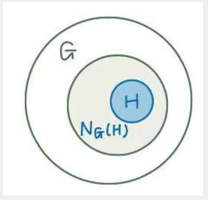
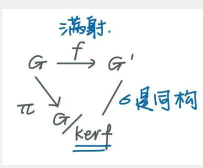
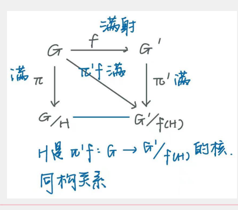
section1 group

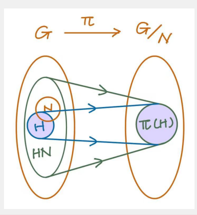
- ❶ 群与半群
  - 证明是群的思路
    - 定义
      - 非空集合
      - 二元运算
      - 结合律
      - （以上三条）半群；幺半群
      - 存在幺元（左幺元）
      - 任意元可逆（任意元存在左幺元）
      - 都换成右也是可以的，但是一左一右就不对了
    - 充要条件
      - 半群
      - $ax=b$、$xa=b$都有解
    - 有限半群满足左右消去律
    - 幺半群中可逆元的全体构成群
  - 群G的运算满足左右消去律
  - 阶
    - 群的阶就是群中元素的个数
    - 群中元素的阶
      - 设$a\in G$，若$\exists n\in N^*, s.t. a^n=e$，而对$\forall m<n$，$m\in N^*$，$a^m\neq e$，则称$a$的阶为$n$;
      - 否则，即对$\forall n\in N^*$，都有$a^n\neq e$，则规定a的阶为∞
      - 有且只有幺元的阶为1
      - G中任意元素a与其逆元素a^{-1}有相同的阶，a与其共轭元bab^{-1}同阶，ab与ba同阶
    - ❗ 群G中每一个非幺元的阶都是2，则G是Abel群
    - 若$a\in G, |a|=d$, 则
      1. $\forall h\in\mathbb{Z}$, 有$a^h=e \iff d|h$
      2. $\forall m,n\in\mathbb{Z}, a^m=a^n \iff d|(m-n)$
      3. $|a^k|=\dfrac{d}{(d,k)}$　　$|a^k|=d \iff (d,k)=1$
      4. $|a|=m, |b|=n$, 当$ab=ba$且$(m,n)=1$时，$|ab|=mn$
      5. 设G为$Abel$群，且G中所有元素有最大阶m，则G中的每个元素的阶都是m的因数

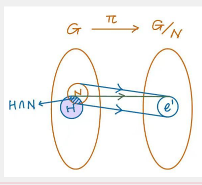
- ❷ 子群与陪集
  - 证明是子群
    - 非空
    - 子集
    - 对群G的运算（乘法和求逆）封闭
      - 对$\forall a,b\in H$, 有$ab\in H, a^{-1}\in H$
      - 对$\forall a,b\in H$, 有$ab^{-1}\in H$
  - 设$H<G, a,b\in G$, 则aH和bH要么互不相交，要么重合，且$aH=bH \iff a^{-1}b\in H$
  - 等价关系
    - 反身性　$\forall a, aRa$
    - 对称性　若aRb, 有bRa
    - 传递性　若aRb且bRc, 有aRc
  - **等价类中的任何元素都可以作为代表元**
    - 若aRb, 则$\bar{a}=\bar{b}$，即等价的两个元素所在的等价类是同一个
  - 商集合
    - 设集合A中有等价关系R，则A中所有不同等价类的集合称为A对R的商集合，记为A/R。
    - 自然映射
      - 设集合A中有等价关系R，则映射$\pi: A\to A/R, \pi(a)=\bar{a}$为$A$到$A/R$的自然映射
      - 若$H\lhd G$，则π是G到商群G/H的自然同态，是满同态
    - 陪集
      - 设H是群G的子群，则由$aRb \iff a^{-1}b\in H$所确定的G中的关系R是一个等价关系，且$\bar{a}=aH$
      - 利用上述等价关系得到的商集合称为G对H的左陪集空间，记为G/H，$|G/H|$称为H在G中的指数，记为$[G:H]$
      - **Lagrange定理**
        - 设G是有限群，$H<G$, 则有$|G|=[G:H]\cdot|H|$
        - $H<G, |H|\mid|G|$, 特别地，$\forall a\in G, |a|\mid|G|$
        - （子群H的阶是群G的阶的因子，任何元素的阶也是｜G｜的因子）
        - G是有限群，$K<G, H<K$, 则有$[G:H]=[G:K]\cdot[K:H]$
  - 一些小结论
    - $H<G, K<G$, 则集合$HK<G \iff HK=KH$
    - H和K为G的有限子群，则有群阶的关系：$|HK|=\dfrac{|H||K|}{|H\cap K|}$
    - 进一步要求H和K有限
  - $\mathbb{Z}_n$
    - $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$
    - $m_1\mathbb{Z}\cap m_2\mathbb{Z}\cap\cdots\cap m_k\mathbb{Z}=[m_1,m_2,\cdots,m_k]\mathbb{Z}$
    - 任取无穷多个两两不同的整数$\{m_k\}_{k\in\mathbb{N}}$, $\bigcap_{k\in\mathbb{N}} m_k\mathbb{Z}=\{0\}$

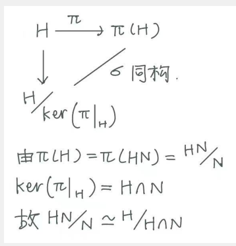
- ❸ 正规子群与商群
  - 证明是正规子群
    - 充要条件
      - 对$\forall g\in G$，$\forall h\in H, ghg^{-1}\in H$
      - 对$\forall g\in G$，$gH=Hg$
      - 对$\forall a,b\in G$，$aH\cdot bH=abH$
    - 充分条件
      - ❗ $[G:H]=2$
      - Abel群的任何子群都是正规子群
  - 关于正规子群的小结论　$N\lhd G$, 取$\forall H<G$, 则
    - (1) $HN=NH$
    - (2) $HN<G$, 且$N\lhd HN$
    - (3) $N\cap H\lhd H$
  - 传递性
    - 子群具有传递性，正规子群不具有传递性
    - 设$H<G, N\lhd G$, 则$H\cap N\lhd H$
  - 共轭关系
    - 设$a,b\in G$, 若$\exists g\in G, s.t. a=gbg^{-1}$, 则称$a$与$b$共轭
    - 共轭关系是等价关系，设$C_a=\{b\mid b与a共轭\}$，从而共轭类C_a成了G的一个分划
    - 如果一个元素只与它自身共轭 $\iff a\in C(G)=\{a\in G\mid ag=ga\}$；$C(G)$称为$G$的中心
    - 群G是一个有限群，它的类方程$|G|=c_0+c_1+\ldots+c_m$, 其中c_0表示$C(G)$中的元素，c_i表示其他共轭类中的元素
  - 正规化子与中心化子
    - S是G的一个非空子集，称$N_G(S)=\{x\mid x\in G, xS=Sx\}$为$S$在$G$中的正规化子
    - 元素a的正规化子简记为$N_G(a)$或$N(a)$
    - 设$H<G$, 则
      - (1)$N_G(H)<G$且$H\lhd N_G(H)$
      - (2)$H\lhd G \iff N_G(H)=G$
      - 

- ❹ 群的同态与同构
  - 核和像
    - 设$f: G\to G'$是群同态
      - $Kerf=\{a\in G\mid f(a)=e'\}$, 称为同态$f$的核
      - $Im(f)=\{f(a)\mid a\in G\}$, 称为同态$f$的像
      - （以上两条）$Imf<G', Kerf\lhd G$
      - f为单射 $\iff Kerf=\{e\}$
    - 若$H<G$, 则$H\lhd G \iff \exists$群G', 同态$f: G\to G', s.t. Kerf=H$
  - 证明是同构
    - 有时需要先证明well-defined　比如对应关系涉及代表元的选取，良定性保证不出现一对多
    - 证明是同态　$f(ab)=f(a)f(b)$
    - 证明是双射
  - 同态基本定理
    - 设$f: G\to G'$是满同态，则$G/kerf\simeq G'$
    - 

    - 推论　如果f不是满射，我们可将其看作G到$f(G)$的满同态，即$G/kerf=f(G)$
  - 定理1.4.21　设$f: G\to G'$是满同态，$N=kerf$
    - (1)f建立了K与$f(K)$的双射，其中，$K<G$且$K\supseteq N, f(K)<G'$
    - (2)f把正规子群映到正规子群
    - (3)若$H\lhd G, N\subseteq H$, 则$G/H\simeq G'/f(H)$
    - 

  - 定理1.4.23　$N\lhd G, \pi: G\to G/H$(自然同态), $H<G$, 则
    - (1)$HN<G$且$N\subseteq HN$, 且$HN=\pi^{-1}(\pi(H))$, 即HN是H在映射π下的像集合$\pi(H)$的完全原像$\pi^{-1}(\pi(H))$
    - 

    - (2)$Ker(\pi|_H)=H\cap N$，从而$(H\cup N)\lhd H$
    - 

    - (3)$HN/N\simeq H/(H\cap N)$　　$|HN|=\dfrac{|H||N|}{|H\cap N|}$
    - 

  - 自同构群
    - 群G到自身的同构映射称为G的内自同构，群G的全体内自同构的集合记为$AutG$
    - $AutG<S_G$
    - 无限循环群的自同构群是一个2阶循环群；
    - n阶循环群的自同构群是一个$\varphi(n)$阶群，其中$\varphi(n)$为$Euler$函数(与n互质的数的个数)
    - 设G是有限$Abel$群，$\varphi(g)=g^k$是G的自同态，则φ_k是G的自同构 $\iff (k,|G|)=1$
  - 内自同构群
    - 对$\forall a\in G$，定义映射$\sigma_a: G\to G, s.t. g\to aga^{-1}, \forall g\in G$;
    - $\sigma_a\in AutG$, 称为由a决定的内自同构，记$InnG=\{\sigma_a\mid a\in G\}, InnG\lhd AutG$
    - 设$f: G\to InnG, s.t. f(a)=\sigma_a, Kerf=C(G)$, 由同态基本定理，$G/C(G)\simeq InnG$

- ❺ 循环群
  - 定义
    - S是G中一个非空子集，$S^{-1}=\{a^{-1}| a\in S\}$, 记$\langle S\rangle=\{x_1x_2\ldots x_m\mid m\in\mathbb{N}, x_1x_2\cdots x_m\in S\cup S^{-1}\}$
    - 如果$\langle S\rangle=G$，则S为群G的一个生成组；如果群G有一个有限的生成组，则G为有限生成群
    - 若$G=\langle a\rangle$, 即群G可以由一个元素a生成，这时称G为循环群，称a为这个循环群的生成元
  - 循环群的同态与同构
    - 无限循环群与$\{\mathbb{Z};+\}$同构，有限n阶循环群与$\{\mathbb{Z}_n;+\}$同构
    - 两个循环群同构当且仅当它们有相同的阶
    - $G=\langle a\rangle, Hom(G)=\{\varphi: G\to G|a\mapsto a^l, l\in\mathbb{Z}\}$
    - 如上φ是自同构当且仅当l与$|G|$互素　$Aut(G)=\{\varphi: G\to G|a\mapsto a^l, (l,|G|)=1\}$
  - 循环群的子群
    - 循环群$G=\langle a\rangle$的任意子群都形如$\langle a^l\rangle, l\in\mathbb{N}$, 从而也是循环群
    - G是n阶群，则：G是循环群 $\iff$ 对$\forall k, k|n$, 存在G的唯一k阶子群
    - G为$Abel$群，则：G为单群 $\iff G$为素数阶循环群
    - $Lagrange$定理的逆定理不成立(反例为S_3没有2阶正规子群)　但是对于循环群是成立的

- ❻ 对称群与交错群
  - 置换
    - 对称群S_n中的一个n元置换σ是$\{1,2,\cdots, n\}$到自身的双射，设$\sigma(k)=i_k$, 表示为：$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$
    - n元置换的个数，也就是1，2,$\cdots$，n排列的个数，即S_n的阶为$n!$
    - 一个n元置换可以有$n!$种记法
    - S_n中的任何元素σ都可表示为S_n中一些不相交的轮换之积，且表法唯一(不计次序)
    - **任何一个有限群与一个置换群同构**
      - $Cayley$定理：任何一个群都与对称群S_G的子群同构
        - 令$T=\{L_a|a\in G, L_a$为由a决定的左平移变换$\}$，$G\simeq T<S_G$
        - (注：右平移变换R_a是反同态)
    - 当$n\geqslant 3$时，S_n的中心$C(S_n)=\{(1)\}$
  - r-轮换
    - $\sigma=(i_1i_2\cdots i_r)$
      - $\sigma(i_1)=i_2, \sigma(i_2)=i_3,\cdots, \sigma(i_{r-1})=i_r, \sigma(i_r)=i_1; \sigma(k)=k, \forall k\in\{i_1,i_2,\cdots, i_r\}$
      - 称$i_1i_2\cdots i_{为}$轮换σ的文字, r称为轮换σ的长
      - 2-轮换称为对换，1-轮换就是恒等置换
      - S_n中的两个不相交的轮换是可交换的
    - 任何一个r-轮换都可写成r-1个对换的乘积
    - 任何一个n元置换都可写成一些对换的乘积
      - 对换个数的奇偶性不变
      - 表示为奇（偶）数个对换的乘积，称为奇（偶）置换
    - ❗ 设$\sigma=\sigma_1\sigma_2\cdots\sigma_s$, 其中$\sigma_i$表示$r_i-$轮换，$\sigma$的阶为$[r_1,r_2,\cdots,r_s]$
    - **两个轮换共轭当且仅当它们的长度相同**
      - ❗ 对$\forall\sigma\in S_n$，$\sigma(i_1i_2\cdots i_r)\sigma^{-1}=\big(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r)\big)$
  - 交错群
    - n元偶置换的全体是$A_n, A_n\lhd S_n$, 称为n元交错群　$n\geqslant 2$时，$|A_n|=\dfrac{n!}{2}$
    - A_1, A_2都是平凡群，A_3是3阶循环群，A_4是12阶群；
    - $\{(1),(12)(34),(13)(24),(14)(23)\}$(记作$K_4$, 同构于$Klein$群)是$A_4$的正规子群，也是唯一的非平凡正规子群
    - $n\geqslant 5$时，A_n都是单群
  - 1~8阶的群结构

|G|	Abel群	非Abel群
1	{e}	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4, \mathbb{K}_4$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	$\mathbb{S}_3(\mathbb{D}_3)$
7	$\mathbb{Z}_7$	
8	${\mathbb{Z}_2}^3, \mathbb{Z}_2\oplus\mathbb{Z}_4, \mathbb{Z}_8$	$\mathbb{Q}_4, \mathbb{D}_4$

    - 分析低阶群结构通过元素的阶来分类讨论