# 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. $\sigma$ 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 $\sigma$ 是双射, 知 $\tau$ 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 $\sigma$ 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 $f^{-1}$. $\tau$ 也是如此定义, 记作 $\sigma^{-1}$, 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 $\sigma$ 交换 $1,3$ 位置. 因此 $\sigma\tau = 213$. 而 $\tau$ 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 $\pi$ 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.

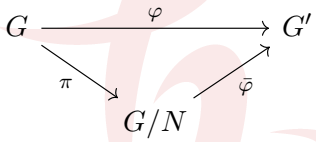
□

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 $\infty$.

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 $\varphi$ 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 $G_{gx} = gG_xg^{-1}$.

## 2.3 作业 2

**练习.** *Find the number of isomorphism classes of actions of $S_4$ on $[5]$.*

**练习.** *Prove that there is no transitive action of $S_6$ on $[7]$. (How about $S_7$ and $[8]$?)*

**练习.** *Suppose that the map $f : G \longrightarrow G$ by $a \mapsto a^{-1}$ is an automorphism of group $G$, then $G$ is abelian.*

**练习.** *Let $G$ be a group generated by real valued functions $f = \frac{1}{x}$ and $g = \frac{x-1}{x}$ via composition of functions. Prove that $G$ is isomorphic to $S_3$.*

**练习.** *Classify subgroups and normal subgroups of $D_n$ for $n \geq 3$.*

**练习.** *Prove that $G = GL(2, \mathbb{F}_2)$ is isomorphic to $S_3$ by the action of $G$ on $(\mathbb{F}_2)^2$.*

**练习.** ***Second Isomorphism Theorem.*** *Let $H$ be a normal subgroup of group $G$ and $K$ be a subgroup of $G$. Prove*

1. *$HK = \{hk | h \in H, k \in K\}$ is a subgroup of $G$.*
2. *$H \cap K$ is a normal subgroup of $K$.*
3. *There is an isomorphism $HK/H \cong K/H \cap K$.*

**练习.** *Let $O_1, \cdots, O_k$ be all the conjugacy classes in a finite group $G$. Choose $x_i \in O_i$ and let $C_i = \{g \in G | gx_ig^{-1} = x_i\}$ (which is called the centralizer of $x_i$). Denote $n_i = |C_i|$. Prove*

$$\frac{1}{n_1} + \frac{1}{n_2} + \cdots \frac{1}{n_k} = 1$$

**练习.** ***Artin, Chapter 6, 8.1*** *Does the rule $P * A = PAP^T$ define an operation of $\mathrm{GL}(n, \mathbb{R})$ on the set of real $n \times n$ matrices? (Here $P^T$ means the transpose of $P$)*

**练习.** 定义 $PGL(2, \mathbb{F}_3) = GL(2, \mathbb{F}_3)/D$. 其中 $D = \{\lambda I_5 \mid \lambda \in \mathbb{F}_5^\times\}$. 证明 $PGL(2, \mathbb{F}_3) \cong S_4$. 提示：考虑 $GL(2, \mathbb{F}_3)$ 在 $(\mathbb{F}_3)^2$ 的所有一维子空间组成的集合上的作用.

**练习.** 令 $G$ 是一个群, $\mathbb{R}^\times$ 是 $\mathbb{R}$ 中非零元素在域的乘法下组成的群。考虑由 $G \to \mathbb{R}$ 的所有映射组成的 $\mathbb{R}$-线性空间 $V$. 假设 $S$ 是由有限个 $G \to \mathbb{R}^\times$ 的群同态组成的集合. 证明 $S$ 中的元素在 $V$ 上线性无关.

**练习.** 证明有限群 $G$ 是循环群当且仅当对任意正整数 $n$, $G$ 至多只有一个阶数为 $n$ 的子群.

**练习.** *(Semidirect product) Let $H$ and $K$ be two groups and $\phi\colon K \to \mathrm{Aut}(H)$ be a group homomorphism. Define a binary operation on $H \times K$ by $(h, k)(h', k') = (h\varphi(k)(h'), kk')$. Check this binary operation gives a group structure. Prove that the subsets $\{e_H\} \times K$ and $H \times \{e_K\}$ are subgroups of this group and $H \times \{e_K\}$ is a normal subgroup. Find one example that $\{e_H\} \times K$ is not a subgroup.*

**练习.** *Prove that $\mathrm{GL}(n, \mathbb{C})$ is isomorphic to a subgroup of $\mathrm{GL}(2n, \mathbb{R})$.*

**练习.** 证明 $\mathbb{C}^\times$ 同构于 $\mathbb{C}/\mathbb{Z}$. 其中 $\mathbb{C}^\times$ 是 $\mathbb{C}$ 中非零元素组成的乘法群. $\mathbb{C}$ 和 $\mathbb{Z}$ 是加法群.

**练习** (思考题，不用交). 证明 $PGL(2, \mathbb{F}_5) \cong S_5$.

**练习** (思考题，不用交，在学完模论之后有更多工具可以做). *Let $G$ be the group $\mathrm{GL}(3, \mathbb{F}_2)$.*

1. *How many conjugacy classes does $G$ have?*
2. *Show that $G$ has exactly two conjugacy classes of size 24.*

# 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 $U=\left\{\begin{pmatrix}1&&*\\&\ddots&\\0&&1\end{pmatrix}\right\}$ 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 $H=\left\{\begin{pmatrix}r\\0\end{pmatrix}\right\}$ 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 $\sigma$ 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 $\sigma$ 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.

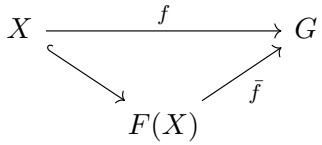
**例子.** 若 $|X|=1$, 则有 $F(X)\simeq\mathbb{Z}$. 若 $|X|\neq|Y|$, 则有 $F(X)\not\simeq F(Y)$.

**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 $\mathrm{Ker}\, f \supset \{x^n, y^2, (yx)^2\}$ *(*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 $\{x^n, y^2, (yx)^2\} \subset \mathrm{Ker}\, f$, 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 $\sigma$ 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 $\sigma$ 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.

## 3.3 作业 3

**练习.** 设 $p$ 为素数，求 $GL(\mathbb{F}_p)$ 中 *Sylow-p* 子群的个数.

**练习.** 如果 $S_n$ 中元素 $\sigma$ 的写成不相交的轮换的乘积 $\sigma = \sigma_1 \cdots \sigma_l$，其中长度为 $m$ 的轮换个数为 $\lambda_m$. *(这里 1-轮换 $(i)$ 表示保持该元素 $i$ 不变)*。我们将 $\sigma$ 的 *type* 记作 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$，并满足 $\sum_i i\lambda_i = n$. 请证明 $S_n$ 中两个元素共轭当且仅当两者有相同的 *type*.

**练习.** *In $S_n$, compute the number of the permutations of type $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$, and prove the following formula*

$$\sum_{\lambda} \frac{1}{\prod_{i=1}^{n} i^{\lambda_i}\lambda_i!} = 1.$$

*Here $\lambda$ is the index $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ such that $\sum_i i\lambda_i = n$.*
*(Hint: 用作业 2)*

**练习.** *Let $n \geq 2$, prove that $(12)$ and $(123\cdots n)$ generate the group $S_n$.*

**练习.** *Let $n \geq 3$. Prove that $(123)$, $(124)$, $\cdots$, $(12n)$ generate the group $A_n$.*

**练习.** 证明 $D_n$ 同构于由两个生成元 $x, y$ 生成，且满足如下关系的群。

$$x^n = y^2 = (xy)^2 = e$$

**练习.** 假设 $p$ 和 $q$ 是两个素数，请分类 $pq$ 阶的群。

**练习.** 请分类 12 阶群。

**练习.** *The conjugation induces an group homomorphism from $G$ to $Aut(G)$. We call the image of this morphism $Inn(G)$ as inner automorphism group. Prove that the group of inner automorphisms of a group $G$ is normal in $Aut(G)$. We call the quotient group $Aut(G)/Inn(G)$ as outer automorphism group $Out(G)$.* 注意：有同学认为半直积的结构由到 $H$ 到 $Out(G)$ 的 *morphism* 确定，这个一般是不对的，参见 *https://math.stackexchange.com/questions/1710620/do-homomorphisms-h-to-operatornameautk-that-coincide-at-the-level-of-o?rq=1*。

**练习.** 证明如果群 $G$ 有有限指数的子群，则 $G$ 有有限指数的正规子群。

**练习.** 证明如果群 $G$ 有两个有限指数的子群 $H$ 和 $K$，则 $H \cap K$ 也是 $G$ 的有限指数子群.

**练习.** 循环群

1. *Let $p$ be a prime number, $G = \{x \in \mathbb{C} \mid \exists\ n \text{ such that } x^{p^n} = 1\}$. Then $G$ is a group with usual multiplication, and every proper subgroup of $G$ are cyclic of finite order.*
2. *Prove that $(\mathbb{Q}, +)$ is not a cyclic group, but any finitely generated subgroup are cyclic.*
3. *Let $G$ be a nonabelian group. Prove that the group $Aut(G)$ is not cyclic. In particular, if $|Aut(G)|$ is a prime number, then $G$ is abelian.*
   *(Hint: Consider the inner automorphism $Inn(G) \leq Aut(G)$, prove that $Inn(G) \cong G/Z(G)$)*

**练习.** *(Burnside lemma) Suppose a finite group $G$ acts on a finite set $S$. Let $F(g) = |\{ x \in S \mid gx = x\}|$, namely the number of fixed point by $g$. Write $t$ as the number of different orbits of action $G$ on $S$. Prove the following formula*

$$t = \frac{\sum_{g\in G} F(g)}{|G|}$$

**练习.** *Let $p$ be a prime number, $G$ is a $p$-group. Prove that the number of non-normal subgroups of $G$ must be multiple of $p$.*

**练习.** *Let $G = GL_n(\mathbb{C})$. Prove that $G$ has no proper subgroups of finite index.*

**练习.** *Let $G$ be a group, and $A$ a normal abelian subgroup. Show that $G/A$ operates on $A$ by conjugation , and in this manner get a homomorphism of $G/A$ into $Aut(A)$.*

**练习** (思考题，不用交)**.** 下面我们确定在正规子群和商群确定时如何分类群的结构。我们引入一些概念。

**定义 3.3.1.** 假设有群 $G_1$,$G_2$, $G_3$ 的同态 $f\colon G_1 \to G_2$, $g\colon G_2 \to G_3$。我们称如下序列

$$G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3$$

在 $G_2$ 处正合，如果 $Im(f) = \ker(g)$。一个元素的群记作 1. 则称序列

$$1 \to G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \to 1$$

为短正合列，如果序列在 $G_1$,$G_2$, $G_3$ 处均正合，即 $f$ 是单同态，$g$ 是满同态，且 $Im(f) = \ker(g)$. 这个序列此时也称作 $G_3$ 关于 $G_1$ 的一个 extension. 另一个 extension

$$1 \to G_1 \xrightarrow{f'} G_2' \xrightarrow{g'} G_3 \to 1$$

和已知的这个同构是指存在 $G_2 \to G_2'$ 的群同构 $F$，使得有如下的图表中的每一个矩形都交换

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_1 & \xrightarrow{f} & G_2 & \xrightarrow{g} & G_3 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & G_1 & \xrightarrow{f'} & G_2' & \xrightarrow{g'} & G_3 & \longrightarrow & 1 \end{array}$$

即 $f' = F \circ f$ 和 $g = g' \circ F$.

**定义 3.3.2.** 短正合列

$$1 \to G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \to 1$$

分裂是指存在同态 $i\colon G_3 \to G_2$ 使得 $g \circ i = Id_{G_3}$。

以下我们假设 $G_1$ 是交换群，其中的群运算记作 $+$，单位元记作 0。则由以上习题知，短正合列

$$1 \to G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \to 1$$

会诱导一个 $G_3$ 在 $G_1$ 上的共轭作用，或者等价于有群同态 $\phi\colon G_3 \to Aut(G_1)$. 我们现在分类这个同态 $\phi$ 给定的情况下的所有 *extension.*

1. 证明当短正合列分裂时，$G_2$ 同构于 $G_1$ 和 $G_3$ 的半直积.
2. 取映射 $s\colon G_3 \to G_2$, 使得 $g \circ s = Id_{G_3}$. 证明这样的 $s$ 可以取到，且若映射 $s'\colon G_3 \to G_2$, 满足 $g \circ s' = Id_{G_3}$, 则存在映射 $y\colon G_3 \to G_1$，使得 $s'(b) = y(b)s(b)$. 我们称这样的 $s$ 为截面.
3. 定义映射 $\alpha\colon G_1 \times G_3 \to G_2$ 为 $\alpha(a,b) = a \cdot s(b)$. 证明这是一个双射.
4. 利用这一双射和 $G_2$ 的群结构在集合 $G_1 \times G_3$ 上诱导一个群结构, 使得 $\alpha$ 是一个群同构. 证明在这个群结构下存在映射 $c\colon G_3 \times G_3 \to G_1$ 使得 $(a_1,b_1)\cdot(a_2,b_2) = (a_1+(\phi(b_1))(a_2)+c(b_1,b_2), b_1b_2)$, 且 $c$ 满足

$$(\phi(b_1))(c\,(b_2,b_3)) - c\,(b_1b_2,b_3) + c\,(b_1,b_2b_3) - c\,(b_1,b_2) = 0$$

   对任意 $b_1,b_2,b_3 \in G_3$ 成立.
5. 假设给定 $c$ 满足如上条件,利用上述公式 $(a_1,b_1)\cdot(a_2,b_2) = (a_1+(\phi(b_1))(a_2)+c(b_1,b_2), b_1b_2)$ 在 $G_1 \times G_3$ 上定义运算，证明这是一个群结构，且做成 $G_3$ 在 $G_1$ 上的 *extension*.
6. 映射 $\{x\colon G_3 \times G_3 \to G_1\}$ 组成的集合有自然的交换群结构, 加法定义为 $(x_1+x_2)(b_1,b_2) = x_1(b_1,b_2) + x_2(b_1,b_2)$. 证明满足以上条件的 $c$ 构成一个子群, 记作 $Z^2(G_3,G_1)$.
7. 不同的截面 $s$ 的选取会对应 $Z^2(G_3,G_1)$ 的一个子群 $B^2(G_3,G_1)$. 具体来说，请证明 $s$ 换成 $s'$ 时，对应的 $c'$ 满足 $c'(b_1,b_2) = c(b_1,b_2) + \phi(b_1)(y(b_2)) - y(b_1b_2) + y(b_1)$. 证明形如 $x(b_1\ b_2) = \phi(b_1)(y(b_2)) - y(b_1b_2) + y(b_1)$ 的映射构成 $Z^2(G_3,G_1)$ 的一个子群, 记作 $B^2(G_3,G_1)$.
8. 证明 $Z^2(G_3,G_1)/B^2(G_3,G_1)$ 分类了所有固定 $\phi$ 的，$G_3$ 关于 $G_1$ 的 *extension* 的同构类. 这个交换群记作 $H^2(G_3,G_1)$.
9. 证明如果 $\phi$ 平凡，则 $G_1$ 在 $G_2$ 的中心里.
10. 假设 $G_1 = \mathbb{Z}$, $G_3 = C_p$ 是素数 $p$ 阶循环群, $\phi$ 平凡. 证明 $H^2(C_p,\mathbb{Z}) \cong C_p$ 并找到对应的 *extension*.

# 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 $\sigma'$ 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. $\sigma$ 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 $\sigma$ 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 $\sigma s_k$ 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.

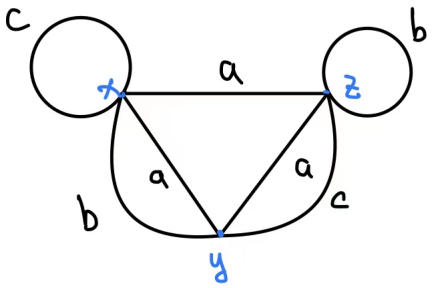
注记. 有限生成群的子群不一定有限生成. 例如考虑 $F(\{x, y\})$ 中 $x^n y x^{-n}$, $n \geq 1$ 生成的子群.

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)*

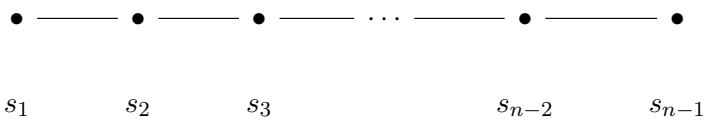
通过上述分析, 我们得到的有向图每个点都有进的 $a, b, c$-箭头, 也有出的 $a, b, c$-箭头, 从而 $G/H = \{x, y, z\}$, 即 $|G/H| = 3$. 且我们有群同态

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

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 $G$,*



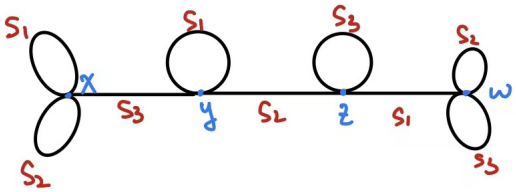

*其中* $G = \langle s_i \mid s_i^2 = e, (s_i s_{i+1})^3 = e, (s_i s_j)^2 = e \rangle$.

*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 $y = s_3 \cdot x$, $z = s_2 \cdot y$, $w = s_1 \cdot z$.

## 4.2 作业 4

**练习.** *Artin Chapter 7, 11.4*

**练习.** *Artin Chapter 7, 11.5*

**练习.** *Artin Chapter 7, 11.6* 任选一个小问做即可.

**练习.** 证明 $A_n$, $n \geq 5$ 是单群.

**练习.** *Prove that the map* $f\colon S_n \to \{\pm 1\}$ *defined by* $f(\sigma) = (-1)^{l(\sigma)}$ *is a group homomorphism. Identify this group homomorphism with the composition of injective homomorphism* $S_n \to GL(n, F)$ *and determinant* det.

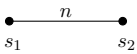
**练习.** 1. 请将长度最长的 $\omega \in S_n$ 写做基础对换的乘积.

2. 证明 $l(\sigma) = l(\sigma^{-1})$
3. 证明 $l(\sigma) + l(\sigma\omega) = \binom{n}{2}$

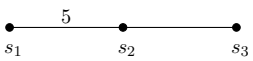
以下题目中 Coxeter diagram 定义的群是指由结点 $s_i$ 生成的群，满足如下关系

1. $s_i^2 = e$
2. $(s_i s_j)^2 = e$，如果 $s_i, s_j$ 之间没有连线
3. $(s_i s_j)^3 = e$，如果 $s_i, s_j$ 之间有连线，且线上没有数字
4. $(s_i s_j)^m = e$, 如果 $s_i, s_j$ 之间有连线，且线上有数字 $m$。

**练习.** 考虑二面体群 $D_n$, 证明这个群和以下 $I_2(n)$-*diagram* 定义的 *Coxeter* 群同构。即群 $D_n \cong \langle s_1, s_2 \mid s_1^2, s_2^2, (s_1 s_2)^n \rangle$.




**练习.** 考虑正十二面体的对称群。证明这个群和以下 $H_3$ *diagram* 定义出的 *Coxeter* 群同构。



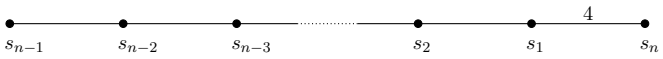

试找出对应的三个反射的法向量。

**练习** (Hyperoctahedral group). *(对* $n = 3$ *是必做题，对一般* $n$ *是选做题，可以不用写)* *The hypercube in* $\mathbb{R}^n$ *is defined as convex hull of* $2^n$ *points* $(\pm 1, \cdots, \pm 1)$ *in* $\mathbb{R}^n$. *Let* $W(B_n)$ *be the group of orthogonal transformations preserving this convex set, in other words, the symmetry group of the hypercube.*

1. *What is the order of $W(B_n)$?*
2. *Identify $W(B_n)$ with the following subgroup of $S_{2n}$. Let $-[n] = \{-1, -2, -3, \cdots, -n\}$. The subgroup consists of permutations of $-[n] \sqcup [n]$ such that $\sigma(-k) = -\sigma(k)$.*
3. *Prove that $W(B_n)$ is generated by $n$-elements of order two $s_n = (1, -1)$ and $s_i = (i, i+1)(-i, -i-1)$ for $1 \leq i \leq n-1$, and the minimal number of generators needed in the expression of $\sigma \in W(B_n)$ (similar as the number of inversions for permutation groups) is given by*

$$\#\{(i,j) \in [n] \times [n] | i < j, \sigma(i) > \sigma(j)\} + \#\{(i,j) \in [n] \times [n] | i \leq j, \sigma(-i) > \sigma(j)\} \quad (4.2.1)$$

4. *Prove that the generators in $s_i$ satisfy the Coxeter relations for type $B_n$ diagram.*




5. *Prove that the group given by generators $s_1, \cdots, s_n$ and relations in the type $B_n$ diagram is isomorphic to $W(B_n)$.*

**练习** (Free product and Ping-Pong lemma)**.**

**定义 4.2.1.** 自由积] 如果两个群 $G$ 和 $H$ 分别写成生成元和关系

$$G = \langle X \mid R \rangle, \quad H = \langle Y \mid S \rangle,$$

则 $G$ 和 $H$ 的自由积定义为 $G \star H = \langle X \sqcup Y \mid R \sqcup S \rangle$. 或者也可定义为 $G$ 和 $H$ 中元素组成的 words, 在定义 words 的乘法时类似于自由群的定义一样，额外加入 $G$ 和 $H$ 中的乘法来消去相邻两个来自同一个群的元素.

1. 证明 *Ping-Pong lemma.* 设 $G$ 有两个阶数不全为 2 的子群 $H_1$ 和 $H_2$, 且 $H_1$ 和 $H_2$ 生成群 $G$. 假设 $G$ 在集合 $A$ 上有作用，且存在 $A$ 的两个不相交的非空子集 $A_1$ 和 $A_2$，使得 $\forall h_1 \in H_1 \backslash \{e\}$, $h_1(A_2) \subset A_1$, $\forall h_2 \in H_2 \backslash \{e\}$, $h_2(A_1) \subset A_2$. 则 $G$ 同构于 $H_1 \star H_2$.
2. 证明由矩阵 $M_1 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ 和 $M_2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ 在 $SL(2, \mathbb{R})$ 中生成的子群同构于两个生成元的自由群. （提示：考虑 $\mathbb{R}^2$ 中子集 $\{(x, y) \mid |x| < |y|\}$ 以及 $\{(x, y) \mid |y| < |x|\}$）
3. 记 $SL(2, \mathbb{Z})$ 为行列式为 1 的 2 阶整数矩阵在矩阵乘法下组成的群, 定义 $PSL(2, \mathbb{Z})$ 为商群 $SL(2, \mathbb{Z})/\pm I$. 考虑元素 $M_3 = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$ 和 $M_4 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ 来证明 $PSL(2, \mathbb{Z})$ 同构于 $C_3 \star C_2$. *(提示：考虑 $PSL(2, \mathbb{Z})$ 在 $\mathbb{R}^2$ 中所有过原点的直线的集合上的作用, 分成斜率小于或等于零的部分以及其他。)*

**练习** (Affine Coxeter group, 选做题，可以不交)**.** 定义 $\tilde{S}_n$ 如下. 考虑 $V = \{(x_1 \cdots x_n) \in \mathbb{R}^n \mid \sum_i x_i = 0\}$. 则 $V_{\mathbb{Z}} = V \cap \mathbb{Z}^n$ 在向量的加法下组成一个群. 对于 $\sigma \in S_n$ 和 $v = (v_1, \cdots, v_n) \in V_{\mathbb{Z}}$. 考虑 $V$ 上由变换 $T(x_1, \cdots, x_n) = (x_{\sigma(1)}, \cdots, x_{\sigma(n)}) + v$. 由这些变换在复合下组成的群记做 $G$.

1. 证明形如 $T(x_1, \cdots, x_n) = (x_1, \cdots, x_n) + v$ 的元素构成了 $\tilde{S}_n$ 的一个同构于 $V_{\mathbb{Z}}$ 的正规子群. 形如 $T(x_1, \cdots, x_n) = (x_{\sigma(1)}, \cdots, x_{\sigma(n)})$ 的元素构成了 $\tilde{S}_n$ 的一个同构于 $S_n$ 的子群. 证明 $\tilde{S}_n$ 同构于 $V_{\mathbb{Z}}$ 和 $S_n$ 的半直积.

2. 利用以上同构，将 $S_n$ 的生成元 $s_1,\cdots,s_{n-1}$ 作为 $\tilde{S}_n$ 中的元素，令 $s_n$ 为如下变换 $s_n(x_1,\cdots,x_n)=(x_n+1,x_2\cdots,x_1-1)$. 证明 $s_1,\cdots,s_n$ 都是相对于某一仿射超平面的反射（不一定过原点），且是 $\tilde{S}_n$ 的生成元. 利用法向量夹角找到这些反射之间的关系并画出对应的 *Coxeter diagram*. 记对应的 *Coxeter* 群为 $G$.
3. 证明对题目中给出的元素 $T$ 写作以上生成元的最小个数为

$$l(T)=\sum_{\sigma(i)<\sigma(j)}|v_i-v_j|+\sum_{\sigma(i)>\sigma(j)}|v_i-v_j-1|.$$

4. 考虑 $n=3$ 和 $\tilde{S}_3$ 在 $V$ 上的作用. 证明 $V$ 中有非平凡的稳定化子的点组成的集合是 $V$ 上一些直线的并，且这些直线的补集是不相交的等边三角形. 如果有两个三角形落在一条直线的两边，则称这条直线将两个三角形分离. 取其中一个三角形 $\Delta$，证明 $l(T)$ 等于 $\Delta$ 与 $T(\Delta)$ 之间分离的直线的数目.
5. 对比 $\tilde{S}_3$ 在这些三角形所在的集合上的作用，以及 *Coxeter-Todd algorithm* 得到的 $G$ 在 $G$ 上的左乘作用，证明 $G$ 与 $\tilde{S}_3$ 同构.

# 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 $[G,G]$.

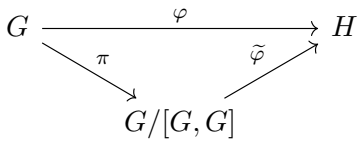
**命题 5.1.11.** 对于群 $G$ 来说, $[G,G]$ 是其正规子群.

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 $\varphi$ 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 作业 5.1

**练习** (Nilpotent groups)**.**

**定义 5.2.1.** Let $G_1 = G/C(G)$, and $G_{n+1} = G_n/C(G_n)$. We call a group $G$ unipotent if and only if $G_m$ has order 1 for some $m$.

1. *Prove that p-groups have nontrivial center and hence nilpotent.*
2. *Prove that a finite group is nilpotent if and only if it is the product of its Sylow subgroups.*
3. *Prove that if $G$ is nilpotent, then the subgroups and quotient groups of $G$ are also nilpotent.*
4. *Prove that the group $U$ consisting of $n \times n$ upper triangular matrices with elements in a ring $R$ and diagonal elements being 1 is nilpotent.*
5. *Prove that a finite group $G$ is nilpotent if and only if it is a isomorphic to a subgroup of $U$ for some $n$ and $R$.*
6. *Prove that if $G$ is nilpotent and $[G : G] = G$, then $G$ has only one element.*

**练习.** *Use the notation from homework 1, question 5. Prove the Bruhat decomposition.*

$$GL(n, F) = \sqcup_{w \in W} BwB. \tag{5.2.1}$$

**练习** (Parabolic subgroup of $PSL(n, F)$)**.** *Let $n \geq 3$ and $F$ a field. Denote by $G = SL(n, F)$ the group of matrices with determinant 1.*

1. *Let $B$ be the subgroup of $G$ consisting of upper triangular matrices, $T$ the subgroup of $G$ consisting of diagonal matrices, $N$ the subgroup consisting of matrices with exactly one nonzero element in each row and column. Prove that $T$ is a normal subgroup of $N$, when $|F| \geq 3$, then $N$ is the normalizer of $T$. Prove that $B$ and $N$ generates $G$.*
2. *Let $e_i$ be the column vector in $F^n$ with $i$-th component 1 and other components 0. Prove that the multiplication of matrices with vectors induces an group operation of $W = N/T$ on the set $\{Span(e_1), \cdots, Span(e_n)\}$. Identify $Span(e_i)$ with $i \in [n]$. Prove this action induces an isomorphism $f : N/T \to S_n$.*
3. *Fixing $w \in S_n$, let $\tilde{w} \in N$ be a representative in $f^{-1}(w)$. Prove that $\tilde{w}B$, $B\tilde{w}$ and $B\tilde{w}B$ do not depend on the choice of $\tilde{w}$. So we can denote by $BwB$ for $B\tilde{w}B$. Prove the following decomposition.*

$$G = \sqcup_{w \in W} BwB. \tag{5.2.2}$$

4. *Let $\{s_1, \cdots, s_{n-1}\}$ be the set of fundamental transpositions. Prove that $s_i$ are not in the normalizer of $B$ and $s_iBw \subset BwB \sqcup Bs_iwB$. In general, when $S_n$ is replaced by other Coxeter groups (not necessarily finite), such a structure is called a $(B, N)$-pair.*
5. *Let $\pi$ be a subset of fundamental transpositions $\{s_1, \cdots, s_{n-1}\}$. Let $W_\pi$ be the subgroup of $S_n$ generated by $\pi$. Prove that*

$$P_\pi = \sqcup_{w \in W_\pi} BwB$$

*is a subgroup of $G$.*

6. *Prove that any subgroup $P$ of $G$ containing $B$ is of the form $P_\pi$. We call them parabolic subgroups. (Hint: if $\tilde{\omega} = \tilde{s}_{i_1} \cdots \tilde{s}_{i_l} \in P$ with length $l(w) = l$, try to prove all $\tilde{s}_{i_j} \in P$. )*
7. *Count the number of parabolic subgroups.*

**练习** (Simplicity of $PSL(n, F)$)**.** *Following the notation in last question and assume $n \geq 3$. Let $U$ be the subgroup of $G$ consisting of upper triangular matrices with diagonal elements being 1. Prove that*

1. *Show that the center of $G$ is*
$$Z = \{\lambda I | \lambda^n = 1\}.$$
2. *$G$ is generated by conjugates of $U$.*
3. *$G = [G, G]$.*
4. *The intersection of conjugates of $B$ is the center of $G$.*
5. *Let $H$ be a normal subgroup of $G$, then either $H \subset Z$ or $HU = G$. (Hint: 1. Use the classification of parabolic groups. 2. Take a look at the proof in the class. 3. Prove that if $s_i \in HU$, then the nearby $s_j \in HU$.)*
6. *Let $H$ be a normal subgroup of $G$, then either $H \subset Z$ or $H = G$.*
7. *Prove that $PSL(n, F)$ is simple for $n \geq 3$.*

**练习.** *Let $V$ be a $n$-dimensional vector space over field $F$.*

**定义 5.2.2** (Flag)**.** A flag $F$ is defined to be a chain of subspaces
$$F : \{0\} = V_0 \subsetneq V_1 \subsetneq V_2 \cdots \subsetneq V_n = V$$
Denote by $FL$ the set of flags.

*Let $G = GL(V)$, and define an action of $G$ on the set of flags by*
$$g \cdot F \colon \{0\} = V_0 \subset g(V_1) \subset g(V_2) \cdots \subset V_n = V.$$

**定义 5.2.3** (Borel subgroup)**.** Let $F$ be a flag, the stablizer of $F$ is denoted by $B$ and called the Borel subgroup of $G$.

*Fixing a flag $F$ and the corresponding Borel subgroup $B$, prove that the linear action of $B$ on $V_i$ induces a linear action on quotient space $V_i/V_{i-1}$, or in other words, there is a group homomorphism*
$$B \to GL(V_n/V_{n-1}) \times GL(V_{n-1}/V_{n-2}) \cdots \times GL(V_1/V_0).$$

**定义 5.2.4** (Nilponent subgroup)**.** Define $U$ to be the kernel of the above homomorphism.

1. *Prove that the action of $G$ on $FL$ is transitive and hence the Borel subgroups are conjugate to each other.*
2. *Restrict the action of $G$ on $FL$ to $B$. Find a bijection between the set of $B$-orbits with $S_n$, and for each orbit corresponding to $\omega \in S_n$, find a bijection to $F^{l(\omega)}$.*

3. *Prove that $B$ is the normalizer of $U$ in $G$.*
4. *Prove that $U$ is a unipotent group.*
5. *Is it true that $U$ is the commutator subgroup of $B$?*
6. *Define a partial flag to be a chain of subspaces*

$$F : \{0\} = V_0 \subsetneq V_1 \subsetneq V_2 \cdots \subsetneq V_m = V.$$

*Find the relations between partial flags and parabolic subgroups.*

**练习.** *Let $F$ be a field. Find the derived subgroup or the commutator subgroup of $GL(n, F)$.*

## 5.3 十月十二日

**定义 5.3.1.** 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 5.3.2.** 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 5.3.3.** *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 5.3.4.** *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 5.3.5.** 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 5.3.6.** 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 5.3.7.** 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 5.3.8.** 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 5.3.9.** 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 5.3.10.** 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 5.3.11.** 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 5.3.12.** 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)*$e_s, s \in R$, 为

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

**命题 5.3.13** (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 $\Phi$:

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

□

**定义 5.3.14.** 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 5.3.15.** 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 5.3.16.** *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 5.3.17.** 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 5.3.18.** 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

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

**定义 5.3.19.** 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 5.3.20.** 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 $\pi$ 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

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

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 5.3.21** (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 5.3.22.** 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 5.3.23** (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.

## 5.4 作业 5.2

**练习.** ***Artin, Chapter 11, 1.7 (a)***

*Let $U$ be an arbitrary set and $R$ be the set of subsets in $U$. Addition and multiplication of elements of $R$ are defined by $A+B=A\cup B-A\cap B$ and $A\cdot B=A\cap B$. Prove that $R$ is a ring.*

**练习.** *Determine whether the division with reminder $g(x)=f(x)q(x)+r(x)$ exists in $R[x]$ for the following $R, f(x), g(x)$. If it exists, find the $q(x), r(x)$.*

1. $R=\mathbb{Z}, f(x)=2x^2+x+1, g(x)=2x^3+7x^2+4x+8$
2. $R=\mathbb{Z}/6\mathbb{Z}, f(x)=2x+1, g(x)=2x^2+2x$
3. $R=\mathbb{Z}/6\mathbb{Z}, f(x)=5x+1, g(x)=2x^2+2x$

**练习.** ***Artin, Chapter 11, 1.8***

*Determine the units in $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$.*

**练习.** *Let $R$ be a ring and $I$, $J$ ideals of $R$. Prove the following*

1. *$I\cap J$ is an ideal of $R$,*
2. *$I+J=\{a+b|a\in I, b\in J\}$ is an ideal of $R$,*
3. *$IJ=\{\sum_{i=0}^{n}a_ib_i|a_i\in I, b_i\in J, n\in\mathbb{Z}_{\geq 0}\}$ is an ideal of $R$.*

**练习.** ***Artin Chapter 11, 3.4*** *Let $\phi\colon \mathbb{C}[x,y]\to\mathbb{C}[t]$ defined by $x\mapsto t+1$ and $y\mapsto t^3-1$. Determine the kernel $K$ of $\phi$ and prove that every ideal $I$ of $\mathbb{C}[x,y]$ that contains $K$ can be generated by two elements.*

# 第六章　第六周

## 6.1　十月十八日

这里我们给出更多关于理想的例子.

**例子.** $\mathbb{Z}$ 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.** $\mathbb{C}[x]$ 中的所有的理想都是形如 $I=(f(x))$ 的主理想, 其中 $f(x)\in\mathbb{C}[x]$. 并且 $(f_1(x))=(f_2(x))$ 当且仅当存在 $g(x), h(x)\in\mathbb{C}[x]$ 使得

$$\begin{cases} f_1(x)=f_2(x)g(x) \\ f_2(x)=f_1(x)h(x) \end{cases}$$

从上式我们可以看出 $g(x), h(x)$ 实际上是非零的零次多项式. 因此 $\mathbb{C}[x]$ 中所有不同的理想都形如 $(f(x))$, 其中 $f(x)$ 是首一多项式.

**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.

**例子.** 考虑如下环同态:

$$\begin{aligned} \varphi:\mathbb{C}[x,y]&\to\mathbb{C}[t] \\ x&\mapsto t \\ y&\mapsto t^2 \end{aligned}$$

并且 $\varphi|_{\mathbb{C}}$ 是恒同映射. 下面我们来确定由这个映射的核决定的理想 $\operatorname{Ker}\varphi$. 首先我们注意到 $y-x^2\in\operatorname{Ker}\varphi$, 下面我们断言

$$\operatorname{Ker}\varphi=(y-x^2)$$

任取 $g(x,y)\in\mathbb{C}[x,y]$, 将其视作 $\mathbb{C}[x][y]$ 中的元素, 用 $y-x^2$ 去对其做带余除法我们有[1]

$$g(x,y)=(y-x^2)q(x,y)+r(x,y)$$

[1]这是可以进行的, 因为将 $y-x^2$ 视作 $\mathbb{C}[x][y]$ 中的元素, 其首项系数在 $\mathbb{C}[x]$ 中是单位.

其中 $r(x,y)$ 视作 $\mathbb{C}[x][y]$ 中元素的次数小于一, 这意味着 $r(x,y)=r(x)$. 假设 $g(x,y)\in\operatorname{Ker}\varphi$, 那么做带余除法之后得到的余式 $r(x)$ 也在 $\operatorname{Ker}\varphi$ 中, 并且由于 $r(x)$ 只和 $x$ 有关, 从而这意味着 $\varphi(r(x))=\varphi(t)=0$, 即 $r=0$, 从而 $g(x,y)=(y-x^2)q(x,y)$, 这就证明了我们的断言.

注记. 根据对应定理, 我们可以直接看出 $\mathbb{C}[x,y]$ 中包含 $(y-x^2)$ 的所有不同理想都形如 $(y-x^2,f(x))$, 其中 $f(x)$ 是 $\mathbb{C}[x]$ 中的首一多项式. 之后我们会考虑 $\mathbb{C}[x,y]$ 中所有的理想的样子.

**命题 6.1.1.** 给定环 $R$ 以及 $a,b\in R$, $\pi$ 为典范的商映射, 那么有

$$\begin{aligned}R/(a,b)&\cong\{R/(a)\}/(\pi(b))\\&\cong\{R/(b)\}/(\pi(a))\end{aligned}$$

注记. 给定环 $R$ 的一个理想 $I$, 上述命题有时可以给出确定商环 $R/I$ 结构的一个好办法.

**定义 6.1.2.** 高斯整数环 $\mathbb{Z}[i]$ 定义为

$$\mathbb{Z}[i]:=\{a+bi\mid a,b\in\mathbb{Z}\}$$

其中 $i$ 是纯虚数.

**例子.** 不难发现 $(i-2)$ 是 $\mathbb{Z}[i]$ 的一个理想, 下面我们来尝试说明 $\mathbb{Z}[i]/(i-2)$ 的结构. 首先我们断言

$$\mathbb{Z}[i]\cong\mathbb{Z}[x]/(x^2+1)$$

这个同构由如下的环同态给出

$$\begin{aligned}\varphi:\mathbb{Z}[x]&\to\mathbb{C}\\x&\mapsto i\end{aligned}$$

并且 $\varphi|_{\mathbb{C}}$ 是恒同. 因此

$$\begin{aligned}\mathbb{Z}[i]/(i-2)&\cong\mathbb{Z}[x]/(x^2+1,x-2)\\&\cong\{\mathbb{Z}[x]/(x-2)\}/(x^2+1+(x-2))\\&\cong\mathbb{Z}/(2^2+1)\\&\cong\mathbb{Z}/5\mathbb{Z}\end{aligned}$$

下面我们来考虑一种比较有趣的构造, 即如何在一个环 $R$ 中 “添加” 新的元素. 特别地, 考虑一个由 $R$ 上多项式决定的方程, 其在 $R$ 上没有根, 如何向 $R$ 中添加新的元素, 使得这个在更大的环中这个这个方程存在根.

**例子.** 给定域 $\mathbb{R}$ 上的一个多项式 $x^2+1$, 容易发现 $x^2+1=0$ 在 $\mathbb{R}$ 中没有根, 我们该如何去寻找一个更大的环 $R$, 使得 $\mathbb{R}$ 自然地嵌入在 $R$ 中, 并且使得 $x^2+1=0$ 在 $R$ 中有根呢? 显然 $\mathbb{C}$ 是我们的一个选择, 但是我们采取如下更一般的构造: 考虑如下自然的嵌入

$$\mathbb{R}\hookrightarrow\mathbb{R}[x]/(x^2+1)$$

那么显然 $x^2+1=0$ 在 $\mathbb{R}[x]/(x^2+1)$ 中存在根, 因为 $\overline{x}:=x+(x^2+1)\in\mathbb{R}[x]/(x^2+1)$ 满足 $(\overline{x})^2+1=\overline{0}\in\mathbb{R}[x]/(x^2+1)$. 实际上, 利用带余除法我们可以给出 $\mathbb{R}[x]/(x^2+1)$ 的更加显式的表达:

$$\mathbb{R}[x]/(x^2+1)=\{a+b\overline{x}\mid a,b\in\mathbb{R}\}$$

利用这种观点, 可以发现实际上我们构造的 $\mathbb{R}[x]/(x^2+1)$ 就是 $\mathbb{C}=\{a+bi\mid a,b\in\mathbb{C}\}$.

**例子.** 类似的, 考虑二元域 $\mathbb{F}_2$ 以及其上的多项式 $x^2+x+1$, 我们可以构造 $\mathbb{F}_2[x]/(x^2+x+1)$ 使得 $x^2+x+1=0$ 在其中存在根, 并且给出如下具体的表达

$$\{0,1,x,x+1\}$$

并且不难发现 $\mathbb{F}_2[x]/(x^2+x+1)$ 构成了一个四个元素的域.

**例子.** 实际上, 给定一般的环 $R$ 以及其上的首一多项式 $f(x)$, 我们都可以仿照上述的办法去找到一个更大的环 $R'$ 使得 $R$ 自然地嵌到 $R'$ 中, 并且 $f(x)$ 在 $R'$ 中存在一个根, 即考虑 $R'=R[x]/(f(x))$, 不难发现 $\overline{x}:=x+(f(x))\in R'$ 满足 $f(\overline{x})=\overline{0}\in R'$. 同样利用带余除法[2], 对于 $R'$ 我们有如下的一组 $R$ 基[3]:

$$1,\overline{x},\overline{x}^2,\ldots,\overline{x}^{n-1}$$

其中 $n=\deg f$.

注记. 如果 $f(x)$ 不是首一的, 我们通常得不到什么好的结果, 比如考虑一个糟糕的例子: 在 $R=\mathbb{Z}/6\mathbb{Z}$ 中考虑 $3x-1$, 你无法在 $R[x]/(3x-1)$ 中找到 $3x-1=0$ 的根.

一般来说, 我们通过上述操作得到的 $R[x]/(f(x))$ 不一定是一个域, 那么对于一个环 $R$ 来说, 什么时候商环 $R/I$ 会是一个域呢? 我们实际上有如下的判据:

**命题 6.1.3.** $F$ 是域当且仅当 $F$ 只有两个理想, 即 $(0)$ 和 $F$ 本身.

证明: 首先, 如果 $I$ 是 $F$ 的一个非零理想, 那么任取 $a\in I$, 我们有 $1=aa^{-1}\in I$, 即 $I=F$. 另一方面, 任取 $a\in F, a\neq 0$, 考虑 $(a)\subseteq F$, 由于 $F$ 只有两个理想, 且 $(a)\neq 0$, 那么 $(a)=F$, 从而存在 $b\in F$ 使得 $ab=1$, 即 $a$ 可逆. □

利用上面的判据, 以及在本节最初关于理想的刻画, 我们可以直接看出:

**例子.** $\mathbb{Z}/p\mathbb{Z}$ 是域, 其中 $p$ 是素数.

**例子.** $\mathbb{R}[x]/(x^2+1)$ 是域.

## 6.2 十月十九日

**定义 6.2.1.** 环 $R$ 的一个真理想 $I$ 被称为极大理想 (maximal ideal), 如果任何包含 $I$ 的理想都是 $R$.

为了说明极大理想总是存在的, 我们需要 Zorn 引理, 而为了陈述这个技术性的引理, 我们需要引入偏序集这个概念.

**定义 6.2.2.** 给定一个集合 $S$, 其上的一个偏序 (partial order)是一个关系 $R\subseteq S\times S$, 如果 $(a,b)\in R$, 我们记作 $a\leq b$, 并且 $R$ 满足

1. $a\leq a$;

[2]这里要求 $f$ 是首一的, 目的是为了能够进行带余除法.

[3]之后在学习模论的时候我们会更严格地定义这件事情, 在这里你可以仿照线性空间的基去理解, 即任取 $x\in R'$, 存在唯一的表达式 $x=a_1+a_2\overline{x}+\cdots+a_{n-1}\overline{x}^{n-1}$, 其中 $a_i\in R, i=1,2,\ldots,n-1$.

2. 如果 $a \leq b$ 并且 $b \leq a$, 那么 $a = b$;
3. 如果 $a \leq b$ 并且 $b \leq c$, 那么 $a \leq c$.

带有偏序关系的一个集合被称为偏序集 (partially ordered set).

**定义 6.2.3.** 偏序集 $S$ 的一个子集 $C$ 被称为一个链 (chain), 如果任取 $a, b \in C$, 我们有 $a \leq b$ 或者 $b \leq a$.

**定义 6.2.4.** 偏序集 $S$ 的一个链 $C$ 称为有上界, 如果存在 $c \in S$ 使得任意 $a \in C$ 都有 $a \leq c$

**引理 6.2.5** (Zorn 引理)**.** *如果偏序集 $S$ 的每一条链都有上界, 那么 $S$ 存在至少一个极大元.*

**命题 6.2.6.** *对于环 $R$ 来说, 极大理想总是存在的.*

*证明:* 考虑集合 $S$ 是由环 $R$ 所有真理想组成的集合, 显然 $S$ 非空, 并且包含关系是 $S$ 上的一个偏序关系. 为了证明极大理想的存在性, 根据 Zorn 引理只需要对每一条由真理想组成的链, 其都存在上界即可. 给定链 $C = \{I_i\}_{i \in I}$, 考虑 $\widetilde{I} = \bigcup_{i \in I} I_i$, 我们有如下事实:

1. $\widetilde{I}$ 是一个理想;
2. $\widetilde{I} \neq R$, 这是因为 $1 \notin \widetilde{I}$, 以及一个理想 $I = R$ 当且仅当 $1 \in I$.

从而 $\widetilde{I}$ 是 $C$ 的一个上界, 从而根据 Zorn 引理可知极大理想存在. □

**命题 6.2.7.** *$I$ 是 $R$ 的极大理想当且仅当 $R/I$ 是域.*

**例子.** 对于任意 $a \in \mathbb{C}$, 我们有 $(x - a) \subseteq \mathbb{C}[x]$ 是一个极大理想. 这个事实可以通过考虑如下映射来得到

$$e_a : \mathbb{C}[x] \to \mathbb{C}$$
$$p(t) \mapsto p(a)$$

实际上你不难验证 $\mathbb{C}[x]$ 的所有极大理想都是形如 $(x - a), a \in \mathbb{C}$ 的样子, 即在集合上有如下的一一对应:

$$\{\mathbb{C}[x]\text{的所有极大理想}\} \overset{1-1}{\Longleftrightarrow} \mathbb{C}$$

**例子.** 考虑实值连续函数环 $R = C((a, b), \mathbb{R})$, 其中 $(a, b)$ 是开区间, 不难发现任取 $a \in \mathbb{R}$, 如下集合构成了 $R$ 的一个极大理想

$$I_a = \{f \in R \mid f(a) = 0\}$$

**问题 6.2.8.** $C((a, b), \mathbb{R})$ 的所有极大理想都是形如 $I_a$ 的样子吗? 如果换成闭区间 $[a, b]$ 呢?

**例子.** 更一般的, 我们有如下的一一对应

$$\{\mathbb{C}[x, y]\text{的所有极大理想}\} \overset{1-1}{\Longleftrightarrow} \mathbb{C}^2$$

这是一个更加困难的事实, 被称为希尔伯特零点定理 *(Hilbert's Nullstellensatz)*. 如果承认这个事实, 回顾我们之前的一个例子, 环同态

$$\varphi : \mathbb{C}[x, y] \to \mathbb{C}[t]$$
$$x \mapsto t$$
$$y \mapsto t^2$$

给出了同构 $\mathbb{C}[x,y]/(x-y^2)\cong\mathbb{C}[t]$, 从而有如下的一一对应

$$\{\mathbb{C}[x,y]/(x-y^2)\text{的所有极大理想}\}\overset{1-1}{\Longleftrightarrow}\{\mathbb{C}[t]\text{的所有极大理想}\}$$

并且根据对应我们知道 $\mathbb{C}[t]$ 的极大理想 $(t-a)$ 会对应到 $\mathbb{C}[x,y]/(x-y^2)$ 中的极大理想 $(x-a,y-a^2)$, 从而 $\mathbb{C}[x,y]/(x-y^2)$ 的极大理想与 $\mathbb{C}^2$ 中的一条抛物线上的点一一对应. 这意味着去研究 $\mathbb{C}^2$ 中的一条曲线与研究 $\mathbb{C}[x,y]/(x-y^2)$ 的极大理想在某些程度上是一样的, 这也是代数几何的最初的想法.

对于希尔伯特零点定理, 会在之后的内容中给出证明, 现在我们将内容转向另一些特殊的理想.

**定义 6.2.9.** 环 $R$ 被称为整环 (domain), 如果对于任意 $a,b\in R$ 满足 $ab=0$, 那么 $a$ 和 $b$ 中至少有一个为 0.

**定义 6.2.10.** 环 $R$ 的理想 $I$ 被称为素理想 (prime ideal), 如果对任意 $a,b\neq I$, 一定有 $ab\neq I$.

**命题 6.2.11.** *对于环 $R$ 的理想 $I$, $R/I$ 是整环当且仅当 $I$ 是素理想.*

*证明:* 根据定义直接验证. □

**命题 6.2.12.** *极大理想一定是素理想*

*证明:* 注意到域一定是整环. □

当环 $R$ 是整环时, 我们有着相对良好的分解性质, 并且有些时候这种分解是非常重要的. 因此在本节接下来的内容中我们主要研究这件性质.

**例子.** *$\sqrt{2}$ 是无理数: 假设 $\sqrt{2}$ 不是无理数, 那么存在互素整数 $p,q$ 使得 $\sqrt{2}q=p$, 即 $2q^2=p^2$. 由于 $p,q$ 互素从而根据整数的唯一分解性质有 $2\mid p$, 不妨假设 $p=2m$, 从而有 $q^2=2m^2$, 即 $2\mid q$, 进而 $2\mid\gcd(p,q)=1$, 矛盾.*

为了后续的需要, 我们来固定一些术语以及列出一些简单的事实, 其中涉及到的所有的元素都是在整环 $R$ 中的:

1. $u$ 是单位当且仅当 $(u)=R$;
2. $a$ 整除 $b$[4]当且仅当 $(b)\subseteq(a)$;
3. $a$ 是 $b$ 的真因子[5]当且仅当 $(b)\subsetneq(a)\subsetneq R$;
4. $a$ 和 $b$ 相伴[6]当且仅当 $(a)=(b)$;
5. $a\neq0$, $a$ 不可约[7]当且仅当 $(a)\subseteq R$ 并且不存在主理想 $(c)$ 使得 $(a)\subsetneq(c)\subsetneq R$;
6. $p$ 是素元[8]当且仅当 $(p)$ 是素理想.

[4]即存在 $c$ 使得 $b=ac$

[5]即 $a$ 不是单位, 并且存在非单位的 $c$ 使得 $b=ac$

[6]即存在某些单位 $c$ 使得 $a=bc$

[7]即 $a$ 不是单位并且 $a$ 没有真因子

[8]$p$ 如果整除 $ab$, 那么 $p$ 整除 $a$ 或 $p$ 整除 $b$

**定义 6.2.13.** 整环 $R$ 被称为主理想整环 (principal ideal domain), 如果 $R$ 的每一个理想都是主理想.

**定义 6.2.14.** 整环 $R$ 被称为欧几里得整环 (Euclidean domain), 如果存在函数 $\sigma : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ 使得任取 $a, b \in R, b \neq 0$, 存在 $q, r \in R$ 使得

$$a = bq + r$$

其中 $r = 0$ 或 $\sigma(r) < \sigma(b)$.

**命题 6.2.15.** 欧几里得整环是主理想整环.

**例子.** $\mathbb{Z}[i]$ 是欧几里得环, 其中 $\sigma(a+bi) = |a+bi|^2$. 考虑 $z_1 = a+bi, z_2 = c+di$, 其中 $a \neq 0, b \neq 0$. 如果想要写成

$$z_2 = z_1 q + r, \quad r \neq 0$$

的形式, 并且满足 $\sigma(r) < \sigma(z_2)$, 我们可以感觉到应该选 $q$ 尽可能的接近 $z_1/z_2$. 我们先如下计算

$$\frac{z_1}{z_2} = (c+di)\frac{a-bi}{a^2+b^2} = m + ni, \quad m, n \in \mathbb{Q}$$

选取 $m_0, n_0 \in \mathbb{Z}$ 使得

$$\begin{cases} |m - m_0| \leq \frac{1}{2} \\ |n - n_0| \leq \frac{1}{2} \end{cases}$$

我们记 $q = m_0 + n_0 i$, 那么

$$q - \frac{z_2}{z_1} = (m_0 - m) + (n_0 - n)i$$

并且满足

$$|q - \frac{z_2}{z_1}|^2 = (m_0 - m)^2 + (n - n_0)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$$

因此

$$|r|^2 = |z_2 - q z_1|^2 = |z_1(\frac{z_2}{z_1} - q)|^2 < |z_1|^2$$

从而 $z_2 = q z_1 + r$ 满足 $\sigma(r) < \sigma(z_1)$.

## 6.3 作业 6

**练习.** *Prove there is a unique ring homomorphism $\phi\colon \mathbb{Z} \to R$. Assume $\ker\phi = (m)$ with $m \geq 0$. Then $m$ is called the characteristic of $R$. Prove that the characteristic of an integral domain must be a prime number. Prove that the number of elements in a finite field must be a power of its characteristic.*

**练习** (Formal power series)**.** *Let $F$ be a field. Define $F[[x]]$ to be the set of formal power series $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ with $a_i \in F$. The ring structure on $F[[x]]$ is defined similarly as ring of polynomials.*

1. *Prove that $F[[x]]$ is a Euclidean domain with size function $\sigma(f) = i$ being the smallest degree of $x^i$ with nonzero coefficient $a_i$.*

2. *Find the units in* $F[[x]]$.
3. *Artin Chapter 11, 3.10, Determine all ideals of the ring* $F[[t]]$ *of formal power series with coefficients in a field* $F$ *(see exerercise 2.2).*
4. *Define* $F((x))$ *to be the set of Laurent series* $f(x) = \sum_{i \geq n} a_i x^i$ *where* $n$ *varies in* $\mathbb{Z}$. *For exerample* $f(x) = -x^{-2} + x^{-1} + 1 + x + x^2 + x^3 + \cdots x^n + \cdots$. *The ring structure on* $F((x))$ *is defined similarly as polynomials. Prove that* $F((x))$ *is a field.*

**练习** (Artin Chapter 11, 3.8)**.** *Let* $R$ *be a ring of prime characteristic* $p$. *Prove that the map* $R \to R$ *defined by* $x \rightsquigarrow x^p$ *is a ring homomorphism. (It is called the Frobenius map.)*

**练习** (Artin Chapter 11, 3.9)**.**
1. *An element* $x$ *of a ring* $R$ *is called nilpotent if some power is zero. Prove that if* $x$ *is nilpotent, then* $1 + x$ *is a unit.*
2. *Suppose that* $R$ *has prime characteristic* $p \neq 0$. *Prove that if* $a$ *is nilpotent then* $1 + a$ *is unipotent, that is, some power of* $1 + a$ *is equal to* $1$.

**练习** (Fractions)**.** *Let* $R$ *be an integral domain. Consider a set* $X = \{(a, b) | a, b \in R, b \neq 0\}$. *Define a relation on* $X$ *by* $(a, b) \sim (c, d)$ *if and only if* $ad = bc$.
1. *Prove that this is an equivalence relation.*
2. *Denote by* $\frac{a}{b}$ *the equivalence class containing* $(a, b)$ *and it is called a fraction. The set of fractions is denoted by* $Frac(R)$ *and there is a map* $f \colon R \to Frac(R)$ *defined by* $a \mapsto \frac{a}{1}$. *Try to define a field structure on* $F$ *such that the map* $f$ *is an injective ring homomorphism. This is called the fraction field of* $R$.
3. *Prove that if there is an injective ring homomorphism* $R \to F$ *with* $F$ *being a field. Then this homomorphism factors through* $R \to Frac(R) \to F$.
4. *Let* $F$ *be a field. Prove that* $Frac(F[[x]])$ *is isomorphic to* $F((x))$.

**练习** (Artin Chapter 11, 4.3)**.** *Try to identify the following rings with forms you think simpler.*
1. $\mathbb{Z}[x]/\left(x^2 - 3, 2x + 4\right)$,
2. $\mathbb{Z}[i]/(2 + i)$,
3. $\mathbb{Z}[x]/(6, 2x - 1)$
4. $\mathbb{Z}[x]/\left(2x^2 - 4, 4x - 5\right)$
5. $\mathbb{Z}[x]/\left(x^2 + 3, 5\right)$.

**练习.** *Classify all the maximal ideals and prime ideals of* $\mathbb{R}[x]$.

**练习.** *Prove that the ring* $\mathbb{Z}[\omega]$ *is a Euclidean domain. Here* $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$.

**练习.** *Prove that the ring* $\mathbb{Z}[\sqrt{-2}]$ *is a Euclidean domain, hence PID.*

**练习.** *Prove that* $\mathbb{C}[x, y]$ *is not a PID.*

**练习** (Product ring)**.** *Let* $R$ *and* $R'$ *be rings. There is a ring structure on the product* $R \times R'$ *defined by* $(a, a') + (b, b') = (a + b, a' + b')$ *and* $(a, a')(b, b') = (ab, a'b')$. *This is called the product ring* $R \times R'$.

1. *What is the multiplicative identity in product ring $R \times R'$?*
2. *An idempotent element $e$ of a ring $S$ is an element in $S$ such that $e^2 = e$. Prove that the principal ideal $(e)$ is itself a ring with identity element $e$.*
3. *If $e$ is an idempotent element, then $1 - e$ is also an idempotent element.*
4. *Prove that $(1, 0) \in R \times R'$ is an idempotent element.*
5. *If $e$ is an idempotent element, Prove that $S$ is isomorphic to the the product ring $(e) \times (1-e)$.*
6. *Prove that there is a bijection between the set of prime ideals in $R \times R'$ and disjoint union of prime ideals in $R$ and prime ideals in $R'$.*

**练习.** ***Artin, Chapter 11, 6.8*** *Let $I$ and $J$ be ideals of a ring $R$ such that $I + J = R$.*

1. *Prove that $IJ = I \cap J$.*
2. *Prove the Chinese Remainder Theorem: For any pair $a, b$ of elements of $R$, there is an element $x$ such that $x \equiv a \mod I$ and $x \equiv b \mod J$. (Here the notation $x \equiv a \mod I$ means $x - a \in I$.*
3. *Prove that if $IJ = 0$, then $R$ is isomorphic to the product ring $R/I \times R/J$. (Hint: consider the natural homomorphism from $R \to R/I \times R/J$.*
4. *Describe the idempotents corresponding to the product decomposition in $(c)$.*

**练习.** ***Artin Chapter 11, 5.1*** *Let $f = x^4 + x^3 + x^2 + x + 1$ and let $\alpha$ denote the residue of $x$ in the ring $R = \mathbb{Z}[x]/(f)$. exerpress $(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1)$ in terms of the basis $(1, \alpha, \alpha^2, \alpha^3)$ of $R$.*

**练习.** *Use $Hibert's Nullstellensatz$ to determine all the maximal ideals in $\mathbb{C}[x, y]/(xy)$.*

**练习.** *Let $\mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} | m, n \in \mathbb{Z}\}$. Is $(\sqrt{-3} + 2)$ a maximal ideal in $\mathbb{Z}[\sqrt{-3}]$? Why?*

**练习.** ***Artin Chapter 11, 8.3*** *Prove that $\mathbb{F}_2[x]/(x^3 + x + 1)$ is a field, but $\mathbb{F}_3[x]/(x^3 + x + 1)$ is not a field.*

**练习** (Artin Chapter 11, 9.13)**.** *Let $\psi \colon \mathbb{C}[x, y] \to \mathbb{C}[t]$ be a homomorphism that is identity on $\mathbb{C}$ and sends $x \mapsto x(t)$, $y \mapsto y(t)$ such that $x(t)$ and $y(t)$ are not both constant. Prove that kernel of $\psi$ is principal ideal.*

**练习** (Artin Chapter 11, M.7)**.** *Let $X$ denote the closed unit interval $[0, 1]$, and let $R$ be the ring of continuous functions $X \to \mathbb{R}$.*

1. *Let $f_1, \ldots, f_n$ be functions with no common zero on $X$. Prove that the ideal generated by these functions is the unit ideal. Hint: Consider $f_1^2 + \cdots + f_n^2$.*
2. *Establish a bijective correspondence between maximal ideals of $R$ and points on the interval.*

# 第七章　第七周

## 7.1　十月二十五

上一次我们介绍了主理想整环以及欧几里得整环, 这次我们要再介绍一种新的环: 唯一分解整环, 并介绍他们之间的关系.

给定整环 $R$, 以及非单位 $a \in R\backslash\{0\}$, 如果 $a$ 不是不可约的, 那么 $a$ 可以写成 $a = a_1a_2$, 其中 $a_1, a_2$ 都不是单位. 如果 $a_1, a_2$ 中存在不是不可约的, 那么对其再进行类似的分解. 我们重复上述操作, 如果在有限次操作停止, 即得到的所有因子都是不可约的, 那么我们将 $a$ 写成如下形式

$$a = a_1 \dots a_n$$

其中 $a_1, \dots, a_n$ 是 $R$ 中的不可约的元素. 此时我们称对 $a$ 的分解终止 (factorization terminates), 并称 $a_1 \dots a_n$ 是 $a$ 的一个不可约分解. 如果 $a$ 有两个不可约分解

$$\begin{aligned} a &= p_1 \dots p_m \\ &= q_1 \dots q_n \end{aligned}$$

这两个不可约分解被称为相同的, 如果 $m = n$, 并且经过合适的顺序排列之后有 $(p_i) = (q_i)$.

**例子.** *在高斯整数环 $\mathbb{Z}[i]$ 中, 对 5 有如下分解*

$$\begin{aligned} 5 &= (1 + 2i)(1 - 2i) \\ &= (2 + i)(2 - i) \end{aligned}$$

*但是这两个分解是相同的, 因为 $(1 + 2i)i = (i - 2)$, 以及 $i$ 是 $\mathbb{Z}[i]$ 的单位.*

**定义 7.1.1.** 整环 $R$ 被称为唯一分解整环 (unique factorization ring), 如果任取非单位 $a \in R\backslash\{0\}$, 如果对 $a$ 的分解终止, 并且得到的任何两个不可约分解是相同的.

**引理 7.1.2.** *在整环 $R$ 中, 任何素元都是不可约元.*

*证明:* 回忆:

1. $p$ 是素元, 如果 $p \mid ab$ 可以推出 $p \mid a$ 或 $p \mid b$.
2. $p$ 是不可约元, 如果 $p = ab$ 意味着 $a$ 或 $b$ 中一定有一个是单位.

下面我们来证明在整环中素元都是不可约元: 假设 $p$ 是素元, 并且 $p = ab$, 那么不妨假设 $p \mid a$, 即 $a = pc$, 从而 $p = pcb$, 这意味着 $bc = 1$(这里用到了整环的性质), 从而 $b$ 是单位, 即 $p$ 是不可约元. □

**引理 7.1.3.** *在主理想整环 $R$ 中, 任何不可约元都是素元*

*证明:* 假设 $p$ 不可约的, 从而不存在主理想 $(c)$ 使得

$$(p) \subsetneq (c) \subsetneq (1)$$

这意味着 $(p)$ 是极大理想, 因为 $R$ 是主理想整环, 从而 $(p)$ 是一个素理想, 这意味着 $p$ 是素元. □

**引理 7.1.4.** *给定整环 $R$, 以及如下两条等价:*

1. *对任意非单位 $a \in R\backslash\{0\}$ 的分解终止;*
2. *$R$ 不存在无穷严格上升的主理想链*

$$(a_1) \subsetneq (a_2) \subsetneq \dots$$

*证明:* 对非单位 $a_1 \in R\backslash\{0\}$ 进行不可约分解

$$\begin{aligned} a_1 &= a_2 b_2 \\ &= a_2 a_3 b_3 \\ &= a_2 a_3 a_4 \dots \end{aligned}$$

我们可以得到一个严格上升的主理想链

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$$

从这里可以观察出 (1) 与 (2) 的等价性. □

**命题 7.1.5.** *给定整环 $R$,*

1. *如果在 $R$ 中对任何元素的分解都终止, 那么 $R$ 是唯一分解整环当且仅当每个不可约元都是素元;*
2. *主理想整环是唯一分解整环.*

*证明:* (1). 我们先假设每个不可约元都是素元: 任取非单位 $a \in R\backslash\{0\}$, 有如下两个不可约分解

$$\begin{aligned} a &= p_1 \dots p_m \\ &= q_1 \dots q_n \end{aligned}$$

那么 $p_1$ 是素元, 并且 $p_1 \mid q_1 \dots q_n$, 从而 $p_1 \mid q_i, 1 \le i \le n$, 然而 $q_i$ 是不可约的, 从而 $p_1$ 和 $q_i$ 是相伴的. 经过合适的顺序调整以及系数条件, 我们不妨假设 $p_1 = q_1$, 从而有

$$q_2 \dots q_n = p_2 \dots p_m$$

利用归纳法即可证明 $m = n$ 并且这两个分解是相同的, 从而 $R$ 是唯一分解整环. 另一方面, 我们假设 $R$ 是唯一分解整环, 取 $a$ 是一个不可约元, 假设 $a \mid bc$, 不妨写作 $ad = bc$, 对 $b, c, d$ 进行唯一分解, 即

$$\begin{aligned} b &= p_1 \dots p_m \\ c &= q_1 \dots q_n \\ d &= r_1 \dots r_s \end{aligned}$$

那么由于唯一分解性, $a$ 一定相伴于某个 $p_i$ 或者 $q_j$, 即 $a \mid b$ 或 $a \mid c$.

(2). 由于在主理想整环中所有不可约元都是素元, 从而只需要证明任取非单位 $a \in R\backslash\{0\}$, 对 $a$ 的分解终止即可, 根据之前的引理可知只需要证明任何严格包含的主理想链都会稳定即可, 考虑

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$$

考虑 $I = \bigcup_{i=1}^{\infty}(a_i)$, 由于 $R$ 是主理想整环从而 $I = (a_j)$ 对某个 $j$ 成立, 这意味着严格升链是有限长的. □

**例子.** 高斯整数环 $\mathbb{Z}[i]$ 是欧几里得整环, 从而是主理想整环, 从而是唯一分解整环.

**例子.** $\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环: 考虑 6 我们有如下分解

$$\begin{aligned} 6 &= 2 \times 3 \\ &= (1+\sqrt{-5})(1-\sqrt{-5}) \end{aligned}$$

**定义 7.1.6.** 给定整环 $R$ 以及 $a, b \in R$, 如果存在 $d \in R, d \mid a, d \mid b$ 满足对任意 $c \mid a, c \mid b$ 有 $c \mid d$, 那么称 $d$ 是 $a, b$ 的最大公因数, 记做 $\gcd(a, b)$.

注记. 在一般的整环 $R$ 中最大公因数不一定存在, 但是在唯一分解整环中最大公因数总是存在的: 将 $a, b$ 做唯一分解

$$\begin{aligned} a &= p_1^{r_1} \dots p_s^{r_s} \\ b &= p_1^{t_1} \dots p_s^{t_s} \end{aligned}$$

其中 $r_i, t_j \geq 0$. 不难发现最大公因子 $d$ 为 $d = p_1^{\min\{r_1,t_1\}} \dots p_s^{\min\{r_s,t_s\}}$.

我们来考虑多项式版本的费马大定理:

**命题 7.1.7.** 假设 $f(x), g(x), h(x) \in \mathbb{C}[x]$, 则当 $n \geq 3$ 时

$$f^n + g^n = h^n$$

不存在解满足 $\deg f \geq 1$ 并且 $\gcd(f, g) = 1$.

证明: 假设存在解, 我们不妨假设 $(f, g, h)$ 是满足 $\deg f + \deg g + \deg h$ 最小的解. 那么

$$\begin{aligned} f^n &= h^n - g^n \\ &= \prod_{k=0}^{n-1}(h - \xi^k g) \end{aligned}$$

其中 $\xi = e^{\frac{2\pi i}{n}}$. 那么 $\gcd(h, g) = 1$ 意味着 $\gcd(h - \xi_k g, h - \xi_l g) = 1$, 其中 $k \neq l$. 由于 $\mathbb{C}[t]$ 是唯一分解整环, 那么

$$\begin{aligned} h - g &= (x(t))^n \\ h - \xi g &= (y(t))^n \\ h - \xi^2 g &= (z(t))^n \end{aligned}$$

并且由于 $n \geq 3$ 我们知道 $1, \xi, \xi^2$ 互不相同. 从而有

$$a(x(t))^n + b(y(t))^n = c(z(t))^n$$

其中 $a, b, c \neq 0$, 从而得到了一个次数更小的解, 相矛盾. □

## 7.2 十月二十六

一般来说, $R$ 是主理想整环, 但 $R[x]$ 不一定是主理想整环, 例如考虑 $\mathbb{Z}[x]$ 的理想 $(2,x)$. 现在的目标是想要证明如果 $R$ 是唯一分解整环, 那么 $R[x]$ 也是唯一分解整环. 我们以 $\mathbb{Z}[x]$ 为例去说明这件事情. 我们将用如下的两个同态去分析 $\mathbb{Z}[x]$:

$$\mathbb{Z}[x] \hookrightarrow \mathbb{Q}[x]$$
$$\varphi_p : \mathbb{Z}[x] \to \mathbb{Z}/(p)[x] \cong \mathbb{F}_p[x]$$

其中 $p$ 是素数.

**定义 7.2.1.** $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x], a_n \neq 0, n \geq 1$ 被称为本元多项式 (primitive polynomial), 如果

$$\gcd(a_n, \ldots, a_0) = 1$$

**例子.** $f(x) = 2x^2 + 2x + 3$ 是本元多项式, $g(x) = 2x^2 + 4x + 6$ 不是本元多项式.

**引理 7.2.2.** *给定素数 $p$, 如下条件等价*

1. $p \mid a_i, 1 \leq i \leq n$
2. $p \mid f$
3. $\varphi_p(f) = 0$

**引理 7.2.3.** *如下条件等价*

1. *$f$ 是本元多项式;*
2. *对任意素数 $p$ 有 $p \nmid f$;*
3. *对任意素数 $p$ 有 $\varphi_p(f) \neq 0$.*

**引理 7.2.4.** *整数 $p$ 在 $\mathbb{Z}[x]$ 中是素元当且仅当 $p$ 是素数.*

*证明:* 注意到

$$\mathbb{Z}[x]/(p) \cong \mathbb{Z}/(p)[x]$$

□

**引理 7.2.5** (高斯引理)**.** *$f, g \in \mathbb{Z}[x]$ 是本元多项式当且仅当 $fg$ 是本元多项式.*

*证明:* $f, g$ 是本元多项式, 等价于对每个素数 $p$ 有 $\varphi_p(f) \neq 0, \varphi_p(g) \neq 0$, 同样地, $fg$ 是本元多项式等价于 $\varphi_p(fg) \neq 0$. 注意到 $\varphi_p(fg) = \varphi_p(f)\varphi_p(g)$, 从而 $f, g$ 是本元多项式当且仅当 $fg$ 是本元多项式, 因为 $\mathbb{F}_p[x]$ 是整环. □

**引理 7.2.6.** *任取 $f \in \mathbb{Q}[x]$, 存在分解 $f = cf_0(x)$, 其中 $c \in \mathbb{Q}, f_0(x) \in \mathbb{Z}[x]$ 是本元多项式, 并且 $f_0(x)$ 在相差 $\pm 1$ 的意义下是唯一的. 特别地, 当 $f \in \mathbb{Z}[x]$ 时, $c \in \mathbb{Z}$.*

*证明:* 存在性: 首先存在 $m \in \mathbb{Z}\backslash\{0\}$ 使得 $mf(x) \in \mathbb{Z}[x]$, 取 $d$ 是 $mf(x)$ 系数的最大公因数, 那么不难发现 $f_0(x) = \frac{m}{d} f(x)$ 是本元多项式, 并且 $c = \frac{d}{m}$. 特别地, 当 $f \in \mathbb{Z}[x]$ 时, $m = 1$, 从而 $c \in \mathbb{Z}$.

唯一性：假设有

$$f(x) = c_0 f_0(x) = \widetilde{c}\widetilde{f_0}(x)$$

那么存在 $m \in \mathbb{Z}\backslash\{0\}$ 使得

$$mf(x) = mcf_0 = m\widetilde{c}\widetilde{f_0}$$

其中 $mc, m\widetilde{c} \in \mathbb{Z}$. 任取素数 $p \mid mc$, 那么 $p \mid mf(x)$, 从而 $p \mid m\widetilde{c}$, 从而对 $mc$ 不可约因子个数的归纳可以得到 $f_0$ 在和 $\widetilde{f_0}$ 相差 $\pm 1$ 的意义下相同 □

注记. 在一般的环 $R$ 中, $f_0$ 和 $\widetilde{f_0}$ 在相差环 $R$ 中的单位的意义下相同.

**定理 7.2.7.** *有如下结果:*

1. *$f_0$ 在 $\mathbb{Z}[x]$ 中是本元多项式, $g \in \mathbb{Z}[x]$, 如果在 $\mathbb{Q}[x]$ 中 $f_0 \mid g$, 那么在 $\mathbb{Z}[x]$ 中 $f_0 \mid g$;*
2. *如果 $f, g$ 是本元多项式, $f, g$ 在 $\mathbb{Q}[x]$ 中有最大公因子, 那么在 $\mathbb{Z}[x]$ 中也有最大公因子.*

*证明:* (1). 假设 $g = f_0 h$, 其中 $h \in \mathbb{Q}[x]$. 假设

$$h = ch_0$$
$$g = c'g_0$$

其中 $c \in \mathbb{Q}, c' \in \mathbb{Z}$ 以及 $h_0, g_0$ 是本元多项式. 根据高斯引理有 $h_0 f_0$ 是本元多项式, 从而 $c$ 和 $c'$ 之间只相差 $\pm 1$, 从而 $c \in \mathbb{Z}$, 从而 $h \in \mathbb{Z}[x]$, 即在 $\mathbb{Z}[x]$ 中 $f_0 \mid g$.

(2). 如果在 $\mathbb{Q}[x]$ 中 $h \mid f, h \mid g$, 那么将 $h$ 写成 $h = ch_0$, 其中 $h_0$ 是本元多项式, 从而在 $\mathbb{Q}[x]$ 中 $h_0 \mid f, h_0 \mid g$, 那么在 $\mathbb{Z}[x]$ 中 $h_0 \mid f, h_0 \mid g$, 从而 $f, g$ 在 $\mathbb{Z}[x]$ 中也有最大公因子. □

**定理 7.2.8.** *如果 $f(x)$ 是 $\mathbb{Z}[x]$ 上的不可约元, 那么 $f(x)$ 只有如下两种可能:*

1. *$f(x)$ 是 $\mathbb{Z}$ 中的素数;*
2. *$f(x)$ 是 $\mathbb{Q}[x]$ 上的不可约元.*

*证明:* 如果 $\deg f = 0$, 那么此时 $f \in \mathbb{Z}$, 从而是 $\mathbb{Z}$ 中的素元; 如果 $\deg f \geq 1$, 不妨记 $f = cf_0$, 由于本元多项式在 $\mathbb{Z}[x]$ 上的不可约性与在 $\mathbb{Q}[x]$ 上的不可约性是一样的, 从而 $f_0$ 是 $\mathbb{Q}[x]$ 上的不可约元, 即 $f$ 也是 $\mathbb{Q}[x]$ 上的不可约元. □

**定理 7.2.9.** *$\mathbb{Z}[x]$ 中的每个不可约元都是素元.*

**定理 7.2.10.** *$\mathbb{Z}[x]$ 是唯一分解整环.*

*证明:* 任取 $f \in \mathbb{Z}[x]$, 将其写作 $f = cf_0$, 其中 $c \in \mathbb{Z}, f_0$ 是本元多项式. 对于 $c$ 我们有如下不可约分解

$$c_0 = c_1 c_2 \dots c_p$$

而对于 $f_0$ 我们在 $\mathbb{Q}[x]$ 中有如下不可约分解

$$f_0 = g_1 g_2 \dots g_k$$

其中 $g_i$ 都是本元的, 从而这也是 $\mathbb{Z}[x]$ 中的分解. □

**推论 7.2.11.** *$\mathbb{Z}[x_1, \dots, x_n]$ 是唯一分解整环.*

注记. 将 $\mathbb{Z}$ 换成一般的唯一分解整环, $\mathbb{Q}$ 换成 $R$ 的分式域, 我们上述的论述依然成立, 即对一般的唯一分解整环 $R$, 依然有 $R[x_1,\dots,x_n]$ 是唯一分解整环.

**命题 7.2.12.** $f(x)\in\mathbb{Z}[x], f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$, $p\nmid a_n$. 如果 $\varphi_p(f(x))=\overline{f}(x)$ 在 $\mathbb{F}_p[x]$ 中不可约, 那么 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

证明: 假设 $f(x)$ 可约, 那么 $f(x)=g(x)h(x)$, 其中 □

**例子.** $f(x)=x^3+x+1$, 则通过直接列出 $\mathbb{F}_2[x]$ 中的不可约多项式不难发现 $\overline{f}(x)$ 在 $\mathbb{F}_2[x]$ 中不可约.

**命题 7.2.13** (艾森斯坦判别法)**.** $f(x)\in\mathbb{Z}[x]$ 是本元多项式, 如果存在素数 $p$ 使得

1. $p\nmid a_n$;
2. $p\mid a_i, i=0,1,\dots,n-1$;
3. $p^2\nmid a_0$

那么 $f$ 是不可约的.

证明: 假设 $f(x)=h(x)g(x)$, 那么

$$\varphi_p(f(x))=\overline{f}(x)=a_nx^n=\overline{g}(x)\overline{h}(x)$$

从而 $\overline{g}(x)=cx^m, \overline{h}(x)=dx^{n-m}$, 从而

$$g(x)=cx^m+\cdots+c_0$$
$$h(x)=dx^{n-m}+\cdots+d_0$$

并且 $p\mid c_0, p\mid d_0$, 从而 $p^2\mid a_0=c_0d_0$, 相矛盾. □

**例子.** $f(x)=x^5+20x^4+5x^3+15$, 取 $p=5$ 即可

**例子** (分圆多项式)**.** 给定素数 $p$, $p$ 次分圆多项式定义为

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+1=\frac{x^p-1}{x-1}$$

我们现在来证明分圆多项式的不可约性. 由于 $\Phi_p(x)(x-1)=x^p-1$, 我们令 $y=x-1$ 则有

$$\begin{aligned}\Phi_p(y+1)&=\frac{(y+1)^p-1}{y}\\&=y^{p-1}+py^{p-2}+\cdots+\binom{p}{i}y^{p-i-1}+\cdots+p\end{aligned}$$

注意到对于 $1\le i\le p-1$, 有 $p\mid\binom{p}{i}$, 从而对素数 $p$ 利用艾森斯坦判别法可知 $\Phi_p(y+1)$ 不可约, 从而 $\Phi_p(x)$ 也是不可约的.

## 7.3 作业 7

**练习.** *Prove that* $\mathbb{Z}[i]/(3)$ *is a field.*

**练习.** *Give an example of irreducible polynomial* $f(x)$ *of degree* 2 *in* $\mathbb{F}_3[x]$*. Use* $f(x)$ *to construct an example of a field consisting of* 9 *elements.*

**练习.** *Decide whether or not* $x^4+6x^3+9x+3$ *is irreducible in* $\mathbb{Q}[x]$*.*

**练习.** *Factor the integral polynomial* $x^5+2x^4+3x^3+3x+5$ *in* $\mathbb{F}_2[x]$*,* $\mathbb{F}_3[x]$ *and* $\mathbb{Q}[x]$*.*

**练习** (Artin Chapter 12, 2.9)**.** *Let* $F$ *be a field. Prove that the ring* $F\left[x,x^{-1}\right]$ *of Laurent polynomials (Chapter 11 , Exercise 5.7) is a principal ideal domain. (Hint: use ring homomorphism* $\phi\colon F[x]\to F\left[x,x^{-1}\right]$ *and pull-back of ideals.)*

**练习.** 假设 $x\in\mathbb{Q}$ 是某一个首一整系数多项式的根，则 $x$ 是整数。

**练习.** 假设 $D$ 是一个正整数.

1. 验证 $\mathbb{Z}[\sqrt{-D}]=\{a+b\sqrt{-D}\mid a,b\in\mathbb{Z}\}$ 是一个 $\mathbb{C}$ 的子环.
2. 求 $\mathbb{Z}[\sqrt{-D}]$ 的乘法可逆元全体.
3. 在 $\mathbb{Z}[\sqrt{-5}]$ 中验证 $2,3,1\pm\sqrt{-5}$ 是不可约元。请指出哪些是素元，为什么？
4. 证明 $\mathbb{Z}[\sqrt{-D}]$ 中的非零素理想都是极大理想。*(Hint: Use ring homomorphism* $\mathbb{Z}\to\mathbb{Z}[\sqrt{-D}]$ *and pull back of ideals.)*

**练习.** *Prove that a prime number* $p$ *can be written as* $p=m^2+2n^2$ *with* $m,n\in\mathbb{Z}$ *if and only if* $x^2+2$ *has a root in* $\mathbb{F}_p$*. (In fact, this is true if and only if* $p=2$ *or* $p\equiv 1,3 \mod 8$*, proved by Fermat.)*

**练习.** 求一组多项式方程 $f^2+g^2=h^2$ 在 $\mathbb{C}[t]$ 上的非平凡解，即 $f,g,h\in\mathbb{C}[t]$ 满足 $\deg f,\deg g,\deg h\geq 1$ 且 $\gcd(f,g,h)=1$.（所有解可以是什么形式？）

**练习.** 尝试描述 $\mathbb{C}[x,y]$ 的所有素理想。

**练习.** *Let* $F$ *be a field and* $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots a_0\in F[x]$*. Define the derivative of* $f$ *similarly as calculus.* $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$*. For* $f(x),g(x)\in F[x]$*, prove*

1. $(fg)'=fg'+f'g$.
2. $(f(g(x)))'=f'(g(x))\cdot g'$.
3. *If* $\gcd(f,f')=1$*, then in the irreducible factorization of* $f$*, there are no factors with multiplicities. (在* $F$ *的特征是零的时候，反过来也对，但我不知道不依赖域论的证明，如果有同学想到如何证明请也写下来)*

**练习.** *Let* $p$ *be a prime number. Prove that* $f(x)=x^p-x-1\in\mathbb{F}_p[x]$ *is irreducible by the following steps.*

1. $f(x+1)=f(x)$
2. *If* $g(x)\in\mathbb{F}_p[x]$ *and* $1\leq\deg g\leq p-1$*, then* $g(x+1)\neq g(x)$.

3. *Let $f = g_1 \cdots g_k$ be irreducible factorization of $f$ with monic factors. Prove that $g_i$ are distinct.*
4. *Let $a \in \mathbb{Z}/p\mathbb{Z}$. Prove that $a \cdot g_i(x) = g_i(x+a)$ defines an action of $C_p$ on the set $\{g_1 \cdots g_k\}$.*
5. *Using enumeration formulas of group operation to prove that $f(x)$ is irreducible.*

*(In fact, for $n \geq 2$, the polynomial $f(x) = x^n - x - 1 \in \mathbb{Z}[x]$ is irreducible.)*

# 第八章　第八周

## 8.1　十一月一

为了确定高斯整环 $\mathbb{Z}[i]$ 的所有素理想, 由于它是欧几里德整环, 从而是主理想整环, 因此只需要确定所有的素元 (不可约元即可).

**命题 8.1.1.** *如下三条等价:*

1. *素数 $p$ 在 $\mathbb{Z}[i]$ 中可约;*
2. *$p = m^2 + n^2, m, n \in \mathbb{Z}$;*
3. *$p = 2$ 或 $p \equiv 1 \pmod 4$.*

*证明:* (1) 与 (2) 等价: 如果 $p = m^2 + n^2$, 那么 $p = (m + in)(m - in)$. 反之, 如果 $p = (a + bi)(c + di)$, 那么有

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

从而有 $p = a^2 + b^2 = c^2 + d^2$.

(1) 与 (3) 等价:

$$\begin{aligned}\mathbb{Z}[i]/(p) &\cong \mathbb{Z}[x]/(x^2 + 1, p)\\ &\cong \mathbb{F}_p[x]/(x^2 + 1)\end{aligned}$$

从而 $p$ 在 $\mathbb{Z}[i]$ 中可约当且仅当 $x^2 + 1$ 在 $\mathbb{F}_p[x]$ 中可约, 这等价于 $x^2 + 1 = 0$ 在 $\mathbb{F}_p$ 中有根.

1. 如果 $p = 2$, $x^2 + 1 = 0$ 在 $\mathbb{F}_2$ 中显然有根 $x = 1$;
2. 如果 $p \neq 2$, $x^2 + 1 = 0$ 意味着 $x$ 在循环群 $\mathbb{F}_p^\times$ 中是 4 阶元, $p - 1$ 阶循环群中 4 阶元存在当且仅当 $4 \mid p - 1$, 即 $p \equiv 1 \pmod 4$.

□

**命题 8.1.2.** *$\mathbb{Z}[i]$ 中的素理想 $I = (a + bi)$ 如下:*

1. *如果 $ab = 0$, 那么 $I = (p)$, 其中 $p \equiv 3 \pmod 4$;*
2. *如果 $ab \neq 0$, 那么 $a^2 + b^2 = p$, 其中素数 $p = 2$ 或 $p \equiv 2 \pmod 4$.*

*证明:* $ab = 0$ 的情况我们已经确定了. 若 $(a + bi), ab \neq 0$ 是素理想, 那么考虑 $a^2 + b^2$ 的如下分解

$$a^2 + b^2 = (a + bi)(a - bi)$$

这个分解是不可约的, 因为 $a + bi, a - bi$ 都是素元. 另一方面在 $\mathbb{Z}$ 中我们可以将 $a^2 + b^2$ 分解成 $p_1 p_2 \dots p_n$, 注意到 $1 \leq n \leq 2$, 这是因为任何一个 $p_i$ 都至少会在 $\mathbb{Z}[i]$ 中分解出一个因子.

1. 如果 $n = 1$, 那么 $a^2 + b^2 = (a - bi)(a + bi) = p$, 即 $p = 2$ 或 $p \equiv 1 \pmod 4$.

2. 如果 $n=2$, 那么不妨记 $a+bi$ 与某个素数 $p$ 相伴, 此时与 $ab\neq 0$ 矛盾.
另一方面, 任取 $a^2+b^2=p, a, b\in\mathbb{Z}$, 则 $a+bi$ 是素元:

$$(a+bi)=(c+di)(m+ni)$$

从而

$$p=a^2+b^2=(c^2+d^2)(m^2+n^2)$$

这意味着 $c+di$ 或 $m+ni$ 中有一个是单位. □

下面我们想要去研究一般二次扩张中的整数环. 给定一个无平方因子的整数 $d$, 即 $\mathbb{C}$ 的如下子域

$$\mathbb{Q}[\sqrt{d}]=\{a+b\sqrt{d}\mid a,b\in\mathbb{Q}\}$$

中的整数环.

**定义 8.1.3.** $\mathbb{C}$ 中的代数整数定义为

$$A=\{x\in\mathbb{C}\mid \text{存在 } \mathbb{Z}[x] \text{ 中的首一多项式 } f(x) \text{ 使得 } f(x)=0\}$$

实际上, $A$ 构成了 $\mathbb{C}$ 的一个子环, 也就是我们想要去研究的代数整数环, 为了证明这个事实, 我们需要如下引理:

**引理 8.1.4.** *$a\in A$ 当且仅当 $a$ 是某一个 $M\in M_n(\mathbb{Z})$ 的特征值.*

*证明:* 给定 $\mathbb{Z}[x]$ 中的首一多项式 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, 考虑其友阵

$$M=\begin{bmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & \cdots & 0 & -a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{bmatrix}$$

则友阵的特征值恰好是 $f(x)$ 的根, 即

$$\det(\lambda I-M)=f(\lambda)$$

□

**引理 8.1.5.** *给定两个矩阵 $B, C$, 其特征值分别为 $\lambda_1,\ldots,\lambda_n$ 和 $\mu_1,\ldots,\mu_n$, 则 $B\otimes C$ 的特征值为 $\lambda_i\mu_j, 1\leq i,j\leq n$.*

**命题 8.1.6.** *$A$ 是 $\mathbb{C}$ 的一个子环.*

*证明:* 根据上面的两个引理即可. □

**练习.** $A\cap\mathbb{Q}=\mathbb{Z}$.

**命题 8.1.7.**

$$R := A \cap \mathbb{Q}[\sqrt{d}] = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{\sqrt{d}+1}{2}] & d \equiv 1 \pmod 4 \end{cases}$$

证明: 取 $a+b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, 我们不妨假设 $b \neq 0$(因为如果 $b=0$ 那么 $a \in A \cap \mathbb{Q}$ 意味着 $a \in \mathbb{Z}$). 不难发现 $a+b\sqrt{d}$ 满足

$$x^2 - 2ax + b^2 d - a^2 = 0$$

因此 $a+b\sqrt{d} \in A$ 当且仅当

$$\begin{cases} 2a \in \mathbb{Z} \\ b^2 d - a^2 \in \mathbb{Z} \end{cases}$$

我们分如下的情况考虑:

1. 如果 $a \in \mathbb{Z}$, 那么 $b^2 d \in \mathbb{Z}$, 由于 $d$ 是无平方因子的, 从而 $b \in \mathbb{Z}$;
2. 如果 $a \in \frac{1}{2} + \mathbb{Z}$, 假设 $a = \frac{1}{2} + m, m \in \mathbb{Z}$, 从而

$$b^2 d = n + m^2 + m + \frac{1}{4}$$

其中 $n \in \mathbb{Z}$, 从而 $4b^2 d \in \mathbb{Z}$, 即同样由于 $d$ 无平方因子可知 $2b \in \mathbb{Z}$
如果令 $m = 2a, n = 2b$, 那么我们一定有 $m, n \in \mathbb{Z}$, 并且 $4 \mid m^2 - dn^2$.

1. 如果 $d \equiv 2 \pmod 4$, 那么

$$0 \equiv m^2 - dn^2 \equiv m^2 + 2n^2 \pmod 4$$

而这只有 $m, n$ 都是偶数的时候才可能发生, 即此时 $a, b$ 都是整数;

2. 如果 $d \equiv 3 \pmod 4$, 分析同上;
3. 如果 $d \equiv 1 \pmod 4$, 那么

$$0 \equiv m^2 - dn^2 \equiv m^2 - n^2 \pmod 4$$

但是 $4 \mid m^2 - n^2$ 当且仅当 $m \equiv n \pmod 2$, 从而此时

$$R = \{\frac{m+n\sqrt{d}}{2} \mid m, n \in \mathbb{Z}, m \equiv 2 \pmod 2\}$$

注意到

$$\frac{m+n\sqrt{d}}{2} = \frac{m+n}{2} + n(\frac{-1+\sqrt{d}}{2}), \quad \frac{m+n}{2} \in \mathbb{Z}$$

从而此时 $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

□

在代数数论中给定了一个代数整数环后, 第一个问题就是去研究这个代数整数环中的单位是哪些, 在这里如果我们考虑 $d < 0$ 的情况, 即虚二次数域 $\mathbb{Q}[\sqrt{d}]$ 的代数整数环 $R = A \cap \mathbb{Q}[\sqrt{d}]$, 我们有如下的刻画: 考虑如下映射

$$N : R \to \mathbb{Z}$$
$$a + b\sqrt{d} \mapsto a^2 - b^2 d$$

不难发现其满足 $N(\alpha\beta) = N(\alpha)N(\beta)$.

**命题 8.1.8.** $\alpha \in R$ 是单位当且仅当 $N(\alpha) = 1$

**例子.** $d = -1$, 即 $R$ 是高斯整数时, 单位是 $\{\pm 1, \pm i\}$

**例子.** $d = -3$ 时, $R$ 的单位是 $\{\pm 1, e^{\frac{\pi}{3}}, e^{\frac{2\pi}{3}}, e^{\frac{-\pi}{3}}, e^{\frac{-2\pi}{3}}\}$

**例子.** 当 $d < 0, d \neq -1, -3$ 时, $R$ 的单位只有 $\{\pm 1\}$

## 8.2 十一月二

另一个问题是什么时候虚二次数域的代数整数环 $R$ 会是唯一分解的呢?

**例子.** $d \equiv 3 \pmod 4, d < 0, d \neq -1$ 时, 我们可以做如下分解

$$\begin{aligned} 1 - d &= 2\frac{1-d}{2} \\ &= (1 - \sqrt{d})(1 + \sqrt{d}) \end{aligned}$$

从而不是唯一分解的. 对 $d \equiv 2 \pmod 4$ 的时候你可以做类似的事情证明这个时候 $R$ 也不是唯一分解的.

我们有如下重要的结果

**定理 8.2.1.** $\mathbb{Q}[\sqrt{d}], d < 0$ 的代数整数环 $R$ 是唯一分解整环当且仅当

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

之后我们将说明, 对于虚二次数域的代数整数环 $R$, 其为唯一分解整环当且仅当其为主理想整环, 并通过计算 $d$ 为上述情况时候的类群来说明这些情况都是唯一分解的, 从而证明上述定理的一方面. 为了说明这些事, 我们需要一些准备.

**引理 8.2.2.** $\mathbb{R}^2$ 中的离散子群只有如下三种

1. $\{0\}$;
2. $\mathbb{Z}a$;
3. $\mathbb{Z}a + \mathbb{Z}b$, 其中 $a, b$ 在 $\mathbb{R}$ 上线性无关, 这个时候称为是 $\mathbb{R}^2$ 的一个格 *(lattice)*.

**命题 8.2.3.** 如果 $I$ 是 $R$ 的一个非零理想, 那么 $I$ 是 $\mathbb{R}^2$ 的一个格.

*证明:* 不妨考虑 $d \equiv 2, 3 \pmod 4$ 的情况, 另一种情况同理: 此时 $R = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ 是 $\mathbb{R}^2$ 的一个格, 从而 $I$ 也是 $\mathbb{R}^2$ 的一个离散子群. 如果其非零, 那么任取 $0 \neq \alpha \in I$, 不难发现 $\alpha, \alpha\sqrt{d}$ 在 $\mathbb{R}$ 上线性无关, 从而 $I$ 是 $\mathbb{R}^2$ 的一个格. □

**命题 8.2.4.** $I \subset R$ 是 $\mathbb{R}^2$ 中的一个格, 那么 $I$ 是一个理想的当且仅当

1. $\sqrt{d}I \subset I$, $d \equiv 2, 3 \pmod 4$;
2. $\frac{\sqrt{d}+1}{2}I \subset I$, $d \equiv 1 \pmod 4$.

证明: 对于第一种情况

$$R = \mathbb{Z} + \mathbb{Z}\sqrt{d}$$

所以 $I$ 是 $R$ 的理想当且仅当 $(Z + \mathbb{Z}\sqrt{d})I \subset I$, 这也当且仅当 $\sqrt{d}I \subset I$, 对于第二种情况来说同理. □

在考虑更一般的情况之前, 我们先来看一下 $\mathbb{Z}[\sqrt{-5}]$ 中的理想是什么样的. 我们有如下的结果:

**定理 8.2.5.** *$R = \mathbb{Z}[\sqrt{-5}]$, $I$ 是 $R$ 的一个非零理想, $\alpha$ 是 $I$ 中有极小范数的元素, 那么只有如下两种可能:*

1. *$(\alpha, \alpha\sqrt{-5})$ 是 $I$ 作为格的基, 此时 $I$ 是主理想 $(\alpha)$;*
2. *$(\alpha, \frac{1}{2}(\alpha + \alpha\sqrt{-5}))$ 是 $I$ 作为格的基, 此时 $I$ 不是主理想.*

为了证明这个结果, 我们需要下面的引理:

**引理 8.2.6.** *$L \subset \mathbb{R}^2$ 是一个格, $r = \min\{|z| \mid z \in L\backslash\{0\}\}$. 对于 $\gamma \in L$ 定义*

$$D(\frac{1}{n}\gamma, \frac{1}{n}r) = \{z \mid |z - \frac{1}{n}\gamma| < \frac{1}{n}r\}$$

*那么如果 $D(\frac{1}{n}\gamma, \frac{1}{n}r) \cap L \neq \varnothing$, 则有*

$$D(\frac{1}{n}\gamma, \frac{1}{n}r) \cap L = \{\frac{1}{n}\gamma\}$$

证明: 假设 $\beta \in D(\frac{1}{n}\gamma, \frac{1}{n}r)$, 即 $|\beta - \frac{1}{n}\gamma| < \frac{1}{n}r$, 这等价于 $|n\beta - \gamma| < r$. 并且 $n\beta - \gamma \in L$, 从而根据 $r$ 的选择可知 $n\beta - r = 0$, 即 $\beta = \frac{1}{n}\gamma$. □

定理 8.2.5证明. 给定 $R = \mathbb{Z}[\sqrt{-5}]$ 的一个理想 $I$, 以及 $\alpha$ 是 $I$ 中有极小范数的元素, 由于 $I$ 包含 $\alpha$, 从而 $I$ 包含 $(\alpha)$, 如果此时 $I = (\alpha)$, 我们即得到了第一种情况. 现假设存在 $\beta \in I$ 并且 $\beta \notin (\alpha)$, 由于 $(\alpha)$ 作为格的基为 $(\alpha, \alpha\sqrt{-5})$, 因此我们不妨假设 $\beta$ 落在由如下关系生成的平行四边形内部

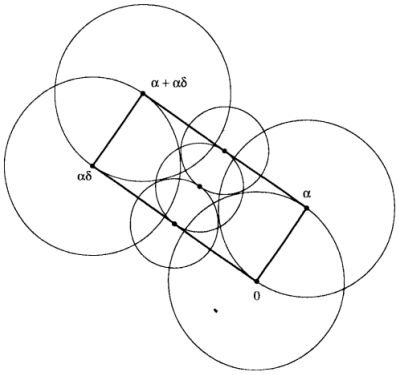
$$\prod = \{r\alpha + s\alpha\sqrt{-5} \mid 0 \leq r, s \leq 1\}$$

对于这个平行四边形 $\prod$, 我们有如下刻画:

1. $\prod$ 实际上是一个长方形, 因为 $\sqrt{-5}$ 是纯虚数;
2. $\prod$ 的边长比为 $1 : \sqrt{5}$;
3. 我们不知道 $\prod$ 具体在 $\mathbb{R}^2$ 中的位置, 这取决于 $\alpha$.

如果可以证明 $\beta$ 正好是这个平行四边形的中心, 我们就得出了我们的结论. 考虑下图[1]中的七个圆盘

[1]图源 Artin's algebra




不难看出这七个圆盘覆盖了整个平行四边形, 并且根据引理8.2.6可知, $I$ 中的元素只可能是这些圆盘的圆心, 并且由于 $\beta \notin (\alpha)$, $\beta$ 只有如下三种可能

1. $\beta = \frac{1}{2}(\alpha + \alpha\sqrt{-5})$;
2. $\beta = \frac{1}{2}\alpha\sqrt{-5}$;
3. $\beta = \alpha + \frac{1}{2}\alpha\sqrt{-5}$.

并且不难发现第二三种情况是一样的, 因为 $\alpha \in I$. 假设第二种情况发生, 那么根据命题8.2.4可知 $\frac{1}{2}\alpha(\sqrt{-5})^2 = -\frac{5}{2}\alpha \in I$, 从而 $\frac{1}{2}\alpha \in I$, 这与 $\alpha$ 的选取矛盾. □

**定义 8.2.7.** 给定环 $R$ 以及两个理想 $I, J$, 乘积理想 $IJ$ 定义为

$$IJ := \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J\}$$

**例子.** $R = \mathbb{Z}[\sqrt{-5}]$, 以及素理想

$$I = (2, 1 - \sqrt{-5}), \overline{I} = (2, 1 + \sqrt{-5})$$
$$J = (3, 1 + \sqrt{-5}), \overline{J} = (3, 1 - \sqrt{-5})$$

直接验证则有

$$I\overline{I} = (4, 2(1 + \sqrt{-5}), 2(1 - \sqrt{-5}), 6) = (2)$$
$$J\overline{J} = (3)$$

从而

$$(6) = (2)(3) = I\overline{I}J\overline{J}$$

上面的事情告诉我们, 虽然 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环, 但是其理想仍然有某种唯一分解成素理想的性质. 实际上, 对于一般的虚二次数域的代数整数环都有如此的性质, 即

**定理 8.2.8.** *$R$ 是某个虚二次数域的代数整数环, $R$ 的每个真理想都可以分解成素理想的乘积, 并且在除去排序的意义下唯一.*

如果证明了上面的事实, 并且加上如下事实

**命题 8.2.9.** *$R$ 是某个虚二次数域的代数整数环, $I$ 是 $R$ 的素理想当且仅当其为极大理想.*

那么

**定理 8.2.10.** 如果 $R$ 是某个虚二次数域的代数整数环, 那么 $R$ 是唯一分解整环当且仅当 $R$ 是主理想整环.

证明: 只需要证明如果 $R$ 是唯一分解整环则 $R$ 是主理想整环: 根据定理8.2.8, $R$ 的每个真理想都是素理想的乘积, 并且主理想的乘积仍然是主理想, 因此只需要证明素理想都是主理想即可. 给定 $R$ 的一个素理想 $P$, $0 \neq \alpha \in P$, 那么由于 $R$ 是唯一分解整环, $\alpha$ 可以分解成不可约元的乘积, 并且它们也是素元. 由于 $P$ 是素理想, 从而 $P$ 包含 $\alpha$ 的某一个素因子 $\pi$, 即 $P$ 包含素理想 $(\pi)$, 并且根据命题8.2.9, $(\pi)$ 是极大理想, 从而 $P = (\pi)$. □

因此, 下面的目的则在于证明定理8.2.8以及命题8.2.9.

**引理 8.2.11.** 如果 $R$ 是某个虚二次数域的代数整数环, 任何 $R$ 的非零理想 $I$ 都有如下的性质

$$I\overline{I} = (n), \quad n \in \mathbb{Z}$$

证明: 由于 $I$ 是 $\mathbb{R}^2$ 中的格, 那么不妨记 $I = (\alpha, \beta)$, 那么则有

$$I\overline{I} = (\alpha\overline{\alpha}, \alpha\overline{\beta}, \overline{\alpha}\beta, \overline{\alpha}\overline{\beta})$$

其中 $\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta} + \overline{\alpha}\beta \in \mathbb{Z}$. 取 $n = \gcd(\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta} + \overline{\alpha}\beta)$, 那么我们断言

$$\alpha\overline{\beta}, \overline{\alpha}\beta \in (n)$$

首先 $\frac{\alpha\overline{\beta}}{n}, \frac{\overline{\alpha}\beta}{n} \in \mathbb{Q}[\sqrt{d}]$, 并且 $\frac{\alpha\overline{\beta}}{n}, \frac{\overline{\alpha}\beta}{n}$ 满足

$$x^2 + ax + b = 0, \quad a, b \in \mathbb{Z}$$

从而有

$$\frac{\alpha\overline{\beta}}{n}, \frac{\overline{\alpha}\beta}{n} \in R$$

即 $I\overline{I} = (n), n \in \mathbb{Z}$. □

**推论 8.2.12.** 在虚二次数域的代数整数环 $R$ 中:

1. 如果 $I_1 J = I_2 J, J \neq (0)$, 那么 $I_1 = I_2$;
2. 如果 $I \supset J \neq (0)$, 那么存在理想 $I'$ 使得 $J = II'$.

证明: (1). 对 $I_1 J = I_2 J$ 两侧同乘 $\overline{J}$ 即可.

(2). 如果 $I = (n)$ 是主理想, 那么任取 $a \in J, a = nb, b \in R$, 从而

$$I' := \frac{J}{n} = \{\frac{a}{n} \mid a \in J\}$$

构成了 $R$ 的一个理想, 并且满足 $J = II'$. 如果 $I$ 不是主理想, 那么 $(I\overline{I}) \supset \overline{I}J$, 这意味着

$$\overline{I}J = \overline{I}II'$$

同时消去 $\overline{I}$ 即可. □

注记. 在虚二次数域的代数整数环 $R$ 中, $I \mid J$(即 $J = II'$) 等价于 $I \supset J$.

**命题 8.2.13.** *在虚二次数域的代数整数环 $R$ 中, $P$ 是 $R$ 的素理想, 那么 $P \mid IJ$ 意味着 $P \mid I$ 或 $P \mid J$.*

*证明:* 根据上述推论, $P \mid IJ$ 等价于 $IJ \subset P$, 由于 $P$ 是素理想, $IJ \subset P$ 意味着 $I \subset P$ 或 $J \subset P$, 再次利用上述推论可知这等价于 $P \mid I$ 或者 $P \mid J$. □

**命题 8.2.14.** *在虚二次数域的代数整数环 $R$ 中, 如果 $I$ 是 $R$ 的一个理想, 则 $R/I$ 有限.*

*证明:* 由于 $I\overline{I} \subset I$, 因此只需要证明 $R/I\overline{I}$ 有限即可, 而根据引理8.2.11可知 $I\overline{I} = (n)$, 注意到

$$\begin{aligned} R/(n) &\cong \mathbb{Z}[x]/(x^2+d, n) \\ &\cong (\mathbb{Z}/n\mathbb{Z})[x]/(x^2+d) \end{aligned}$$

从而可知 $|R/(n)| = n^2 < \infty$. □

**推论 8.2.15.** *在虚二次数域的代数整数环 $R$ 中, $(0) \neq I \subset R$ 是一个理想, 那么 $R$ 中包含 $I$ 的理想只有有限多个.*

命题8.2.9*证明.* 给定虚二次数域代数整数环 $R$ 的一个素理想 $I$, 那么 $R/I$ 是一个有限整环, 从而是域, 即 $I$ 是极大理想. □

定理8.2.8*证明.* 如果 $(0) \neq I$ 不是极大理想, 那么一定可以写成

$$I = P_1 I'$$

其中 $P_1$ 是包含 $I$ 的一个 (素) 极大理想, 并且由于包含 $I$ 的理想只有有限多个, 从而分解会在有限步停止. □

*注记.* 利用相同的论证可以证明任何一个维数是 1 的环其为唯一分解整环当且仅当其为主理想整环.

# 第九章　第九周

## 9.1　十一月八日

上一次课我们证明了对于虚二次数域的代数整数环 $R$ 其为唯一分解整环当且仅当其为主理想整环, 并且我们也用格的想法去研究了 $\mathbb{Z}[\sqrt{-5}]$ 中的理想的形式. 对于一般的情况, 我们需要有一种办法来刻画这个环距离主理想整环的差距, 即接下来要引入理想类群这件事情.

**定义 9.1.1.** 给定虚二次数域的代数整数环 $R$, $R$ 的类群 (class group)定义为

$$\mathscr{C}(R) := \{I \neq 0, I\text{是 } R \text{ 的理想}\}/\sim$$

其中非零理想 $I \sim I'$ 当且仅当存在 $\alpha \in \mathbb{Q}[\sqrt{d}]$ 使得 $I = \alpha I'$. 对于理想 $I$ 我们用 $[I]$ 去记其在类群中的等价类.

注记. 现在 $\mathscr{C}(R)$ 只是一个等价类组成的集合, 我们还没有给它赋予群结构.

**引理 9.1.2.** *平凡理想 $R$ 的等价类 $[R]$ 是由全体主理想组成.*

*证明:* 根据定义, 对于 $R$ 的理想 $I$, $[I] = [R]$ 当且仅当 $I = \alpha R$, 其中 $\alpha \in \mathbb{Q}[\sqrt{d}]$[1], 这也当且仅当 $I$ 是主理想 $(\alpha)$. □

**命题 9.1.3.** *虚二次数域的代数整数环 $R$ 的类群 $\mathscr{C}(R)$ 构成了一个阿贝尔群, 其中群结构由理想的乘法给出, 即对于非零理想 $A, B$, $[AB] := [A][B]$.*

*证明:* 我们如下依次验证:

1. 假设 $[A] = [A'], [B] = [B']$, 即 $A = \alpha A', B = \beta B'$, 那么 $AB = \alpha\beta A'B'$, 从而 $[AB] = [A'B']$, 即群运算是良好定义的;
2. 群运算具有结合律和交换律, 这是因为理想的乘法具有结合律和交换律;
3. $[R]$ 是类群中的单位元, 因为 $[R][A] = [RA] = [A]$;
4. $[\overline{A}]$ 是 $[A]$ 的逆元, 因为根据引理8.2.11, 可知 $A\overline{A}$ 是主理想, 从而 $[A][\overline{A}] = [R]$.

□

**推论 9.1.4.** *虚二次数域的代数整数环 $R$ 是唯一分解整环当且仅当类群 $\mathscr{C}(R)$ 是平凡群.*

由于虚二次数域的代数整数环 $R$ 的任何理想都可以写成素理想的乘积, 因此 $\mathscr{C}(R)$ 可以由素理想对应的等价类生成, 但是这依然是一个无法验证的事情, 下面我们的目的在于通过证明类群可以由某些 “有限” 大小的素理想生成, 从而证明 $|\mathscr{C}(R)| < \infty$, 并且给了我们一种可计算的方法.

[1]此时 $\alpha$ 不仅仅在 $\mathbb{Q}[\sqrt{d}]$ 中, 它也在 $R$ 中.

**定理 9.1.5.** *在虚二次数域的代数整数环 $R$ 中, 素理想 $0 \neq P$ 只有如下两种形式:*

1. *$P = (p)$, 其中 $p \in \mathbb{Z}$ 是素数;*
2. *$P\overline{P} = (p)$, 其中 $p \in \mathbb{Z}$ 是素数.*

*证明:* 首先根据引理8.2.11, 我们总有 $P\overline{P} = (n)$, 其中 $n\mathbb{Z}$, 并且在 $\mathbb{Z}$ 中分解 $n$, 只有如下两种可能:

1. $n = p_1p_2$, 其中 $p_1, p_2$ 是素数;
2. $n = p$, 其中 $p$ 是素数

不难发现这两种情形分别对应我们需要的两种情形. □

**定理 9.1.6.** *在虚二次数域的代数整数环 $R$ 中, 一个素数 $p$ 生成了 $R$ 中的一个素理想当且仅当:*

1. *$x^2 - d$ 在 $\mathbb{F}_p[x]$ 中不可约, 如果 $d \equiv 2, 3 \pmod 4$;*
2. *$x^2 - x - h$ 在 $\mathbb{F}_p[x]$ 中不可约, 其中 $h = \frac{1}{4}(1-d)$, 如果 $d \equiv 1 \pmod 4$.*

*证明:* 假设 $d \equiv 2, 3 \pmod 4$, 则 $R = \mathbb{Z}[\sqrt{d}]$ 同构于 $\mathbb{Z}[x]/(x^2 - d)$, 素数 $p$ 在 $R$ 中生成素理想当且仅当 $R/(p)$ 是域, 这当且仅当 $x^2 - d$ 在 $\mathbb{F}_p[x]$ 中不可约, 另一种情况的证明类似. □

**引理 9.1.7.** *给定虚二次数域代数整数环 $R$ 的非零理想 $I, J_1, J_2$, 其中 $J_1 \subset J_2$, 如果记 $[J_1 : J_2] := |J_1/J_2|$, 那么有*

$$[IJ_1 : IJ_2] = [J_1 : J_2]$$

*证明:* 如果 $I$ 是主理想 $(n)$, 那么不难发现 $[nJ_1 : nJ_2] = [J_1 : J_2]$. 由于 $R$ 中的任何理想都可以分解成素理想的乘积, 那么我们不妨假设 $I$ 是素理想, 并且不是主理想, 根据定理9.1.5, 我们知道存在素数 $p$ 使得 $I$ 满足 $I\overline{I} = (p)$. 注意到

$$p^2 = [J_1 : I\overline{I}J_1] = [J_1 : IJ_1][IJ_1 : I\overline{I}J_1]$$

并且根据消去性以及 $I \neq R$, 我们可知 $[J_1 : IJ_1] > 1, [IJ_1 : I\overline{I}J_1] > 1$, 从而有 $[J_1 : IJ_1] = p$, 同样可以证明 $[J_2 : IJ_2] = p$. 根据指数的传递性有

$$[J_1 : J_2][J_2 : IJ_2] = [J_1 : IJ_1][IJ_1 : IJ_2]$$

即

$$[J_1 : J_2] = [IJ_1 : IJ_2]$$

□

## 9.2 十一月九日

回忆在 $\mathbb{Z}[\sqrt{-5}]$ 的时候, 给定非零理想 $I$, 如果 $\alpha$ 是在 $I$ 中有极小范数的元素, 那么 $I/(\alpha)$ 可以给出一种刻画 $I$ 距离主理想差距到底有多大的量, 这是我们的直观感觉. 下面我们要去严格的说明给定 $R$ 的两个理想, 我们该如何去比较它们.

首先给定 $\mathbb{R}^2$ 的两个格 $L_1 \supset L_2$, 其中 $\alpha, \beta$ 是 $L_1$ 的基, $a, b$ 是 $L_2$ 的基. 那么存在整系数矩阵 $M$ 满足

$$(a, b) = (\alpha, \beta)\begin{pmatrix} m_1 & m_2 \\ m_3 & m_4 \end{pmatrix}$$

我们不妨假设 $M$ 是对角矩阵, 因为我们总可以通过选取合适的基做到这件事, 即 $m_2 = m_3 = 0$, 那么则有

$$\mathbb{Z}\alpha + \mathbb{Z}\beta/\mathbb{Z}(m_1\alpha) + \mathbb{Z}/(m_4\beta) \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_4\mathbb{Z})$$

从而有 $\Delta(L_1)/\Delta(L_2) = |L_1/L_2| = |m_1 m_4| = |\det M|$, 其中 $\Delta(L)$ 表示格 $L$ 的面积.

**定义 9.2.1.** 给定虚二次数域的代数整数环 $R$ 的一个理想 $I$, 其范数 $N(I)$ 定义为 $n$, 其中 $I\overline{I} = (n)$.

**命题 9.2.2.** *对于理想的范数, 我们有如下的性质:*

1. $N(IJ) = N(I)N(J)$;
2. *如果 $I = (\alpha)$ 是主理想, 那么 $N(I) = N(\alpha)$.*

*证明:* (1). 假设 $N(I) = m, N(J) = n$, 那么 $I\overline{I} = (m), J\overline{J} = (n)$, 从而

$$(IJ)(\overline{IJ}) = (m)(n) = (mn)$$

即 $N(IJ) = N(I)N(J)$.

(2). 假设 $I = (\alpha)$, 并且用 $n$ 记 $\alpha$ 的范数 $\alpha\overline{\alpha}$, 那么

$$I\overline{I} = (\alpha)(\overline{\alpha}) = (\alpha\overline{\alpha}) = (n)$$

即 $N(I) = n = N(\alpha)$. □

因此给定虚二次数域的代数整数环 $R$ 中的非零理想 $I$, 一方面我们可以谈它的范数 $N(I)$, 它有很好的可乘性; 另一方面, 我们可以将其将其视作 $\mathbb{R}^2$ 中的格, 并且有 $|R/I| = \Delta(R)/\Delta(I)$.

**命题 9.2.3.** *给定虚二次数域的代数整数环 $R$, $I$ 是其非零理想, 那么:*

$$N(I) = |R/I| = \Delta(R)/\Delta(I)$$

*证明:* 假设 $N(I) = n$, 即 $I\overline{I} = (n)$, 那么有

$$n^2 = |R/(n)| = |R/I\overline{I}| = [R : I][I : I\overline{I}]$$

然而根据引理9.1.7, 有 $[I : I\overline{I}] = [R : \overline{I}] = [R : I]$, 从而 $|R/I| = n$. □

如果我们取 $\alpha$ 是非零理想 $I$ 中最小范数的元素, 由于自然地有包含关系 $(\alpha) \subset L$, 从而有 $N(\alpha) \geq N(I)$, 另一方面, 我们有如下的界:

**命题 9.2.4.** $N(\alpha) \leq \mu\, N(I)$, *其中*

$$\mu = \begin{cases} 2\sqrt{\frac{|d|}{3}}, & d \equiv 2, 3 \pmod 4 \\ \sqrt{\frac{|d|}{3}}, & d \equiv 1 \pmod 4 \end{cases}$$

*是一个不依赖于 $I$ 的数.*

证明: 由于 $\alpha$ 是 $I$ 中范数最小的元素, 从而 $\Delta(L) \geq \frac{\sqrt{3}}{2}N(\alpha)$, 而 $N(I) = \Delta(R)/\Delta(I)$, 从而有

$$N(\alpha) \leq \frac{2}{\sqrt{3}}\Delta(I) = \frac{2}{\sqrt{3}}N(I)\Delta(R)$$

但是根据命题8.1.7

$$\Delta(R) = \begin{cases} \sqrt{|d|}, & d \equiv 2,3 \pmod 4 \\ \frac{1}{2}\sqrt{|d|}, & d \equiv 1 \pmod 4 \end{cases}$$

从而得到我们想要的结果. □

**定理 9.2.5.** 给定虚二次数域的代数整数环 $R$, 我们有如下结果:

1. 对于任意 $[I] \in \mathscr{C}(R)$, 存在 $I' \in [I]$ 使得 $N(I') \leq \mu$;
2. 类群 $\mathscr{C}(R)$ 由那些范数是素数 $p$, 并且小于等于 $\mu$ 的素理想生成;
3. $|\mathscr{C}(R)| < \infty$.

证明: (1). 取 $I$ 的有最小范数的元素 $\alpha$, 根据推论8.2.12, $(\alpha) \subset I$ 意味着存在理想 $J$ 使得 $(\alpha) = IJ$, 从而

$$(\alpha)\overline{J} = IJ\overline{J} = I(n) \implies I = \frac{\alpha}{n}\overline{J}$$

这意味着 $\overline{J} \in [I]$, 并且

$$N(\alpha) = N(I)N(J) \implies N(\overline{J}) = N(J) \leq \mu$$

那么 $\overline{J}$ 就是我们想要找的 $I'$.

(2). 任取 $[I] \in \mathscr{C}(R)$, 我们不妨假设 $N(I) \leq \mu$, 对 $I$ 做素理想分解则有 $I = P_1 \dots P_k$, 那么 $N(I) = N(P_1) \dots N(P_k)$, 从而 $N(P_i) \leq \mu, 1 \leq i \leq k$, 因此范数小于等于 $\mu$ 的素理想可以生成 $\mathscr{C}(R)$. 根据定理9.1.5, 素理想 $P$ 的范数要么是 $p$, 要么是 $p^2$, 其中 $p$ 是素数, 并且是后者时 $P$ 是主理想, 从而对应于类群中的单位元, 因此我们可以认为范数是素数 $p$, 并且小于等于 $\mu$ 的素理想对应的等价类生成了整个类群 $\mathscr{C}(R)$.

(3). 由 (2) 即得. □

如上定理即给了我们一个可计算的条件, 根据上述定理, 我们只需要考虑虚二次数域的代数整数环 $R$ 中有限多种素理想, 如果它们都是主理想的话, 此时我们就得到了类群 $\mathscr{C}(R)$ 是平凡群, 我们将通过这种办法去进行计算.

**例子.** $d = -163$ 时, 注意到 $-163 \equiv 1 \pmod 4$, 则 $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, 并且 $\lfloor \mu \rfloor = 8$, 因此我们需要考虑那些范数为 $2,3,5,7$ 的素理想 $P$, 这样的素理想存在当且仅当 $p = 2,3,5,7$ 在 $R$ 中没有生成素理想, 而是分裂成 $P\overline{P}$ 的情形. 对于 $p = 2,3,5,7$ 来说, $x^2 - x + 41$ 模 $p$ 总是不可约的, 从而 $p = 2,3,5,7$ 在 $R$ 中总是生成素理想, 即此时类群平凡.

注记. 用同样的办法, 给定任何 $d < 0$, 你都可以去计算此时的类群是平凡群或不是平凡群, 从而达到了我们最初的目的.

# 第十章　第十周

## 10.1　十一月十五

**定义 10.1.1.** 给定环 $R$, 一个 $R$-模 ($R$-module)是一个阿贝尔群 $(M,+)$ 以及一个 $R$ 的作用 $R\times M\to M$, 记做 $(r,m)\mapsto rm$, 满足如下公理:

1. $1v=1$;
2. $(rs)m=r(sm)$;
3. $(r+s)m=rm+sm$;
4. $r(m_1,m_2)=rm_1+rm_2$.

其中 $r,s\in R$ 以及 $m_1,m_2\in M$.

**例子.** 域 $\mathbb{F}$ 上的线性空间 $V$ 是 $\mathbb{F}$-模.

**例子.** 任意阿贝尔群都是 $\mathbb{Z}$-模.

**例子.** 给定域 $\mathbb{F}$, $\mathbb{F}$-线性空间 $V$ 以及一个线性变换 $T:V\to V$, 此时 $V$ 上具有一个 $\mathbb{F}[x]$-模结构, 如下给出:

$$\mathbb{F}[x]\times V\to V$$
$$(f(x),v)\mapsto f(T)v$$

**例子.** 给定环 $R$, 我们有如下 $R$-模:

1. 环 $R$ 可以看成一个 $R$-模, 其中 $R\times R\to R$ 由 $R$ 自身的乘法给出;
2. 环 $R$ 的任何理想 $I$ 可以看出一个 $R$-模;
3. $R^n=R\times\cdots\times R$, 也可以看成是 $R$-模, 被称为自由 $R$-模.

**定义 10.1.2.** 给定 $R$-模 $M$, $M$ 的子模 (submodule)是 $M$ 的一个阿贝尔群子群 $N$, 并且对 $R$ 的作用封闭.

**命题 10.1.3.** 环 $R$ 的一个子集 $I$ 是 $R$ 作为 $R$-模的子模当且仅当 $I$ 是 $R$ 的理想.

证明: 直接根据定义. □

**定义 10.1.4.** 给定 $R$-模 $M$ 以及 $M$ 的子模 $N$, 商群 $M/N$ 上有一个自然的 $R$-模结构, 由如下给出:

$$R\times M/N\to M/N$$
$$(r,m+N)\to rm+N$$

**定义 10.1.5.** 给定 $R$-模 $M_1, M_2$, 阿贝尔群的外直和 $M_1 \oplus M_2$ 上有自然的 $R$-模结构，由如下给出:

$$R \times M_1 \oplus M_2 \to M_1 \oplus M_2$$
$$(r, (m_1, m_2)) \to (rm_1, rm_2)$$

**定义 10.1.6.** 给定 $R$-模 $M_1, M_2$, $R$-模同态 ($R$-module homomorphism)是一个阿贝尔群 $\varphi : M_1 \to M_2$ 之间的群同态, 并且满足

$$r\varphi(m) = \varphi(rm)$$

对任意 $r \in R, m \in M_1$ 成立.

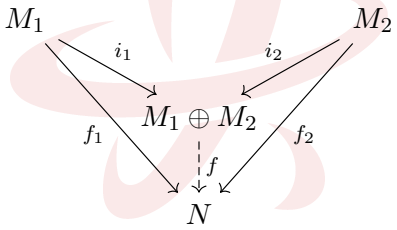
*注记.* $R$-模同态 $\varphi$ 是单（满，同构，自同构）的, 如果 $\varphi$ 作为群同态是单（满，同构，自同构）的. $R$-模同态的核 (像) 定义为它作为群同态的核 (像).

**例子.** *给定 $R$-模 $M$ 以及 $M$ 的子模 $N$, 如果考虑 $M/N$ 上自然的 $R$-模结构, 此时投影映射 $\pi : M \to M/N$ 是 $R$-模同态.*

**例子.** *给定 $R$-模 $M_1, M_2$ 以及 $R$-模同态 $\varphi$, 此时 $\ker\varphi$ 是 $M_1$ 的子模, $\operatorname{im}\varphi$ 是 $M_2$ 的子模.*

我们有如下与群论/环论中平行的结果:

**命题 10.1.7.** *给定 $R$-模同态 $f_1 : M_1 \to N, f_2 : M_2 \to N$, 那么存在唯一的 $R$-模同态 $f : M_1 \oplus M_2 \to N$ 使得下图交换:*




**命题 10.1.8.** *给定 $R$-模 $M_1, M_2$ 以及 $R$-模同态 $\varphi : M_1 \to M_2$.*

1. *如果 $R$-模 $N$ 满足 $N \subset \ker\varphi$, 那么存在唯一的 $R$-模同态 $\overline{\varphi}$ 使得下图交换:*
2. *$M_1/\ker\varphi \cong \operatorname{im}\varphi$*
3. *(对应定理) 如果 $\varphi$ 此时是满 $R$-模同态, 那么 $M_1$ 包含 $\ker\varphi$ 的子模与 $M_2$ 的子模一一对应.*

**定义 10.1.9.** 给定 $R$-模 $M$ 的子模 $M_1, M_2$, $M$ 称为 $M_1, M_2$ 的内直和, 如果满足

1. $M_1, M_2$ 生成 $M$;
2. $M_1 \cap M_2 = \{0\}$.

**命题 10.1.10.** *如果 $R$-模 $M$ 是子模 $M_1, M_2$ 的内直和, 那么有 $R$-模同构 $M \cong M_1 \oplus M_2$.*

**定义 10.1.11.** 给定 $R$-模 $M_1, M_2, M_3$ 以及 $R$-模同态 $\varphi : M_1 \to M_2, \psi : M_2 \to M_3$, 如下序列被称为在 $M_2$ 处正合 (exact)

$$M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3$$

如果 $\ker\psi = \operatorname{im}\varphi$.

**例子.** $\varphi: M_1 \to M_2$ 是满射当且仅当 $M_1 \xrightarrow{\varphi} M_2 \to 0$ 在 $M_2$ 处正合; $\varphi: M_1 \to M_2$ 是单射当且仅当 $0 \to M_1 \xrightarrow{\varphi} M_2$ 在 $M_1$ 处正合.

**例子.** 下述 $R$-模序列被称为一个短正合列, 如果下列序列在 $M_i, i = 1, 2, 3$ 处都正合:

$$0 \to M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \to 0$$

**定义 10.1.12.** 给定集合 $X$ 以及环 $R$, 定义

$$R^X := \{\sum_{x \in X} a_x x \mid a_x \in R, \text{ 只有有限多个 } a_x \text{ 非零.}\}$$

并且如下定义其上的 $R$-模结构:

$$\begin{cases} (\sum_{x\in X} a_x x) + (\sum_x b_x x) = \sum_{x\in X}(a_x + b_x)x \\ r(\sum_{x\in X} a_x x) = \sum_{x\in X}(ra_x)x \end{cases}$$

**命题 10.1.13.** 任何映射 $\varphi: X \to M$ 给出了一个 $R$-模映射 $\widetilde{\varphi}: R^X \to M$.

证明: 考虑

$$\begin{aligned} \widetilde{\varphi}: R^X &\to M \\ \sum_{x\in X} a_x x &\to \sum_{x\in X} a_x \varphi(x) \end{aligned}$$

□

**定义 10.1.14.** $R$-模 $M$ 被称为自由模 (free module), 如果存在某个集合 $X$ 使得 $M \cong R^X$ 作为 $R$-模同构. 特别地, $M$ 被称为有限生成自由模 (finitely generated free module), 如果 $X$ 是有限集.

**定义 10.1.15.** 给定 $R$-模 $M$, $M$ 的子集 $B$ 称为 $M$ 的基, 如果:

1. $M$ 由 $B$ 生成, 即任取 $m \in M, m = \sum_{b\in B} r_b b$, 其中 $r_b \in R$ 并且只有有限多个 $b$ 不是零;
2. $B$ 是 $R$-线性无关的, 即如果 $0 = \sum_{b\in B} r_b b$, 则 $r_b = 0$.

**命题 10.1.16.** 给定 $R$-模 $M$ 以及其的基 $B$, 那么有如下同构

$$\begin{aligned} R^B &\to M \\ b &\mapsto b \end{aligned}$$

特别地如果 $|B| = n$, 那么 $M \cong R^n$.

证明: 基的第一个条件保证了满射, 第二个条件保证了单射. □

注记. 上面的命题告诉我们, $R$-模 $M$ 是自由模当且仅当其存在一组基; $R$-模 $M$ 是有限生成自由模当且仅当其存在一组有限基.

当 $R$ 是域的时候不难看出此时有限生成自由 $R$-模就是有限维线性空间, 并且我们知道对于有限维线性空间来说其维数就已经完全决定了它本身. 那么现在一个自然的问题就是, 对于有限生成自由模来说, 如果 $B, C$ 都是它的基, 那么我们是否有 $|B| = |C|$ 呢? 为了解决这个问题, 我们需要借助取值在一般环上的矩阵, 并借助这个工具来研究我们的问题.

环 $R$ 上的矩阵定义为

$$M_{m\times n}(R) := (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$$

其中 $a_{ij}\in R$, 为了方便我们记 $M_{n\times n}(R)$ 为 $M_n(R)$. 与域上的矩阵类似, 我们有如下的事情:

1. 矩阵乘法与之前相同, 并且此时矩阵乘法也具有结合律, 因为我们的环 $R$ 具有结合律;
2. 我们可以同样地定义行列式映射

$$\det : M_n(R)\to R$$

并且也满足 $\det(AB)=\det A\cdot\det B$ 对任意 $A,B\in M_n(R)$ 成立;

3. 对于 $A\in M_n(R)$, 我们可以同样地定义伴随矩阵 $A^*$, 并且满足 $A^*A=AA^*=\det A\cdot I_n$.

**定义 10.1.17.** 矩阵 $A\in M_{m\times n}(R)$ 被称为可逆 (invertible), 如果存在 $B\in M_{n\times m}(R)$ 使得 $AB=I_m$ 以及存在 $C\in M_{m\times n}(R)$ 使得 $CA=I_n$.

**命题 10.1.18.** *如果 $A\in M_{m\times n}(R)$ 可逆, 此时一定有 $m=n$, 并且 $A$ 可逆当且仅当 $\det A\in R^\times$, 此时 $B=C=(\det A)^{-1}A^*$.*

*证明:* 取 $R$ 的一个极大理想 $I$, 此时 $R/I$ 是一个域. 对 $AB=I_m, CA=I_n$ 中的分量做商, 在 $R/I$ 中考虑等式

$$\overline{AB}=I_m,\quad \overline{CA}=I_n$$

根据线性空间的结果我们可知 $m=n$.

现在假设 $A\in M_n(R)$ 是可逆的, 则 $1=\det I_m=\det A\cdot\det B$ 意味着 $\det A\in R^\times$; 另一方面, 对 $B=C=(\det A)^{-1}I_n$ 直接验证 $AB=CA=I_n$. □

**定义 10.1.19.** 环 $R$ 上的一般线性群定义为 $\mathrm{GL}_n(R):=\{R\in M_n(R)\mid R\text{ 可逆.}\}$.

## 10.2 十一月十六

这节课我们首先来解决上次遗留的问题: 有限生成自由 $R$-模 $M$ 来说, 如果 $B,C$ 都是它的基, 那么我们是否有 $|B|=|C|$ 呢? 这实际上要考虑两个不同的基之间该如何转换.

**定义 10.2.1.** 给定有限生成自由 $R$-模 $M$ 以及其一组基 $B=\{b_1,\dots,b_n\}$, 由于任意 $v\in M$ 可以被唯一写成 $v=\sum_{i=1}^n v_ib_i$, 我们称如下列向量为 $v$ 在基 $B$ 下的坐标:

$$[v]_B := \begin{pmatrix} v_1\\ \vdots\\ v_n\end{pmatrix}$$

现在假设 $M$ 的任何一个有限子集 $C=\{c_1,\dots,c_m\}$, 以及 $B$ 是 $M$ 的一组基, 我们有:

**命题 10.2.2.** *$([c_1]_B,\dots,[c_m]_B)=P$ 可逆当且仅当 $C$ 是 $M$ 的一组基. 特别地, $M$ 的任何两组基有相同的元素个数.*

证明: 为了方便起见我们用 $(b_1,\dots,b_n)[c_i]_B$ 去记:

$$c_i=\sum_{j=1}^{n}[c_i]_B^j b_j$$

其中 $[c_i]_B^j$ 是 $[c_i]_B$ 的第 $j$-行. 利用这种记号, 我们可以记 $(c_1,\dots,c_m)=(b_1,\dots,b_n)P$.

假设 $P$ 可逆, 即此时 $m=n$, 并且存在 $Q\in M_n(R)$ 使得 $PQ=I_n$, 那么:

$$\begin{aligned}(c_1,\dots,c_n)Q&=((b_1,\dots,b_n)P)Q\\&=(b_1,\dots,b_n)(PQ)\\&=(b_1,\dots,b_n)\end{aligned}$$

从而:

1. 任取 $v\in M$, $v=(b_1,\dots,b_n)[v]_B=(c_1,\dots,c_n)(Q[v]_B)$, 即 $M$ 可由 $C$ 生成;
2. $0=(b_1,\dots,b_n)[0]_B=(c_1,\dots,c_n)(Q[0]_B)$, 由于 $[0]_B$ 是全零组成的列向量, 从而 $Q[0]_B$ 也是.

综上所述 $C$ 此时是 $M$ 的一组基.

假设 $B,C$ 都是 $M$ 的基, 那么

$$\begin{aligned}(c_1,\dots,c_m)&=(b_1,\dots,b_n)=P\\(b_1,\dots,b_n)&=(c_1,\dots,c_n)=Q\end{aligned}$$

从而有

$$\begin{aligned}(c_1,\dots,c_m)&=(c_1,\dots,c_m)QP\\(b_1,\dots,b_n)&=(b_1,\dots,b_n)PQ\end{aligned}$$

从而 $QP=I_m,PQ=I_n$, 从而此时 $P,Q$ 可逆, 并且 $m=n$. □

上面的结果告诉我们有限生成自由模的基的大小是良定义的, 即如果 $R^m\cong R^n$, 那么一定有 $m=n$. 我们利用的工具是 $R$ 上的矩阵, 这与线性空间情形我们所做的事情几乎完全一致. 实际上, 我们完全可以通过一些约化将这个问题重新回归到线性代数的情形.

给定环 $R$ 的一个理想 $I$ 以及一个 $R$-模 $M$, 那么

$$IM:=\{\sum_{i=1}^{n}r_im_i\mid r_i\in I,m_i\in M\}$$

是 $M$ 的一个子模. 特别地, 如果 $I$ 是一个主理想 $(a)$, 此时 $IM=aM=\{am\mid m\in M\}$. 在 $M/IM$ 上有一个自然的 $R/I$-模结构, 并且不难发现作为 $R/I$-模我们有如下同构:

$$(M_1\oplus M_2)/I(M_1\oplus M_2)\cong M_1/IM_1\oplus M_2/IM_2$$

其中 $M_1,M_2$ 是 $R$-模.

**推论 10.2.3.** 给定环 $R$, 如果 $R^m\cong R^n$, 那么 $m=n$.

证明: 取 $R$ 的极大理想 $I$, 那么有作为 $R/I$-模我们有

$$(R/I)^n \cong R^n/IR^n \cong R^m/IR^m \cong (R/I)^m$$

然而 $R/I$ 是一个域, 从而

$$(R/I)^n \cong (R/I)^m$$

是作为线性空间的同构, 从而 $m = n$. □

总而言之, 有限生成自由模的结构总是简单的. 事实上, 我们更关心那些有限生成模的结构.

**定义 10.2.4.** $R$-模 $M$ 被称为是有限生成的 (finitely generated), 如果存在一个有限生成模 $R^n$ 以及如下满同态

$$R^n \xrightarrow{\varphi} M \to 0$$

即 $M \cong R^n/\ker\varphi$.

注意到有限生成自由模的子模并不一定有限生成, 从而 $\ker\varphi$ 一般来说可能会很复杂. 现在我们期待一个比较好的条件, 使得此时的 $\ker\varphi$ 都是有限生成模.

**命题 10.2.5.** *对于环 $R$ 来说, 如下条件等价:*

1. *没有严格递增的理想序列*
$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$
*其中 $I_i$ 都是 $R$ 的理想;*
2. *$R$ 的任何理想都是有限生成的;*
3. *任何有限生成 $R$-模的子模都是有限生成的.*

*满足上述条件之一的环被称为诺特环 (noetherian ring).*

证明: (1) 到 (2). 假设 $I$ 不是有限生成的, 任取 $a_1 \in I$, 则 $(a_1) \subsetneq I$, 取 $a_2 \in I\backslash(a_1)$, 从而 $(a_1) \subsetneq (a_1, a_2) \subsetneq I$. 不断重复上述操作则可以得到一个理想的严格升链.

(2) 到 (1). 任给一个理想序列 $I_1 \subset I_2 \subset \dots$, 考虑 $I = \bigcup_{i=1}^{\infty} I_i$, 由于 $I$ 是有限生成的, 这意味着存在 $a_1, \dots, a_n \in I$ 使得 $I = (a_1, \dots, a_n)$. 并且不难发现存在足够大的 $N$ 使得 $a_1, \dots, a_n \in I_N$, 这意味着这个理想升链到 $I_N$ 时已经稳定, 即不是严格上升.

(3) 到 (2). 注意到 $R$ 作为 $R$-模的子模恰是 $R$ 的理想;

(2) 到 (3). 首先我们有如下观察:

1. 对于正合列 $M_1 \xrightarrow{\varphi} M_2 \to 0$, 如果 $M_1$ 是有限生成的, 那么 $M_2$ 也是. 这是显然的, 因为 $M_1$ 是有限生成的等价于存在满射 $R^n \to M_1$, 只需要复合 $\varphi$ 即可得到 $R^n$ 到 $M_2$ 的满射;
2. 对于短正合列 $0 \to M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\psi} M_3 \to 0$, 如果 $M_1, M_3$ 都是有限生成的, 那么 $M_2$ 也是. 假设 $M_3$ 由 $v_1, \dots, v_n$ 生成, 那么选取 $\overline{v}_1, \dots, \overline{v}_n$ 使得 $\psi(\overline{v}_i) = v_i, 1 \le i \le n$. 假设 $M_1$ 由 $w_1, \dots, w_m$ 生成, 并且记 $\widetilde{w}_i = \varphi(w_i)$. 任取 $\widetilde{v} \in M_2$, 记 $\psi(\widetilde{v}) = \sum_{i=1}^n r_i v_i$, 那么
$$\psi(\widetilde{v} - \sum_{i=1}^n r_i \widetilde{v}_i) = 0$$
从而 $\widetilde{v} - \sum_{i=1}^n r_i\widetilde{v}_i \in \ker\psi = \operatorname{im}\varphi$, 即 $\widetilde{v} - \sum_{i=1}^n r_i\widetilde{v}_i = \sum_{j=1}^m s_j\widetilde{w}_j$. 即 $M_2$ 可由 $\widetilde{v}_1, \dots, \widetilde{v}_n, \widetilde{w}_1, \dots, \widetilde{w}_m$ 生成.

根据上述观察, 我们做以下约化:

1. 根据对应定理以及观察 (1), 我们只需要对有限生成自由模 $R^n$ 证明其所有的子模都是有限生成的即可.
2. 注意到我们有如下的短正合列:

$$0 \to R^{n-1} \to R^n \to R \to 0$$

3. 利用归纳, 我们只需要证明 $R$ 作为 $R$-模的子模都是有限生成的即可, 然而这恰是 (2).

□

**命题 10.2.6.** *如果 $R$ 是诺特环, 则对任意理想 $I$ 有 $R/I$ 是诺特环.*

**定理 10.2.7.** *如果 $R$ 是诺特环, 则 $R[x]$ 是诺特环.*

**例子.** *$R$ 是主理想整环, 则 $R$ 是诺特环.*

现在如果 $R$ 是诺特环, $M$ 是有限生成 $R$-模, 即存在如下正合列:

$$\ker\varphi \to R^n \xrightarrow{\varphi} M \to 0$$

并且此时 $\ker\varphi$ 是有限生成的, 从而存在满态射 $R^m \to \ker\varphi$, 即我们可以写作正合列:

$$R^m \xrightarrow{\psi} R^n \xrightarrow{\varphi} M \to 0$$

并且 $M \cong R^n/\operatorname{im}\psi$. 如果我们能对态射 $\psi$ 有很好的刻画, 那么我们就可以对诺特环上的有限生成模有一个较好的刻画.

给定 $R^n$ 的一组基 $B = \{b_1, \dots, b_n\}$ 以及 $R^m$ 的一组基 $C = \{c_1, \dots, c_m\}$, 我们可以将 $\psi$ 写成矩阵的形式, 即:

$$(\psi(c_1), \dots, \psi(c_m)) = (b_1, \dots, b_n)A$$

其中 $A = (a_{ij})$ 由如下关系给出:

$$\psi(c_j) = \sum_{i=1}^{n} a_{ij} b_i$$

为了表示 $A$ 对于基 $B, C$ 的依赖性, 我们通常也记做 $[\psi]_B^C := A$. 如果我们能够选取 $R^n, R^m$ 合适的基 $B, C$, 使得矩阵 $[\psi]_B^C$ 有尽可能简单的形式, 从而我们可以得到我们期待的结果. 幸运的是, 当 $R$ 是主理想整环的时候, 确实有如此好的事情.

*注记.* 由于 $\psi \circ \varphi = 0$, 从而

$$\sum_{i=1}^{n} a_{ij}\psi(b_i) = 0$$

并且由于 $\{\psi(b_1), \dots \psi(b_n)\}$ 生成了 $M$, 因此我们可以将 $M$ 视作是由 $\{\psi(b_1), \dots \psi(b_n)\}$ 生成, 并且满足上述关系.

# 第十一章　第十一周

## 11.1　十一月二十二

在本节中, 如果不加特殊说明, $R$ 都是指主理想整环.

**定理 11.1.1.** 给定 $R$-模同态 $\psi : R^m \to R^n$, 我们可以选出 $R^m, R^n$ 的基使得 $\psi$ 在这些基下的表达式为

$$[\psi]_B^C = \left[\begin{array}{cccc|ccc} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_s & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right]_{n\times m}$$

其中 $d_1 \mid d_2 \mid \cdots \mid d_s$.

**推论 11.1.2.** 如果 $M$ 是有限生成 $R$-模, 则

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_s) \oplus R^{n-s}$$

其中 $d_1 \mid d_2 \mid \cdots \mid d_s$.

**定理 11.1.3.** 给定有限生成 $R$-模 $M$, 如果 $(d_1) \neq R$, 我们有 $d_1, \ldots, d_s$ 被 $M$ 完全决定. 此时 $(d_1, \ldots, d_s)$ 称为 $M$ 的不变因子组.

**例子.** $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$, 即此时 $d_1 = 6$.

**例子.** $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$, 此时 $d_1 = 3, d_2 = 18$.

定理11.1.1的证明. 首先给定 $R^n, R^m$ 的基 $B, C$, 并且令 $B' = BP, C' = CQ$, 那么有

$$[\psi]_{B'}^{C'} = P^{-1}[\psi]_B^C Q$$

这是 $\psi$ 在基变换下的变换公式. 回忆我们在线性空间的时候, 我们可以通过初等行列变换来得到矩阵的相抵标准型, 这里我们要做类似的事情. 给定矩阵非零矩阵

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & & \\ \vdots & & \end{pmatrix}$$

首先我们假设 $R$ 是欧几里德整环, 其上的带有的函数记做 $\sigma$.

1. 第一步: 通过变换行与列, 我们可以选取 $a_{11}$ 使得 $\sigma(a_{11}) = \min_{i,j}\{\sigma(a_{ij}) \mid a_{ij} \neq 0\}$
2. 第二步: 通过带余除法, 我们可以做到 $\sigma(a_{1i}) < \sigma(a_{11}), \sigma(a_{1j}) < \sigma(a_{11})$, 对任意的 $i = 2, \ldots, m, j = 2, \ldots, n$.
3. 此时再重复上述一、二两个步骤, 经过有限次行列变换之后, 我们可以得到 $a_{11} \neq 0, a_{1i} = a_{1j} = 0$, 对任意的 $i = 2, \ldots, m, j = 2, \ldots, n$ 成立. 即此时有:
$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$
4. 第三步: 此时我们需要 $a_{11}$ 可以整除右下角的 $(n-1) \times (m-1)$ 阶的子矩阵中每一个元素. 如果不然, 不妨假设 $a_{11} \nmid a_{i2}$, 我们不妨将第 $i$ 行加到第一行得到
$$\begin{pmatrix} a_{11} & a_{i2} & \ldots & a_{in} \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$
此时再重复第一、二步即可.
5. 通过归纳假设, 我们可以得到经过有限次行列变换之后, $A$ 的相抵标准型为我们期待的结果.

对于 $R$ 是主理想整环的时候, 我们不能再进行辗转相除法, 但是整体上的思路是几乎一致的:

1. 第一步: 通过变换行与列, 我们可以选取 $a_{11} \neq 0$.
2. 第二步: 当 $i \geq 2$ 时, 我们考虑如下两种情况:
   (a) 如果 $(a_{1i}) \subset (a_{11})$, 那么直接通过行列变换将 $a_{1i}$ 消去;
   (b) 如果 $(a_{1i}) \subsetneq (a_{11})$, 那么考虑 $(a_{11}, a_{1i})$ 生成的主理想 $(d)$, 此时有
   $$d = ka_{11} + la_{1i}$$
   $$a_{11} = md$$
   $$a_{1i} = nd$$
   其中 $k, l, m, n \in R$. 考虑 $A$ 右乘 $B$, 其中 $B$ 是 $(1,1), (1,i), (i,1), (i,i)$ 元分别为 $k, -n, l, m$, $j \neq 2$ 的时候 $(j,j)$ 元为 1, 其余都为零的可逆矩阵. 如果用 $A'$ 去记这个新得到的矩阵, 即 $a'_{11} = d$, 那么我们有 $(a'_{11}) \supsetneq (a_{11})$. 如果还存在 $i \geq 2$ 使得 $(a'_{1i}) \subsetneq (a'_{11})$, 则不断重复上述操作, 由于升链总会稳定, 因此在有限步行列变换之后我们一定可以得到一个矩阵, 使得第一行除了 $(1,1)$ 元以外都是零; 同样的可以对列做同样的事情, 最终可以得到
   $$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

3. 第三步: 同之前.

□

注记. 在主理想整环证明的情形, 我们实际上也可以找一个函数来替代欧几里德整环情形下的 $\sigma$: 给定 $r \in R$, 我们用 $\sigma(r)$ 记 $r$ 的素因子分解中的素因子个数. 此时我们需要一个类似辗转相除的操作来使得进行这个操作后得到的元素满足函数 $\sigma$ 在其上的值严格小于操作前. 这实际上是我们在第二步 $(b)$ 中的操作: 假设 $(a_{1i}) \subsetneq (a_{11})$, 我们可以找到一个可逆矩阵 $B'$ 使得 $AB'$ 的 $(1,i)$ 元为 $a_{1i}, a_{11}$ 的最大公因子 $d$, 显然 $d$ 的素因子分解的素因子个数严格小于 $a_{1i}$, 这便达成了我们的要求.

**定义 11.1.4.** 如果 $R$ 是一个整环, 给定 $R$-模 $M$, 其挠子模 (torsion submodule)定义为:

$$M_{tor} := \{m \in M \mid \text{存在 } r \in R\backslash\{0\} \text{ 使得 } rm = 0\}$$

注记. 可以根据定义直接验证 $M_{tor}$ 是一个子模.

给定一个有限生成 $R$-模 $M$, 首先我们可以将其分解为

$$M = R/(d_1) \oplus \cdots \oplus R/(d_s) \oplus R^{n-s}$$

我们现在的目的在于说明如果 $(d_1) \neq R$, $d_1, \ldots, d_s$ 是被 $M$ 唯一决定的. 首先从上述同构可以看出 $M_{tor} \cong R/(d_1) \oplus \cdots \oplus R/(d_s)$, 即我们有如下短正合列:

$$0 \to M_{tor} \to M \to R^{n-s} \to 0$$

此时我们有 $s$ 是内蕴的, 即 $s$ 由 $M$ 唯一决定. 为了想要进一步说明 $d_1, \ldots, d_s$ 都由 $M$ 决定, 我们需要考虑更精细的结构.

## 11.2 十一月二十三

在本节中, 如果不加特殊说明, $R$ 都是指主理想整环.

**定义 11.2.1.** 给定一般的环 $R$, $R$-模 $M$ 被称为循环模 (cyclic module), 如果存在下述正合列:

$$R \to M \to 0$$

**命题 11.2.2.** *假设 $R$-模 $M$ 是循环模, 则有如下分解*

$$M \cong R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_k^{n_k})$$

*其中 $p_1, \ldots, p_k$ 是互不相同的素元.*

*证明:* 由于 $R$-模 $M$ 是循环模, $R$ 是主理想整环, 从而 $M \cong R/(d), d \neq 0$, 将 $d$ 做如下分解:

$$d = p_1^{n_1} \ldots p_k^{n_k}$$

其中 $p_1, \ldots, p_k$ 是不同的素元, 再利用中国剩余定理即可. □

现在回到我们的情况, 假设 $R$-模 $M$ 有如下同构

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_s)$$

我们可以对 $d_s$ 做如下分解:

$$d_s = p_1^{n_{1,s}} \dots p_k^{n_{k,s}}$$

其中 $n_{i,s} \geq 1, 1 \leq i \leq k$. 由于有整除关系，我们可知对任意的 $1 \leq r \leq s$, 我们有

$$d_r = p_1^{n_{1,r}} \dots p_k^{n_{k,r}}$$

其中 $0 \leq n_{i,1} \leq \cdots \leq n_{i,r} \leq \cdots \leq n_{i,s}, 1 \leq i \leq k$. 从而我们有如下分解

$$\begin{aligned} M \cong \quad & R/(p_1^{n_{1,1}}) \oplus \cdots \oplus R/(p_k^{n_{k,1}}) \\ & \oplus R/(p_1^{n_{1,2}}) \oplus \cdots \oplus R/(p_k^{n_{k,2}}) \\ & \cdots \\ & \oplus R/(p_1^{n_{1,s}}) \oplus \cdots \oplus R/(p_k^{n_{k,s}}) \end{aligned} \tag{11.2.1}$$

我们称 $\{p_i^{n_{i,r}} \mid n_{i,r} \geq 1\}$ 为 $M$ 的初等因子.

**命题 11.2.3.** *给定 $R$-模 $M$, 其初等因子组与不变因子组之间可以相互决定.*

*证明:* 与线性代数的时候情形相同. □

**定义 11.2.4.** $R$ 是一个整环, 给定环 $R$ 的一个素元 $p$ 以及 $R$-模 $M$, 其 $p$-挠子模 ($p$-torsion submodule)定义为:

$$M_{(p)} := \{m \in M \mid \text{存在 } n \in \mathbb{Z}_{\geq 1} \text{ 使得 } p^n m = 0\}$$

*注记.* 可以根据定义直接验证 $M_{(p)}$ 是一个子模.

**命题 11.2.5.** *分解11.2.1可以被写成*

$$M \cong M_{(p_1)} \oplus \cdots \oplus M_{(p_s)}$$

*证明:* 任取 $m = m_1 + \cdots + m_s$, 其中 $m_i \in R/(p_i^{n_{i,1}}) \oplus \cdots \oplus R/(p_i^{n_{i,s}})$. 如果 $m \in M_{(p_1)}$, 那么存在 $n \in \mathbb{Z}_{\geq 1}$ 使得

$$p_1^n m = 0$$

这意味着 $p_1^n m_i = 0$ 对每一个 $i$ 都成立. 现在假设 $i \geq 2$, 我们把 $m_i$ 更详细的写成 $m_i = m_{i,1} + \cdots + m_{i,s}$, 其中 $m_{i,r} \in R/(p_i^{n_{i,r}})$. 那么有

$$p_1^n (m_{i,1} + \cdots + m_{i,s}) = 0$$

意味着 $p_1^n m_{i,r} = 0$ 对 $1 \leq r \leq s$ 都成立. 由于 $p_1$ 和 $p_i, i \geq 2$ 互素可知 $m_{i,r} = 0$, 即此时有 $m \in R/(p_1^{n_{1,1}}) \oplus \cdots \oplus R/(p_1^{n_{1,s}})$, 即

$$M_{(p_1)} \subseteq R/(p_1^{n_{1,1}}) \oplus \cdots \oplus R/(p_1^{n_{1,s}})$$

反包含关系是显然的, 从而我们有

$$M_{(p_1)} = R/(p_1^{n_{1,1}}) \oplus \cdots \oplus R/(p_1^{n_{1,s}})$$

即

$$M \cong M_{(p_1)} \oplus \cdots \oplus M_{(p_s)}$$

□

上述结果表明 $M$ 的初等因子组可以由 $M_{(p_i)}$ 的分解来决定, 那么问题在于我们如何确定出每一个 $M_{(p_i)}$ 该如何分解呢?

例如我们先考虑下述简单的例子:

$$M \cong \mathbb{Z}/(p^2) \oplus \mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$$

其中 $p$ 是一个素数. 我们现在想定义一个内蕴的量来区分 $p$ 和 $p^2$, 自然的想法如下:

**定义 11.2.6.** $R$ 是一个一般的环, $p$ 是 $R$ 的一个素元, $M$ 是一个 $R$-模, 我们定义如下子模

$$M[p] := \{m \in M \mid pm = 0\}$$

并且不难发现 $M[p]$ 上存在 $R/(p)$-模结构.

特别地, 当 $R$ 是主理想整环, $p$ 是 $R$ 的素元时, $R/(p)$ 是一个域, 即此时 $M[p]$ 是一个线性空间, 并且

$$\dim_{R/(p)} M[p]$$

完全由 $M$ 本身决定, 例如在上面的例子中, 可以直接看出 $M[p] = \mathbb{Z}/(p) \oplus \mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$, 此时 $M[p]$ 作为 $\mathbb{Z}/(p)$-线性空间的维数为 3.

**命题 11.2.7.** *假设 $R$-模 $M$ 同构于*

$$M \cong R/(p^{n_1}) \oplus \ldots R/(p^{n_s})$$

*其中 $p$ 是 $R$ 的素元, $n_1 \leq \cdots \leq n_s$, 那么 $M[p] \cong (R/(p))^{\oplus s}$.*

到这里实际上我们几乎已经解决了我们的问题. 类似地我们可以定义 $M[p^2]$ 等等, 从 $M \cong \mathbb{Z}/(p^2) \oplus \mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$ 我们可以看出 $\dim_{\mathbb{Z}/(p)} M$ 确定了 $\geq 1$ 的 $n_r$ 的个数, 同样的 $\dim_{\mathbb{Z}/(p^2)} M$ 确定了 $\geq 2$ 的 $n_r$ 的个数.

因此对于 $R$-模 $M$, 如果我们想要确定其初等因子组 $\{p_i^{n_{i,r}} \mid n_{i,r} \geq 1\}$, 我们只要对每一个可能的 $p_i$ 不断计算 $M[p_i], M[p_i^2], \ldots$ 的维数, 我们就可以从 $M$ 确定其初等因子组. 再由于初等因子组可以唯一确定不变因子组, 至此我们证明了定理11.1.3.

至此我们已经证明了主理想整环上的有限生成模的结构定理, 现在我们来看一看它的众多重要的推论.

**定义 11.2.8.** 如果 $R$ 是一个整环, $R$-模 $M$ 被称为无挠的, 如果 $M_{tor} = 0$.

**推论 11.2.9.** *$M$ 是有限生成 $R$-模, $R$ 是主理想整环[1], 则 $M$ 无挠等价于 $M$ 自由.*

**推论 11.2.10** (有限阿贝尔群的结构定理)**.** *$M$ 是有限生成阿贝尔群, 则有*

$$M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \oplus \mathbb{Z}^l$$

*其中 $2 \leq d_1 \mid \cdots \mid d_s, l \geq 0$, 并且这些数由 $M$ 唯一决定.*

另一个重要的应用就是用这个观点重新看我们在线性代数中所学过的事情. $\mathbb{F}$ 是一个域, 给定有限维 $\mathbb{F}$-线性空间 $V$ 以及其上的线性变换 $T$, 我们如下给 $V$ 一个 $\mathbb{F}[x]$-模结构:

$$\begin{aligned} \mathbb{F}[x] \times V &\to V \\ (f(x), v) &\mapsto f(T)v \end{aligned}$$

记做 $(V, T)$. 此时 $V$ 作为 $\mathbb{F}[x]$-模也是有限生成的. 对于另一个线性变换 $T'$, 称 $(V, T)$ 和 $(V, T')$ 是等价的, 如果他们作为 $\mathbb{F}[x]$-模是同构的.

**命题 11.2.11.** *如果记 $T, T'$ 在 $V$ 的一组基 $B$ 下的矩阵表示分别为 $[T]_B, [T']_B$, 那么 $(V, T)$ 于 $(V, T')$ 等价当且仅当 $[T]_B$ 和 $[T']_B$ 相似.*

*证明:* 根据定义直接验证. □

**推论 11.2.12.** *我们有如下一一对应:*

$$\{\text{域 } \mathbb{F} \text{ 上 } n \text{ 阶矩阵的相似类}\} \overset{1-1}{\Longleftrightarrow} \{\dim_{\mathbb{F}} V = n, V \text{ 上 } \mathbb{F}[x]\text{-模结构的同构类}\}$$

现在我们只需要应用我们的结构定理去给出 $\mathbb{F}[x]$-模同构类的情况, 从而给出 $n$ 阶矩阵相似类的情况. 先给定 $V$ 的一组基 $B = \{v_1, \ldots, v_n\}$, 并用矩阵 $[T]_B$ 来记 $T$ 在这组基下的矩阵. 由于作为 $\mathbb{F}$-模, $V$ 可以由 $B$ 生成, 从而作为 $\mathbb{F}[x]$-模, $V$ 也可以由 $B$ 生成. 由于

$$x \cdot (v_1, \ldots, v_n) = (v_1, \ldots, v_n)\,[T]_B$$

从而我们有

$$\left(xI - [T]_B^t\right) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = 0$$

其中 $[T]_B^t$ 表示 $[T]_B$ 的转置. 这是 $V$ 作为 $\mathbb{F}[x]$-模生成元所满足的关系. 根据注记10.2, 我们可知只要将 $\left(xI - [T]_B^t\right)$ 通过行列变换化为

$$\left[\begin{array}{cccc|ccc} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_s & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right]$$

[1]虽然在本节开头已经声明如无特殊声明 $R$ 都是主理想整环, 但在这里我们还是依然强调这个事实.

的形式, 则有 $V$ 作为 $\mathbb{F}[x]$-模同构于

$$\mathbb{F}[x]/(d_1) \oplus \cdots \oplus \mathbb{F}[x]/(d_s) \oplus (\mathbb{F}[x])^{n-s}$$

其中 $d_1|\cdots|d_s$ 是首一多项式. 由于 $\mathbb{F}[x]$ 作为 $\mathbb{F}$-线性空间是无穷维的，而 $V$ 作为 $\mathbb{F}$-线性空间是有限维的, 从而一定有 $n=s$. 即作为 $\mathbb{F}[x]$-模有如下同构

$$V \cong \mathbb{F}[x]/(d_1) \oplus \cdots \oplus \mathbb{F}[x]/(d_n)$$

需要注意的是某些 $d_i$ 可能为常多项式, 此时 $\mathbb{F}[x]/(d_i)=0$. 我们将这些平凡的因子除去再重新标号, 不妨假设 $\{d_i\}_{i=1}^k, 1 \le k \le n$ 是非常数的多项式.

这些 $\{d_i\}_{i=1}^k$ 就是在线性代数中所学到的线性变换 $T$ 的不变因子组. 不妨假设 $d_i = x^{n_i} + a_{n_i-1}x^{n_i-1} + \cdots + a_0$, 那么 $\mathbb{F}[x]/(d_i)$ 视作 $\mathbb{F}$-线性空间有一组基 $\left\{1, x, \ldots, x^{n_i-1}\right\}$, 并且

$$T\left(1, x, \ldots, x^{n_i-1}\right) = \left(1, x, \ldots, x^{n_i-1}\right) A_i$$

其中 $A_i$ 是 $d_i$ 的友阵. 因此我们可以找到 $V$ 的一组基使得 $T$ 在这组基下的矩阵为分块对角矩阵 $\operatorname{diag}\{A_1, \ldots, A_k\}$, 其中 $A_i$ 是 $d_i$ 的友阵, 这叫作 $T$ 的有理标准型.

# 索引