若$a =_h b$，$c =_h d$，

  则$h(a) = h(b)$，$h(c) = h(d)$，

  则$h(a * c) = h(a) \circ h(c) = h(b) \circ h(d) = h(b * d)$，

  即$a * c =_h b * d$.

  易证$=_h$是等价关系，所以$=_h$是同余关系。

群同态基本定理（一）

Proof

- （1）h诱导的G上的等价关系$=_h$是同余关系，

  $$\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$$

- 证：

  $\forall a, b, c, d$，若$a =_h b$，$c =_h d$，

  则$h(a) = h(b)$，$h(c) = h(d)$，

  则$h(a * c) = h(a) \circ h(c) = h(b) \circ h(d) = h(b * d)$，

  即$a * c =_h b * d$.

  易证$=_h$是等价关系，所以$=_h$是同余关系。

群同态基本定理（一）

Proof

- （1）h诱导的G上的等价关系$=_h$是同余关系，

  $$\forall a, b \in G,\ \ a =_h b \Longleftrightarrow h(a) = h(b)$$

- 证：

  $\forall a, b, c, d$，若$a =_h b,\ \ c =_h d$,

  则$h(a) = h(b),\ \ h(c) = h(d)$,

  则$h(a * c) = h(a) \circ h(c) = h(b) \circ h(d) = h(b * d)$,

  即$a * c =_h b * d$.

  易证$=_h$是等价关系，所以$=_h$是同余关系。

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \text{ 有 } h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \ h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \ \therefore \ K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \ a^{-1} * k * a \in K, \ K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a|a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \quad \text{有} h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \quad h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \quad \therefore \quad K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \quad k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \quad a^{-1} * k * a \in K, \quad K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \quad \text{有} h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \quad h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \quad \therefore \quad K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \quad k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \quad a^{-1} * k * a \in K, \quad K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \quad 有 h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \quad h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \quad \therefore \quad K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \quad k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \quad a^{-1} * k * a \in K, \quad K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

  $$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \text{ 有} h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \ h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \ \therefore \ K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \ a^{-1} * k * a \in K, \ K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \text{ 有 } h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \ h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \ \therefore \ K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \ a^{-1} * k * a \in K, \ K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \ \text{有} h(k_1) = h(k_2) = \mathbb{I},$$
$$\therefore \ h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$
$$k_1 * k_2^{-1} \in K, \ \therefore \ K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \ k \in K,$$
$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$
$$\therefore \ a^{-1} * k * a \in K, \ K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \quad 有 h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \quad h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \quad \therefore \quad K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \quad k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \quad a^{-1} * k * a \in K, \quad K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

  $$K = ker(h) \triangleq \{a|a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \text{ 有} h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \ h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \ \therefore \ K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \ a^{-1} * k * a \in K, \ K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

  $$K = ker(h) \triangleq \{a|a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$$\forall k_1, k_2 \in K, \text{ 有} h(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \ h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \ \therefore \ K \leqslant G.$$

② $K \lhd G$:

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$

$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$$\therefore \ a^{-1} * k * a \in K, \ K \lhd G.$$

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a|a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$\forall k_1, k_2 \in K$, 有$h(k_1) = h(k_2) = \mathbb{I}$,

$\therefore\ h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$

$k_1 * k_2^{-1} \in K$, $\therefore\ K \leqslant G$.

② $K \lhd G$:

$\forall a \in G,\ k \in K$,

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$\therefore\ a^{-1} * k * a \in K$, $K \lhd G$.

群同态基本定理（二）

Proof

- （2）h的同态核K是$< G, *, e >$的正规子群，

$$K = ker(h) \triangleq \{a | a \in G \wedge h(a) = h(e) = \mathbb{I}\}$$

- 证：

① $K \leqslant G$:

$\forall k_1, k_2 \in K$, 有$h(k_1) = h(k_2) = \mathbb{I}$,

$\therefore \ h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$

$k_1 * k_2^{-1} \in K$, $\therefore \ K \leqslant G$.

② $K \lhd G$:

$\forall a \in G, \ k \in K$,

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

$\therefore \ a^{-1} * k * a \in K, \ K \lhd G$.

群同态基本定理（三）

Proof

- （3）K陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。
- 证：a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$:

$$\forall a, b \in G,$$

$$a =_h b \Longleftrightarrow h(a) = h(b)$$

$$\Longleftrightarrow h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$$

$$\Longleftrightarrow a^{-1} * b \in K,$$

即，a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$

群同态基本定理（三）

Proof

- （3）K陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。
- 证：a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$:

$$\forall a, b \in G,$$

$$a =_h b \Longleftrightarrow h(a) = h(b)$$

$$\Longleftrightarrow h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$$

$$\Longleftrightarrow a^{-1} * b \in K,$$

即，a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$

群同态基本定理（三）

Proof

- （3）K陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。
- 证：a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$：

  $\forall a, b \in G,$

  $a =_h b \Longleftrightarrow h(a) = h(b)$

  $\Longleftrightarrow h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$

  $\Longleftrightarrow a^{-1} * b \in K,$

  即，a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$

群同态基本定理（三）

Proof

- （3）K陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。
- 证：a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$：

$$\forall a, b \in G,$$

$$a =_h b \Longleftrightarrow h(a) = h(b)$$

$$\Longleftrightarrow h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$$

$$\Longleftrightarrow a^{-1} * b \in K,$$

即，a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$

群同态基本定理（三）

Proof

- （3）K陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。
- 证：a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$：

  $\forall a, b \in G,$

  $a =_h b \Longleftrightarrow h(a) = h(b)$

  $\Longleftrightarrow h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$

  $\Longleftrightarrow a^{-1} * b \in K,$

  即，a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$

群同态基本定理（三）

Proof

- （3）K陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。
- 证：a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$：

$$\forall a, b \in G,$$

$$a =_h b \Longleftrightarrow h(a) = h(b)$$

$$\Longleftrightarrow h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$$

$$\Longleftrightarrow a^{-1} * b \in K,$$

即，a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$

群同态基本定理（三）

Proof

- （3）K陪集关系（正规子群的陪集关系）就等于上述同余关系$=_h$。
- 证：a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$：

$$\forall a, b \in G,$$

$$a =_h b \Longleftrightarrow h(a) = h(b)$$

$$\Longleftrightarrow h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$$

$$\Longleftrightarrow a^{-1} * b \in K,$$

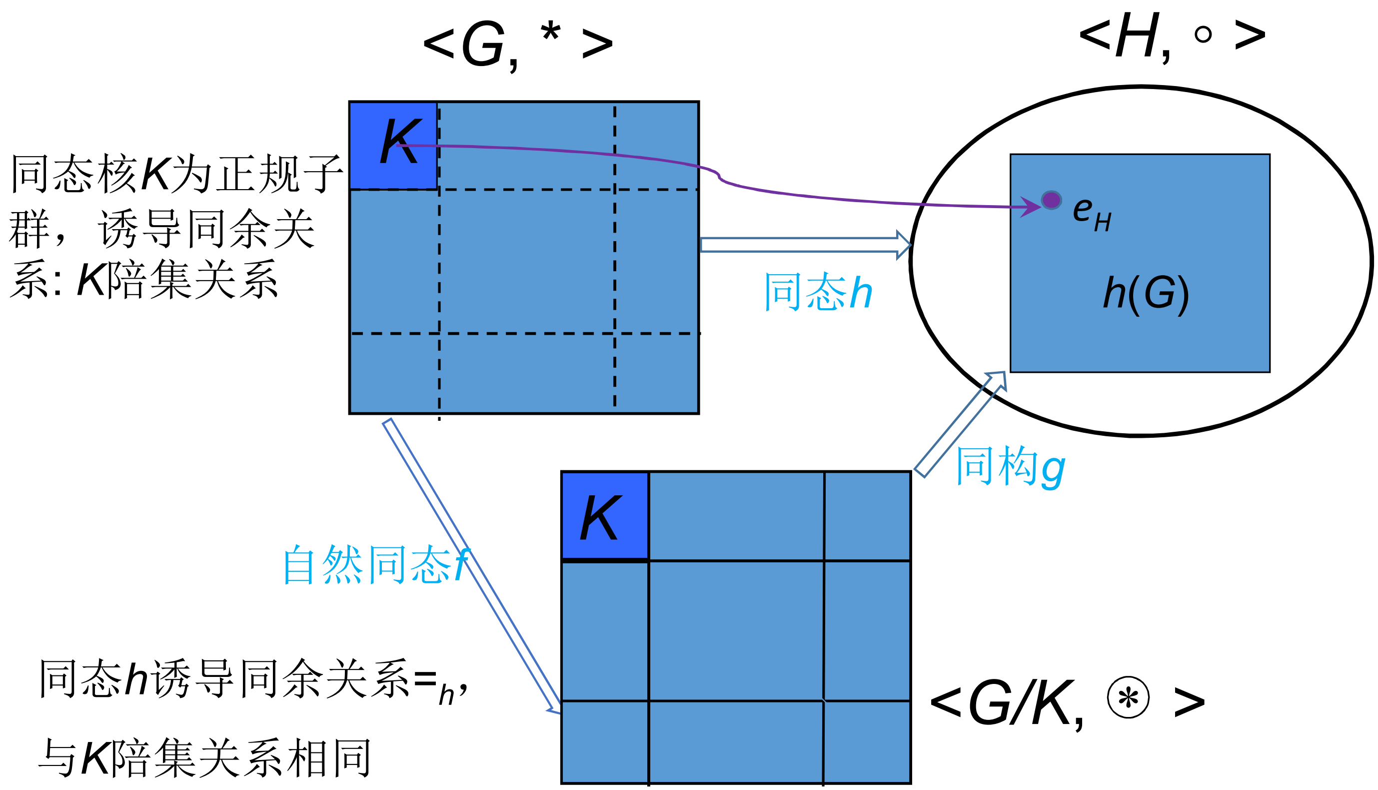
即，a, b有K陪集关系$\Longleftrightarrow$ a, b也有同余关系$=_h$

群同态基本定理

定理

- 设h是从群$< G, * >$到群$< H, \circ >$的同态，K是同态核，则$< G/K, \circledast >$同构于$< h(G), \circ >$.

■ 群同态基本定理：设h是从群〈G，$*$〉到群〈H, ∘〉的同态，K是同态h的核，则〈G/K, ⊛〉同构于〈$h(G)$, ∘〉.



小结

1. 群的性质
   - 群的性质
   - 元素的阶
2. 陪集和拉格朗日定理
   - 陪集的定义和性质
   - 拉格朗日定理
   - 陪集关系