代数 1 H 课程讲义

Instructor: 余成龙
Notes Taker: 刘博文, 唐龙天

Qiuzhen College, Tsinghua University
2022 Spring

课程信息:

- 授课人: 余成龙;
- 办公室: 近春园西楼 260;
- 邮箱: yuchenglong@mail.tsinghua.edu.cn;
- 成绩分布: 作业 (20%) + 期中 (30%) + 期末 (50%), 习题课讲题加分项;
- 参考书: M.Artin *Algebra*, 姚慕生 抽象代数学, S.Lang *Algebra*.

内容大纲:

- 群;
- 环 (交换环);
- 模 (环上的线性代数);
- 二次型.

目录

第一章　第一周

1.1　九月十三日

定义 1.1.1. 群 $(G,\cdot)$ 是指一个非空集合 G, 有一个 "二元运算". 这里运算是指映射

$$G\times G\to G$$
$$(a,b)\mapsto a\cdot b=:ab.$$

输入一个有序对 (a,b), 输出 $ab\in G$. 且 $\cdot$ 满足

1. 结合律 (Associativity): 对任意 $a,b,c\in G$ 有 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.
2. 单位元/恒等元 (Identity element): 存在 $e\in G$ 使得对任意 $a\in G$ 有 $ae=ea=a$.
3. 逆 (Inverse) 对任意 $a\in G$, 存在 $b\in G$ 使得 $ab=ba=e$.

注记. 结合律保证记号 $a_1a_2\cdots a_n$ 无歧义.

例子.
- $(\mathbb{Z},+)$, 0 是单位元;
- 对正整数 n, 模 n 同余类有群结构 $(\mathbb{Z}/n\mathbb{Z},+)$.
- $(\mathbb{Q},+)$ 和 $(\mathbb{Q}^\times=\mathbb{Q}\backslash\{0\},\times)$ 是群.
- 对素数 p, $(\mathbb{F}_p^\times=\mathbb{Z}/p\mathbb{Z}\backslash\{\bar{0}\},\times)$ 是群.

同样有许多反例:
- (奇数, $+$) 不是群, 因为 "二元运算" 不良定义;
- $\mathbb{Z}_{\geq 0}$ 不是群, 因为不存在逆元;
- $(\mathbb{R}^3$, 叉乘) 不是群, 因为没有结合律.

问题 1.1.2. 思考是否存在不满足结合律, 但有单位元和逆的结构?

命题 1.1.3. 单位元唯一, 即 $e_1,e_2\in G$ 都是单位元, 则有 $e_1=e_2$.

证明: 注意到 $e_1=e_1e_2=e_2$. □

命题 1.1.4. 逆元唯一, 即若 b,c 都是 a 的逆元, 则 $b=c$

证明: 考虑 bac, 我们有

$$c=ec=(ba)c=b(ac)=be=b.$$

□

我们现在可以记 a^{-1} 为 a 的逆元. 对任意 $n\in\mathbb{Z}_{>0}$, 令 $a^n=\underbrace{a\cdots a}_{n\text{ 个}}$, 令 $a^{-n}=(a^{-1})^n$; 对 $n=0$, 令 $a^0=e$.

练习. 验证: $a^{-n}=(a^{-1})^n$, $(a^m)^n=a^{mn}$, $a^ma^n=a^{m+n}$.

一个重要的例子是 n 元置换群 (Permutation group/Symmetric group). 用 $[n]$ 表示 n 元集合 $\{1,2,\cdots,n\}$.

定义 1.1.5. 集合 $S_n=\{\sigma\colon [n]\to[n]\mid \sigma \text{ 双射}\}$ 可以定义二元算

$$\sigma\tau:=\sigma\cdot\tau$$

是映射的复合, 即 $(\sigma\cdot\tau)(i)=\sigma(\tau(i))$.

例子. 通常将置换记为

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix},$$

也可以记为 $\sigma=\sigma(1),\cdot,\sigma(n)$, 通常称为 $1,\cdots,n$ 的排列.

命题 1.1.6. $(S_n,\cdot)$ 是群.

证明: (0) 二元运算良定义, 因为单射复合单射还是单射, 满射复合满射还是满射.

(1) 结合性. 对任意 $\sigma_1,\sigma_2,\sigma_3\in S_n$, 我们有

$$\begin{aligned}((\sigma_1\sigma_2)\sigma_3)(i)&=(\sigma_1\sigma_2)(\sigma_3(i))\\ &=\sigma_1(\sigma_2(\sigma_3(i)))\\ (\sigma_1(\sigma_2\sigma_3))(i)&=\sigma_1(\sigma_2(\sigma_3(i))).\end{aligned}$$

从而有 $(\sigma_1\sigma_2)\sigma_3=\sigma_1(\sigma_2\sigma_3)$.

(2) 恒等元. 定义 $e\colon[n]\to[n]$ 满足 $e(i)=i$. 验证知

$$\begin{aligned}\sigma e(i)&=\sigma(e(i))=\sigma(i)\\ e\sigma(i)&=e(\sigma(i))=\sigma(i)\end{aligned}$$

从而有 $e\sigma=\sigma e=\sigma$.

(3) 逆. σ 满射, 则对任意 $i\in[n]$, 存在 $j\in[n]$ 使得 $\sigma(j)=i$. 定义

$$\begin{aligned}\tau\colon[n]&\to[n]\\ i&\mapsto j\end{aligned}$$

由于 σ 是双射, 知 τ 也是双射. 且 $\sigma\tau(i)=\sigma(j)=i$. 利用结合律, 有

$$\sigma(\tau(\sigma(i)))=(\sigma\tau)(\sigma(i))=\sigma(i).$$

又由于 σ 是双射, 则有 $\tau\sigma(i)=i$, 从而 $\tau\sigma=\sigma\tau=e$.

□

注记. 对一般 $f\colon X\to Y$ 双射, 存在 $g\colon Y\to X$ 使得 $f\circ g=\mathrm{Id}_Y$ 及 $g\circ f=\mathrm{Id}_X$. g 记作 f^{-1}. τ 也是如此定义, 记作 σ^{-1}, 无歧义.

定义 1.1.7. 群 G 的元素个数称为阶 (order), 记作 $|G|$.

命题 1.1.8. 对于置换群有 $|S_n| = n!$.

例子. 考虑 S_3, 令

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

计算得

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} = (132), \ \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix} = (213)$$

这告诉我们 $\sigma\tau \neq \tau\sigma$, 即 S_3 不是交换群. 我们也可以用另外一种看法, 即 σ 交换 $1,3$ 位置. 因此 $\sigma\tau = 213$. 而 τ 是向后平移次, 从而

$$\tau\sigma = \text{ 平移 } 321 = 132 \neq \sigma\tau.$$

定义 1.1.9. 群 $(G, \cdot)$ 称为 Abel 群, 若满足对任意 $a, b \in G$ 都有 $ab = ba$. 此时通常将二元运算记作 $+$, 单位元记作 0.

命题 1.1.10. 对于 $n \geq 3$, S_n 不是 *Abel* 群.

例子. 考虑 $D_n = \{$二维平面上将正 n 边形映到自身的旋转和反射, 包括恒等映射$\}$, 二元运算是映射的复合, D_n 构成群, 称为二面体群 *(Dihedral group)*.

练习. 验证 D_n 是群.

例子. 对于 $\mathbb{R}$ 线性空间 V, 定义

$$\mathrm{GL}(V) = \{f \colon V \to V \mid f \text{ 是可逆线性变换}\},$$

二元运算是复合, $\mathrm{GL}(V)$ 构成群, 称为一般线性群 *(General linear group)*. 特别地, $\mathrm{GL}(n;\mathbb{R})$ 是所有 $n \times n$ 可逆矩阵的群, 运算时矩阵乘法. 对于域 $F = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p$, $\mathrm{GL}(n;F)$ 只在 $n = 1$ 时是 *Abel* 群.

定义 1.1.11. 对于群 $(G_1, \cdot)$ 和 $(G_2, \cdot)$, 定义

$$G_1 \times G_2 = \{(a, b) \mid a \in G_1, \ b \in G_2\},$$

二元运算是逐分量乘法, 即

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2).$$

$(G_1 \times G_2, \cdot)$ 是群, 称为 G_1 与 G_2 的积群 (Product group).

1.2 九月十四日

定义 1.2.1. 对群 G 的子集 H, 若 H 在 G 的乘法下构成群, 称 H 为 G 的子群 (subgroup).

例子. 对 $G = S_n$, 我们令

$$H = \{\sigma \in S_n \mid \sigma(n) = n\},$$

有 H 是 G 的子群. 我们只需验证 H 在 G 的运算下封闭, 并且对取逆封闭.

- 对 $\sigma, \tau \in H$, 有 $\sigma(\tau(n)) = \sigma(n) = n$, 即 $\sigma\tau \in H$;
- 若 $\sigma(n) = n$, 则有 $\sigma^{-1}(n) = \sigma^{-1}(\sigma(n)) = n$, 即 $\sigma^{-1} \in S_n$.

事实上, 我们还能证明 $H \simeq S_{n-1}$.

定理 1.2.2 (Lagrange)**.** G 是有限群, 对任意子群 $H \subset G$ 都有 $|H| \big| |G|$.

为证明此定理, 我们引入陪集 (coset) 的概念. 这里考虑左陪集 (left coset).

定义 1.2.3. 对群 G, H 是正规子群. G 中形如 $gH = \{gh \mid h \in H\}$ 的子集称为 G 的左 H-陪集.

例子. 1. $eH = H$ 是左 H-陪集.

2. 考虑 $H = \{\sigma \mid \sigma(n) = n\} \subset S_n$. 左 H 陪集的分类如下

$$X_i = \{\sigma \in S_n \mid \sigma(n) = i\},\ i = 1, 2, \cdots, n.$$

对任意给定 $g \in S_n$, 令 $i = g(n)$, 我们证明 $gH = X_i$. 首先对任意 $h \in H$, 有 $gh(n) = g(n) = i$, 即有 $gH \subset X_i$. 另一方面, 对任意 $\sigma \in X_i$, 有

$$\sigma = (g^{-1}g)\sigma = g(g^{-1}\sigma).$$

令 $h = g^{-1}\sigma$, 有 $h(n) = g^{-1}(i) = n$, 即 $h \in H$, 从而 $X_i \subset gH$. 因此有 $gH = X_i$.

定义 1.2.4. 定义集合 $G/H = \{gH \mid g \in G\}$, 每一个元素都是 G 的子集, 称为商集 (quotient set).

例子. 考虑 S_n, $H = \{\sigma \in S_n \mid \sigma(n) = n\}$, 有 $S_n/H = \{X_1, \cdots, X_n\}$.

定理 1.2.5. G 有左陪集分解

$$G = \coprod_{gH \in G/H} gH.$$

证明: 1. 无交, 若有 $gH \cap g'H \neq 0$, 即存在 $a \in gH \cap g'H$. 断言, 若 $a \in gH$, 则有 $aH = gH$. 设 $a = gh$, 对任意 $h' \in H$, 有

$$ah' = ghh' = g(hh') \in gH,$$

即 $aH \subset gH$. 另一方面, 对任意 $h'/ \in H$, 有

$$gh' = ah^{-1}h' = a(h^{-1}h') \in aH,$$

即 $gH \subset aH$. 从而 $aH = gH$. 因此 $gH = gH'$.

2. 并, 因为 $g = ge \in gH$.

□

命题 1.2.6. $H \to gH\colon h \mapsto gh$ 是双射.

证明: 若 $gh = gh'$, 则有

$$h = g^{-1}gh = g^{-1}gh' = h'.$$

而满射由定义保证. □

定理 1.2.2 证明. 由于 $|G| < \infty$, 因此我们有 $|H| = |gH|$. 利用左陪集分解

$$G = \coprod_{gH \in G/H} gH,$$

我们有 $|G| = |G/H| \cdot |H|$, 即得 $|H| \big| |G|$. □

定义 1.2.7. 对集合 S, $X \subset S \times S$ 是子集. 若 $(a, b) \in X$, 记为 $a \sim b$. 若 $\sim$ 满足

(1) 传递性 (transitive): $\forall\, a, b, c \in S$, 若 $a \sim b, b \sim c$, 则有 $a \sim c$.

(2) 对称性 (symmetric): 若 $a \sim b$, 则有 $b \sim a$.

(3) 自反性 (reflextive): 对任意 a, 有 $a \sim a$.

则称 $\sim$ 为 S 上的等价关系 (equivalence relation).

把 S 分成非空子集的无交并称为 S 的一个划分 (partition). 从等价关系我们可以自然诱导一个划分. 考虑 S 上的等价关系 $\sim$, 对任意 $a \in S$, 定义

$$C_a = \{b \in S \mid a \sim b\} \subset S.$$

令 $\bar{S} = \{C_a \mid a \in S\}$ 是所有等价类构成的集合. 我们有划分

$$S = \coprod_{C_a \bar{S}} C_a,$$

且有满射 $S \to \bar{S}\colon a \mapsto C_a$. 反过来, 从一个给定划分也可以定义等价关系.

特别地, 设 $H \subset G$ 是子群, 我们可以定义等价关系, 即

$$a \sim g \text{ 当且仅当 } \exists\, h \in H, \text{ 使得 } a = gh.$$

有满射 $G \twoheadrightarrow G/H$, 称为商映射 (quotient map). 一个自然的问题是 G/H 上是否有自然的群结构? 我们先尝试定义运算

$$\begin{aligned} G/H \times G/H &\longrightarrow G/H \\ (aH, bH) &\longmapsto abH \end{aligned}$$

我们希望这是良定义的, 即对

$$a' = ah_1,\ b' = bh_2,$$

需要 $a'b'H = abH$. 注意到

$$\begin{aligned} a'b' &= ah_1bh_2 = abb^{-1}h_1bh_2 \\ &= ab(b^{-1}h_1b)h_2, \end{aligned}$$

因此只需要, 对任意 $b \in G$, $h \in H$ 有 $b^{-1}hb \in H$. 如果假设这一点, 我们容易发现 G/H 确实有群结构, 因为有单位元 eH 和逆元 $g^{-1}H$. 因此, 从中抽取出正规子群的概念.

定义 1.2.8. 若子群 $H \subset G$ 满足对任意 $h \in H$, $g \in G$ 都有 $ghg^{-1} \in H$, 则称 H 为正规子群 (normal subgroup). 此时 G/H 有群结构, 称为商群 (quotient group).

注记. 可以定价定义为, 对任意 $g \in G$, 有 $gHg^{-1} = \{ghg^{-1} \mid h \in H\} = H$.

命题 1.2.9. *Abel 群的子群都是正规子群.*

证明: 对任意 $h \in H$, $g \in G$, 有 $ghg^{-1} = gg^{-1}h = h \in H$. □

例子. 考虑加法群 $(\mathbb{Z}, +)$, $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\} \subset \mathbb{Z}$ 是正规子群. 有商群 $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \cdots, \overline{n-1}\}$, 其中 $\bar{i} = \{i + na \mid a \in \mathbb{Z}\}$.

例子. 也容易给出非正规子群的例子. 考虑 $G = S_3$, $H = \{\sigma \in S_3 \mid \sigma(3) = 3\}$. 取

$$h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ g^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

我们有 $(ghg^{-1})(3) = gh(2) = g(1) = 1$, 即 $ghg^{-1} \notin H$. 因此 H 不是正规子群.

定义 1.2.10. 群 G_1, G_2, 双射 $f\colon G_1 \to G_2$ 称为群同构 (group isomorphism), 若对任意 $a, b \in G_1$ 都有 $f(ab) = f(a)f(b)$.

注记. 此时对于子群 $H = \{\sigma \in S_n \mid \sigma(n) = n\} \subset S_n$, 我们知道有群同构 $H \simeq S_{n-1}$.

1.3 作业 1

练习. 计算下列 S_6 中的元素的乘积. 其中 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 6 & 5 & 2 \end{pmatrix}$ 和 $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

- ◇ $\sigma \cdot \tau$.
- ◇ $\sigma \cdot \tau \cdot \sigma^{-1}$.

练习. 列出 S_4 的所有子群, 并指出哪些是正规子群.

练习. 对群 G 中的任意元素 g, h, 证明 $(gh)^{-1} = h^{-1}g^{-1}$.

练习. 分类 $(\mathbb{Z}, +)$ 的所有子群.

练习. 构造同构 $f\colon \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$.

练习. D_n 是二面体群, 计算 $|D_n|$ 并判断 D_n 是否为 Abel 群, 给出论证.

练习. 对给定素数 p, 群 $G = GL(n, \mathbb{F}_p)$. 考虑 G 的如下子集

- B 是 G 中上三角矩阵的全体.
- W 是每行每列有且仅有一个 1，其余位置是 0 的方阵全体. (请说明为什么 W 是 G 的子集)
- H 是每行每列有且仅有一个位置非零, 其余位置是 0 的方阵全体. (请说明为什么 H 是 G 的子集)
- T 是 G 中的对角阵全体.
- U 是 G 中对角线都是 1 的上三角矩阵全体.
- D 是 G 中纯量矩阵全体，即 $D = \{\lambda I_n \mid \lambda \neq 0\}$.
- $\mathrm{SL}(n, \mathbb{F}_q)$ 是 G 中行列式等于 1 的矩阵全体.

请完成以下证明或者计算:

1. 证明以上子集都是 G 的子群.
2. 判断这些子群和 G 本身是不是 *Abel* 群.
3. 求这些子群和 G 的阶数.
4. 判断哪些子群是 G 的正规子群.
5. 对于有严格包含关系的子群，判断小的群是否是大的群的正规子群.

练习. 判断 $\mathrm{GL}(2, \mathbb{F}_2)$ 是否与 S_3 同构, 给出论证.

练习. 对群 G, H 是其子群, 完成如下问题:

- 给出右 H-陪集的定义. 证明右 H-陪集数量等于左 H-陪集数量 (假设有限).
- 证明 H 是正规子群当且仅当对任意 $g \in G$ 都有 $gH = Hg$.
- 左 H-陪集的数量称为 H 在 G 中的指数 (*index*), 记作 $[G : H]$. 证明若 $[G : H] = 2$, 则 H 为正规子群.

我们下面需要用到所谓半群的概念. 集合 S 和运算 $\cdot : S \times S \to S$ 构成的对 $(S, \cdot)$ 称为半群 (semi group), 若 $\cdot : S \times S \to S$ 满足结合律.

练习. G 是所有秩小于等于 r 的 $n \times n$ 矩阵构成的集合. 证明 G 关于矩阵乘法构成半群.

练习. 对半群 G, 假设:

1. 存在左单位. 即存在 $e \in G$ 对任意 $a \in G$, 都有 $ea = a$;
2. 存在左逆. 即对任意 $a \in G$, 存在 $a^{-1} \in G$ 使得 $a^{-1}a = e$.

练习. 令 $G = \{(a, b) \mid a \neq 0\}$, 定义运算

$$\cdot : G \times G \longrightarrow G$$
$$(a, b) \cdot (c, d) \longmapsto (ac, ad + b).$$

证明 $(G, \cdot)$ 是群.

练习. 设 G 是偶数阶群, 证明 $x^2 = e$ 的解数也是偶数.

练习. 对群 G, $a, b \in G$. 若有 $a^5 = e$, $a^3b = ba^3$, 求证 $ab = ba$.

练习. 证明 $(\mathbb{R},+)$ 与 $(\mathbb{R}_{>0},\times)$ 同构.

练习. 对有限群群 G, $H\subsetneq G$ 是真子群. 证明

$$G\neq\bigcup_{g\in G}gHg^{-1}.$$

注记. 对于无限群, G 可能等于某个子群的全体共轭的并.

第二章　第二周

2.1　九月二十日

定义 2.1.1. 群 G_1, G_2, 映射 $f\colon G_1 \to G_2$ 称为群同态 (group homomorphism), 若对任意 $a, b \in G_1$, 有 $f(ab) = f(a)f(b)$.

例子. *H 是 G 正规子群, 商映射 $\pi\colon G \to G/H$ 是群同态. 因为*

$$\pi(ab) = abH = (aH)(bH) = \pi(a)\pi(b).$$

实际上, 商集 G/H 上存在唯一一个群结构使得 π 是群同态, 反过来, 我们也可以用此来定义 G/H 的群结构.

命题 2.1.2. *$f\colon G_1 \to G_2$ 是群同态, 则有*

(1) $f(e_{G_1}) = e_{G_2}$;

(2) $f(g^{-1}) = f(g)^{-1}$.

证明: (1) 对任意 $g \in G_1$, 有

$$f(g) = g(e_{G_1}g) = f(e_{G_1})f(g).$$

两边同时乘以 $f(g)^{-1}$, 即得结论

(2) 对任意 $g \in G_1$, 有

$$f(g)f(g^{-1}) = f(e_{G_1}) = e_{G_2}$$
$$f(g^{-1})f(g) = f(e_{G_1}) = e_{G_2}.$$

□

例子. *对任意 $a \in G$, 有群同态*

$$\mathbb{Z} \longrightarrow G$$
$$n \longmapsto a^n.$$

对任意 $n \in \mathbb{Z}$, 商映射 $\mathbb{Z} \to n\mathbb{Z}$, $n \mapsto \bar{n}$ 也是群同态.

命题 2.1.3. *(1) 像 (image) $\mathrm{Im}(f) := \{f(g) \mid g \in G_1\}$ 是 G_2 的子群;*

(2) 核 (kernel) $\mathrm{Ker}(f) := \{g \mid f(g) = e_{G_2}\}$ 是正规子群.

证明: (1) 对于任意 $g_1, g_2 \in G_1$, 按定义和命题 1.4.2 有

$$f(g_1g_2) = f(g_1)f(g_2),\ f(g_1)^{-1} = f(g_1^{-1}) \in \operatorname{Im} f,$$

因此 $\operatorname{Im} f$ 是 G_1 的子群.

(2) 和 (1) 一样可验证 $\operatorname{Ker}(f)$ 是子群. 考虑任意 $g \in G_1$, $h \in \operatorname{Ker}(f)$, 我们有

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e_{G_2},$$

从而 $ghg^{-1} \in \operatorname{Ker}(f)$, 即 $\operatorname{Ker}(f)$ 是正规子群.

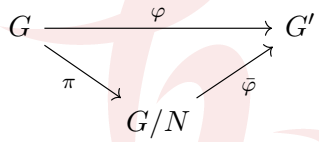
□

回忆集合论里类似的 "同构定理", 对任意满射 $f\colon X \to Y$. 我们定义等价关系 $\sim$ 如下:

$$x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2).$$

等价类集合记作 $\bar{X}$, 从而我们可以将 f "典范" 的分解为 $f = \bar{f} \circ \pi\colon X \to \bar{X} \to Y$.

定理 2.1.4 (第一同构定理 (First isomorphism theorem)). *对于满同态 $\varphi\colon G \to G'$, 令 $N = \operatorname{Ker}\varphi$. 存在唯一群同构 $\bar{\varphi}\colon G/N \to G'$, 使得 $\varphi = \bar{\varphi} \circ \pi$. 也即下图表交换*



证明: 我们先验证, 对任意 $g \in G$, 均有

$$\varphi^{-1}(\{\varphi(g)\}) = gN.$$

对任意 $h \in \varphi^{-1}(\{\varphi(g)\})$, 有 $\varphi(h) = \varphi(g)$. 从而 $g^{-1}h \in N$, 即有 $h = g(g^{-1}h) \in gN$. 另一方面, 对任意 $h = ga$, $a \in N$, 我们有

$$\varphi(h) = \varphi(g)\varphi(a) = \varphi(g)e_{G'} = \varphi(g),$$

即有 $gN \subset \varphi^{-1}(\{\varphi(g)\})$.

因此, 这诱导了良定义的双射

$$\begin{aligned} \bar{\varphi}\colon G/N &\longrightarrow G' \\ gN &\longmapsto \varphi(g). \end{aligned}$$

我们再说明这是群同态, 因为

$$\begin{aligned} \bar{\varphi}(g_1N \cdot g_2N) &= \varphi(g_1g_2) \\ &= \varphi(g_1)\varphi(g_2) \\ &= \bar{\varphi}(g_1N) \cdot \bar{\varphi}(g_2N). \end{aligned}$$

至此完成了证明. □

例子. 对任意 $a \in G$, 定义映射 f_n

$$\begin{aligned} f_n \colon \mathbb{Z} &\longrightarrow G \\ n &\longmapsto a^n. \end{aligned}$$

有 $\mathrm{Im}(f_n) \subset G$ 是子群.

定义 2.1.5. 子群 $\{a^n \mid n \in \mathbb{Z}\}$ 称为 G 中由 a 生成的子群, 记作 $\langle a \rangle$.

通过 Bézout 定理, 可知 $\mathbb{Z}$ 的子群均形如 $n\mathbb{Z}$, 对某个 $n \geq 0$. 对任意 $a \in G$, 都存在 $n_a \in \mathbb{Z}_{\geq 0}$ 使得

$$\langle a \rangle \simeq \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}.$$

定义 2.1.6. 当 $n_a \geq 0$ 时, n_a 称为元素 a 的阶 (order). 当 $n_a = 0$, 定义 a 的阶为 ∞.

注记. 事实上, 元素 a 的阶是使得 $a^n = e$ 的最小正整数 n.

定义 2.1.7. 若存在 $a \in G$, 使得 $G = \langle a \rangle$ 成立, 则称 G 为循环群 (cyclic group). 对于循环群, 我们有 $G \simeq \mathbb{Z}$ 或 $G \simeq \mathbb{Z}/n\mathbb{Z}$.

定理 2.1.8 (对应定理)**.** 商同态 $f \colon G \to G/N$ 诱导了双射

$$\begin{aligned} \{G/N \text{ 的子群}\} &\overset{F}{\longleftrightarrow} \{G \text{ 中包含 } N \text{ 的子群}\} \\ \bar{H} &\longmapsto f^{-1}(H). \end{aligned}$$

并且 F 将 G/N 的正规子群变为 G 中包含 N 的正规子群. 逆映射由

$$\begin{aligned} \{G \text{ 中包含 } N \text{ 的子群}\} &\overset{F^{-1}}{\longleftrightarrow} \{G/N \text{ 的子群}\} \\ H &\longmapsto H/N. \end{aligned}$$

更一般地, 我们有 F 限制在 G/N 的正规子群上也是一一对应, 这是因为若 $H \subset G$ 正规, 则有

$$G/H \simeq (G/N)/(H/N).$$

证明: 考虑商映射 $\varphi \colon G \to G/N \to (G/N)/(H/N)$, 直接验证有 $\mathrm{Ker}\,\varphi = H$, 从而有

$$G/H \simeq (G/N)/(H/N).$$

□

例子. 我们可以用对应定理分类循环群 $\mathbb{Z}/n\mathbb{Z}$ 的子群 $(n \geq 1)$. 注意到 $n\mathbb{Z} \subset m\mathbb{Z}$ 当且仅当 $m|n$. 即

$$\{\mathbb{Z} \text{ 中包含 } n\mathbb{Z} \text{ 的子群}\} = \{m\mathbb{Z} \mid m|n,\ m \geq 1\}.$$

从而 $\mathbb{Z}/n\mathbb{Z}$ 中的子群形如 $m\mathbb{Z}/n\mathbb{Z} \simeq d\mathbb{Z}$, 其中 $dm = n$.

命题 2.1.9. 对 n 阶循环群 G, 和整数 $d|n$, 存在唯一 d 阶子群.

注记. 反过来, 这一性质也刻画了循环群, 参考第二次作业.

例子. *(1) 考虑行列式映射* $\det\colon \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}^\times$, $A \mapsto \det A$, *这是群同态, 由第一同构定理, 有*

$$\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R}) \simeq \mathbb{R}^\times.$$

(2) 考虑指数映射

$$\begin{aligned} \exp\colon \mathbb{C} &\to \mathbb{C}^\times \\ z &\mapsto e^z. \end{aligned}$$

这是群同态.

我们回忆积群 $G_1 \times G_2$, 我们有正规子群 $G_1 \simeq G_1 \times G_1 \times \{e_{G_2}\}$, 以及 $G_2 \simeq \{e_{G_1}\} \times G_2$. 这是从两个群构造一个新的群. 反过来, 我们可以对给定群 G, 及其子群 $H, K \subset G$, 判断能否从 H, K 的结构还原 G 的结构

命题 2.1.10. *H, K 是 G 的子群, 则*

$$\begin{aligned} f\colon H \times K &\longrightarrow G \\ (h,k) &\longmapsto hk \end{aligned}$$

是群同构当且仅当以下三条同时成立.

(1) $H \cap K = \{e\}$;

(2) $HK = \{hk \mid h \in H, k \in K\} = G$

(3) H, K *为正规子群.*

2.2 九月二十日

我们接着上一次课, 给出定理 2.1.10 的证明.

证明: “当” 部分: 先证明 $hk = kh$, 对任意 $h \in H, k \in K$ 成立. 我们考虑元素 $hkh^{-1}k^{-1}$, 由于 K 是正规子群, 有 $hkh^{-1} \in K$, 从而 $hkh^{-1}k^{-1} \in K$. 同理有 $hkh^{-1}k^{-1} \in H$, 由条件 (1) 知

$$hkh^{-1}k^{-1} \in H \cap K = \{e\}.$$

从而 $hk = kh$ 对任意 $h \in H, k \in K$ 成立. 这保证了 f 是群同态.

条件 (2) 保证了 f 是满射, 下证 f 是单射. 考虑

$$\mathrm{Ker}\, f = \{(h,k) \mid hk = e\} = \{(h,k) \mid h = k^{-1}\} = \{(e,e)\}.$$

最后一个单号用到了条件 (3).

“仅当” 部分: 我们只需注意到 $H \simeq (H, e_K) \subset H \times K$ 以及 $K \simeq (e_H, K) \subset H \times K$. □

例子. *将循环群 $\mathbb{Z}/n\mathbb{Z}$ 记作 C_n, 我们证明 $C_6 \simeq C_2 \times C_3$. 除去直接验证, 我们来看一个更加 “内蕴” 的方法. 取 C_6 的 2 阶子群 $H \simeq C_2$, 以及 3 阶子群 $K \simeq C_3$. 我们有 $H \cap K = \{0\}$, 且它们均为正规子群, 这保证了*

$$H \times K \to C_6$$

是单射. 而 $|H \times K| = 6 = |C_6|$ 保证了这是满射.

群作用

研究群的另一种方法是研究其在一些对象上的作用, 这也是群表示的观点.

定义 2.2.1 (群作用 (group action))**.** 对于集合 X, G 在 X 上 (左) 作用是指二元运算

$$\begin{aligned}\varphi\colon G\times X &\longrightarrow X\\ (g,x) &\longmapsto g\cdot x\end{aligned}$$

满足下两条条件

(1) 对任意 $g,h\in G$ 及 $x\in X$, 有 $(gh)\cdot x=g\cdot(h\cdot x)$;

(2) 对于单位元 $e\in G$, 有 $e\cdot x=x$.

例子. 最简单的例子是考虑 $X=G$, 此时群作用就是群 G 上的乘法. 上面的作用也称为左作用, 右称作用定义为

$$\begin{aligned}G\times X &\longrightarrow X\\ (g,x) &\longmapsto g*x=xg^{-1}.\end{aligned}$$

我们可以验证结合律, 即对任意 $g,h\in G$ 及 $x\in X$ 有

$$(gh)*x=x(gh)^{-1}=xh^{-1}g^{-1}=g*(xh^{-1})=g*(h*x).$$

可以说明, 如果我们简单定义 $g*x=xg$, 此时作用没有 "结合律".

另一件重要的事是左乘与右乘作用交换. 对任意 $g,h\in G$, 我们有

$$h*_{右}(g*_{左}x)=(gx)h^{-1}=g(xh^{-1})=g*_{左}(h*_{右}x).$$

这诱导了 $G\times G$ 在 X 上的作用, 即

$$\begin{aligned}(G\times G)\times X &\longrightarrow X\\ ((g_1,g_2),x) &\longmapsto g_1x(g_2)^{-1}.\end{aligned}$$

例子. 现有 $G\curvearrowright X$, 希望从中得到一些新的群作用.

(1) 限制: $H\subset G$ 是子群, 则 $h=g_1\in H\subset G$, 我们可定义

$$h\cdot x:=g_1\cdot x$$

作为 G 在 X 上的作用.

(2) 定义幂集 $2^X=\{X\text{ 所有子集}\}$, 对任意 $A\subset X$, 即 $A\in 2^X$, 可定义

$$g\cdot A:=\{ga\mid a\in A\}.$$

定义 2.2.2. 取 $X=G$, 共轭作用 (conjugation) 是群作用

$$\begin{aligned}G\times X &\longrightarrow X\\ (g,x) &\longmapsto gxg^{-1}.\end{aligned}$$

注记. 共轭作用的另一看法是 $G\times G$ 作用在 G 上, 然后限制在子群 $G\simeq\{(g,g)\mid g\in G\}$ 上得到的群作用.

例子. 考虑置换群 $G=S_n$, 集合 $X=[n]:=\{1,2,\cdots,n\}$, 有群作用

$$\begin{aligned} S_n\times[n]&\longrightarrow[n]\\ (\sigma,i)&\longmapsto\sigma(i)\end{aligned}$$

对于更一般的集合 X, 我们也可以考虑类似的置换作用, 即 X 上的对称群.

定义 2.2.3. 令 $S_X=\{f\colon X\to X \text{ 双射}\}$, 在映射的复合下构成群. 有群作用

$$\begin{aligned} S_X\times X&\longrightarrow X\\ (f,x)&\longmapsto f(x).\end{aligned}$$

给定一个群作用 $G\curvearrowright X$, 可以定义映射

$$\begin{aligned} \varphi\colon G&\longmapsto S_X\\ g&\longmapsto(m_g\colon x\to g\cdot x)\end{aligned}$$

从 m_g 是双射 (因为有逆映射 $m_{g^{-1}}$) 知 φ 是良定义映射. 由群作用条件 (1) (即结合律) 知 $\varphi(gh)=\varphi(g)\varphi(h)$, 由群作用条件 (2) (即单位律) 知 $m_e=\mathrm{Id}$. 反过来, 如果有群同态 $\varphi\colon G\to S_X$, 从而可以定义群作用

$$g\cdot x=(\varphi(g))x$$

定义 2.2.4. 对于域 F (F 为 $\mathbb{R},\mathbb{C},\mathbb{Q},\mathbb{F}_p$), 设 X 为 F 上 n 维线性空间. G 作用于 X, 且满足对任意 $\lambda\in F$, $v,w\in X$ 有

(1) $g(v+w)=g(v)+g(w)$;

(2) $g(\lambda v)=\lambda g(v)$.

则 $\varphi\colon G\to S_X$, 有 $\mathrm{Im}\,\varphi\subset\mathrm{GL}(X)$, 这样的作用称为 G 的线性表示 (linear representation).

例子. 考虑 $S_n\curvearrowright[n]$, 取 $\mathbb{R}^n$ 上一组基 $\{e_1,\cdots,e_n\}$, 我们可以定义

$$\sigma(\sum_{i=1}^n\lambda_ie_i)=\sum_{i=1}^n\lambda_ie_{\sigma(i)}.$$

我们有群同态 $\varphi\colon S_n\to\mathrm{GL}(n,\mathbb{R})$. 定义符号映射

$$\mathrm{sgn}\colon S_n\to\mathrm{GL}(n,\mathbb{R})\overset{\det}{\to}\mathbb{R}^\times,$$

有 $\mathrm{Im}(S_n)=\{\pm1\}$, 定义交错群 *(alternative group)* $A_n:=\mathrm{Ker}(\mathrm{sgn})$. 可以说明 A_n 是由所有偶置换构成的子群 *(考虑置换矩阵的行列式)*.

现考虑 n 阶有限群 G, 有群同态 $\varphi\colon G\to S_G$. 选取一个双射 $G\leftrightarrow[n]$, 有同态

$$\varphi\colon G\to S_n.$$

命题 2.2.5. $\operatorname{Ker}\varphi = \{e\}$.

证明： 注意到

$$\begin{aligned} g \in \operatorname{Ker}\varphi &\Longleftrightarrow \{gx = x \mid \forall\ x \in G\} \\ &\Longleftrightarrow \{g = e\}\ (\text{两边乘 } x^{-1}). \end{aligned}$$

□

下面引入群同构的概念.

定义 2.2.6. 群 G 作用于集合 X, Y, 映射 $f\colon X \to Y$ 称为**群作用的同态**若

(1) 对任意 $g \in G$, 有 $f(g \cdot x) = g \cdot f(x)$.

特别地, 在 f 为双射时, 称 f 为**群作用的同构**.

注记. 群作用的同态可用下交换图表描述

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ {\scriptstyle (\mathrm{Id},f)}\downarrow & & \downarrow{\scriptstyle f} \\ G \times Y & \longrightarrow & Y \end{array}$$

在有群作用的集合 X 上, 我们可以定义自然的等价关系

$$x_1 \sim x_2 \Longleftrightarrow \exists g \in G,\ gx_1 = x_2.$$

此等价关系的等价类被称为 G 作用的轨道 (orbit). 对任意 $x \in X$, 令 $O_x := \{gx \mid g \in G\}$. 记

$$G\backslash X = \{O_x \mid x \in X\}.$$

进而有分划

$$X = \coprod_{O_x \in G\backslash X} O_x.$$

当 $|X| < +\infty$ 时, 我们有 $|X| = |O_1| + \cdots + |O_n|$, 其中 $n = |G\backslash X|$.

定义 2.2.7. 群作用 $G \curvearrowright X$ 称为可迁 (transitive) 若轨道数为 1.

我们想要分类群作用. 注意到 $G \curvearrowright X_1, X_2$, 则可诱导作用 $G \curvearrowright X_1 \coprod X_2$. 因此, 分类的大致思路是

(1) 将 X 分成无交并 $X = O_1 \amalg \cdots \amalg O_n$;

(2) 分类 G 在 O_i 上的可迁作用.

例子. *$H \subset G$ 是子群, 定义 $H \curvearrowright G$ 为 $h * g := gh^{-1}$. 对任意 $g \in G$, 有*

$$O_g = \{h * g \mid h \in H\} = \{gh^{-1} \mid h \in H\} = gH.$$

即子群右作用 (这也解释为什么商要写在右边) 的轨道是左 H 陪集

$$G/H = \{g_1H, \cdots, g_nH\}.$$

若 $H \subset G$ 是正规子群, 则 $G \curvearrowright G/H$ 的作用为

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ g * (g'H) &\longmapsto (gg')H, \end{aligned}$$

这是一个可迁作用.

一般地, 若 $G_1, G_2 \curvearrowright X$ 作用, 且交换, 则 $G_2\backslash X$ 上有自然的 G_1 作用, 且

$$\pi \colon X \to G_2\backslash X$$

是 G_1 作用.

定义 2.2.8. 对 $G \curvearrowright X$, 任意 $x \in X$, 定义

$$G_x = \{g \in G \mid gx = x\},$$

称为 x 的稳定化子 (stabilizer), 其是 G 的子群。

例子. $G \curvearrowright G/H$ 上 eH 的稳定化子为 H.

定理 2.2.9. 作用 $G \curvearrowright X$ 可迁, 则有 G 作用同构 *(给定 x)*

$$\begin{aligned} f \colon G/G_x &\longrightarrow X \\ gG_x &\longmapsto g \cdot x. \end{aligned}$$

命题 2.2.10. 对任意 $g \in G$, $x \in X$ 有 $G_{gx} = gG_xg^{-1}$.

第三章　第三周

3.1　九月二十七日

回忆对于群作用 $G \curvearrowright X$, 我们有

(1) $X = \coprod_{O \in G\backslash X} O$, 其中 $G\backslash X = \{$轨道的集合$\}$;

(2) 可迁作用, 有 $G/G_x \xrightarrow{\simeq} O$ (g 作用同构), $\forall\, x \in O$, 其中 $G_x = \{g \mid gx = g\}$ 是 x 的稳定化子.

(3) $G_{gx} = gG_xg^{-1}$.

通过 (1) (2), 即 $X = \coprod_{i=1}^{n} O_i$, 我们能得到计数公式

$$|X| = |O_1| + \cdots + |O_n|$$
$$|O| = [G : G_x] = \frac{|G|}{|G_x|}.$$

例子. *考虑正四面体 $\Omega = ABCD$, 设*

$$G = \{\mathbb{R}^3 \text{ 旋转反射, 将 } \Omega \text{ 映到 } \Omega\} = \Omega \text{ 的对称群.}$$

注意到 $G \curvearrowright \{A, B, C, D\}$ 作用可迁. 且对任意一个顶点, 稳定化子都是二面体群 D_3, 从而有 $|G| = 4 \times 6 = 24$.

定义 3.1.1. 对于素数 p, 若群 G 满足 $|G| = p^s$, $s \geq 1$, 则称 G 为 p 群 (p group).

命题 3.1.2. *对于 p 群 G, 我们有*

(1) 若 $|G| = p$, 则对任意 $a \in G\backslash\{e\}$, 有 $G = \langle a \rangle$.

(2) 若 $|G| = p^2$, G 是交换群.

证明: 我们考虑 $G \curvearrowright X = G$ 是共轭作用, 有如下事实

(1) $ag = ga \Leftrightarrow g \in G_a$;

(2) a 与 G 中元素均交换 $\Leftrightarrow G_a = a \Leftrightarrow O_a = a$.

(3) 定义 $C := \{a \in G \mid ag = ga, \forall\, g \in G\}$, 称为群 G 的中心 (center).

注意到 $p \mid \sum_{i=1}^{n} |O_i|$, 且对任意 i, 有 $|O_i| = 1, p, p^2$. 不妨 $O_1 = \{e\}$, 则存在 $i \geq 2$ 使得 $|O_i| = 1$, 即 p 群 G 的中心非平凡. 从而 $|G/C| = 1$ 或 p, 使用如下引理即得结论. □

引理 3.1.3. *若 C 是 G 的中心, 且 G/C 是循环群, 则有 $G = C$.*

证明: 假设 $G=\bigcup_{i=-\infty}^{\infty}a^iC$, 对任意 $b,c\in C$, 我们有

$$(a^ib)(a^jc)=a^{i+j}bc=a^{i+j}cb=(a^jc)(a^ib)$$

从而知 $G=C$. □

练习. 分类 p^3 阶群.

Sylow 定理

定义 3.1.4. 设 $|G|=p^sm$, 其中 $s\geq 1$ 且 $p\nmid m$. 若 H 是 G 的子群, 且 $|H|=p^s$, 称 H 是 Sylow p 子群 (Sylow p subgroup).

定理 3.1.5 (Sylow 定理)**.** 对于群 G

(1) 若 $p||G|$, 则 G 中存在 *Sylow* p 子群, 且它们两两共轭;

(2) 若 H 是 G 的 p 子群, 则存在 *Sylow* p 子群 H' 满足 $H\subset H'$;

(3) 记 $a_p=\#\{Sylow\ p\ 子群\}$, 有 $a_p|m$ 且 $a_p\equiv 1(\mathrm{mod}\,p)$.

例子. 考虑 $\mathbb{F}_p$ 上的一般线性群 $\mathrm{GL}(n,\mathbb{F}_p)$, 我们有

$$\begin{aligned}|G|&=(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})\\&=p^{\frac{n(n-1)}{2}}(p^n-1)\cdots(p-1).\end{aligned}$$

即 $|G|=p^{\frac{n(n-1)}{2}}m$, 其中 $p\nmid m$. 考虑 $U=\{\begin{pmatrix}1&&*\\&\ddots&\\0&&1\end{pmatrix}\}$ 是由对角线为 1 的上三角矩阵构成的子群, 满足 $|U|=p^{\frac{n(n-1)}{2}}$, 则 U 是 G 的 *Sylow* p 子群.

我们先证明如下引理

引理 3.1.6. $H\subset G$ 是子群, G 中有 *Sylow* p 子群 U. 则 $\exists g\in G$ 使得 $H\cap(gUg^{-1})$ 是 H 的 *Sylow* p 子群.

证明: 考虑群作用 $G\curvearrowright G/U=:X$, 记陪集中元素 U 为 x. 有此作用可迁并且 $G_x=U$, $G_{gx}=gUg^{-1}$. 考虑轨道分解

$$G=\coprod O_i\Leftrightarrow|X|=|O_1|+\cdots+|O_n|.$$

由于 U 是 Sylow p 子群, 则有 $p\nmid|X|$, 从而存在 i 使得 $p\notin|O_i|$. 任取 $gU\in O_i$, 有

(1) $H_x=G_x\cap H=U\cap H$;

(2) $H_{gx}=G_{gx}\cap H=(gUg^{-1})\cap H$.

我们有 $p\notin|O_i|=\frac{|H|}{|H_{gU}|}$. 而 $|H_{gU}||U|=p^s$, 从而 H_{gU} 是 H 的 Sylow p 子群. □

注记. 可迁作用限制在子群上不一定可迁. 例如 $\mathbb{R}^2\curvearrowright\mathbb{R}^2$, 定义为 $a*b:=a+b$. 限制在子群 $H=\{\begin{pmatrix}r\\0\end{pmatrix}\}$ 上, 不是可迁作用.

回忆上次课构造的 S_n 到 $\mathrm{GL}(n,F)$ 的群同态. 对于一般的群 G, 我们也可以做类似的考虑 (正则表示 (regular representation)). 取线性空间

$$V = F \cdot G = \{\sum_{g\in G} a_g g \mid a_g \in G\}.$$

作用 $G \curvearrowright V$ 定义为

$$h(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g (hg).$$

定理 3.1.5 证明.

(1) 对于存在性, 考虑取 $F = \mathbb{F}_p$. 然后用上面的结果知 G 同构于 $\mathrm{GL}(n,\mathbb{F}_p)$ 的子群, 用引理及 $\mathrm{GL}(n,\mathbb{F}_p)$ 存在 Sylow p 子群, 知 G 有 Sylow p 子群. 对于共轭性, 在引理中取 H 是 G 的任意 Sylow p 子群, U 是另一个 Sylow p 子群，由引理知 $H = gUg^{-1} \cap H$. 考虑元素个数即知 $H = gUg^{-1}$.

(2) 在引理中取 H 为 p 子群, 再结合 Sylow p 子群的共轭还是 Sylow p 子群即得结论.

(3) 设 $X = \{G$ 中所有 Sylow p 子群$\}$. 考虑 $G \curvearrowright X$ 是共轭作用, 则由 (1) 这是可迁作用. 考虑 $x = U$, 则有 $G_x \supset U$, 知

$$a_p = |X| = \frac{|G|}{|G_x|}.$$

结合

$$m = \frac{|G|}{|U|} = \frac{|G|}{|G_x|} \cdot \frac{|G_x|}{|U|}$$

知 $\frac{|G_x|}{|U|}$ 是整数. 设 $H \in X = \{H = H_1, \cdots, H_{a_p}\}$, 我们将此共轭作用限制在 H 上. 利用下引理, 有如下事实, 从而得到 $a_p \equiv 1 (\mod p)$

- $|X| = \sum_{i=1}^{n} |O_i|$, 且 $|O_i| \big| |H| = p^s$;
- $|O_i|$ 有且仅有 1 个为 1, 即 H 所在的轨道 $O = \{H\}$.

□

引理 3.1.7. *若 H 是 H' 的稳定化子 (即 H 的共轭作用不改变 H'), 且 H, H' 均为 G 的 Sylow p 子群, 则有 $H = H'$.*

证明: 定义 H' 的正规化子 (normalizer) 为

$$N_{H'} := G_{H'} = \{g \in G \mid gH'g^{-1} = H'\} \text{ (也即共轭作用的稳定化子).}$$

则有 H' 是 $N_{H'}$ 的正规子群. 则有 $H, H' \subset N_{H'}$ 均为 Sylow p 子群, 运用 Sylow 定理 (定理 3.1.5), 知 H 与 H' 在 $N_{H'}$ 中共轭, 则有 $H = H'$. □

例子. *考虑 15 阶群 G, 有 Sylow 3 子群 $H \simeq C_3$, 且 $a_3 = 1$. 有 Sylow 5 子群 $K \simeq C_5$, 且 $a_5 = 1$. 这保证了 H, K 均为正规子群. 更多地, 有 $H \cap K = \{e\}$, 我们有 $G \simeq C_3 \times C_5$.*

考虑 21 阶群 G, 结果稍有不同. H 是 Sylow 3 子群, 但 $a_3 = 1$ 或 7; K 是 Sylow 7 子群, 是正规子群. 如果 $a_3 = 1$, 则有同构 $G \simeq C_3 \times C_7$. 若 $a_3 = 7$, 那 G 是什么? 答案是所谓的半直积 (semi product), 若 G 存在, 可验证

(1) G=HK;

(2) $H \times K \to$, $(h,k) \mapsto hk$ *是双射 (不是群同态);*

(3) 构造群同态, 注意 $(h_1k_1)(h_2k_2) = h_1h_2(h_2^{-1}k_1h_2)k_2$, *这与* H *在* K *上作用有关.*

3.2 九月二十七日

我们接着考虑上一次的例子, 希望找到 G 中的乘法使得双射

$$\begin{aligned} \varphi\colon H \times K &\longrightarrow G \\ (h,k) &\longmapsto hk \end{aligned}$$

是群同构. 考虑 $g_1 = h_1k_1$, $g_2 = h_2k_2$, 此时有

$$g_1g_2 = h_1k_1h_2k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2.$$

由于 K 是 G 的正规子群, 我们知道 H 在 K 上有共轭作用, 即 $h * k = hkh^{-1}$. 这诱导了群同态 $H \to S_K$, 由此有群同态 $H \xrightarrow{\sigma} \mathrm{Aut}(K) = \{f\colon K \to K \text{ 同构}\}$. 此时可以将 G 的群结构定义为

$$(h_1k_1)\cdot(h_2k_2) := (h_1h_2)\cdot(\sigma(h_2^{-1})(k_1)k_2).$$

更一般地, 除了共轭作用 σ 可以这样定义乘法, 对于任意从 H 到 K 自同构群的同态 $\sigma\colon H \to \mathrm{Aut}(K)$, 都能按照上式定义 $H \times K$ 的群结构. 这样得到的群记作 $H \rtimes_\sigma K$, 称为 H, K 关于 σ 的半直积.

自由群和关系

定义 3.2.1. 集合 X, 由 X 生成的自由群 (free group) $F(X)$ 是集合

$$F(X) = \{e, x_1^{a_1}\cdots x_n^{a_n} \mid x_i \in X, a_i \in \mathbb{Z}\backslash\{0\}, \text{ 且相邻元素不同}\}.$$

其中 $x_1^{a_1}\cdots x_n^{a_n}$ 称为以 X 为字母的单词 (word). 配备如下乘法

(1) $e \cdot x_1^{a_1}\cdots x_n^{a_n} = x_1^{a_1}\cdots x_n^{a_n}\cdot x = x_1^{a_1}\cdots x_n^{a_n}$;

(2) 对单词 $x_1^{a_1}\cdots x_n^{a_n}$ 和 $y_1^{b_1}\cdots y_m^{b_m}$, 若 $x_n \neq y_1$, 则

$$(x_1^{a_1}\cdots x_n^{a_n})\cdot(y_1^{b_1}\cdots y_m^{b_m}) := x_1^{a_1}\cdots x_n^{a_n}\cdot y_1^{b_1}\cdots y_m^{b_m}.$$

若 $x_n = y_1$, 则 $x_n^{a_n}y_1^{b_1} = x_n^{a_n+b_1}$. 对 $n+m$ 使用归纳法定义.

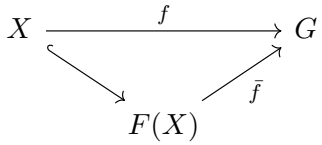
例子. *若* $|X| = 1$, *则有* $F(X) \simeq \mathbb{Z}$. *若* $|X| \neq |Y|$, *则有* $F(X) \not\simeq F(Y)$.

命题 3.2.2. *自由群的子群是自由群.*

定义 3.2.3. 群 G, 集合 $X \subset G$, 由 X 生成的子群 H 是所有包含 X 的子群的交. 具体来说, 是由元素和逆的乘积构成的集合.

定义 3.2.4. 群 G, 集合 $X \subset G$, 由 X 生成的正规子群 H 是所有包含 X 的子群的交. 具体来说, 是由元素和逆的共轭元的乘积的集合.

命题 3.2.5. 集合 X, 对任意映射 $f\colon X \to G$, 存在唯一群同态 $\bar{f}\colon F(X) \to G$, 使得如下图表交换



特别地, 若 X 为 G 的生成元集, 则有满同态 $F(X) \twoheadrightarrow G$. 我们有 $\ker \bar{f}$ 为 $F(X)$ 的正规子群, 若 R 为 $\ker \bar{f}$ 的生成元, 将 G 记作 $\langle X \mid R\rangle$, R 称为生成元 X 的关系 *(relation)*.

例子. 对于二面体群 $D_n = \{n$ 个旋转, n 个反射$\}$. 令 x 表示逆时针旋转 $\frac{2\pi}{n}$, y 表示沿任意一条对角线做反射. 则 $\{e, x, \cdots, x^{n-1}\}$ 是 n 个旋转, $\{y, xy, x^2y, \cdots, x^{n-1}y\}$ 是 n 个互不相同的. 考虑满射

$$f\colon F(\{x,y\}) \longmapsto G,$$

我们有 $\operatorname{Ker} f \supset \{x^n, y^2, (yx)^2\}$ *(*因为可以直接验证 $yxy^{-1} = x^{-1}$, 即 $(yx)^2 = e$*)*. $K = \langle x\rangle$ 是 n 阶正规子群, $H = \langle y\rangle$ 是 2 阶子群, 有 $HK = D_n$, $H \cap K = \{e\}$. 断言有

$$D_n = \langle x, y \mid x^n, y^2, (yx)^2\rangle,$$

也可以写作 $D_n = \langle x, y \mid x^n = e, y^2 = e, yxy^{-1} = x^{n-1}\rangle$. 分为两步

- ◇ 由于 $\{x^n, y^2, (yx)^2\} \subset \operatorname{Ker} f$, 因此有满射

$$f\colon D_n = \langle x, y \mid x^n, y^2, (yx)^2\rangle \twoheadrightarrow D_n;$$

- ◇ 对任意单词 $g = x^{a_1}y^{b_1}\cdots$, 使得 $f(g) = e$, 可以通过关系约化为 $g = x^{a_1}y^{b_1}$ *(*注意到 $yx = xy^{n-1}$, 因此可以一直交换*)*. 要 $f(g) = e$, 只能 $n|a_1$, $2|b_1$, 即证.

S_n 的循环分解

定义 3.2.6. 置换 $\sigma \in S_n$ 称为轮换 (cycle), 若存在 $\{i_1, \cdots, i_m\} \subset [n]$ (此时 σ 记作 $\sigma = (i_1\ \cdots\ i_n)$) 使得

- ◇ $\sigma(i_j) = i_{j+1}$, $1 \le j \le m-1$;
- ◇ $\sigma(i_m) = i_1$;
- ◇ $\sigma(i = i)$ 若 $i \notin \{i_1, \cdots, i_m\}$.

我们称轮换 $\sigma = (i_1\ \cdots\ i_m)$ 和 $\tau = (j_1\ \cdots\ j_n)$ 不相交, 若 $\{i_1, \cdots, i_m\} \cap \{j_1, \cdots, j_n\} = \phi$. 有如下 S_n 的结构定理

定理 3.2.7. 任意 $\sigma \in S_n$, 存在互补相交的轮换 $\sigma_1, \cdots, \sigma_k$ 使得 $\sigma = \sigma_1 \cdots \sigma_k$. 且 $\{\sigma_1, \cdots, \sigma_k\}$ 由 σ 唯一决定.

例子. 对轮换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, 有轮换分解 $\sigma = (2\ 6\ 5\ 4\ 3)(1\ 7)$. 从中看出, 这些分解事实上是 $\sigma \curvearrowright [n]$ 的轨道.

第四章　第四周

4.1　十月四日

回忆上一次课, 我们看到 S_n 可以分解为不交轮换的复合, 事实上, 这与共轭类分类密切相关. 这一次课, 我们证明更强的结果, 任意置换都能分解成若干 “基础对换” 的乘积.

例子. *考虑 S_3 中的元素 $(1\ 2\ 3)$ 和 $(1\ 3)$ (这是一个 “非基础” 对换), 我们有分解*

$$(1\ 2\ 3) = (1\ 3)(1\ 2)$$
$$(1\ 3) = (1\ 2)(2\ 3)(1\ 2) = (2\ 3)(1\ 2)(2\ 3).$$

定义 4.1.1. 对换 (2-轮换) $s_i = (i\ i+1)$, $1 \le i \le n-1$ 被称为基础对换.

命题 4.1.2. *任意 $\sigma \in S_n$, 均可以写为 $\sigma = s_{i_1} \cdots s_{i_k}$.*

证明有两种思路, 一是使用归纳法, 尝试多乘一些对换, 让 σ' 固定 n; 二是考虑 “逆序对”.

定义 4.1.3. 对 $\sigma \in S_n$, 集合 $\{(i,j) \in [n] \times [n] \mid i < j,\ \sigma(i) > \sigma(j)\}$ 中的元素称为逆序对. σ 的长度 $l(\sigma) =$ 逆序对的个数.

例子. *对于基础对换 S_i, 有 $l(S_i) = 1$.*

命题 4.1.4. *对任意 $\sigma \in S_n$, 有 $l(\sigma) = l(\sigma^{-1})$.*

对 $w = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$, 我们有 $l(w) = \frac{n(n-1)}{2}$.

证明: 作业. □

命题 4.1.5. *对 $\sigma \in S_n$, 都有 $l(\sigma) + l(\sigma w) = \frac{n(n-1)}{2}$.*

定理 4.1.6. *若 σ 的长度为 l, 则 $\sigma = s_{i_1} \cdots s_{i_l}$. 且若 $\sigma = s_{j_1} \cdots s_{j_m}$, 均有 $m \ge l$.*

注记. 分解出的基础对换中, 可能有相同项, 且最短的分解不唯一, 参考前面的例子.

先证明如下引理:

引理 4.1.7. *对于 σs_k 的长度有*

$$l(\sigma s_k) = \begin{cases} l(\sigma) + 1, & \sigma(k) < \sigma(k+1) \\ l(\sigma) - 1, & \sigma(k) > \sigma(k+1) \end{cases}$$

证明: 只需注意到

$$\sigma s_k = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(k+1) & \sigma(k) & \cdots & \sigma(n) \end{pmatrix}.$$

□

定理 4.1.6 证明. 考虑对 $l = l(\sigma)$ 用归纳法, $l = 0$ 是成立. 假设对 $l(\sigma) = l$ 成立, 考虑 $l(\sigma) = l + 1 \geq 1$, 知存在 i 使得 $\sigma(i+1) > \sigma(i)$. 从而有 $l(\sigma s_i) = l + 1 - 1 = l$, 用归纳假设, 可设

$$\sigma s_i = s_{i_1} \cdots s_{i_l},$$

从而有 $\sigma = s_{i_1} \cdots s_{i_l} s_i$. □

可以发现基础对换满足一些关系:

(1) 对 i, 有 $s_i^2 = e$;
(2) 对 $|j - i| \geq 2$, 有 $s_i s_j = s_j s_i$;
(3) 对 $|j - i| = 1$ 有 $s_i s_j s_i = s_j s_i s_j$, 也即 $(s_i s_j)^3 = e$.

事实上, 这也完全刻画了对称群.

定理 4.1.8. *对群 $G = \langle s_1, \cdots, s_n \mid s_i^2, (s_i s_j)^2, (s_i s_{i+1})^3 \rangle$, 有 $G \simeq S_n$.*

有两种思路:

- 记 G 中生成元的关系为 R. 按定义, 我们有满射 $f\colon F(\{s_1, \cdots, s_{n-1}\}) \twoheadrightarrow S_n$, 我们想证明 $\operatorname{Ker} f$ 由 R 中的元素生成. 即若 $s_{i_1} \cdots s_{i_k} = e$, 去证能通过关系 R 将左边调整为 e. 这个方法稍显繁琐;
- 使用下面介绍一般的判断一组生成元和关系能否给出想要的群的算法.

Coxeter–Todd 算法

$G = \langle X \mid R \rangle$, 假设 $|X|, |R| < +\infty$ (称 G 有限表现 (finite prsentation)). $H \subset G$ 是子群, 且 H 有限生成.

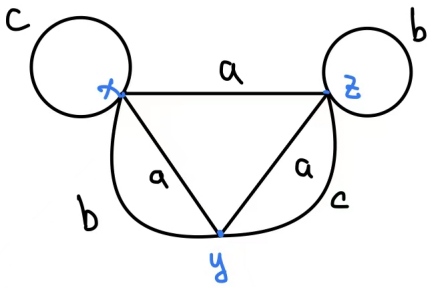
注记. 有限生成群的子群不一定有限生成. 例如考虑 $F(\{x, y\})$ 中 $x^n y x^{-n}$, $n \geq 1$ 生成的子群.

先研究 $G \curvearrowright G/H$, 我们希望从中反映出 G 的信息, 注意到

(1) $G \curvearrowright G/H$ 的作用定义为 "置换作用", 即 $g(tH) = (gt)H$;
(2) H 的生成元作用在陪集 eH 上是恒等元;
(3) G 的关系 R 作用在 G/H 上市恒等元;
(4) $G \curvearrowright G/H$ 可迁.

下面介绍 Coxeter–Todd 算法, 它通过 $G \curvearrowright G/H$ 的作用通过画点与点之间的路径表达, 来反映 $|G/H|$ 和 $G \to S_{G/H}$ 的信息. 我们从一例子来理解其中的思想.

例子. *取 $G = \langle a, b, c \mid a^3, b^2, c^2, cba \rangle$, 其子群 $H = \langle c \rangle$, 我们有 $|H| \leq 2$.*



(参考上图理解) 考虑点 $x = eH$, 由于 $c \in eH$, 知 c 在 eH 上的作用就是映到自己. 设 $y = a \cdot (eH)$, $z = a^2 \cdot (eH)$, 我们知道有 $a \cdot z = x$ *(由关系 $x^3 = e$)*. 令 $w = b \cdot y$, 由 $cba = e$ 知 $x = cba \cdot x = cb \cdot y = c \cdot w$, 则有 $w = c^{-1} \cdot x = x$, 即有 $x = by$.

令 $w' = cy$, 利用 $b = b^{-1}$ 有 $z = cba \cdot z = cb \cdot x = c \cdot y = w'$, 从而有 $z = c \cdot y$. 最后可得 $b \cdot z = z$. *(这里其是应该画有向图更容易看清结构)*

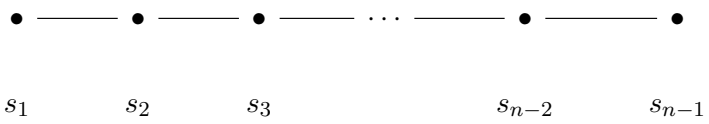
通过上述分析, 我们得到的有向图每个点都有进的 a, b, c-箭头, 也有出的 a, b, c-箭头, 从而 $G/H = \{x, y, z\}$, 即 $|G/H| = 3$. 且我们有群同态

$$\begin{aligned} \varphi \colon G &\longrightarrow S_3 \\ a &\longmapsto (1\ 2\ 3) \\ b &\longmapsto (1\ 2) \\ c &\longmapsto (2\ 3). \end{aligned}$$

因此 $G \hookrightarrow S_3$, 而 $|G| = 3 \times 2$, 从而 $G \simeq S_3$.

下面考虑所谓的 Coxeter 图 (Coxeter diagram) (一般的定义参考作业 4) 定义的 Coxeter 群 (Coxeter 群), 我们证明

命题 4.1.9. *群 S_n 同构于由下图定义的群 G,*



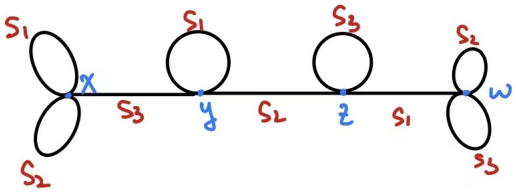
其中 $G = \langle s_i \mid s_i^2 = e, (s_i s_{i+1})^3 = e, (s_i s_j)^2 = e \rangle$.

证明: 使用数学归纳法. $n = 2$ 时, 有 $\langle s_1 \mid s_1^2 = e \rangle = \mathbb{Z}/2\mathbb{Z} \simeq S_2$.

考虑 $n \geq 3$, 假设对 $n-1$ 结论成立, 我们令 H 为 G 中由 $s_1, \cdots, s_{n-2}$ 生成的子群. 由于有满同态 $S_{n-1} \twoheadrightarrow H$, $G \twoheadrightarrow S_n$, 知 $|H| \leq (n-1)!$ 且 $|G| \geq n!$, 只需证 $|G/H| = n$. □

在给出一般的证明之前, 我们还是来对 S_4 的情况操作一遍 Coxeter–Todd 算法.

例子. *令 $H = \langle s_1, s_2 \rangle$ 是 S_4 中有 1,2 基础对换生成的子群.*



(参考上图) 则有 s_1, s_2 在 $x = eH$ 上是平凡作用, 我们令 $y = s_3 \cdot x$, $z = s_2 \cdot y$, $w = s_1 \cdot z$.

第五章　第五周

5.1　十月十一日

我们今天来考虑 $\mathrm{PSL}(2,\mathbb{F})$ 的单性, 其中域 $\mathbb{F}$ 满足 $|\mathbb{F}| \geq 4$, 并且我们将在作业中考虑 $n \geq 3$ 的情况. 首先我们有如下众所周知的结果:

命题 5.1.1.

$$C(\mathrm{GL}(2,\mathbb{F})) = \{\lambda \mathrm{I} \mid \lambda \in \mathbb{F}^\times\}$$
$$C(\mathrm{SL}(2,\mathbb{F})) = \{\pm \mathrm{I}\}$$

在本节的最后, 我们将证明当 $|\mathbb{F}| \geq 4$ 的时候, $\mathrm{SL}(2,\mathbb{F})$ 的正规子群要么形如 $C(\mathrm{SL}(2,\mathbb{F}))$, 要么是 $\mathrm{SL}(2,\mathbb{F})$, 从而证明 $\mathrm{PSL}(2,\mathbb{F})$ 的单性. 为了证明我们的结果, 先介绍一些工具.

定义 5.1.2. 对于群 G, 其中 G 为 $\mathrm{GL}(2,\mathbb{F})$ 或 $\mathrm{SL}(2,\mathbb{F})$, 其形如

$$B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

的子群被称为 G 的波雷尔子群 (Borel subgroup).

定义 5.1.3. 对于 $\mathrm{GL}(2,\mathbb{F})$, 其外尔群 (Weyl group)是如下两个元素组成的子群

$$W = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\} = \{\mathrm{I}, w_0\}$$

类似的, 对于 $\mathrm{SL}(2,\mathbb{F})$, 其外尔群 (Weyl group)是如下两个元素组成的子群

$$W = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\} = \{\mathrm{I}, w_0\}$$

注记. 对于波雷尔子群 B, 我们通常记 $\overline{B} := w_0 B w_0^{-1}$, 经过计算不难发现其是形如

$$\overline{B} = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$$

的子群.

命题 5.1.4. $\mathrm{SL}(2,\mathbb{F})$ 的波雷尔子群 B 其所有共轭子群的交是 $\mathrm{SL}(2,\mathbb{F})$ 的中心.

证明: 注意到

$$w_0Bw_0^{-1}\cap B=\{\begin{pmatrix}a&0\\0&a^{-1}\end{pmatrix}\}$$

并且

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a&0\\0&a^{-1}\end{pmatrix}\begin{pmatrix}1&-1\\0&1\end{pmatrix}=\begin{pmatrix}a&a^{-1}-a\\0&a^{-1}\end{pmatrix}\in\{\begin{pmatrix}a&0\\0&a^{-1}\end{pmatrix}\}$$

这意味着 $a=a^{-1}$, 即 $a=\pm1$. □

命题 5.1.5 (Bruhat 分解)**.** 对 $\mathrm{GL}(2,\mathbb{F})$, 我们有如下分解:

$$\mathrm{GL}(2,\mathbb{F})=\coprod_{w\in W}BwB=B\coprod Bw_0B$$

类似的, 对 $\mathrm{GL}(2,\mathbb{F})$, 我们有如下分解

$$\mathrm{SL}(2,\mathbb{F})=\coprod_{w\in W}BwB=B\coprod Bw_0B$$

证明: 这里我们对 $\mathrm{GL}(2,\mathbb{F})$ 进行证明, $\mathrm{SL}(2,\mathbb{F})$ 的情况类似. 任取 $A\in\mathrm{GL}(2,\mathbb{F})$, 形如

$$A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$$

如果 $c=0$，那么 $A\in B$, 这种情况是平凡的, 因此不妨假设 $c\neq0$, 在这种情况下，我们只需要寻找可逆的 $A_1,A_2\in B$, 使得

$$A_1\begin{pmatrix}a&b\\c&d\end{pmatrix}A_2=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

即可. 然而我们知道左乘 (右乘) 一个可逆矩阵相当于是对其进行行 (列) 变换, 因此这实际上是在通过行列变换将 A 中的 a,d 两项消去，这在 $c\neq0$ 的情况下显然是可以做到的. □

推论 5.1.6. 对于群 G, 其中 G 为 $\mathrm{GL}(2,\mathbb{F})$ 或 $\mathrm{SL}(2,\mathbb{F})$, G 的波雷尔子群 B 是其极大子群.

证明: 任意 G 的子群 H 使得 B 真包含于 H, 那么存在 $A\in H\cap Bw_0B$, 即存在 $A_1,A_2\in B$ 使得 $A=A_1w_0A_2\in H$, 这意味着 $w_0=A_1^{-1}AA_2^{-1}\in H$. 根据 Bruhat 分解我们可以直接得到 $G\subseteq H$, 从而任何真包含 B 的子群都是 G 自身, 即 B 是 G 的极大子群. □

下面再来考虑波雷尔子群的一类交换子群

$$U=\{\begin{pmatrix}1&a\\0&1\end{pmatrix}\mid a\in\mathbb{F}\}\subset B$$

显然我们有 $U\cong(\mathbb{F},+)$, 群同构由下面的映射给出

$$\begin{pmatrix}1&a\\0&1\end{pmatrix}\mapsto a$$

命题 5.1.7. U 是 B 的正规子群.

证明: 留作作业. □

命题 5.1.8. $Bw_0B = Bw_0U$, 且后一种写法唯一.

证明: 存在性: 我们只需要在 Bruhat 分解证明过程中行列变换最后一步将非零元化为 1 的时只进行行变换不进行列变换即可.

唯一性: 如果 $A_1w_0A_2 = A_3w_0A_4$, 其中 $A_1, A_3 \in B, A_2, A_4 \in U$, 那么有

$$w_0^{-1}A_3^{-1}A_1w_0 = A_4A_2^{-1}$$

注意到左侧是一个下三角矩阵, 右侧是 U 中的元素, 即是主对角线全是 1 的上三角矩阵, 从而只能是单位阵. □

命题 5.1.9. $\mathrm{SL}(2,\mathbb{F})$ 由如下元素生成

$$U = \{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\}, \overline{U} = w_0Uw_0^{-1} = \{\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}\}$$

证明: 取 $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{F})$. 我们分如下的一些情况考虑:

1. 假设 $b \neq 0$, 那么

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (d-1)/b & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ (a-1)/b & 1 \end{pmatrix}.$$

2. 假设 $c \neq 0$, 那么

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & (a-1)/c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\begin{pmatrix} 1 & (d-1)/c \\ 0 & 1 \end{pmatrix}$$

3. 如果 $b = c = 0$, 那么 A 实际上形如 $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$, 那么

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (1-a)/a & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1/a \\ 0 & 1 \end{pmatrix}.$$

□

定义 5.1.10. 对于群 G, 其交换子 (commutator)是指由形如 $aba^{-1}b^{-1}, a, b \in G$ 生成的子群, 被记做 $[G,G]$.

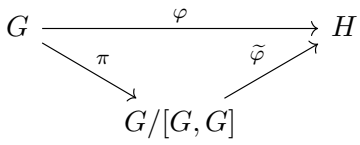
命题 5.1.11. 对于群 G 来说, $[G,G]$ 是其正规子群.

证明: 注意到任取 $a, b, g \in G$, 我们有

$$g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in [G,G]$$

□

命题 5.1.12. 任取群同态 $\varphi : G \to H$, 如果 H 是交换群, 那么 φ 一定经过 $G/[G,G]$, 即存在 $\widetilde{\varphi} : G/[G,G] \to H$ 使得下图交换



证明: 只需要证明 $[G,G]\subseteq \operatorname{Ker}\varphi$, 直接验证即可. □

以上所有的结果我们都没有用到 $|F|\geq 4$, 从下面开始, 我们总是需要假设这个关键条件.

命题 5.1.13. 当 $|F|\geq 4$ 时, 我们有 $\mathrm{SL}(2,\mathbb{F})=[\mathrm{SL}(2,\mathbb{F}),\mathrm{SL}(2,\mathbb{F})]$.

证明: 由于 $\mathrm{SL}(2,\mathbb{F})$ 可以由 $U,\overline{U}$ 生成, 所以只需要验证 $U\subset[\mathrm{SL}(2,\mathbb{F}),\mathrm{SL}(2,\mathbb{F})]$ 即可. 注意到

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{pmatrix}$$

由于 $|\mathbb{F}|\geq 4$, 那么一定存在 a 使得 $a^2\neq 1$, 从而

$$U=\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\subset[\mathrm{SL}(2,\mathbb{F}),\mathrm{SL}(2,\mathbb{F})]$$

并且由于 $[\mathrm{SL}(2,\mathbb{F}),\mathrm{SL}(2,\mathbb{F})]$ 是正规子群, 从而 $\overline{U}\in[\mathrm{SL}(2,\mathbb{F}),\mathrm{SL}(2,\mathbb{F})]$. □

命题 5.1.14. 若 H 是 $\mathrm{SL}(2,\mathbb{F})$ 的正规子群, 其中 $|F|\geq 4$, 那么 $H\subset\{\pm \mathrm{I}\}$ 或 $H=\mathrm{SL}(2,\mathbb{F})$.

证明: 在证明中, 我们用 G 来指代 $\mathrm{SL}(2,\mathbb{F})$. 若 H 正规, 那么 $HB=BH$ 是 G 的包含 B 的子群, 而由于 B 是 G 的极大子群, 从而只有如下两种情况:

1. $HB=B$;
2. $HB=G$.

对于第一种情况, 我们可知 $H\subset B$, 并且由于 H 是正规子群, 那么 H 包含在 B 的所有共轭子群的交中, 从而 $H\subseteq\{\pm \mathrm{I}\}$.

对于第二种情况, 此时我们断言 $HU=G$. 如果断言成立, 那么有:

$$\begin{aligned} G/H &\cong HU/H \\ &\cong U/H\cap U \end{aligned}$$

由于 U 是交换的, 从而根据上面的同构可知 G/H 也是交换的, 因此 $G=[G,G]\subset H$, 即 $G=H$.

现在我们在第二种情况的假设下证明 $HU=G$: 由于 G 由 $U,\overline{U}$ 生成, 并且显然 $U\subset HU$, 所以只需要证明 $\overline{U}\subset HU$ 即可. 由 $HB=G$, 我们有 $w_0\in HB$, 不妨记 $w_0=hb, h\in H, b\in B$, 那么

$$\overline{U}=w_0Uw_0^{-1}=hbUb^{-1}h^{-1}\subset HUH=HU$$

□

推论 5.1.15. 当 $|F|\geq 4$ 时, $\mathrm{PSL}(2,\mathbb{F})$ 是单群.

5.2 十月十二日

定义 5.2.1. 一个环 (ring), 是一个集合 R 有如下两种运算:

1. 加法运算 "$+$", 使得 R 构成一个阿贝尔群 $(R,+)$, 其中的单位元被记做 0;
2. 乘法运算 "$\times$", 使得 R 构成一个幺半群, 即对于乘法运算存在单位元 1 以及满足结合律;
3. 乘法与加法运算之间存在分配律.

注记. 更严格的来说, 我们这里定义的是含有单位元的环, 这与一些教材上对环的定义不一样.

定义 5.2.2. 一个交换环 (communicative ring), 是指一个乘法运算交换的环.

注记. 实际上, 我们之后只关心带有幺元的交换环, 并简称带单位元的交换环为环.

例子. *一些交换环的例子:*

- $(\mathbb{Z},+,\times,0,1)$;
- $(\mathbb{Q},+,\times,0,1)$;
- 零环 $R=\{0\}$, 即只有一个元素组成的环.

命题 5.2.3. *在环 R 中, 有 $0\times a=0$ 对任意 $a\in R$ 成立.*

证明: 首先由于 $0+0=0$, 那么任取 $a\in A$, 根据分配律可知

$$\begin{aligned} 0\times a &= (0+0)\times a \\ &= 0\times a+0\times a \end{aligned}$$

两侧同时加上 $-(0\times a)$, 则有

$$0=0\times a$$

□

命题 5.2.4. *如果在环 R 中满足 $1=0$, 那么 R 是零环.*

证明: 任取 $a\in R$, 则 $a=1\times a=0\times a=0$, 即 R 是零环. □

定义 5.2.5. 一个环 R 中的元素 a 被称为单位 (unit), 如果 a 存在一个乘法逆 b, 即存在 $b\in R$ 使得 $ab=ba=1$.

注记. 与处理群中的逆元类似, 不难证明一个元素 a 如果存在逆那么其逆一定唯一, 我们通常记做 a^{-1}.

定义 5.2.6. 给定一个环 R, 其上的一个形式多项式 (formal polynomial)$f(x)$, 是形如下式的元素

$$f(x):=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,\quad a_n\neq 0, a_i\in R, i=0,1,2,\ldots,n$$

其中 x 被称为单项式 (monomial), n 被称作多项式的次数, 记做 $\deg f$. 两个形式多项式

$$\begin{aligned} f(x)&=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0 \\ g(x)&=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0 \end{aligned}$$

当且仅当 $m=n, a_i=b_i$ 对任意的 i 成立.

定义 5.2.7. 给定一个环 R, 其上的多项式环 (polynomial ring)定义为

$$R[x] := \{f(x) \mid f(x)\text{是 } R \text{ 上的形式多项式}\}$$

其中给定 $f, g \in R[x]$, 加法乘法运算如下给出:

1. $f + g(x) := (a_0 + b_0) + (a_1 + b_1)x + \ldots$;
2. $fg(x) := a_0b_0 + (a_0b_1 + a_1b_0)x + (a_1b_1 + a_2b_0 + a_0b_2)x^2 + \ldots$.

练习. 验证 $R[x]$ 构成了一个环.

注记. 如果在构造多项式环时取环 $R' = R[x]$, 其中 R 是一个环, 那么我们可以定义 R 上的二元多项式环 $R[x, y]$ 为 $R[x][y]$.

定义 5.2.8. 给定 $f(x), g(x) \in R[x]$, 如果存在 $q(x), r(x) \in R[x]$ 使得

$$g(x) = f(x)q(x) + r(x)$$

其中 $\deg r < \deg f$, 那么我们称 $f(x)$ 带余式 $r(x)$ 除 $g(x)$, 这个过程被称为带余除法 (division with remainder)

命题 5.2.9. 带余除法总可以进行, 只要除式 $f(x)$ 的首项 a_n 是 R 中的单位.

定义 5.2.10. 对于环 R, 如果 $R\backslash\{0\}$ 都是 R 中的单位, 那么 R 被称为一个域 (field).

例子. 一些域的例子:

- $\mathbb{Q}$;
- $\mathbb{R}$;
- $\mathbb{C}$;
- $\mathbb{Z}/p\mathbb{Z}$, 其中 p 是素数.

定义 5.2.11. 环 R 的一个子环 (subring)R' 指的是 R 的一个子集, 满足对加、减、乘运算封闭, 并且环 R 的 $0, 1$ 在 R' 中.

定义 5.2.12. 给定两个环 R_1, R_2, 一个映射 $f : R_1 \to R_2$ 被称为环同态 (ring homomorphism), 如果

1. f 保持加法乘法运算;
2. $f(1) = 1$.

注记. 注意, f 保持加法运算我们则一定有 $f(0) = 0$, 但是保持乘法运算不一定有 $f(1) = 1$(为什么?), 因此我们需要在第二条中要求这件事情.

例子. 对于多项式环 $R[x]$, 我们定义其上的赋值映射 *(evaluation map)*, 定义为

$$\begin{aligned} e_s : R[x] &\to R \\ p(x) &\mapsto p(s) \end{aligned}$$

命题 5.2.13 (替换准则 (substitution principle))**.** *给定环同态 $f : R_1 \to R_2$, 任取 $\alpha \in R_2$, 存在唯一的环同态*

$$\Phi : R_1[x] \to R_2$$

使得 $\Phi(x) = \alpha$ 以及 $\Phi|_{R_1} = f$. 更一般地, 任取 $\alpha_1, \alpha_2, \ldots, \alpha_n \in R_2$, 存在唯一的环同态 $\Phi : R_1[x_1, x_2, \ldots, x_n] \to R_2$, 使得 $\Phi(x_i) = \alpha_i$ 以及 $\Phi|_{R_1} = f$

证明: 我们如下定义 Φ:

$$\Phi : R_1[x] \to R_2$$
$$a_n x^n + \cdots + a_0 \mapsto f(a_n)\alpha^n + \cdots + f(a_0)$$

□

定义 5.2.14. 一个环同态 f 被称为环同构 (ring isomorphism), 如果其作为映射是双射.

定义 5.2.15. 给定环同态 $f : R_1 \to R_2$, 映射的核 (kernel)被定义为

$$\mathrm{Ker}(f) = \{a \in R_1 \mid f(a) = 0_{R_2}\}$$

命题 5.2.16. *对于环同态 $f : R_1 \to R_2$ 的核 $\mathrm{Ker}(f)$, 我们有如下性质:*

1. *$\mathrm{Ker}(f)$ 对加法构成子群;*
2. *任取 $s \in \mathrm{Ker}(f), r \in R_1$, 有 $rs \in \mathrm{Ker}(f)$;*
3. *如果 f 是环同构, 那么 $\mathrm{Ker}(f) = \{0_{R_1}\}$*
4. *如果 $1_{R_1} \in \mathrm{Ker}(f)$, 那么 $\mathrm{Ker}(f) = R_1$.*

证明: 显然. □

注记. 上述命题表示 1 不一定在环同态 f 的核中, 即一般来说环同态的核不是子环, 这与我们在群的时候情况并不一样.

有关环同态核的性质, 我们抽象出来, 即得到了理想的概念, 这是环论中非常非常重要的概念.

定义 5.2.17. 环 R 的一个子集 I 被称为 R 的理想 (ideal), 如果

1. 对于加法 I 构成子群;
2. 任取 $s \in I, r \in R$, 有 $rs \in I$.

例子. *对于环 R 来说, 其存在两个平凡理想:R 本身与 $\{0\}$, 其他的理想被称为非平凡理想.*

例子. *对环同态 $f : R_1 \to R_2$ 来说, $\mathrm{Ker}(f)$ 是 R_1 的理想.*

定义 5.2.18. 环 R 的一个理想 I 被称为主理想 (principal ideal), 如果存在 $s \in R$, 使得

$$I = (s) := \{sr \mid r \in R\}$$

定义 5.2.19. 环 R 的一个理想 I 被称为有限生成理想 (finitely generated ideal), 如果存在 $s_1, s_2, \ldots, s_r \in R$, 使得

$$I = (s_1, \ldots, s_r) := \{\sum_{i=1}^{r} r_i s_i \mid r_i \in R\}$$

命题 5.2.20. 给定一个环 R 以及一个理想 I, 在集合 R/I 上存在唯一的环结构, 使得如下映射是环同态:

$$\pi : R \to R/I$$
$$a \mapsto a + I$$

我们称 R/I 是一个商环 *(quotient ring)*.

证明: 首先如果只考虑 R 以及 I 上的加法结构, 显然 R/I 构成了一个商群, 因此我们只需要去定义 R/I 上的乘法结构即可. 注意到如果想要 π 是一个环同态, 我们只能如下定义我们的乘法结构: 任取 $a+I, b+I \in R/I$,

$$(a+I)(b+I) := ab + I$$

此时我们需要验证我们的定义不依赖于代表元的选取, 即如果

$$a_1 + I = a_2 + I$$
$$b_1 + I = b_2 + I$$

那么一定有

$$a_1 b_1 + I = a_2 b_2 + I$$

根据理想的定义, 我们有

$$b_1(a_1 - a_2) \in I$$
$$a_2(b_1 - b_2) \in I$$

上面两式相加即有 $a_1 b_1 - a_2 b_2 \in I$, 即我们的乘法运算是良好定义的. □

定理 5.2.21 (第一同构定理)**.** 如果 $f : R_1 \to R_2$ 是满的环同态, 那么 $R_1/I \cong R_2$, 其中 I 是 f 的核.

命题 5.2.22. 给定环同态 $f : R_1 \to R_2$ 以及 R_1 的一个理想 I, 我们记 $K = \mathrm{Ker}(f), \pi : R \to R/I$, 那么:

1. 如果 $I \subset K$, 那么存在唯一的映射 $\widetilde{f} : \overline{R} := R_1/I \to R_2$, 使得 $\widetilde{f} \circ \pi = f$.
2. $I = K$ 当且仅当上述映射 $\widetilde{f}$ 是一个同构.

例子. 考虑赋值映射 $e_2 : \mathbb{Q}[x] \to \mathbb{Q}$, 定义为 $e_2(p(x)) = p(2), p(x) \in \mathbb{Q}[x]$. 显然 $(x-2) \in \mathrm{Ker}(e_2)$, 并且根据带余除法我们可知 $\mathbb{Q}[x]/(x-2) \cong \mathbb{Q}$, 从而由上述命题可知 $\mathrm{Ker}(e_2) = (x-2)$ 是一个主理想.

定理 5.2.23 (对应定理)**.** 给定满的环同态 $f : R_1 \to R_2$, 并记 $K = \mathrm{Ker}(f)$, 那么我们有如下的一一对应:

$$\{R_1 \text{中包含 } K \text{ 的理想}\} \overset{1-1}{\Longleftrightarrow} \{R_2 \text{中的理想}\}$$

并且一一对应如下给出:

1. 如果 $K \subset I$, 那么其对应到 R_2 中的理想 $f(I)$;
2. 如果 $\widetilde{I}$ 是 R_2 中的理想, 那么 $f^{-1}(\widetilde{I})$ 是 R_1 中包含 K 的理想.

下面我们要做的事情是对一些常见的环分类它的所有非平凡理想.

例子. 我们断言 $\mathbb{Z}$ 中所有的理想都是形如 $I=(a), a\in\mathbb{Z}$ 的主理想. 假设 I 是 $\mathbb{Z}$ 的一个理想, 我们选取 I 中有最小非零绝对值的元素 a, 那么任取 $b\in I$, 我们用 a 去对 b 做带余除法得到

$$b=am+r$$

其中 $|r|<a$, 然而由于 $b, am\in I$, 从而 $r\in I$, 根据我们对 a 的选取有 $r=0$, 从而 $I=(a)$.

注记. 值得注意的是, 这里的证明成立只依赖于带余除法在 $\mathbb{Z}$ 中成立这个事实, 因此在一个环中只要带余除法成立, 其所有的理想就一定是主理想.

例子. $\mathbb{C}[x]$ 中的所有里的都是形如 $I=(f(x))$ 的主理想, 其中 $f(x)\in\mathbb{C}[x]$.

例子. 根据对应定理, $\mathbb{Z}/n\mathbb{Z}$ 的所有理想一一对应于 $\mathbb{Z}$ 中包含 (n) 的理想, 而 $\mathbb{Z}$ 的一个理想 (a) 包含 (n) 当且仅当 $a\mid n$, 从而我们也分类了 $\mathbb{Z}/n\mathbb{Z}$ 的所有理想.

索引