内含
- 非空集合
- 代数运算
  - 结合律 $(a*b)*c = a*(b*c)$ → 其群满足结合律，称为乘法群
    - $a\cdot a\cdot a\cdots a = a^n$
    - 单位元 $a^0 = 1$
    - $a^{-n} = (a^n)^{-1} = (a^{-1})^n$
    - $a^m \cdot a^n = a^{m+n}$
    - $(a^m)^n = a^{mn}$
  - 交换律 $a*b = b*a$
  - 幂等律 $a*a = a$
  - 分配律 (*对+满足) $\Rightarrow a*(b+c) = (a*b)+(a*c)$
    $(b+c)*a = (b*a)+(c*a)$
  - 吸收律 (*与+满足) $\Rightarrow a*(a+b) = a$
    $a+(a*b) = a$
  - 消去律 若 $a*b = a*c$ 则 $b = c$
    $b*a = c*a$ 则 $b = c$

运算唯一 ~~[illegible]~~，且不可 $a*a=a$

证法
- Ⅰ ①半群 ②有1 ③有逆
- Ⅱ ①左1：$1\cdot a = a$ ②左逆 $a^{-1}\cdot a = 1$
- Ⅲ 有 $x\in G$ 使 $x\cdot a = b$，有 $y\in G$ 使 $a\cdot y = b$

元素1称为此半群/群的单位元，a^{-1}称为a的逆元素

半群 ①非空 ②封闭 ③满足结合律
→ 有1：$1\cdot a = a\cdot 1 = a$；有逆：$a\cdot a^{-1} = a^{-1}\cdot a = 1$ → 群

群必满足消去律

环中乘法不一定满足消去律，也不是群

群必不满足幂等律

任意元素都大有一个且为循环群

分类
- Abel群/交换群：满足交换律
  - 称为加法来，运算符号一般写作 +
  - $a+b = b+a$
  - 单位元 $a+0 = a$
  - 逆元：$a+(-a) = 0$ 不可写作 $a-a=0$
  - $(m+n)a = ma+na$
  - $m(a+b) = ma+mb$ m、n是整数，不属于群
  - $m(na) = (mn)a$
- n次对称群
  - n元置换全体作成的集合 S_n 对置换的乘法作成的群
  - 置换 $\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$
    - 乘法 $\sigma\cdot\tau(a) = \sigma\cdot(\tau(a))$
    - 单位元：n元恒等置换 $\begin{pmatrix} a_1 & a_2 & a_3 & \cdots \\ a_1 & a_2 & a_3 & \end{pmatrix}$
    - 逆元：$\begin{pmatrix} a_1 & a_2 & \cdots \\ b_1 & b_2 & \end{pmatrix}^{-1} = \begin{pmatrix} b_1 & b_2 & \cdots \\ a_1 & a_2 & \end{pmatrix}$
  - 轮换 $\sigma = (a_1\ a_3\ a_4\cdots a_q)$
    - 若 σ_1 与 σ_2 中元素不相同，则称其不相交，其乘法适合结合律
    - 任意置换可写成不相交轮换乘积形式
  - 对换 $\sigma = (a_1\ a_3)$（长度为2的轮换）
    - 任意轮换可写成对换的乘积
    - 奇置换：可表示为奇数个对换之积
    - 偶置换：同上
    - 元数 − 几个轮换（包含长度为1的）
  - S_n 中奇置换与偶置换个数相等（当 $n>1$）
- n次交换群：n元置换中所有偶置换组成的群

- 子群
  - 分类
    - 平凡子群：{1} 与 G本身
    - 非平凡子群
  - 证法（H是G的子集）
    - I：① $a\in H$ $b\in H$，则 $ab\in H$ ② $a\in H$ 则 $a^{-1}\in H$ ③H非空
    - II：① $a\in H$，$b\in H$，则 $ab^{-1}\in H$ ② H非空
    - III：H对G的运算是封闭的 $a\in H$ $b\in H$ 则 $ab\in H$（H是有限非空集）
  - 子群内必包含原群中单位元
  - 循环子群：$a\in G$，a的所有幂 a^n 做成的G的一个子群(a)
    - 不同元素生成的循环子群可能是相同的
    - 循环子群元数一定整除G自身元数
    - 循环子群元数=周期
    - 求循环子群类题：I 生成子群的元的阶数必为G的阶数的因数
  - 子群陪集
    - $\forall g\in G$，$gH=Hg$ 子群无论左右一定为正规子群
    - 证明：$\forall g\in G$，$gHg^{-1}\subseteq H$

子群元素个数是整除群的元数

- 循环群/巡回群（循环群必为交换群）
  - 可由它的某元素a生成 $G=(a)$
  - a为G的生成元
  - 循环群生成元不一定
  - 循环群中元素的周期必为除整个群元数
  - 分类
    - 无穷循环群：a的周期为∞或无穷大，生成元为a及a^{-1}
    - n元循环群
      - 共n个元素
      - 生成元a，$a^n=1$
      - a的周期为n
      - a^k为(a)生成元的充要条件为(n,k)=1互质
      - 故(a)共有$\varphi(n)$个生成元（n小且与n互质）

（与任何数互质，数与自己不互质）

- 陪集
  - 合同关系：H为G的子群，$h\in H$，$ab\in G$，$a=bh$，则a合同于b(右模H)
  - 右陪集
    - G在合同关系(右模H)下的等价类称为H的右陪集
    - H本身也是H自己的一个右陪集
    - H在G中指数：G的元数除以H的元数所得的商，记为(G:H)（H的指数即H的右陪集个数）
    - H元数=H的陪集的元数
    - $aH=bH$ 充要条件为 $a^{-1}b\in H$（a、b在同一右陪集的充要）

- 同态映射
  - 定义：(G,·)是一个群，(K,*)是一个代数系统，称G到K的一个映射σ为一个同态映射，若：$\sigma(a\cdot b)=\sigma(a)*\sigma(b)$（$\sigma(ab)=\sigma(a)\sigma(b)$）
  - 若所有σ(G)仅为K中部分元素，称σ为G到K内的一个同态映射
  - G'中同态像的元数≤原G群中元数.
  - 证明：
    - ①证σ为映射
      - G中任意元素，在K中都有唯一元素与之对应
    - ②证同态性
  - $G'=\sigma(G)$必为群，其中$\sigma(1)$即为G'的单位元，若K为群，则G'必为K的子群
  - G'的原象集合，便是映射.

同态核：$N=\underline{\sigma^{-1}(1')}=\{g\in G \mid \sigma(g)=1'\}$ 即称N为σ的核
↳ G'中的单位元

核N必为G的一个正规子群

G'的元素与N在G中的陪集一一对应，且这些陪集互不相交

商群：映射：N的所有陪集与陪集间乘法作成一个群$\bar{G}$，令$\sigma: a\to aN$
则σ是G到$\bar{G}$上的一个同态映射，其核为N

$\bar{G}$称为G对N的商群，记为G/N，若G为有限群，则商群中元素个数等于N在G中的指数，即其陪集个数

构建同态：已给群G，同态核N，构造G'与σ，使$\sigma(N)=1'$ $G\xrightarrow{\sigma}G'$

定理：设σ为G到G'上的一个同态映射，若σ的核为N，则$G'\cong \frac{G}{N}$

性质：当且仅当 $N\le H$，$\sigma^{-1}(\sigma(H))=H$
若H为G子群，$H'=\sigma(H)$，σ^{-1}不一定$=H$不一定$=NH$

同构映射：定义：σ为G到$\sigma(G)$上的1-1同态映射，称G与$\sigma(G)$同构，记为$G\cong\sigma(G)$

证明：①映射 ②单射 ③满射 ④同态性

群与群间可存在多个同构映射

自同构映射：G到G上的同构映射，不唯一

环：构成：非空集合R
运算：加法、乘法两种

证明：①非空 ②加封闭 ③乘封闭

让R对加法构成Abel群：
④ $a+(b+c)=(a+b)+c$
⑤ $\exists 0\in R$，使 $a+0=a$
⑥ $\forall a\in R$，$\exists -a$ 使 $a+(-a)=0$
⑦ $a+b=b+a$

让R对乘法构成半群：
⑧ $a(bc)=(ab)c$

让乘法对加法满足分配律：
⑨ $a(b+c)=(ab)+(ac)$
$(a+b)c=(ac)+(bc)$

性质：
1. m为整数，$a,b\in$环R
$a(mb)=(ma)b=\underline{m(ab)}$ → 不是m乘(ab)，而是m个(ab)相加
特别的：$0a=\underline{0}$ 0个a相加=R的单位元
整数0 环R的单位元
2. $a0=0$ $0a=0$ 0为R中单位元
3. $a(c+(-b))=ac+(-ab)$ $(c+(-b))a=(a+(-b)a)$
4. $a(-b)=-(ab)$ $(-a)b=-(ab)$ $(-a)(-b)=ab$
5. $a^{m+n}=a^m a^n$ $(a^m)^n=a^{mn}$ 乘法不是群，无单位元，不满足$a^0=1$
6. 若有$a,b\in R$，$a\neq 0$，$b\neq 0$，但$ab=0$，则称a、b为零因子

分类

交换环
- 定义：乘法满足交换律的环
- 性质：$(ab)^n=a^nb^n$
  $(a+b)^n=$ 二项式定理

消去环
- 定义：无零因子的环
- R为消去环当且仅当R中非零元消去律成立 → 针对乘法
- 性质：~~非0的元素在加法下周期相同，且为0或为质数~~
  $nb=0$ 则b周期为n
  0周期为1

有1环
- 定义：环R不只有1个元素，且有一个元素满足 $1a=a1=a$，则称R为含单位元的环
- 证明：①环 ②积1个元素
  ③$1\cdot a=a\cdot 1=1$
  0是加法单位元，1是乘法单位元
  但不代表此时乘法是群
- 性质：含1环的1唯一且≠0
- 任意环R均可扩充成一个含1环 R^+

整区：交换 + 消去 + 有1

子环
- 证明
  ① $S\neq\varnothing$
  ② $a\in S, b\in S$，则 $a-b\in S$
  ③ $ab\in S$
- 乘法群的1与其子群1一致，但环的1未必与子环的1一致，子环有没有1都不一定
  R与{0}是R的平凡子环

环有1 ⇏ 子环有1
子环有1 ⇏ 环有1

体
- 条件：若去掉0后R的其余元素可以作成一个乘法群
- 体有①1且②无零因子，其中任意非零元素有逆
  但有1且无零因子的不一定是体
- 域
  - 条件：交换体
  - 域中，ab^{-1} 可写作 a/b
- 体的子环若仍为体，则叫子体；若又为域，则叫子域，
  同样，对域F，也有F的子环与子域