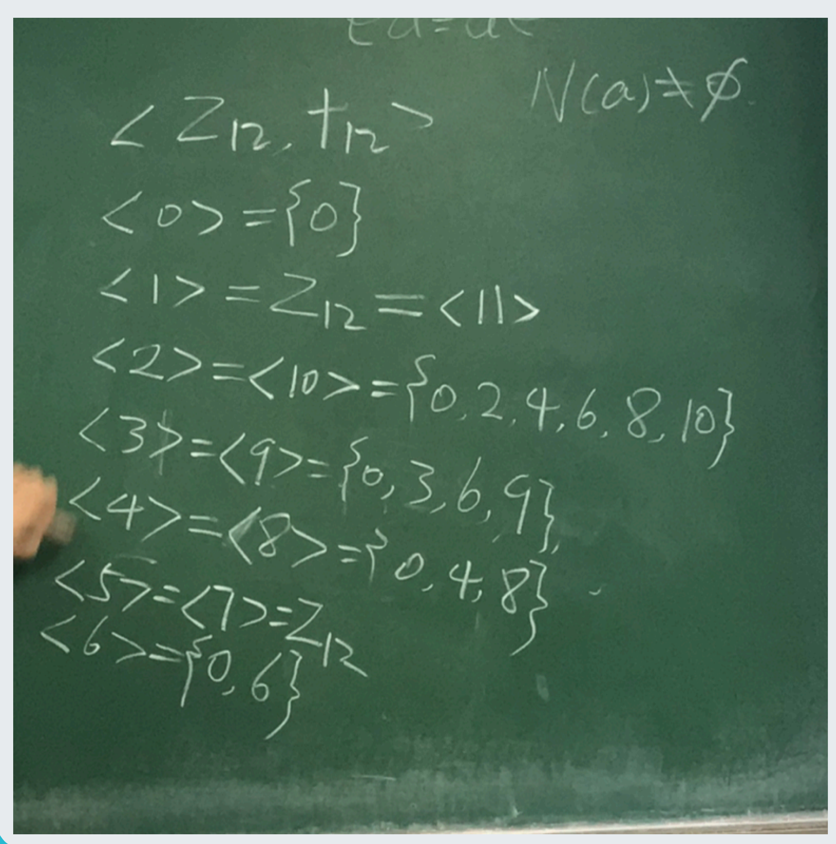
子群

定义 设G为群，H是G的非空子集，若H关于G中运 算构成群，则称H为G的子群，记作$H\le G$. 如果子群H是G的真子集，则称为真子群，记作$H<G$.

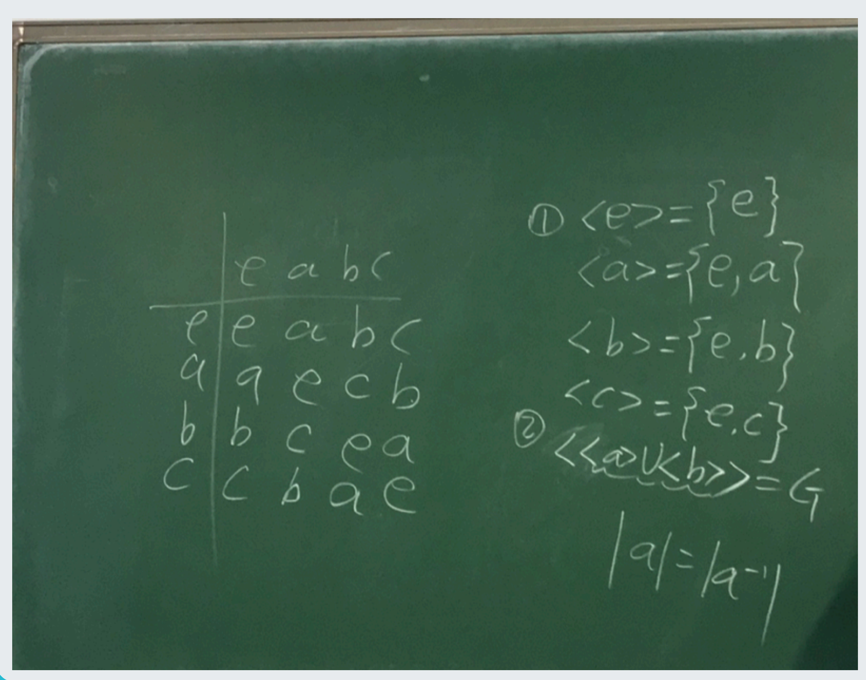
- $xe' = x = xe \Rightarrow e' = e$
- $xx' = e' = e = xx^{-1} \Rightarrow x' = x^{-1}$

重要子群

- a生成的子群 $<a> = \{ a^k \mid k\in Z \}$，$a\in G$
- B生成的子群 $<B>=\cap\{H\mid H\le G, B\subseteq H\}, B\subseteq G$
  - $<B>=\{b^{e_1}b^{e_2}!b^{e_n} \mid b \in B, e =\pm 1, i=1,2,!,n, n\in Z^+\}$ 12nii
- H的正规化子群 $N(H)=\{x\mid x\in G, xHx^{-1}=H\}, H\le G$
- a的正规化子群 $N(a) = \{ x \mid x\in G, xa=ax \}, a\in G$
- 中心 $C = \{ a \mid a\in G, \forall x\in G(ax=xa) \}$
- 共轭子群 $xHx^{-1} = \{ xhx^{-1} \mid h\in H \}$其中$H\le G, x\in G$
- 子群的交
  - $H, K\le G$, 则
  - (1) $H\cap K\le G$
  - (2) $H\cup K\le G \Leftrightarrow H\subseteq K \vee K\subseteq H$
- Z_{12}的子群

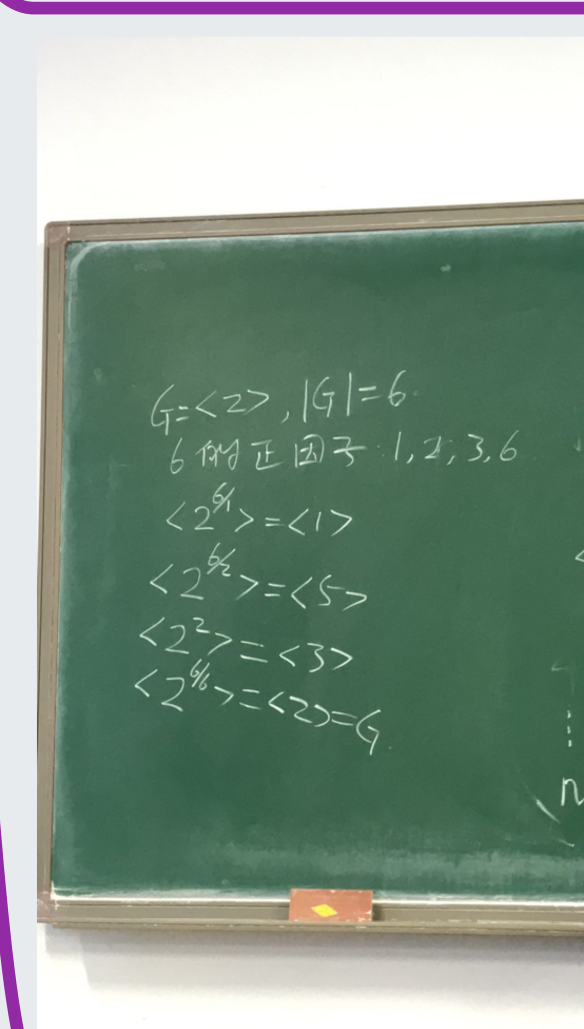


- Klein四元群



循环群

- 定义 $G=<a>=\{a^k \mid k\in Z\}, a\in G$， 称$G$为循环群，$a$为$G$的生成元.
- 分类:
  - (n,r)
    - 定义：n与r的最大公约数
    - 性质：$\exists u,v\in Z\,(un+rv = (n,r))$
      - $(n,r)=1$, n与r互质（互素）
      - $\Leftrightarrow \exists u,v\in Z\,(un+rv=1)$
  - $[n,r]$
    - 定义：n与r的最小公倍数
    - 性质：$[m,n]=\frac{mn}{(m,n)}$
- 生成元的阶无限，则G为无限循环群
- 生成元a为n阶元，则$G=\{e,a,a^2,\cdots,a^{n-1}\}$为$n$阶循环群
- 实例 $<Z,+>$为无限循环群,生成元是1和-1
  $<Z_n,\oplus>$为n阶循环环群，生成元是1、n-1
- 定理1 $G=<a>$是循环群
  - (1) 若G是无限循环群，则G的生成元是a和a^{-1}; (2) 若G是n阶循环群，则G有$\varphi(n)$个生成元，
  - 当n=1 时, $G=<e>$的生成元为e;
  - 当n>1 时, $\forall r(r\in Z^+ \wedge r<n)$, a^r是G的生成元
  - $\Leftrightarrow(n,r)=1$. j(n): 欧拉函数。对于任何正整数n，
  - j(n)是小于等于n且与n互质的正整数个数。



- 定理2 $G=<a>$是循环群，那么
  - (1) G的子群也是循环群
  - (2) 若G是无限阶，则G的子群除$\{e\}$外也是无限阶 (3) 若G是n阶的，则G的子群的阶是n的因子，
  - 对于n的每个正因子d, 在G中有且仅有一个d阶子群.