近世代数

孙天阳

2022 年 9 月 10 日

目录

Chapter 1

环论

1 集合与映射

- 单射、满射与双射这些概念与集合上的其他结构无关.
- $x \in [a] \Longrightarrow [a] = [x]$.
- $[a] \cap [b] \neq \varnothing \Longrightarrow [a] = [b]$.
- 映射基本定理

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, two heads, "\pi"'] & Y \\ X/\overset{f}{\sim} \arrow[r, "\bar{f}"] & \mathrm{Im}(f) \arrow[u, hook, "\iota"'] \end{tikzcd}$$

例 1.1 (包含映射)**.**

$$\iota : A \hookrightarrow B, x \mapsto x$$

定义 1.2. $f : X \to Y, f' : X' \to Y'$,$f$ 和 f' 相等是指 $X = X', Y = Y'$ 且任意 $x \in X$,$f(x) = f'(x)$.

定义 1.3 (单射、满射与双射)**.**

- $f : X \to Y$ 称为单射, 若对 $x, x' \in X$,$f(x) = f(x')$, 总有 $x = x'$, 记作 $\hookrightarrow$.
- $f : X \to Y$ 称为满射, 若任意 $y \in Y$, 存在 $x \in X$, 使得 $f(x) = y$, 记作 $\twoheadrightarrow$.
- $f : X \to Y$ 称为双射, 若 f 既单且满.

例 1.4. 设 $f : A \to B$ 是集合的映射,A 是非空集合. 试证:

(1) f 为单射 $\Leftrightarrow$ 存在 $g : B \to A$ 使得 $g \circ f = Id_A$

(2) f 为满射 $\Leftrightarrow$ 存在 $g : B \to A$ 使得 $f \circ h = Id_B$

(3) f 为双射 $\Leftrightarrow$ 存在 $g : B \to A$ 使得 $g \circ f = Id_A, f \circ g = Id_B$, 此时 g 是唯一的

例 1.5. 设 $f : A \to B$, 证明 f 是单射当且仅当对任意的

在已有的集合的基础上, 我们可以构造新的集合.

(1) $X \sqcup Y$, 无交并

(2) $X \times Y$

(3) $Map(X, Y) = \{f : X \to Y\}$

(4) $\mathcal{P}(X) = \{A \subset X\}$

注记.

$$Map\,(X, \{0,1\}) \xrightarrow{\sim} \mathcal{P}(X)$$
$$\chi_A \mapsto A$$

注记.

$$Map(X \sqcup Y, Z) \xrightarrow{\sim} Map(X, Z) \times Map(Y, Z)$$

$$Map(Z, X \times Y) \xrightarrow{\sim} Map(Z, X) \times Map(Z, Y)$$

定义 1.6 (等价关系)**.** $X \neq \varnothing$,X 上的等价关系 $R \subset X \times X$, 满足

(1) $(x, x) \in R, \forall x \in X$

(2) $(x, y) \in R \Rightarrow (y, x) \in R$

(3) $(x, y) \in R, (y, z) \in R \Rightarrow (x, z) \in R$

若 $(x, y) \in R$, 记 $x \overset{R}{\sim} y$.

引理 1.7. 设 X 是非空集合,$\sim$ 是 X 上的等价关系, 对任意 $a, b \in X$ 只有两种情况

- $\bar{a} \cap \bar{b} = \varnothing$
- $\bar{a} = \bar{b}$

定义 1.8. X 关于 $\overset{R}{\sim}$ 的商集为

$$X/\overset{R}{\sim} := \left\{\text{等价类全体}\right\} \subset \mathcal{P}(X)$$

有一个典范的商映射

$$\pi : X \to X/\overset{R}{\sim}$$
$$a \mapsto [a]$$

定义 1.9. 关于 $\overset{R}{\sim}$ 的完全代表元系**:** $S \subset X$ 使得对任意的 $x \in X$, 存在唯一的 $s \in S$ 使得 $[s] = [x]$.
此时

$$S \overset{inc}{\hookrightarrow} X \overset{\pi}{\twoheadrightarrow} X/\overset{R}{\sim}$$

是双射! 此时

$$X = \bigsqcup_{s \in S} [s].$$

定义 1.10. 集合 X 的分析:

$$\left\{X_i \middle| i \in I\right\} \subset (x)$$

满足

(1) $X_i \neq \varnothing$

(2) $X_i \cap X_j = \varnothing, \forall i \neq j$

(3) $X = \bigsqcup_{i \in I} X_i$

定理 1.11. 设 $X \xrightarrow{f} Y$ 为满射, 考虑商集 $X/\sim$, 令 $\pi : X \longrightarrow X/\sim$ 为自然投射, 则存在唯一的双射 $\varphi : Y \longrightarrow X/\sim$ 使下列图表交换:

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\pi"'] & & Y \arrow[dl, dashed, "\exists! \varphi"] \\
& X/\sim &
\end{tikzcd}$$

定理 1.12 (映射基本定理). $f : X \to Y, \overset{f}{\sim}$ 为 X 上的由 f 给出的等价关系, 则 f 诱导双射

$$\begin{aligned}
\bar{f} : X/\overset{f}{\sim} &\to \operatorname{Im}(f) \\
[x] &\mapsto f(x)
\end{aligned}$$

$$\begin{tikzcd}
X \arrow[r] \arrow[d, two heads] & Y \\
X/\overset{f}{\sim} \arrow[r] & \operatorname{Im}(f) \arrow[u, hook]
\end{tikzcd}$$

X 上的二元运算:

$$\begin{aligned}
\Psi : X \times X &\to X \\
(x, y) &\mapsto \psi(x, y)
\end{aligned}$$

$$\begin{tikzcd}
X \times X \times X \arrow[r] \arrow[d] & X \times X \arrow[d] \\
X \times X \arrow[r] & X
\end{tikzcd}$$

2 含幺交换环

定义、性质和例子

定义 2.1. 称非空集合 R 为含幺交换环, 如果其上有两个二元运算 $+$ 和 $\cdot$, 满足:

(A1) 存在零元: 存在 $0_R \in R$ 使得 $a + 0_R = a, \forall\, a \in R$.

(A2) 存在逆元: 对任意 $a \in R$, 存在 $b \in R$, 使得 $a + b = 0_R$. 称 b 为 a 的逆元, 记为 $-a$.

(A3) 加法结合律: $(a + b) + c = a + (b + c)$.

(A4) 加法交换律: $a + b = b + a$.

(M1) 存在幺元: 存在 1_R 使得 $1_R \cdot a = a \cdot 1_R = a, \forall\, a \in R$.

(M2) 乘法结合律: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(M3) 乘法交换律: $a \cdot b = b \cdot a$.

(D) 分配律: $(a + b) \cdot c = a \cdot c + b \cdot c$.

如果只是前七个条件, 那么 R 只具有阿贝尔群 $(R, +)$ 和阿贝尔半群 $(R, \cdot)$ 两个彼此独立的代数结构. 正是分配律将这两个运算联系在一起, 从而形成新的代数结构——含幺交换环.

注记. 设 R 为含幺交换环, 则

- 零元唯一: $0_R = 0_R + 0'_R = 0'_R$.
- 逆元唯一: $b = b + a + b' = b'$. 从而可记作 $-a$.
- 幺元唯一: $1_R = 1_R 1'_R = 1'_R$.
- 因为加法满足结合律, 所以可定义 R 上的有限求和符号 $\sum_{i=1}^{n} a_i := a_1 + a_2 + \cdots + a_n$.
- $-(-a) = a$. 按定义验证.
- 整数与环中元素的乘法: $na := \begin{cases} 0a = 0_R \\ na = \underbrace{a + \cdots + a}_{n\text{个}} \\ (-n)a = \underbrace{(-a) + \cdots + (-a)}_{n\text{个}} \end{cases}$

例 2.2.

- 含幺交换环的例子:
  - 整数环 $\mathbb{Z}$
  - 同余类环 $\mathbb{Z}_n$
  - Gauss 整数环 $\mathbb{Z}[\sqrt{-1}] = \{m + n\sqrt{-1} \mid m, n \in \mathbb{Z}\}$
  - 有理系数多项式环 $\mathbb{Q}[x]$

- 含幺非交换环的例子：
  - 矩阵环 $M_n(\mathbb{F})$

例 2.3. 设 R 为含幺交换环, 则 $0_R = 1_R \iff R = \{0_R\} \iff R$ 仅有一个元素.

例 2.4. 二项式定理

整环

定义 2.5. 称含幺交换环 R 为整环, 如果 $ab = 0_R \Rightarrow a = 0_R$ 或 $b = 0_R$.

例 2.6.

(1) $\mathbb{Z}$ 是整环.

(2) $\mathbb{Z}_4$ 不是整环,$[2][2] = [0]$.

单位、单位群和域

定义 2.7. 设 R 是含幺交换环,$a \in R$, 若存在 $b \in R$ 满足 $a \cdot b = 1_R$, 则称 a 是 R 的可逆元或单位.

注记. 正是因为 R 是含幺交换环, 所以我们才不必考虑左逆与右逆的概念.

命题 2.8. 设 R 为含幺交换环, 则

- 逆元唯一：$b' = b'1_R = b'(ab) = (b'a)b = 1_Rb = b$
- $(1_R)^{-1} = 1_R$,$(-1_R)^{-1} = -1_R$
- 若 a 可逆, 则 a^{-1} 也可逆并且 $\left(a^{-1}\right)^{-1} = a$
- 若 a,b 都可逆, 则 ab 也可逆并且 $(ab)^{-1} = b^{-1}a^{-1}$
- 0_R 可逆 $\iff R$ 为零环
- 对于可逆元 a 可对任意 $n \in \mathbb{Z}$ 定义 a^n

定义 2.9 (R 的单位群)**.** $U(R) := \left\{u \in R \middle| u\text{可逆}\right\}$.

- $1_R \in U(R)$
- 若 $a \in U(R)$, 则 $a^{-1} \in U(R)$
- 若 $a,b \in U(R)$, 则 $ab \in U(R)$
- $U(R)$ 是 Abel 群

例 2.10.

(1) $U(\mathbb{Z}) = \{1, -1\}$

(2) $U(\mathbb{Q}) = \mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$

(3) $U(\mathbb{Z}_n) = \left\{[m] \middle| (m,n) = 1\right\}$

(4) $U(\mathbb{Z}[\sqrt{-1}]) = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$

注记. 消去律.

- 对一般的含幺交换环来说, 可逆元有消去律.
- 对整环来说, 非零元都有消去律.
- 但要注意二者的机理不同，前者是左右同乘逆元消去，后者是整环的性质迫使的.

定义 2.11. 称含幺交换环 R 为域, 如果 $U(R) = R^{\times}$.

例 2.12.

(1) $\mathbb{Z}$ 不是域

(2) $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ 都是域

命题 2.13. 域是整环.

整环与域

命题 2.14. $\mathbb{Z}_n$ 为整环 $\iff$ n 为素数 $\iff$ $\mathbb{Z}_n$ 为域.

证明.

- (1) $\implies$ (2) 假设 $n = ab$, 那么 $[a][b] = [n] = [0]$, 矛盾.
- (2) $\implies$ (3) Bezout 定理.
- (3) $\implies$ (1) 显然.

□

更一般地，我们有

命题 2.15. 设 R 是有限环, 那么它是整环当且仅当它是域.

证明. 只证充分性.

设非零元 a 不可逆, 那么对任意的元素 $b \in R$,$ab \neq 1_R$.

定义 R 上的一个变换 $\sigma : R \to R, b \mapsto ab$. 由上可知 σ 不是满射.

由于 R 是有限环, 则 σ 也不是单射. 因此存在 $b_1 \neq b_2$ 使得 $ab_1 = ab_2$.

也就是存在 $b_1 - b_2 \neq 0$ 使得 $a(b_1 - b_2) \neq 0$, 这与 R 是整环矛盾！ □

子环

定义 2.16. 设 R 是含幺交换环, $S \subset R$ 非空, 如果

(1) $1_R \in S$

(2) S 对减法和乘法封闭

那么 $(S, +, \cdot)$ 成为含幺交换环，称 S 为 R 的子环.

例 2.17. $2\mathbb{Z}$ 不是 $\mathbb{Z}$ 的子环，但 $2\mathbb{Z}$ 对加法、减法和乘法都封闭.

例 2.18. $\mathbb{Z}$ 没有真子环.

证明. $\square$

例 2.19. 分类 $\mathbb{Z}[\sqrt{-1}]$ 的子环.

定义 2.20. 设 K 是域, $S \subset K$ 是 K 的子环，如果对 $\forall\ a \in S \backslash \{0_S\}$ 有 $a^{-1} \in S$，那么 S 成为域，称 S 为 K 的子域.

例 2.21. $\mathbb{Q}, \mathbb{F}_p$ 没有真子域.

证明. $\square$

例 2.22. 若 $S \subset \mathbb{Q}(\sqrt{-1})$ 是子域，则 $S = \mathbb{Q}$ 或 $S = \mathbb{Q}(\sqrt{-1})$.

证明. $\square$

3 环同态、商环与理想

定义 3.1. 设 R, S 是含幺交换环, 称映射 $\theta: R \to S$ 为环同态, 如果

(1) $\theta(1_R) = 1_S$

(2) $\theta(a+b) = \theta(a) + \theta(b)$

(3) $\theta(a \cdot b) = \theta(a) \cdot \theta(b)$

如果 θ 还是一个满射/单射/双射, 则相应地称之为满同态/单同态/环同构.

回忆

定理 3.2 (映射基本定理)**.**

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, two heads, "\pi"'] & Y \\ X/\overset{f}{\sim} \arrow[r, leftrightarrow, "\tilde{f}"] & \operatorname{Im} f \arrow[u, hook, "inc"'] \end{tikzcd}$$

我们将映射基本定理应用到环同态 $\theta: R \to S$ 上,

$$\begin{tikzcd} R \arrow[r, "\theta"] \arrow[d, two heads, "\pi"'] & S \\ R/\overset{\theta}{\sim} \arrow[r, leftrightarrow, "\tilde{\theta}"] & \operatorname{Im}\theta \arrow[u, hook, "inc"'] \end{tikzcd}$$

由于 R 和 S 本身的环结构以及 θ 对结构的保持, 我们能说更多的事情:

- $\operatorname{Im}\theta$ 具有环结构, 从而不仅仅是 S 的子集而且是 S 的子环.
  - 由于 θ 保加法和乘法, 所以 $\operatorname{Im}\theta$ 对 S 的加法和乘法封闭.
  - 由于 θ 将 R 的幺元映为 S 的幺元, 所以 $\operatorname{Im}\theta$ 含幺.
  - 与第一条相同的理由,$\operatorname{Im}\theta$ 对 S 的减法封闭.
- $R/\overset{\theta}{\sim}$ 具有环结构.
  - 首先我们需要定义其上的加法和乘法
    $$\bar{r}_1 + \bar{r}_2 := \overline{r_1 + r_2}$$
    $$\bar{r}_1 \cdot \bar{r}_2 := \overline{r_1 \cdot r_2}$$
  - 自然会问, 上面这两个运算是良好定义的吗?
    即, 如若 $r_1 \sim r_1', r_2 \sim r_2'$, 是否有 $r_1 + r_2 \sim r_1' + r_2'$ 和 $r_1 \cdot r_2 \sim r_1' \cdot r_2'$?
    再按定义翻译一下, 就是, 如果 $\theta(r_1) = \theta(r_1'), \theta(r_2) = \theta(r_2')$, 是否有 $\theta(r_1 + r_2) = \theta(r_1' + r_2')$ 和 $\theta(r_1 \cdot r_2) = \theta(r_1' \cdot r_2')$? 显然多了对吧哈哈哈.
  - 容易验证在上面两个运算下 $R/\overset{\theta}{\sim}$ 确实构成含幺交换环.
- $\tilde{\theta}$ 是环同态, 从而不仅仅是双射, 而且是环同构.

下面我们换一种方式来刻画 θ 在 R 上诱导的等价关系,

$$
\begin{aligned}
& r \sim r' \\
\Longleftrightarrow & \theta(r)=\theta(r') && \text{这是映射基本定理中最初的版本, 很平凡} \\
\Longleftrightarrow & \theta(r)-\theta(r')=0 && \text{这里已经用到了}S\text{中的元素可以做减法, 但还是比较平凡} \\
\Longleftrightarrow & \theta(r-r')=0 && \text{用到了}\theta\text{是环同态, 不太平凡了} \\
\Longleftrightarrow & r-r' \in \theta^{-1}(0)=:\ker\theta && \text{和上一条说的是相同的事, 但我们开始关注}\ker\theta\text{这个集合}
\end{aligned}
$$

我们知道, 当我们用 $r \sim r' \Longleftrightarrow \theta(r)=\theta(r')$ 这条刻画来验证 $R/\overset{\theta}{\sim}$ 上的加法和乘法的良定性的时候, 我们用到了 θ 保加法和保乘法的条件. 现在想知道, 在 $r\sim r' \Longleftrightarrow r-r'\in\ker\theta$ 的刻画下, 验证良定性时会用到 $\ker\theta$ 什么样的性质？当然, 你有理由相信,$\ker\theta$ 的这些性质归根结底还是来自于 θ 保加法和保乘法.

若 $r_1\sim r_1', r_2\sim r_2'$, 即 $r_1-r_1'\in\ker\theta, r_2-r_2'\in\ker\theta$, 则

$$(r_1+r_2)-(r_1'+r_2')=(r_1-r_1')+(r_2-r_2')\in\ker\theta,$$

这是因为 $\ker\theta$ 对加法封闭, 本质上是因为 θ 保加法,$0+0=0$.

$$r_1\cdot r_2-r_1'\cdot r_2'=r_1\cdot(r_2-r_2')+r_2'(r_1-r_1')\in\ker\theta,$$

这是因为 $\ker\theta$ 对倍乘封闭, 本质上是因为 θ 保乘法,0 乘任何数都等于 0.

事实上, 从上边的讨论可以看出, 若非空集合 $I\subset R$ 满足对加法封闭和对倍乘封闭, 便可以由 $r-r'\in I$ 诱导出 R 上的一个等价关系 $\sim$, 且 $R/\sim$ 上有环结构.

我们将满足这样条件的子集抽象出来成为一个定义

定义 3.3. 非空子集 $I\subseteq R$ 称为是理想, 若

(1) $a,b\in I\Rightarrow a+b\in I$

(2) $a\in R, x\in I\Rightarrow ax\in I$

记作 $I\lhd R$.

定理 3.4 (环同态基本定理)**.** 设 $\theta: R\to S$ 是环同态, 则存在唯一的环同构 $\bar\theta: R/\ker\theta\xrightarrow{\sim}\mathrm{Im}(\theta)$ 使得下列图表交换:

$$
\begin{tikzcd}
R \arrow[r, "\theta"] \arrow[d, two heads, "\mathrm{can}"'] & S \\
R/\ker\theta \arrow[r, "\bar\theta"', "\bar r\mapsto\theta(r)"] & \mathrm{Im}\,\theta \arrow[u, hook, "\mathrm{inc}"']
\end{tikzcd}
$$

证明. 应用映射基本定理, 剩下的只需要验证 $\bar\theta$ 确实是环同态.

$$\bar\theta([r_1]+[r_2])=\bar\theta([r_1+r_2])=\theta(r_1+r_2)=\theta(r_1)+\theta(r_2)=\bar\theta([r_1])+\bar\theta([r_2])$$

$$\bar\theta([r_1][r_2])=\bar\theta([r_1r_2])=\theta(r_1r_2)=\theta(r_1)\theta(r_2)=\bar\theta([r_1])\bar\theta([r_2])$$

□

命题 3.5. 设 R,S 是含幺交换环,$\theta:R\to S$ 是环同态, 则

- $\theta(0_R) = 0_S$
- $\theta(-a) = -\theta(a)$
- $\theta(a^m) = (\theta(a))^m, m = 0, 1, 2, \cdots$
- 若 a 可逆, 则 $\theta(a^{-1}) = (\theta(a))^{-1}$

命题 3.6. 设 $\theta : R \to S$ 同态, 若 $a \in U(R)$, 则 $\theta(a) \in U(S)$, 并且 θ 诱导一个群同态.

注记. θ 可以将不可逆元映成可逆元, 如 $\theta : \mathbb{Z} \to \mathbb{Q}, n \mapsto n$.

例 3.7. 证明: 存在唯一环同态 $\theta : \mathbb{Z} \to \mathbb{Z}_8$.

证明. 假设存在环同态, 由环同态的定义,$\theta(1) = [1]$. 由于环同态保加法, 所以 $\theta(n) = [n]$. 这样我们就唯一确定了 θ. 易验证 $\theta(ab) = [ab] = [a][b] = \theta(a)\theta(b)$, 因此 θ 保乘法, 从而 θ 确实是环同态. □

例 3.8. 证明: 不存在环同态 $\theta : \mathbb{Q} \to \mathbb{Z}_8$.

证明. 同证明存在从 $\mathbb{Z}$ 到 $\mathbb{Z}_8$ 的唯一环同态的情形一样, 我们必须要求 $\theta(n) = [n]$. 但不同的是, 拿 $\theta(2) = [2]$ 来说,[2] 是 $\mathbb{Z}_8$ 中的不可逆元,2 在 $\mathbb{Z}$ 中不是可逆元但在 $\mathbb{Q}$ 中却是可逆元. 因此在 $\mathbb{Z} \to \mathbb{Z}_8$ 时可以存在的环同态在 $\mathbb{Q} \to \mathbb{Z}_8$ 的情形中不可能成立. □

注记. [2] 不仅是 $\mathbb{Z}_8$ 中的不可逆元, 还是 $\mathbb{Z}_8$ 中的零因子. 我们知道零因子一定是不可逆元, 但不可逆元不一定是零因子, 比如 $\mathbb{Z}$ 中的 2. 这也告诉我们 θ 可以将不可逆的非零因子映成零因子.

命题 3.9. 设 $\theta : R \to S$ 是环同态, 那么 θ 一定将零因子映成零因子.

例 3.10. 证明: 不存在环同态 $\theta : \mathbb{Z}_8 \to \mathbb{Q}$.

注记.

$$\text{可逆元} > \text{不可逆的非零因子} > \text{零因子}$$

环同态下, 两边不可能往中间去, 中间可能往两边去.

这可以成为判断两个环之间是否存在环同态的一个方法, 但它不是万能的. 比如不存在环同态 $\theta : \mathbb{Z}_2 \to \mathbb{Z}$, 但按照上面相同的推理,$\theta([0]) = 0, \theta([1]) = 1$, 并不与上面的规则相矛盾. 不存在环同态的原因是 $\theta([1] + [1]) \neq 1 + 1$. 这提示我们环同态下还有其他需要保持的不变量. 可能等学到群的时候这件事会更明晰.

例 3.11 (R 的特征同态)**.** 对任意的环 R, 存在唯一的环同态 $\theta : \mathbb{Z} \to R$.

证明. 定义 $\theta : n \mapsto n1_R$. 由此前的作业题知这的确是一个环同态. □

容易验证环同态的复合还是环同态, 恒等映射是环同态, 因此这是一个范畴.

引理 3.12. 设 $\theta : R \to S$ 是环同构, 则 $\theta^{-1} : S \to R$ 也是环同构.

定义 3.13 (R 的自同构群)**.** 设 R 是环, 定义

$$\mathrm{Aut}(R) := \{\theta : R \to R \text{ 是环自同构}\}$$

容易验证 $\mathrm{Aut}(R)$ 包含恒等映射, 并且它在复合运算和取逆运算下封闭, 于是 $\mathrm{Aut}(R)$ 是群, 称为 R 的自同构群.

例 3.14. $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}\}$.

证明. □

例 3.15. $\mathrm{Aut}(\mathbb{Z}[\sqrt{-1}]) = \left\{\mathrm{Id}_{\mathbb{Z}[\sqrt{-1}]}, \sigma : z \mapsto \bar{z}\right\}$.

证明. □

同构的环本质一样, 设 $\theta : R \to S$ 是环同构, 则

- $a \in U(R) \Leftrightarrow \theta(\alpha) \in U(S)$, 注意当 θ 为环同态是我们只能从左推到右.
- θ 诱导群同构 $U(R) \to U(S)$ 和 $\mathrm{Aut}(R) \to \mathrm{Aut}(S)$.
- R 是整环当且仅当 S 是整环,R 是域当且仅当 S 是域.

定义 3.16 (θ 的核)**.** $\ker\theta = \theta^{-1}(0_S) = \left\{r \in R \middle| \theta(r) = 0_S\right\}$.

- $\ker\theta$ 对加减乘运算封闭.
- ker 不是子环, 因为 $1_R \notin R$.
- $\ker\theta$ 对倍元封闭, 对任意 $a \in R, r \in \ker\theta$,$\theta(ar) = \theta(a)\theta(r) = \theta(a)0_S = 0_S$
- $a \overset{\theta}{\sim} b \Leftrightarrow a - b \in \ker\theta$
- $[a] := a + \ker\theta := \left\{a + r \middle| r \in \ker\theta\right\}$
- $R/\overset{\theta}{\sim} \longleftrightarrow \mathrm{Im}\,\theta$

注记. θ 在诱导环 R 上 $\overset{\theta}{\sim}$ 这个等价关系时的表现与一般集合 X 上的一般映射 f 的表现别无二致, 特殊的地方在于现在我们有了一个 $a \overset{\theta}{\sim} b$ 的一个充要条件: $a - b \in \ker\theta$. 注意到能有这个充要条件 R 和 S 的环结构以及 θ 对运算的保持均功不可没, 如果没有环结构, 就无从谈起 $\theta(a)$ 与 $\theta(b)$,a 与 b 的运算; 如果没有环同态, 就无法从一般的 $\theta(a) = \theta(b)$ 走向 $\theta(a - b) = 0_S$.

$a \overset{\theta}{\sim} b \Leftrightarrow a - b \in \ker\theta$ 这个充要条件相当重要, 当我们不再从环同态出发, 而是从环同态的核的类似物, 理想 I, 出发时, 我们的等价关系就是反过来用 $a - b \in I$ 来定义的.

由定义, 我们能够推出

- $x \in I \Rightarrow -1_R x = -x \in I$, 即 I 对取逆运算封闭.
- $0_R \in I$
- 对任意环同态 $\theta : R \to S$,$\ker\theta \lhd R$.

例 3.17. 理想的例子.

(1) $R \lhd R$

(2) $\{0_R\} \lhd R$

(3) $(a) = aR = \left\{ax \middle| x \in R\right\} \lhd R$, 称为由 a 生成的主理想

注记. 定义

$$\tau_a : R \to R, x \mapsto ax$$

- 这个映射看起来不错, 但它不是环同态. 它只保持加法, 既不把幺元映成幺元, 也不保持乘法.
- $(a) = \operatorname{Im} \tau_a$, 下列命题等价:

  (1) τ_a 是满射

  (2) a 是可逆元

  (3) $1_R \in (a)$

  (4) $(a) = R$

- τ_a 是满射 $\Rightarrow \tau_a$ 是单射.
- τ_a 是单射 $\not\Rightarrow \tau_a$ 是满射,$\tau_a : \mathbb{Z} \to \mathbb{Z}, n \mapsto 2n$.
- τ_a 不是单射 $\Rightarrow \tau_a$ 不是满射 $\Leftrightarrow a$ 不可逆 $\Leftrightarrow (a)$ 是真理想.

命题 3.18. 设 $I \lhd R$, 则 I 是真理想当且仅当 $1_R \notin I$.

证明.

$\Leftarrow$ 显然.

$\Rightarrow$ 假设 $1_R \in I$, 则对任意的 $a \in R$,$a1_R = a \in I$, 即 $R \subset I$, 矛盾. □

命题 3.19. R 是域当且仅当 R 只有平凡理想.

证明.

$\Rightarrow$ 设 $I \lhd R$ 并且 $I \neq \{0_R\}$, 则存在 $a \neq 0_R \in I$, 对于 $a^{-1} \in R$ 有 $a^{-1}a = 1_R \in I$, 则 $I = R$.

$\Leftarrow$ 对任意的 $a \neq 0_R$,$(a) \lhd R$, 由假设 $(a) = R$, 则存在 b 使得 $ab = 1_R$, 即 $a \in U(R)$. □

例 3.20. 分类 $\mathbb{Z}$ 的理想.

解. 设 $\{0_R\} \subsetneq I \lhd R$, 那么存在 $0 \neq n \in I$ 使得 $|n|$ 最小.

断言,$I = n\mathbb{Z} = \big\{nm \big| m \in \mathbb{Z}\big\}$.

- $n\mathbb{Z} \subset I$, 显然.
- $I \subset n\mathbb{Z}$. 对任意 $r \in I$,$r = nq + r'$, 其中 $q \in \mathbb{Z}$,$0 \leqslant r' < |n|$, 则 $r' = r - nq \in I$, 因此 $r' = 0$, 否则与 $|n|$ 最小矛盾. 因此 $n|r$.

综上所述,$\mathbb{Z}$ 的全部理想为 $n\mathbb{Z}, n \geqslant 0$. □

定义 3.21. 设 $I \lhd R$, 定义商环 R/I 如下:

Step1 定义 R 上的等价关系 $a \equiv b \mod I \Leftrightarrow a - b \in I$

- $a - a = 0_R \in I$
- 若 $a - b \in I$, 则 $b - a = -(a - b) \in I$
- 若 $a - b \in I, b - c \in I$, 则 $a - c = (a - b) + (b - c) \in I$

Step2 定义 $R/I := R/\equiv = \{\overline{a} | a \in R\}$. 在 R/I 上有自然运算:

$$\overline{a} + \overline{b} := \overline{a+b},$$

$$\overline{a} \cdot \overline{b} := \overline{ab}$$

验证良定性, 若 $a - a' \in I, b - b' \in I$, 则

- $(a+b) - (a'+b') = (a-a') + (b-b') \in I$
- $ab - a'b' = ab - a'b + a'b - a'b' = (a-a')b + a'(b-b') \in I$

Step3 $(R/I, +, \cdot)$ 自然是环,R 上加法和乘法的性质被自动保持, 而 $0_{R/I} = \overline{0}_R, 1_{R/I} = \overline{1}_R$.

定义了商环之后, 我们有从 R 到 R/I 的典范的环同态:

$$\begin{aligned} \mathrm{can} : R &\twoheadrightarrow R/I \\ a &\mapsto \overline{a} \end{aligned}$$

值得注意的是 $\ker \mathrm{can} = I$!

例 3.22. $n\mathbb{Z} \lhd \mathbb{Z}$,$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

命题 3.23. 设 $\theta : R \to S$ 是环同态,$I \lhd R$,$\mathrm{can} : R \twoheadrightarrow R/I$, 则

$$I \subset \ker \theta \Longleftrightarrow \theta = \theta' \circ \mathrm{can}$$

$$\begin{tikzcd} R \arrow[r, "\theta"] \arrow[d, two heads, "\mathrm{can}"'] & S \\ R/I \arrow[ur, dashed, "\theta'"'] & \end{tikzcd}$$

证明. $\Leftarrow \ker \theta \supseteq \ker \mathrm{can} = I$

$\Rightarrow$ 定义

$$\begin{aligned} \theta' : R/I &\to S \\ \overline{a} &\mapsto \theta(a) \end{aligned}$$

验证良定性, 如果 $\overline{a} = \overline{a'}$, 则 $a - a' \in I \subseteq \ker \theta$, 则 $\theta(a - a') = 0_S$, 所以 $\theta(a) = \theta(a')$ □

定理 3.24 (第三同构定理)**.** 设 $I \lhd R, J \lhd R$, 并且 $I \subset J$, 定义

$$\begin{aligned} \varphi : R/I &\twoheadrightarrow R/J \\ a + I &\mapsto a + J \end{aligned}$$

(1) 验证良定性

(2) 证明 $\ker \varphi = J/I = \{a + I | a \in J\}$

(3) 证明 $J/I \lhd R/I$

(4) 应用同态基本定理, 证明

$$\begin{aligned} \bar{\varphi} : (R/I)/(J/I) &\xrightarrow{\sim} R/J \\ \bar{a} + J/I &\mapsto a + J \end{aligned}$$

- 对任意元素 a, 如果 $a \in a+J$, 那么 $a+I \subset a+J$
- 对任意两个元素 $a, b \in a+J$, 由第一条知 $a+I \subset a+J$ 且 $b+I \subset a+J$, 那么 $a+I$ 与 $b+I$ 要么相等, 要么交集为空集. 假设存在 $c \in a+I \cap b+I \neq \varnothing$, 则 $a-c \in I, b-c \in I$,$a-b = a-c+c-b \in I$, 因此 $a+I = b+I$.
- 因此 $a+J$ 可被划分为不知道多少个 $a+I$ 的互不相交的等价类, 两个等价类内的元素之间在更大更粗糙的 J 的意义下是等价的, 但在更小更精细的 I 的意义下是不等价的.
- 特别地, 集合 J 可以被集合 I 作分割. 其他形如 $a+J$ 的等价类不过是 J 的平移, 它们与 J 的大小是一样的.
- J 中包含着不知道多少个 I 的等价类, 之前在 I 的意义下它们是不同的, 现在在 J 的意义下它们是相同的, 也就是说 J/I 这些等价类就是新的该被视为相同的元素, 也就是核.
- 也就是说我们不把分类过程用 J 一步到位, 而是分两步, 先用 I 做, 再补 I 相较 J 差的那些.

证明.

(1) 每次验证良定性你都要想清楚到底是为什么要验证. 在这里我们定义 R 模去 I 得到的等价类的像是用等价类里的元素所在的 R 模去 J 得到的等价类来定义的. 那么我对于同一个 R 模去 I 得到的等价类中的不同元素, 按照上面的对应规则是否会得到不同的对应结果？答案显然是否定的, 这是因为 $I \subset J$.

$\square$

4 分式域

设 R 是整环, 在 $R \times R^{\times}$ 上定义等价关系如下：

$$(a,x) \simeq (b,y) \Longleftrightarrow ay = bx.$$

反身性与对称性显然, 只验证传递性. 若 $(a,x) \simeq (b,y), (b,y) \simeq (c,z)$, 按定义有 $ay = bx, bz = cy$, 第一式同乘 z, 第二式同乘 x, 得到 $ayz = bxz = bzx = cyx$, 由于 $y \neq 0$, 可在两侧消去 y 得到 $az = cx$, 即 $(a,x) \simeq (c,z)$.

将 $R \times R^{\times} / \simeq$ 记作 $\mathrm{Frac}(R)$, 将 (a,x) 所在的等价类记作 $\dfrac{a}{x}$, 称为分式.

自然定义：

$$\frac{a}{x} + \frac{b}{y} = \frac{ay+bx}{xy},$$
$$\frac{a}{x} \cdot \frac{b}{y} = \frac{ab}{xy}.$$

下面验证该定义是良定的.

$$\frac{ay+bx}{xy} = \frac{a'y'+b'x'}{x'y'} \Leftrightarrow ayx'y' + bxx'y' = a'y'xy + b'x'xy$$

$$\frac{ab}{xy} = \frac{a'b'}{x'y'} \Leftrightarrow abx'y' = a'b'xy$$

当 $ax' = xa'$,$by' = yb'$ 时, 上两式显然成立, 因此是良定的！

命题 4.1. $\mathrm{Frac}(R)$ 是含幺交换环.

证明.

- 加法结合律.
$$\left(\frac{a}{x} + \frac{b}{y}\right) + \frac{c}{z} = \frac{ay+bx}{xy} + \frac{c}{z} = \frac{ayz+bxz+cxy}{xyz},$$
$$\frac{a}{x} + \left(\frac{b}{y} + \frac{c}{z}\right) = \frac{a}{x} + \frac{bz+cy}{yz} = \frac{ayz+xbz+xcy}{xyz}.$$
- 加法交换律. 显然.
- 存在零元
$$\frac{0_R}{1_R} + \frac{a}{x} = \frac{0_R x + 1_R a}{1_R x} = \frac{a}{x}.$$
- 存在逆元
$$\frac{a}{x} + \frac{-a}{x} = \frac{ax-ax}{x^2} = \frac{a-a}{x} = \frac{0_R}{x} = \frac{0_R}{1_R}.$$
- 乘法结合律. 显然.
- 乘法交换律. 显然.
- 存在幺元.
$$\frac{1_R}{1_R} \cdot \frac{a}{x} = \frac{1_R a}{1_R x} = \frac{a}{x}$$

- 分配律

$$\frac{a}{x}\cdot\left(\frac{b}{y}+\frac{c}{z}\right)=\frac{a}{x}\cdot\frac{bz+cy}{yz}=\frac{abz+acy}{xyz}$$

$$\frac{a}{x}\cdot\frac{b}{y}+\frac{a}{x}\cdot\frac{c}{z}=\frac{ab}{xy}+\frac{ac}{xz}=\frac{abxz+xyac}{xyxz}=\frac{abz+yac}{xyz}$$

□

命题 4.2. Frac(R) 是域.

证明. 设 $\frac{a}{x}\neq\frac{0_R}{1_R}$, 即 $a\neq 0_R$, 容易验证 $\frac{a}{x}\cdot\frac{x}{a}=\frac{ax}{ax}=\frac{1_R}{1_R}$. □

定理 4.3. 设 R 是整环,K 是域, 对任意单同态 $\varphi: R\hookrightarrow K$, 存在唯一的单同态 $\tilde\varphi: Frac(R)\hookrightarrow K$ 使得下列图表交换:

$$\begin{tikzcd} R \arrow[r, hook, "\mathrm{can}_R"] \arrow[d, hook, "\varphi"'] & Frac(R) \arrow[dl, hook, dashed, "\tilde\varphi"] \\ K & \end{tikzcd}$$

证明.

- 至多唯一性. 若 $\tilde\varphi$ 存在, 则

$$\tilde\varphi\left(\frac{a}{x}\right)=\tilde\varphi\left(\frac{a}{1_R}\cdot\frac{1_R}{x}\right)=\tilde\varphi\left(\frac{a}{1_R}\cdot\left(\frac{x}{1_R}\right)^{-1}\right)=\tilde\varphi\left(\frac{a}{1_R}\right)\cdot\tilde\varphi\left(\frac{x}{1_R}\right)^{-1}=\varphi(a)(\varphi(x))^{-1}$$

- 存在性. 定义 $\tilde\varphi: Frac(R)\to K, \frac{a}{x}\mapsto\varphi(a)(\varphi(x))^{-1}$

  - 验证良定性. 若 $\frac{a}{x}=\frac{a'}{x'}$, 是否有 $\varphi(a)(\varphi(x))^{-1}=\varphi(a')(\varphi(x'))^{-1}$?

    若 $\frac{a}{x}=\frac{a'}{x'}$, 则 $ax'=a'x$, 则 $\varphi(a)\cdot\varphi(x')=\varphi(a')\varphi(x)$, 得证.
  - 验证 $\tilde\varphi$ 是同态.

$$\tilde\varphi\left(\frac{a}{x}+\frac{a'}{x'}\right)=\tilde\varphi\left(\frac{ax'+a'x}{xx'}\right)=\varphi(ax'+a'x)(\varphi(xx'))^{-1}$$
$$=\varphi(ax')(\varphi(xx'))^{-1}+\varphi(a'x)(\varphi(xx'))^{-1}=\tilde\varphi\left(\frac{ax'}{xx'}\right)+\tilde\varphi\left(\frac{a'x}{xx'}\right)=\tilde\varphi\left(\frac{a}{x}\right)+\tilde\varphi\left(\frac{a'}{x'}\right)$$

$$\tilde\varphi\left(\frac{a}{x}\cdot\frac{a'}{x'}\right)=\tilde\varphi\left(\frac{aa'}{xx'}\right)=\varphi(aa')(\varphi(xx'))^{-1}=\varphi(a)(\varphi(x))^{-1}\varphi(a')(\varphi(x'))^{-1}=\tilde\varphi\left(\frac{a}{x}\right)\tilde\varphi\left(\frac{a'}{x'}\right)$$

  - 验证 $\tilde\varphi$ 是单的.

$$\tilde\varphi\left(\frac{a}{x}\right)=\varphi(a)\varphi^{-1}(x)=0\Longrightarrow\varphi(a)=0\Longrightarrow\ker\tilde\varphi=\left\{\frac{0_R}{1_R}\right\}.$$

□

5 素理想与极大理想

素理想

定义 5.1. 设 $\mathfrak{p}\triangleleft R$ 是真理想，若 $ab\in\mathfrak{p}\Longrightarrow a\in\mathfrak{p}$ 或 $b\in\mathfrak{p}$，则称 $\mathfrak{p}$ 为 R 的素理想.

例 5.2. 真理想 $\mathfrak{p}$ 是素理想当且仅当 $R/\mathfrak{p}$ 是整环. 特别地，零理想是素理想当且仅当 R 是整环.

证明.

- $\Longrightarrow$ 任取 $\overline{a},\overline{b}\in R/\mathfrak{p}$ 且不为 $\overline{0}_R$, 即 $a,b\notin\mathfrak{p}$, 按定义,$ab\notin\mathfrak{p}$, 所以 $\overline{a}\cdot\overline{b}=\overline{ab}\neq\overline{0}_R$
- $\Longleftarrow$ 任取 $ab\in\mathfrak{p}$, 即 $\overline{ab}=\overline{0}_R$, 因为 $R/\mathfrak{p}$ 是整环, 所以 $\overline{a}=\overline{0}_R$ 或 $\overline{b}=\overline{0}_R$, 即 $a\in\mathfrak{p}$ 或 $b\in\mathfrak{p}$.

□

命题 5.3. 真理想 $\mathfrak{p}$ 是素理想当且仅当 $I_1I_2\subset\mathfrak{p}$ 蕴含 $I_1\subset\mathfrak{p}$ 或 $I_2\subset\mathfrak{p}$.

例 5.4. 设 R 是 *PID*, 则 $\operatorname{Spec}R=\{(0_R)\}\cup\left\{(p)\middle|p\in R\text{不可约}\right\}$.

证明. 设 $(0_R)\neq(r)\triangleleft R$ 是真理想, 则 $r\notin U(R)$.

- 若 r 是不可约元, 在 PID 中不可约元是素元, 所以 (r) 是素理想.
- 若 r 不是不可约元, 则 r 在 R 中有非平凡分解 $r=ab$. 断言 $a\notin(r)$ 且 $b\notin(r)$. 假设 $a\in(r)$, 则存在 $c\in R$ 使得 $a=rc=abc$, 即 $bc=1$,$b\in U(R)$, 这与 $r=ab$ 是非平凡分解矛盾. 同理可证 $b\notin(r)$, 从而 $ab\in(r)$ 但 $a\notin(r)$ 且 $b\notin(r)$, 即 (r) 不是素理想.

□

特别地,

- $\operatorname{Spec}\mathbb{Z}=\{(0)\}\cup\left\{p\mathbb{Z}\middle|p\text{是素数}\right\}$.
- $\operatorname{Spec}k[x]=\{(0)\}\cup\left\{(f(x))\middle|f(x)\text{是不可约多项式}\right\}$.

例 5.5. $\operatorname{Spec}\mathbb{Z}[x]=\{(0)\}\cup\big\{(f(x))\,\big|\,f(x)\text{是不可约元}\big\}\cup\big\{(p,f(x))\,\big|\,p\in\mathbb{Z}\text{是素数},\bar{f}(x)\text{在}\mathbb{F}_p[x]\text{中不可约}\big\}$.

证明. 设 $\mathfrak{p}$ 为 $\mathbb{Z}[x]$ 的素理想.

- 若 $\mathfrak{p}$ 是主理想, 那么类似 PID 的情形可证 $\mathfrak{p}$ 是零理想或 $(f(x))$, 其中 $f(x)$ 是 $\mathbb{Z}[x]$ 中不可约元. 要注意 $p\in\mathbb{Z}$ 为素数也是 $\mathbb{Z}[x]$ 中不可约元.

- 若 $\mathfrak{p}$ 不是主理想, 考虑 $\mathfrak{q}=\mathfrak{p}\cap\mathbb{Z}$, 则 $\mathfrak{q}$ 为 $\mathbb{Z}$ 的素理想.

  (1) 断言 $\mathfrak{q}\neq(0)$. 只需证明 $\mathfrak{q}$ 中含有一个非零常数.
  任取 $\mathfrak{p}$ 中的一个非零多项式 $f(x)$, 不妨设 $f(x)$ 不可约, 否则以 $f(x)$ 的非平凡因子替换.
  由假设 $\mathfrak{p}$ 不是主理想, 所以 $(f(x))\nsubseteq\mathfrak{p}$, 即存在 $g(x)\in\mathfrak{p}$ 但 $f(x)\nmid g(x)$. 经过一番细致的讨论可知 $f(x)\nmid g(x)$ 在 $\mathbb{Q}[x]$ 中也成立.（Why?）从而存在 $u,v\in\mathbb{Q}[x]$ 使得 $uf+vg=1$. 消去分母得 $\mathbb{Z}[x]$ 中多项式 u',v' 使得 $u'f+v'g=n\neq 0$. 则 $n\in\mathfrak{p}\cap\mathbb{Z}$, 从而 $\mathfrak{q}\neq(0)$.

  (2) $\dfrac{\mathbb{Z}[x]}{\mathfrak{p}}\cong\dfrac{\mathbb{Z}[x]/\mathfrak{q}}{\mathfrak{p}/\mathfrak{q}}=\dfrac{\mathbb{Z}[x]/q\mathbb{Z}}{\mathfrak{p}/q\mathbb{Z}}\cong\dfrac{\mathbb{F}_q[x]}{\mathfrak{p}/q\mathbb{Z}}$
  由 $\mathfrak{p}$ 是 $\mathbb{Z}[x]$ 的素理想知 $\dfrac{\mathbb{Z}[x]}{\mathfrak{p}}$ 是整环, 从而 $\dfrac{\mathbb{F}_q[x]}{\mathfrak{p}/q\mathbb{Z}}$ 是整环, 从而 $\mathfrak{p}/q\mathbb{Z}$ 是 $\mathbb{F}_q[x]$ 的素理想. 但 $\mathfrak{p}/q\mathbb{Z}$ 不可能是零理想, 否则 $\mathfrak{p}$ 是主理想, 因此 $\mathfrak{p}/q\mathbb{Z}=(\bar{f}(x))$, 其中 $\bar{f}(x)\in\mathbb{F}_q[x]$ 是不可约元. 则 $\mathfrak{p}=(q,f(x))$.

□

极大理想与商域

定义 5.6 (极大理想)**.** 真理想 $\mathfrak{m} \triangleleft R$ 称为极大理想若 $\mathfrak{m} \subset I \triangleleft R$ 能推出 $\mathfrak{m} = I$ 或 $I = R$.

命题 5.7. $\mathfrak{m} \triangleleft R$ 是极大理想当且仅当 $R/\mathfrak{m}$ 是域.

证明.

- $\Rightarrow$ 任取 $\overline{0}_R \neq \overline{x} \in R/\mathfrak{m}$, 即 $x \notin \mathfrak{m}$.
  那么 $\mathfrak{m} \subsetneq (x) + \mathfrak{m} = \left\{ax + y \middle| a \in R, y \in \mathfrak{m}\right\} \triangleleft R$.
  因为 $\mathfrak{m}$ 是极大理想, 所以 $(x) + \mathfrak{m} = R$. 则存在 a_0, y_0 使得 $a_0x + y_0 = 1_R$.
  即 $\overline{a}_0\overline{x} = \overline{1}_R, \overline{x}^{-1} = \overline{a}_0$.
- $\Leftarrow$ 设 $\mathfrak{m} \subsetneq I \triangleleft R$, 则 $\{\overline{0}\} \neq I/\mathfrak{m} \triangleleft R/\mathfrak{m}$. 因为 $R/\mathfrak{m}$ 是域所以 $I/\mathfrak{m} = R/\mathfrak{m}$.
  对任意 $a \in R$,$\overline{a} \in R/\mathfrak{m} = I/\mathfrak{m}$. 则存在 $b \in I$ 使得 $b - a \in \mathfrak{m}$. 因为 $\mathfrak{m} \subset I$, 所以 $a \in I$.
  所以 $I = R$.

□

素元与不可约元

定义 5.8. 设 R 是整环，称 $0_R \neq a \in R$ 为素元，如果 $(a) \in \mathrm{Spec}(R)$.

- 按素理想的定义,$(a) \neq R$, 因此素元不可逆.
- a 是素元当且仅当 $a \mid xy \Rightarrow a \mid x$ 或 $a \mid y$.
-

定义 5.9. 称 $0_R \neq a \in R$ 为不可约元, 如果 $a \notin U(R)$ 且 $a = bc \Rightarrow b$ 或 c 可逆.

- 不可约元只有平凡分解 $a = u \cdot (u^{-1}a), u \in U(R)$.

命题 5.10. 素元是不可约元.

证明. 设 a 是素元，则 $a \neq 0_R$ 且 $a \notin U(R)$. 设 $a = bc$，那么 $a \mid bc$，按素元定义有 $a \mid b$ 或 $a \mid c$. 不妨设 $b = ax$，那么 $a = axc$，由整环的消去律有 $1_R = xc$，从而 c 可逆. □

例 5.11. 在 $\mathbb{Z}$ 中素元 $\Longleftrightarrow$ 不可约元 $\Longleftrightarrow \pm p$.

例 5.12. $\mathbb{Z}[\sqrt{-3}]$ 中 2 是不可约元但不是素元.

命题 5.13. p 不可约 $\Rightarrow (p) \triangleleft R$ 之间没有主理想.

证明. 假设 □

6 一元多项式环

R 上关于 x 的（形式）多项式

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 = \sum_{i=0}^{n} a_n x^n$$

其中 $a_i \in R$

x^i 是用来记录 a_i 的位置

- 多项式相等 := 对应系数一样.
- 约定,$0_R x^i$ 略去不写；$1_R x^i = x^i$
- $R[x] =$ 全体以 R 为系数的多项式
- 称 a_0 为常数项.
- 若 $a_n \neq 0_R$,$a_n x^n$ 称为首项,a_n 称为首项系数
- 若 $a_n \neq 0$,$\deg f(x) = n$
- $f(x) = a_0 \neq 0$, 常值多项式,$\deg f = 0$
- $\det 0$ 不定义.

事实. $R[x]$ 自然成为环.

(1) 加法：对应系数相加

(2) 乘法

$$f(x) = a_n x^m + \cdots + a_1 x + a_0$$

$$g(x) = b_m x^m + \cdots + b_1 x + b_0$$

$$f(x) \cdots g(x) = \sum_{l=0}^{m+n} c_l x^l, c_l = \sum_{i=0}^{l} a_i b_{l-i}$$

(3) $0_{R[x]} =$ 零多项式 $= 0_R$

(4) $1_{R[x]} = 1_R$

注记.

(1) $a_n x^n + \cdots a_1 x + a_0$ 可看成 $a_i x^i$ 的求和. 之前只是形式上的记号.

(2) $x^n = \underbrace{x \cdot x \cdots x}_{n\text{次}}$

(3) $R \to R[x], r \mapsto r$ 是环的单同态. 一般认为 R 是嵌入到 $R[x]$ 中的

(4) 可定义 $R[y]$,y 是字母.

例 6.1 (Ex1)**.** 抽象定义 $R[x]$

定义 $\tilde{R} = \left\{\underline{a} = (a_0, a_1, \cdots) \middle| a_i, a_i = 0, i >> 0 \in R\right\}$

定义

$$\underline{a} + \underline{b} = (a_0 + b_1, a_1 + b_1, \cdots) \in R[x]$$

$0_{R[x]} = \underline{0}_R = (0_R, 0_R, \cdots)$

$\underline{a} \cdot \underline{b} = \underline{c} = (c_0, c_1, \cdots) \in \tilde{R}$ 其中 $c_l = \sum\limits_{i \geqslant 0} a_i b_{l-i}$

因此 $\tilde{R}$ 是环.

证明 $\tilde{R} \cong R[x], (0, 1, 0, 0, \cdots) \leftarrow\!\shortmid x$

命题 6.2. R 是整环 $\Longrightarrow$ $R[x]$ 是整环.

证明.

$$f(x) \cdots g(x) = (a_n b_m) x^{n+m} + \cdots$$

□

注记. 对于 $f, g \neq 0$,$\deg fg = \deg f + \deg g$

命题 6.3. $U(R[x]) = U(R)$.

证明. □

命题 6.4. 设 R 为含幺交换环. 对任意的含幺交换环 S、任意的 $s \in S$ 和任意的环同态 $\psi \colon R \to S$, 存在唯一的环同态 $\Psi \colon R[x] \to S$ 满足 $\Psi\big|_R = \psi$ 且 $\Psi(x) = s$. 具有这样的性质的环是唯一的?

证明.

(1) 至多唯一性.

$$\tilde{\psi}(x^i) = s^i$$

$$\tilde{\psi}(a_i x^i) = \tilde{\psi}(a_i)\tilde{\psi}(x^i) = \psi(a_i) s^i$$

(2) 存在性

□

例 6.5. 取 $Id_R : R \to R$, 取 $a \in R$, 存在唯一的环同态 $R[x] \to R$, $r \in R \mapsto r, x \mapsto a, f(x) = \sum\limits_{i=0}^{n} a_i x^i \mapsto \sum\limits_{i=0}^{n} a_i x^i$.

危险的记号: $f(a)$!

称这个同态为 ev_a.*evaluation at* $a \in R$

$f(a)g(a) = (f \cdot g)(a)$

$f(a) + g(a) = (f + g)(a)$

注记. 由 $f(x) \in R[x]$ 得到 $f \in Map(R, R)$

例 6.6 (Ex)**.** 任意集合 X,R 是环, 证明 $Map(X, R)$ 自然成环.

注记. (1) $Map(R, R)$ 是环

(2)

$$R[x] \overset{ev}{\to} Map(R, R), f(x) \mapsto f\text{多项式函数}$$

证明是环同态.（Ex）

注记. 有时不是单射, 危险！这告诉我们要严格区分多项式和多项式函数.

例 6.7. $\mathbb{F}_p[x] \to Map(\mathbb{F}_p, \mathbb{F}_p)$
$x^p - x \mapsto 0$

(3)

$$\begin{tikzcd} R[x] & & Map(R,R) \\ & \circlearrowleft & \\ & & R \end{tikzcd}$$

设 k 是域,$k[x]$ =k 上多项式
对于域上多项式我们总是可以首一化.

定理 6.8. $k[x]$ 上有带余除法. 任意 $f(x) \in k[x], 0_R \neq h[x] \in k[x]$, 则存在唯一的表达式

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

使得 $q(x)$ 和 $r(x) \in k[x]$ 且 $r(x) = 0$ 或 $\deg r < \deg h$.

证明.

- $\deg f < \deg h$

$$f = 0h + f$$

- 否则,$h(x) = a_n x^n + \cdots$,$f(x) = b_m x^m + \cdots$
$f(x) = \left(\dfrac{b_m}{a_n} x^{m-n}\right) h(x) + \bar{f}(x)$,$\bar{f} = 0_R$ 或 $\deg \bar{f} < m$.

□

注记. $h(x) \mid f(x)$ 当且仅当 $r(x) = 0$.

推论 6.9 (余数定理)**.** $h(x) = x - a$,$a \in R$
对任意 $f(x) \in R[x]$, 存在唯一的 $q(x)$ 使得

$$f(x) = q(x)(x - a) + f(a)$$

7 主理想整环

定义 7.1. 设 R 是整环，如果任意 $I \lhd R$ 都是主理想，则称 R 是主理想整环，即 PID.

定理 7.2. $\mathbb{Z}$ 与 $k[x]$ 均为 PID.

证明. 任取 $0 \neq I \lhd k[x]$. 取 $0 \neq h(x) \in I$ 次数最小. 断言 $I = (h(x))$，只需证 $I \subset (h(x))$.

任取 $f(x) \in I$，由带余除法有 $f(x) = q(x)h(x) + r(x)$，那么 $r(x) = f(x) - q(x)h(x) \in I$.

因为 $\deg h$ 已经最小，这就迫使 $r(x) = 0$，从而 $h(x) \mid f(x)$，即 $f(x) \in (h(x))$. □

gcd 存在且 Bézout 等式成立

定义 7.3. 设 R 是整环. 对于 $a, b \in R\backslash\{0_R\}$，如果存在 $d \neq 0_R$ 满足

(1) $d \mid a$ 且 $d \mid b$

(2) 对任意 $d' \neq 0_R$ 满足 $d' \mid a$ 且 $d' \mid b$，有 $d' \mid d$

则称 d 为 a, b 在 R 中的最大公因子，记作 $\gcd(a, b)$.

命题 7.4. $\gcd(a, b)$ 若存在则在相伴的意义下唯一.

回忆 $a_1 \mid a_2 \iff (a_2) \subset (a_1)$，整除关系可理解为主理想的反向包含关系. 因此我们有下面的

命题 7.5. $d = \gcd(a, b) \iff (d)$ 是包含 $(a) + (b)$ 的最小主理想.

由以上命题，容易有

命题 7.6. 设 R 是 PID，那么对任意 $a, b \in R\backslash\{0_R\}$，$\gcd(a, b)$ 存在且成立 Bézout 等式.

PID 中不可约元是素元

PID 中非零素理想是极大理想

命题 7.7. 设 R 是主理想整环, 那么

$$\operatorname{Spec} R = \{(0_R)\} \sqcup \operatorname{Max} R.$$

$\mathbb{C}[x, y]$ 中 $\mathfrak{p} = (x)$ 是素理想但不极大理想. 去考虑商后是不是域. 做不出来可以问助教.Ex

证明. $\mathfrak{p} = (a) \subsetneq I = (b) \lhd R$

$b \mid a$, 要么 b 与 a 相伴要么 b 是可逆元, 因此 $I = R$. 所以是极大理想. □

证明. 任取 $\mathfrak{p} \neq (0_R) \in \operatorname{Spec} R$. 因为 R 是主理想整环, 所以存在 $p \in R$ 使得 $\mathfrak{p} = (p)$.

假设 $\mathfrak{p}$ □

考察 $k[x]$, 仅考虑首一多项式.

- $Spec(k[x])$

例 7.8 (Ex)**.** 固定 a, 证明 $k[x]/(x - a) \cong k$

例 7.9 (Ex)**.** 假设 $\theta : R \to S$ 环同态, 则 θ 自然延拓成环同态 $\tilde{\theta} : R[x] \to S[x]$

8 添根构造

设 $f(x)\in k[x]$,

$$Root_k(f)=\{a\in k \big| f(a)=0_k\}$$

事实. $|Root_k(f)|\leqslant \deg f(x)<+\infty$

证明. 设 $\alpha\in Root_k(f)$, 当且仅当 $x-\alpha\mid f(x)$
则 $f(x)=(x-\alpha)\cdot g(x)$ in $k[x]$
假设 $\beta\neq\alpha, f(\beta)=(\beta-\alpha)g(\beta)$ in k
$Root_k(f)=\{\alpha\}\bigcup Root_k(g)$
由归纳法得证. □

设 $k\subset K$, 则 $f(x)\in k[x]\subset K[x]$

- $Root_k(f)\subset Root_K(f)$.
- $f(x)$ 在 $k[x]$ 中不可约推不出 $f(x)$ 在 $K[x]$ 中不可约.
- 设 $f(x),g(x)\in k[x]$, 则 $d'=\underset{k[x]}{\gcd}(f,g)=\underset{K[x]}{\gcd}(f,g)=d$
  - 在小的里面整除推出在大的里面整除,$d'\mid d$
  - $d'(x)=u(x)f(x)+v(x)g(x)$,$u(x),v(x)\in k[x]$, 所以 $d\mid d'$

设 $\theta:k\hookrightarrow K$ 是域同态,（$k\cong Im(\theta)\subset K$）

$$\tilde{\theta}:k[x]\to K[x],a_0+\cdots+a_nx^n\mapsto\theta(a_0)+\cdots+\theta(a_n)x^n$$

- $\theta(Root_{k[x]}f)\subset Root_k(\theta(f))$
- $f(x)$ 在 $k[x]$ 中不可约推不出 $\theta(f)$ 不可约
- Ex: 写出来. 设 $f(x),g(x)\in k[x]$, 则 $\theta(\gcd(f,g))=\gcd(\theta(f),\theta(g))$

添根构造
设 k 是域,$f(x)\in k[x]$ 是首一的不可约多项式,$\deg f\geqslant 2$, 则 $Root_k(f)=\varnothing$
考虑主理想 $(f(x))\in Maxk[x]$, 因此得到商域

$$K=k[x]/(f(x))$$

K 是关于理想的等价类！$\overline{g}(x)=g(x)+(f(x))$
$\overline{f(x)}=\overline{0}$,$\overline{g}(x)=\overline{h}(x)\Leftrightarrow f(x)\mid g-h$
任意 $\lambda\in k$, 可以将 λ 看成 $k[x]$ 中的零次多项式, 进而可以考虑 λ 关于 $(f(x))$ 的同余类 $\bar{\lambda}=\lambda+(f(x))$
这就得到同态

$$\theta:k\hookrightarrow K,\lambda\mapsto\overline{\lambda}$$

记

- $\theta(\lambda)=\bar{\lambda}$ 记为 λ.

- $\bar{x}=x+(f(x))=u\in K$

  考察 $k[x]\mapsto K[x]$,
  关键事实！$u\in Root_K(\theta(f))$. 即

$$u^n+\bar{a}_{n-1}u^{n-1}+\cdots+\bar{a}_1u+\bar{a}_0=\bar{0}\in K$$

$$\bar{x}^n+\bar{a}_{n-1}\bar{x}^{n-1}\cdots+\bar{a}_1$$

- K 是 k-线性空间.

- $\dim_k K=\deg f(x)$, 而且 K 有 k-基 $\left\{1,u,\cdots,u^{n-1}\right\}$
  - $\bar{g}(x)\in K$,$g(x)=q(x)f(x)+r(x)$, 所以 $\bar{g}(x)=\bar{r}(x)$
  - k-线性无关

注记. K 中元素均形如 $\overline{r(x)},\deg r\leqslant n-1$
$\overline{r_1}(x)+\overline{r_2}(x)=\overline{r_1(x)+r_2(x)}$

泛性质：记 $\theta:k\to K=k[x]/(f(x))$ 如上.
任给 $\delta:k$
设 $k\subset K$, 则 $k[x]\subset K[x]$, 并且有下列事实

(1) $\mathrm{Root}_k(f)\subset\mathrm{Root}_K(f)$

(2) $k[x]$ 中的不可约元在 $K[x]$ 中可能可约

(3) 最大公因子在扩域下保持不变

证明. 我们只证 (3). 设 $d(x)=\gcd\limits_{k[x]}(f,g),D(x)=\gcd\limits_{K[x]}(f,g)$, 我们来证明 $d(x)\mid D(x)$,$D(x)\mid d(x)$. 要注意这两个整除关系都是在 $K[x]$ 的语境中讨论的.

因为 $k[x]$ 中 f,g 的公因式 $d(x)$ 也是 $K[x]$ 中 f,g 的公因式, 按最大公因式的定义有 $d(x)\mid D(x)$.

由 Bezout 等式, 存在 $u(x),v(x)\in k[x]$ 使得 $d(x)=u(x)f(x)+v(x)g(x)$. 这本是 $k[x]$ 中的等式, 但我们可以将其视为 $K[x]$ 中的等式. 因为在 $K[x]$ 中有 $D(x)\mid f(x)$ 和 $D(x)\mid g(x)$, 所以在 $K[x]$ 中有 $D(x)\mid d(x)$. □

如果把上面的 $k\subset K$ 换成存在 $\theta:k\hookrightarrow K$ 使得 k 嵌入到 K 中, 则上述命题应进行如下调整

(1) $\theta(\mathrm{Root}_k(f))\subset\mathrm{Root}_K(\theta(f))$

(2) $f\in k[x]$ 不可约但 $\theta(f)\in K[x]$ 可能可约

(3) $\theta(\gcd\limits_{k[x]}(f,g))=\gcd\limits_{K[x]}(\theta(f),\theta(g))$

证明. 还是只证 (3). 设 $d(x) = \underset{k[x]}{\gcd}(f,g), D(x) = \underset{K[x]}{\gcd}(\theta(f),\theta(g))$, 我们来证明 $\theta(d(x)) \mid D(x)$,$D(x) \mid \theta(d(x))$. 要注意这两个整除关系都是在 $K[x]$ 的语境中讨论的.

因为 $d(x)$ 整除 $f(x)$ 和 $g(x)$, 所以 $\theta(d(x))$ 整除 $\theta(f(x))$ 和 $\theta(g(x))$, 按最大公因式的定义,$\theta(d(x)) \mid D(x)$.

由 Bezout 等式, 存在 $u(x), v(x) \in k[x]$ 使得 $d(x) = u(x)f(x) + v(x)g(x)$. 因此在 $K[x]$ 中有 $\theta(d(x)) = \theta(u(x))\theta(f(x)) + \theta(v(x))\theta(g(x))$. 因为 $D(x) \mid \theta(f(x)), D(x) \mid \theta(g(x))$, 所以 $D(x) \mid \theta(d(x))$. □

定理 8.1. *设 $\theta : k \hookrightarrow K = k[x]/(f(x))$, 任给 $\delta : k \hookrightarrow F$, 使得 F 中元素 $\alpha \in \mathrm{Root}_F(\delta(f))$, 那么存在唯一的 $\delta' : K \hookrightarrow F$ 使得 $\delta' \circ \theta = \theta$ 并且 $\delta'(u) = \alpha$.*

例 8.2. $x^2 + 1 \in \mathbb{R}[x]$ 不可约,$\theta : \mathbb{R} \to \mathbb{R}[x]/(x^2 + 1) =: K$.

例 8.3. 证明：$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

证明. 定义映射 $\theta : \mathbb{R}[x]/(x^2 + 1) \to \mathbb{C}, \overline{f(x)} = \overline{ax + b} = \bar{a}u + \bar{b} \mapsto a\mathrm{i} + b$.

由带余除法, 余式 $ax + b$ 唯一, 因此该映射是良定的.

- 保加法

$$\begin{aligned}\theta(\overline{a_1x + b_1} + \overline{a_2x + b_2}) &= \theta(\overline{(a_1 + a_2)x + (b_1 + b_2)}) = (a_1 + a_2)\mathrm{i} + (b_1 + b_2)\\ =&(a_1\mathrm{i} + b_1) + (a_2\mathrm{i} + b_2) = \theta(\overline{a_1x + b_1}) + \theta(\overline{a_2x + b_2})\end{aligned}$$

- 保乘法. 课上已经证明过 $(a_1u + b_1)(a_2u + b_2) = (a_1b_2 + a_2b_1)u + (b_1b_2 - a_1a_2)$, 因此

$$\begin{aligned}\theta((a_1u + b_1)(a_2u + b_2)) &= \theta((a_1b_2 + a_2b_1)u + (b_1b_2 - a_1a_2)) = (a_1b_2 + a_2b_1)\mathrm{i} + (b_1b_2 - a_1a_2)\\ =&(a_1\mathrm{i} + b_1)(a_2\mathrm{i} + b_2) = \theta(a_1u + b_1)\theta(a_2u + b_2)\end{aligned}$$

- 单射.$\overline{f(x)} \in \ker\theta$ 当且仅当 $f(x) \equiv 0 \mod (x^2 + 1)$, 即 $\overline{f(x)} = \overline{x^2 + 1} = \bar{0}$. 因此是单射.
- 满射. 对任意 $a\mathrm{i} + b \in \mathbb{C}$, 容易验证 $\theta(\overline{au + b}) = a\mathrm{i} + b$, 因此是满射.

□

例 8.4. $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$,$x^2 + x + \bar{1} \in F_2[x]$ 不可约, 这是因为（唉要不要考虑本原的问题啊, 虽然这里 $\mathbb{F}_2$ 阶数太低了不大用考虑, 阶数高了会不会用考虑啊, 欸似乎不用考虑因为 $\mathbb{F}_p$ 是域所以系数都可逆所以不会因为系数而导致一个东西变成可约的, 比如 $\mathbb{F}_3[x]$ 中的 $\bar{2}x + \bar{2}$ 就不可约, 但 $\mathbb{Z}[x]$ 中的 $2x + 2$ 就是可约的. 那么问题来了, 我们什么时候讨论容度呢？对于 $\mathbb{F}_3[x]$ 中的 $\bar{2}x + \bar{2}$ 讨论不讨论其容度呢？唉讨论不讨论的都与此问题无关, 我现在只需要知道 $\mathbb{F}_2[x]$ 中不会因为系数出现可约性了.）域上二阶多项式的非平凡分解只有两个一次多项式的乘积, 倘若能分解成一次多项式的乘积便意味着在 $\mathbb{F}_2$ 中有根, 代入 $\bar{0}$ 和 $\bar{1}$ 发现均不为 $\bar{0}$, 因此无根, 因此无非平凡分解, 因此 $x^2 + x + \bar{1}$ 确实不可约.

我可以直接预测 $\mathbb{F}_2[x]/(x^2+x+\bar{1})$ 是 $\mathbb{F}_2$-2 维线性空间, 并且有基 $\{1, u\}$, 其中 $u = x+(x^2+x+\bar{1})$.

$\mathbb{F}_4$ 中元素形如 $a \cdot \bar{1} + b \cdot u$, 其中 $a, b \in \mathbb{F}_2$. 因此 $|\mathbb{F}_4| = 4 = 2^2$. 底数 2 是 $\mathbb{F}_2$ 有两个元素的 2, 指数 2 是 f 的次数.

在 $\mathbb{F}_4[x]$ 中, 我知道 $x - u$ 一定是 $x^2 + x + \bar{1}$ 的因子, 也就是 u 一定是 $x^2 + x + \bar{1}$ 在 $\mathbb{F}_4$ 中的根. 然后用朴素的凑的方法就能将 $x^2 + x + \bar{1} = (x - u)(x + u + 1)$ 找出来.

9 欧式整环

定义 9.1. 整环 R 称为欧几里得整环, 如果存在 *size function*

$$\varphi : R^{\times} : R\backslash\{0\} \to \{0,1,2,\cdots\}$$

使得任意 $a,b \in R^{\times}$ 存在 $q,r \in R$ 使得 $a = qb + r$, 其中 $r = 0_R$ 或者 $\varphi(r) < \varphi(b)$.

注记. q,r 一般不唯一.

定理 9.2. 欧几里得整环是主理想整环.

证明. 任取 $0 \neq I \triangleleft R$, 存在 $0 \neq b \in I$ 使得 $\varphi(b)$ 最小. 断言：$(b) = I$. 只证 $I \subset (b)$.

对任意 $a \in I$,$a = qb + r$, 则 $r = a - qb \in I$. 按照我们对 b 的选取, 只能 $r = 0_R$. 所以 $b \mid a$. □

注记. 存在主理想整环不是欧几里得整环.

定理 9.3. $\mathbb{Z}[\sqrt{-1}] = \left\{m + n\sqrt{-1}\middle|m,n \in \mathbb{Z}\right\}$ 是欧几里得整环从而是主理想整环.

证明. 断言,$\left(\mathbb{Z}[\sqrt{-1}]\right)^* \to \mathbb{Z}, m + n\sqrt{-1} \mapsto m^2 + n^2$ 是 size function.

对任意的 $x,y \in \mathbb{Z}[\sqrt{-1}]$,

$$\frac{x}{y} = \frac{x \cdot \bar{y}}{N(y)} = \alpha + \beta\sqrt{-1} \xlongequal{\text{取整}} (m + n\sqrt{-1}) + ((\alpha - m) + (\beta - n)\sqrt{-1})$$

其中 $\alpha, \beta \in \mathbb{Q}, m,n \in \mathbb{Z}, |\alpha - m| \leqslant \dfrac{1}{2}, |\beta - n| \leqslant \dfrac{1}{2}$.

令 $q = m + n\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$,$r = y \cdot ((\alpha - m) + (\beta - n)\sqrt{-1}) = x - qy \in \mathbb{Z}[\sqrt{-1}]$.

断言 $N(r) < N(y)$.

$$N(r) = N(y) \cdot ((\alpha - m)^2 + (\beta - n)^2) \leqslant N(y)\left(\frac{1}{4} + \frac{1}{4}\right) < N(y).$$

□

例 9.4. 计算 $\gcd(4 + 7\mathrm{i}, 3 + 4\mathrm{i})$.

定理 9.5. $\mathbb{Z}[\sqrt{-2}]$ 是欧几里得整环从而是主理想整环.

证明. $\dfrac{x}{y} = q + r', r' = \varepsilon + \eta\sqrt{-2}, |\varepsilon| \leqslant \dfrac{1}{2}, |\eta| \leqslant \dfrac{1}{2}, N(r') \leqslant \left(\dfrac{1}{4} + \dfrac{1}{4} \cdot 2\right) < 1.$ □

容易看出上述证明对 $\mathbb{Z}[\sqrt{-3}]$ 来说不再适用.

例 9.6. $2 \in \mathbb{Z}[\sqrt{-3}]$ 是不可约元, 但不是素元, 从而 $\mathbb{Z}[-3]$ 不是主理想整环.

证明.

- 2 不可约. 设 $2 = xy$, 则 $4 = N(x)N(y)$, 则 $N(x) = 1$ 或 $N(y) = 1$.
- 2 非素元.

□

10 Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$

命题 10.1. $U(\mathbb{Z}[\mathrm{i}])=\{\pm 1,\pm \mathrm{i}\}$.

证明. 设 $x,y\in\mathbb{Z}[\mathrm{i}]$ 满足 $xy=1$, 两侧取范数得到 $N(x)N(y)=1$, 这迫使 $N(x)=N(y)=1$, 因此 $U(\mathbb{Z}[\mathrm{i}])\subset\{\pm 1,\pm \mathrm{i}\}$, 反包含关系是显然的. □

引理 10.2. *设 $z\in\mathbb{Z}[\mathrm{i}]$, 若 $N(z)=p$ 是素数, 则 z 是 Gauss 素数.*

定理 10.3 (Fermat 二平方和定理)**.**

证明.

- Step1 证明：$\mathbb{Z}[x]/(x^2+1)\cong\mathbb{Z}[\mathrm{i}]$.

  定义 $\theta:\mathbb{Z}[x]\to\mathbb{Z}[\mathrm{i}], f(x)\mapsto f(i)$, 由同态基本定理,$\mathbb{Z}[x]/\ker\theta\cong\mathbb{Z}[\mathrm{i}]$.

  容易验证 $(x^2+1)=\ker\theta$.

□

定理 10.4.

证明.

$\Longleftarrow (1^2+1^2)^l(0^2+p_1^2)^{\frac{m_i}{2}}(a_i^2+b_i^2)^{m_i}$

$\Longrightarrow$

存在 $z\in\mathbb{Z}[i]$, 使得 $N(z)=n$.

断言, 存在素因子分解,

$$z=z_1\cdots z_t, z_i$$

$N(z)=N(z_1)\cdots N(z_t)$ □

$Spez\mathbb{Z}[\mathrm{i}]$

回忆：设 $R\subset S$ 是子环, 任给 $q\in Spec(S)$,$q\cap R\in\mathrm{Spec}(R)$

映射

$$\mathrm{Spec}(S)\to\mathrm{Spec}(R), q\mapsto q\cap R$$

连续映射, 不一定是满射, 下面的例子很幸运是满射

例 10.5.

$$\mathbb{Z}\hookrightarrow\mathbb{Z}[\mathrm{i}]$$

$$\mathrm{Spec}(\mathbb{Z})$$

$$(1+\mathrm{i})\cap\mathbb{Z}\supset 2\mathbb{Z}$$

由于 $2\mathbb{Z}$ 是极大理想,1 又不包含在里面, 所以上面是等号

$$\mathbb{Z}/2\mathbb{Z}\hookrightarrow\mathbb{Z}[\mathrm{i}]/(1+\mathrm{i})$$

例 10.6. $\mathbb{F}_5 \hookrightarrow \mathbb{Z}[\mathrm{i}]/(1+2\mathrm{i})$

断言, 任意 z, 模 $(1+2\mathrm{i})$ 同余于 $0,1,2,3,4$.

$$\mathrm{i}-2 \in (1+2\mathrm{i}), z = m+n\mathrm{i} \equiv m+2n \equiv 0,1,2,3,4$$

命题 10.7. 设 $a+b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, 且 $a^2+b^2=p$ 为素数, 则 $\mathbb{Z}[\mathrm{i}]/(a+b\mathrm{i}) \cong \mathbb{F}_p$.

证明. 因为 $a^2+b^2=p$ 是素数, 所以 $(a,b)=1$. 由 Bezout 等式, 存在整数 u,v 使得 $au+bv=1$. 于是 $(a+b\mathrm{i})(v+u\mathrm{i}) = (av-bu)+\mathrm{i}$, 这表明在 $\mathbb{Z}[\mathrm{i}]/(a+b\mathrm{i})$ 中, 存在 $r \in \mathbb{Z}$ 使得 $\bar{\mathrm{i}} = \bar{r}$. 又因 $\bar{p} = \bar{0}$, 所以对任意的 $c+d\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ 有 $\overline{c+d\mathrm{i}} = \overline{c+dr} = \bar{n}$, 其中 $n \in \{0,1,\cdots,p-1\}$. 容易验证 $\{0,1,\cdots,p-1\}$ 中元素两两不同余, 因此 $\mathbb{Z}[\mathrm{i}]/(a+b\mathrm{i}) \cong \mathbb{F}_p$. □

引理 10.8. 设 p 是素数且 $p \equiv 1 \mod 4$, 那么存在整数 m 满足 $m^2 \equiv -1 \mod p$.

证明. □

11 唯一分解整环

定义与基本性质

定义 11.1. 设 R 是整环. 如果 R 满足

(1) 对任意 $a \neq 0$ 且 $a \notin U(R)$, 存在不可约分解 $a = c_1c_2\cdots c_r$，其中 c_i 是不可约元.

(2) 若 $a = c_1c_2\cdots c_r = c_1'c_2'\cdots c_t'$ 都是不可约分解, 则 $t = r$, 且在相差一个置换的意义下 $c_i \sim c_i'$.

则称 R 为唯一分解整环，简称 UFD.

命题 11.2. 设 R 是 UFD, 则不可约元都是素元.

证明. 设 $a \in R$ 是不可约元. 假设 $a \mid bc$, 则存在 d 使得 $ad = bc$.
对 b, c, d 作不可约分解, 由不可约分解的唯一性知 $a \mid b$ 或 $a \mid c$. □

因此 UFD 中的不可约分解也是素分解.
在 a 的不可约分解中，我们将相伴的元素合并，得到所谓的标准分解

$$a = up_1^{n_1}\cdots p_r^{n_r}$$

其中 $u \in U(R), p_i$ 不可约,$p_i \not\sim p_j, i \neq j, n_i \geqslant 1$. 易知 a 的因子的形式总为

$$vp_1^{m_1}\cdots p_r^{m_r}, \quad v \in U(R), 0 \leqslant m_i \leqslant n_i.$$

由此我们还知道 a 的因子在相伴的意义下的个数为 $(n_1+1)\cdots(n_r+1)$.

命题 11.3. gcd, lcm 总存在

证明. □

引理 11.4. 设 R 是 UFD，$\gcd(a, b) \sim 1$，那么 $a \mid bc \Longrightarrow a \mid c$.

命题 11.5. 设 R 是唯一分解整环，$K = Frac(R)$，那么任给 K 中的元素 $\frac{a}{b}$，存在既约形式 $\frac{a'}{b'} = \frac{a}{b}$，其中 $\gcd(a', b') \sim 1$. 既约形式在相伴的意义下是唯一的.

证明. 设 $\frac{a}{b} = \frac{c}{d}$，其中 $\gcd(a, b) \sim \gcd(c, d) \sim 1$. 因为 $ad = bc$，用两次上面的引理有 $a \mid c$ 和 $c \mid a$，从而 $a \sim c$，同理 $b \sim d$. 任给 $\frac{a}{b}$，设 $a = a'\gcd(a, b), b = b'\gcd(a, b)$，则 $\frac{a'}{b'}$ 便是 $\frac{a}{b}$ 的既约形式. □

Noether 环 $\Longrightarrow$ 存在不可约分解

定义 11.6. 设 R 是整环，如果任意 $I \lhd R$ 都是有限生成的，则称 R 为 Noether 环.

定理 11.7 (Hilbert 基定理)**.** 设 R 是 Noether 环，则 $R[x]$ 也是 Noether 环.

证明. 参见代数几何笔记. □

命题 11.8. *Noether* 环中不存在真理想的无限升链.

证明. □

定理 11.9. 任何 *Noether* 整环都有不可约分解.

证明. $0 \neq a \notin U(R)$, 我们要证明 a 有不可约分解.

否则, 若存在 a 没有不可约分解, 则 a 一定可约,$a = a_1 a_1'$ 并且 $a_1, a_1' \notin U(R)$, 设 a_1 没有分解.

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

□

没有不可约分解的整环的例子https://math.stackexchange.com/questions/96790/integral-domain-that-is-not-a-factorization-domain

一些一般性命题

命题 11.10. 设 R 为整环，若 a 有素分解，则 a 的不可约分解唯一

证明. □

推论 11.11. 设 R 有不可约分解，则 R 为 UFD $\Longleftrightarrow$ 不可约元是素元

证明. □

推论 11.12. PID 是 UFD.

一些例子

例 11.13. 内容...

例 11.14. $\mathbb{Z}[\sqrt{-5}]$

Gauss 定理

定理 11.15. 设 R 为 UFD，则 $R[x]$ 是 UFD.

证明. □

12 小结

- 我们讨论的环含幺交换
- 整环：无零因子.
- 整环是我们讨论各种具有良好性质的环是最先加上的要求.
- 整环中可以讨论整除、公因子的概念.

	整环	UFD	PID	ED
最大公因子	不一定存在, 相伴意义下至多唯一	存在	存在, 有 Bezout 等式	可以用辗转相除法算
不可约元		是素元	是素元	

- 素元与素理想的关系比较微妙. 一方面, 素理想不一定是主理想, 因此不是每个素理想都能对应到在相伴意义下唯一的素元；另一方面, 零理想是素理想, 但规定零元不是素元.
- 谈论到素元就是它生成的主理想就是素理想.
- 理想的包含关系是整除关系的推广, 但不完全是整除关系, 当素理想是主理想时, 就可以理解为是整除关系.
- 素元都是不可约元.
- 约定不可约元不是零元, 不是可逆元.
- 不可约元的定义是只有平凡分解.

Chapter 2

域论

1 域扩张

定义 1.1 (域扩张)**.** 域扩张是指域的单同态 $\theta : k \hookrightarrow K$, 记作 K/k.

- k 到 K 可能有不同的单同态, 不同的同态要视作不同的域扩张.

命题 1.2. 设 $\theta : k \hookrightarrow K$ 是域扩张, 则 K 上有 k-线性空间结构.

证明.

- 线性空间的加法就是域的加法.
- 线性空间的数乘定义为 $\lambda v = \theta(\lambda) \cdot v$, 其中 $\cdot$ 是域的乘法.
- 线性空间的加法不依赖于域扩张 θ, 但乘法依赖.
- 既然有 k-线性空间结构, 我们便可以讨论 $\dim_k K$ 和 k-基.

□

定义 1.3 (域扩张同构)**.** 称域扩张 $\theta : k \hookrightarrow K$ 和 $\theta' : k \hookrightarrow K'$ 同构, 若存在域同构 $\varphi : K \to K'$, 使得 $\theta' = \varphi \circ \theta$, 即使得下列图表交换

$$\begin{tikzcd} & K \arrow[dd, dashed, "\varphi"] \\ k \arrow[ur, hook, "\theta"] \arrow[dr, hook, "\theta'"'] & \\ & K' \end{tikzcd}$$

也称 φ 为 θ 到 θ' 域扩张同构.

命题 1.4. 域扩张同构 $\varphi : K \to K'$ 同样是 k-线性同构.

证明. $\varphi(\lambda v) = \varphi(\theta(\lambda)v) = \varphi(\theta(\lambda))\varphi(v) = \theta'(\lambda)\varphi(v) = \lambda\varphi(v)$. □

例 1.5. 设 $f(x) \in k[x]$ 是不可约元,$d := \deg f(x) \geqslant 2$, 那么

$$f(x)\text{是不可约元} \xrightarrow{PID} f(x)\text{是素元} \longrightarrow (f(x))\text{是素理想} \xrightarrow{PID} (f(x))\text{是极大理想}.$$

因此 $K := k[x]/(f(x))$ 是域.

- 这个例子还算已经看得比较清楚了
- $k \hookrightarrow k[x] \twoheadrightarrow K, \lambda \mapsto \lambda \mapsto \lambda + (f(x))$
- $u := x + (f(x))$
- K 是 k 上 d 维线性空间, 有一组基是 $\{1, u, \cdots, u^{d-1}\}$
- $k[x] \subset K[x]$
- $f(x)$ 在 $k[x]$ 中不可约 $\Leftrightarrow f(x)$ 在 $k[x]$ 中无真因式.
- $f(x)$ 在 k 上无根 $\Leftrightarrow f(x)$ 在 $k[x]$ 中无一次因式.
- 不可约一定无根, 无根不一定不可约. 不可约才可以做添根构造.
- $u \in \mathrm{Root}_K f$.
- 这个例子是 $k[x]$ 的商域作为 k 的扩域, 下一个例子是 $k[x]$ 的分式域作为 k 的扩域.

例 1.6.

定义 1.7 (域扩张自同构)**.** 称 $\theta : k \to K$ 到自身的域扩张同构为 θ 的域扩张自同构,θ 的域扩张自同构全体记作 $\mathrm{Aut}(K/k)$.

- $\mathrm{Aut}(K/k) \subset \mathrm{Aut}(K)$ 是子群.
- 如果视 θ 为包含, 那么域扩张自同构就是使得 k 不动的自同构.
- $\mathrm{Aut}(K/k)$ 基本上有限,$\mathrm{Aut}(K)$ 基本上无限.

定义 1.8 (代数元与超越元)**.** 称 $\alpha \in K$ 为 k 上代数元, 如果存在 $f(x) \in k[x] \subset K[x]$ 使得 $f(\alpha) = 0_K$. 否则, 称 α 为 k 上超越元.

2 分裂域

- 分裂域是域扩张而不是扩域.
- 对于有高次不可约因式的多项式, 分裂才是有效的.
- 分裂域是有限生成的代数扩张.

例 2.1. 求 $x^2+x+\bar{1}\in\mathbb{F}_2[x]$ 的分裂域.

例 2.2. $x^3-2\in\mathbb{Q}[x]$, 令 $E=\mathbb{Q}(\sqrt[3]{2},\omega), Q\hookrightarrow E$, 要算 $\operatorname{Aut}(E/\mathbb{Q})=\operatorname{Aut}(E)$ 一般这里不是等号.

解. $|\operatorname{Aut}(E)|\leqslant 6$. □

例 2.3. $\mathbb{F}_4$

定义 2.4. $0\neq f(x)\in k[x]$ 有重根, 若存在某一个 E/k, 某个 $a\in E$, 使得

$$(x-a)^2\mid f(x) inE[x].$$

反之称为无重根.

例 2.5. $(x^2+1)^2\in\mathbb{R}[x]$ 有重根.

注记. 这个定义不好因为一般无法验证.

引入形式微分

$$f(x)=a_nx^n+\cdots a_1x+a_0\in k[x]$$

定义形式微分

$$f'(x)=(na_n)x^{n-1}+\cdots+(2a_2)x+a_1\in k[x]$$

例 2.6. $x^p\in\mathbb{F}^p$. 它的形式微商是 0.

注记. 特征零的时候次数是 $n-1$, 特征 p 的时候可能会小于 $n-1$.

可验证,Lebniz 法则

$$(f(x)g(x))'=f'(x)g(x)+f(x)g'(x).$$

引理 2.7. $f(x)\in k[x]$ 无重根当且仅当 $\gcd(f(x),f'(x))=1$

证明. $\Longrightarrow$ 否则,$\gcd(f,f')=g(x),\deg g\geqslant 1$. 取域扩张 $k\hookrightarrow K$ 使得 g 在 K 上成立. □

定义 2.8. $0\neq f(x)\in k[x]$ 称为 k 上可分的, 若 $f(x)$ 的不可约因子均无重根.

定理 2.9. $f(x)\in k[x]$, 取 $k\hookrightarrow E$ 为 $f(x)$ 的分裂域.
$f(x)$ 在 k 上可分当且仅当 $|\operatorname{Aut}(E/k)|=\dim_k E$.

证明. □

3 有限域

- char $E = p$
- $\mathbb{F}_p \hookrightarrow E$
  - $E/\mathbb{F}_p$ 是域扩张.
  - E 成为 $\mathbb{F}_p$-线性空间.
- 设 $\dim_{\mathbb{F}_p} E = n$,$E \cong \mathbb{F}_p^n \Longrightarrow |E| = p^n$.

定义 3.1. $\sigma : E \to E, a \mapsto a^p$, 断言 σ 是环同构.*Frobenius* 自同构.

注记. $\sigma(n) = n$,$p \mid (n^p - n)$.

3.1 单位群

我们需要群论中的以下结果

引理 3.2. 任意 $a \in E^\times$, 都有

$$a^{p^n - 1} = 1.$$

推论 3.3. 任意 $a \in E$, 都满足方程

$$x^{p^n} - x = 0.$$

定理 3.4. 对任意 $n \geqslant 1$, 存在且唯一存在 p^n 元域, 记作 $\mathbb{F}_{p^n}$.

证明.

- 至多唯一性. 假设 E 存在, 断言 $E/\mathbb{F}_p$ 是 $x^{p^n} - x \in \mathbb{F}_p[x]$ 的分裂域.
  - 由推论3.3,E 中元素都是 $x^{p^n} - x$ 的根. 由于 E 恰有 p^n 个元素, 所以 E 正好是 $x^{p^n} - x$ 的所有根的集合, 从而 $x^{p^n} - x$ 在 E 上分裂.
  - 第二条是显然的.

  由分裂域的唯一性知 E 存在则唯一.
- 存在性. 取 E 为 $x^{p^n} - x \in \mathbb{F}_p[x]$ 的分裂域, 考虑

$$K = \left\{ a \in E \middle| a^{p^n} - a = 0 \right\} \subset E.$$

  - K 是子域.
  - $E = \mathbb{F}_p(K) = K$.
  - $x^{p^n} - x$ 无重根 $\Longrightarrow |E| = p^n$.

□

命题 3.5.

$$x^{p^n}-x=\prod_{d|n}\prod_{\text{首一}d\text{次不可约}}f(x)$$

是 $x^{p^n}-x$ 在 $\mathbb{F}_p[x]$ 中的不可约分解.

证明. □

3.2 分类子域

设 $|E|=p^n$, 则

- $K\subset E$ 是子域 $\Longrightarrow |K|=p^d, d\mid n$.
- 对任意 $d\mid n$, 存在唯一子域 $K\subset E$ 使得 $|K|=p^d$.

证明.

- $\mathbb{F}_p\subset K\subset E$, 由维数公式得 $d\mid n$.
-

□

3.3 $E/\mathbb{F}_p$ 是单扩张

设 $n=q_1^{n_1}\cdots q_s^{n_s}$, 其中 q_i 是素数.

- E 恰有 s 个极大真子域 K_i, 其中 $|K_i|=p^{\frac{n}{q_i}}$.
- $\bigcup_{i=1}^{s}K_i\neq E$.
  - 即使将 K_i 中的元素单独计数,$\sum_{i=1}^{s}p^{\frac{n}{q_i}}\leqslant s\cdot p^{\frac{n}{2}}<p^n$.
- 因此存在 $u\in E$, 它不在任意的 K_i 里.
- $\mathbb{F}_p(u)=E$,$E/\mathbb{F}_p$ 是单扩张!
- u 的最小多项式 f 的次数为 n.
- 断言, 任意 $1\leqslant i\leqslant n-1$,$\sigma^i(u)\neq u$.
  - 首先,$\sigma^n(u)=u^{p^n}=u$. 所以存在最小的正整数 d, 使得 $\sigma^d(u)=u$.
  - 断言 $d\mid n$.
    - $n=dm+d'$,$d'<d$.$\sigma^n=\sigma^{d'}\circ(\sigma^d)^{q'}$
    - $u=\sigma^n(u)=\sigma^{d'}(u)$, 与 d 的最小性矛盾.
  - u 落在 p^d 阶子域里, 但 $\mathbb{F}_p(u)=E$, 所以 $d=n$.
- $\sigma^i(u)\neq\sigma^j(u)$, 任意 $1\leqslant i\neq j\leqslant n-1$.

- $f(x) = \prod_{i=0}^{n-1}(x - \sigma^i(u))$
  - $f(u) = 0 \Longrightarrow f(\sigma^i(u)) = 0.$

4 分圆域

- n 次单位根,$\zeta^n = 1$.
    - ζ 当然是多项式 $x^n - 1$ 的根, 但对一般域来说无法断言它是否有 1 之外的非平凡单位根.
    - 如果 ζ 是 n 次单位根, 那么对于任意正整数 k,ζ^k 也是 n 次单位根. 但不知道通过这种方式能得到多少新的 n 次单位根, 甚至有可能得不到新的 n 次单位根.
    - $\mathbb{C}$ 中 n 次单位根都形如 $\mathrm{e}^{2\pi\mathrm{i}k/n}, k = 0, 1, 2, \cdots, n-1$.
    - $\mathbb{C}$ 中 $x^n - 1 = \prod\limits_{\zeta^n=1}(x - \zeta)$.
- 单位根的阶：使得 $\zeta^n = 1$ 成立的最小正整数 n. 此时称 ζ 为 n 次本原单位根.
    - 设 ζ 是 n 次本原单位根, 则 $\zeta^0, \zeta^1, \zeta^2, \cdots, \zeta^{n-1}$ 都是 n 次单位根且两两不同.
        * 都是 n 次本原单位根显然.
        * 设 $\zeta^r = \zeta^s$, 其中 $0 \leqslant r < s \leqslant n-1$. 那么 $\zeta^{s-r} = 1$, 其中 $s - r \leqslant n - 1$, 这与 ζ 是 n 次本原单位根矛盾.
    - $\mathbb{C}$ 中对任意 n 都存在 n 次本原单位根, 而不管 n 是素数还是合数.
    - 上上条是说, 只要存在 n 次本原单位根, 便可以由它生成全部的 n 次单位根.
    - 对于 n 次单位根的全体, 它显然是群. 但不太清楚它的结构.
    - 如果存在 n 次本原单位根, 群是循环群, 本原单位根是生成元.
    - 设 ζ 是 n 次本原单位根, 则 ζ^m 也是 n 次本原单位根当且仅当 $(m, n) = 1$.
        * $\Longrightarrow$ 设 $m = dr, n = ds$, 则 $(\zeta^m)^s = (\zeta^n)^r = 1$, 这与 ζ^m 是 n 次本原单位根矛盾.
        * $\Longleftarrow$ 设 ζ^m 不是 n 次本原单位根, 则存在 $1 \leqslant d \leqslant n-1$ 使得 $\zeta^{md} = 1$, 从而 $n \mid md$. 因为 $(m, n) = 1$, 所以 $n \mid d$, 这与 $1 \leqslant d \leqslant n - 1$ 矛盾.
- 如果域特征为 p, 那么 p 次单位根只有 1 自己.
    - $\omega^p - 1 = \omega^p - 1^p = (\omega - 1)^p = 0 \Longrightarrow \omega = 1$.

Chapter 3

群

1 群的基本定义

- 群的定义.
- 乘法左右消去律.
- 求逆运算是双射. 群同构 $\Longleftrightarrow G$ 是 Abel 群.
- 子群：非空集合对乘法和求逆运算封闭.
  - 非空与对求逆运算封闭推出 $1_G \in H$.

定义 1.1. *群,Group,$(G,\cdot)$,G 是一个非空集合,$\cdot : G \times G \to G$, 满足*

$(G1)$ *结合律.*

$(G2)$ *有幺元. 存在 1_G, 对于任意 a, 成立 $a \cdot 1_G = a = 1_G \cdot a$.*

$(G3)$ *有逆元. 任意 $a \in G$, 存在 $b \in G$ 使得 $a \cdot b = 1_G = b \cdot a$.*

- 幺元唯一.
  - $1'_G = 1'_G 1_G = 1_G$.
- 逆元唯一
  - $b = b \cdot 1_G = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = 1_G \cdot b' = b'$

定义 1.2. *群 G 称为 Abel 群, 若 $a \cdot b = b \cdot a$, 任意 $a,b \in G$.*

- 左右乘法消去律
  - $a \cdot b = a \cdot c \Longrightarrow b = c$.
  - $b \cdot a = c \cdot a \Longrightarrow b = c$.
- $(a^{-1})^{-1} = a$.
- $(-)^{-1} : G \to G, g \mapsto g^{-1}$, 双射.

  - 满射, 任意元素都可以写成它的逆的逆.
  - 单射, 逆元唯一.
- $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.
- 任意 $n \in Z$,$a^n \in G$.
  - 任意 $n, m \in \mathbb{Z}$,$a^{n+m} = a^n \cdot a^m$.

定义 1.3. $\varnothing \neq H \subset G$ 是子群, 若对任意 $a, b \in H$,

$(SG1)$ $a \cdot b \in H$.

$(SG2)$ $a^{-1} \in H \Longrightarrow 1_G \in H$.

记作 $H \leqslant G$.

- $(H, \cdot)$ 也是群.
- $\{1_G\} \leqslant G, G \leqslant G$.

2 群的例子

例 2.1.

(1) 来自环.R 环.

- R 的加法群.$(R,+)$.$Abel$ 群. 不关心.
- R 的单位群.$U(R)$.$Abel$ 群.
- R 的自同构群.$\mathrm{Aut}(R)$. 非空,$\mathrm{Id}_R \in \mathrm{Aut}(R)$. 一般不 *Abel*.
- $R = \mathbb{Z}$.
  - $(\mathbb{Z},+)$.
  - $U(\mathbb{Z}) = \{\pm 1\}$.
  - $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}\}$.
- $R = \mathbb{Z}_n$,$n \geqslant 2$.
  - $(\mathbb{Z}_n,+)$, 有限群.
  - $U(\mathbb{Z}_n) = \big\{\bar{m}\big| \gcd(m,n) = 1\big\}$,$\phi(n)$ 阶群.
  - $\mathrm{Aut}(\mathbb{Z}_n) = \{\mathrm{Id}_{\mathbb{Z}_n}\}$.
- $R = \mathbb{Z}[\mathrm{i}]$.
  - $(\mathbb{Z}[\mathrm{i}],+)$, 秩为 2 的自由 $Abel$ 群.
  - $U(\mathbb{Z}[\mathrm{i}]) = \{\pm 1, \pm \mathrm{i}\}$, 四阶循环群.
  - $\mathrm{Aut}(\mathbb{Z}[\mathrm{i}]) = \big\{\mathrm{Id}_{\mathbb{Z}[\mathrm{i}]}, \sigma\big\}$.
- 域扩张 K/k
  - $\mathrm{Aut}(K/k) \leqslant \mathrm{Aut}(K)$.

(2) 来自矩阵.

- $GL_n(\mathbb{C})$
- $SL_n(\mathbb{C}) \leqslant GL_n(\mathbb{C})$
- $GL_n(\mathbb{R}) \leqslant GL_n(\mathbb{C})$
- $SL_n(\mathbb{R}) \leqslant GL_n(\mathbb{R})$
- $O_n = \big\{A \in GL_n(\mathbb{R})\big| AA^T = I_n\big\}$
- $SO_n \leqslant O_n$
  - $P \subset \mathbb{R}^n$,P 的对称群 $\Sigma(P) = \big\{g \in O_n\big| g(P) = P\big\} \leqslant O_n$.
  - $g \in \Sigma(P)$, 称为 P 的对称.

(3) 对称群.X 抽象集合, 置换 $\sigma : X \to X$ 双射.

X 的对称群 $S(X) = \{X\text{上的所有置换}\}$.

定理 2.2. 任何群本质上都是对称群的子群.

3 陪集分解与 Lagrange 定理

- 陪集分解
- Lagrange 定理及其证明
- 元素的阶
  - 若 $\mathrm{ord}(a)=d$, 则 $a^n=1 \iff d \mid n$.
  - $|G|<\infty$,$a\in G$, 则 $\mathrm{ord}(a)\big||G|$.
    - $H=\left\{1,a,a^2,\cdots,a^{d-1}\right\}$ 是子群！用 Lagrange 定理！

命题 3.1. 设 $H\leqslant G$, 下列四种关系都是等价关系：

(1) $aH=bH$

(2) $a^{-1}b\in H$

(3) $Ha=Hb$

(4) $ab^{-1}\in H$

且 (1) 与 (2) 诱导的等价关系相同,(3) 与 (4) 诱导的等价关系相同.

证明. 容易验证它们四个都是等价关系. 只证 (1) $\iff$ (2),(3) $\iff$ (4) 同理.

- 设 $a^{-1}b\in H$, 即存在 $h\in H$ 使得 $a^{-1}b=h$.
  - 任取 $ah'\in aH$, 由于 $a=bh^{-1}$, 所以 $ah'=bh^{-1}h'\in bH$, 从而 $aH\subset bH$.
  - 任取 $bh'\in aH$, 由于 $b=ah$, 所以 $bh'=ahh'\in aH$, 从而 $bH\subset aH$.
- 设 $aH=bH$. 则存在 $h,h'\in H$ 使得 $ah=bh'$, 从而 $a^{-1}b=hh'^{-1}\in H$.

□

定义 3.2. 称 $G=\bigsqcup\limits_{a\in I}Ha$ 为 G 关于子群 H 的右陪集分解.

注记. Ha 一般不是子群, 但我们将要看到,H 的共轭 aHa^{-1} 是子群！

命题 3.3. $|Ha|=|H|$.

定理 3.4 (Lagrange 定理)**.** 设 G 是有限群,$H\leqslant G$, 则 $|G|=[G:H]\cdot|H|$.

定义 3.5. $a\in G$ 的阶 $\mathrm{ord}(a)$, 最小的 $d>0$ 使得 $a^d=1$.

事实. 若 $|G|<\infty$, 则 $a\in G$,$\mathrm{ord}(a)<\infty$.

事实. 若 $a\in G$ 有 $ord(a)=d<+\infty$, 则 $a^n=1_G \iff d\mid n$.

命题 3.6. $|G|<\infty$,$a\in G$. 则 $\mathrm{ord}(a)\big||G|$.

证明. $H=\left\{1,a,\cdots,a^{d-a}\right\}$ 是 G 的子群而且两两不同. □

例 3.7 (Fermat 小定理)**.** 设 p 是素数, 考虑 $\mathbb{F}_p^{\times}$,$a^{p-1} \equiv 1 \mod p$.

例 3.8. $U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
ord	1	2	2	2

例 3.9. $(\mathbb{Z}_4, +)$ 加法群.

定义 3.10. $f : G \to G'$ 称为群同态若 $f(a \cdot b) = f(a) \cdot f(b)$

注记. 蛮神奇的嗷, 群同态只需要保持群乘法, 自然推出保持逆

但是拓扑群就要求群乘法是连续的, 逆是连续的.

定义 3.11. 称 $f : G \to G'$ 是群同构, 如果 f 是群同态且是双射.

事实. 若 $f : G \to G'$ 同构,$a \in G$, 则 $\operatorname{ord}(a) = \operatorname{ord} f(a)$.

推论 3.12. $U(\mathbb{Z}_8) \not\simeq \mathbb{Z}_4$.

例 3.13.

- $H \leqslant G$, 嵌入映射是同态.
- G, K 是群, 直积 $G \times K = \big\{(g, h) \big| g \in G, h \in H\big\}$,$(g, h) \cdot (g', h') := (g \cdot g', h \cdot h')$.

例 3.14. 设 $\mu_2 = \{1, -1\}$, 乘法群.

Klein 四元群 $V_4 = \mu_2 \times \mu_2$.

4 循环群

- $U(\mathbb{Z}_8)$.
- $\mathbb{Z}_4$.
- 群同态.
- 设 $f: G \to G'$ 是群同构, 则 $\mathrm{ord}(a) = \mathrm{ord}(f(a))$.
  - 元素的阶是群同构不变量!
- 群的直积.
- $\mu_2 \times \mu_2$
- 循环群.
- 本质上循环群只有 $\mathbb{Z}$ 和 $\mathbb{Z}_n$.

设 $X \subset G$, 记 (X) 为 G 中包含 X 的最小子群.

称 $X \subset G$ 为 G 的生成元集, 若 $(X) = G$.

定义 4.1. *群 G 称为循环群, 若存在 $a \in G$, 使得 $(a) = G$.*

命题 4.2. *设 G 为循环群, 则 G 同构于 $\mathbb{Z}$ 或 $\mathbb{Z}_n$.*

证明. □

命题 4.3. *设 $G(a)$ 是循环群.*

(1) 若 $|G| = +\infty$, 则

- G 的生成元只有 a 和 a^{-1}.
- G 的子群
  - $\{1_G\}$
  - $(a^d) = \left\{\cdots, a^{-d}, 1_G, a_d, \cdots\right\}$
- a_d 同构于 G.

(2) 若 $|G| = n$

- G 恰有 $\phi(n)$ 个生成元 $\left\{a^k \middle| \gcd(k,n) = 1\right\}$
- 任意 $d \mid n$, 存在且唯一存在 d 阶子群 $H_d = (a^P \dfrac{n}{d}) \leqslant G = \left\{1, a^{\frac{n}{d}}, a^{\frac{2n}{d}}, \cdots\right\}$

注记. 循环群对任意因子有子群且唯一, 其他不一定哦.

命题 4.4. *$|G| = n < \infty$, 则 G 循环 $\Longleftrightarrow G$ 含有 n 阶元.*

- K_4 不是循环群.
- $\mu_2 \times \mu_3 \simeq \mu_6$

- 容易验证 $\mathrm{ord}(-1,\omega)=6$.

- $\mathbb{Z}_2\times\mathbb{Z}_3\simeq\mathbb{Z}_6$.

  - 跟中国剩余定理有什么关系?

- p 是素数,$|G|=p\Longrightarrow G$ 是循环群.

定理 4.5. 设 $|G|=n<\infty$, 则 G 是循环群当且仅当对任意 $d\mid n$, 至多存在一个 d 阶子群.

证明. 任意 $d\mid n$, 考虑 $S_d=\left\{g\in G\middle|\,\mathrm{ord}(g)=d\right\}$, 要证 S_n 非空.

若 $S_d\neq\varnothing$, 存在 G 中 d 阶子群 $H_d.S_d\subset H_d$ 这个包含关系用到了至多唯一性. 所以 $|S_d|\leqslant\phi(d)$.

$$n=|G|=\sum_{d|n}\leqslant\sum_{d|n}\phi(d)=n$$

□

定理 4.6. k 域.$G\leqslant k^\times$ 有限子群, 则 G 循环群.

定理 4.7.

例 4.8. $\mathbb{F}_9=\mathbb{F}_3[x]/(x^2+\bar{1})$.

例 4.9. $\mathbb{C}^\times$ 的有限子群

5 正规子群与商群

定义 5.1. 设 G 是群, 称 $N \leqslant G$ 为正规子群, 如果对任意 $a \in G$, 成立 $aN = Na$. 记作 $N \lhd G$.

- $N \lhd G \Longleftrightarrow N = aNa^{-1} \Longleftrightarrow aN = Na$.
- 当 $N \lhd G$,$ab^{-1} \in N \Longleftrightarrow a^{-1}b \in N$.

事实. 任意同态 $f : G \to H$, 则 $\ker f \lhd G$.

命题 5.2.

例 5.3. $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$

$$\mathrm{GL}_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad - bc \neq \bar{0} \right\} = SL_2(\mathbb{F}_2)$$

注记. 为什么考虑 $\mathbb{F}_2$, 因为希望得到有限群.

例 5.4. $\det : GL_n(\mathbb{C}) \to \mathbb{C}^\times$

核 $SL_n(\mathbb{C}) \lhd GL_n(\mathbb{C})$.

定义 5.5. 设 $N \lhd G$, 定义商群 $G/N = \big\{aN \big| a \in G\big\}$, 乘法为 $\bar{a} \cdot \bar{b} = \overline{ab}$.

- 良定性. 即证 $a^{-1}a' \in N$ 且 $b^{-1}b' \in N \Longrightarrow (ab)^{-1}a'b' \in N$.

  $(ab)^{-1}a'b' = b^{-1}a^{-1}a'b' = b^{-1}nb' = b^{-1}b'n' \in N$.
- 其余三条都继承自群 G.

命题 5.6 (群同态基本定理)**.**

事实. 设 $N \lhd G$, 设 $f : G \to H$ 同态满足 $N \subset \ker(f)$. 则: 存在唯一同态 $G/N \to H$ 使得下图交换

$$\begin{matrix} G & & G/N \\ & & \\ H & & \end{matrix}$$

定理 5.7. 设 $N \lhd G$,$H \leqslant G$, 则

(1) $(H \cap N) \lhd H$,$N \lhd NH$;

(2) 且 $\dfrac{H}{N \cap H} \simeq \dfrac{NH}{N}$.

6 Zappa-Szép 积、半直积与直积

6.1 Zappa-Szép 积

6.2 半直积

- 给定两个群 N, H, 给定群同态 $\varphi : H \to \mathrm{Aut}(N)$, 我们能构造半直积 $N \rtimes_\varphi H$
  - 作为集合,$N \rtimes_\varphi H$ 是 $N \times H$.
  - 记 $N' = \{(n, e_H) \mid n \in N\}$, 容易验证 N' 是 $N \rtimes_\varphi H$ 的正规子群
  - 记 $H' = \{(e_N, h) \mid h \in H\}$, 容易验证 H' 是 $N \rtimes_\varphi H$ 的子群
- 给定群 G,$N \triangleleft G, H < G$,$G = NH, H \cap N = \{e\}$. 令 $\varphi : H \to \mathrm{Aut}(N), h \mapsto c_h$, 则 $G \cong N \rtimes_\varphi H$.

6.3 直积

- 群的直积是从两个给定的群构造一个新的群的操作. 记作 $G \times H$.
- $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$.
- 危险言论：Abel 群的情形下, 群的直积也叫直和.
- 设 G 和 H 是群, 令 $P = G \times H$, 考虑 P 的如下两个子集：

  $$G' = \{(g, 1) : g \in G\} \quad H' = \{(1, h) : h \in H\}.$$

  这两个群实际上都是 P 的子群, 前者同构于 G, 后者同构于 H. 如果我们把它们分别视作 G 和 H, 那么我们可以认为直积 P 包含最初的群 G 和 H 作为子群.

  P 的这些子群有如下三条性质：

  –

咳咳

- 给定一列群, 这些群的直和或直积, 都是可以理解的
- 然后, 如果说一个群是两个群的直和或直积, 理解为该群同构于这两个群的直和或直积.
- 这等价于是说, 该群以这两个群为子群, 并且二者都是正规子群, 交集为单位, 能生成整个群.

7 群的直和

8 对称群

X 集合,$S(X)$ 是 X 的对称群.

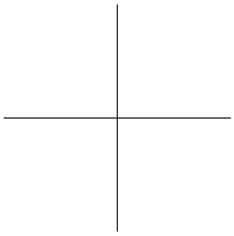
命题 8.1. *若存在双射 $\delta : X \to Y$, 则存在群同构 $\Phi : S(X) \to S(Y)$.*

例 8.2. S_4

- 1^4,Id
- $1^2 2^1$,$\dfrac{n(n-1)}{2} = 6$ 个,$(12),(13),(14),(23),(24),(34)$
- $1^1 3^1$,$\dfrac{n(n-1)(n-2)}{3} = 8$ 个,$(123),(124),(132),(134),(142),(143),(234),(243)$
- 2^2,$(12)(34)$,$(13)(24)$,$(14)(23)$.
- 4^1,$(1234),(1243),(1324),(1342),(1423),(1432)$.

例 8.3. $S_3 \hookrightarrow S_4$ 不是正规子群. 对共轭不封闭.

例 8.4.



引理 8.5. *任意 $\sigma \in S_n$ 均可写成对换之积.*

证明. □

引理 8.6. *S_n 可由 $(12),(23),\cdots,(n-1,n)$ 生成.*

S_n 可自然嵌入到 $\mathrm{GL}_n(\mathbb{R})$ 中. 任取 $\sigma \in S_n$, 则它诱导了置换方阵

$$P_\sigma : \mathbb{R}^n \to \mathbb{R}^n, e_i \mapsto e_{\sigma(i)}$$

容易验证

$$\varphi : S_n \hookrightarrow \mathrm{GL}_n(\mathbb{R}), \sigma \mapsto P_\sigma$$

是群同态. 进而考虑

$$S_n \hookrightarrow \mathrm{GL}_n(\mathbb{R}) \overset{\det}{\twoheadrightarrow} \mathbb{R}^*,$$

即

$$sign : S_n \twoheadrightarrow \{\pm 1\}, (ij) \mapsto -1.$$

综上,$sign(\sigma) = -1 \Longleftrightarrow \sigma$ 可以写成奇数个对换之积；$sign(\sigma) = 1 \Longleftrightarrow \sigma$ 可以写成偶数个对换之积.

此外, 我们还得到了

$$A_n := \ker sign = \{\text{偶置换全体}\} \triangleleft S_n.$$

因为 $S_n / A_n = \{\pm 1\}$, 所以 $|A_n| = \dfrac{n!}{2}$. 称 A 为交错群. 这意味着我们总能得到 S_n 的一个指数为 2 的正规子群. 事实上, 当 $n \geqslant 5$ 时,A_n 是 S_n 的唯一非平凡正规子群!

例 8.7. $A_3 \lhd S_3$.

- S_3 由恒等、对换和三轮换组成, 按定义 A_3 是恒等和三轮换 $\{\mathrm{Id}, (123), (132)\}$.
- 由 *Lagrange* 定理,S_3 的子群只有 2 阶和 3 阶循环群, 对应着 S_3 的三阶元和二阶元, 因此 S_3 的三阶子群只有 A_3.
- 容易验证 S_3 的三个二阶子群都对共轭类不封闭, 在 S_n 中同型的元素互相共轭.
- 可画出 S_3 的子群格.

例 8.8. 求 S_4 所有正规子群.

- *Lagrange* 定理作为成为子群的必要条件.
- 对共轭类封闭作为成为正规子群的必要条件.
- S_4 按共轭类可分为 $24 = 1 + 6 + 8 + 3 + 6$ 共 5 类.
- 由于全体对换生成 S_n, 所以欲找非平凡正规子群, 不可包含对换.
- 已经知道 $A_4 \lhd S_4$, 它是所有偶置换, 即恒等、两个对换和三轮换.
- 由 *Lagrange* 定理,S_4 的非平凡正规子群的阶数只能为 $12, 8, 6, 4, 3, 2$.
-

9 单群

定理 9.1. 当 $n \geqslant 5$ 时,A_n 是单群.

证明.

(1) A_n 由 3− 轮换生成.

A_n 可以写成偶数个对换之积, 只需要证明两个对换之积可以写成若干个三轮换之积.

注意到 $(ijk) = (ik)(ij)$, 则

$$(ij)(rs) = \begin{cases} (isj), & r = i, j \neq s \\ (ij)(jr)(ri)(rs) = (irj)(rsi), & \end{cases}$$

注记. $A_3 = \{Id, (123), (132)\} \triangleleft S_3$, 在 S_3 中 (123) 与 (132) 同型从而共轭, 但它们在 A_3 中不共轭.

(2) 当 $n \geqslant 5$ 时,3− 轮换在 A_n 中也互相共轭.

任取 (ijk) 和 $(i'j'k')$. 对于某个 $\gamma \in S_n$,

$$\gamma(ijk)\gamma^{-1} = (i'j'k')$$

- 若 $\gamma \in A_n$, 结束
- 若 $\gamma \notin A_n$, 取 $r \neq s \notin \{i'j'k'\}$, 则

$$(rs)\gamma \cdot (ijk)\gamma^{-1}(rs)^{-1}$$

注记. 这是因为 n 足够大, 元素足够多, 回旋的余地比较大.

(3) $\{Id\} \neq N \triangleleft A_n$, 存在 3-轮换 $\in N$. 不证了.

□

推论 9.2. 当 $n \geqslant 5$ 时,A_n 时 S_n 的唯一非平凡正规子群.

例 9.3. $|A_4| = 12$.

- Id
- $(12)(34), (13)(24), (14)(23)$

  问是否存在 $\sigma(12)(34)\sigma^{-1} = (13)(24)$
- (123) 和 (132). 枚举可以. $\sigma(132)\sigma^{-1} = (123)$

  注记. 后面将讲到共轭类的大小将整除群的阶.

  – $(123), (142), (134), (243)$
  – $(132), (124), (143), (234)$

因此 $12 = 1 + 3 + 4 + 4$

注记. 无六阶子群, 因为它指数是 2, 因此一定正规, 因此是共轭类的并, 但加不出 6.

10 群作用

定义与例子

定义 10.1. 设 G 是群,X 是集合, 那么 G 在 X 上的一个左作用是指一个映射

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

满足

(1) $1_G \cdot x = x$;

(2) $h \cdot (g \cdot x) = (hg) \cdot x$.

记作 $G \curvearrowright X$, 称 (X, ψ) 为 G-集.

由定义可以推出,$\psi(g, \cdot)$ 是 X 上的一个双射, 其逆映射为 $\psi(g^{-1}, \cdot)$.

因此, 我们可以将群作用等价地定义为从给定的群 G 到 X 的置换群 $S(X)$ 的一个群同态. 这两种观点各有各的好处.

当 X 上还有结构时, 我们将群作用定义为从群 G 到 X 的自同构群 $\mathrm{Aut}(X)$ 的一个群同态.

例 10.2. $S(X) \curvearrowright X$,$(\sigma, x) \mapsto \sigma(x)$.

例 10.3. 设 V 是 n 维 $\mathbb{F}$-线性空间, 则 $\mathrm{Aut}(V) \simeq \mathrm{GL}(n, \mathbb{F}) \curvearrowright V$.

例 10.4. 设 X 是拓扑空间, 则 $\mathrm{Aut}(X) \curvearrowright X$, 其中 $\mathrm{Aut}(X)$ 是 X 的自同胚.

例 10.5. 设 $\mathbb{D}$ 是单位开圆盘, 则 $\mathrm{Aut}(\mathbb{D}) \curvearrowright \mathbb{D}$, 其中 $\mathrm{Aut}(\mathbb{D})$ 是 $\mathbb{D}$ 上的全纯自同构.

轨道与稳定化子

考虑群作用, 就应该考虑它的轨道和稳定化子, 这应该成为本能.

定义 10.6. 设 $G \curvearrowright X$,$x \in X$, 定义 x 的 G-轨道

$$\mathcal{O}_x = \left\{ g \cdot x \middle| g \in G \right\}.$$

可以在 X 上定义一个等价关系,$x \simeq y \iff \exists g \in G \text{ s.t. } y = g \cdot x$. 容易看出 x 所在的等价类就是 x 的 G-轨道.

X 有 G-轨道分解

$$X = \bigsqcup_{x \in I} \mathcal{O}_x,$$

其中 I 是轨道的完全代表元系.

定义 10.7. 称 $G \curvearrowright X$ 为可迁的, 若对任意的 $x, y \in X$, 存在 $g \in G$ 使得 $y = g \cdot x$.

我们总可以假定 $G \curvearrowright X$ 是可迁的, 若不然, 考虑 $\mathcal{O}_x$, 则 $G \curvearrowright \mathcal{O}_x$ 便是可迁的. 这有点拓扑里面总可以假定覆叠空间 $\widetilde{X}$ 和底空间 X 都是道路连通那味, 若不然, 可取道路连通分支.

上面这种观察是将其看成“群作用”而不是“置换表示”的好处.

不同轨道之间确实是毫无联系的, 就好像拓扑中不同道路连通分支的覆叠可以完全不同一样. 给定 $G \curvearrowright X$ 和 $G \curvearrowright Y$, 其中 X 和 Y 毫不相关, 自然地就有 $G \curvearrowright (X \sqcup Y)$.

定义 10.8. 设 $G\curvearrowright X$,$x\in X$, 定义 x 的稳定化子

$$G_x=\{g\in G\big|g\cdot x=x\}.$$

容易验证 $G_x\leqslant G$.

引理 10.9. 若 $x=hy$, 即 x 与 y 在同一轨道中, 则 $G_x=hG_yh^{-1}$.

这有点拓扑中在同一个道路连通分支里面以不同点为基点的基本群互相共轭那味了.

例 10.10. 设 $H\leqslant G$, 考虑左陪集 $G/H=\{aH\big|a\in G\}$.
当 H 不是正规子群时 G/H 上无群结构, 但 G 自然作用到 G/H 上,

$$g\cdot aH\longmapsto (ga)H,$$

称为左诱导作用.

- 可迁.$aH=a\cdot H$.
- $G_H=\{g\in G\big|gH=H\}=H$.
  $G_{aH}=aHa^{-1}$.

若取 $H=\{1_G\}$, 则 G/H 就是 G, 即 $G\curvearrowright G$, 称为左正则作用. 此时稳定化子是平凡的.

例 10.11. $S_n\curvearrowright\underline{n}=\{1,2,\cdots,n\}$.

- 可迁.
- n 的稳定化子: S_{n-1}.
  1 的稳定化子: $(1n)S_{n-1}(1n)^{-1}$.

例 10.12. K/k, 研究 $\mathrm{Aut}(K/k)=\{\sigma\in\mathrm{Aut}(K)\big|\sigma(\lambda)=\lambda,\forall\lambda\in k\}$.
取 $f(x)\in k[x]$, 考虑 $Root_K(f)=\{u\in K\big|f(u)=0_K\}$,
断言 $\mathrm{Aut}(K/k)\curvearrowright Root_K(f)$.

设 $f(x)\in k[x]$,$k\subset E$ 是 $f(x)$ 的分裂域.
$\mathrm{Aut}(E/k)\curvearrowright Root_E(f)=\{u_1,\cdots,u_n\}$
从而 $\mathrm{Aut}(E/k)\hookrightarrow S_n$

例 10.13. $\mathrm{GL}_2(\mathbb{F}_2)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\mid a,b,c,d\in\mathbb{F}_2,ad-bc=\bar{1}\right\}$.

记 $V=\mathbb{F}_2^2$, 则 $|V|=4$.

$|\mathrm{GL}_2(\mathbb{F}_2)|=6$. 因为第一列只有三种选择 $(\bar{1},\bar{0})^T,(\bar{0},\bar{1})^T,(\bar{1},\bar{1})^T$, 即 $V\backslash\{(\bar{0},\bar{0})^T\}$, 第二行为了与第一行不平行只有两种选择.（用同样的方法我们可数出 $|\mathrm{GL}_2(\mathbb{F}_3)|=8\times 6=48$）

$\mathrm{GL}_2(\mathbb{F}_2)\curvearrowright V$. 易知 $(\bar{0},\bar{0})$ 自己是一个轨道, 因此 $\mathrm{GL}_2(\mathbb{F}_2)\curvearrowright V^\times:=V\backslash\{(\bar{0},\bar{0})^T\}$.

所以 $\mathrm{GL}_2(\mathbb{F}_2)\longrightarrow S(V^\times)\simeq S_3$, 易知是单射, 从而 $\mathrm{GL}_2(\mathbb{F}_2)\simeq S_3$.

第十二周暨第十次作业 Ex2.6 要求你把 $\mathrm{GL}_2(\mathbb{F}_2)\curvearrowright V$ 具体写出来.

$\mathrm{GL}_2(\mathbb{F}_2)$ 中的二阶元是

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix},\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

$\mathrm{GL}_2(\mathbb{F}_2)$ 中的三阶元是

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

- 三阶元平方后得到另一个三阶元
- 一个二阶元跟另外两个二阶元作用分别得到两个三阶元
- 交换两个相乘的二阶元的位置得到另一个三阶元

例 10.14. $G \curvearrowright G$ 共轭作用

$g.x = gxg^{-1}$

定理 10.15. $G \curvearrowright X$,$x \in X$, 则有双射

$$G/G_x \to \mathcal{O}_x, aG_x \mapsto ax$$

当 $|G| < \infty$ 时, 轨道-稳定化子公式

$$|G_x| \cdot |\mathcal{O}_x| = |G| \Rightarrow$$

证明.

- 良定.
- 满.
- 单.

□

定义 10.16. 称 $G \curvearrowright X$ 平凡的, 若 $\forall g \in G, x \in X$, 成立 $gx = x$.

- $G_x = G$.
- $\rho : G \to S(X)$ 是平凡同态.

例 10.17. $G \curvearrowright$, 不动点集 $X^G = \left\{x \in X \middle| gx = x, \forall g \in G\right\}$

若它不空,$G \curvearrowright X^G$ 是平凡的.

例 10.18. 共轭作用.

$$G \curvearrowright G = G, g.x = gxg^{-1}$$

- $x \in X$, 轨道, 记为 $C_x = \left\{gxg^{-1} \middle| g \in G\right\}$.
- 共轭类.C_X
- x 的中心化子 $Z(x) = \left\{g \in G \middle| gx = x\right\}$.
- 重要.$|C_X||Z(x)| = |G|$

定义 10.19. 设 p 为素数,G 称为 $p-$ 群, 若 $|G| = p^n$.

例 10.20. 若 $|G| = p$, 则 $G \cong p$ 阶循环群.

命题 10.21. p^2 阶群是 *Abel* 群, 且同构于 $\mathbb{Z}_p$ 或 $\mathbb{Z}_p \times \mathbb{Z}_p$.

证明.

□

11 Sylow 定理

- 对于初学者来说, 知道定义, 知道例子, 会算例子, 其中的技巧性不要追究.

定义 11.1. $|G| = p^r m, p \nmid m$. *子群 $P \leqslant G$ 称为 Sylowp-子群, 若 $|P| = p^r$.*

- $[G : P] = m$.

- 为什么关心 Sylow$p$ 子群

定理 11.2 (Sylow,1872)**.** *设 $|G| = p^r m, p \nmid m$, 则*

(1) *总存在 Sylowp-子群.*

(2) *Sylowp-子群之间相互共轭.*

(3) *个数是 m 的因子, 形如 $kp + 1$.*

(4) *任何 p-子群 $B \leqslant G$, 总存在 Sylowp 子群 $P \leqslant G$ 使得 $B \leqslant P$.*

- p 群可以理解为群的局部.

- 证明可以先忽略不计. 看 S_4 的子群.

- 某种意义上说,Sylow 定理将一般的群归结为 p 群.

12 群的表现

引理 12.1. 约化是唯一的.

定义 12.2. 集合 X 上的自由群

$$F(X)=\left\{\text{所有以}X\cup X^{-1}\text{为字母的既约字}\right\}$$

乘法: 连接 + 约化

定义 12.3. 群 G 的有限表现, 是指

$$G=\left\langle x_1,\cdots,x_n\middle|r_1,r_2,\cdots,r_m\right\rangle,$$

其中 x_i 称为生成元,$r_i\in F(x_1,\cdots,x_n)$ 称为关系.

它的实际数学含义是 $F(x_1,\cdots,x_n)/N(r_1,\cdots,r_m)$, 其中 $N(r_1,\cdots,r_n)$ 是包含 $r_1,\cdots,r_m$ 的最小正规子群.

命题 12.4. 设 $G=\left\langle x_1,\cdots,x_n\middle|r_1,\cdots,r_m\right\rangle$,$H$ 群, 映射 $\theta:\{x_1,\cdots,x_n\}\to H$, 则 θ 可延拓为群同态 $G\xrightarrow{\tilde\theta}H$ 当且仅当 $\theta(x_1),\cdots,\theta(x_n)$ 中满足关系 r_i.

注记.

-

例 12.5. $\mu_n=\left\{z\in\mathbb{C}^*\middle|z^n=1\right\}=\left\{1,\omega,\cdots,\omega^{n-1}\right\},\omega=\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}$

$\nu_n\simeq\left\langle g\middle|g^n=1\right\rangle=F(\{g\})/N(g^n)$.

例 12.6. $S_3\simeq\left\langle a,b\middle|a^2=1=b^2,(ab)^3=1\right\rangle$

13 有限生成 Abel 群

本质上本节内容属于模论, 而不是群论.

定义 13.1. 设 A 为 *Abel* 群,

(1) 称 A 是有限生成的, 若存在有限集 $S=\{s_1,s_2,\cdots s_n\}\subset A$ 生成 A, 即对任意的 $a\in A$, 存在 $\lambda_1,\lambda_2,\cdots,\lambda_n\in\mathbb{Z}$ 使得 $a=\lambda_1 s_1+\lambda_2 s_2+\cdots\lambda_n s_n$. 此时称 S 为 A 的生成集.

(2) 若 S 还是 $\mathbb{Z}$-线性无关的, 则称 S 为 A 的有限基.

命题 13.2. 设 A 为 *Abel* 群, 则 A 有有限基 $S\Longleftrightarrow A\simeq\mathbb{Z}^n$.

命题 13.3. 设 A 为有限生成 *Abel* 群, 则存在 $n\in\mathbb{N}$ 和 $K\leqslant\mathbb{Z}^n$ 使得 $A\simeq\mathbb{Z}^n/K$.

证明. 设 $S=\{s_1,s_2,\cdots,s_n\}$ 为 A 的有限基. 考虑映射

$$\varphi:\mathbb{Z}^n\twoheadrightarrow A,\quad(\lambda_1,\lambda_2,\cdots,\lambda_n)^T\longmapsto\lambda_1 s_1+\lambda_2 s_2+\cdots+\lambda_n s_n,$$

则 $A\simeq\mathbb{Z}^n/\ker\varphi$. □

引理 13.4. 设 G 是群,$N\lhd G$, 若 N 和 G/N 都是有限生成的, 则 G 也是有限生成的.

证明. 设 $U=\{u_1,u_2,\cdots,u_r\}$ 有限生成 N,$\overline{V}=\{\bar v_1,\bar v_2,\cdots,\bar v_s\}$ 有限生成 G/N.

设 $\varphi:G\twoheadrightarrow G/N$ 是自然同态. 任取 $v_i\in G$ 使得 $\varphi(v_i)=\bar v_i$,$1\leqslant i\leqslant s$.

断言 $\{u_1,\cdots,u_r,v_1,\cdots,v_s\}$ 是 G 的生成集.

任取 $g\in G$,$\varphi(g)=\bar v_{i_1}^{\epsilon_1}\cdots\bar v_{i_n}^{\epsilon_n}$, 其中 $\epsilon\in\{1,-1\}$,$1\leqslant i_j\leqslant s$,$1\leqslant j\leqslant n$,$n\in\mathbb{N}$.

所以存在 $n\in N$ 使得 $g=nv_{i_1}^{\epsilon_1}\cdots v_{i_n}^{\epsilon_n}=u_{j_1}^{\delta_1}\cdots u_{j_m}^{\delta_m}v_{i_1}^{\epsilon_1}\cdots v_{i_n}^{\epsilon_n}$. □

命题 13.5. 设 $K\leqslant\mathbb{Z}^n$, 则 K 是有限生成的.

证明.

(1) 当 $n=1$ 时, 设 $K\leqslant\mathbb{Z}$, 则 $K=\{0\}$ 或 $K=d\mathbb{Z}$, 其中 $d\geqslant 1$.

(2) 当 $n=2$ 时, 设 $K\leqslant\mathbb{Z}\oplus\mathbb{Z}$.

取 $e_1=(1,0),e_2(0,1)$, 记 $\mathbb{Z}e_1=\mathbb{Z}\oplus\{0\},\mathbb{Z}e_2=\{0\}\oplus\mathbb{Z}$.

$K\cap\mathbb{Z}e_1\leqslant\mathbb{Z}e_1\simeq\mathbb{Z}^1$, 由 $n=1$ 的情况知 $K\cap\mathbb{Z}e_1$ 是有限生成的.

$\dfrac{K}{K\cap\mathbb{Z}e_1}\simeq\dfrac{K+\mathbb{Z}e_1}{\mathbb{Z}e_1}\leqslant\dfrac{\mathbb{Z}\oplus\mathbb{Z}}{\mathbb{Z}e_1}\simeq\mathbb{Z}^1$, 由 $n=1$ 的情况知 $\dfrac{K}{K\cap\mathbb{Z}e_1}$ 是有限生成的.

由引理知 K 是有限生成的.

□

注记. $\mathbb{Z}\oplus\mathbb{Z}$ 的子群不一定形如 $d_1\mathbb{Z}\oplus d_2\mathbb{Z}$, 比如由 $(1,1)$ 生成的子群.

定义 13.6. 有限生成自由 *Abel* 群范畴.

- 对象是列空间 $\mathbb{Z}^n$,$n\in\mathbb{N}$.
- 态射是矩阵 $\mathbf{A}\in\mathbb{Z}^{n\times m}$.

命题 13.7. 设 $\mathbb{Z}^n \simeq \mathbb{Z}^m$ 群同构, 则 $n = m$.

证明. $AB = I_n, BA = I_m$, 取迹知 $n = m$. □

定义 13.8. 设 $\mathbf{A} \in \mathbb{Z}^{n\times m}, \phi_{\mathbf{A}} : \mathbb{Z}^m \to \mathbb{Z}^n$, 定义 $\phi_{\mathbf{A}}$ 的余核为

$$\operatorname{coker}\phi_{\mathbf{A}} := \mathbb{Z}^n / \operatorname{Im}\phi_{\mathbf{A}}.$$

命题 13.9. 任意有限生成 *Abel* 群 A 均同构于某个 $\operatorname{coker}\phi_{\mathbf{A}}$.

定义 13.10. $\mathrm{GL}_n(\mathbb{Z}) := \left\{A \in \mathbb{Z}^{n\times n} \middle| \exists B \in \mathbb{Z}^{n\times n} \text{ s.t. } AB = BA = I\right\} = \left\{A \in \mathbb{Z}^{n\times n} \middle| \det A = \pm 1\right\}$.

要体会为什么要考虑 $\mathrm{GL}_n(\mathbb{Z})$ 而不考虑 $\mathbb{Z}^{n\times n} \cap \mathrm{GL}_n(\mathbb{Q})$.

命题 13.11. 设 $\mathbf{A} \in \mathbb{Z}^{n\times n}$, 则 $\mathbf{A} \in \mathrm{GL}_n(\mathbb{Z}) \Longleftrightarrow \phi_{\mathbf{A}} : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ 是同构.

证明.

- $\Longrightarrow \phi_{\mathbf{A}} \circ \phi_{\mathbf{A}^{-1}} = \mathrm{Id}, \phi_{\mathbf{A}^{-1}} \circ \phi_{\mathbf{A}} = \mathrm{Id}$.
- $\Longleftarrow$ 由 $\phi_{\mathbf{A}} \circ \phi_{\mathbf{B}} = \mathrm{Id}$ 知 $\mathbf{AB} = \mathbf{I}$.

□

定义 13.12. 设 $\mathbf{A}, \mathbf{B} \in \mathbb{Z}^{n\times m}$, 称 $\mathbf{A}, \mathbf{B}$ 相抵, 如果存在 $\mathbf{P} \in \mathrm{GL}_n(\mathbb{Z})$ 和 $\mathbf{Q} \in \mathrm{GL}_m(Z)$ 使得 $\mathbf{B} = \mathbf{PAQ}$.

命题 13.13. 若 $\mathbf{A}, \mathbf{B}$ 相抵, 则 $\operatorname{coker}\phi_{\mathbf{A}} \simeq \operatorname{coker}\phi_{\mathbf{B}}$.

定理 13.14 (Smith 标准型)**.** 设 $\mathbf{A} \in \mathbb{Z}^{n\times m}$, 则 $\mathbf{A}$ 相抵于

Chapter 4

Galois 理论

1 Galois 扩张

2 三次多项式的分类

我对于三次多项式的分裂域的 Galois 群什么时候是 S_3 什么时候是 A_3 较为感兴趣, 可参见http://www.ms.uk
hum/ma561/notes/workspace/books/cubicquartic.pdf

3

定义 3.1. 偏序集

例 3.2. $SubG$ 是偏序集.

定义 3.3. 设 $(L, \leqslant)$ 是偏序集,$a, b \in L$,

(1) 定义 $(a \vee b) \in L$ 为 a, b 的最小上界, 满足

- $a \leqslant (a \vee b)$,$b \leqslant (a \vee b)$
- 若 $a \leqslant c$,$b \leqslant c$, 则 $(a \vee b) \leqslant c$

(2) 定义 $(a \wedge b) \in L$ 为 a, b 的最小上界, 满足

- $a \leqslant (a \vee b)$,$b \leqslant (a \vee b)$
- 若 $a \leqslant c$,$b \leqslant c$, 则 $(a \vee b) \leqslant c$

(3) 称 $(L, \leqslant)$ 为格, 若任意 $a, b \in L$,$a \vee b$ 及 $a \wedge b$ 都存在.

- 将 $a \vee b$ 读作"a 并 b", 将 $a \wedge b$ 读作"a 交 b", 当 $(L, \leqslant) = (2^X, \subset)$ 时, 确实就是并与交.
- $a \vee b$ 和 $a \wedge b$ 都不一定存在, 但二者存在则唯一.

例 3.4. $Sub(G)$ 是格. 设 $H, K \leqslant G$,

- $H \vee G =$ 由 $H \cup K$ 生成的子群.
- $H \wedge G = H \cap K$.
- 最小上界不平凡!

例 3.5. 设 K/k 为域扩张, 定义

$$Lat(K/k) = \left\{ E \middle| k \subset E \subset K \right\}.$$

- E, F 是中间域,$E \vee F =$ 由 $E \cup F$ 生成的子域.
- $E \wedge F = E \cap F$.

例 3.6. 设 $(L, \leqslant)$ 为格, 定义反格 $(L^{op}, \leqslant^{op})$

- $L^{op} = L$.
- $a \leqslant^{op} b := b \leqslant a$.

定义 3.7. 设 L, L' 为格,$f : L \to L'$ 为双射, 称 f 是一个偏序集同构, 如果 f 和 f^{-1} 都保持序结构.

引理 3.8. 设 L, L' 为格, 设 $f : L \to L'$ 为偏序集同构, 则 f 保持 $\vee$ 和 $\wedge$.

例 3.9. 设 $n \leqslant 1$, 定义

- $L_n = \left\{ d \middle| 1 \leqslant n, d \mid n \right\}$

- $d \preccurlyeq d' := d \mid d'$.

断言 $(L_n, \preccurlyeq)$ 是格.

- $d_1 \vee d_2 = \mathrm{lcm}(d_1, d_2)$
- $d_1 \wedge d_2 = \gcd(d_1, d_2)$

例 3.10. 取 $C_n = \langle g \big| g^n = 1 \rangle = \{1, g, \cdots, g^{n-1}\}$, 则存在格同构

$$Sub(C_n) \xrightarrow{\sim} L_n$$
$$\langle g^{\frac{n}{d}} \rangle \longmapsto d$$

定理 3.11 (Galois 理论的基本定理)**.** 设 K/k 是有限维 Gal 扩张,$G = Gal(k/k)$, 则存在格同构

$$Sub(G) \xrightarrow{\sim} Lat(K/k)^{op}$$
$$H \longmapsto K^H$$

推论 3.12. 设 $H, U \leqslant G$, 则

$$K^{H \vee U} = K^H \cap K^U, K^{H \cap U} = K^{H \cap U} K^H \vee K^U$$

第一条平凡, 第二条不平凡

推论 3.13. $k \subset B, E \subset K$

$$Gal(K/B \vee E) = Gal(K/B) \cap Gal(K/E)$$

$$Gal(K/B \cap E) = Gal(K/B) \vee Gal(K/E)$$

前者平凡, 后者不平凡

推论 3.14. 设 $H \leqslant G$, 则 $\dim K^H = [G : H]$.

这个公式计算起来很有用.

观察,

- $G \curvearrowright Sub(G), \sigma \cdot H = \sigma H \sigma^{-1}$.
- $H \in Sub(G)^G \iff H \triangleleft G$.
- $G \curvearrowright Lat(K/k), \sigma \cdot E = \sigma(E)$
- 断言 Galois 对应保持 $G-$ 作用.

推论 3.15. 设 K/k 有限 *Galois*,$k \subset E \subset K$, 则

$$E/kGalois \iff Gal(K/E) \triangleleft G$$

此时 $G/Gal(K/E) \simeq Gal(E/k)$.

证明. □

Chapter 5

作业

1 第一周

1.

2. 证明：

(1) $\mathrm{Map}(X\bigsqcup Y,Z)\xrightarrow{\sim}\mathrm{Map}(X,Z)\times\mathrm{Map}(Y,Z)$

(2) $\mathrm{Map}(Z,X\times Y)\xrightarrow{\sim}\mathrm{Map}(Z,X)\times\mathrm{Map}(Z,Y)$

(3) $\mathrm{Map}(X\times Y,Z)\xrightarrow{\sim}\mathrm{Map}(X,\mathrm{Map}(Y,Z))$

证明. (1)

$$F:\mathrm{Map}(X\bigsqcup Y,Z)\to\mathrm{Map}(X,Z)\times\mathrm{Map}(Y,Z)$$
$$f\mapsto(f\big|_X,f\big|_Y)$$

- F 是满射. 对任意 $g\in\mathrm{Map}(X,Z),h\in\mathrm{Map}(Y,Z)$, 定义
$$f(a)=\begin{cases}g(a),a\in X\\ h(a),a\in Y\end{cases}$$
则 $F(f)=(g,h)$.
- F 是单射. 设 $(f_1\big|_X,f_1\big|_Y)=(f_2\big|_X,f_2\big|_Y)$, 则 $f_1\big|_X=f_2\big|_X,f_1\big|_Y=f_2\big|_Y$, 则 $f_1=f_2$.

(2)

$$F:\mathrm{Map}(Z,X\times Y)\to\mathrm{Map}(Z,X)\times\mathrm{Map}(Z,Y)$$
$$f\mapsto(g,h)$$

其中若 $f(z)=(x,y)$, 则定义 $g(z)=x,h(z)=y$.

- F 是满射. 对于任意的 $g\in\mathrm{Map}(Z,X),h\in\mathrm{Map}(Z,Y)$, 定义 $f:Z\to X\times Y$ 为 $f(z)=(g(z),h(z))$, 按定义显然 $F(f)=(g,h)$.
- F 是单射. 若 $(g_1,h_1)=(g_2,h_2)$, 则 $g_1=g_2,h_1=h_2$, 则 $f_1=f_2$.

(3)

$$F:\mathrm{Map}(X\times Y,Z)\to\mathrm{Map}(X,\mathrm{Map}(Y,Z))$$
$$f\mapsto g$$

其中若 $f(x,y)=z$, 则定义

$$g(x)=h:Y\to Z$$
$$y\mapsto z$$

- F 是满射. 对于任意的 $g\in\mathrm{Map}(X,\mathrm{Map}(Y,Z))$, 定义 $f(x,y)=g(x)(y)$, 则按定义有 $F(f)=g$.

- F 是单射. 若 $g_1 = g_2$, 则 $g_1(x) = g_2(x)$, 则 $g_1(x)(y) = g_2(x)(y)$, 则 $f_1(x, y) = f_2(x, y)$.

$\square$

3. 证明：$\mathbb{Z}_n$ 上的 $+$ 和 $\cdot$

$$[i] + [j] = [i + j]$$

$$[i] \cdot [j] = [ij]$$

是良好定义的, 进一步地,$(\mathbb{Z}_n, +, \cdot)$ 是环.

证明. 设 $i - i' \equiv 0 \mod n, j - j' \equiv 0 \mod n$, 则

$$i + j - (i' + j') = (i - i') + (j - j') \equiv 0 \mod n$$

$$ij - i'j' = ij - i'j + i'j - i'j' = j(i - i') + i'(j - j') \equiv 0 \mod n$$

因此 $+$ 和 $\cdot$ 是良定的.

$\mathbb{Z}_n$ 上加法的结合律、交换律, 乘法的结合律, 加法与乘法的左右分配律都继承自 $\mathbb{Z}$, 只验证存在零元、逆元和幺元.

$$[0] + [a] = [0 + a] = [a]$$

$$[-a] + [a] = [-a + a] = [0]$$

$$[1] \cdot [a] = [1a] = [a]$$

因此 $(\mathbb{Z}_n, +, \cdot)$ 是含幺环. $\square$

4. 证明：对任意 $m, n \in \mathbb{Z}$,$a \in R$, 成立

$$ma + na = (m + n)a.$$

证明.

- 当 m, n 中至少一个为 0 时. 不妨设 $m = 0$, 则

$$\text{LHS} = 0_R + na = na = \text{RHS}$$

- 当 m, n 同号时. 不妨设 $m, n > 0$, 则

$$\text{LHS} = \underbrace{a + \cdots + a}_{m\text{个}} + \underbrace{a + \cdots + a}_{n\text{个}} = \underbrace{a + \cdots + a}_{(m+n)\text{个}} = \text{RHS}$$

- 当 m, n 异号时.
  - 当 $|m| = |n|$ 时. 不妨设 $m = -n > 0$, 则

$$\text{LHS} = \underbrace{a + \cdots + a}_{m\text{个}} + \underbrace{(-a) + \cdots + (-a)}_{(-n)\text{个}} = 0_R = \text{RHS}$$

  - 当 $|m| \neq |n|$ 时. 不妨设 $m > -n > 0$, 则

$$\text{LHS} = \underbrace{a + \cdots + a}_{m\text{个}} + \underbrace{(-a) + \cdots + (-a)}_{(-n)\text{个}} = \underbrace{a + \cdots + a}_{(m+n)\text{个}} = \text{RHS}$$

□

5. 证明：对任意 $n \in \mathbb{Z}$,$a \in R$, 成立

$$na = (n1_R) \cdot a.$$

证明.

- 当 $n = 0$ 时.

$$\text{LHS} = 0_R, \text{RHS} = 0_R \cdot a = 0_R.$$

- 当 $n \neq 0$ 时. 不妨设 $n > 0$, 则

$$\text{RHS} = (\underbrace{1_R + \cdots + 1_R}_{n\text{个}}) \cdot a = \underbrace{1_R \cdot a + \cdots + 1_R \cdot a}_{n\text{个}} = \underbrace{a + \cdots + a}_{n\text{个}} = \text{LHS}$$

□

2 第二周

Ex1.1 给定 R,$a,b\in R$, 证明:

$$(a+b)^n=a^n+\cdots+b^n.$$

证明. 当 $n=1$ 时, 显然成立.

假设当 $n=k$ 时成立, 证 $n=k+1$ 时成立.

$$\begin{aligned}(a+b)^{k+1}&=(a+b)^k(a+b)\\&=(C_k^0a^k+C_k^1a^{k-1}b^1+\cdots+C_k^ra^{k-r}b^r+\cdots+C_k^kb^k)(a+b)\\&=C_k^0a^{k+1}+(C_k^1+C_k^0)a^kb+\cdots+(C_k^{r+1}+C_k^r)a^{k-r}b^{r+1}+\cdots+(C_k^k+C_k^{k-1})ab^k+C_k^kb^{k+1}\\&=C_{k+1}^0a^{k+1}+C_{k+1}^1a^kb+\cdots+C_{k+1}^{r+1}a^{k-r}b^{r+1}+\cdots+C_{k+1}^kab^k+C_{k+1}^{k+1}b^{k+1}\end{aligned}$$

得证. □

Ex1.2 证明：有限环 R 是整环当且仅当 R 是域.

证明. 只证充分性.

设非零元 a 不可逆, 那么对任意的元素 $b\in R$,$ab\neq 1_R$.

定义 R 上的一个变换 $\sigma:R\to R,b\mapsto ab$. 由上可知 σ 不是满射.

由于 R 是有限环, 则 σ 也不是单射. 因此存在 $b_1\neq b_2$ 使得 $ab_1=ab_2$.

也就是存在 $b_1-b_2\neq 0$ 使得 $a(b_1-b_2)\neq 0$, 这与 R 是整环矛盾！ □

Ex1.3 证明：$\mathbb{Q}[\sqrt{-1}]$ 的子域只有 $\mathbb{Q}$ 和它本身.

证明. 容易验证 $\mathbb{Q}$ 和它本身都是 $\mathbb{Q}[\sqrt{-1}]$ 的子域.

设 $\mathbb{F}$ 是 $\mathbb{Q}[\sqrt{-1}]$ 的除了 $\mathbb{Q}$ 之外的真子域, 那么存在 $a+b\sqrt{-1}\in\mathbb{F}$ 且 $b\neq 0$.

则 $a+b\sqrt{-1}-a=b\sqrt{-1}\in\mathbb{F}$, 则 $b^{-1}b\sqrt{-1}=\sqrt{-1}\in\mathbb{F}$, 则 $\mathbb{Q}[\sqrt{-1}]\subset\mathbb{F}$, 矛盾.

因此 $\mathbb{Q}[\sqrt{-1}]$ 的子域只有 $\mathbb{Q}$ 和它本身 □

Ex1.4 分类 $\mathbb{Z}[\sqrt{-1}]$ 的子环.

解. 容易验证对任意的 $n=0,1,2\cdots$,

$$S_n=\left\{a+bn\sqrt{-1}\middle|a,b\in\mathbb{Z}\right\}$$

都是 $\mathbb{Z}[\sqrt{-1}]$ 的子环.

当 $n=0$ 时 S_n 就是 $\mathbb{Z}$. 接下来要说明任意的非 $\mathbb{Z}$ 子环 R 一定可以写成 S_n 的形式.

由假设存在 $a+b\sqrt{-1}\in R$, 其中 $b\neq 0$. 取出 R 中所有形如 $b\sqrt{-1}$ 的元素前方的系数 b, 断言其中绝对值最小的且大于零的 b_{min} 一定能够整除其他所有的 b, 否则总能用带余除法构造出更小的 b. 则 $R=S_{b_{min}}$.

最后要说明当 $n\neq m$ 时,S_n 与 S_m 不同构.

假设 φ 是从 S_n 到 S_m 的同构映射. 则易知 φ 限制在 $\mathbb{Z}$ 上是恒同映射, 则

$$\varphi(n\sqrt{-1})\varphi(n\sqrt{-1})=\varphi(-n^2)=-n^2.$$

假设 $\varphi(n\sqrt{-1}) = a + bm\sqrt{-1}$, 则有

$$a^2 - b^2m^2 + 2abm\sqrt{-1} = -n^2.$$

若 $bm = 0$, 则 $\varphi(n\sqrt{-1}) = a$, 显然 φ 不是满射.

若 $a = 0$, 则 $b^2m^2 = n^2$, 因为 $m \neq n$, 则 $b^2 > 1$, 则 $\varphi(n\sqrt{-1}) = bm$, 此时 φ 依然不是满射.

所以当 $n \neq m$ 时,S_n 与 S_m 不同构. □

Ex1.5 证明：不存在环同态 $\varphi : \mathbb{Z}_8 \to \mathbb{Q}$.

证明. 假设存在环同态 $\varphi : \mathbb{Z}_8 \to \mathbb{Q}$, 则 $\varphi([0]) = 0, \varphi([1]) = 1$, 但

$$0 = \varphi([8]) = 8\varphi([1]) = 8$$

矛盾！因此不存在环同态 $\varphi : \mathbb{Z}_8 \to \mathbb{Q}$. □

P64.4

(1) 确定环 $\mathbb{Z}[\sqrt{-1}]$ 的单位群, 并证明此环为整环但不是域.

(2) 对于环 $\mathbb{Z}[\sqrt{-3}] = \left\{a + b\sqrt{-3} \middle| a, b \in \mathbb{Z}\right\}$ 作同样事情.

证明.

(1) 设 $a \neq 0$ 且 $b \neq 0$, 易知 $a + b\sqrt{-1}$ 在 $\mathbb{C}$ 中的逆为

$$\frac{1}{a + b\sqrt{-1}} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\sqrt{-1}$$

若 $a + b\sqrt{-1}$ 在 $\mathbb{Z}[\sqrt{-1}]$ 中也可逆, 其逆也只能为 $\dfrac{1}{a + b\sqrt{-1}} = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2}\sqrt{-1}$, 所以我们只需看 $\dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2}\sqrt{-1}$ 什么时候在 $\mathbb{Z}[\sqrt{-1}]$ 里.

当 $|a| > 1$ 或 $|b| > 1$,$\dfrac{a}{a^2 + b^2}$ 和 $\dfrac{b}{a^2 + b^2}$ 中必有一个绝对值小于 1, 又知 $a, b \neq 0$, 则不成立.

当 $|a| = |b| = 1$ 时, 同样的论证可知不成立.

在剩下的情形中, 容易验证 $\pm 1, \pm\sqrt{-1}$ 都可逆.

因此 $U(\mathbb{Z}[\sqrt{-1}]) = \left\{\pm 1, \pm\sqrt{-1}\right\} \neq \mathbb{Z}[\sqrt{-1}]^\times$, 因此此环不是域.

由于 $\mathbb{C}$ 中非零元相乘不为零, 于是在 $\mathbb{Z}[-1]$ 中非零元相乘也不为零.

(2) 同 (1) 相同论证可知, 只有 ± 1 可逆.

□

P64.8. 求证 $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \middle| a, b \in \mathbb{Q}\right\}$ 是实数域 $\mathbb{R}$ 的子域.

证明.

- $1 \in \mathbb{Q}[\sqrt{2}]$
- $(a_1 + b_1\sqrt{2}) \pm (a_2 + b_2\sqrt{2}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

- $(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=a_1a_2+2b_1b_2+(a_1b_2+a_2b_1)\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$
- $\dfrac{1}{a+b\sqrt{2}}=\dfrac{a}{a^2-2b^2}-\dfrac{b}{a^2-2b^2}\sqrt{2}\in\mathbb{Q}[\sqrt{2}]$

□

P64.9.

(1) 确定 $\mathbb{Z}_m$ 的全部子环（其中 m 为正整数）；

(2) 确定 $\mathbb{Q}$ 和 $\mathbb{Q}[\sqrt{2}]$ 的全部子域；

(3) 确定 $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}])$,$\mathrm{Aut}(\mathbb{Z}_m)$.

证明.

(1) 由于我们要求子环含幺, 于是我们高兴地发现 $\mathbb{Z}_m$ 的子环只有它本身.

(2) 容易证明任何数域都包含有理数域, 有理数域是最小的数域, 有理数域的子域只有它本身.
设 $\mathbb{F}$ 是 $\mathbb{Q}[\sqrt{2}]$ 的除了 $\mathbb{Q}$ 之外的真子域, 即 $\mathbb{Q}\subsetneqq\mathbb{F}\subsetneqq\mathbb{Q}[\sqrt{2}]$, 那么存在 $a+b\sqrt{2}\in\mathbb{F}$ 且 $b\neq 0$.
则 $a+b\sqrt{2}-a=b\sqrt{2}\in\mathbb{F}$, 则 $b^{-1}b\sqrt{2}=\sqrt{2}\in\mathbb{F}$, 则 $\mathbb{Q}[\sqrt{2}]\subset\mathbb{F}$. 矛盾.
因此 $\mathbb{Q}[\sqrt{2}]$ 的子域只有 $\mathbb{Q}$ 和它本身.

(3) 设 $\varphi\in\mathrm{Aut}(\mathbb{Q}[\sqrt{2}])$, 易知 φ 限制在 $\mathbb{Q}$ 上为恒同映射.
对于任意的 $a+b\sqrt{2}$,$\varphi(a+b\sqrt{2})=a+b\varphi(\sqrt{2})$, 因此我们只需要确定 $\varphi(\sqrt{2})$ 的值.
设 $\varphi(\sqrt{2})=x+y\sqrt{2}$, 我们要求对任意的 $c+d\sqrt{2}$ 存在 $a+b\sqrt{2}$ 使得 $a+b(x+y\sqrt{2})=c+d\sqrt{2}$, 即 $a+bx+by\sqrt{2}=c+d\sqrt{2}$. 易见只要 $y\neq 0$ 便可以满足要求. 因此

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2}])=\left\{\varphi(a+b\sqrt{2})=a+b\varphi(\sqrt{2})\middle|\varphi(\sqrt{2})=x+y\sqrt{2},y\neq 0\right\}.$$

注记. *$\varphi(\sqrt{2})^2=2$, 所以没多少, 为啥我写了那么多种???*

$\mathrm{Aut}(\mathbb{Z}_m)$ 中只有恒同映射.

□

Ex2.1 设 R 为环, 定义双射

$$\theta: X\to R$$

定义

$$x\oplus x'=\theta^{-1}(\theta(x)+\theta(x')),\forall x,x'\in X$$

$$x\cdot x'=\theta^{-1}\left(\theta(x)\theta(x')\right),\forall x,x'\in X$$

证 $(X,\oplus,\cdot)$ 为环且 θ 是环同构.

证明.

(1)
- 加法结合律

$$\begin{aligned}(x_1 \oplus x_2) \oplus x_3 &= \theta^{-1}\left(\theta(x_1)+\theta(x_2)\right) \oplus x_3 \\ &= \theta^{-1}\left(\theta \circ \theta^{-1}(\theta(x_1)+\theta(x_2))+\theta(x_3)\right) \\ &= \theta^{-1}\left((\theta(x_1)+\theta(x_2))+\theta(x_3)\right) \\ &= \theta^{-1}\left(\theta(x_1)+\theta(x_2)+\theta(x_3)\right) \\ &= x_1 \oplus (x_2 \oplus x_3)\end{aligned}$$

- 加法交换律

$$x \oplus x' = \theta^{-1}(\theta(x)+\theta(x')) = \theta^{-1}(\theta(x')+\theta(x)) = x' \oplus x$$

- 存在零元. 设 $\theta(x_0)=0_R$, 则

$$x_0 \oplus x = \theta^{-1}(\theta(x_0)+\theta(x)) = \theta^{-1}(0_R+\theta(x)) = \theta^{-1}(\theta(x)) = x$$

- 存在逆元. 对任意 $x \in X$, 设 $x' = \theta^{-1}(-\theta(x))$, 则

$$x \oplus x' = \theta^{-1}(\theta(x)+\theta(x')) = \theta^{-1}(\theta(x)-\theta(x)) = \theta^{-1}(0_R) = x_0$$

- 乘法结合律.

$$\begin{aligned}(x_1 \cdot x_2) \cdot x_3 &= \theta^{-1}\left(\theta(x_1)\theta(x_2)\right) \cdot x_3 \\ &= \theta^{-1}\left(\theta \circ \theta^{-1}(\theta(x_1)\theta(x_2))\theta(x_3)\right) \\ &= \theta^{-1}\left((\theta(x_1)\theta(x_2))\theta(x_3)\right) \\ &= \theta^{-1}\left(\theta(x_1)\theta(x_2)\theta(x_3)\right) \\ &= x_1 \cdot (x_2 \cdot x_3)\end{aligned}$$

- 存在幺元. 设 $\theta(x_1)=1_R$, 则

$$x_1 \cdot x = \theta^{-1}(\theta(x_1)\theta(x)) = \theta^{-1}(1_R\theta(x)) = \theta^{-1}(\theta(x)) = x$$

- 左分配律.

$$\begin{aligned}x_1 \cdot (x_2 \oplus x_3) &= \theta^{-1}(\theta(x_1)\theta(x_2 \oplus x_3)) \\ &= \theta^{-1}(\theta(x_1)\theta(\theta^{-1}(\theta(x_2)+\theta(x_3)))) \\ &= \theta^{-1}(\theta(x_1)(\theta(x_2)+\theta(x_3))) \\ &= \theta^{-1}(\theta(x_1)\theta(x_2)+\theta(x_1)\theta(x_3)) \\ x_1 \cdot x_2 \oplus x_1 \cdot x_3 &= \theta^{-1}(\theta(x_1)\theta(x_2)) \oplus \theta^{-1}(\theta(x_1)\theta(x_3)) \\ &= \theta^{-1}(\theta\left(\theta^{-1}(\theta(x_1)\theta(x_2))\right)+\theta\left(\theta^{-1}(\theta(x_1)\theta(x_3))\right)) \\ &= \theta^{-1}(\theta(x_1)\theta(x_2)+\theta(x_1)\theta(x_3))\end{aligned}$$

  因此

$$x_1 \cdot (x_2 \oplus x_3) = x_1 \cdot x_2 \oplus x_1 \cdot x_3.$$

- 右分配律. 验证同左分配律.

(2)

$$\theta(x \oplus x') = \theta(\theta^{-1}(\theta(x) + \theta(x'))) = \theta(x) + \theta(x')$$
$$\theta(x \cdot x') = \theta(\theta^{-1}(\theta(x)\theta(x'))) = \theta(x)\theta(x')$$

□

Ex2.2 设有环同态 $\mathbb{F}_p \xrightarrow{\psi} R$, 证明

(1) ψ 是单射

(2) 对任意 $\lambda \in \mathbb{F}_p$,$a \in R$, 定义 $\lambda a := \psi(\lambda)a$, 证明：$R$ 成为 $\mathbb{F}_p$-线性空间.

(3) $|R| = p^n$, 其中 n 是某个正整数.

证明.

(1) 即证 $\ker\psi = \{[0]\}$. 假设存在非零元 $[a]$ 使得 $\psi([a]) = 0_R$, 由初等数论的知识可知存在正整数 n 使得 $a^n \equiv 1 \mod p$, 则

$$0_R = \psi([a])^n = \psi([a]^n) = \psi([1]) = 1_R$$

矛盾.

注记. 域的理想只有 $\{0\}$ 和自己. 而 Ker 一定是理想. 如果是自己, 那映射是零映射.

(2) 线性空间中的加法就是环中的加法, 性质自动满足, 只验证其余四条.

- 数乘对向量加法的分配律. 任取 $\lambda \in \mathbb{F}_p$,$a, b \in R$,

$$\lambda(a + b) = \psi(\lambda)(a + b) = \psi(\lambda)a + \psi(\lambda)b = \lambda a + \lambda b$$

- 数乘对标量加法的分配律. 任取 $\lambda_1, \lambda_2 \in \mathbb{F}_p$,$a \in R$,

$$(\lambda_1 + \lambda_2)a = \psi(\lambda_1 + \lambda_2)a = (\psi(\lambda_1) + \psi(\lambda_2))a = \psi(\lambda_1)a + \psi(\lambda_2)a = \lambda_1 a + \lambda_2 a$$

- 任取 $\lambda_1, \lambda_2 \in \mathbb{F}_p$,$a \in R$,

$$\lambda_1(\lambda_2 a) = \lambda(\psi(\lambda_2)a) = \psi(\lambda_1)(\psi(\lambda_2)a) = (\psi(\lambda_1)\psi(\lambda_2))a = \psi(\lambda_1\lambda_2)a = (\lambda_1\lambda_2)a$$

- 任取 $a \in R$

$$[1]a = \psi([1])a = 1_R a = a$$

(3) 因为 R 是有限环, 则 R 不可能是无限维线性空间. 则 R 必是有限维线性空间, 设 $\dim R = n$, 则 $R \cong (\mathbb{F}_p)^n$, 则 $|R| = p^n$.

□

Ex2.3（对应定理）给定 $I \triangleleft R$, 则存在双射 $\{J \triangleleft R | J \supset I\} \leftrightarrow \{L \triangleleft R/I\}$

$$\{J \triangleleft R | J \supset I\} \leftrightarrow \{R/I\text{的理想}\}$$
$$J \mapsto J/I = \{\bar{a} | a \in J\}$$
$$\{x \in R | \bar{x} \in L\} \leftarrow\!\shortmid L \triangleleft (R/I)$$

证明.

注记. 补证良好定义.

-

给定 J,$J/I=\{\bar{a}\big|a\in J\}$. 设 $L=J/I$, 显然 $J\subset\{x\in R\big|\bar{x}\in L\}$, 只需证 $\{x\in R\big|\bar{x}\in L\}\subset J$.

设存在 $b\in R\backslash J\in\{x\in R\big|\bar{x}\in L\}$, 则 $\bar{b}\in L=\{\bar{a}\big|a\in J\}$, 则 $b-a\in I$, 即存在 $c\in I$ 使得 $b=a+c$, 但 $I\subset J$, 所以 $c\in J$, 由于 J 是理想对加法封闭, 所以 $b\in J$. 命题得证. □

Ex2.4 分类 $\mathbb{Z}_n$ 的理想.

证明.

注记. 用上一题!

设 $[r]\in I$,$r\neq 0$. 若 $(r,n)=1$, 则由 Bezout 等式知存在 a,b 使得 $ar+bn=1$, 则 $\mathbb{Z}_n\subset I$.

设 $(r,n)=t$ 是 n 的因子, 则由 Bezout 等式知 $[t]\in I$. 断言

$$I=\left\{[0],[t],2[t],\cdots,\left(\frac{n}{t}-1\right)[t]\right\}$$

是 $\mathbb{Z}_n$ 的理想. 显然 I 对加法封闭. 对任意 $[a]\in\mathbb{Z}_n$,$[a]\cdot i[t]=[ait]\in I$. 所以 I 是 $\mathbb{Z}_n$ 的理想.

对任意 I 是 $\mathbb{Z}_n$ 的理想, 找到其中非零的最小元 t,I 便可以写为上面这种形式. □

Ex2.5 证明:

(1) $+,\cdot$ 定义合理

(2) $(\mathrm{Frac}(R),+,\cdot)$ 是含幺交换环

(3) $(\mathrm{Frac}(R),+,\cdot)$ 是域

证明.

(1)
$$\frac{ay+bx}{xy}=\frac{a'y'+b'x'}{x'y'}\Leftrightarrow ayx'y'+bxx'y'=a'y'xy+b'x'xy$$
$$\frac{ab}{xy}=\frac{a'b'}{x'y'}\Leftrightarrow abx'y'=a'b'xy$$

当 $ax'=xa'$,$by'=yb'$ 时, 上两式显然成立, 因此是良定的!

(2)
- 加法结合律.
$$\left(\frac{a}{x}+\frac{b}{y}\right)+\frac{c}{z}=\frac{ay+bx}{xy}+\frac{c}{z}=\frac{ayz+bxz+cxy}{xyz},$$
$$\frac{a}{x}+\left(\frac{b}{y}+\frac{c}{z}\right)=\frac{a}{x}+\frac{bz+cy}{yz}=\frac{ayz+xbz+xcy}{xyz}.$$
- 加法交换律. 显然.
- 存在零元
$$\frac{0_R}{1_R}+\frac{a}{x}=\frac{0_Rx+1_Ra}{1_Rx}=\frac{a}{x}.$$

- 存在逆元
$$\frac{a}{x}+\frac{-a}{x}=\frac{ax-ax}{x^2}=\frac{a-a}{x}=\frac{0_R}{x}=\frac{0_R}{1_R}.$$
- 乘法结合律. 显然.
- 乘法交换律. 显然.
- 存在幺元.
$$\frac{1_R}{1_R}\cdot\frac{a}{x}=\frac{1_Ra}{1_Rx}=\frac{a}{x}$$
- 分配律
$$\frac{a}{x}\cdot\left(\frac{b}{y}+\frac{c}{z}\right)=\frac{a}{x}\cdot\frac{bz+cy}{yz}=\frac{abz+acy}{xyz}$$
$$\frac{a}{x}\cdot\frac{b}{y}+\frac{a}{x}\cdot\frac{c}{z}=\frac{ab}{xy}+\frac{ac}{xz}=\frac{abxz+xyac}{xyxz}=\frac{abz+yac}{xyz}$$

(3) 设 $\frac{a}{x}\neq\frac{0_R}{1_R}$, 即 $a\neq 0_R$, 容易验证 $\frac{a}{x}\cdot\frac{x}{a}=\frac{ax}{ax}=\frac{1_R}{1_R}$.

□

3 第三周

Ex1.1 设 $R = \mathbb{Z}[\sqrt{-3}]$, 证明 2 是不可约元但不是素元.

证明. 设 $2 = (a+b\sqrt{-3})(c+d\sqrt{-3})$, 则 $2 = \bar{2} = (a-b\sqrt{-3})(c-d\sqrt{-3})$, 则 $4 = (a^2+3b^2)(c^2+3d^2)$. 容易讨论出只可能是 $a = 1, c = 2, b = d = 0$ 的组合. 因此 2 是不可约元.

但 $2 \mid 4 = (1+\sqrt{-3})(1-\sqrt{-3})$. 设 $(1+\sqrt{-3}) = 2(a+b\sqrt{-3})$, 则 $2a = 1, 2b = 1$, 无解. 因此 $2 \nmid (1+\sqrt{-3})$, 同理可证 $2 \nmid (1-\sqrt{-3})$, 因此 2 不是素元. □

P70.2 设 I 是（含幺）交换环 R 中的理想. 求证：集合

$$\sqrt{I} = \left\{ r \in R \middle| \exists n \geqslant 1,\ \text{s.t. } r^n \in I \right\}$$

也是环 R 的理想.

证明.

- 任取 $a, b \in I$, 存在 m, n 使得 $a^m, b^n \in I$, 则 $(a+b)^{m+n} \in I$, 这是因为展开式中的每一项要么 a 的指标大于等于 m, 要么 b 的指标大于等于 n, 由 I 对倍乘封闭得到该单项属于 I, 由 I 对加法封闭得到 $(a+b)^{m+n} \in I$, 因此 $a+b \in \sqrt{I}$.
- 任取 $a \in I$, 存在 m 使得 $a^m \in I$. 任取 $r \in R$,$(ar)^m = a^m r^m \in I$. 因此 $ar \in \sqrt{I}$.

□

P71.5 设 I_1 和 I_2 均是环 R 的理想. 求证：

(1) $I_1 I_2$ 也是环 R 的理想, 并且 $I_1 I_2 \subseteq I_1 \cap I_2$. 问是否一定有 $I_1 I_2 = I_1 \cap I_2$?

(2) $I_1 + I_2$ 也是环 R 的理想, 并且它恰好是包含 I_1 和 I_2 的最小理想；

(3) 设 $I_1 = n\mathbb{Z}, I_2 = m\mathbb{Z}(n, m \geqslant 1)$ 是整数环 $\mathbb{Z}$ 的两个理想. 则 $I_1 I_2 = nm\mathbb{Z}, I_1 + I_2 = (n, m)\mathbb{Z}, I_1 \cap I_2 = [n, m]\mathbb{Z}$.

证明.

(1)
$$I_1 I_2 = \left\{ \sum_{j=1}^{n} i_{1j} i_{2j} \middle| i_{1j} \in I_1, i_{2j} \in I_2, n \geqslant 1 \right\}$$

按定义 $I_1 I_2$ 对加法封闭. 任取 $i_1 \in I_1, i_2 \in I_2$, 则 $i_1 i_2 \in I_1 I_2$. 任取 $r \in R$,$i_2 r \in I_2$,$i_1 i_2 r \in I_1 I_2$. 由于 $I_1 I_2$ 对加法封闭, 所以 $\left(\sum_{j=1}^{n} i_{1j} i_{2j} \right) r \in I_1 I_2$.

设 $i_1 \in I_1, i_2 \in I_2$, 则 $i_1 i_2 \in I_1, i_1 i_2 \in I_2$, 则 $i_1 i_2 \in I_1 \cap I_2$, 则 $I_1 I_2 \subset I_1 \cap I_2$.

不一定有, 反例在第 (3) 小问.

(2)

$$I_1+I_2=\{i_1+i_2 \big| i_1\in I_1, i_2\in I_2\}$$

任取 $i_{11}+i_{21}, i_{12}+i_{22}\in I_1+I_2$, 则 $(i_{11}+i_{21})+(i_{12}+i_{22})=(i_{11}+i_{12})+(i_{21}+i_{22})\in I_1+I_2$.

任取 $i_1+i_2\in I_1+I_2$, 任取 $r\in R$, 则 $(i_1+i_2)r=i_1r+i_2r\in I_1+I_2$.

因此 I_1+I_2 也是环 R 的理想（我真的很想只敲一句容易验证 I_1+I_2 是环 R 的理想）.

若某理想 I 包含 I_1 和 I_2, 按定义 I 对加法封闭, 则 $I_1+I_2\subset I$, 因此 I_1+I_2 是包含 I_1 和 I_2 的最小理想.

(3) 我们已经证明过了 $\mathbb{Z}$ 的理想都是主理想, 生成元是最小的非负元素, 能够整除其他所有元素.

设 $i_1i_2\in I_1I_2$, 因 $n\mid i_1, m\mid i_2$, 则 $nm\mid i_1i_2$.

设 $i_1+i_2\in I_1+I_2$, 则 $(n,m)\mid n\mid i_1, (n,m)\mid m\mid i_2$, 因此 $(n,m)\mid i_1+i_2$.

设 $i\in I_1\cap I_2$, 则 $n\mid i, m\mid i$, 因此 $[n,m]\mid i$.

□

P71.6 设 $f:R\to S$ 是环的同态.I 和 J 是环 R 和 S 的理想, 并且 $f(I)\subset J$, 按以下方式作商环之间的映射：

$$\bar{f}:R/I\to S/J, \bar{a}\mapsto [f(a)],$$

其中对于 $a\in R, \bar{a}=a+I$ 为 R/I 中的元素, 而 $[f(a)]=f(a)+J$ 为 S/J 中元素.

(1) 求证：上述映射 $\bar{f}$ 是可定义的, 并且是环同态；

(2) 求证：$\bar{f}:R/I\to S/J$ 是环的同构 $\Longleftrightarrow f(R)+J=S$ 并且 $I=f^{-1}(J)$.

证明.

(1) 要证 $\bar{f}$ 是良定的, 即验证对于 $a_1-a_2\in I$, 则有 $f(a_1)-f(a_2)\in J$. 这是由于 $f(I)\subset J$ 并且 f 是环同态.

下证 $\bar{f}$ 是环同态,

$$\bar{f}(a_1+a_2)=[f(a_1+a_2)]=[f(a_1)+f(a_2)]=[f(a_1)]+[f(a_2)]=\bar{f}(a_1)+\bar{f}(a_2),$$

$$\bar{f}(a_1a_2)=[f(a_1a_2)]=[f(a_1)f(a_2)]=[f(a_1)][f(a_2)]=\bar{f}(a_1)\bar{f}(a_2).$$

(2) $\Longrightarrow$ 显然 $f(R)+J\subset S$, 只证 $S\subset f(R)+J$, 即证 $S/J\subset [f(R)]$. 任取 $[b]\in S/J$, 因为 $\bar{f}$ 是环同构, 所以存在 $\bar{a}\in R/I$ 使得 $f(\bar{a})=[b]$, 按定义 $[b]=[f(a)]$, 得证.

下证 $I=f^{-1}(J)$. 因为 $f(I)\subset J$, 所以 $I\subset f^{-1}(J)$；假设存在 $a\notin I$ 使得 $f(a)\in J$, 那么 $\bar{a}\neq\bar{0}$, 并且 $\bar{f}(\bar{a})=[f(a)]=[0]$, 这与 $\bar{f}$ 是单射矛盾.

$\Longleftarrow$ 即证 $\bar{f}$ 是双射. 由于 $I=f^{-1}(J)$, 所以 $\bar{f}^{-1}([0])=\{\bar{0}\}$, 因此 $\bar{f}$ 是单射.

由于 $f(R)+J=S$, 所以对任意 $b\in S$, 存在 a 使 $[f(a)]=[b]$, 即 $\bar{f}(\bar{a})=[b]$, 因此 $\bar{f}$ 是满射.

□

P71.8 设 $(R,+,\cdot)$ 是含幺（交换）环. 对于 $a,b\in R$, 定义

$$a\oplus b=a+b+1, a\odot b=ab+a+b.$$

求证：$(R,\oplus,\odot)$ 也是含幺（交换）环, 并且与环 $(R,+,\cdot)$ 同构.

证明.

- 加法结合律.
$$(a\oplus b)\oplus c=(a+b+1)\oplus c=a+b+1+c+1=a+b+c+2=a\oplus(b\oplus c).$$
- 加法交换律.
$$a\oplus b=a+b+1=b+a+1=b\oplus a.$$
- 存在零元.
$$-1\oplus a=-1+a+1=a.$$
- 存在逆元.
$$(-a-2)\oplus a=-a-2+a+1=-1.$$
- 乘法结合律.
$$(a\odot b)\odot c=(ab+a+b)\odot c=(ab+a+b)c+(ab+a+b)+c=abc+ac+bc+ab+a+b+c=a\odot(b\odot c)$$
- 存在幺元.
$$0\odot a=0a+0+a=a.$$
- 乘法交换律.
$$a\odot b=ab+a+b=ba+b+a=b\odot a.$$
- 分配律.
$$a\odot(b\oplus c)=a(b\oplus c)+a+(b\oplus c)=a(b+c+1)+a+(b+c+1)=ab+ac+2a+b+c+1.$$
$$a\odot b\oplus a\odot c=(ab+a+b)\oplus(ac+a+c)=ab+a+b+ac+a+c+1=ab+ac+2a+b+c+1.$$

因此 $(R,\oplus,\odot)$ 确实是含幺（交换）环, 下证它与环 $(R,+,\cdot)$ 同构. 为此我们要找一个同构映射 $\theta:(R,+,\cdot)\to(R,\oplus,\odot)$. 猜测映射 $\theta(r)=r-1$ 满足要求, 下证明之.

- 显然 θ 是双射.
- $\theta(a+b)=a+b-1,\theta(a)\oplus\theta(b)=(a-1)\oplus(b-1)=a-1+b-1+1=a+b-1.$
- $\theta(ab)=ab-1,\theta(a)\odot\theta(b)=(a-1)\odot(b-1)=ab-a-b+1+a-1+b-1=ab-1.$

得证！ □

P71.11 设 $I_1,\cdots,I_n,\cdots$ 均是环 R 中的理想, 并且 $I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$. 求证集合 $\bigcup\limits_{n=1}^{\infty}I_n$ 也是环 R 的理想.

证明.

- 任取 $a,b\in\bigcup_{n=1}^{\infty}I_n$, 必存在 $l,m\geqslant 1$, 使得 $a\in I_l,b\in I_m$, 不妨设 $l\leqslant m$, 由于 I_n 是单调上升的, 所以 $a\in I_m$, 由于 I_m 是理想, 所以 $a+b\in I_m$, 所以 $a+b\in\bigcup_{n=1}^{\infty}I_n$.

- 任取 $a\in\bigcup_{n=1}^{\infty}I_n$, 必存在 $m\geqslant 1$ 使得 $a\in I_m$. 任取 $r\in R$, 由于 I_m 是 R 的理想, 那么 $ar\in I_m$, 因此 $ar\in\bigcup_{n=1}^{\infty}I_n$.

得证! □

P78.3 设 D 为整环,m 和 n 为互素的正整数.$a,b\in D$, 如果 $a^m=b^m,a^n=b^n$, 求证 $a=b$.

证明. 设 $m,n>1$, 否则平凡.

因为 m,n 互素, 所以存在整数 u,v 使得 $um+vn=1$. 显然 u,v 都不可能为零, 也不可能同号, 因此不妨设 $u<0<v$. 不妨将 $-u$ 重记为 u, 则 $vn=1+um$.

则有 $a^{vn}=a\cdot a^{um}$, 则 $b\cdot b^{um}=b^{vn}=a\cdot b^{um}$, 因为 D 是整环, 由消去律有 $a=b$. □

P79.13 设 $f:R\to S$ 是环的满同态,$K=\ker f$. 求证：

(1) 若 P 是 R 的素理想并且 $P\supseteq K$, 则 $f(P)$ 也是 S 的素理想；

(2) 若 Q 是 S 的素理想, 则 $f^{-1}(Q)=\{a\in R|f(a)\in Q\}$ 也是 R 的素理想；

(3) S 中素理想和 R 中包含 K 的素理想是一一对应的. 将“素理想”改成“极大理想”则此论断也成立.

证明. 先在本题的条件下证明两个断言：

- 断言若 Q 是 S 中理想, 则 $f^{-1}(Q)$ 是包含 K 的 R 理想. 因为 $0\in Q$, 所以 $f^{-1}(Q)\supset K$. 任取 $a,b\in f^{-1}(Q)$, 则 $f(a),f(b)\in Q$, 则 $f(a+b)\in Q$, 则 $a+b\in f^{-1}(Q)$, 则 $f^{-1}(Q)$ 对加法封闭；任取 $a\in f^{-1}(Q)$ 和 $r\in R$, 有 $f(a)\in Q$, 由于 Q 是理想所以 $f(ar)=f(a)f(r)\in Q$, 因此 $ar\in f^{-1}(Q)$, 即 $f^{-1}(Q)$ 对倍乘封闭, 因此 $f^{-1}(Q)$ 的确是包含 K 的 R 理想.

- 断言若 P 是 R 中理想, 则 $f(P)$ 是 S 中理想. 任取 $f(a),f(b)\in f(P)$, 则 $f(a)+f(b)=f(a+b)\in f(P)$. 任取 $f(a)\in f(P)$ 和 $s\in S$, 因为 f 是满射所以存在 $r\in R$ 使得 $f(r)=s$, 由于 $ar\in P$, 所以 $f(ar)=f(a)s\in f(P)$, 所以 $f(P)$ 对倍乘封闭, 因此 $f(P)$ 是理想.

下面只针对“素”和“极大”进行证明.

(1) 任取 $c,d\in S$ 使得 $c\cdot d\in f(P)$. 由于 f 是满同态所以存在 a,b 使得 $c=f(a),d=f(b)$, 则有 $f(a\cdot b)\in f(P)$. 则存在 $p\in P$ 使得 $f(a\cdot b)=f(p)$, 则 $a\cdot b-p\in K\subset P$, 则 $a\cdot b\in P$, 因为 P 是素理想, 所以或者 $a\in P$ 或者 $b\in P$, 即或者 $c\in f(P)$ 或者 $d\in f(P)$, 因此 $f(P)$ 是 S 的素理想.

(2) 任取 $a,b\in R$ 使得 $a\cdot b\in f^{-1}(Q)$, 即 $f(a\cdot b)=f(a)\cdot f(b)\in Q$, 因为 Q 是素理想, 所以或者 $f(a)\in Q$ 或者 $f(b)\in Q$, 即或者 $a\in f^{-1}(Q)$ 或者 $b\in f^{-1}(Q)$. 因此 $f^{-1}(Q)$ 是 R 的素理想.

(3) 结合第 (2) 问和第一条断言知, 若 Q 是 S 的素理想, 则 $f^{-1}(Q)$ 是包含 K 的素理想.

在 S 中素理想和 R 中包含 K 的素理想之间建立映射 $\theta(Q)=f^{-1}(Q)$.

这是满射因为对任意 R 中包含 K 的素理想, 由 (1) 知 $f(P)$ 也是 S 的素理想, 断言 $f^{-1}(f(P))=P$. 显然 $P\subset f^{-1}(f(P))$, 只证 $f^{-1}(f(P))\subset P$. 若存在 R 中元素 a 使得 $f(a)\in f(P)$, 则存在 p 使得 $f(a)=f(p)$, 则 $a-p\in K\subset P$, 则 $a\in P$, 断言得证.

假如有两个理想 $Q_1,Q_2\triangleleft S$ 满足 $f^{-1}(Q_1)=f^{-1}(Q_2)$. 则对任意元素 $q\in Q_1$, 由于 f 是满射, 所以存在 $p\in R$ 使得 $f(p)=q$, 所以 $p\in f^{-1}(Q_1)=f^{-1}(Q_2)$, 但这意味着 $f(p)=q\in Q_2$, 所以 $Q_1\subset Q_2$, 同理可证 $Q_2\subset Q_1$, 因此 $Q_1=Q_2$, 所以是单射.

接下来将“素理想”替换为“极大理想”重新证明 (1)(2) 两小问, 如果得证, 照搬上面的证明便可得到 S 中极大理想和 R 中包含 K 的极大理想是一一对应的.

$(1)'$ 设 $f(P)\subsetneq Q\triangleleft S$, 则 $P\subsetneq f^{-1}(Q)\triangleleft R$, 由 P 是极大理想知 $f^{-1}(Q)=R$, 则 $f(R)=Q$, 由 f 是满射知 $f(R)=S$ 所以 $Q=S$, 故 $f(P)$ 是极大理想.

$(2)'$ 设 $f^{-1}(Q)\subsetneq P\triangleleft R$, 则 $Q\subsetneq f(P)\triangleleft S$, 由 Q 是极大理想知 $f(P)=S$, 则 $P=f^{-1}(S)=R$, 故 $f^{-1}(Q)$ 是极大理想.

□

P79.14 设 $I\triangleleft R$, 求证 R/I 中素理想均可写成形式 P/I, 其中 P 是 R 中素理想并且包含 I.

证明. $f:R\to R/I, a\mapsto \bar{a}$ 是满同态,$\ker f=I$, 由上一题得证. □

P79.15 $m\geqslant 2$. 试确定环 $\mathbb{Z}_m=\mathbb{Z}/m\mathbb{Z}$ 的全部素理想和极大理想.

解. 由第 13 题, 我们只需要确定 $\mathbb{Z}$ 中包含 $m\mathbb{Z}$ 的全部素理想和极大理想.

$\mathbb{Z}$ 中的理想都是主理想 (a). 若 $m\mathbb{Z}=(m)\subset(a)$, 则 $a\mid m$.

- 由于 (a) 是 $\mathbb{Z}$ 的素理想当且仅当 a 是素数, 因此对 m 进行素因子分解 $m=p_1^{\alpha_1}\cdots p_n^{\alpha_n}$. 则 $(p_i)/m\mathbb{Z}$ 是 $\mathbb{Z}_m$ 的全部素理想.
- 由于 $\mathbb{Z}$ 的素理想和 $\mathbb{Z}$ 的极大理想是一样的, 所以答案是一样的.

□

Ex2.1 定义 $\tilde{R}=\left\{\underline{a}=(a_0,a_1,\cdots)\middle|a_i\in R,a_i=0_R \text{ for } i\gg 0\right\}$. 定义

$$\underline{a}+\underline{b}=(a_0+b_0,a_1+b_1,\cdots)\in\tilde{R}$$

$$\underline{a}\cdot\underline{b}=\underline{c}=(c_0,c_1,\cdots),c_l=\sum_{i\geqslant 0}a_ib_{l-i}\in R,\forall l$$

可验证 $\tilde{R}$ 是环. 证明：$\tilde{R}$ 同构于 $R[x]$.

证明. x 是 $R[x]$ 的生成元, 对于从 $R[x]$ 到另一个环 S 的环同态, 知道了 x 的同态象 $\theta(x)$ 是什么以后, 我们几乎完全确定了这个同态. 具体地说,$\theta(ax^n)=\theta(a)\cdot(\theta(x))^n$, 其中 $a\in R$. 其中 θ 限制在 R 上就为 R 到 S 的一个环同态.

定义环同态 $\theta: R[x] \to \tilde{R}$,$\theta(x) = (0,1,0,0,\cdots)$, $\theta(a) = (a,0,0,\cdots)$, $a \in R$, 因为我们要求 θ 是环同态, 这就必须有

$$\begin{aligned}
\theta(\sum_{i=0}^{n} a_i x^i) &= \sum_{i=0}^{n} \theta(a_i)(\theta(x))^i \\
&= \sum_{i=0}^{n} (a_i,0,0,\cdots)(0,1,0,0,\cdots)^i \\
&= \sum_{i=0}^{n} (a_i,0,0,\cdots)(\underbrace{0,\cdots,0}_{i\text{个}},1,0,\cdots) \\
&= \sum_{i=0}^{n} (\underbrace{0,\cdots,0}_{i\text{个}},a_i,0,\cdots) \\
&= (a_0,a_1,\cdots,a_n,0,\cdots)
\end{aligned}$$

接下来验证它是一个双射.

- 满射. 对于 $(a_0,a_1,\cdots,a_n,\cdots)$, 按定义 $\theta(\sum_{i=0}^{n} a_i x^i) = (a_0,a_1,\cdots,a_n,0,\cdots)$.
- 单射. 若 $\sum_{i=0}^{n} a_i x^i = \sum_{j=0}^{m} b_j x^j$, 按定义系数 a_i 与 b_j 对应相等. 因此它们的像也相等.

□

Ex2.2.1 任意集合 X,R 是环,$Map(X,R)$ 自然成环.

证明. 逐点地定义 $Map(X,R)$ 上的加法和乘法, 加法和乘法所满足的性质继承自 R, 因此 $Map(X,R)$ 成为环. □

Ex2.2.2 $ev: R[x] \to Map(R,R), f(x) \mapsto f$ 是环同态.

证明. 要证两个函数 $ev(f(x)+g(x))$ 和 $ev(f(x))+ev(g(x))$ 相等, 即证它们在每点处的取值相等.

$$ev_a(f(x)+g(x)) = f(a)+g(a) = ev_a(f(x))+ev_a(g(x)).$$

同理可证

$$ev_a(f(x)g(x)) = f(a)g(a) = ev_a(f(x))ev_a(g(x)).$$

而又有 $ev(1)=1$, 后面的 1 指将每个 R 中元素映成 1 的常值映射.

因此 ev 是环同态! □

Ex2.3 $\mathbb{C}[x,y]$ 中, 设 $\mathfrak{p}=(x)$, 验证 $\mathfrak{p}$ 是素理想但不是极大理想.

证明. 假设 $f(x,y), g(x,y) \notin (x)$, 则 $f(x,y)$ 和 $g(x,y)$ 都至少存在一个单项不含 x, 选取其中 y 的次数最高的, 不妨设

$$f(x,y) = \tilde{f}(x,y) + a_n y^n + lower\ terms,$$

$$g(x,y) = \tilde{g}(x,y) + b_m y^m + lower\ terms,$$

则

$$f(x,y)g(x,y) = \widetilde{fg}(x,y) + a_n b_m y^{n+m} + lower\ terms \notin \mathfrak{p},$$

即 $\mathfrak{p}$ 是素理想.

但 $\mathfrak{p}$ 不是极大理想, 这是因为 $\mathfrak{p} \subsetneq (x)+(y) \lhd \mathbb{C}[x,y]$ 但 $1 \notin (x)+(y)$. □

Ex2.4 证明：对固定的 $a \in k$,

$$k[x]/(x-a) \cong k.$$

证明. 定义 $\theta : k[x]/(x-a) \to k$,$\theta([f(x)]) = f(a)$.

- 验证良定性. 若 $(x-a) \mid (g(x)-h(x))$, 则 $g(a)-h(a)=0$, 即 $g(a)=h(a)$, 因此是良定的.
- 证明是环同构.

$$\begin{tikzcd} k[x] \arrow[r, "ev_a"] \arrow[d, "\pi"'] & k \\ k[x]/(x-a) \arrow[r, "\theta"] & k \arrow[u, "inc"'] \end{tikzcd}$$

由同态基本定理,θ 是环同构!

□

Ex2.5 设 $\theta : R \to S$ 是环同态, 则 θ 自然延拓成环同态 $\tilde{\theta} : R[x] \to S[x]$.

证明. 定义 $\tilde{\theta}(r) = \theta(r), \forall r \in R, \tilde{\theta}(x) = x$, 正如我们在 $Ex2.1$ 中提到过的一样, 由

$$\tilde{\theta}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \tilde{\theta}(a_i)(\tilde{\theta}(x))^i = \sum_{i=0}^{n} \tilde{\theta}(a_i)x^i$$

定义出来的 $\tilde{\theta}$ 就是环同态. 这不需要验证, 因为它需要满足的性质正是我们的定义. □

P101.1 如果 D 为整环但不是域, 求证 $D[x]$ 不是主理想整环.

证明. 设非零因子 $a \in D$ 不可逆, 断言 (a,x) 不是主理想.

假设 $(a,x) = (f(x))$, 那么 $(x) \subset (f(x))$, 则 $f(x) \mid x$, 则 $\deg f \leqslant 1$, 若 $\deg f = 1$, 则 $f(x) \mid a$, 矛盾. 因此 $\deg f = 0$, 即 $f(x) = b$,$b \mid a$ □

证明. 设非零因子 $a \in D$ 不可逆, 断言 $(a)+(x)$ 不是主理想.

假设 $(a)+(x) = (f(x))$, 那么 $(x) \subset (f(x))$, 则 $f(x) \mid x$, 则 $\deg f \leqslant 1$, 若 $\deg f = 1$, 则 $f(x) \mid a$, 矛盾. 因此 $\deg f = 0$, 即 $f(x) = b$,$b \mid a$. 则 $(x) \subset (b)$, 则 $b \mid x$, 则 b 可逆, 则 $(a)+(x) = D[x]$, 但这是矛盾的, 因为 $1 \notin (a)+(x)$. □

P101.2 试确定环 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 的自同构群.

- $\mathrm{Aut}\mathbb{Z}[x] = \{Id\}$.
- $\mathrm{Aut}\mathbb{Q}[x] = \{\varphi | \varphi(r) = r, \forall r \in Q, \varphi(x) = qx, q \in \mathbb{Q}\}$

P101.4 $2x+2$ 在 $\mathbb{Z}[x]$ 中和 $\mathbb{Q}[x]$ 中是否为不可约元?

x^2+1 在 $\mathbb{R}[x]$ 和 $\mathbb{C}[x]$ 中是否为不可约元?

答. $2x+2$ 在 $\mathbb{Z}[x]$ 中为可约元, 因为它可以写成 $2x+2=2(x+1)$, 而 2 和 $x+1$ 在 $\mathbb{Z}[x]$ 中都是不可逆的；$2x+2$ 在 $\mathbb{Q}[x]$ 中为不可约元, 由于 $2x+2$ 的次数为 1, 因此 $2x+2$ 只能够被写为非零常数与一次因式的乘积, 而 $\mathbb{Q}$ 中的非零常数都是可逆元, 因此 $2x+2$ 在 $\mathbb{Q}[x]$ 中只有平凡分解, 从而为不可约元.

x^2+1 在 $\mathbb{R}[x]$ 中为不可约元, 因为它不能够被分解为一次因式的乘积；但 x^2+1 在 $\mathbb{C}[x]$ 中为可约元, 因为它有非平凡分解 $x^2+1=(x+\mathrm{i})(x-\mathrm{i})$. □

P101.7 设 $f=\sum a_ix^i\in\mathbb{Z}[x]$ 为首 1 多项式,p 为素数, 以 a 表示 $a\in\mathbb{Z}$ 在环的自然同态 $\mathbb{Z}\to\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$ 之下的像, 而令 $\bar{f}(x)=\sum\bar{a}_ix^i\in\mathbb{Z}_p[x]$. 求证：

(1) 如果对某个素数 p,$\bar{f}(x)$ 在 $\mathbb{Z}_p[x]$ 中不可约, 则 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约；

(2) 如果 $f(x)$ 不是 $\mathbb{Z}[x]$ 中的首 1 多项式, 试问 (1) 中的结论是否成立？

证明.

(1) 设 $f(x)$ 在 $\mathbb{Z}[x]$ 中可约, 则 $f(x)=g(x)h(x)$, 由 $f(x)$ 首一可推出 $g(x)$ 和 $h(x)$ 首一. 因此 $g(x)$ 和 $h(x)$ 在自然同态下的像的 deg 大于等于 1. 则 $\bar{f}(x)=\bar{g}(x)\bar{h}(x)$ 是非平凡分解,$\bar{f}$ 在 $\mathbb{Z}_p[x]$ 中可约, 矛盾！

(2) 不成立. 考虑 $\mathbb{Z}[x]$ 中的可约元 $f(x)=(2x+1)(x+1)=2x^2+3x+1$, 它在自然同态 $\mathbb{Z}\to\mathbb{Z}_2$ 下的像 $\bar{f}=x+\bar{1}$ 不可约.

□

4 第四周

Ex1.1 $\theta(\underset{k[x]}{\gcd}(f,g)) = \underset{K[x]}{\gcd}(\theta(f),\theta(g))$

证明. 设 $d(x) = \underset{k[x]}{\gcd}(f,g), D(x) = \underset{K[x]}{\gcd}(\theta(f),\theta(g))$, 我们来证明 $\theta(d(x)) \mid D(x)$,$D(x) \mid \theta(d(x))$. 要注意这两个整除关系都是在 $K[x]$ 的语境中讨论的.

因为 $d(x)$ 整除 $f(x)$ 和 $g(x)$, 所以 $\theta(d(x))$ 整除 $\theta(f(x))$ 和 $\theta(g(x))$, 按最大公因式的定义,$\theta(d(x)) \mid D(x)$.

由 Bezout 等式, 存在 $u(x), v(x) \in k[x]$ 使得 $d(x) = u(x)f(x) + v(x)g(x)$. 因此在 $K[x]$ 中有 $\theta(d(x)) = \theta(u(x))\theta(f(x)) + \theta(v(x))\theta(g(x))$. 因为 $D(x) \mid \theta(f(x)), D(x) \mid \theta(g(x))$, 所以 $D(x) \mid \theta(d(x))$. □

Ex1.2 证明泛性质中 δ' 的至多唯一性.

证明. 我们要求 $\delta' \circ \theta = \delta$, 这样我们就知道了 $\delta'(\bar{\lambda}) = \delta(\lambda)$, 其中 $\lambda \in k$

我们要求 $\delta'(u) = \alpha$. 由于 K 是 k-线性空间, 并且它有一组基 $\left\{\bar{1}, u, u^2, \cdots, u^{n-1}\right\}$, 其中 $n = \deg f$. 而 $\delta'(u^i) = (\delta'(u))^i, 1 \leqslant i \leqslant n-1$.

因此我们就知道了 δ' 在所有元素上的作用效果, 因此 δ' 是至多唯一的. □

Ex1.3 证明：$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

证明. 定义映射 $\theta : \mathbb{R}[x]/(x^2+1) \to \mathbb{C}, \overline{f(x)} = \overline{ax+b} = \bar{a}u + \bar{b} \mapsto a\mathrm{i} + b$.

由带余除法, 余式 $ax+b$ 唯一, 因此该映射是良定的.

- 保加法

$$\begin{aligned}&\theta(\overline{a_1x+b_1} + \overline{a_2x+b_2}) = \theta(\overline{(a_1+a_2)x + (b_1+b_2)}) = (a_1+a_2)\mathrm{i} + (b_1+b_2)\\ =&(a_1\mathrm{i}+b_1) + (a_2\mathrm{i}+b_2) = \theta(\overline{a_1x+b_1}) + \theta(\overline{a_2x+b_2})\end{aligned}$$

- 保乘法. 课上已经证明过 $(a_1u+b_1)(a_2u+b_2) = (a_1b_2+a_2b_1)u + (b_1b_2 - a_1a_2)$, 因此

$$\begin{aligned}&\theta((a_1u+b_1)(a_2u+b_2)) = \theta((a_1b_2+a_2b_1)u + (b_1b_2-a_1a_2)) = (a_1b_2+a_2b_1)\mathrm{i} + (b_1b_2-a_1a_2)\\ =&(a_1\mathrm{i}+b_1)(a_2\mathrm{i}+b_2) = \theta(a_1u+b_1)\theta(a_2u+b_2)\end{aligned}$$

- 单射.$\overline{f(x)} \in \ker\theta$ 当且仅当 $f(x) \equiv 0 \mod (x^2+1)$, 即 $\overline{f(x)} = \overline{x^2+1} = \bar{0}$. 因此是单射.
- 满射. 对任意 $a\mathrm{i}+b \in \mathbb{C}$, 容易验证 $\theta(\overline{au+b}) = a\mathrm{i}+b$, 因此是满射.

□

Ex2.1 $\mathbb{F}_9$ 的乘法表.

解.

	$\bar{0}$	$\bar{1}$	$\bar{2}$	u	$\bar{1}+u$	$\bar{2}+u$	$\bar{2}u$	$\bar{1}+\bar{2}u$	$\bar{2}+\bar{2}u$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	u	$\bar{1}+u$	$\bar{2}+u$	$\bar{2}u$	$\bar{1}+\bar{2}u$	$\bar{2}+\bar{2}u$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\bar{2}u$	$\bar{2}+\bar{2}u$	$\bar{1}+\bar{2}u$	u	$\bar{2}+u$	$\bar{1}+u$
u	$\bar{0}$	u	$\bar{2}u$	$\bar{2}$	$\bar{2}+u$	$\bar{2}+\bar{2}u$	$\bar{1}$	$\bar{1}+u$	$\bar{1}+\bar{2}u$
$\bar{1}+u$	$\bar{0}$	$\bar{1}+u$	$\bar{2}+\bar{2}u$	$2\bar{+}u$	$\bar{2}u$	$\bar{1}$	$\bar{1}+\bar{2}u$	$\bar{2}$	u
$\bar{2}+u$	$\bar{0}$	$\bar{2}+u$	$\bar{1}+\bar{2}u$	$\bar{2}+\bar{2}u$	$\bar{1}$	u	$\bar{1}+u$	$\bar{2}u$	$\bar{2}$
$\bar{2}u$	$\bar{0}$	$\bar{2}u$	u	$\bar{1}$	$\bar{1}+\bar{2}u$	$\bar{1}+u$	$\bar{2}$	$\bar{2}+\bar{2}u$	$\bar{2}+u$
$\bar{1}+\bar{2}u$	$\bar{0}$	$\bar{1}+\bar{2}u$	$\bar{2}+u$	$\bar{1}+u$	$\bar{2}$	$\bar{2}u$	$\bar{2}+\bar{2}u$	u	$\bar{1}$
$\bar{2}+\bar{2}u$	$\bar{0}$	$\bar{2}+\bar{2}u$	$\bar{1}+u$	$\bar{1}+\bar{2}u$	u	$\bar{2}$	$\bar{2}+u$	$\bar{1}$	$\bar{2}u$

□

Ex2.2 证明 $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm(1+\omega)\}$.

证明. 我们证明一个稍一般的结论. 如果 size functionφ 满足 $\varphi(ab) = \varphi(a)\varphi(b)$, 则 x 可逆的必要条件是 $\varphi(x) = 1$.（我感觉这应该是一个充要条件, 但充分性我不会证）

设 $\varphi(ab) = \varphi(a)\varphi(b)$, 令 $a = 1$ 有 $\varphi(1) = 1$. 若 $xy = 1$, 则 $\varphi(x)\varphi(y) = 1$, 则 $\varphi(x) = \varphi(y) = 1$.

具体到本题中, 设 $x = a + b\omega, y = c + d\omega$, 则

$$\varphi(x) = a^2 + b^2 - ab, \varphi(y) = c^2 + d^2 - cd,$$

$$\varphi(x)\varphi(y) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 - a^2cd - b^2cd - abc^2 - abd^2 + abcd.$$

$$xy = ac + bd\omega^2 + (ad + cb)\omega = (ac - bd) + (ad + cb - bd)\omega$$

$$\varphi(xy) = a^2c^2+b^2d^2-2abcd+a^2d^2+c^2b^2+b^2d^2+2abcd-2abd^2-2b^2cd-a^2cd-abc^2+abcd+abd^2+b^2cd-b^2d^2$$

$$\varphi(xy) = a^2c^2 + a^2d^2 + c^2b^2 + b^2d^2 - abd^2 - b^2cd - a^2cd - abc^2 + abcd$$

满足 $\varphi(xy) = \varphi(x)\varphi(y)$. 因此 x 可逆的必要条件是 $\varphi(x) = 1$.

设 $x = a + b\omega$, 则 $\varphi(x) = a^2 + b^2 - ab$. 若 $a^2 + b^2 - ab = 1$, 则 $(a - b)^2 = 1 - ab$.

容易看出 $U(\mathbb{Z}[\omega]) \subset \{\pm 1, \pm\omega, \pm(1+\omega)\}$.

容易验证 $1 \cdot 1 = 1, \omega \cdot \omega^2 = 1, (1+\omega)(-\omega) = 1$, 因此 $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm(1+\omega)\}$. □

Ex2.3 证明 $\mathbb{Z}[\sqrt{3}]$ 是欧几里得整环但 $\mathbb{Z}[\sqrt{5}]$ 不是.

证明. 设 $x = a + b\sqrt{3}$, 定义 $N(x) = |a^2 - 3b^2|$, 只需注意到对于 $r = m + n\sqrt{3}$, 其中 $|m|, |n| \leqslant \dfrac{1}{2}$, 我们有 $N(r) = |m^2 - 3n^2| \leqslant \dfrac{3}{4} < 1$. 因此 $\mathbb{Z}[\sqrt{3}]$ 是欧几里得整环.

要证 $\mathbb{Z}[\sqrt{5}]$ 不是欧几里得整环, 只需注意到 2 是不可约元, 但它不是素元, 因为 $2 \mid (\sqrt{5}-1)(\sqrt{5}+1)$, 但 $2 \nmid (\sqrt{5}-1)$ 且 $2 \nmid (\sqrt{5}+1)$. □

Ex2.4 证明 $\mathbb{Q}(\sqrt{-3}) \cong Frac(\mathbb{Z}[\omega])$

证明. 由 $\sqrt{-3} = 2\omega + 1$, 显然有 $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$, 因此只需证 $\mathbb{Q}(\omega) \cong Frac(\mathbb{Z}[\omega])$.

回忆分式域的泛性质. 已知存在自然嵌入 $\varphi : \mathbb{Z}[\omega] \hookrightarrow \mathbb{Q}(\omega)$, 那么存在单同态 $\tilde{\varphi} : Frac(\mathbb{Z}[\omega]) \hookrightarrow \mathbb{Q}(\omega)$, 它的定义是 $\tilde{\varphi}(\frac{y}{z}) = \varphi(y)(\varphi(z))^{-1}$. 要证明同构只需证明它是满的. 对任意 $x = \frac{a}{b} + \frac{c}{d}\omega \in \mathbb{Q}(\omega)$,$x = \frac{ad + bc\omega}{bd}$, 取 $y = ad + bc\omega, z = bd$, 则 $\tilde{\varphi}(\frac{y}{z}) = x$. $\square$

5 第五周

Ex1.1 设 $p = a^2 + b^2$ 形如 $4k+1$, 其中 $a, b > 0$, 证明

$$\mathbb{Z}[\mathrm{i}]/(a+b\mathrm{i}) \simeq \mathbb{F}_p.$$

证明. 断言,$\mathbb{Z}[\mathrm{i}] = \mathbb{Z} + (a+b\mathrm{i})$. 若断言成立, 由第二同构定理,

$$\mathbb{F}_p = \frac{\mathbb{Z}}{\mathbb{Z} \cap (a+b\mathrm{i})} \simeq \frac{\mathbb{Z}+(a+b\mathrm{i})}{(a+b\mathrm{i})} = \mathbb{Z}[i]/(a+b\mathrm{i}).$$

下证断言, 只需证 $\mathrm{i} \in \mathbb{Z} + (a+b\mathrm{i})$. 由于 $(b,p) = 1$, 存在 u, v 使得 $ub + vp = 1$. 因此 $\Im(u(a+b\mathrm{i}) + vp) = 1$, 从而 $\mathrm{i} \in \mathbb{Z} + (a+b\mathrm{i})$. □

P92.2 分别将 60 和 $81 + 8\sqrt{-1}$ 在环 $\mathbb{Z}[\sqrt{-1}]$ 中分解成不可约元之积.

解.

$60 = 2^2 \times 3 \times 5 = (1+\mathrm{i})^2(1-\mathrm{i})^2 \times 3 \times (2+\mathrm{i})(2-\mathrm{i})$.

由于 $N(81+8\mathrm{i}) = 5^3 \times 53 = (2+\mathrm{i})^2(2-\mathrm{i})^3(7+2\mathrm{i})(7-2\mathrm{i})$.

故 $81 + 8\mathrm{i} = \mathrm{i}(2+\mathrm{i})^3(7+2\mathrm{i})$. □

Ex2.1 $\mathbb{Z}[\sqrt{-3}]/(2) \simeq \mathbb{F}_2[x]/(x^2+\bar{1})$.

证明. $\mathbb{Z}[\sqrt{-3}]/(2) = \dfrac{\mathbb{Z}[x]/(x^2+3)}{(2, x^2+3)/(x^2+3)} \simeq \dfrac{\mathbb{Z}[x]}{(2, x^2+3)} \simeq \dfrac{\mathbb{Z}[x]/(2)}{(2, x^2+3)/(2)} \simeq \mathbb{F}_2[x]/(x^2+\bar{1})$. □

Ex2.2 $c \in R$, 证明 $R[x]/(c) \simeq R/(c)[x]$.

证明. 由自然同态 $\varphi : R \to R/(c)$ 诱导了环同态 $\tilde{\varphi} : R[x] \to R/(c)[x]$.

由 φ 是满射知 $\tilde{\varphi}$ 是满射.

$f(x) \in \ker\tilde{\varphi} \Longleftrightarrow \tilde{f}(x) = 0 \Longleftrightarrow c$ 整除各项系数 $\Longleftrightarrow c$ 整除 $f \Longleftrightarrow f(x) \in (c)$.

由同态基本定理知 $R[x]/(c) \simeq R/(c)[x]$. □

Ex2.3 考虑 $k[x,y]/(y^2 - x^3) = A$, 找出 A 的 k-基,A 是 UFD?

证明. 到现在也没有完全弄懂. □

Ex2.4 $\sigma : \mathbb{Z}[x] \to \mathbb{Z}[x]$,$f(x) \mapsto f(x+1)$, 证明 σ 是自同构.

证明. 断言, 对任意 $a \in \mathbb{Z}$,$\sigma_a : \mathbb{Z}[x] \to \mathbb{Z}[x], f(x) \mapsto f(x+a)$ 为环同态.

若断言成立,$\sigma_a \circ \sigma_{-a} = \sigma_{-a} \circ \sigma_a = id_{\mathbb{Z}[x]}$, 所以 σ_a 是环同构.

下证断言.

- $\sigma(f) + \sigma(g) = f(x+a) + g(x+a) = (f+g)(x+a) = \sigma(f+g)$.
- $\sigma(f) \cdot \sigma(g) = f(x+a)g(x+a) = (fg)(x+a) = \sigma(fg)$.

□

P102.11 将 $x^n - 1 (3 \leqslant n \leqslant 10)$ 在 $\mathbb{Z}[x]$ 中作素因子分解.

解.

- $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+x+1)$,$p=2,3,5,7$.
  - $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$,$g(x):=f(x+1)\equiv x^{p-1} \mod p$.Eisenstein.
- $x^4-1=(x-1)(x+1)(x^2+1)$
  - x^2+1 在 $\mathbb{R}$ 中无根从而在 $\mathbb{Z}$ 中无根, 从而不可约.
- $x^6-1=(x^3-1)(x^3+1)=(x-1)(x+1)(x^2+x+1)(x^2-x+1)$
  - x^2+x+1,x^2-x+1 在 $\mathbb{R}$ 中无根从而在 $\mathbb{Z}$ 中无根, 从而不可约.
- $x^8-1=(x-1)(x+1)(x^2+1)(x^4+1)$
  - $f(x)=x^4+1$,$g(x):f(x+1)=x^4+4x^3+6x^2+4x+2$.Eisenstein.
- $x^9-1=(x-1)(x^2+x+1)(x^6+x^3+1)$
  - $f(x)=x^6+x^3+1$,$g(x):f(x+1)=x^6+6x^5+15x^4+21x^3+18x^2+9x+3$.Eisenstein.
- $x^{10}-1=(x-1)(x+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)$

□

P102.12 设 D 为整环,$f(x)\in D[x]$,$c\in D$. 求证：

(1) $f(x)$ 在 $D[x]$ 中本原 $\Longleftrightarrow f(x+c)$ 在 $D[x]$ 中本原；

(2) $f(x)$ 在 $D[x]$ 中不可约 $\Longleftrightarrow f(x+c)$ 在 $D[x]$ 中不可约.

证明.

(1)
- 要讨论本原多项式的概念, 应假设 D 为 UFD.
- 我要证 p 是 $f(x)$ 的系数的公因子 $\Longleftrightarrow p$ 是 $f(x+c)$ 的系数的公因子, 从而 $f(x)$ 与 $f(x+c)$ 有相同的容度. 只需要证 $\Longrightarrow$, 另一侧取 $c'=-c$ 即得.

  对 f 的次数进行归纳.

  当 $\deg f=1$ 时, 设 $f(x)=a_1x+a_0$,$f(x+c)=a_1x+a_1c+a_0$. 若 $p\mid a_1$ 且 $m\mid a_0$, 则 $p\mid a_1$ 且 $p\mid a_1c+a_0$.

  设当 $\deg f=k\geqslant 1$ 时命题成立, 要证 $\deg f=k+1$ 时成立. 设 $f(x)=a_{k+1}x^{k+1}+g(x)$, 其中 $\deg g=k$. $f(x+c)=a_{k+1}(x+c)^{k+1}+g(x+c)$. 设 $p\mid a_{k+1}$ 且整除 $g(x)$ 的各项系数, 断言 p 也整除 $f(x+c)$ 的各项系数.

  $f(x+c)$ 的最高次项系数为 a_{k+1},$p\mid a_{k+1}$.

  观察 $f(x+c)$ 的其他次项的系数, 它们由两项加起来组成, 第一项含有因子 a_{k+1}, 从而被 p 整除, 第二项是 $g(x+c)$ 的对应次项前系数, 由归纳假设, 他被 p 整除, 从而两项加起来也被 p 整除.

(2) $f(x)$ 的分解总是对应 $f(x+c)$ 的一个分解. 可逆元不含 x, 在平移作用下不变. 所以 $f(x)$ 只有平凡分解当且仅当 $f(x+c)$ 只有平凡分解.

□

6 第六周

Ex1.1 设 φ 是 $\theta : k \hookrightarrow K$ 到 $\theta' : k \hookrightarrow K'$ 的域扩张同构, 证明：$\alpha \in K$ 在 k 上代数当且仅当 $\varphi(\alpha) \in K'$ 在 k 上代数, 且 α 与 $\varphi(\alpha)$ 有相同的最小多项式.

证明. 只需证明 α 的零化多项式也是 $\varphi(\alpha)$ 的零化多项式.

设 $f(x) \in k[x]$ 是 α 的零化多项式, 则 $\theta(f)(\alpha) = 0_K$.

将 φ 作用到等式两侧, 得到 $\theta'(f)(\varphi(\alpha)) = 0_{K'}$, 即 $f(x)$ 也是 $\varphi(\alpha)$ 的零化多项式.

同理可证 $\varphi(\alpha)$ 的零化多项式也是 α 的零化多项式. 得证. □

P111.1 设 F/K 为域的扩张,$u \in F$ 是 K 上奇次代数元素. 求证 $K(u) = K(u^2)$.

证明. 显然 $K(u^2) \subset K(u)$, 只需证 $K(u) \subset K(u^2)$, 只需证 $u \in K(u^2)$.

采取构造性证明. 设 $f(x)$ 是 u 的极小多项式, 取出 $f(x)$ 所有的偶数次项记为 $g(x) = g'(x^2)$, 取出 $f(x)$ 所有的奇数次项记为 $x \cdot h(x) = x \cdot h'(x^2)$, 则 $f(x) = g'(x^2) + x \cdot h'(x^2)$. 由于 $f(x)$ 是奇次的, 所以 $h'(x^2) \neq 0$. 由于 $f(x)$ 是最小多项式, 所以 $h'(u^2) \neq 0$. 将 ev_u 作用于两侧得到 $f(u) = g'(u^2) + u \cdot h'(u^2) = 0$, 则 $u = -\dfrac{g'(u^2)}{h'(u^2)} \in K(u^2)$. □

P111.2 给出域扩张 F/K 的例子, 使得 $F = K(u, v)$,u 和 v 均是 K 上超越元素, 但是 $F \ncong K(x_1, x_2)$.

证明. 考虑 $K = \mathbb{Q}$,$F = \mathbb{Q}(\mathrm{e}, 2\mathrm{e}) = \mathbb{Q}(\mathrm{e}) \cong \mathbb{Q}(x_1)$.$\mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_1)(x_2)$. 假设 $\varphi : \mathbb{Q}(x_1) \to \mathbb{Q}(x_1)(x_2)$ 是同构, 断言存在域扩张 $\theta : \mathbb{Q}(x_1) \hookrightarrow \mathbb{Q}(x_1)$ 和域扩张 $\theta' : \mathbb{Q}(x_1) \hookrightarrow \mathbb{Q}(x_1)(x_2)$ 使得 φ 是 θ 和 θ' 之间的域扩张同构. 只需取 θ 为恒同映射,$\theta' = \varphi \circ \theta$. 因此 φ 也是线性空间同构, 但 $\mathbb{Q}(x_1)$ 作为 $\mathbb{Q}(x_1)$-线性空间是有限维（1 维）的,$\mathbb{Q}(x_1)(x_2)$ 作为 $\mathbb{Q}(x_1)$-线性空间是无限维的, 矛盾. □

P111.3 设 p 为素数, 分别求扩张 $\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/p})/\mathbb{Q}$ 和 $\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/8})/\mathbb{Q}$ 的次数.

证明. $x^{p-1} + \cdots + x + 1$ 和 $x^4 + 1$ 分别是 $\mathrm{e}^{2\pi\mathrm{i}/p}$ 和 $\mathrm{e}^{2\pi\mathrm{i}/8}$ 在 $\mathbb{Q}$ 上的不可约零化多项式, 从而两个域扩张的次数分别为 $p - 1$ 和 4. □

P111.4 求元素 a 在域 K 上的极小多项式, 其中

(1) $a = \sqrt{2} + \sqrt{3}, K = \mathbb{Q}$;

(2) $a = \sqrt{2} + \sqrt{3}, K = \mathbb{Q}(\sqrt{2})$;

(3) $a = \sqrt{2} + \sqrt{3}, K = \mathbb{Q}(\sqrt{6})$.

解. 设 a 在 K 的极小多项式为 $f(x)$,$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{6})$.

(1) $\deg f(x) = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, 而 $x^4 - 10x^2 + 1$ 是 $\sqrt{2} + \sqrt{3}$ 的零化多项式, 因此 $f(x) = x^4 - 10x^2 + 1$.

(2) 同理 $f(x) = x^4 - 10x^2 + 1$.

(3) 同理 $f(x) = x^2 + 2\sqrt{6} - 5$.

□

P111.5 设 u 属于 K 的某个扩域, 并且 u 在 K 上代数. 如果 $f(x)$ 为 u 在 K 上的极小多项式, 则 $f(x)$ 必为 $K[x]$ 中不可约多项式. 反之, 若 $f(x)$ 是 $K[x]$ 中首 1 不可约多项式, 并且 $f(u)=0$, 则 $f(x)$ 为 u 在 K 上的极小多项式.

证明. 若 $f(x)$ 为 u 在 K 上的极小多项式. 设 $f(x)=g(x)h(x)$, 则有 $g(u)=0$ 或 $h(u)=0$. 不妨设 $g(u)=0$, 则 $g(x)\mid h(x)$, 而 $f(x)\mid g(x)$, 因此 $f(x)=g(x)$. 从而 $f(x)$ 不可约.

反之, 设 $g(x)$ 为 u 在 K 上的极小多项式, 则 $g(x)\mid f(x)$. 而 $K[x]$ 是 UFD, 知 $g(x)=f(x)$. □

P111.6 设 u 是域 K 的某扩域中的元素, 并且 x^n-a 是 u 在 K 上的极小多项式. 对于 $m\mid n$, 求 u^m 在域 K 上的极小多项式.

证明. 设 u^m 的极小多项式为 $f(x)$, 则 $f(x)\mid x^{n/m}-a$; 而 $f(x^m)$ 是 u 的零化多项式, 因此 $x^n-a\mid f(x^m)$. 故 $x^{n/m}-a\mid f(x)$. 因此 $f(x)=x^{n/m}-a$. □

Ex2.1 证明 $\mathbb{Q}(\sqrt[3]{2})$,$\mathbb{Q}(\sqrt[3]{2}\omega)$,$\mathbb{Q}(\sqrt[3]{2}\omega^2)$ 作为 $\mathbb{C}$ 的子域两两不同, 但作为域扩张是同构的.

证明. $\sqrt[3]{2}$,$\sqrt[3]{2}\omega$,$\sqrt[3]{2}\omega^2$ 是 x^3-2 的三个根.

显然有 $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\notin\mathbb{Q}(\sqrt[3]{2})$.

断言,$\sqrt[3]{2}\notin\mathbb{Q}(\sqrt[3]{2}\omega)$. 若不然,$\mathbb{Q}(\sqrt[3]{2})\subset\mathbb{Q}(\sqrt[3]{2}\omega)$. 考虑域扩张 $\mathbb{Q}\hookrightarrow\mathbb{Q}(\sqrt[3]{2})\hookrightarrow\mathbb{Q}(\sqrt[3]{2}\omega)$, 由于 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2}\omega):\mathbb{Q}]=3$, 所以 $[\mathbb{Q}(\sqrt[3]{2}\omega):\mathbb{Q}(\sqrt[3]{2})]=1$, 因此 $\mathbb{Q}(\sqrt[3]{2})=\mathbb{Q}(\sqrt[3]{2}\omega)$, 矛盾.

同理可证 $\sqrt[3]{2}\notin\mathbb{Q}(\sqrt[3]{2}\omega^2)$.

假设 $\sqrt[3]{2}\omega\in\mathbb{Q}(\sqrt[3]{2}\omega^2)$, 则 $\omega\in\mathbb{Q}(\sqrt[3]{2}\omega^2)$, 则 $\sqrt[3]{2}\in\mathbb{Q}(\sqrt[3]{2}\omega^2)$, 矛盾.

同理可证 $\sqrt[3]{2}\omega^2\notin\mathbb{Q}(\sqrt[3]{2}\omega)$.

因此 $\mathbb{Q}(\sqrt[3]{2})$,$\mathbb{Q}(\sqrt[3]{2}\omega)$,$\mathbb{Q}(\sqrt[3]{2}\omega^2)$ 作为 $\mathbb{C}$ 的子域两两不同. □

Ex2.2 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证明. 显然有 $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$.

而 $\dfrac{1}{\sqrt{2}+\sqrt{3}}=\sqrt{3}-\sqrt{2}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$, 因此 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$. □

Ex2.3 $x^3-2\in\mathbb{Q}(\omega)[x]$ 不可约.

证明. 设 $a+b\omega$ 为 x^3-2 的根,$a,b\in\mathbb{Q}$, 则 $(a+b\omega)^2=2$, 得

$$(a^3+b^3-3ab^2-2)+3ab(b-a)\omega=0.$$

从而 $a^3+b^3-3ab^2-2=0, 3ab(b-a)=0$, 解得 $\begin{cases}a=0,\\ b=\sqrt[3]{2}/\sqrt[3]{2}\omega/\sqrt[3]{2}\omega^2\end{cases}$, $\begin{cases}a=\sqrt[3]{2}/\sqrt[3]{2}\omega/\sqrt[3]{2}\omega^2,\\ b=0\end{cases}$, $a=b=-\sqrt[3]{2}/-\sqrt[3]{2}\omega/-\sqrt[3]{2}\omega^2$. 都不成立, 因此无根, 从而不可约. □

Ex2.4 $\overline{Q}$ 是代数闭的.

证明. 任意 $f(x)\in\overline{Q}[x]$,$f(x)$ 在 $\mathbb{C}[x]$ 上完全分裂, 即 $f(x)=\prod_{i=1}^{n}(x-a_i)$. 而 $f(x)\in\overline{Q}[x]$, 故 $a_i\in\overline{\overline{Q}}$. 而 $\overline{\overline{\mathbb{Q}}}$ 在 $\overline{Q}$ 上代数,$\overline{Q}$ 在 $\mathbb{Q}$ 上代数, 故 $\overline{\overline{Q}}$ 在 $\mathbb{Q}$ 上代数. 故 $a_i\in\overline{Q}$, 即 $f(x)$ 在 $\overline{Q}[x]$ 上完全分裂. □

P112.9 设 K 为域,$u\in K(x), u\notin K$, 求证 x 在域 $K(u)$ 上代数.

证明. 设 $u=\dfrac{\sum_{i=0}^{n}a_ix^i}{\sum_{j=0}^{m}b_jx^j}$, 其中 $a_nb_m\neq 0, m+n>0$, 从而 $\sum\limits_{i=0}^{n}a_ix^i-u\left(\sum\limits_{j=0}^{m}b_jx^j\right)=0$, 由于 $u\in K(x)\backslash K$, 可以知道该多项式不为零多项式, 因此 x 在 $K(u)$ 上代数. □

P112.10 设 u 是多项式 x^3-6x^2+9x+3 的一个实根.

(1) 求证 $[\mathbb{Q}(u):\mathbb{Q}]=3$.

(2) 试将 $u^4,(u+1)^{-1},(u^2-6u+8)^{-1}$ 表示成 $1,u,u^2$ 的 $\mathbb{Q}$ 线性组合.

证明.

(1) 利用 Eisenstein 判别法知 x^3-6x^2+9x+3 不可约, 从而 $[\mathbb{Q}(u):\mathbb{Q}]=3$.

(2)
- $u^4=27u^2-57u-18$.
- $(u+1)^{-1}=\dfrac{1}{13}u^2-\dfrac{7}{13}u+\dfrac{16}{13}$.

□

P112.11 设 $u=\dfrac{x^3}{x+1}$, 试问 $[\mathbb{Q}(x):\mathbb{Q}(u)]=?$

解. $f(y)=y^3-uy-u\in\mathbb{Q}(u)[y]$ 是 x 在 $\mathbb{Q}(u)$ 上的零化多项式. 由于 $\mathbb{Q}[u]$ 是 UFD, 且 $\mathbb{Q}[u]/(u)\simeq\mathbb{Q}$, 即 u 是不可约元. 由 Eisenstein 判别法 $f(y)$ 在 $\mathbb{Q}[u][y]$ 中不可约. 从而在 $\mathbb{Q}(u)[y]$ 上不可约. 故 $[\mathbb{Q}(x):\mathbb{Q}(u)]=3$. □

P112.14 设 M/K 为域的扩张,M 中元素 u,v 分别是 K 上的 m 次和 n 次代数元素,$F=K(u)$,$E=K(v)$.

(1) 求证 $[FE:K]\leqslant mn$;

(2) 如果 $(m,n)=1$, 则 $[FE:K]=mn$.

证明.

(1) 设 u,v 在 K 上的极小多项式分别为 $f(x)$ 和 $g(x)$. 由于 $f(x)$ 是 u 在 $E=K(v)$ 上的零化多项式. 因此 $[FE;E]\leqslant\deg f=m$. 因此 $[FE:K]=[FE:E][E:K]\leqslant mn$.

(2) $m=[F:K]\mid[FE:K]$. 同理 $n\mid[FE:K]$. 由于 $(m,n)=1$,$mn\mid[FE:K]$, 而 $[FE:K]\leqslant mn$, 从而 $[FE:K]=mn$.

□

7 第七周

Ex1.1 $f: R \to R'$ 是环同构,$I \lhd R$, 则 f 诱导 R/I 到 $R'/f(I)$ 的一个环同构.

证明.

- 首先验证 $f(I)$ 是一个理想.
  - 对任意 $f(a)+f(b)$, 其中 $a,b\in I$, 由于 I 是理想,f 是环同构, 所以 $f(a+b)\in f(I)$.
  - 对任意 $f(a),s$, 其中 $a\in I, s\in R'$, 由于 f 是满射, 所以存在 $r\in R$ 使得 $f(r)=s$. 由于 I 是理想, 所以 $ar\in I$. 从而 $f(a)\cdot s = f(a)\cdot f(r) = f(ar)\in f(I)$.
- 考虑 $\varphi: R\to R'/f(I), r\mapsto f(r)+f(I)$.
  - 首先验证良好定义. 对任意 $r-r'\in I$,$f(r)-f(r')\in f(I)$, 因此是良好定义的.
  - φ 是环同构 $f: R\to R'$ 和自然映射 $\pi: R'\to R'/f(I)$ 的复合, 从而是满同态.
  - $r\in\ker\varphi \Longleftrightarrow f(r)\in f(I) \Longleftrightarrow r\in I$.
  - 由同态基本定理 $\tilde{\varphi}: R/I\to R'/f(I)$ 是环同构.

□

Ex1.2 $\mathbb{F}_9 \simeq \mathbb{F}_9' \simeq \mathbb{F}_9''$

证明. $\mathbb{F}_3[x]$ 中的首一不可约二次多项式只有三个,

$$f_1(x) = x^2+\bar{1}, f_2(x) = x^2+x-\bar{1}, f_3(x) = x^2-x-\bar{1}.$$

相应地, 我们可以构造出三个 $\mathbb{F}_9$,

$$\theta_1: \mathbb{F}_3 \hookrightarrow \mathbb{F}_3[x]/(x^2+\bar{1}), u := x+(x^2+\bar{1}), u^2+\bar{1}=0.$$

$$\theta_2: \mathbb{F}_3 \hookrightarrow \mathbb{F}_3[x]/(x^2+x-\bar{1}), v := x+(x^2+x-\bar{1}), v^2++v-\bar{1}=0.$$

$$\theta_3: \mathbb{F}_3 \hookrightarrow \mathbb{F}_3[x]/(x^2-x-\bar{1}), w := x+(x^2-x-\bar{1}), w^2-w-\bar{1}=0.$$

欲证 $\mathbb{F}_3(u)\simeq\mathbb{F}_3(v)$,$u$ 在 $\mathbb{F}_3$ 上的最小多项式是 $x^2+\bar{1}$, 恒同映射映过去还是 $x^2+\bar{1}$, 在 $\mathbb{F}_3[v]$ 中分解得 $x^2+\bar{1} = (x-v+\bar{1})(x+v+\bar{2})$, 于是

$$\varphi: \mathbb{F}_3(u)\to\mathbb{F}_3(v), u\mapsto v\to\bar{1}$$

是 $\mathbb{F}_3(u)$ 到 $\mathbb{F}_3(v)$ 的同构映射. 同理可证 $\mathbb{F}_3(u)\simeq\mathbb{F}_3(w)$. □

Ex2.1 求 $\mathrm{Aut}(\mathbb{F}_9)$.

解. $x^2+\bar{1} = (x-u)(x-\bar{2}u)$.

因此 $\mathrm{Aut}(\mathbb{F}_9)$ 只有两个元素, 一个是恒同映射, 一个将 u 映成 $\bar{2}u$. □

Ex2.2 $k=\mathbb{F}_p(t)$,$x^p-t\in k[x]$, 证明它不可约.

证明.

引理 7.1. 设 F 的特征为素数 p,$a\in F$. 则 x^p-a 或者在 $F[x]$ 中不可约, 或者是 $F[x]$ 中一次多项式的 p 次幂. 并且对于前一种情形,x^p-a 是 F 上的不可分多项式.

证明. 设 E 为 x^p-a 在 F 上的分裂域, 则 E 的特征也为 p.

设 $b,c\in E$ 为 x^p-a 的两个根, 则 $b^p-c^p=(b-c)^p=0\Longrightarrow b=c$, 从而 $x^p-a=(x-b)^p$.

若 $b\in F$, 则 x^p-a 为 $(x-b)\in F[x]$ 的 p 次幂.

若 $b\notin F$, 断言 x^p-a 在 $F[x]$ 中不可约, 从而是 F 上的不可分多项式.

设在 $F[x]$ 中有分解 $x^p-a=f(x)g(x)$, 该式在 $E[x]$ 中同样成立, 所以 $f(x)=u(x-b)^k\in E[x]$. 因为 $f(x)\in F[x]$, 所以 $u(x-b)^k\in F[x]$, 所以首项系数 $u\in F$, 常数项 $\pm ub^k\in F$, 从而 $b^k\in F$. 但是 $b^p=a\in F$,$(k,p)=1$, 从而 $b\in F$, 矛盾. □

回到本题, 假设 $b\in k$ 满足 $b^p=t$, 不妨设 $b=\dfrac{m(t)}{n(t)}$, 则 $m^p(t)=tn^p(t)$, 比较两侧次数得 $p(\deg m-\deg n)=1$, 显然不存在这样的 b. 因此 x^p-t 不可约. □

Ex2.3 在 $\mathbb{F}_2[x]$ 中分解 $x^{16}-x$.

解. 先在 $\mathbb{Z}[x]$ 中对 $x^{16}-x$ 进行初步分解:

$$x^{16}-x=x(x^{15}-x)=x\Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x)=x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)\Phi_{15}(x).$$

下面列出 $\mathbb{F}_2[x]$ 中所有的 4 次首一多项式, 通过代入 $\bar{0}$ 和 $\bar{1}$, 筛掉其中绝大部分, 然后注意到唯一的 2 次不可约多项式是 x^2+x+1, 对其平方得 x^4+x^2+1. 所以除 $\Phi_5(x)$ 之外的 4 次不可约多项式是 x^4+x+1 和 x^4+x^3+1.

所以在 $\mathbb{F}_2[x]$ 中

$$x^{16}-x=x(x+\bar{1})(x^2+x+\bar{1})(x^4+x^3+x^2+x+\bar{1})(x^4+x+\bar{1})(x^4+x^3+\bar{1}).$$

□

Ex2.4 $d_1,d_2\mid n$, 证明 $E_{d_1}\cap E_{d_2}=E_{(d_1,d_2)}$

证明. 记 $d=(d_1,d_2)$, 则存在 a,b 使得 $d_1=ad,d_2=bd$, 存在 u,v 使得 $ud_1+vd_2=d$.

设 $e\in E_d$. 则 $\sigma^{d_1}(e)=(\sigma^d)^a(e)=e$, 从而 $e\in E_{d_1}$. 同理 $e\in E_{d_2}$, 因此 $E_{(d_1,d_2)}\subset E_{d_1}\cap E_{d_2}$.

设 $e\in E_{d_1}\cap E_{d_2}$.$\sigma^d(e)=\sigma^{ud_1+vd_2}(e)=e$. 因此 $E_{d_1}\cap E_{d_2}\in E_d$. □

8 第八周暨第八次前半部分

Ex1 设 $f(x), g(x) \in \mathbb{Z}[x]$ 本原, 若在 $\mathbb{Q}[x]$ 中 $f(x) \mid g(x)$, 则在 $\mathbb{Z}[x]$ 中 $f(x) \mid g(x)$.

证明. 设 $g(x) = f(x)h(x)$,$h(x) \in \mathbb{Q}[x]$, 则 $h(x) = ah'(x)$, 其中 $a \in \mathbb{Z}$,$h'(x) \in \mathbb{Z}[x]$ 是本原多项式, 而由 Gauss 引理,$h'(x)f(x) = \dfrac{g(x)}{a}$ 本原, 因此 $a = \pm 1$, 因此在 $\mathbb{Z}[x]$ 上,$f(x) \mid g(x)$. □

Ex2 $x^n - 1 = f(x) \cdot g(x) \cdot h(x) \in \mathbb{Q}[x]$, 可证 $h(x) \in \mathbb{Z}[x]$.

证明. 注意到 $x^n - 1$ 是本原多项式, 由上一题立得. □

Ex3 证明 $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + \bar{1})$ 中除了 $\bar{0}, \bar{1}, \bar{2}, u, \bar{2}u$ 外, 其他元素阶均为 8.

证明. 因为 $\mathbb{F}_9^*$ 是 8 阶循环群, 故有 $\varphi(9) = 4$ 个 8 阶元, 故其他元素阶均为 8. □

Ex4 构造一个八元域.

证明. 容易验证 $x^3 + x + 1$ 在 $\mathbb{F}_2$ 上不可约, 因此 $\mathbb{F}_2[x]/(x^3 + x + 1)$ 是一个八元域. □

Ex5 列出 $\mathbb{F}_2$ 上全部次数 $\leqslant 4$ 的不可约多项式.

证明.

-
  - $x, x+1$
  - $x^3 + x + 1, x^3 + x^2 + 1$
  - $x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1$
-
  - $x, x+1, x+2$
  - $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$

□

Ex6

(1) 由于 $f(x)$ 是 $\mathbb{F}_p[x]$ 中的首一不可约多项式,$\mathbb{F}_p[u] \cong \mathbb{F}_p[x]/(f(x))$ 是 $q = p^n$ 元域, 由 Frobenius 自同构

$$\sigma_p : \mathbb{F}_p[u] \to \mathbb{F}_p[u], a \mapsto a^p,$$

且 σ_p 的阶数为 n.

令 $f(x) = \sum_{i=0}^{n} a_i x^i$, 则 $\sum_{i=0}^{n} a_i u^i = 0$, 从而

$$\sum_{i=0}^{n} a_i(\sigma_\rho^j(u))^i = \sigma_p^j(\sum_{i=0}^{n} a_i u^i) = 0, \forall j > 0.$$

即 $\sigma_p^j(u) = u^{p^i}$ 是 $f(x)$ 的根, 而 σ_p 的阶为 n, 因此 $u, u^p, \cdots, u^{p^{n-1}}$ 是 $f(x)$ 两两不同的根.

(2) 由 (1) 知 $\sigma_p^i(u) \in \mathbb{F}_p^*[u]$ 是 $f(x)$ 的根, 由于 $\mathbb{F}_p^*[u]$ 是循环群,$\langle \sigma_p^*(u) \rangle$ 也是 $\mathbb{F}_p^*[u]$ 的生成元.

(3) 由 (2) 知, 一个本原多项式有 n 个 $\mathbb{F}_{p^n}$ 的乘法群的生成元, 由于 $\mathbb{F}_{p^n}^*$ 有 $\varphi(p^n - 1)$ 个生成元, 故 $\mathbb{F}_{p^n}^*$ 的本原多项式有 $\dfrac{\varphi(p^n - 1)}{n}$ 个.

9 期中考试

一. 考虑 Gauss 整数环 $R=\mathbb{Z}[\mathrm{i}]$ 以及 $K=\left\{a+b\mathrm{i}\middle|a,b\in\mathbb{Q}\right\}$. 设域扩张 E/K 使

(1) 证明：K 同构于 R 的分式域.

(2) 请列出 R 的所有子环, 说明哪些子环是唯一分解整环.

(3) 在 R 中, 计算最大公因子 $\gcd(4+7\mathrm{i},4-3\mathrm{i})$.

(4) 计算商环 $R/(4+7\mathrm{i},4-3\mathrm{i})$ 的阶数.

(5) 考虑商环 $S=R/(4-3\mathrm{i})$. 试给出 S 的所有理想, 并指出那些为素理想.

(6) 判断并论证：多项式 $x^4+x^3+x^2+x+1\in K[x]$ 是否可约.

(7) 计算维数 $\dim_{\mathbb{Q}}E=[E:\mathbb{Q}]$.

(8) 判断并论证：域自同构群 $\mathrm{Aut}(E)$ 是否为 Abel 群.

证明.

(1) 存在自然嵌入 $\varphi:R\hookrightarrow K$, 由分式线性变换的泛性质,$FracR\hookrightarrow K=\mathbb{Q}[i]$. 但 K 的子域只有 $\mathbb{Q}$ 和 $\mathbb{Q}[i]$, 容易验证 $i\in FracR$.

    也可以证明是满射.

(2) $S_n=\{a+bn\mathrm{i}\}$. 验证 S_n 和 S_m 是否同构?

    UFD 只有 $\mathbb{Z}$ 和 $\mathbb{Z}[\mathrm{i}]$.

    现在要说明 S_n 不是 UFD,$n\neq 0,1$.

    $(n\mathrm{i})(n\mathrm{i})=-n^2=-p_1^2\cdots p_k^2$

(3) $2+\mathrm{i}$. 取范?

(4) $R/(4+7\mathrm{i},4-3\mathrm{i})=R/(2+\mathrm{i})\cong\mathbb{F}_5$.

(5) 由对应定理,S 的理想一一对应于 R 中包含 $(4-3\mathrm{i})$ 的所有理想.

(6) 平移,$2+i$ 用 Eisenstein 判别法.

(7)

(8) i 是四次单位根,ξ_5 是五次单位根.$\mathrm{Aut}(E)\subset\mathrm{Aut}(\mathbb{Q}(\xi_{20}))$（事实上相等）. 其中 $\mathrm{Aut}(\mathbb{Q}(\xi_{20}))$ 是交换群！

□

二. 考虑八元域 $\mathbb{F}_8=\mathbb{F}_2[x]/(x^3+x+\bar{1})$. 记 $u=\bar{x}$. 于是

(1)

(2) $\mathbb{F}_8[x]$ 中共有多少个首一的二次不可约多项式?

(3) 将多项式 $x^3+x+\bar{1}$ 在 $\mathbb{F}_8$ 中进行不可约分解, 给出论证.

(4) 将多项式 $x^{16}+x$ 在 $\mathbb{F}_8[x]$ 中进行不可约分解, 给出论证.

(5) 计算 $(u^2+\bar{1})^{-1}$.

(6) 考虑商环 $R=\mathbb{F}_2[y]/(y^3+y^2+\bar{1})$. 请论证并具体构造环同构 $R\simeq\mathbb{F}_8$.

证明.

(1) 此题实际上是想让你证有限整环是域.$[\mathbb{F}_8,\mathbb{F}_2]=3$, 因子只有 $1,3$, 分别对应 $\mathbb{F}_2$ 和 $\mathbb{F}_8$.

(2) 二次多项式 x^2+ax+b 共有 64 个. 可约必形如 $(x-\alpha)(x-\beta)$, 共有 $C_8^2+8=36$ 个, 因此不可约的共有 $64-36=28$ 个.

另证：$x^{8^2}-x=\prod\limits_{d|2}\prod\limits_{d\text{次不可约}}f(x)$. 老师讲的时候是 $\mathbb{F}_p$ 上的. 事实上对 $\mathbb{F}_{p^n}$ 也正确.

(3) 已知 u 是 $x^3+x+\bar{1}$ 的根, 用 Frobenius 自同构得到 u^2 和 u^4 也是根!

(4)
- 硬算.$x^4+x^3+x^2+x+\bar{1}$ 在 $\mathbb{F}_8[x]$ 中不可约. 若它有根

(5)

(6) 关键引理

另证：$\mathbb{F}_2[y]\to\mathbb{F}_2[x]\to\mathbb{F}_8$.

□

三. 考虑一元有理函数域 $K=\mathbb{Q}(t).E=\mathbb{Q}(t^4)$ 为 K 中包含 t^4 的最小子域.

(1) 证明：域 E 同构于 K.

(2) 计算域扩张 K/E 的维数 $\dim_E K=[K:E]$.

(3) 计算域扩张 K/E 自同构群 $\mathrm{Aut}(K/E)$ 的阶数.

(4) 判断并论证：$\mathbb{Q}(t^2)$ 上的任何自同构是否均可延拓为 K 上的自同构?

证明.

(1) 分式域泛性质. 另证：单扩张的结构定理.

(2) 为什么 t^4 是素元? 因为 $\mathbb{Q}[t^4]/(t^4)\cong\mathbb{Q}$, 所以是极大理想, 所以是素元.

(3)

□

四. 设 R 为整环, 记 $R^\times=R\backslash\{0_R\}$. 试证明以下等价：

(1) 环 R 为主理想整环 PID.

(2) 存在映射 $\phi:R^\times\to\mathbb{N}$ 满足如下条件：对于任意 $a,b\in R^\times$, 要么 $b\mid a$, 要么存在适当的 $\delta,\gamma\in R$ 使得 $\phi(a\delta-b\gamma)<\phi(b)$.（注：两种情况可能同时发生.）

10 第十周暨第八次后半部分

Ex1.1 任意 $n, m \in \mathbb{Z}$,$a^{n+m} = a^n \cdot a^m$.

证明. 这就是第一周的练习, 不想再证了. □

Ex2.2 写出 $\Sigma(\square)$ 中的表示对称的元素.

解. $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$ □

P11.17 证明有理数加群 $\mathbb{Q}$ 和非零有理数乘法群 $\mathbb{Q}^*$ 不同构.

证明. 对任意元素 $a \in (\mathbb{Q}, +)$, 存在 b 使得 $b + b = a$;
但对任意元素 $a \in (\mathbb{Q}^\times, \times)$, 不一定存在 b 使得 $b \times b = a$. □

Ex2.1 若 $G = \bigsqcup_{i \in I} Ha_i$, 则 $G = \bigsqcup_{i \in I} a_i^{-1}H$.

证明. 只需证明 $a_i^{-1} \notin a_j^{-1}H$,$i \neq j$.
假设 $a_i^{-1} \in a_j^{-1}H$,$i \neq j$. 则存在 $h \in H$ 使得 $a_i^{-1} = a_j^{-1}h$, 从而 $a_j = ha_i$, 矛盾. □

Ex2.2 设 f 是群同态. 任意 $a \in G$,$f(a^{-1}) = f(a)^{-1}$.

证明. $f(a^{-1})f(a) = f(a^{-1}a) = f(1) = 1$. □

Ex2.3 设 f 是群同构, 则 f^{-1} 也是群同构.

证明. 任取 $a', b' \in G'$, 存在 a, b 使得 $f(a) = a'$,$f(b) = b'$.
$f^{-1}(a'b') = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(a)f^{-1}(b)$. □

Ex2.4 设 G 是群, 证明 $\sigma : G \to G, g \mapsto g^{-1}$ 是群同态当且仅当 G 是 Abel 群.

证明.

- 设 σ 是群同态. 则任取 $a, b \in G$,$ab = (a^{-1}b^{-1})^{-1} = ba$, 从而 G 是 Abel 群.
- 设 G 是 Abel 群, 则 $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

□

Ex2.5 在 $G \times H$ 中,

$$(g, h) = (1_G, h) \cdot (g, 1_H) = (g, 1_H) \cdot (1_G, h)$$

证明 $\operatorname{ord}((g, h)) = \operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h))$.

证明. 设 $d = \operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h))$, 则显然 $\operatorname{ord}((g, h)) \mid d$.
另一方面,$\operatorname{ord}(g) \mid \operatorname{ord}((g, h))$,$\operatorname{ord}(h) \mid \operatorname{ord}((g, h))$, 从而 $d \mid \operatorname{ord}((g, h))$. □

Ex2.6 证明 $V_4 \simeq U(\mathbb{Z}_8)$.

证明. $(1, 1) \mapsto \bar{1}, (-1, 1) \mapsto \bar{3}, (1, -1) \mapsto \bar{5}, (-1, -1) \mapsto \bar{7}$, 容易验证是同构. □

Ex2.7 证明 $\mathbb{C}^\times$ 不是循环群.

证明. $\mathbb{C}^\times$ 与 $\mathbb{Z}$ 之间不存在双射, 因此 $\mathbb{C}^\times$ 不可能是循环群. □

P17.5 设 A, B 是群 G 的两个子群. 试证：$AB \leqslant G$ 当且仅当 $AB = BA$.

证明.

- 设 $AB \leqslant G$.
  任取 $ab \in AB$, 则 $(ab)^{-1} \in AB$, 即存在 $a'b'$ 使得 $(ab)^{-1} = a'b'$, 则 $ab = b'^{-1}a'^{-1} \in BA$.
  任取 $ba \in BA$,$(ba)^{-1} = a^{-1}b^{-1} \in AB$, 所以 $ba \in AB$.
- 设 $AB = BA$.
  $a_1b_1, a_2b_2 \in AB.a_1b_1a_2b_2 = a_1a_2'b_1'b_2 \in AB$.
  $ab = b'a'$,$(ab)^{-1} = a'^{-1}b'^{-1} \in AB$.

□

P18.13 设 a, b 是群 G 的任意两个元素. 试证：a 和 a^{-1},ab 和 ba 有相同的阶.

证明.

- 设 a 的阶为 d_1,a^{-1} 的阶为 d_2.$1 = 1^{d_1} = (aa^{-1})^{d_1} = (a^{-1})^{d_1}$, 因此 $d_2 \mid d_1$, 同理 $d_1 \mid d_2$. 因此 $d_1 = d_2$.
- 设 ab 的阶为 d_1,ba 的阶为 d_2.$(ab)^{d_1} = 1$, 左乘 a^{-1}, 右乘 a, 得到 $(ba)^{d_1} = 1$, 从而 $d_2 \mid d_1$, 同理 $d_1 \mid d_2$. 因此 $d_1 = d_2$.

□

P20.3 试证：有理数加群 $\mathbb{Q}$ 不是循环群, 但它的任意有限生成的子群都是循环群.

证明.

- 任意有理数 a, 存在有理数 b 使得 $2b = a$. 若 a 是 $\mathbb{Q}$ 的生成元, 则 b 也是 $\mathbb{Q}$ 的生成元. 容易验证 $b \neq a$ 且 $b \neq -a$. 这与无限循环群的生成元只有 a 和 $-a$ 矛盾.
- 设 $\left\{\frac{p_1}{q_1}, \frac{p_2}{q_2}\right\}$ 是子群 H 的生成元集. 令 $d = \gcd(p_1q_2, p_2q_1)$, 则由 Bezout 等式,$\frac{d}{q_1q_2} \in H$. 且存在整数 m, n 使得 $\frac{p_1}{q_1} = m\frac{d}{q_1q_2}$,$\frac{p_2}{q_2} = n\frac{d}{q_1q_2}$. 即 $H = \left\langle \frac{d}{q_1q_2} \right\rangle$. 由归纳容易证明其余情况.

□

P20.10 设 p 是一个素数,G 是方程 $x^p = 1, x^{p^2} = 1, \cdots, x^{p^n} = 1, \cdots$ 的所有根在复数乘法下的群. 试证 G 的任意真子群都是有限阶的循环群.

证明. 记 G_n 是方程 $x^{p^n} = 1$ 的根在复数乘法下的群, 则容易看出 $G_1 \subset G_2 \subset \cdots \subset G_n \subset \cdots$, 且 $\{G_n\}$ 单调递增至 G. 任取 $g \in G$, 存在一个最小的 n 使得 g 在 G_n 中第一次出现, 容易看出 g 是 p^n 阶元, 是 G_n 的生成元. 同时考虑到递增包含关系, 可以断言对 G 的任意真子群 H, 存在最高阶元, 否则 $H = G$. 所以 H 就形如 G_n, 即是有限阶的循环群.

□

11 第十一周暨第九次

Ex1.1 $N \leqslant G$, 证明 $N \simeq aNa^{-1}$, 任意 $a \in G$.

证明. $\varphi : N \to aNa^{-1}, n \mapsto ana^{-1}$.

- 群同态.$\varphi(m)\varphi(n) = ama^{-1}ana^{-1} = amna^{-1} = \varphi(mn)$.
- 满射. 显然.
- 单射. 设 $\varphi(n) = 1$, 即 $ana^{-1} = 1$, 则 $n = 1$.

□

Ex1.2 $N \triangleleft G$, 群同态 $f : G \to H$,$N \subset \ker f$. 定义 $\tilde{f} : G/N \to H$,$\tilde{f}(aN) = f(a)$, 证明 $\tilde{f}$ 良定.

证明. 任意 $aN = bN$,$ab^{-1} \in N \subset \ker f$, 则 $f(ab^{-1}) = 1_H$, 则 $f(a) = f(b)$. □

P25.1 令 G 是实数对 (a, b),$a \neq 0$ 带有乘法

$$(a, b)(c, d) = (ac, ad + b)$$

的群. 试证：$K = \big\{(1, b)\big|b \in \mathbb{R}\big\}$ 是 G 的正规子群且 $G/K \cong \mathbb{R}^*$.

证明.

- 验证 G 是群.
  - 结合律.
    $((a, b)(c, d))\,(e, f) = (ac, ad + b)(e, f) = (ace, acf + ad + b)$
    $(a, b)\,((c, d)(e, f)) = (a, b)(ce, cf + d) = (ace, acf + ad + b)$
  - 幺元. $(1, 0)(a, b) = (a, b), (a, b)(1, 0) = (a, b)$.
  - 可逆. $(a, b)(\dfrac{1}{a}, -\dfrac{b}{a}) = (1, 0), (\dfrac{1}{a}, -\dfrac{b}{a})(a, b) = (1, 0)$.
- 考虑映射 $\varphi : G \to \mathbb{R}^*, (a, b) \mapsto a$. 容易验证 φ 是群同态,$\ker \varphi = K$.

  从而 K 是正规子群,$G/K \cong \mathbb{R}^*$.

□

P25.4 试证群 G 的指数为 2 的子群一定是 G 的正规子群.

证明. 设 $H \leqslant G$ 且 $[G : H] = 2$, 那么存在 $a \in G$ 使得 $G = H \sqcup aH$.
要证 $H \triangleleft G$, 只需证对任意 $b \in G$,$bH = Hb$.

- 当 $b \in H$, 显然有 $bH = H = Hb$.
- 当 $b \notin H$, 只能有 $bH = aH = Hb$.

因此 $H \triangleleft G$. □

P25.6 设 $f : G \to H$ 是群同态,$M \leqslant G$. 试证 $f^{-1}(f(M)) = KM$, 这里 $K = \ker f$.

证明.

- $KM \subset f^{-1}(f(M))$. 任取 $km \in KM$,$f(km) = f(k)f(m) = f(m) \in f(M)$.
- $f^{-1}(f(M)) \subset KM$. 任取 $a \in f^{-1}(f(M))$, 存在 $m \in M$ 使得 $f(a) = f(m)$, 则 $am^{-1} \in K$, 存在 k 使得 $a = km$.

□

P25.7 设 M 和 N 分别是群 G 的正规子群. 如果 $M \cap N = \{1\}$, 则对任意 $a \in M$,$b \in N$,$ab = ba$.

证明. 因为 $N \lhd G$, 所以对任意的 $a \in M$,$aN = Na$. 任取 $b \in N$,$ab \in Na$, 存在 $c \in N$ 使得 $ab = ca$. 若 $c = b$, 命题得证. 若 $c \neq b$, 固定住选出的 a, b, c. 因为 $M \lhd G$, 所以对上面选出的 $b \in N$ 有 $bM = Mb$. 因此 $ab \in bM$, 存在 $d \in M$ 使得 $ab = bd$, 从而 $ca = bd$, 其中 $c \neq b$. 移项得 $b^{-1}c = da^{-1}$, 其中 $b^{-1}c \in N$,$da^{-1} \in M$. 因为 $c \neq b$, 所以 $b^{-1}c \neq 1$. 这与 $M \cap N = \{1\}$ 矛盾！ □

P25.8 设 $f : G \to H$ 是群同态. 如果 g 是 G 的一个有限阶元素, 则 $f(g)$ 的阶整除 g 的阶.

证明. 设 $g \in G$ 的阶为 d, 则 $g^d = 1$, 则 $f(g)^d = f(g^d) = 1$, 从而 $f(g)$ 的阶整除 g 的阶. □

P25.10 如果 $G/C(G)$ 是循环群, 则 G 是 Abel 群.

证明. 观察到, 若 G 是 Abel 群, 则 $C(G) = G$. 这提供了更强的信息, 让我们知道如何导出矛盾！

记 $N = C(G)$. 设 aN 是 G/N 的生成元, 不妨设 $aN \neq N$, 否则 G 已经是 Abel 群.

因为 $a \notin N$, 所以存在 $b \in G$ 使得 $ab \neq ba$. 考虑 bN, 因为 G/N 是循环群, 所以存在 m 使得 $bN = a^mN$. 因此存在 $c \in N$ 使得 $b = a^mc$. 但此时 $ab = aa^mc = a^{m+1}c = a^mca = ba$, 矛盾！ □

Ex2.1 对应定理

证明. 有自然同态

$$\varphi : G \twoheadrightarrow G/N,$$

则我们有 $f_1(K) = \varphi(K), f_2(K') = \varphi^{-1}(K')$. □

Ex2.2 若 $K/N \lhd G/N$, 则 $K \lhd G$.

证明. 由上一题, 我们有子群间的一一对应, 若 $K/N \lhd G/N$, 则 $f_1(K) = gf_1(K)g^{-1} = f_1(gKg^{-1})$, 因此 $K = gKg^{-1}$, 故 $K \lhd G$. □

P30.2 讨论置换

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$$

的奇偶性.

证明.

(1) 设 $n = 2k+1$, 则 $\sigma = (1n)(2, n-1)\cdots(k-1, k+1)$

- 设 $k = 2l$, 则为奇置换, 此时 $n = 4k+1$
- 设 $k = 2l+1$, 则为偶置换, 此时 $n = 4l+3$

(2) 设 $n = 2k$, 则 $\sigma = (1n)(2, n-1)\cdots(k, k+1)$

- 设 $k = 2l$, 则为偶置换, 此时 $n = 4k$
- 设 $k = 2l+1$, 则为奇置换, 此时 $n = 4l+2$

□

P30.5 试证一个置换的阶等于它的轮换表示中各个轮换的长度的最小公倍数.

证明. 设置换 σ 的阶为 d, 设它的轮换表示 $\sigma_1\cdots\sigma_n$ 中各个轮换的长度的最小公倍数为 d'.

已知轮换的长度就是轮换的阶数.

- $\sigma^{d'} = \sigma_1^{d'}\cdots\sigma_n^{d'} = 1.$

  上面可以交换是因为轮换表示两两不交. 因此 $d \mid d'$.

- $\sigma_1^d\cdots\sigma_n^d = \sigma^d = 1$. 假设 $\sigma_i^d \neq 1$, 则其余部分是它的逆, 但轮换表示两两不交, 这不可能. 因此 $\sigma_i^d = 1$. 从而 $d' \mid d$.

□

P30.6 试确定 S_4 的全部正规子群.

解.

- S_4 的共轭类如下：
  - 1^4,Id
  - $1^2 2^1$,$(12), (13), (14), (23), (24), (34)$
  - $1^1 3^1$,$(123), (124), (132), (134), (142), (143), (234), (243)$
  - 2^2,$(12)(34), (13)(24), (14)(23)$.
  - 4^1,$(1234), (1243), (1324), (1342), (1423), (1432)$.
- S_4 按共轭类可分为 $24 = 1+6+8+3+6$ 共 5 类.
- 由于全体对换生成 S_n, 所以欲找非平凡正规子群, 不可包含对换.
- 已经知道 $A_4 \lhd S_4$, 它是所有偶置换, 即恒等、两个对换和三轮换.
- 由 Lagrange 定理,S_4 的非平凡正规子群的阶数只能为 $12, 8, 6, 4, 3, 2$.
- 容易看出不存在其他 12 阶子群, 不存在 $8, 6, 3, 2$ 阶子群
- $K_4 \lhd S_4$, 它是所有的两个对换.
- 还有平凡正规子群 $\{\mathrm{Id}\}$ 和 S_4 本身.

□

P30.7 试证 A_4 没有 6 阶子群.

证明. 若 A_4 有 6 阶子群 H, 则 $[A_4 : H] = 2$, 从而 H 是 A_4 的正规子群, 但计算知 A_4 的共轭类有

- $[1^4]$ 型：1 个
- $[2^2]$ 型：3 个
- $[1^1 3^1]$ 型的一部分：4 个
- $[1^1 3^1]$ 型的另一部分：4 个

因此没有 6 阶正规子群. □

P30.8 试证：当 $n \geqslant 3$ 时,$C(S_n) = \{1\}$.

证明. 已知 $C(S_n) \lhd S_n$.

- 当 $n = 3$ 时,S_3 的正规子群只有 $\{1\}, A_3, S_3$.

  若 $C(S_3) = A_3$ 或 S_3, 则 $S_3/C(S_3)$ 为循环群, 则 S_3 为 Abel 群, 矛盾!

- 当 $n = 4$ 时,S_4 的正规子群只有 $\{1\}, K_4, A_4, S_4$, 同理可知 $C(S_4)$ 不为 A_4 或 S_4.

  由于

  $$(13)(12)(34)(13) = (14)(23) \neq (12)(34),$$

  所以 $C(S_4) \neq K_4$.

- 当 $n = 5$ 时,S_5 的正规子群只有 $\{1\}, A_n, S_n$, 同前可证.

□

12 第十二周暨第十次

Ex1.1

(1) 证 H 恰由 $(1234),(13)$ 生成.

证明. 由 $|\langle(1234)\rangle| = 4$ 且 $(13) \notin \langle(1234)\rangle$ 知 $|\langle(1234),(13)|\rangle| > 4$, 由 Lagrange 定理知 $|\langle(1234),(13)|\rangle| \mid |H| = 8$, 所以 $|\langle(1234),(13)|\rangle| = 8$, 因此 $\langle(1234),(13)|\rangle = H$. □

(2) $\langle(1324),(12)\rangle$

(3) $\langle(1243),(14)\rangle$

Ex1.2 求所有 $\sigma \in S_3$, 使得 $(12) = \sigma(13)\sigma^{-1}$.

证明. $(12) = \sigma(13)\sigma^{-1} = (\sigma(1)\sigma(3))$, 故 $\sigma = (23)$ 或 (123). □

Ex1.3 若 G 是 Abel 群, 则 G 是单群 $\Longleftrightarrow G$ 是 p 阶循环群, 其中 p 素.

证明.

- $\Longleftarrow$ 显然.
- $\Longrightarrow$ GAbel 群 $\Longrightarrow$ 任意 $N \leqslant G$ 都是正规子群, 由于 G 是单群, 所以 G 的子群只有平凡子群, 取 $1 \neq a \in G$, 则 $\langle a\rangle \leqslant G$, 从而 $\langle a\rangle = G$.

  若 $|a| = \infty$, 则 $a \notin \langle a^2\rangle$, 则 $\langle a^2\rangle \subsetneq \langle a\rangle$,$\langle a^2\rangle = \{1\}$, 矛盾.

□

P29.3 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $\dfrac{n!}{\prod_{i=1}^{n}\lambda_i!i^{\lambda_i}}$ 个, 由此证明

$$\sum_{\substack{\lambda_i \geqslant 0 \\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}} \frac{1}{\prod_{i=1}^{n}\lambda_i!i^{\lambda_i}} = 1$$

证明. 对任意 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 型置换 σ 均可写成以下形式

$$\sigma = \underbrace{(a_1)\cdots(a_n)}_{\lambda_1}\underbrace{(a_{\lambda_1+1}a_{\lambda_1+2})\cdots(a_{\lambda_1+2\lambda_2-1}a_{\lambda_1+2\lambda_2})}_{\lambda_2}\cdots$$

其中若 $i \neq j$, 则 $a_i \neq a_j$,$a_i \in \{1,\cdots,n\}$, 若 $\lambda_i = 0$, 则不存在 i 轮换.$a_1,\cdots,a_n$ 的可能取值有 $n!$ 种, 由于在 λ_i 个 i 轮换中, 它们的次序改变不影响 σ, 且每个 i 轮换中,$(b_1b_2\cdots b_i) = (b_2b_2\cdots b_ib_1) = \cdots = (b_ib_1\cdots b_{i-1})$, 故 σ 的个数只有 $\dfrac{n!}{\prod_{i=1}^{n}a_i!i^{\lambda^i}}$ 个, 由于不同型的元素不在同一等价类, 因此

$$\sum_{\substack{\lambda_i \geqslant 0 \\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}} \frac{n!}{\prod_{i=1}^{n}\lambda_i!i^{\lambda_i}} = n!,$$

从而

$$\sum_{\substack{\lambda_i \geqslant 0 \\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}} \frac{1}{\prod_{i=1}^{n}\lambda_i!i^{\lambda_i}} = 1.$$

□

Ex2.1 求所有 $\sigma \in A_3$ 使得 $\sigma(123)\sigma^{-1}(132)$.

证明. $\sigma(123)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)) = (132)$, 得 $\sigma = (23),(13),(12)$, 故不存在 $\sigma \in A_3$ 满足条件. □

Ex2.2 验证 ρ 是群同态.

证明. 任意 $g,h \in G$, 任意 $x \in X$

$$\rho(gh)(x) = (gh)\cdot x = g(h\cdots x) = \rho(g)(\rho(h)(x))$$

故 $\rho(gh) = \rho(g)\rho(h)$, 即 $\rho : G \to S(X)$ 是群同态. □

Ex2.3 G 是群, 验证反群 $G^{op} = G$,$x * y = yx$ 是群, 且 G 与 G^{op} 同构.

证明. (1) $1_{G^{op}} = 1_G$

(2) 任意 $x \in G^{op}$,x^{-1} 即为 x 在 G^{op} 中的逆

(3) 任意 $x,y,z \in G^{op}$,

$$x*(y*z) = (zy)x = z(yx) = (x*y)*z.$$

(4) 构造

$$\varphi : G \to G^{op}, x \mapsto x^{-1},$$

易验证任意 $x,y \in G$,

$$\varphi(xy) = \varphi(x) * \varphi(y).$$

□

Ex2.4 $H \leqslant G$,$H\backslash G = \{Ha \big| a \in G\}$, 构造 $(H\backslash G) \curvearrowleft G$.

证明. 构造

$$H\backslash G \times G \to H\backslash G, (Ha,g) \mapsto Hag.$$

□

Ex2.5 验证是单射.

证明. 由 $\mathrm{Aut}(E/k) \curvearrowright Root_E(f)$ 知 θ 是同态, 任意 $\sigma \in \ker\theta$,$\sigma\big|_k = \mathrm{Id}$,$\sigma\big|_{\{u_1,\cdots,u_n\}} = \mathrm{Id}$, 由关键引理,$\sigma$ 由 $\{u_1,\cdots,u_n\}$ 唯一决定, 故 $\sigma = \mathrm{Id}_E$, 因此 $\ker\theta = \{\mathrm{Id}\}$, 因此 θ 是单射. □

Ex2.6 写出来!

证明. 记 $x_1 = (1,0)^T, x_2 = (0,1)^T, x_3 = (1,1)^T$, 构造

$$\phi : \mathrm{GL}_2(\mathbb{F}_2) \times X \longrightarrow X$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

则 ϕ 是群作用.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x_1 = \begin{pmatrix} a \\ c \end{pmatrix} = \begin{cases} x_1 & a=1, c=0 \\ x_2 & a=0, c=1 \\ x_3 & a=1, c=1 \end{cases}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x_2 = \begin{pmatrix} b \\ d \end{pmatrix} = \begin{cases} x_1 & b=1, d=0 \\ x_2 & b=0, d=1 \\ x_3 & b=1, d=1 \end{cases}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x_3 = \begin{pmatrix} a+b \\ c+d \end{pmatrix} = \begin{cases} x_1 & a+b=1, c+d=0 \\ x_2 & a+b=0, c+d=1 \\ x_3 & a+b=1, c+d=1 \end{cases}$$

这诱导了群同态 $\psi : \mathrm{GL}_2(\mathbb{F}_2) \to S_3$, 其中

$$\psi \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} = (12), \quad \psi \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{pmatrix} = (13),$$

故 $\operatorname{Im} \psi \supset \langle (12), (13) \rangle = S_3$, 从而 ψ 是满射, 而 $|S_3| = 6 = |\operatorname{GL}_2(\mathbb{F}_2)|$, 从而 ψ 是单射. □

Ex2.7 构造群满同态 $S_4 \twoheadrightarrow S_3$.

证明. 考虑 S_4 在其子集 $[2^2]$ 上的共轭作用,

$$\phi : S_4 \times [2^2] \to [2^2], (\tau, \sigma) \mapsto \tau\sigma\tau^{-1}$$

由于 $[2^2]$ 是 S_4 的一个共轭元素类, 所以 ϕ 是良好定义的, 因此诱导了一个群同态

$$\psi : S_4 \to S_3.$$

记 $x_1 = (23)(14), x_2 = (13)(24), x_3(12)(34)$, 则 $\psi((12)) = (12)$, 同理 $\psi((13)) = (13)$, 从而 $\operatorname{Im} \psi \supset \langle (12), (13) \rangle = S_3$, 从而 $\operatorname{Im} \psi = S_3$. □

Ex2.8check 左作用!

证明. 定义 $\phi : G \times G \to G, (g, h) \mapsto g \cdot h = ghg^{-1}$, 容易验证

(1) $(gg') \cdot h = gg'hg'^{-1}g^{-1} = g \cdot (g' \cdot h), \forall g, g, h \in G$

(2) $1 \cdot h = h$,$h \in G$.

□

13 第十三周暨第十一次

Ex1.1 $\Sigma(\square)=\left\{1,\tau,\tau^2,\tau^3,\sigma,\tau\sigma,\tau^2\sigma,\tau^3\sigma\right\}$, 验证

$$\mathcal{Z}(\Sigma(\square))=\left\{\mathrm{Id},\tau^2\right\}.$$

证明. 由于任意 $\tau^i\sigma^j,\tau^k\sigma^l\in\Sigma(\square)$, 其中 $i,k=0,1,2,3,j,l=0,1$, 有

$$\tau^i\sigma^j(\tau^k\sigma^l)(\tau^i\sigma^j)^{-1}=\tau^i\tau^{(-1)^jk}\tau^{-(-1)^li\sigma^j}$$

(1) 当 $k=0,2$ 时, 上式为 $\tau^{i+k-(-1)^li}\sigma^l$, 则 $\tau^k\sigma^l\in\mathcal{Z}(\Sigma(\square))$ 当且仅当 $l=0$, 此时 $\tau^k\sigma^l=\mathrm{Id}$ 或 τ^2.

(2) 当 $k=1,3$ 时, 上式为 $\tau^{i-k-(-1)^li}\sigma^l\neq\tau^k\sigma^l$, 否则,$2k\equiv i-(-1)^li \mod 4$, 所以 $l=1$, 从而 $2k\equiv 2i \mod 4$, 矛盾.

因此,$\mathcal{Z}(\Sigma(\square))=\left\{\mathrm{Id},\tau^2\right\}$. □

Ex1.2 设 $|G|=p^2$,$g\in\mathcal{Z}(G)$, 且 $\operatorname{ord}g=p$. 记 $H=\langle g\rangle$, 设 $g'\in G\backslash H$, 记 $K=\langle g'\rangle$, 验证

$$\begin{aligned}\phi:H\times K&\longrightarrow G\\(g^i,g'^j)&\longmapsto g^ig'^j\end{aligned}$$

是同态.

证明.

$$\phi((g^{i_1},g'^{j_1})\cdot(g^{i_2},g'^{j_2}))=\phi((g^{i_1+i_2},g'^{j_1+j_2}))=g^{i_1+i_2}g'^{j_1+j_2}=g^{i_1}g'^{j_1}g^{i_2}g'^{j_2}=\phi((g^{i_1},g'^{j_1}))\phi((g^{i_2},g'^{j_2})).$$

□

P34.1 设 G 作用在集合 Σ 上, 对任意 $a,b\in\Sigma$, 若存在 $g\in G$ 使得 $ga=b$, 则 $G_a=g^{-1}G_bg$. 换句话说, 同一轨道中元素的固定子群彼此共轭.

证明. 设 $\sigma\in G_b$, 则 $g^{-1}\sigma ga=g^{-1}\sigma b=g^{-1}b=a$. 即 $g^{-1}G_bg\subset G_a$, 反之亦然. □

P34.3 设群 G 在集合 Σ 上的作用是传递的,N 是 G 的正规子群, 则 Σ 在 N 作用下的每个轨道由同样多的元素.

证明. 任取 $a,b\in\Sigma$, 由于 G 在 Σ 上的作用是可迁的, 所以存在 $g\in G$ 使得 $b=ga$. 由上一题知 $G_a=g^{-1}G_bg$. 故

$$N_a=N\cap G_a=N\cap g^{-1}G_bg=g^{-1}Ng\cap g^{-1}G_bg=g^{-1}N_bg,$$

即 a 与 b 在 N 下的稳定化子互相共轭, 由轨道稳定化子公式知 $|O_a|=|O_b|$. □

P34.12 设 p 是 $|G|$ 的最小素因子. 若 p 阶子群 $A\triangleleft G$, 则 $A\leqslant C(G)$.

证明. 不太会, 要再想想. □

Ex2.1 $\langle K_4,(13)\rangle,\langle K_4,(12)\rangle,\langle K_4,(14)\rangle$ 两两不同.

证明. 若 $\langle K_4,(13)\rangle = \langle K_4,(12)\rangle$, 则 $(12)(13)=(132)\in\langle K_4,(13)\rangle$, 从而 $\mathrm{ord}(132)\mid 8$, 但 $\mathrm{ord}(132)=3$, 矛盾. 其他同理可得. □

Ex2.2 分析 S_3 的情况

证明. $|S_3|=6=2\times 3$.

- Sylow2-子群. 设 Sylow2-子群的个数为 r, 则 r 形如 $2k+1$ 且 $r\mid 3$, 则 $r=1$ 或 3. 若 $r=1$ 则该子群为正规子群, 矛盾. 因此 S_3 的 Sylow2-子群有三个, 正是 S_3 的三个二阶子群 $\langle(12)\rangle,\langle(13)\rangle,\langle(23)\rangle$.
- Sylow3-子群. 设 Sylow3-子群的个数为 r, 则 r 形如 $3k+1$ 且 $r\mid 2$, 所以 $r=1$. 因此 S_3 的 Sylow3-子群只有 A_3.

□

Ex2.3 设 G 是 Abel 群,$|G|=p_1^{s_1}\cdots p_r^{s_r}$ 是素因子分解, 则:

(1) 存在唯一的 $P_i\leqslant G$, 使得 $|P_i|=p_i^{r_i}$.

(2) 存在同构

$$\begin{aligned}\varphi: P_1\times\cdots\times P_r &\longrightarrow G\\ (h_1,\cdots,h_r)&\longmapsto h_1\cdots h_r.\end{aligned}$$

证明.

(1) Sylow 定理断言了 P_i 的存在性, 因为 Abel 群的所有子群都是正规子群, 所以唯一.

(2) - φ 是同态.

$$\begin{aligned}\varphi((h_1,\cdots,h_r)\cdot(l_1,\cdots,l_r)) &= \varphi((h_1l_1,\cdots,h_rl_r))\\ &= h_1l_1\cdots h_rl_r\\ &= h_1\cdots h_rl_1\cdots l_r\\ &= \varphi(h_1,\cdots,h_r)\varphi(l_1,\cdots,l_r).\end{aligned}$$

- 设 $H=\varphi(P_1\times\cdots\times P_r)$, 则 $p_i^{r_i}\mid H$, 所以 $H=G$.

□

Ex2.4 已知: 设 $H\leqslant A$,$P\leqslant A$ 是 Sylowp-子群,$|A|=p^s\cdot m$,$(p,m)=1$, 则存在 $g\in A$, 使得 $gPg^{-1}\cap H$ 是 H 的 Sylowp-子群. 运用以上事实, 证明:

(2) A 的 Sylowp-子群彼此共轭.

(4) 设 P 是 A 的一个 Sylowp-子群, 则 A 的 Sylowp-子群的个数为 $[A:N_A(P)]$.

证明.

(2) 设 P 和 P' 是任意给定的 A 的 Sylowp-子群, 则由事实知, 存在 $g \in A$, 使得 $gPg^{-1} \cap P'$ 是 P' 的 Sylowp-子群. 而 P' 的 Sylowp-子群唯一且是自身, 因此 $gPg^{-1} \cap P' = P'$, 故 $gPg^{-1} \supset P'$, 同理存在 $h \in G$ 使得 $hP'h^{-1} \supset P$, 故

$$hgPg^{-1}h^{-1} \supset hP'h^{-1} \supset P,$$

从而

$$|P| = |hgPg^{-1}h^{-1}| \geqslant |hP'h^{-1}| \geqslant |P|,$$

因此 $P = hP'h^{-1}$, 即 P 与 P' 共轭.

(4) 不太清楚 (4) 在说什么, 需要再想一下.

□

P40.2 设 G 是一个 n 阶群,p 是 n 的素因子. 试证：方程 $x^p = 1$ 在群 G 中解的个数是 p 的倍数.

证明. 考虑 $S = \{(e_1, \cdots, e_p) \big| e_1 \cdot e_2 \cdots e_p = 1, e_i \in G\}$. 则 $|S| = n^{p-1}$.

群 $\mathbb{Z}_p$ 作用在集合 S 上, 它的不动点集 $|S_0|$ 正是 $x^p = 1$ 的解, 从而

$$|S| \equiv |S_0| \equiv 0 \mod p.$$

□

P40.4 试证 200 阶群 G 一定含有一个正规的西罗子群.

证明. 其 Sylow-5 子群的个数形如 $5k+1$ 且整除 2, 因此只能有 1 个 Sylow-5 子群, 因此它正规. □

P40.7 设 N 是有限群 G 的一个正规子群. 如果 p 和 $|G/N|$ 互素, 则 N 包含 G 的所有西罗 p-子群.

证明. 对任意 G 的 Sylowp-子群 P, 存在 $g \in G$, 使得 $gPg^{-1} \cap N$ 是 N 的 Sylowp-子群, 而 $(P, |G/N|) = 1$, 所以 $gPg^{-1} \cap N = gPg^{-1}$, 从而 $gPg^{-1} \subset N$, 从而 $P \subset g^{-1}Ng = N$. 因此 N 包含 G 的所有 Sylowp-子群. □

P40.8 设 G 是任意一个有限群,N 是 G 的正规子群,P 是 G 的一个 Sylowp-子群. 试证：

(1) $N \cap P$ 是 N 的 Sylowp-子群；

(2) PN/N 是 G/N 的 Sylowp-子群；

(3) $N_G(P)N/N \cong N_{G/N}(PN/N)$.

证明.

(1) 存在 $g \in G$, 使得 $N \cap gPg^{-1}$ 是 N 的 Sylowp-子群. 因此

$$N \cap P = g^{-1}(N \cap gPg^{-1})g$$

是 N 的 Sylowp-子群.

(2) $|PN/N| = |P/(P \cap N)| = \dfrac{|P|}{|P \cap N|}$. 设 $|G| = p^r m$, 其中 $(p, m) = 1$, 则 $|P| = p^r$, 设 $|N| = p^k n$, 其中 $(p, n) = 1$, 则 $|P \cap N| = p^k$,$|G/N| = p^{r-k}\dfrac{m}{n}$, 从而 $|PN/N| = p^{r-k}$, 进而 PN/N 是 G/N 的 Sylowp-子群.

(3) 想不清楚这是在说什么.

□

P40.13 设 P 是 G 的 Sylowp-子群, 且 $N_G(P)$ 是 G 的正规子群. 试证 P 是 G 的正规子群.

证明. 由于 $P \subset N_G(P)$,$|G/N_G(P)|$ 与 P 互素, 故 N_G 包含所有的 Sylowp-子群, 而 $P \triangleleft N_G(P)$, 故 Sylowp-子群只有一个, 从而 $P \triangleleft G$. □

Ex2.5 既约字唯一

证明. 设由非空集合 X 形成的所有既约字组成的集合是 Ω, 任意 $x \in X$, 定义

$$\sigma_x : \Omega \to \Omega, \omega \mapsto \overline{x\omega}, \forall \omega \in \Omega,$$

因为 ω 是既约字, 因此 σ_x 是 Ω 到自身的双射, 从而 σ_x 是一个置换. 对于任意一个字

$$u = x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t}$$

规定

$$\sigma_u := \sigma_{x_1}^{n_1} \sigma_{x_2}^{n_2} \cdots \sigma_{x_l}^{n_l}.$$

令

$$H = \left\{ \sigma_\omega \middle| \omega \in \Omega \right\},$$

则 H 对于置换的乘法成为一个群, 并且如果一个字化简成既约字 ω, 则 $\sigma_u = \sigma_\omega$.

设同一个字 u 用两种不同的方式化简成既约字 ω_1, ω_2, 则据上述,$\sigma_{\omega_1} = \sigma_u = \sigma_{\omega_2}$. 由于 σ_{ω_1} 把空字映成 ω_1,σ_{ω_2} 把空字映成 ω_2, 所以 $\omega_1 = \omega_2$. □

14 第十四周暨第十二次

Ex1.1 证明：

$$N(r_1,\cdots,r_m)=\left\langle\left\{\omega r_i\omega^{-1}\middle|1\leqslant i\leqslant m,\omega\in F(x_1,\cdots,x_n)\right\}\right\rangle.$$

证明. 记 $N=N(r_1,\cdots,r_m)$,$N'=\left\langle\left\{\omega r_i\omega^{-1}\middle|1\leqslant i\leqslant m,\omega\in F(x_1,\cdots,x_n)\right\}\right\rangle$.

- 因为 $N\lhd F(x_1,\cdots,x_n)$, 所以对任意的 $\omega\in F(x_1,\cdots,x_n)$, 有 $\omega r_i\omega^{-1}\in N$. 所以 $N'\subset N$.
- 要证 $N\subset N'$, 因为 N 按定义是包含 $r_1,\cdots,r_m$ 的最小的正规子群,N' 显然包含 $r_1,\cdots,r_m$, 因此只需证 N' 是正规子群, 即证 N' 对共轭封闭.

  任取 $y\in N'$, 任取 $v\in F(x_1,\cdots,x_n)$. 注意到 y 形如 $\omega_1 r_{i_1}\omega_1^{-1}\omega_2 r_{i_2}\omega_2^{-1}\cdots\omega_l r_{i_l}\omega_l^{-1}$, 则

  $$v\omega_1 r_{i_1}\omega_1^{-1}\omega_2 r_{i_2}\omega_2^{-1}\cdots\omega_l r_{i_l}\omega_l^{-1}v^{-1}=(v\omega_1)r_{i_1}(v\omega_1)^{-1}(v\omega_2)r_{i_2}(v\omega_2)^{-1}\cdots(v\omega_l)r_{i_l}(v\omega_l)^{-1}\in N'.$$

□

Ex1.2 证明：在 $F(a,b)$ 中,

$$N(a^2,b^2,(ab)^3)=N(a^2,b^2,abab^{-1}a^{-1}b^{-1}).$$

证明. 记 $N=N(a^2,b^2,(ab)^3)$,$N'=N(a^2,b^2,abab^{-1}a^{-1}b^{-1})$.

- 由于 $N'\lhd F(a,b)$,

  $$b(abab^{-1}a^{-1}b^{-1}\cdots b^2)b^{-1}=babab^{-1}a^{-1}\in N'.$$

  重复这个步骤, 得 $(ba)^3\in N'$. 因此

  $$(ab)^3=a(ba)^3a^{-1}\in N',$$

  从而 $N\subset N'$.
- 类似可证 $N'\subset N$.

□

P44.2 如果 n 为正奇数, 求证 $D_{2n}\cong D_n\times Z_2$.

证明. $D_n=\left\langle a,b\middle|a^n=b^2=(ab)^2=1\right\rangle$,$\mathbb{Z}_2=\left\langle c\middle|c^2=1\right\rangle$, 我们有自然的满同态

$$\pi:F(x,y)\to D_n\times\mathbb{Z}_2,$$

其中 $\pi(x)=(a,c)$,$\pi(y)=(b,c)$.

显然 $N(x^n,y^2,(xy)^2)\subset\ker\pi$.

因此诱导了满同态

$$\tilde{\pi}:D_{2n}\to D_n\times\mathbb{Z}_2.$$

而 $|D_{2n}|=|D_n\times\mathbb{Z}_2|=4n$, 因此 $\tilde{\pi}$ 是单射, 从而 $D_{2n}\cong D_n\times\mathbb{Z}^2$. □

P44.3 若 $n\geqslant 3$, 试问 $A_n\times\mathbb{Z}_2$ 与 S_n 是否同构》

证明. $C(A_n \times \mathbb{Z}_2) = C(A_n) \times C(\mathbb{Z}_2) \supset \mathbb{Z}_2$.

但 $C(S_n) = \{1\}$, 故 $S_n \not\cong A_n \times \mathbb{Z}_2$. □

P44.4 设 G_1, G_2, G_3 为群, 则

(1) $G_1 \times G_2 \cong G_2 \times G_1$

(2) $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$.

证明.

(1) $(g_1, g_2) \longleftrightarrow (g_2, g_1)$.

(2) $((g_1, g_2), g_3) \longleftrightarrow (g_1, (g_2, g_3))$.

□

P44.5 设 G_i 为群, 则

(1) $C(G_1 \times G_2 \times \cdots \times G_n) = C(G_1) \times C(G_2) \times \cdots \times C(G_n)$.

(2) $G_1 \times G_2 \times \cdots \times G_n$ 为 Abel 群当且仅当 G_i 为 Abel 群.

证明.

(1) $(g_1, \cdots, g_n) \in C(G_1 \times \cdots \times G_n)$

$\Longleftrightarrow (g_1, \cdots, g_n)(h_1, \cdots, h_n) = (h_1, \cdots, h_n)(g_1, \cdots, g_n), \forall (h_1, \cdots, h_n) \in G_1 \times \cdots \times G_n$

$\Longleftrightarrow g_i h_i = h_i g_i$

$\Longleftrightarrow g_i \in C(G_i)$.

(2) $G_1 \times \cdots \times G_n$ 为 Abel 群

$\Longleftrightarrow C(G_1 \times \cdots \times G_n) = \{1\}$

$\Longleftrightarrow C(G_i) = \{1\}$

$\Longleftrightarrow G_i$ 为 Abel 群.

□

P44.6 设 G_i 为群,$N_i \leqslant G_i$, 则

(1) $N_1 \times \cdots \times N_n \leqslant G_1 \times \cdots G_n$

(2) $N_1 \times \cdots \times N_n \triangleleft G_1 \times \cdots G_n \Longleftrightarrow N_i \leqslant G_i$

(3) 当 $N_1 \times \cdots \times N_n \triangleleft G_1 \times \cdots G_n$ 时,

$$G_1 \times \cdots \times G_n / N_1 \times \cdots \times N_n \cong G_1/N_1 \times \cdots G_n/N_n.$$

证明.

(1) 对任意 $(x_1, \cdots, x_n), (y_1, \cdots, y_n) \in N_1 \times \cdots \times N_n$,

$$(x_1, \cdots, x_n)(y_1, \cdots, y_n)^{-1} = (x_1 y_1^{-1}, \cdots, x_n y_n^{-1}) \in N_1 \times \cdots \times N_n.$$

(2) 任意 $(x_1,\cdots,x_n)\in G_1\times\cdots\times G_n$,

$$(x_1,\cdots,x_n)(N_1\times\cdots\times N_n)(x_1,\cdots,x_n)^{-1}=x_1N_1x_1^{-1}\times\cdots\times x_nN_nx_n^{-1}=N_1\times\cdots N_n$$

$\Longleftrightarrow x_iN_ix_i^{-1}=N_i$, 即 $N_i\lhd N_i$.

(3) 有自然满同态

$$\begin{aligned}\pi:G_1\times\cdots\times G_n&\to G_1/N_1\times\cdots\times G_n/N_n\\(g_1,\cdots,g_n)&\mapsto(g_1N_1,\cdots,g_nN_n),\end{aligned}$$

易知 $\ker\pi=N_1\times\cdots\times N_n$.

□

Ex2.1 证明：

$$Z^n\simeq\left\langle x_1,\cdots,x_n\middle|x_ix_j=x_jx_i,1\leqslant i<j\leqslant n\right\rangle.$$

证明.

(1) $f:X\to\mathbb{Z}^n,x_i\mapsto e_i$.

(2) 由自由群的泛性质,f 诱导了 $\tilde f:F(X)\twoheadrightarrow\mathbb{Z}^n$.

(3) 由于 $\tilde f(x_ix_j)=e_i+e_j=e_j+e_i=\tilde f(x_jx_i)$, 所以 $\tilde f$ 满足关系 $x_ix_j=x_jx_i$,$1\leqslant i<j\leqslant n$.
所以 $\tilde f$ 诱导了
$$\bar f:F(x_1,\cdots,x_n)/N(x_ix_jx_i^{-1}x_j^{-1}\big|1\leqslant i<j\leqslant n)\twoheadrightarrow\mathbb{Z}^n.$$

(4) 下证 $\bar f$ 是单射, 任取 $y\in\ker\bar f$,y 形如 $\bar{x_1}^{k_1}\bar{x_2}^{k_2}\cdots\bar{x_n}^{k_n}$, 且 $\bar f(y)=0$, 即

$$k_1e_1+k_2e_2+\cdots+k_ne_n=0.$$

而 $e_1,\cdots,e_n$ 是 $\mathbb{Z}^n$ 的一组基, 因此 $k_1=\cdots=k_n=0$, 即 $g=1$, 从而 $\bar f$ 是单射.

□

Ex2.2 设 G 是群,$N\lhd G$, 若 N 和 G/N 都是有限生成的, 则 G 也是有限生成的.

证明. 设 $U=\{u_1,u_2,\cdots,u_r\}$ 有限生成 N,$\overline{V}=\{\bar v_1,\bar v_2,\cdots,\bar v_s\}$ 有限生成 G/N.
设 $\varphi:G\twoheadrightarrow G/N$ 是自然同态. 任取 $v_i\in G$ 使得 $\varphi(v_i)=\bar v_i$,$1\leqslant i\leqslant s$.
断言 $\{u_1,\cdots,u_r,v_1,\cdots,v_s\}$ 是 G 的生成集.
任取 $g\in G$,$\varphi(g)=\bar v_{i_1}^{\epsilon_1}\cdots\bar v_{i_n}^{\epsilon_n}$, 其中 $\epsilon\in\{1,-1\}$,$1\leqslant i_j\leqslant s$,$1\leqslant j\leqslant n$,$n\in\mathbb{N}$.
所以存在 $n\in N$ 使得 $g=nv_{i_1}^{\epsilon_1}\cdots v_{i_n}^{\epsilon_n}=u_{j_1}^{\delta_1}\cdots u_{j_m}^{\delta_m}v_{i_1}^{\epsilon_1}\cdots v_{i_n}^{\epsilon_n}$. □

Ex2.3 设 $\mathbf{A}\in\mathbb{Z}^{n\times n}$, 则 $\mathbf{A}\in\mathrm{GL}_n(\mathbb{Z})\Longleftrightarrow\phi_{\mathbf{A}}:\mathbb{Z}^n\longrightarrow\mathbb{Z}^n$ 是同构.

证明.

- $\Longrightarrow\phi_{\mathbf{A}}\circ\phi_{\mathbf{A}^{-1}}=\mathrm{Id}$,$\phi_{\mathbf{A}^{-1}}\circ\phi_{\mathbf{A}}=\mathrm{Id}$.
- $\Longleftarrow$ 由 $\phi_{\mathbf{A}}\circ\phi_{\mathbf{B}}=\mathrm{Id}$ 知 $\mathbf{AB}=\mathbf{I}$.

□

Ex2.4 $\phi_P(\operatorname{Im}\phi_B) = \operatorname{Im}\phi_A$

证明. 因为 $B = P^{-1}AQ$, 所以 $PB = AQ$, 所以 $\phi_P\phi_B = \phi_A\phi_Q$.

从而 $\phi_P(\operatorname{Im}\phi_B) = \phi_A(\operatorname{Im}\phi_Q) = \phi_A(\mathbb{Z}^n) = \operatorname{Im}\phi_A$. □

15 第十五周暨第十三次

P49.7 试证：当 $(m,n)=1$ 时,$\mathbb{Z}_m \oplus \mathbb{Z}_n$ 的不变因子为 $\{mn\}$；而当 $(m,n)>1$ 时,$\mathbb{Z}_m \oplus \mathbb{Z}_n$ 的不变因子为 $\{(m,n),[m,n]\}$.

证明.

- 当 $(m,n=1)$ 时,$\mathbb{Z}_m \oplus \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$, 这是中国剩余定理.
-

$\square$

Chapter 6

另一条脉络

1 有限群

1.1 四元群

循环群

- $U(\mathbb{Z}[\mathrm{i}]) = \{\pm 1, \pm \mathrm{i}\}$, 运算是复数乘法, 生成元是 i.
- $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, 运算是同余类加法, 生成元是 $\bar{1}$.

Klein 四元群（实际上是域）

- $\mathbb{Z}[\mathrm{i}]/(2) = \{\bar{0}, \bar{1}, \mathrm{i}, \bar{1} + \mathrm{i}\}$
- $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + \bar{1}) = \{\bar{0}, \bar{1}, u, u + \bar{1}\}$

1.2 六元群

循环群

S_3

- 无六阶元
- 非 Abel
- $\mathrm{GL}_2(\mathbb{F}_2)$

2 不可约性的判定

- Eisenstein, 永远滴神.
- 模素数 p 后不可约则原式不可约.
  - 但容易构造不可约多项式模素数 p 后可约.
  - 甚至 x^4+1 模任意素数 p 后可约.
- 平移. 平移前后不可约性不变.
  - $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$,$g(x):=f(x+1)\equiv x^{p-1} \mod p$.Eisenstein.
  - $f(x)=x^4+1$,$g(x):f(x+1)=x^4+4x^3+6x^2+4x+2$.Eisenstein.
  - $f(x)=x^6+x^3+1$,$g(x):f(x+1)=x^6+6x^5+15x^4+21x^3+18x^2+9x+3$.Eisenstein.
- 有无根 $\Longleftrightarrow$ 有无一次因式.
  - 有限域上直接代值试.
  - 二次实系数多项式比如 x^2+1 判别式小于 $0\Longrightarrow$ 在 $\mathbb{R}$ 上无根, 从而在 $\mathbb{R}$ 的各种子域比如 $\mathbb{Q}(\sqrt{2})$ 上无根.
  - 判断在单扩张如 $\mathbb{Q}(\omega)$ 上有无根直接将根设成 $a+b\omega$ 代入暴算.
- $\mathbb{Q}[x]$ 中的不可约性等同于 $\mathbb{Z}[x]$ 中的不可约性.
- 曲线救国：
  - 商掉它生成的主理想后是域.
    - 域 $\Longrightarrow$ 极大理想 $\Longrightarrow$ 素理想 $\Longrightarrow$ 素元 $\Longrightarrow$ 不可约元
  - 它是某个代数元的化零多项式, 并且单扩张的扩张次数与它的次数相同.

3 $\mathbb{F}_9$

直接验证, 易知 $\mathbb{F}_3[x]$ 中的首一不可约二次多项式只有三个,$x^2+\bar{1}, x^2+x-\bar{1}, x^2-x-\bar{1}$.
$\mathbb{F}_9$ 的乘法表.

解.

	$\bar{0}$	$\bar{1}$	$\bar{2}$	u	$\bar{1}+u$	$\bar{2}+u$	$\bar{2}u$	$\bar{1}+\bar{2}u$	$\bar{2}+\bar{2}u$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	u	$\bar{1}+u$	$\bar{2}+u$	$\bar{2}u$	$\bar{1}+\bar{2}u$	$\bar{2}+\bar{2}u$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\bar{2}u$	$\bar{2}+\bar{2}u$	$\bar{1}+\bar{2}u$	u	$\bar{2}+u$	$\bar{1}+u$
u	$\bar{0}$	u	$\bar{2}u$	$\bar{2}$	$\bar{2}+u$	$\bar{2}+\bar{2}u$	$\bar{1}$	$\bar{1}+u$	$\bar{1}+\bar{2}u$
$\bar{1}+u$	$\bar{0}$	$\bar{1}+u$	$\bar{2}+\bar{2}u$	$\bar{2}+u$	$\bar{2}u$	$\bar{1}$	$\bar{1}+\bar{2}u$	$\bar{2}$	u
$\bar{2}+u$	$\bar{0}$	$\bar{2}+u$	$\bar{1}+\bar{2}u$	$\bar{2}+\bar{2}u$	$\bar{1}$	u	$\bar{1}+u$	$\bar{2}u$	$\bar{2}$
$\bar{2}u$	$\bar{0}$	$\bar{2}u$	u	$\bar{1}$	$\bar{1}+\bar{2}u$	$\bar{1}+u$	$\bar{2}$	$\bar{2}+\bar{2}u$	$\bar{2}+u$
$\bar{1}+\bar{2}u$	$\bar{0}$	$\bar{1}+\bar{2}u$	$\bar{2}+u$	$\bar{1}+u$	$\bar{2}$	$\bar{2}u$	$\bar{2}+\bar{2}u$	u	$\bar{1}$
$\bar{2}+\bar{2}u$	$\bar{0}$	$\bar{2}+\bar{2}u$	$\bar{1}+u$	$\bar{1}+\bar{2}u$	u	$\bar{2}$	$\bar{2}+u$	$\bar{1}$	$\bar{2}u$

□

- u 和 $\bar{2}u$ 的最小多项式是 $x^2+\bar{1}$.
- $u+\bar{1}$ 和 $\bar{2}u+\bar{1}$ 的最小多项式是 $x^2+x-\bar{1}$.
- $u+\bar{2}$ 和 $\bar{2}u+\bar{2}$ 的最小多项式是 $x^2-x-\bar{1}$.

4 Zorn 引理及其应用

4.1 预备

4.2 极大理想的存在性

4.3 无穷维线性空间基的存在性

我们首先将有限维线性空间中基的概念推广到任意线性空间：

定义 4.1. 设 V 是域 k 上线性空间,$Y \subset V$.

(1) 称 Y 线性无关如果 Y 的任意有限子集是线性无关的.

(2) 称 Y 张成 V 如果每个 $v \in V$ 都是 Y 中有限多个元素的线性组合, 记作 $V = \langle Y \rangle$.

(3) V 的一组基是张成 V 的线性无关子集.

在 V 中, 只有有限和是被允许的, 这是因为 V 上没有定义拓扑, 因此没有序列收敛的概念.

例 4.2. $Y = \{1, x, x^2, \cdots, x^n, \cdots\}$ 是 $V = k[x]$ 的基.

定理 4.3. 任意域 $\mathbb{F}$ 上线性空间有一组基. 事实上,V 的每组线性无关子集 B 都被包含在 V 的某组基中, 即, 存在 B' 使得 $B \cup B'$ 是 V 的一组基.

证明. □

一个很好的 notes：http://www.math.lsa.umich.edu/ kesmith/infinite.pdf

4.4 用素理想刻画 Noetherian 环

4.5 域的代数闭包