群：

① ② ③ ④.

定义：封闭　结合律　单位元　逆元

①② $\Rightarrow$ 半群　　$\Downarrow$ 消去律

①②③ $\Rightarrow$ 含幺半群　（注意环中元）.

交换群（Abel群）　交换律

单位元逆元唯一.

"n阶元"　n是使 $a^n = e$ 的最小整数.

有限群，阶有限

子群：$\forall a, b \in H$　$a * b \in H$　子群也是群.

$\forall a \in H$，$a' \in H$

循环群 $\langle G, * \rangle$，$g \in G$，$G = \{g^n \mid n \in \mathbb{Z}\}$.

记为 $\langle g \rangle$　g：生成元.

同构于 模n加法群.

置换群：置换：$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix} = [12345]$

一种重排列的方式 $\begin{bmatrix} 1 & 3 & 2 & 5 & 4 \\ 3 & 2 & 5 & 4 & 1 \end{bmatrix} = [13254]$.

置换合成不满足交换律.

所有群与一个置换群同构

群同构

$\langle G_1, * \rangle$ $\langle G_2, \cdot \rangle$ 同构

$\varphi(a * b) = \varphi(a) \cdot \varphi(b)$ φ 双射.

特点：保持运算

$$\begin{array}{ccc} a, b & \xrightarrow{\ *\ } & a * b \\ \downarrow \varphi & & \downarrow \varphi \\ \varphi(a), \varphi(b) & \xrightarrow{\ \cdot\ } & \varphi(a * b) \end{array}$$

商群

"模 H 同余" H：子群，$h_1, h_2 \in H$.

对 $\exists h_1, h_2 \in H$ st. $\underline{a \cdot h_1 = b \cdot h_2}$

$\Updownarrow$

$\Rightarrow a \equiv b \pmod H$ $a \cdot b^{-1} \in H$.

模 H 同余的集合：$Ha = \{ h * a \mid h \in H \}$.

"右陪集" $\longrightarrow$ a：代表元.

"左陪集"即 $aH = \cdots\cdots$

左陪集 = 右陪集 $\Rightarrow$ 正规子群 H

正规子群：$\forall g, h$，$g^{-1} * h * g \in H$.

Lagrange 定理 $|G| = \overset{=k}{[G:H]}\,|H|$ $\underline{\dfrac{|G|}{|H|} \in \mathbb{Z}}$ ☆.

可进行陪集分割

陪集间不相交. $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$

素数阶群都是循环群

$|H|, |K|$ 都是子群 $|HK| = \dfrac{|H|\,|K|}{|H \cap K|}$

商群：

N：正规子群

$\langle \{Ng \mid g\in G\}, \cdot \rangle$ 为 G/N.

右陪集乘法：$Ng_1 \cdot Ng_2 = \{(n_1 * g_1 * n_2 * g_2) \mid n_1, n_2 \in N\}$

$= N(g_1 * g_2)$.

商群元素个数 $|G/N| = |G| / |N|$

群同态：$f: G_1 \to G_2$ $\boxed{\text{不确定讲过没}}$

$f(a*b) = f(a)\cdot f(b)$

"类似同构，不要求双射

~~Ker~~ $\mathrm{Ker} f = \{a \mid a\in G_1, f(a) = e_2\}$.

映射到 G_2 中单位元. ~~Ker~~

$\mathrm{Ker} f$ 是 G_1 的正规子群.

群同态基本定理. $G_1 / \mathrm{Ker} f = G_2$.

G_1 是按同态核 $\mathrm{Ker} f$ 映到 G_2 的.

推论：H, K 是 G 正规子群，$K \subseteq H$.

$$G/H \cong \frac{G/K}{\cancel{G/}\, H/K}$$

环：$\langle R, +, \cdot \rangle$.

$\langle R, + \rangle$ 交换群．$\langle R, \cdot \rangle$ 半群 $\Rightarrow$ 不可逆.

乘法分配律 体现"+"与"·"联系

交换环：$a \cdot b = b \cdot a$

常见环：$\langle Z, +, \times \rangle$，$\langle$多项式$, +, \cdot \rangle$

0_R：零元　1_R 乘法单位元

整环：交换环，$m \cdot n = 0 \Rightarrow m = 0$ or $n = 0$

无 0 division

有乘法单位元　素元必是不可约元

整环中有左右消去律.

$a * b = a * c$.

$a * (b - c) = 0$.　$a = 0$ or $(b - c) = 0$

域：有限整环.

理想：I 是理想，I 封闭 $(+, *)$.

$\forall\, r \in R$，$i \in I$，$ir, ri \in I$.

主理想：$(a) = \{a \cdot r \mid r \in R\}$.

"由 a 生成的理想"

主理想环：所有理想是主理想

环内概念

整除 $a|b \Leftrightarrow \exists n$ st. $an=b$

素元 $q|n\cdot m \Rightarrow q|n$ or $q|m$

不可约元 $q=q_1q_2 \Rightarrow q_1$ or q_2 是单位

单位: $a\cdot b=1_R,\ b\cdot a=1_R$

a,b 是单位. 单位即有乘法逆元.

素理想: R: 交换环 P: 素理想 $P\neq R$

$r_1,r_2\in R,\ r_1 * r_2\in P.$

$\Rightarrow r_1\in P$ or $r_2\in P$

极大理想: R: 环 M: 极大理想

真包含 M 的理想只有 R.

讨 $M\subseteq I \Rightarrow I=M$ or $I=R$.

主理想环:

$$\begin{array}{ccc} \text{极大理想} & \Leftrightarrow & \text{素理想} \\ \Updownarrow & & \Updownarrow \\ \text{不可约元} & \Leftrightarrow & \text{素元} \end{array}$$