Ex 1.

2. 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 $g\circ f=1_A$； $\Leftrightarrow$ 左消去律

(2) f 为满射 $\Leftrightarrow$ 存在 $h:B\to A$，使得 $f\circ h=1_B$. $\Leftarrow$ 右消去律

Ex 2

记明：

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

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

Ex 2

证明:

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

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

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

Ex 3 (选做)

$\mathbb{Z}_n$ 上定义 "+" 和 "·"

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

$$[i][j] = [ij]$$

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

Ex 4 $\forall m, n \in \mathbb{Z}$, $a \in R$

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

ma, na: R 上的加法; $(m+n)a$: $\mathbb{Z}$ 上的加法.

Ex 5 $\forall n \in \mathbb{Z}$, $a \in R$ 有

$$na = (n 1_R) \cdot a$$

$1_R \cdot a$: R 上的乘法

作业中的环均是含幺交换环，同态 $\varphi: R \to S$ 满足 $\varphi(1_R) = 1_S$.

Ex 1. 给定 R. $a, b \in R$. 证明: $(a+b)^n = a^n + \cdots + b^n$.

最多归纳法.

Ex 2. 有限环 R 是整环 $\Leftrightarrow$ R 是域.

证明: "$\Leftarrow$" 定义.

"$\Rightarrow$" 设 $|R| = n$. $\forall\, 0 \neq a \in R$, 考虑集合 $A = \{a^i \mid i \in \mathbb{N}\}$

由于 $A \subseteq R$, $|A| \leq |R|$, 从而存在 $m, n \in \mathbb{N}$ 且 $m \neq n$

(不妨设 $m > n$), 使得 $a^m = a^n$, 即 $a^n(a^{m-n} - 1) = 0$

从而 $a^{m-n} - 1 = 0$, 即 $a^{m-n} = 1$. 因此 $a \in U(R)$ □

Ex 3. $\mathbb{Q}[i]$ 的子域只有 $\mathbb{Q}[i]$ 和 $\mathbb{Q}$.

证明. 设 K 是 $\mathbb{Q}[i]$ 的子域. 则 $1 \in K$. 从而由运算的封闭性

知 $\mathbb{Q} \subseteq K$. 则

1° $\mathbb{Q} = K$

2° $\mathbb{Q} \subsetneq K$. 从而存在 $a + bi \in K \setminus \mathbb{Q}$. 因此 $i \in K$.

因此 $p + qi \in K$, $\forall\, p, q \in \mathbb{Q}$, 即 $\mathbb{Q}[i] \subseteq K$. 从而

$K = \mathbb{Q}[i]$.

综上 $\mathbb{Q}[i]$ 的子域只有 $\mathbb{Q}[i]$ 和 $\mathbb{Q}$. □.

Ex 4. 分类 $\mathbb{Z}[\sqrt{-1}]$ 的子环.

(提示: $S_n = \{a + bn\sqrt{-1} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}[\sqrt{-1}]$ 子环)

解. 设 S 是 $\mathbb{Z}[\sqrt{-1}]$ 的子环. 则 $1 \in S$, 由运算封闭性知,

$\mathbb{Z} \subseteq S$. 则

1° $\mathbb{Z} = S$.

2°. $\mathbb{Z} \subsetneq S$. 则存在 $k+l\sqrt{-1} \in S \setminus \mathbb{Z}$, $l \neq 0$. 从而 $l\sqrt{-1} \in S$.

因此 $S_l \subseteq S$. 考虑集合

$$N = \{ b \in \mathbb{Z} \mid a+bi \in S, \text{对某个 } a \in \mathbb{Z} \text{ 且 } b \neq 0 \}.$$

$$= \{ b \in \mathbb{Z} \mid bi \in S, b \neq 0 \} \text{ (由于 } S \text{ 对减法封闭)}.$$

由于 $S_l \subseteq S$, $l \in N$. 从而 $N \neq \emptyset$. 因此由最小数原理知 N 中有绝对值最小的整数, 不妨设为 n. 从而 $S_n \subseteq S$. (容易验证 $\forall a, b \in S_n$, $a-b, ab \in S_n$ 且 $1 \in S_n$. 从而 S_n 是 $\mathbb{Z}[\sqrt{-1}]$ 的子环). $\forall c+di \in S$, $c, d \in \mathbb{Z}$, 有 $di \in S$. 从而 $ni \in S$, 由于 $n \in N$. 由带余除法知, $d = nq + r$, 其中 $q \in \mathbb{Z}$, $0 \leq r < |n|$. 从而 $ri = di - nqi \in S$, $r \in S$. 由 n 的选择知, $r = 0$. 因此 $di = nqi \in S_n$, 从而 $c+di \in S_n$. 因此, $S \subseteq S_n$. 容易验证 $S_m \not\subseteq S_n$ 若 $|m| \neq |n|$. □.

Exc 5 证: 环同态 $\mathbb{Z}_8 \longrightarrow \mathbb{Q}$

证明. 设 $\phi: \mathbb{Z}_8 \to \mathbb{Q}$ 为环同态. 则

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

矛盾! 因此不存在 $\mathbb{Z}_8$ 到 $\mathbb{Q}$ 的环同态. □

Ex 6. 描述 $\mathbb{Z}[\sqrt{-3}] = \{ a+b\sqrt{-3} \mid a, b \in \mathbb{Z} \}$ 的单位群, 并证明此环为整环但不是域.

解. $\forall a+b\sqrt{-3} \in U(\mathbb{Z}[\sqrt{-3}])$, $\exists c+d\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$, s.t.

$$(a+b\sqrt{-3})(c+d\sqrt{-3}) = 1.$$

则

$$(a^2+3b^2)(c^2+3d^2) = (a+b\sqrt{-3})(c+d\sqrt{-3})\overline{(a+b\sqrt{-3})(c+d\sqrt{-3})}$$

$$= 1 \cdot \overline{1} = 1$$

而 $a^2+3b^2, c^2+3d^2 \in \mathbb{Z}$，可知

$$\begin{cases} a^2+3b^2=1 \\ c^2+3d^2=1. \end{cases}$$

从而 $b=d=0$，$a=\pm 1$. 从而 $a+b\sqrt{-3}=\pm 1$. 因此

$$U(\mathbb{Z}[\sqrt{-3}]) \cong \mathbb{Z}_2 \neq \mathbb{Z}[\sqrt{-3}]$$

从而 $\mathbb{Z}[\sqrt{-3}]$ 不是域. 由 $\mathbb{Z}[\sqrt{-3}]$ 是 $\mathbb{C}$ 的子环知，$\mathbb{Z}[\sqrt{-3}]$ 是整环. □

Ex.7. 求证 $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$ 是实数域 $\mathbb{R}$ 的子域.

验证 $\forall x,y\in\mathbb{Q}[\sqrt{2}]$，都有 $x-y, xy^{-1}$（此时 $y\neq 0$）$\in\mathbb{Q}[\sqrt{2}]$ 即可. □

Ex 8. (1) 确定 $\mathbb{Z}_m$ 的全部子环（m 是正整数）.

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

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

思路. (1). $S\subseteq\mathbb{Z}_m$ 是子环.

$[1]\in S \Rightarrow [n]\in S$（加法封闭），$\forall n\geq 0$.

(2) 类似于 Ex.3.

(3). $\phi\in\mathrm{Aut}(\mathbb{Q}[\sqrt{2}]) \Rightarrow \phi(1)=1 \Rightarrow \phi|_{\mathbb{Q}}=\mathrm{id}_{\mathbb{Q}}$

ϕ 是同态，只需确定 $\phi(\sqrt{2})$ 的值. 而

$$[\phi(\sqrt{2})]^2=\phi(2)=2$$

从而 $\phi(\sqrt{2})=\pm\sqrt{2}$. 再验证 $\phi(a+b\sqrt{2})=a+b\sqrt{2}$ 和 $\phi(a+b\sqrt{2})=a+b\sqrt{2}$ 分别是环自同构即可.

$\psi \in Aut(\mathbb{Z}_m) \Rightarrow \psi([1]) = [1] \Rightarrow \psi([n]) = [n]$

从而 $\psi = id_{\mathbb{Z}_m}$. □

Ex.9. 设 R 为环，X 为集合. $\theta: X \to R$ 是双射. 定义

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

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

证明 $(X, \oplus, \cdot)$ 是环且 θ 是同构.

证明要点. (1) "$\oplus$" 和 "$\cdot$" 是良定的.

(2) $(X, \oplus, \cdot)$ 是环，环的公理 + 交换律.

(3) θ 是同态. □

Ex.10. 设有环同态 $\mathbb{F}_p \xrightarrow{\psi} R$，证明

(1) ψ 单

(2) $(R, +)$，定义 $\lambda \in \mathbb{F}_p$, $a \in R$, $\lambda a = \psi(\lambda) a \in R$

证明 R 成为 $\mathbb{F}_p$-线性空间

(3) 若 R 是有限环，则 $|R| = p^n$, $n > 0$.

证明. (1). 考虑 $\ker \psi$. $\ker \psi \lhd \mathbb{F}_p$ 且 $\mathbb{F}_p$ 是域. 因此 $\ker \psi = \{0\}$ 或 $\ker \psi = \mathbb{F}_p$ (否则，因为此时 ψ 是 0 态射).

(2) 显然，$\lambda a = \psi(\lambda) a$ 良定. 只需验证线性空间的公理即可 (不作赘述).

(3). 取 R 的 $\mathbb{F}_p$-极大线性无关组 Σ，由 $\Sigma \subseteq R$ 知 Σ 是有限的. 从而 R 是有限维 $\mathbb{F}_p$-线性空间. 设 $n = \dim_{\mathbb{F}_p} R$, 则 $R \cong \mathbb{F}_p^n$. 从而 $|R| = p^n$. □

Ex.11 (对应定理) 设 $I \lhd R$, 则有双射

$$\{J \supset I \mid J \text{为} R \text{的理想}\} \longleftrightarrow \{R/I \text{的理想}\}$$

证明. 记自然同态 $f: R \twoheadrightarrow R/I$. 定义映射

$$\Phi: \{J \supset I \mid J \lhd R\} \longrightarrow \{R/I \text{的理想}\}$$

$$J \longmapsto f(J)$$

$$\Psi: \{R/I \text{的理想}\} \longrightarrow \{J \supset I \mid J \lhd R\}$$

$$L \longmapsto f^{-1}(L).$$

先验证 Φ 和 Ψ 是良定的, 即 $f(J) \lhd R/I$ 和 $f^{-1}(L) \lhd R$ 且 $f^{-1}(L) \supset I$. 再记 $\Phi^{-1} = \Psi$, 即 $f(f^{-1}(L)) = L$ 且 $f^{-1}(f(J)) = J$. □

Ex.12 分类 $\mathbb{Z}_n$ 的理想. ($\mathbb{Z}_n$ 不是 UFD! 我们定义因子是在 UFD 上的)

证明. 由 Ex.11 知 $\mathbb{Z}_n$ 的理想均为形如 $m\mathbb{Z}/n\mathbb{Z}$, 其中 $m\mathbb{Z} \subseteq n\mathbb{Z}$, i.e. $m \mid n$. 若 $m_1, m_2 \mid n$ 且 $m_1\mathbb{Z}/n\mathbb{Z} = m_2\mathbb{Z}/n\mathbb{Z}$, 则 $m_1 = m_2$ (由于 $m_1 \equiv m_2 \pmod{n}$). □

Ex.13. R 的分式域 $\mathrm{Frac}(R)$ 上定义了 "$+$" 和 "$\cdot$". 证明:

(1) "$+$", "$\cdot$" 是良定的.

(2) $\mathrm{Frac}(R)$ 是含幺交换环.

(3) $\mathrm{Frac}(R)$ 是域

(4) $R \xrightarrow{\mathrm{can}_R} \mathrm{Frac}(R)$, $a \longmapsto \frac{a}{1_R}$ 是单的环同态.

思路 (1). 略.

(2) 八条公理 + 交换. 其中单位是 $\frac{1_R}{1_R}$，零元是 $\frac{0_R}{1_R}$.

(3) $\frac{a}{x} \neq \frac{0}{1_R} \Rightarrow a \neq 0 \Rightarrow \frac{x}{a}$ 良定且 $\left(\frac{a}{x}\right)\left(\frac{x}{a}\right) = \frac{1_R}{1_R}$.

(4) 先验证 can_R 是环同态.

考虑 $\ker(can_R)$. $\forall a \in \ker(can_R) \Rightarrow can_R(a) = \frac{0}{1_R}$

即 $\frac{a}{1_R} = \frac{0}{1_R} \Rightarrow a = a \cdot 1_R = 0 \cdot 1_R = 0$. $\Rightarrow \ker(can_R) = \{0\}$

即 can_R 单.

□

Ex 1. $R=\mathbb{Z}[\sqrt{-3}]$，说明2是不可约元且 $2\nmid(1+\sqrt{-3})$，$2\nmid(1-\sqrt{-3})$

解. 设 $2=(a+b\sqrt{-3})(c+d\sqrt{-3})$，其中 $a,b,c,d\in\mathbb{Z}$

两边取模长，则 $4=(a^2+3b^2)(c^2+3d^2)$ 则有

1°. $\begin{cases} a^2+3b^2=2 \\ c^2+3d^2=2, \end{cases}$ 无整解

2°. $\begin{cases} a^2+3b^2=4 \\ c^2+3d^2=1 \end{cases}$ 或 $\begin{cases} a^2+3b^2=1 \\ c^2+3d^2=4 \end{cases}$

解得 $\begin{cases} a=\pm 2 \\ b=0 \end{cases}$ 或 $\begin{cases} a=\pm 1 \\ b=0 \end{cases}$

综上，2没有真因子，即为不可约元.

若 $2\mid(1+\sqrt{-3})$，则 $1+\sqrt{-3}=2(a+b\sqrt{-3})$，$a,b\in\mathbb{Z}$.

得 $\begin{cases} 2a=1, \\ 2b=1 \end{cases}$ 无整数解. 因此 $2\nmid(1+\sqrt{-3})$ 同理 $2\nmid(1-\sqrt{-3})$ □

Ex 2. 设 I 是交换环，证明集合

$$\sqrt{I}=\{r\in R\mid \exists n\geq 1,\ s.t.\ r^n\in I\}$$

也是 R 的理想.

证明. 1°. $\forall a,b\in\sqrt{I}$，$\exists m,n\geq 1$，s.t. $a^m, b^n\in I$. 则由交换环的二项式定理，$(a-b)^{m+n-1}\in I$，即 $a-b\in I$.

2° 显然，$\forall a\in\sqrt{I}$，$r\in R$，$ar\in\sqrt{I}$.

因此 $\sqrt{I}\lhd R$. □

（直接验证 $a+b$ 和 ra 也是可以的，个人建议这个）

Ex 3. 设 $I_1, I_2 \lhd R$, 求证

(1) $I_1 I_2 \lhd R$, 且 $I_1 I_2 \subset I_1 \cap I_2$, 问: 是否一定有 $I_1 I_2 = I_1 \cap I_2$?

(2) $I_1 + I_2 \lhd R$, 且它是包含 I_1 和 I_2 的最小理想.

(3) 设 $R = \mathbb{Z}$, $I_1 = n\mathbb{Z}$, $I_2 = m\mathbb{Z}$, 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). $\forall a, b \in I_1 I_2$, $r \in R$, $a = \sum_{\text{finite}} x_i y_i$, $b = \sum_{\text{finite}} x_i' y_i'$, 其中 $x_i, x_i' \in I_1$, $y_i, y_i' \in I_2$. 则

1°. $a - b \in I_1 I_2$

2° $ra \in I_1 I_2$

因此 $I_1 I_2 \lhd R$. 由于 $a \in I_1$ 且 $a \in I_2$, $a \in I_1 \cap I_2$. 因此 $I_1 I_2 \subset I_1 \cap I_2$. (反例见(3)).

(2) $\forall a, b \in I_1 + I_2$, 有 $a = a_1 + a_2$, $b = b_1 + b_2$, 其中 $a_1, b_1 \in I_1$, $a_2, b_2 \in I_2$, 则 $a - b = (a_1 - b_1) + (a_2 - b_2) \in I_1 + I_2$

$\forall r \in R$, 有 $ra = ra_1 + ra_2 \in I_1 + I_2$. 因此 $I_1 + I_2 \lhd R$.

设 $J \lhd R$, 且 $J \supseteq I_1, I_2$. 则 $\forall a \in I_1 + I_2$, $a = a_1 + a_2 \in J$, 其中 $a_i \in I_i$, $i = 1, 2$. 因此 $J \supseteq I_1 + I_2$. 即 $I_1 + I_2$ 是包含 I_1 和 I_2 的最小理想.

(3). 略 (集合间的相等). □

Ex4. 设 $f: R \to S$ 环同态，$I \lhd R$，$J \lhd S$ 且 $f(I) \subset J$. 作商环 R/I，S/J，定义

$$\bar{f}: R/I \to S/J, \quad a+I \mapsto f(a)+J.$$

证明. (1) $\bar{f}$ 为良定的环同态

(2) $\bar{f}$ 是同构 $\iff f(R)+J=S$ 且 $I=f^{-1}(J)$.

证明 (1). $\forall\, a+I, a'+I \in R/I$ 且 $a+I=a'+I$，即 $a-a' \in I$，有

$f(a)-f(a')=f(a-a') \in f(I) \subset J$，即 $f(a)+J=f(a')+J$

故 $\bar{f}$ 是良定的. 易证是环同态

(2). $\bar{f}$ 是同构. $\forall s \in S$，$s+J \in S/J$，则 $\exists\, r+I \in R/I$，s.t. $\bar{f}(r+I)=s+J$，从而 $f(r)+J=s+J$，即 $f(r)-s \in J$.

因此 $s=f(r)+b \in f(R)+J$，其中 $b \in J$. 因此 $f(R)+J \supseteq S$. 显然 $S \subseteq f(R)+J$，从而 $S=f(R)+J$.

$\forall\, a \in f^{-1}(J)$，$f(a) \in J$，则 $\bar{f}(a+I)=f(a)+J=J$. 于是 $a \in I$，从而 $f^{-1}(J) \subseteq I$. 从而 $f(I) \subset J$.

另一方面，若 $f(R)+J=S$，则 $\forall s \in S$，$s=f(r)+b$，其中 $r \in R$，$b \in J$. 则 $s+J=f(r)+b+J=f(r)+J=\bar{f}(r+I)$

从而 $\bar{f}$ 是满的. $\forall\, r+I \in \ker(\bar{f})$，$f(r)+J=\bar{f}(r+I)=J$

即 $f(r) \in J$，即 $r \in f^{-1}(J)=I$，即 $\ker(\bar{f})=I$. 因此 $\bar{f}$ 是单的.

□

这道题本质上就是同态基本定理的推广吧.

Ex 5. 设 $(R,+,\cdot)$ 为含幺环，$\forall a,b\in R$，定义

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

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

思路. 定义映射

$$\theta: R\longrightarrow R,\ a\longmapsto a+1.$$

显然是双射. 则

$$a\oplus b=a+b+1=\theta^{-1}(\theta(a)+\theta(b)).$$

$$a\odot b=ab+a+b=\theta^{-1}(\theta(a)\cdot\theta(b))$$

由第二次作业 Ex 9，得证！ □

Ex 6. 设 $\{I_n\}$ 是理想，且 $I_n\subset I_{n+1}$，$\forall n\in\mathbb{N}^+$. 证明 $\bigcup_{n=0}^{\infty} I_n$ 也是理想. (可以试着用这个结论证明含幺交换环一定有极大理想，从而一定有素理想)

略. □

Ex 7. 设 D 是整环，m,n 互素，若 $a^m=b^m$，$a^n=b^n$，则 $a=b$.

证明. $(m,n)=1$，由 Bezout 定理，$\exists x,y\in\mathbb{Z}$，s.t. $xm+yn=1$.

考虑 $D\xhookrightarrow{i}\mathrm{Frac}\,D$. 则 a,b 在 $\mathrm{Frac}\,D$ 中可逆. 在 $\mathrm{Frac}\,D$ 中考虑 ab^{-1}

$ab^{-1}=a^{xm+yn}(b^{xm+yn})^{-1}=b^{xm+yn}(b^{xm+yn})^{-1}=1$. 因此在分式域中 $a=b$. 由 i 是单的知，在 D 中，$a=b$ □

注. 这道题若在 D 中考虑，则需考虑 x,y 的正负，讨论起来比较麻烦！故将 D 嵌入 $\mathrm{Frac}\,D$ 在考虑 (若将 D 看成 $\mathbb{Z}$，嵌入仍是一个十分自然的想法！)

Ex 8. 证明：含幺交换有限环的素理想必为极大理想

思路. P 素 $\Leftrightarrow R/p$ 整环，m 极大 $\Leftrightarrow R/m$ 域. 再利用第二次作业 Ex 2. □

Ex 9. 设 $f: R \to S$ 是环的满同态. $K = \ker f$. 求证:

(1) 若 $P \lhd R$ 是素理想且 $P \supseteq K$, 则 $f(P)$ 也是 S 的素理想

(2) 若 $Q \lhd S$ 是素理想, 则 $f^{-1}(Q)$ 也是 R 的素理想.

(3) S 中的素理想和 R 中含 K 的素理想一一对应.

将"素理想"换成"极大理想"也正确.

思路. 由同态基本定理, $R/K \cong S$. 不妨设 $S = R/K$.

(1) 由 Ex 4, $f: R \to R/K$ 诱导了环同构

$$\bar{f}: R/P \longrightarrow \frac{R/K}{f(P)}$$ (其实就是同态基本定理)

这个是良定义的(因为由对应定理, $f(P) = P/K$ 是理想), 从而 $f(P)$ 是素理想.

(2) 由对应定理知, $f^{-1}(Q) \lhd R$. 再一次利用 Ex 4.

(3) 由对应定理和 (1), (2).

将素理想换成极大理想证明思路相同. 但也可利用序 ($P_1 \subseteq P_2 \Leftrightarrow f(P_1) \subseteq f(P_2)$) □

Ex 10. $I \lhd R$. 证明: R/I 中的素理想均可写成 P/I, 其中 P 为 R 中包含 I 的素理想.

思路: 对 $\pi: R \to R/I$ 利用 Ex 9. □

Ex 11. $m \geq 2$. 试确定环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 的全部素理想和极大理想. (这里我在习题课上说错了, $\mathbb{Z}_m$ 的零理想若为素理想, 则 m 为素数, 从而对应于 $\mathbb{Z}$ 中的 $m\mathbb{Z}$ 是极大理想, 因为素=极大.)

思路. 利用 Ex 10, $\mathbb{Z}$ 是 PID 且 $\mathbb{Z}$ 中的非零素理想均为极大理想. □

Ex 12. 定义 $\widetilde{R} = \{\underline{a} = (a_i)_{i\in\mathbb{N}} \mid a_i \in R, a_i = 0_R, i >> 0\}$.

$\underline{a} + \underline{b} = (a_i + b_i)_{i\in\mathbb{N}}$, $\underline{a} - \underline{b} = \underline{c} = (c_i)_{i\in\mathbb{N}}$, 其中

$c_\ell = \sum_{i\leq \ell} a_i b_{\ell - i}$, $\forall \ell$. 证明 $\widetilde{R} \simeq R[x]$ 同构.

思路: 先证构造 2 环, 再利用第二次作业 Ex 9 □

Ex 13. (1) $\forall X$ 集合, R 环. 证明: $\mathrm{Map}(X, R)$ 自然成环.

(2). $R[x] \xrightarrow{ev} \mathrm{Map}(R, R)$, $f(x) \longmapsto f$ 是环同态.

($f(x)$: 多项式; f: 多项式函数)

有了这个 ev 同态, 我们才有资格区一谈论映射才有像, $R[x]$ 里的元素不是映射!)

思路. (1) $\forall f, g \in \mathrm{Map}(X, R)$, 定义

$$f+g : X \longrightarrow R,\ x \longmapsto f(x)+g(x)$$

$$f\cdot g : X \longrightarrow R,\ x \longmapsto f(x)g(x)$$

验证 $(\mathrm{Map}(X,R), +, \cdot)$ 是环.

(2) 略 □

Ex 14. $\mathbb{C}[x,y]$ 中, $p = (x)$. $p \in \mathrm{Spec}\,\mathbb{C}[x,y]$ 但不极大!

思路. 考虑 $\pi : \mathbb{C}[x,y] \longrightarrow \mathbb{C}[y]$, $f(x,y) \longmapsto f(0,y)$. 类似于 Ex 13, 可以说明 π 是环同态. 显然 π 是满的. $\ker\pi = p$. 由同态基本定理, $\mathbb{C}[x,y]/p \simeq \mathbb{C}[y]$ 是整环不是域. □

Ex 15. 证明：固定 $a\in k$，则 $k[x]/(x-a)\cong k$

思路：考虑 $k[x]\to k$，$f(x)\mapsto f(a)$.（类似于Ex 14）. □

Ex 16. $R\xrightarrow{\theta} S$ 环同态，则 θ 自然延拓成 $\widehat{\theta}: R[x]\to S[x]$ 是环同态.

思路：$\widehat{\theta}: R[x]\to S[x]$，$\sum_{i=1}^{n} r_i x^i \to \sum_{i=1}^{n}\theta(r_i)x^i$. 验证 $\widehat{\theta}$ 是环同态且 $\widehat{\theta}|_R=\theta$. □

Ex 17. 若 D 是整环但不是域. 求证：$D[x]$ 不是PID.

证明：只需证其逆否命题. 假设 $D[x]$ 是PID. $\forall 0\neq a\in D$，$(a,x)=(f)$，其中 $f\in D[x]$. 从而 $f\mid a$ 且 $f\mid x$. 则 $\deg f=0$，即 $f\in D$. 而 $x=fg$，其中 $g\in D[x]$. 对比系数和 $f\in U(D)$. 因此 $(a,x)=(1)$. 从而存在 $u,v\in D[x]$，s.t. $au+xv=1$. 赋值得 $au(0)=1$，即 a 是 D 中的单位. 因此 D 是域. □

Ex 18. 试确定 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 的自同构群.

思路：$\forall \sigma\in\mathbb{Z}[x]$，$\sigma(1)=1\Rightarrow \sigma|_{\mathbb{Z}}=id$. 只需定义 $\sigma(x)$

$\deg \sigma(x)=1$. 否则

1° $\deg\sigma(x)=0$，σ 显然不是自同构.

2° $\deg\sigma(x)>1$，$\sigma^{-1}(x)$ 没有原像（对比次数）.

3° $\sigma(x)=0$，与1°相同.

得之 $\sigma(x)=ax+b$. 而 $\sigma^{-1}(x)=\frac{y-b}{a}\in\mathbb{Z}[x]$, 因此 $a=\pm1$. 即证 $\sigma(x)=\pm x+b$, $b\in\mathbb{Z}$ 是自同构.

$\mathbb{Q}[x]$ 的情况与 $\mathbb{Z}[x]$ 相似. 即证 $\sigma(x)=qx+r$, $q,r\in\mathbb{Q}$, 是自同构即可. □

Ex 19 (1) $2x+2$ 在 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 中是否为不可约元?

(2) x^2+1 在 $\mathbb{R}[x]$ 和 $\mathbb{C}[x]$ 中是否为不可约元?

思路 (1) $2x+2=2(x+1)$, $2,(x+1)$ 均不是单位, $\Rightarrow$ 2 是约元 in $\mathbb{Z}[x]$

$2x+2$ 与 $x+1$ 在 $\mathbb{Q}[x]$ 相差一个单位, 只需考虑 $x+1$ 是否为不可约元. 设 $x+1=fg$, f,g 均为首一. 则 $\deg(f)+\deg(g)=\deg(fg)=1$. 从而 $\deg f=0$ 或 $\deg g=0$ 即其中一个为单位. 因此 $x+1$ 在 $\mathbb{Q}[x]$ 上不可约.

(2). 在 $\mathbb{C}[x]$ 上, $x^2+1=(x+i)(x-i)$, 且 $(x+i)$ 和 $(x-i)$ 不是单位 (因为单位的次数是零). 因此 x^2+1 在 $\mathbb{C}[x]$ 上可约. 而在 $\mathbb{R}[x]$ 上, 若 x^2+1 可约, 则 $x^2+1=f(x)g(x)$ 且 $\deg f(x)=\deg g(x)=1$, 即 x^2+1 在 $\mathbb{R}$ 上有零点, 矛盾. □

Ex 20. 设 $f=\sum a_i x^i\in\mathbb{Z}[x]$ 首一, p 素. 记 $\bar{f}(x)=\sum\bar{a}_i x^i\in\mathbb{Z}_p[x]$.

求证:

(1) 若对某个素数 p, $\bar{f}$ 在 $\mathbb{Z}_p[x]$ 中不可约, 则 f 在 $\mathbb{Z}[x]$ 中不可约

(2) 若 f 不首一, 结论是否成立?

思路. (1) 若 f 可约，则 $f=gh$，从而 $\overline{f}=\overline{g}\,\overline{h}$，而 g,h 首一

因此 $\overline{g},\overline{h}$ 不是单位，从而 $\overline{f}$ 可约.

(2). f 不首一，取 $f=(2x+1)(x+1)$

$p=2$，$\overline{f}=x+1$ 不可约

Ex1 设 $\theta: k \hookrightarrow K$ 域同态 ($k \xrightarrow{\sim} \mathrm{Im}\theta \subseteq K$). 诱导了环同态

$$\theta: k[x] \to K[x],\ f=\sum_{i=0}^{n} a_i x^i \longmapsto \theta(f)=\sum_{i=0}^{n} \theta(a_i)x^i.$$

问: $\gcd(\theta(f),\theta(g)) \neq \theta(\gcd(f,g))$.

解. 由 $k \xrightarrow{\sim} \mathrm{Im}\theta$ 同构诱导了环同构 $k[x] \xrightarrow{\sim} (\mathrm{Im}\theta)[x]$. 则显然 $\gcd_{(\mathrm{Im}\theta)[x]}(\theta(f),\theta(g)) \cong \theta(\gcd_{k[x]}(f,g))$ (因为 θ^{-1} 也是同构)

而我们证明过 $\gcd_{k[x]}(\theta(f),\theta(g)) = \gcd_{(\mathrm{Im}\theta)[x]}(\theta(f),\theta(g))$ (因为 $\mathrm{Im}\theta \subseteq K$). 因此 $\gcd(\theta(f),\theta(g)) = \theta(\gcd(f,g))$. □

注. 当然也可以用类似于 $k \subseteq K$ 的做法来证明.

Ex2. (泛性质) 记 $\theta: k \to K = k[x]/(f(x))$ ($u=\bar{x}$). 给定 $\delta: k \hookrightarrow F$ 以及 $\alpha \in \mathrm{Root}_F(\delta(f))$ [$\delta(f) \in F[x]$]. 则 $\exists!$ 域同态 $\delta': K \hookrightarrow F$, s.t.

$$\begin{cases} \delta' \cdot \theta = \delta \\ \delta'(u) = \alpha \end{cases}$$

证明. 由 $k \xrightarrow{\sim} F$ 诱导了环同态 $k[x] \xrightarrow{\delta} F[x]$. (由第三次作业 Ex16)

由 ev 同态, 我们得环同态 $F[x] \xrightarrow{v} F[\alpha]=F$, $f \mapsto f(\alpha)$. 因此我们得环同态 $k[x] \xrightarrow{v\delta} F$, $\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \delta(a_i)\alpha^i$. 由 $\delta(f)=0$, $v\delta$ 诱导了映射 $\delta': K \hookrightarrow F$, $\sum_{i=0}^{n} a_i u^i \longmapsto \sum_{i=0}^{n} \delta(a_i)\alpha^i$

即存在性得证. 设 δ'' 满足上述性质, 则

$$\begin{cases} (\delta'-\delta'')\cdot\theta = 0 \\ (\delta'-\delta'')(u) = 0. \end{cases}$$

从而 $(\delta'-\delta'')\left(\sum_{i=0}^{n} a_i u^i\right) = \sum_{i=0}^{n} (\delta'-\delta'')(a_i)(\delta'-\delta'')(u) = 0$. 因此 $\delta'=\delta''$. 唯一性得证. (或者直接说明 $k[x] \to F$ 是同态)

Ex 3. $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ 域同构. (注意! - 之前说错了!)

思路. 利用Ex2的结论. $k=\mathbb{R}$, $f(x)=x^2+1$, $F=\mathbb{C}$, $\alpha=\pm i$. 所以

与域同态 $\delta_1', \delta_2' : \mathbb{R}[x]/(x^2+1) \hookrightarrow \mathbb{C}$, s.t.

$$\begin{cases} \delta_1' \circ \theta = \delta \\ \delta_1'(u) = i \end{cases}, \quad \begin{cases} \delta_2' \circ \theta = \delta \\ \delta_2'(u) = -i \end{cases}.$$

只需验证 δ_1' 和 δ_2' 是满的. 可以看出 $\mathbb{R}[x]/(x^2+1)$ 到 $\mathbb{C}$ 的域同构至少有两个.

Ex 4. $\mathbb{F}_9$ 乘法表. $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$

·	0	1	2	u	u+1	u+2	2u	2u+1	2u+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	u	u+1	u+2	2u	2u+1	2u+2
2	0	2	1	2u	2u+2	2u+1	u	u+2	u+1
u	0	u	2u	2	u+2	2u+2	1	u+1	2u+1
u+1	0	u+1	2u+2	u+2	2u	1	2u+1	2	u
u+2	0	u+2	2u+1	2u+2	1	u	u+1	2u	2
2u	0	2u	u	1	2u+1	u+1	2	2u+2	u+2
2u+1	0	2u+1	u+2	u+1	2	2u	2u+2	u	1
2u+2	0	2u+2	u+1	2u+1	u	2	u+2	1	2u

Ex 5. 验证 $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}$

解. 显然 $U(\mathbb{Z}[\omega]) \supseteq \{\pm 1, \pm\omega, \pm\omega^2\}$. 反过来, $\forall a+b\omega \in U(\mathbb{Z}[\omega])$, $a,b\in\mathbb{Z}$, $\exists c+d\omega \in \mathbb{Z}[\omega]$, $c,d\in\mathbb{Z}$, s.t. $(a+b\omega)(c+d\omega)=1$. 从而 $a^2-ab+b^2 = c^2-cd+d^2 = 1$.

考虑 $a^2-ab+b^2-1=0$. 其有整数解的必要条件是 $\Delta_a = b^2-4(b^2-1) = -3b^2+4 \geq 0$ 且为平方数. 故 $b^2=0$ 或 1

即 $b=0$ 或 ± 1, 分别代入不定方程, 得

$$\begin{cases} b=0 \\ a=\pm 1 \end{cases}, \quad \begin{cases} b=1 \\ a=0 \text{ 或 } 1 \end{cases} \text{ 或 } \begin{cases} b=-1 \\ a=0 \text{ 或 } -1. \end{cases}$$

即 $a+b\omega \in \{\pm 1, \pm\omega, \pm\omega^2\}$. □

Ex 6. $\mathbb{Z}[\sqrt{3}]$ 是 ED 但 $\mathbb{Z}[\sqrt{5}]$ 不是 ED.

思路. 由于 $4 = (1+\sqrt{5})(-1+\sqrt{5}) = 2\times 2$, 且 $\pm 1+\sqrt{5}$, 2 均是 $\mathbb{Z}[\sqrt{5}]$ 中的不可约元, 且 2 和 $\pm 1+\sqrt{5}$ 不相伴. 故 4 有两种分解方式 (参见课本第 84 页). 因此 $\mathbb{Z}[\sqrt{5}]$ 不是 UFD, 从而不是 ED. 对于 $\mathbb{Z}[\sqrt{3}]$, 我们定义

$$\varphi: \mathbb{Z}[\sqrt{3}] \longrightarrow \mathbb{N}$$
$$a+b\sqrt{3} \longmapsto |a^2-3b^2|, \quad a,b\in\mathbb{Z}$$

容易验证 (参见 P87, 例 7).

(1) $\varphi(x)=0 \Leftrightarrow x=0$

(2) 对于 $x,y\in\mathbb{Z}[\sqrt{3}]$, $y\neq 0$, 均有 $q,r\in\mathbb{Z}[\sqrt{3}]$, s.t.

$$x = yq+r, \text{ 并且 } \varphi(r) < \varphi(b)$$

从而 $\mathbb{Z}[\sqrt{3}]$ 是 ED.

注意! ED 与 φ 的选取有关, 而 φ 只需是满足 (1) 和 (2) 的映射 (因此, 一般地, 我们无法穷举所有情况). 因此利用 φ 来说明不是 ED 是不严谨的!

Ex] $\mathrm{Frac}(\mathbb{Z}[w]) = \mathbb{Q}(\sqrt{-3})$.

思路: 由嵌入 $\mathbb{Z}[w] \hookrightarrow \mathbb{Q}(\sqrt{-3})$ 及分式域的泛性质诱导了域嵌入 $\mathrm{Frac}(\mathbb{Z}[w]) \hookrightarrow \mathbb{Q}(\sqrt{-3})$. 而 $\mathbb{Q}(\sqrt{-3})$ 的子域只有 $\mathbb{Q}$ 和 $\mathbb{Q}(\sqrt{-3})$ 且 $\sqrt{-3} \in \mathrm{Frac}(\mathbb{Z}[w])$, 因此 $\mathrm{Frac}(\mathbb{Z}[w]) = \mathbb{Q}(\sqrt{-3})$

注意! 良定一定要说明!

Ex 1 将 60 和 $81+8\sqrt{-1}$ 在 $\mathbb{Z}[\sqrt{-1}]$ 中分解成不可约元乘积.

解. $60 = 2^2\times 3\times 5 = (1+\sqrt{-1})^2(1-\sqrt{-1})^2\times 3\times(2+\sqrt{-1})(2-\sqrt{-1})$

由于 $N(81+8\sqrt{-1}) = (2+\sqrt{-1})^3(2-\sqrt{-1})^3(7+2\sqrt{-1})(7-2\sqrt{-1})$,

故 $81+8\sqrt{-1} = \sqrt{-1}\,(2+\sqrt{-1})^3(7+2\sqrt{-1})$ □

Ex 2. 证明 $p = a^2+b^2$ 且 $p\equiv 1 \pmod 4$ 则

$$\mathbb{Z}[\sqrt{-1}]/(a+b\sqrt{-1}) \cong \mathbb{F}_p.$$

证明: 由 $\mathbb{Z}[\sqrt{-1}]$ 是 PID 及 $a+b\sqrt{-1}$ 是不可约元知, $(a+b\sqrt{-1})$ 是极大理想. 由第三次作业 Ex 4, 我们有环同态(进而是域嵌入):

$$\mathbb{F}_p = \mathbb{Z}/(\mathbb{Z}\cap(a\pm b\sqrt{-1})) \xrightarrow{i} \mathbb{Z}[\sqrt{-1}]/(a\pm b\sqrt{-1})$$

$(p) = (a+b\sqrt{-1})(a+b\sqrt{-1})$. 由于 $(a+b\sqrt{-1})+(a-b\sqrt{-1}) \Rightarrow (p, 2a)$

$= \mathbb{Z}[\sqrt{-1}]$ ($p\neq 2$, $(p,2a)=1$) 由 CRT 知

$$\mathbb{Z}[\sqrt{-1}]/(p) = \mathbb{Z}[\sqrt{-1}]/(a+b\sqrt{-1}) \times \mathbb{Z}[\sqrt{-1}]/(a-b\sqrt{-1})$$

由同态基本定理知

$$\mathbb{Z}[\sqrt{-1}]/(p) \cong \mathbb{Z}[x]/(x^2+1) \Big/ p\left(\mathbb{Z}[x]/(x^2+1)\right)$$

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

$$\cong \mathbb{F}_p[x]/(x^2+1) \cong \mathbb{F}_p[\sqrt{-1}].$$

由此 $\left|\mathbb{Z}[\sqrt{-1}]/(a+b\sqrt{-1})\right|\left|\mathbb{Z}[\sqrt{-1}]/(a-b\sqrt{-1})\right| = \left|\mathbb{F}_p[\sqrt{-1}]\right| = |\mathbb{F}_p|^2$

由 i 是域嵌入知 $\left|\mathbb{Z}[\sqrt{-1}]/(a\pm b\sqrt{-1})\right| = p$. □

Ex3. 证明. $\mathbb{Z}[\sqrt{-3}]/(2) \cong \mathbb{F}_2[x]/(x^2+1)$

证明. $\mathbb{Z}[\sqrt{-3}]/(2) \cong \mathbb{Z}[x]/(x^2+3) \Big/ 2\left(\mathbb{Z}[x]/(x^2+3)\right)$

$$\cong \mathbb{Z}[x]/(x^2+3) \Big/ \left((2),(x^2+3)\right)/(x^2+3)$$

$$\cong \mathbb{Z}[x]/(2) \Big/ \left((2),(x^2+3)\right)/(2)$$

$$\cong \mathbb{F}_2[x]/(x^2+1)$$ □

Ex4 $c \in R$, 证明. $R[x]/(c) \cong R/(c)[x]$.

思路. 由自然同态, $R \xrightarrow{\varphi} R/(c)$ 诱导了环同态,

$$R[x] \xrightarrow{\bar{\varphi}} R/(c)[x].$$

利用 φ 是满的推出 $\bar{\varphi}$ 是满的. 再求出 $\ker \bar{\varphi}$, 最后用同态基本定理.

注意! Ex2 和 Ex3 均用了这个结论.

Ex5. $A = k[x,y]/(y^3-x^2)$ 为整环，找出 A 的 k-基，A 是 UFD 吗？

思路. $\sum := \{\bar{x}^i\bar{y}^j \mid i=0,1; j\in\mathbb{N}\}$ 是 A 的 k-基. 在 $k[y][x]$ 上做带余除法，易知 $\forall f\in A$ 可由 $\sum$ k-线性表出. 设

$$\sum_{i=0}^{1}\sum_{j=0}^{\infty} a_{ij}\bar{x}^i\bar{y}^j = 0$$

则有

$$\sum_{i=0}^{1}\sum_{j=0}^{\infty} a_{ij}x^iy^j = (y^3-x^2)\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} b_{ij}x^iy^j$$

对比 x^i 的系数，$b_{ij}=0$，从而 $a_{ij}=0$. 因此 $\sum$ 是 A 的 k-基.

考虑 $u=\bar{x}^2=\bar{y}^3\in A$. 若 A 是 UFD，则 $\bar{y}\mid\bar{x}$，从而

$$x = yf(x,y) + (y^3-x^2)g(x,y)$$

对比度数，$f(x,y)=0$，$g(x,y)=0$，从而 $x=0$，矛盾. 因此 A 不是 UFD □

Ex6. 求证. $\sigma: \mathbb{Z}[x]\to\mathbb{Z}[x]$，$f(x)\mapsto f(x+1)$ 为环同构.

思路. 说明 $\forall a\in\mathbb{Z}$，$\sigma_a: \mathbb{Z}[x]\to\mathbb{Z}[x]$，$f(x)\mapsto f(x+a)$ 为环同态，由于 $\sigma_a\circ\sigma_{-a} = \sigma_{-a}\circ\sigma_a = id_{\mathbb{Z}[x]}$，$\sigma_a$ 是同构.

或者：说明 σ_a 是双射，利用第二次作业 Ex9 说明 σ_a 是同构！

□

Ex7. 将 x^n-1 $(3\le n\le 10)$ 在 $\mathbb{Z}[x]$ 中作素因子分解.

解. 1° $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+1)$, $p=2,3,5,7$ (p 为素数).

2° $x^4-1=(x-1)(x+1)(x^2+1)$

3° $x^6-1=(x^3-1)(x^3+1)=(x-1)(x^2+x+1)(x+1)(x^2-x+1)$

($x^3+1=-[(-x)^3-1]$, 利用 1°)

4° $x^8-1=(x^4-1)(x^4+1)=(x-1)(x+1)(x^2+1)(x^4+1)$

($(x+1)^4+1=x^4+4x^3+6x^2+4x+2$ 不可约)

5° $x^9-1=(x^3-1)(x^6+x^3+1)=(x-1)(x^2+x+1)(x^6+x^3+1)$

($(x+1)^6+(x+1)^3+1=x^6+6x^5+15x^4+21x^3+18x^2+9x+3$ 不可约)

6° $x^{10}-1=(x^5-1)(x^5+1)=-(x^5-1)((-x)^5-1)$

$=(x-1)(x+1)(x^4+x^3+\cdots+1)(x^4-x^3+\cdots+1)$ □

(要说明是素因子(不可约)分解!)

Ex8. 设 D 是整环, $f(x)\in D[x]$, $c\in D$, $g(x)=f(x+c)\in D[x]$

求证:

(1) $f(x)$ 在 $D[x]$ 中本原 $\Leftrightarrow$ $g(x)$ 在 $D[x]$ 中本原;

(2) $f(x)$ 在 $D[x]$ 中不可约 $\Leftrightarrow$ $g(x)$ 在 $D[x]$ 中不可约.

注记. 类似于 Ex6, 记映射 $\forall c\in D$, $\sigma_c: D[x]\to D[x]$, $f(x)\mapsto f(x+c)$ 是同构. 则有 $c(f)=1\Leftrightarrow c(g)=1$, $f(x)$ 不可约 $\Leftrightarrow$ $g(x)$ 不可约.

□

Ex1. 设 $\theta: k \hookrightarrow K \ni \alpha$

$\theta': k \hookrightarrow K' \ni \phi(\alpha)$ 域扩张

其中 $K \xrightarrow{\phi} K'$, $\phi \cdot \theta = \theta'$

证. α 在 k 上代数 $\Leftrightarrow \phi(\alpha)$ 也是. 此时 α 和 $\phi(\alpha)$ 的极小多项式一样!

证. 若 α 在 k 上代数, 设其极小多项式为 $f(x)=\sum_{i=0}^{n} a_i x^i$. 则 $f(\alpha)=\sum_{i=0}^{n} a_i \alpha^i=0$, 从而 $\sum_{i=0}^{n} a_i \phi(\alpha)^i=0$, 即 $f(x)$ 也是 $\phi(\alpha)$ 的零化多项式.

设 $g(x)$ 为 $\phi(\alpha)$ 的极小多项式, 则 $g(x) \mid f(x)$. 因于 ϕ 是同构, 同理可得 $f(x) \mid g(x)$. 因此 $f(x)=g(x)$. □

Ex2 设 F/K 为域的扩张, $u \in F$ 是 K 上的奇次代数元素. 求证 $K(u)=K(u^2)$.

证. 由于 x^2-u^2 是 u 在 $K(u^2)$ 上的零化多项式, $[K(u):K(u^2)] \le 2$

而 $[K(u):K(u^2)] \mid [K(u):K]$, $[K(u):K(u^2)]=1$.

另证: 显然 $K(u^2) \subseteq K(u)$. 设 u 在 K 上的极小多项式为 $f(x)=\sum_{i=0}^{2k+1} a_i x^i$, 即 $f(u)=\sum_{i=0}^{2k+1} a_i u^i=0$. 则 $u\sum_{j=0}^{k} a_{2j+1} u^{2j}=\sum_{l=0}^{k} a_{2l} u^{2l}$

即 $u \in K(u^2)$. 因此 $K(u) \subseteq K(u^2)$ □.

Ex3. 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 $F \neq K(x_1, x_2)$.

解. 取 $K=\mathbb{Q}$，$u=x$，$v=x^{-1}$. 则 $F=\mathbb{Q}(x, x^{-1})=\mathbb{Q}(x)$. 则 $F \neq K(x_1, x_2)$. 用反证法. 由于 $K=\mathbb{Q}$，若 $\varphi: \mathbb{Q}(x) \to \mathbb{Q}(x_1, x_2)$ 是同构，则必是 $\mathbb{Q}$-不变的. 因此只需考虑 x 的像. 设 $u=\varphi(x)$. 则 $\mathbb{Q}(u)=\mathbb{Q}(x_1, x_2)$. u 在 $\mathbb{Q}(x_1)$ 上是代数的(利用 Ex12). 而 $x_2 \in \mathbb{Q}(u)$，x_2 在 $\mathbb{Q}(u)$ 上是代数的，因此 x_2 在 x_1 上是代数的. 矛盾. 因此 $F \neq K(x_1, x_2)$.

Ex4. 设p为素数，分别求扩张$\mathbb{Q}(e^{\frac{2\pi i}{p}})/\mathbb{Q}$和$\mathbb{Q}(e^{2\pi i/8})/\mathbb{Q}$的次数. (用到了第2次作业Ex7的结论).

解: $e^{\frac{2\pi i}{p}}$在$\mathbb{Q}$上的零化多项式为$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$，其为$\mathbb{Q}$上的不可约多项式. 因此$[\mathbb{Q}(e^{\frac{2\pi i}{p}}):\mathbb{Q}]=p-1$. $e^{2\pi i/8}$在$\mathbb{Q}$上的不可约零化多项式是$f(x)=x^4+1$因此$[\mathbb{Q}(e^{2\pi i/8}):\mathbb{Q}]=4$. □

Ex5. 求元素α在域K的极小多项式，其中

(1) $\alpha=\sqrt{2}+\sqrt{3}$, $K=\mathbb{Q}$;

(2) $\alpha=\sqrt{2}+\sqrt{3}$, $K=\mathbb{Q}(\sqrt{2})$;

(3) $\alpha=\sqrt{2}+\sqrt{3}$, $K=\mathbb{Q}(\sqrt{6})$;

解. 设α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). $\deg f(x)=[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$.

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) $\deg f(x)=[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$. 而

$x^2-2\sqrt{2}x-1$是$\sqrt{2}+\sqrt{3}$的零化多项式. 故$f(x)=x^2-2\sqrt{2}x-1$.

(3) 同理$f(x)=x^2+2\sqrt{6}-5$.

(这里利用了Ex9，也可先证这个，再来证Ex9)

Ex6. 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：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 $g(x)|f(x)$，而 $f(x)|g(x)$，因此 $f(x)=g(x)$.

反之. 设 $g(x)$ 为 u 在 K 上的极小多项式. 则 $g(x)|f(x)$. 而 $K[x]$ 是 UFD，$g(x)=f(x)$.

注. "⇒" 利用 $K[x]/(f(x))\cong K(u)$，和 $f(x)$ 不可约.

Ex7. 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 $m|n$，求 u^m 在域 K 的的极小多项式.

解. 设 u^m 的极小多项式为 $f(x)$. 则 $f(x)|x^{n/m}-a$. 而 $f(x^m)$ 是 u 的零化多项式，因此 $x^n-a|f(x^m)$. 故 $x^{n/m}-a|f(x)$. 因此 $f(x)=x^{n/m}-a$. □.

Ex8. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}\omega^2)$ (可以尝试先证Ex10再证Ex8)

$\neq \mathbb{Q}(\sqrt[3]{2})$ $\neq \mathbb{Q}(\sqrt[3]{2}\omega)$.

证明. 由于 $\mathbb{Q}(\sqrt[3]{2}\omega^2) \not\subseteq \mathbb{R}$, $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, $\mathbb{Q}(\sqrt[3]{2}\omega^2) \neq \mathbb{Q}(\sqrt[3]{2})$.

若 $\mathbb{Q}(\sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}\omega)$, 则 $\mathbb{Q}(\sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega^2)$. 从而 $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}\omega^2)$. 即 $[\mathbb{Q}(\sqrt[3]{2}\omega^2):\mathbb{Q}]=3$ 且 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}\omega^2)$. 矛盾.

Ex9. $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证: 显然 $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. 而 $\frac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$,

因此 $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. 因此 $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Ex10. $x^3-2 \in \mathbb{Q}(\omega)[x]$ 不可约.

思路1. 若 $x^3-2 \in \mathbb{Q}(\omega)[x]$ 可约, 则必有一次因式, 从而有根. 而 x^3-2 的根有 $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ 和 $\sqrt[3]{2}\omega^2$. 因此只需证 $\mathbb{Q}(\omega) \neq \mathbb{Q}(\omega, \sqrt[3]{2}) (= \mathbb{Q}(\omega, \sqrt[3]{2}\omega) = \mathbb{Q}(\omega, \sqrt[3]{2}\omega^2))$, 若 $\mathbb{Q}(\omega) = \mathbb{Q}(\omega, \sqrt[3]{2})$, 则类似于Ex8, 导出矛盾.

思路2. 若 x^3-2 可约, 则 x^3-2 在 $\mathbb{Q}(\omega)$ 上有根. 设 $a+b\omega$ 为 x^3-2 的根, $a,b \in \mathbb{Q}$, 则 $(a+b\omega)^3 = 2$ 得 $a^3+3a^2b\omega+3ab^2\omega^2-b^3 = 2$,

即 $(a^3+b^3-2-3ab^2)+(3a^2b-3ab^2)\omega = 0$. 从而

$$\begin{cases} a^3+b^3-2-3ab^2=0 \\ 3a^2b-3ab^2=0 \end{cases} \Rightarrow \begin{cases} a=0 \\ b=\sqrt[3]{2}\omega, \end{cases} \begin{cases} b=0 \\ a=\sqrt[3]{2}\omega \end{cases} \text{或 } a=b=-\sqrt[3]{2}\omega.$$

因此 $x^3-2 \in \mathbb{Q}(\omega)[x]$ 不可约. (进而可以证明Ex8).

思路3. 说明2在 $\mathbb{Z}[\omega]$ 中不可约, 再利用Eisenstein判别法.

思路4. 利用Ex15.

Ex11 $\mathbb{Q}\subseteq\mathbb{C}$, $\overline{\mathbb{Q}}=\{\alpha\in\mathbb{C}\mid\alpha$ 在 $\mathbb{Q}$ 上代数$\}$. 证 $\overline{\mathbb{Q}}$ 是代数闭的.

证: $\forall f(x)\in\overline{\mathbb{Q}}[x]$, $f(x)$ 在 $\mathbb{C}[x]$ 上完全分裂, 即 $f(x)=\prod_{i=1}^{n}(x-a_i)$.

而 $f(x)\in\overline{\mathbb{Q}}[x]$, 故 $a_i\in\overline{\overline{\mathbb{Q}}}$ $(1\le i\le n)$. 而 $\overline{\mathbb{Q}}$ 在 $\mathbb{Q}$ 上代数, $\mathbb{Q}$ 在 $\mathbb{Q}$ 上代数, 我们知道 $\overline{\mathbb{Q}}$ 在 $\mathbb{Q}$ 上代数, 即 $\overline{\overline{\mathbb{Q}}}\subseteq\overline{\mathbb{Q}}$. 因此 $a_i\in\overline{\mathbb{Q}}$, 即 $f(x)$ 在 $\overline{\mathbb{Q}}[x]$ 上完全分裂.

Ex12 设 K 是域, $u\in K(x)$, $u\notin K$, 求证 x 在域 $K(u)$ 上代数.

证 由条件知 $u=\dfrac{\sum_{i=0}^{n}a_ix^i}{\sum_{j=0}^{m}b_jx^j}$, 其中 $a_nb_m\neq0$, $m+n>0$. 从而

$\sum_{i=0}^{n}a_ix^i-u\left(\sum_{j=0}^{m}b_jx^j\right)=0$, 由于 $u\in K(x)\setminus K$, 可以知道左边多项式不为零多项式. 因此 x 在 $K(u)$ 上代数.

Ex13 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.

(1)证. 利用 Eisenstein 判别法, 知 x^3-6x^2+9x+3 不可约 $(p=3)$.

则 $[\mathbb{Q}(u):\mathbb{Q}]=3$.

(2). 略.

Ex 14. 设 $u=x^3/(x+1)$，求问 $[\mathbb{Q}(x):\mathbb{Q}(u)]=?$

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 $\mathbb{Q}[u]/(u)\cong\mathbb{Q}$，即 u 是不可约元，由 Eisenstein 判别法，$f(y)$ 在 $\mathbb{Q}[u][y]$ 中不可约（$p=y$）. 从而在 $\mathbb{Q}(u)[y]$ 上不可约. 故 $[\mathbb{Q}(x):\mathbb{Q}(u)]=3$.

Ex 15. 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 $[FE:K]\le mn$;

(2) 如果 $(m,n)=1$，则 $[FE:K]=mn$.

(1) 证：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 $[FE:E]\le\deg f=m$.

因此 $[FE:K]=[FE:E][E:K]\le mn$.

(2) $m=[F:K]\mid[FE:K]\ (=[FE:F][F:K])$. 同理，$n\mid[FE:K]$

由于 $(m,n)=1$，$mn\mid[FE:K]$. 而 $[FE:K]\le mn$，$[FE:K]=mn$.

Ex 1. $f: R \xrightarrow{\sim} R'$ 环同构, $I \lhd R$, 则 f 诱导同构 $R/I \xrightarrow{\sim} R'/f(I)$.

证明: $f(R) = R'$, $I = f^{-1}(f(I))$, 由第三次作业 Ex 4, f 诱导了同构 $R/I \xrightarrow{\sim} R'/f(I)$.

注. 这里 $S = R'$, $J = f(I)$

Ex 2. $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$, $\mathbb{F}_9' = \mathbb{F}_3[x]/(x^2-x-1)$, $\mathbb{F}_9'' = \mathbb{F}_3[x]/(x^2+x-1)$

证明 $\mathbb{F}_9 \cong \mathbb{F}_9' \cong \mathbb{F}_9''$.

证明 $f: \mathbb{F}_3[x] \to \mathbb{F}_3[x]$, $\varphi(x) \mapsto \varphi(x+1)$ 显然是环同构 (第二次作业 Ex 8). 而 $f(x^2+1) = (x+1)^2 + 1 = x^2 - x - 1$, 由 Ex 1 得 $\mathbb{F}_9 \cong \mathbb{F}_9'$. 令 $g: \mathbb{F}_3[x] \to \mathbb{F}_3[x]$, $\varphi(x) \mapsto \varphi(x-1)$, 同理得 $\mathbb{F}_9 \cong \mathbb{F}_9''$

Ex 3. $\mathrm{Aut}(\mathbb{F}_9) = \mathrm{Aut}(\mathbb{F}_9/\mathbb{F}_3)$.

证明. 显然 $\mathrm{Aut}(\mathbb{F}_9/\mathbb{F}_3) \subseteq \mathrm{Aut}(\mathbb{F}_9)$. $\forall \sigma \in \mathrm{Aut}(\mathbb{F}_9)$, $\sigma(1) = 1$ 故 $\sigma(\mathbb{F}_3) = \mathbb{F}_3$, $\sigma \in \mathrm{Aut}(\mathbb{F}_9/\mathbb{F}_3)$.

Ex 4. 证 $x^p - t \in \mathbb{F}_p(t)[x]$ 不可约.

证明. 注意到 $\mathbb{F}_p[t]$ 是 UFD, $x^p - t$ 是 $\mathbb{F}_p[t]$ 上的本原多项式, 也是 $\mathbb{F}_p[t]$ 中的素元 ($\mathbb{F}_p[t]/(t) \cong \mathbb{F}_p$), 即为不可约元, 由 Eisenstein 判别法知 $x^p - t$ 在 $\mathbb{F}_p[t][x]$ 不可约, 从而在 $\mathbb{F}_p(t)[x]$ 上不可约.

Ex5. $\mathbb{F}_2[x]$ 中，求 $x^{16}-x$ 的素因子分解.

思路. $\mathbb{F}_q[x]$ 中，$x^{q^n}-x=\prod_{d\mid n}\prod f(x)$，其中 $q=p^m$，p 素数，f 是 $\mathbb{F}_q$ 内中所有 d 次不可约多项式

$$x^{16}-x=x(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1) \quad (*)$$

对于 $g(x)=x^2+x+1$，$g(0)=g(1)\neq 0$，即无根，从而不可约.

而 $x^2+1=(x+1)^2$，x^2 明可约，$x^{16}-x$ 的次数小于2而因子又有3个，进而有3个次数为4而不可约因子，即对于 $f(x)=\sum_{i=0}^{4}a_ix^i$，要使 $f(x)$ 不可约，$a_0=a_4=1$. 因为无根，$f(1)=a_1+a_2+a_3=1$

从而 $f(x)=x^4+x^3+x^2+x+1$，x^4+x^3+1，x^4+x^2+1（备注，$x^4+x^2+1=(x^2+x\pm 1)^2$ 可约）或 x^4+x+1. 共3个，因此 $(*)$ 为不可约分解.

Ex6. $d_1,d_2\mid n$，求证 $E_{d_1}\cap E_{d_2}=E_{(d_1,d_2)}$.

思路. $a\in E_{d_1}\cap E_{d_2}\iff \sigma^{d_i}(a)=a$，$i=1,2$

$\iff \sigma^{(d_1,d_2)}=\sigma^{k_1d_1+k_2d_2}(a)=a$，$k_1,k_2\in\mathbb{Z}$

（$\Leftarrow$ 显然，$\Rightarrow$ 由 Bézout 定理）.

$\iff a\in E_{(d_1,d_2)}$

Ex 1 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，其它元素阶均为 8.

思路 $\mathrm{ord}(\bar{1})=1$, $\mathrm{ord}(\bar{2})=2$, $\mathrm{ord}(u)=\mathrm{ord}(\bar{2}u)=4$.

可直接计算得其它元素阶均为 8（暴算！）

也可利用 $\mathbb{F}_9^*$ 是 8 阶循环群，故有 $\varphi(8)=4$ 个 8 阶元，故其它元素阶均为 8.

Ex 2 构造一个 8 元域，并写出它的加法表和乘法表.

思路 $\mathbb{F}_2[x]$ 上，$x^{2^3}-x=x(x+1)(x^3+x+1)(x^3+x^2+1)$. 由于 x 和 $x+1$ 是 $\mathbb{F}_2[x]$ 的所有不可约多项式，x^3+x+1, x^3+x^2+1 不可约（也可利用无根判断不可约）. 因此可构造 8 元域 $\mathbb{F}_2[x]/(x^3+x+1)$ 或 $\mathbb{F}_2[x]/(x^3+x^2+1)$.

Ex 3 列出 $\mathbb{F}_2$ 上全部次数 ≤ 4 的不可约多项式，列出 $\mathbb{F}_3$ 上全部 2 次不可约多项式.

思路 由 Ex 3 知 $\mathbb{F}_2$ 上次数为 1 和 3 的不可约多项式.

由 $x^{2^2}-x=x(x+\bar{1})(x^2+x+\bar{1})$ 知 2 次不可约多项式只有一个

由 $x^{2^4}-x=x(x+\bar{1})(x^2+x+\bar{1})(x^4+x^3+x^2+x+\bar{1})$

$(x^4+x^3+\bar{1})(x^4+x+\bar{1})$

知 4 次不可约多项式有 3 个.

由 $x^{3^2}-x=x(x+\bar{1})(x+\bar{2})(x^2+\bar{1})(x^2+x+\bar{2})(x^2+\bar{2}x+\bar{2})$.

知所有次数 ≤ 2 的不可约多项式

Ex4 设 $f(x)$ 是 $\mathbb{F}_p[x]$ 中首1不可约多项式

(1) 若 u 为 $f(x)$ 的一个根，则 $f(x)$ 共有 n 个彼此不同的根，并且它们为 $u, u^p, u^{p^2}, \cdots, u^{p^{n-1}}$;

(2) 若 $f(x)$ 的一个根 u 为域 $\mathbb{F}=\mathbb{F}_p(u)$ 的乘法循环群 $\mathbb{F}^*=\mathbb{F}-\{0\}$ 的生成元，则 $f(x)$ 的多个根也是 $\mathbb{F}^*$ 的生成元;

定义. 如果 $f(x)$ 的根 u 是 $\mathbb{F}_p(u)$ 的乘法群的生成元，我们称 $f(x)$ 为 $\mathbb{F}_p[x]$ 中 n 次本原多项式.

(3) 证明 $\mathbb{F}_p[x]$ 中 n 次本原多项式共有 $\varphi(p^n-1)/n$ 个，其中 $\varphi(n)$ 是欧拉函数.

解. (1) 由于 $f(x)$ 是 $\mathbb{F}_p[x]$ 中首一不可约多项式，$\mathbb{F}_p[u] \cong \mathbb{F}_p[x]/(f(x))$ 是 $q=p^n$ 元域. 由定理1 (P123)，我们有 Frobenius 自同构

$$\sigma_p : \mathbb{F}_p[u] \longrightarrow \mathbb{F}_p[u]$$
$$a \longmapsto a^p$$

是 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

$$\sum_{i=0}^{n} a_i (\sigma_p^j(u))^i = \sigma_p^j\left(\sum_{i=0}^{n} a_i u^i\right) = 0, \ \forall j>0,$$ 即 $\sigma_p^j(u)=u^{p^j}$ 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，$\langle \sigma_p^i(u) \rangle$ 也是 $\mathbb{F}_p^*[u]$ 的生成元.

(3) 由(2)知，一个本原多项式有 n 个 $F_{p^n}=\{x\mid x^{p^n}-x=0\}$ 的乘法除 m 域元. 由于 $F_{p^n}^*$ 有 $\varphi(p^n-1)$ 个生成元，$F_{p^n}^*$ 的本原多项式有 $\varphi(p^n-1)/n$ 个.

Ex5. $\forall \zeta\in\mu_n$，素数 $p\nmid n$. 若 $f(\zeta)=0$，假设 $f(\zeta^p)\neq 0$，令 ζ^p 在 $\mathbb{Q}[x]$ 中的极小多项式为 $g(x)$，且 $g(x)$ 为 $\mathbb{Z}[x]$ 中本原多项式. 设 $x^n-1=f(x)g(x)h(x)$，则 $h(x)\in\mathbb{Q}[x]$，证明 $h(x)\in\mathbb{Z}[x]$.

思路：反复论 Ex6 (x^n-1 本原多项式).

Ex6. $f(x)$，$g(x)$ 是 $\mathbb{Z}[x]$ 中本原多项式. 若在 $\mathbb{Q}[x]$ 中 $f(x)\mid g(x)$. 证明：$\mathbb{Z}[x]$ 中也有 $f(x)\mid g(x)$.

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，$h'(x)f(x)=\frac{g(x)}{a}$ 本原. 因此 $a=\pm 1$. 因此在 $\mathbb{Z}[x]$ 上，$f(x)\mid g(x)$.

Ex7. $\forall a\in G$，$n,m\in\mathbb{Z}$. 证明 $a^{n+m}=a^n\cdot a^m$

思路：分类讨论. 与第一次作业 $(m+n)a=ma+na$ 的证明相同.

Ex8. 求正方形的对称群 $\Sigma(\square)$ 中4个对称映射的变换矩阵.

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

Ex9. 证明有理数加法群 $\mathbb{Q}$ 和非零有理数乘法群 $\mathbb{Q}^*$ 不同构.

证明：假设 $\varphi:\mathbb{Q}\to\mathbb{Q}^*$ 是同构. 则 $\exists a\in\mathbb{Q}$，s.t. $\varphi(a)<0$. 而 $\varphi(a)=\varphi(\frac{a}{2})\varphi(\frac{a}{2})>0$，矛盾. 因此 $(\mathbb{Q},+)\not\cong(\mathbb{Q}^*,\cdot)$.

Ex10. 证明：若 $\{a_i \mid i\in I\}$ 是 G 的右陪集代表元系，则 $\{a_i^{-1} \mid i\in I\}$ 是左陪集代表元系.

证明. $G=\bigsqcup_{i\in I} Ha_i$. $\forall g\in G$, $g^{-1}\in G$. 故 $\exists i\in I$, $h\in H$, s.t. $g^{-1}=ha_i$,

则 $g=a_i^{-1}h^{-1}\in a_i^{-1}H$. 因此 $G=\bigcup_{i\in I} a_i^{-1}H$. 由于

$$Ha_i=Ha_j \Leftrightarrow a_ia_j^{-1}\in H \Leftrightarrow (a_i^{-1})^{-1}a_j^{-1}\in H \Leftrightarrow a_i^{-1}H=a_j^{-1}H,$$

$\{a_i^{-1} \mid i\in I\}$ 是左陪集代表元系

Ex11. 证明：$\forall a\in G$, $f(a^{-1})=(f(a))^{-1}$ ($f: G\to G'$ 是群同态)

思路. $1_{G'}=f(1_G)=f(a^{-1})f(a)$

Ex12. 若 $f: G\to G'$ 是群同构，证明 $f^{-1}: G'\to G$ 是群同态.

思路. 考虑 $f^{-1}(f(a)f(b))$, $f^{-1}(f(1))$.

Ex13. $(-)^{-1}: G\xrightarrow{1:1} G$, $g\mapsto g^{-1}$. 证明：$(-)^{-1}$ 是同态 $\Leftrightarrow$ G 是Abel群

思路. $(-1)^{-1}$ 同态 $\Leftrightarrow$ $g_1^{-1}g_2^{-1}=(g_1g_2)^{-1}\Leftrightarrow g_1g_2=g_2g_1\Leftrightarrow G$ 是Abel群

Ex14. $G\times H=\{(g,h) \mid g\in G, h\in H\}$. 证明

$$\mathrm{ord}(g,h)=\mathrm{lcm}(\mathrm{ord}(g),\mathrm{ord}(h)).$$

思路. 令 $m=\mathrm{ord}(g)$, $n=\mathrm{ord}(h)$, $k=\mathrm{ord}(g,h)$, $g^m=1_G$, $h^n=1_H$

$\Rightarrow (g,h)^{\mathrm{lcm}(m,n)}=1\Rightarrow k\mid \mathrm{lcm}(m,n)$.

另一方面. $g^k=1$, $h^k=1$. 有 $m\mid k$, $n\mid k$, 故 $\mathrm{lcm}(m,n)\mid k$.

Ex15. $V_4=\{(1,1),(1,-1),(-1,1),(-1,-1)\}$. 证明 $V_4\cong U(\mathbb{Z}_8)$.

思路 记 $e=(1,1)$, $a=(1,-1)$, $b=(-1,1)$, $c=(-1,-1)$.

利用乘法表验证 $\varphi: V_4\to U(\mathbb{Z}_8)$, 其中 $\varphi(e)=\bar{1}$, $\varphi(a)=\bar{3}$, $\varphi(b)=\bar{5}$, $\varphi(c)=\bar{7}$, 是同态. 而 φ 是双射, 从而是同构.

Ex16. 证明 $\mathbb{C}^*$ 不是循环群.

思路 若 $\mathbb{C}^*$ 是循环群, 则 $\mathbb{C}^*\overset{\varphi}{=}\mathbb{Z}$, 从而 φ 是双射. 而 $\mathbb{Z}$ 可数, $\mathbb{C}^*$ 不可数, 矛盾.

Ex17. 设 A,B 是群 G 的两个子群. 试证:

$$AB\leq G \Leftrightarrow AB=BA$$

证明: "$\Rightarrow$" $AB\leq G$. 则 $\forall ab\in AB$, 由于 $a^{-1}\in A$, $b^{-1}\in B$, $a^{-1}b^{-1}\in AB$, 从而 $b^{-1}a^{-1}\in AB$ ($a^{-1}b^{-1}a^{-1}b^{-1}\in AB$). 故 $\exists a_1,b_1\in AB$, s.t. $b^{-1}a^{-1}=a_1b_1$. 因此 $ab=b_1^{-1}a_1^{-1}\in BA$. 故 $AB\subseteq BA$.

另一方面, $\forall ba\in BA$, $ab\in AB$. 从而 $ba\in AB$ ($abab\in AB$).

"$\Leftarrow$" $\forall a_1b_1,a_2b_2\in AB$, $a_1b_1(a_2b_2)^{-1}=a_1b_1b_2^{-1}a_2^{-1}=a_1[(b_1b_2^{-1})a_2^{-1}]$

$=a_1[a_3b_3]\in AB$. 故 $AB\leq G$.

Ex18. 设 a,b 是群 G 的任意两个元素, 试证 a 和 a^{-1}, ab 和 ba 有相同阶.

证明: 设 $ord(a)=n$, $ord(a^{-1})=m$. 则 $a^n=1$. 而 $a^na^{-n}=1$, $a^{-n}=1$, 从而 $m\mid n$. 而 $a=(a^{-1})^{-1}$, 同理得 $n\mid m$. 因此 $m=n$.

设 $ord(ab)=n$, $ord(ba)=m$. 则 $a(ba)^nb=(ab)^{n+1}=ab$ 从而 $(ba)^n=1$. 因此 $m\mid n$. 同理 $n\mid m$. 因此 $m=n$.

Ex19 试证：有理数加群$\mathbb{Q}$不是循环群，但它的任意有限生成的群都是循环群。

证明：用反证法，假设$\mathbb{Q}$是循环群，则$\exists \frac{p}{q}\in\mathbb{Q}$，$p,q>0$互素，s.t. $\mathbb{Q}=\langle\frac{p}{q}\rangle$.

1° $q=1$，则$\mathbb{Q}=p\mathbb{Z}$，显然不可能.

2° $q>1$，则$\frac{p}{q^2}\notin\langle\frac{p}{q}\rangle$，矛盾.

因此$\mathbb{Q}$不是循环群.

设$H=\langle\frac{q_1}{p_1},\cdots,\frac{q_n}{p_n}\rangle$是$\mathbb{Q}$的任意给定的有限生成群

则$H\leq\langle\frac{1}{p}\rangle$，其中$p=p_1\cdots p_n$. 因此$H$是循环群.

Ex20 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：设H是G的真子群，则$|H|<\infty$. 否则$\forall N>0$，$\exists n\geq N$，s.t. $x^{p^n}=1$的所有根（是一个循环群）在H中，从而$x^{p^k}=1$ $k\leq n$的所有根在H中. 因此$\forall N>0$，$x^{p^N}=1$所有根在H中. 因此$G\subseteq H$，即$G=H$，矛盾.

由上面讨论知H的形式为$K_n=\{x\mid x^{p^n}=1\}$，而K_n是循环群. 因此H是循环群.

Ex1. $N \trianglelefteq G$, 证明存在群同构 $\theta: N \simeq aNa^{-1}$, $\forall a \in G$.

思路. 验证双射和同态即可. □

Ex2. $N \trianglelefteq G$, 群同态 $f: G \to H$, $N \subseteq \ker f$. 构造同态 $\tilde{f}: G/N \to H$, $\tilde{f}(aN) = f(a)$ $(\forall a \in G)$. 证明 $\tilde{f}$ 良定.

证明. 若 $aN = bN$, 则 $ab^{-1} \in N \subseteq \ker f$, 从而 $f(ab^{-1}) = e_H$

$$\tilde{f}(aN) = f(a) = f(b) = \tilde{f}(bN).$$ □

Ex3. 令 G 是实数对 (a,b), $a \neq 0$ 带有乘法

$$(a,b)(c,d) = (ac, ad+b)$$

试证: $K = \{(1,b) \mid b \in \mathbb{R}\}$ 是 G 的正规子群且 $G/K \cong \mathbb{R}^*$

证明. 构造映射

$$\varphi: G \to \mathbb{R}^*$$

$$(a,b) \mapsto a$$

显然是满射, 由于 $\varphi((a,b)(c,d)) = ac = \varphi((a,b))\varphi((c,d))$,

φ 是同态. 而 $\forall (a,b) \in \ker\varphi$, $a = \varphi((a,b)) = 1$. 故 $\ker\varphi \subseteq K$

$\forall (1,b) \in K$, $\varphi((1,b)) = 1$. 故 $K \subseteq \ker\varphi$. 因此

$K = \ker\varphi$ 是正规子群且 $G/\ker\varphi \cong \mathbb{R}^*$. □

另证. 因为 $\forall (a,b) \in G$, $(a,b)(1,0) = (a,b)$, 知 $e_G = (1,0)$

易知 $(a,b)^{-1} = (a^{-1}, -a^{-1}b)$

$\forall (1,a), (1,b) \in K$

$$(1,a)(1,b)^{-1} = (1,a)(1,-b) = (1, a-b) \in K.$$

因此 $K \leq G$. 而 $\forall (1,b) \in K$, $\forall (c,d) \in G$.

$$(c,d)(1,b)(c,d)^{-1}=(c,cb+d)(c^{-1},-c^{-1}d)$$
$$=(1,cb)\in K$$

故 $K\trianglelefteq G$. 构造映射 $\varphi: G\to \mathbb{R}^*, (a,b)\mapsto a$. 显然是满射. 由于 $\varphi((a,b)(c,d))=ac=\varphi((a,b))\varphi((c,d))$, φ 是同态. 而 $\forall (a,b)\in\ker\varphi$, $a=\varphi((a,b))=1$. 故 $\ker\varphi\subseteq K$. 从而 $K=\ker\varphi$. 由同态基本定理, $G/K\cong\mathbb{R}^*$

Ex4. 若 $[G:N]=2$, 则 $N\trianglelefteq G$.

证明. 由于 $[G:N]=2$, G 有陪集分解 $G=N\sqcup aN=N\sqcup Na$.

$(N\neq Na\Leftrightarrow a\notin N\Leftrightarrow N\neq aN)$. 从而 $aN=Na$. □

Ex5. 设 $f: G\to H$ 是群同态, $M\leq G$. 试证 $f^{-1}(f(M))=KM$, 这里 $K=\ker f$

证明. 由于 $f(K)=\{e\}$. $f(KM)=f(M)$. 故

$$f^{-1}(f(M))=f^{-1}(f(KM))\supseteq KM.$$

$\forall a\in f^{-1}(f(M))$, $f(a)\in f(M)$. 故 $\exists b\in M$, s.t. $f(a)=f(b)$. 故 $ab^{-1}\in\ker f=K$. 从而 $\exists k\in K$, s.t. $ab^{-1}=k$. 即 $a=kb\in KM$. 从而 $f^{-1}(f(M))\subseteq KM$.

Ex 6. 设 M 和 N 分别是群 G 的正规子群. 若 $M\cap N=\{1\}$, 则

$\forall a\in M, b\in N$, $ab=ba$.

证明. 由于 $M\trianglelefteq G$, $bab^{-1}\in M$, 从而 $bab^{-1}a^{-1}\in M$. 同理

$bab^{-1}a^{-1}\in N$. 于是 $bab^{-1}a^{-1}\in M\cap N=\{1\}$. 于是 $ab=ba$. □

Ex 7. 设 $f: G\to H$ 是群同态. 若 $|g|<\infty$, $g\in G$, 则 $|f(g)|\,\big|\,|g|$.

证明. 设 $|g|=n$. 则 $g^n=1_G$. 从而 $(f(g))^n=f(g^n)=1_H$. 因

此 $|f(g)|\,\big|\,|g|$.

Ex 8. 若 $G/C(G)$ 是循环群, 则 G 是阿贝尔群.

证明. 设 $G/C(G)=\langle\bar a\rangle$, 其中 $\bar a\in G/C(G)$. $\forall g_1, g_2\in G$,

$\exists m_1, m_2\geq 0$, s.t. $\bar g_1=\bar a^{m_1}$, $\bar g_2=\bar a^{m_2}$. 从而 $\exists c_1, c_2\in$

$C(G)$, s.t. $g_1=a^{m_1}c_1$, $g_2=a^{m_2}c_2$. 于是

$$g_1g_2=a^{m_1+m_2}c_1c_2=a^{m_2+m_1}c_2c_1=g_2g_1.$$

因此 G 是 Abel 群.

Ex9 $N \triangleleft G$

$$\{K \mid N \le K \le G\} \overset{1:1}{\Longleftrightarrow} \{G\text{的子群}\}$$

$$f_1: \quad K \longmapsto K/N$$

$$\{g \in G \mid gN \in K'\} \longleftarrow K' \quad : f_2$$

证明 f_1, f_2 互逆.

思路. 类似于泡妹的对应定理.

我们有自然同态

$$\varphi: G \twoheadrightarrow G/N$$

则我们有 $f_1(K) = \varphi(K)$. $f_2(K') = \varphi^{-1}(K')$.

Ex10. 若 $K/N \triangleleft G/N$, 证明 $K \triangleleft G$

证明. 由Ex9, 我们知有子群间的一一对应

$$\{K \mid N \le K \le G\} \underset{f_2}{\overset{f_1}{\rightleftarrows}} \{G\text{的子群}\}.$$

若 $K/N \triangleleft G/N$, 则 $f_1(K) = g f_1(K) g^{-1} = f_1(gKg^{-1})$. 因此

$K = gKg^{-1}$. 即 $K \triangleleft G$.

Ex11. 讨论置换

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ n & n-1 & \cdots & 1\end{pmatrix}$$

的奇偶性.

思路 1° $n=2k+1$, $\sigma=(1n)(2,n-1)\cdots(k,k+1)$

则分为两种情况

1) $k=2l$, 此时σ为偶置换, 此时 $n=4l+1$

2) $k=2l+1$, 此时σ为奇置换, 此时 $n=4l+3$

2° $n=2k$, $\sigma=(1n)(2,n-1)\cdots(k-1,k+1)$

则分为两种情况

1) $k=2l$, 此时σ为奇置换, 此时 $n=4l$

2) $k=2l+1$, 此时σ为偶置换 此时 $n=4l+2$.

因此 $n=4l$ 和 $4l+3$ 时为奇置换, $n=4l+1$ 和 $4l+2$ 时为偶置换.

Ex12. 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.

思路. 由第八次作业 Ex14.

Ex13. 试确定 S_4 的全部正规子群.

解. S_4 的所有共轭类:

$[1^4]$: 1个　　$[2^2]$: 3个

$[1^2 2^1]$: 6个　　$[4^1]$: 6个.

$[1^1, 3^1]$: 8个

设 $K \lhd S_4$. 则 $|K| \mid |S_4|$, 从而 $|K| = 1, 2, 3, 4, 6, 8, 12, 24$

由于正规子群在共轭作用下不变, 所以 K 是 S_4 的共轭类之和. 从而 $|K|$ 可以取得的数只有 1, 4, 12, 24

1° $|K| = 1$ 和 24 时 K 为平凡正规子群.

2° $|K| = 12$ 时, $K = A_4 \lhd S_4$

3° $|K| = 4$ 时, $K = K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$

验证知 K_4 是子群 (零验证). 而 K 在共轭作用下不变, 从而 $K_4 \lhd S_4$.

因此 S_4 的正规子群有 $\{1\}$, K_4, A_4 和 S_4.

Ex14. 试证 A_4 没有 6 阶子群

证明. 若 A_4 有 6 阶子群 H, 则 $[A_4 : H] = 2$ (Lagrange 定理)

从而 H 是 A_4 的正规子群 (Ex4). A_4 的型有 $[1^4]$, $[1^1 3^1]$

和$[2^2]$. 计算知A_4的共轭类有

1° $[1^4]$型: 1个

2° $[2^2]$型: 3个.

3° $[1^1 3^1]$型不同一部分: 4个

4. $[1^1 3^1]$型不同其余部分: 4个.

因此没有6阶(正规)子群.

综上, 当$n\geq 3$时, $C(S_n)=\{1\}$.

思路: $C(S_n)\triangleleft S_n$

1° $n=3$时, S_3的正规子群共有$\{1\}$, A_3, S_3.

由$[S_3:A_3]=2$知, $C(S_3)\neq A_3$ (由Ex8)

同理 $C(S_3)\neq S_3$. 故$C(S_3)=\{1\}$

2° $n=4$时, S_4的正规子群共有$\{1\}$, A_4, K_4, S_4. (Ex13)

类似于1°知$C(S_4)\neq A_4, S_4$. 由于

$$((12)(34))(13)((12)(34))^{-1}=(24)\neq(13)$$

知$C(S_4)\neq K_4$. 因此$C(S_4)=\{1\}$.

3° $n\geq 5$时, S_n的正规子群共有$\{1\}$, A_5, S_5. 类似于1°

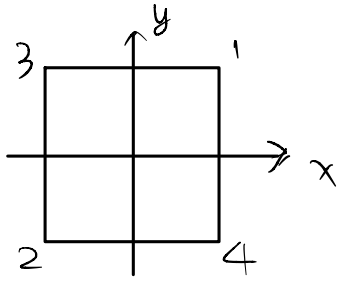
知$C(S_n)=\{1\}$.

另: 也可利用$\tau(a_1\cdots a_m)\tau^{-1}=(\tau(a_1)\cdots\tau(a_m))$来验证.

Ex1. $H=\{Id, (1234), (13)(24), (1432), (14)(23), (12)(34), (13), (24)\}$

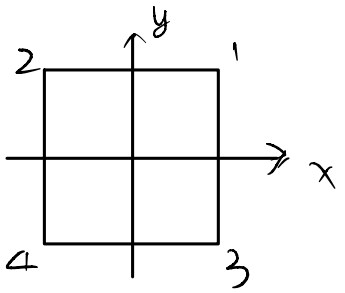
(1) 证明 H 由 $(1234), (13)$ 生成

(2)



算 $\Sigma(\square) \hookrightarrow S_4$ 的像.

(3)



算 $\Sigma(\square) \hookrightarrow S_4$ 的像.

证明. (1) 因 $(1234), (13) \in H$ 知 $\langle (1234), (13) \rangle \subseteq H$. 因 $|\langle (1234) \rangle| = 4$ 且 $(13) \notin \langle (1234) \rangle$ 知 $|\langle (1234), (13) \rangle| > 4$. 由 Lagrange 定理知 $|\langle (1234), (13) \rangle| \mid |H| = 8$. 知 $|\langle (1234), (13) \rangle| = 8$. 因此 $\langle (1234), (13) \rangle = H$

(2) 因 (1) 知 $\Sigma\left(\begin{smallmatrix} 2 & 1 \\ 3 & 4 \end{smallmatrix}\right) \cong \langle (1234), (13) \rangle \subseteq S_4$.

则 $\Sigma\left(\begin{smallmatrix} \sigma(2) & \sigma(1) \\ \sigma(3) & \sigma(4) \end{smallmatrix}\right) \cong \langle (\sigma(1)\sigma(2)\sigma(3)\sigma(4)), (\sigma(1)\sigma(3)) \rangle$. 从而

$$\Sigma\left(\begin{smallmatrix} 3 & 1 \\ 2 & 4 \end{smallmatrix}\right) \cong \langle (1324), (12) \rangle \subseteq S_4$$

(3) 同理, $\Sigma\left(\begin{smallmatrix} 2 & 1 \\ 4 & 3 \end{smallmatrix}\right) \cong \langle (1243), (14) \rangle \subseteq S_4$.

Ex2 求所有$\sigma \in S_3$使得$(12)=\sigma(13)\sigma^{-1}$

解 $(12)=\sigma(13)\sigma^{-1}=(\sigma(1)\sigma(3))$ 因此有

$$\begin{cases}\sigma(1)=1\\ \sigma(3)=2\end{cases} \text{ 或 } \begin{cases}\sigma(1)=2\\ \sigma(3)=1\end{cases}$$

故 $\sigma=(23)$ 或 (123)

Ex3 G是Abel群，证明：G是单群 $\Leftrightarrow$ G是p阶循环群(p是素数)

证明 "$\Leftarrow$"显然

"$\Rightarrow$" G Abel $\Rightarrow \forall N \trianglelefteq G$ 都是正规子群.

G是单群 $\Rightarrow$ G的子群只有平凡子群.

取 $1\neq a\in G$. 则 $\langle a\rangle \subseteq G$ 从而 $\langle a\rangle = G$.

若 $|a|=\infty$, $a\notin\langle a^2\rangle \Rightarrow \langle a^2\rangle \subsetneq \langle a\rangle \Rightarrow \langle a^2\rangle = \{1\}$ 矛.

Ex4 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $n!/\prod_{i=1}^{n}\lambda_i!\,i^{\lambda_i}$ 个，由此

证明

$$\sum_{\substack{\lambda_i\geq 0\\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}} \frac{1}{\prod_{i=1}^{n}\lambda_i!\,i^{\lambda_i}}=1$$

证明 对任意 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 型置换 σ，均可写以下的式

$$\sigma=\underbrace{(a_1)\cdots(a_{\lambda_1})}_{\lambda_1\text{个}}\underbrace{(a_{\lambda_1+1}a_{\lambda_1+2})\cdots(a_{\lambda_1+2\lambda_2-1}a_{\lambda_1+2})}_{\lambda_2\text{个}}\cdots\cdots$$

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 轮中，$(b_1b_2\cdots b_i)=(b_2b_3\cdots b_ib_1)=\cdots=(b_ib_1\cdots b_{i-1})$，故 σ 的个数共有 $\dfrac{n!}{\prod_{i=1}^{n}\lambda_i!\,i^{\lambda_i}}$ 个. 由于不同型的元素不在同一等价类，因此：

$$\sum_{\substack{\lambda_i\geq 0\\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}} \frac{n!}{\prod_{i=1}^{n}\lambda_i!\,i^{\lambda_i}}=n!$$

从而

$$\sum_{\substack{\lambda_i\geq 0\\ \lambda_1+2\lambda_2+\cdots+n\lambda_n=n}} \frac{1}{\prod_{i=1}^{n}\lambda_i!\,i^{\lambda_i}}=1$$

Ex5 求所有 $\sigma\in A_3$, s.t. $\sigma(123)\sigma^{-1}=(132)$

解 $(132)=\sigma(123)\sigma^{-1}=(\sigma(1)\sigma(2)\sigma(3))$. 因此有

$$\begin{cases}\sigma(1)=1\\ \sigma(2)=3\\ \sigma(3)=2\end{cases}\text{ 或 }\begin{cases}\sigma(1)=3\\ \sigma(2)=2\\ \sigma(3)=1\end{cases}\text{ 或 }\begin{cases}\sigma(1)=2\\ \sigma(2)=1\\ \sigma(3)=3\end{cases}$$

故 $\sigma=(23),(13)$ 或 (12). 从而不存在 $\sigma\in A_3$, s.t. $\sigma(123)\sigma^{-1}=(132)$.

Ex6. X 是 G-集, $\rho: G\to S(X)$, $g\mapsto \rho(g)$. 其中

$$\rho(g): X\to X,\quad x\mapsto g\cdot x$$

验证 ρ 是群同态.

解. $\forall g,h\in G$, $\forall x\in X$

$$\rho(gh)(x)=(gh)\cdot x=g\cdot(h\cdot x)=\rho(g)(\rho(h)(x))$$

故 $\rho(gh)=\rho(g)\rho(h)$. 即 $\rho: G\to S(X)$ 是群同态.

Ex7. 对群 G 定义反群 G^{op}: $x*y=yx$. 证明 G^{op} 是群且 G 与 G^{op} 同构.

证明 1° $1_{G^{op}}=1_G$

2° $\forall x\in G^{op}$, x^{-1} 仍为 x 在 G^{op} 上的逆.

3° $\forall x,y,z\in G^{op}$,

$$x*(y*z)=(zy)x=z(yx)=(x*y)*z.$$

故 $(G^{op},*)$ 是群.

构造 $G\xrightarrow{\varphi}G^{op}$, $x\mapsto x^{-1}$. 验证 $\forall x,y\in G$, 恒有

$$\varphi(xy)=\varphi(x)*\varphi(y)$$

即可.

Ex 8. 定义 G 右作用于 X 上 (X^G) 为

$$\phi: X \times G \to X, (x, g) \mapsto x \cdot g$$

① $x \cdot 1_G = x$. ② $(x \cdot g)h = x(g \cdot h)$ $\forall x \in X, g, h \in G$

从中中找出群同态 $G \to S(X)^{op}$

反之由群同态也可以得出作用 ϕ

思路 构造

$$\psi: G \to S(X)^{op}$$
$$g \mapsto \psi(g): X \to X$$
$$x \mapsto x \cdot g.$$

验证 $\forall g, h \in G, x \in X$, $\psi(gh)(x) = \psi(g) * (\psi(h)(x))$ 即可.

反之, 若有群同态,

$$\psi: G \to S(X)^{op}$$
$$g \mapsto \psi(g): X \to X$$
$$x \mapsto x \cdot g.$$

不合适

$$\phi: X \times G \to X$$
$$(x, g) \mapsto x \cdot g = \psi(g)h$$

验证 ① ② 即可.

Ex9. $H \leq G$, $H\backslash G = \{Ha \mid a \in G\}$, 构造 $(H\backslash G) \curvearrowleft G$

思路 构造

$$H\backslash G \times G \longrightarrow H\backslash G$$

$$(Ha, g) \longmapsto Hag.$$

幂验证①②(Ex8).

Ex10. $f(x) \in k[x]$, $k \subseteq E$ 是 $f(x)$ 的分裂域

$$f(x) = (x-u_1)\cdots(x-u_n) \in E[x],\ E = k(u_1, \cdots, u_n)$$

$$Aut(E/k) \curvearrowright Root_E(f) = \{u_1, \cdots, u_n\}$$

$$\theta: Aut(E/k) \hookrightarrow S(\{u_1, \cdots, u_n\}) = S_n$$

$$\sigma \longmapsto \sigma|_{\{u_1, \cdots, u_n\}}$$

验证 θ 是单同态.

证明 由 $Aut(E/k) \curvearrowright Root_E(f)$ 和 θ 是同态

$\forall \sigma \in \ker\theta$, $\sigma|_k = id$, $\sigma|_{\{u_1, \cdots, u_n\}} = id$. 由关键引理和 σ

由 $\{u_1, \cdots, u_n\}$ 的任意性唯一确定, 知 $\sigma = id_E$. 因此 $\ker\theta = \{id\}$, 即 θ 是单同态.

Ex11. $GL_2(\mathbb{F}_2)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|\ \begin{matrix}a,b,c,d\in\mathbb{F}_2\\ ad-bc=\bar{1}\end{matrix}\right\}$

$\mathbb{F}_2^2=\left\{\begin{pmatrix}a\\b\end{pmatrix}\middle|\ a,b\in\mathbb{F}_2\right\}$

$GL_2(\mathbb{F}_2)\curvearrowright\mathbb{F}_2^2\setminus\left\{\begin{pmatrix}\bar{0}\\\bar{0}\end{pmatrix}\right\}\triangleq X$，写出σ使得 $GL_2(\mathbb{F}_2)\cong S_3$

思路：记 $x_1=\begin{pmatrix}1\\0\end{pmatrix}$，$x_2=\begin{pmatrix}0\\1\end{pmatrix}$，$x_3=\begin{pmatrix}1\\1\end{pmatrix}$. 构造

$$\phi: GL_2(\mathbb{F}_2)\times X\longrightarrow X$$

$$\left(\begin{pmatrix}a&b\\c&d\end{pmatrix},\begin{pmatrix}x\\y\end{pmatrix}\right)\longmapsto\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$$

则φ是群作用（这是由矩阵乘法所得）

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}x_1=\begin{pmatrix}a\\c\end{pmatrix}=\begin{cases}x_1, & a=1,\ c=0\\ x_2, & a=0,\ c=1\\ x_3, & a=1,\ c=1\end{cases}$$

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}x_2=\begin{pmatrix}b\\d\end{pmatrix}=\begin{cases}x_1, & b=1,\ d=0\\ x_2, & b=0,\ d=1\\ x_3, & b=1,\ d=1.\end{cases}$$

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}x_3=\begin{pmatrix}a+b\\c+d\end{pmatrix}=\begin{cases}x_1, & a+b=1,\ c+d=0\\ x_2, & a+b=0,\ c+d=1\\ x_3, & a+b=1,\ c+d=1.\end{cases}$$

这诱导了群同态 $\psi: GL_2(\mathbb{F}_2)\longrightarrow S_3$，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 $\mathrm{Im}\psi \supseteq \langle (12),(13)\rangle = S_3$. 从而 ψ 是满射. 而 $|S_3|=6$ $=|GL_3(\mathbb{F}_2)|$. 故 ψ 是单的. □

Ex 12. 构造非满同态 $S_4 \twoheadrightarrow S_3$

证明: 考虑 S_4 在其3阶集 $[2^2]$ 上的共轭作用

$$\phi: S_4 \times [2^2] \longrightarrow [2^2]$$
$$(\tau,\sigma) \longmapsto \tau\sigma\tau^{-1}$$

因为 $[2^2]$ 是 S_4 的一个共轭元素类, ϕ 是良好的定义的. 因此诱导了一个非平凡同态 $\psi: S_4 \to S_3$.

记 $x_1=(23)(14)$, $x_2=(13)(24)$, $x_3=(12)(34)$. 则 $\psi((12))=(12)$ ($\psi((12))x_1=x_2$, $\psi((12))x_2=x_1$). 同理, $\psi((13))=(13)$. 从而 $\mathrm{Im}\psi \supseteq \langle (12),(13)\rangle = S_3$. 从而 $\mathrm{Im}\psi = S_3$.

Ex 13. 定义共轭作用 $G \curvearrowright G$, 验证它是左作用.

思路: 定义 $G\times G \xrightarrow{\phi} G$, $(g,h)\longmapsto g\cdot h = ghg^{-1}$, 验证下列事件即可:

① $(gg')\cdot h = g\cdot(g'\cdot h)$, $\forall g,g',h\in G$

② $1\cdot h = h$, $\forall h\in G$

Ex1. $\Sigma(\square)=\{1,\tau,\tau^2,\tau^3,\sigma,\tau\sigma,\tau^2\sigma,\tau^3\sigma\}$，验证：

$$Z(\Sigma(\square))=\{Id,\tau^2\}.$$

解. 由于 $\forall\ \tau^i\sigma^j,\ \tau^k\sigma^l\in\Sigma(\square)$，$i,k=0,1,2,3$，$j,l=0,1$.

$$\tau^i\sigma^j(\tau^k\sigma^l)(\tau^i\sigma^j)^{-1}=\tau^i(\sigma^j\tau^k\sigma^j)\sigma^l\tau^{-i}$$

$$=\tau^i\tau^{(-1)^jk}\tau^{-(-1)^li}\sigma^l$$

1° 当 $k=0,2$ 时，上式 $=\tau^{i+k-(-1)^li}\sigma^l$，则 $\tau^k\sigma^l\in Z(\Sigma(\square))$

$\Leftrightarrow l=0$，此时 $\tau^k\sigma^l=Id$ 或 τ^2.

2° 当 $k=1,3$ 时，上式 $=\tau^{i-k-(-1)^li}\sigma^l\neq\tau^k\sigma^l$，否则，

$2k=i-(-1)^li\pmod 4$，若 $l=1$，则 $2k\equiv 2i\pmod 4$

矛盾（即 $i=0$ 或 2）.

综上，$Z(\Sigma(\square))=\{Id,\tau^2\}$.

Ex2. 令 $H=\langle g\rangle$, $K=\langle g'\rangle$, $H, K \cong \mathbb{Z}_p$. 验证

$$\phi: H\times K \longrightarrow G$$
$$(g^i, g'^j) \longmapsto g^i g'^j$$

是同态

证明.

Ex3. 设 G 作用在集合 Σ 上，对任意 $a, b \in \Sigma$，若存在 $g \in G$, s.t. $ga = b$，则 $G_a = g^{-1} G_b g$. 换句话说，同一轨道中元素的固定子群彼此共轭.

证明. $h \in G_a \Leftrightarrow ha = a \Leftrightarrow hg^{-1}ga = g^{-1}ga$

$\Leftrightarrow ghg^{-1}(ga) = ga \Leftrightarrow ghg^{-1}b = b$

$\Leftrightarrow ghg^{-1} \in G_b \Leftrightarrow h \in g^{-1}G_b g$.

Ex 4. 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 作用下的每个轨道有同样多的元素.

证明. $\forall a, b \in \Sigma$，由于 G 在 Σ 上的作用是传递的，$\exists g \in G$, s.t. $b = ga$，由 Ex 3 知 $G_b = gG_ag^{-1}$. 而

$$N_b = N \cap G_b = N \cap gG_ag^{-1} = gNg^{-1} \cap gG_ag^{-1} = gN_ag^{-1}$$

从而 $N(b) = [G : N_b] = [G : gN_ag^{-1}] = [G : N_a] = N(a)$

注意：这里 $|G|$ 可能不是有限的！

Ex 5. 设 p 是 $|G|$ 的最小素因子. 若 p 阶子群 $A \lhd G$, 则 $A \leq C(G)$.

记图用考虑共轭作用

$$\psi: G \times A \to A$$
$$(g, a) \longmapsto gag^{-1}$$

这诱导了同态

$$\varphi: G \longrightarrow S(A)$$
$$g \longmapsto \varphi(g): A \to A$$
$$a \longmapsto gag^{-1}$$

由于 $\forall g \in G$, $\varphi(g)$ 是 A 上的自同构 ($\ker \varphi(g) = \{e\}$, $|A| < \infty$)

因此 $\mathrm{Im}\,\varphi$ 的每个元素均由 A 的生成元决定, 从而 $\mathrm{Im}\,\varphi \cong \mathbb{Z}_{p-1}$

($|A| = p \Rightarrow A = \langle a \rangle$). 因此 $|\mathrm{Im}\,\varphi| = (p-1)$ 而 $\forall e \neq g \in G$, $|\varphi(g)| \mid |g| \geq p$. 故 $|\varphi(g)| = 1$, 从而 $|\varphi(G)| = 1$. 即 ψ 是平凡的. 从而 $A \leq C(G)$.

Ex6. $\langle K_4, (13)\rangle$, $\langle K_4, (12)\rangle$, $\langle K_4, (14)\rangle$ 两两不同!

证明. 若 $\langle K_4, (13)\rangle = \langle K_4, (12)\rangle$, 则 $(12)(13) \in \langle K_4, (13)\rangle$, 从而 $|(12)(13)| \mid 8$. 而 $|(12)(13)| = 3$, 矛盾. 同理 $\langle K_4, (13)\rangle \neq \langle K_4, (12)\rangle$. 同理可证, 这三个群两两不同.

Ex7 分析 S_3 的情况.

解. $|S_3|=6$. S_3 的非平凡子群只有3阶子群和2阶子群.

由 Sylow 定理知 S_3 的 Sylow 3-子群个数在且个数 r 满足

$$r\equiv 1 \pmod 3 \text{ 且 } r\mid 2$$

解得 $r=1$. 即 S_3 只有一个 Sylow 3-子群 A_3.

Sylow 2-子群个数 r, 满足

$$r\equiv 1 \pmod 2 \text{ 且 } r\mid 3$$

故 $r=1$ 或 3. 若 $r=1$, 则 S_3 的 Sylow 2-群只有一个, 从而是正规子群, 矛盾. 因此 S_3 的 Sylow 2-子群有3个, 分别为 $\langle(12)\rangle$, $\langle(13)\rangle$ 和 $\langle(23)\rangle$.

Ex8 G Abel. $|G| = p_1^{s_1} \cdots p_r^{s_r}$, p_i 素. 则

(1) $\exists!\ P_i \leq G$, $|P_i| = p_i^{s_i}$

(2) $\psi: P_1 \times P_2 \times \cdots \times P_r \xrightarrow{\sim} G$

$(h_1, h_2, \cdots, h_r) \longmapsto h_1 h_2 \cdots h_r$

是同构

验证: ψ 是同态.

Ref

Ex9 Fact: $H \leq A$. 设 $P \subseteq A$ Sylow p-子群. $|A| = p^s \cdot m$. 则 $\exists g \in A$, s.t.

$$gPg^{-1} \cap H \text{ 是 } H \text{ 的 Sylow } p\text{-子群}$$

证明: Fact $\Rightarrow$ (2) A 的 Sylow p-子群彼此共轭;

(4) 设 P 是 A 的一个 Sylow p-子群, 则 A 的 Sylow p-子群的个数为 $[A : N_A(P)]$.

证明. (2) 设 P, P' 是任意给定的 A 的 Sylow p-子群. 则由 Fact 知, $\exists g \in A$, s.t.

$$gPg^{-1} \cap P' \text{ 是 } P' \text{ 的 Sylow } p\text{-子群}$$

而 P' 的 Sylow p-子群是自身. 因此 $gPg^{-1} \cap P' = P'$. 故 $gPg^{-1} \supseteq P'$. 同理 $\exists h \in G$, s.t. $hP'h^{-1} \supseteq P$. 故

$$hgPg^{-1}h^{-1} \supseteq hP'h^{-1} \supseteq P$$

从而 $|P| = |hgPg^{-1}h^{-1}| \geq |hP'h^{-1}| \geq |P|$.

因此 $P = hP'h^{-1}$, 即 P 与 P' 共轭.

(4) 取 $\Sigma = \{gPg^{-1} \mid g \in A\}$, 考虑作用

$$A \times \Sigma \longrightarrow \Sigma, \ (h, gPg^{-1}) \longrightarrow hgPg^{-1}h^{-1}$$

则 $|\Sigma| = [A : A_p] = [A : N_A(P)]$. $(N_A(P) \triangleq A_p)$.

引理 设 G 是一个 n 阶群，p 是 n 的一个素因子。则方程 $x^p=1$ 在群 G 中解的个数是 p 的倍数。

证明 若 $x\in G$，满足 $x^p=1$，则 $\langle x\rangle$ 是 p 阶循环群。不同的循环子群非空且两两不交，而 p 阶群的个数为 $N(p)\equiv 1 \pmod p$，从而 $x^p=1$ 在群 G 中解的个数是

$$N(p)(p-1)+1\equiv 0 \pmod p$$

即为 p 的倍数。

Ex 11. 设阶200的群G一定含有一个正规的Sylow子群.

证明 $200 = 2^3 \times 5^2$. 故G只有Sylow 2-子群和Sylow 5-子群

由Sylow定理2, Sylow 5-子群的个数 r 满足

$$\begin{cases} r \equiv 1 \pmod 5 \\ r \mid 8 \end{cases}$$

解得, $r = 1$. 故G有一个正规的Sylow子群.

Ex 12. 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 Sylow p-子群.

证明 由 Ex 9 的 Fact 知, 对任意 G 的 Sylow p-子群 P, $\exists g \in G$, s.t.

$$gPg^{-1} \cap N \text{ 是 } N \text{ 的 Sylow } p\text{-子群}.$$

而 $(p, |G/N|) = 1$, $gPg^{-1} \cap N = gPg^{-1}$. 从而 $gPg^{-1} \subseteq N$. 从而 $P \subseteq g^{-1}Ng = N$. 因此 N 包含 G 的所有 Sylow p-子群.

Ex 5. 设 G 是论素的一个有限群，N 是 G 的正规子群，P 是 G 的一个 Sylow p-子群 试证：

(1) $N\cap P$ 是 N 的 Sylow p-子群；

(2) PN/N 是 G/N 的 Sylow p-子群；

(3) $N_G(P)N/N \cong N_{G/N}(PN/N)$

证明：(1) 由Ex 9的Frattini，$\exists g\in G$，s.t. $N\cap gPg^{-1}$ 是 N 的 Sylow p-子群. 因为 $N\cap P = g^{-1}(N\cap gPg^{-1})g$ 是 N 的 Sylow p-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 Sylow p-子群.

(3) $\forall gN\in N_G(P)N/N$，$g^{-1}Pg = P$. 视在 G/N 上，有 $(gN)^{-1}(PN/N)(gN) = PN/N$. 故 $gN\in N_{G/N}(PN/N)$. 因为 $N_G(P)N/N \subseteq N_{G/N}(PN/N)$. $\forall gN\in N_{G/N}(PN/N)$ $(gN)^{-1}(PN/N)(gN) = PN/N$，则 $g^{-1}pg\in PN$，$\forall p\in P$. 视 $g^{-1}Pg\subseteq PN$. 因为 $g^{-1}Pg$ 和 P 均为 PN 的 Sylow p-子群 从而 $\exists p\in P$，$n\in N$，s.t. $(np)^{-1}g^{-1}Pgnp = P$ ($N\lhd G$). 因为 $(gn)^{-1}P(gn) = P$. 因为 $g\in N_G(P)n^{-1}\subseteq N_G(P)N$

Ex14. 设 P 是 G 的 Sylow p-子群，且 $N_G(P)$ 是 G 的正规子群. 证明 P 是 G 的正规子群.

证明. 由于 $P \subseteq N_G(P)$，$|G/N_G(P)|$ 与 P 互素，而 $N_G(P)$ 包含所有的 Sylow p-子群(Ex12). 而 $P \lhd N_G(P)$，且 Sylow p-子群共有一个. 从而 $P \lhd G$.

定理 任意字可约化为唯一的既约字.

证明: 设由非空集合 X 所成的所有既约字组成的集合是 Ω.

$\forall x \in X$, 定义

$$\sigma_x : \Omega \longrightarrow \Omega,\ w \longmapsto \overline{x}w,\ \forall w \in \Omega$$

因为 w 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

$$\sigma_u \triangleq \sigma_{x_1}^{n_1} \sigma_{x_1}^{n_2} \cdots \sigma_{x_t}^{n_t}.$$

令

$$H = \{\sigma_w \mid w \in \Omega\}$$

则 H 对于置换的乘法成为一个群, 并且如果一个字 u 化简成既约字 w, 则 $\sigma_u = \sigma_w$.

设同一个字 u 用两种不同的方式化简成既约字 w_1, w_2, 则根据上述, 有 $\sigma_{w_1} = \sigma_u = \sigma_{w_2}$. 因为 σ_{w_1} 把空字映成 w_1, σ_w 把空字映成 w_2. 因此 $w_1 = w_2$ □

(参见丘维声. 抽象代数基础(第二版). P76–77).

Ex1 证明

$$N(r_1, r_2, \cdots, r_m) = \left\langle \left\{ w r_i w^{-1} \;\middle|\; \begin{matrix} 1 \le i \le m \\ w \in F(x_1, \cdots, x_n) \end{matrix} \right\} \right\rangle$$

证明. 记 $N' = \left\langle \left\{ w r_i w^{-1} \;\middle|\; \begin{matrix} 1 \le i \le m \\ w \in F(x_1, \cdots, x_n) \end{matrix} \right\} \right\rangle$. $N = N(r_1, \cdots, r_m)$

因为 $N \lhd F(x_1, \cdots, x_n)$, $w r_i w^{-1} \in N$, $\forall w \in F(x_1, \cdots, x_n)$.

因此 $N' \subseteq N$. $\forall y \in N'$, $\forall v \in F(x_1, \cdots, x_n)$, 有 $y = w x w^{-1}$,

从而 $v(wxw^{-1})v^{-1} = (vw)x(vw)^{-1} \in N'$. 因此 $N' \lhd F(x_1, \cdots, x_n)$

由 N 的定义, $N \subseteq N'$. 因此 $N = N'$.

Ex 2. 证明: $N(a^2, b^2, (ab)^3) = N(a^2, b^2, abab^{-1}a^{-1}b^{-1})$ in $F(a,b)$.

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 $N' \lhd F(a,b)$, $b(abab^{-1}a^{-1}b^{-1}b^2)b^{-1} = babab^{-1}a^{-1} \in N'$

重复这个步骤, 得 $(ba)^3 \in N'$. 因此 $(ab)^3 = a(ba)^3a^{-1} \in N'$.

因此 $N \subseteq N'$. 类似地, 可证明 $N' \subseteq N$. 因此 $N = N'$.

Ex3. 如果n为正奇数，求证 $D_{2n} \cong D_n \times \mathbb{Z}_2$.

证明. $D_n = \langle a, b \mid a^n = b^2 = (ab)^2 = 1 \rangle$, $\mathbb{Z}_2 = \langle c \mid c^2 = 1 \rangle$

我们有自然满同态(因n是奇数得)

$$F(x, y) \xrightarrow{\pi} D_n \times \mathbb{Z}_2,$$

其中 $\pi(x) = (a, c)$, $\pi(y) = (b, c)$. 显然 $N(x^n, y^2, (xy)^2) \subseteq \ker \pi$. 因此诱导了满同态 $D_{2n} \xrightarrow{\pi} D_n \times \mathbb{Z}_2$. 而 $\#(D_{2n}) = 4n$, $\#(D_n \times \mathbb{Z}_2) = 2n \times 2 = 4n$. 因此 π 是单射. 从而

$$D_{2n} \cong D_n \times \mathbb{Z}_2$$

Ex4. 若 $n\geq 3$，试问 $A_n\times \mathbb{Z}_2$ 与 S_n 是否同构？

证明 $n=3$ 时，由第十一次作业 Ex7 和 S_3 只有一个非平凡正规子群 A_3. 此时 $A_3\times\mathbb{Z}_2$ 有2个非平凡正规子群 A_3 和 $\mathbb{Z}_2$

$n=4$ 时，由第九次作业 Ex3 和 S_4 的非平凡正规子群只有 A_4 和 K_4，没有与 $\mathbb{Z}_2$ 同构的正规子群.

$n\geq 5$ 时，S_n 的非平凡正规子群只有 A_n，没有与 $\mathbb{Z}_2$ 同构的正规子群.

因此 $A_n\times\mathbb{Z}_2\not\cong S_n$.

另证. 利用 Ex6，$C(A_n\times\mathbb{Z}_2)=C(A_n)\times C(\mathbb{Z}_2)\supseteq\mathbb{Z}_2$.

而 $C(S_n)=\{1\}$. 故 $S_n\not\cong A_n\times\mathbb{Z}_2$.

事实上 S_n 是 A_n 与 $\langle(12)\rangle$ 的半直积.

Ex5. 设 G_1, G_2, G_3 为群，则

(1) $G_1 \times G_2 \cong G_2 \times G_1$

(2) $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$

直接构造映射 φ 可.

直积在范畴 $\mathcal{C}$ 上的定义

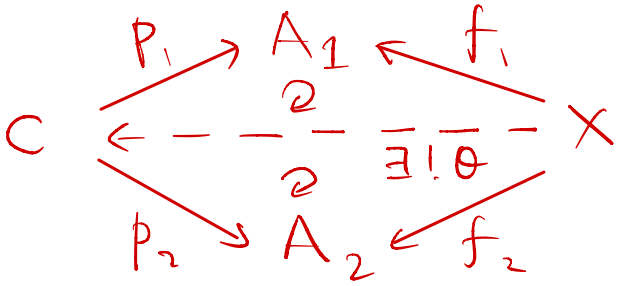
$A_i \in Obj(\mathcal{C})$, $i \in I$. 则它们的直积为 (C, p_i), 其中

$p_i : C \to A_i$, s.t. $\forall X \in Obj(\mathcal{C})$, $f_i \in Mor_{\mathcal{C}}(X, A_i)$

$\exists! \theta : X \to C$, s.t. $p_i \theta = f_i$, $\forall i \in I$. 即有如下交换图:

此时记 $C = \prod_{i \in I} A_i$ (参见 Rotman, An introduction to Homological Algebra. P221).

特殊情况, $I = \{1, 2\}$.



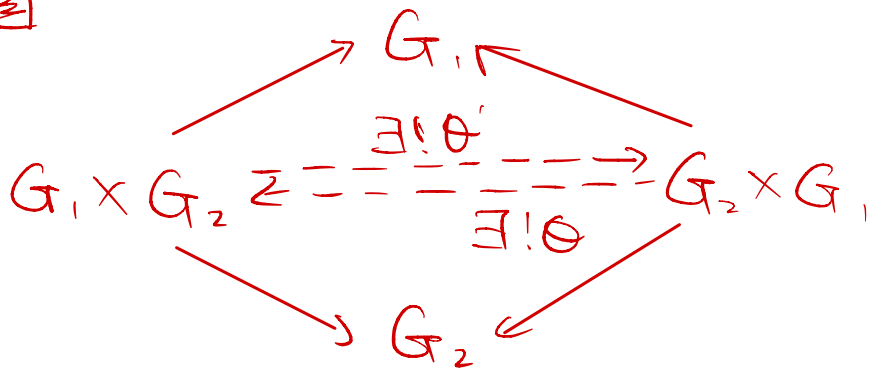
这是直积的范性质.

本题 $\mathcal{C}=$ Groups, $Obj(\mathcal{C})=\{$所有的群$\}$. $\forall G_1, G_2 \in Obj\,\mathcal{C}$, $Mor_{\mathcal{C}}(G_1, G_2)=\{G_1$到$G_2$的所有群同态$\}$. 现验证: $G_1\times G_2$是G_1和G_2的直积.

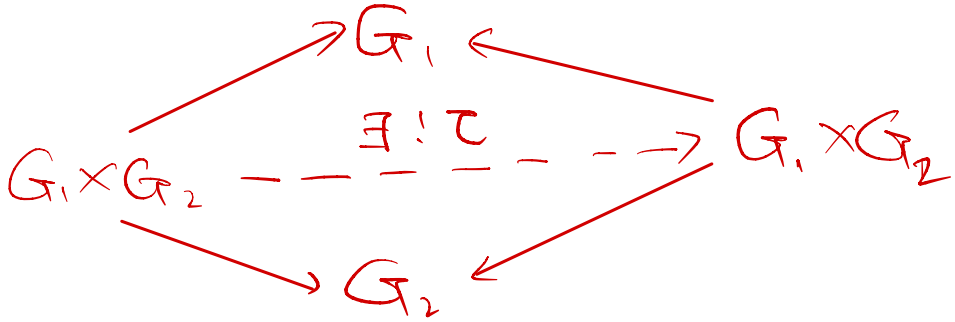
任意给定群G, 群同态 $f_i: G\longrightarrow G_i$, $i=1,2$.

定义 $\theta: G\longrightarrow G_1\times G_2$, $g\longmapsto (f_1(g), f_2(g))$. 容易验证$\theta$是群同态, 且 $p_i\theta=f_i$, $\forall i=1,2$. 由于$\theta(g)$由$f_1(g)$和$f_2(g)$决定, 因此可以看为θ被唯一确定.

同样地, 可以证明$G_2\times G_1$是G_2和G_1的直积. 则有以下交换图



考虑



可知 $id=\tau=\theta\theta'$. 同理, $id=\theta'\theta$. 因此θ是同构.

类似地, 可以证明$(G_1\times G_2)\times G_3\cong G_1\times(G_2\times G_3)$.

Ex6 设 $G_i\ (1\le i\le n)$ 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 $\Leftrightarrow G_i$ 为 Abel 群, $\forall i$.

证明 (1) $(g_1,\cdots,g_n)\in C(G_1\times G_2\times\cdots\times G_n)$,

$\Leftrightarrow (g_1,\cdots,g_n)(h_1,\cdots,h_n)=(h_1,\cdots,h_n)(g_1,\cdots,g_n)$

$\forall (h_1,\cdots,h_n)\in G_1\times G_2\times\cdots\times G_n$

$\Leftrightarrow g_ih_i=h_ig_i,\ \forall i\in\{1,\cdots n\}\Leftrightarrow g_i\in C(G_i),\ \forall i$.

因此

$C(G_1\times G_2\times\cdots\times G_n)=C(G_1)\times C(G_2)\times\cdots\times C(G_n)$;

(2) $G_1\times G_2\times\cdots\times G_n$ 为 Abel 群

$\Leftrightarrow C(G_1\times G_2\times\cdots\times G_n)=\{1\}$

$\Leftrightarrow C(G_1)\times C(G_2)\times\cdots\times C(G_n)=\{1\}$

$\Leftrightarrow C(G_i)=\{1\},\ \forall i$.

$\Leftrightarrow G_i$ 为 Abel 群, $\forall i$.

Ex 7. 设 $G_i\ (1\le i\le n)$ 为群，$N_i \le G_i$. 则

(1) $N_1\times N_2\times\cdots\times N_n \le G_1\times G_2\times\cdots\times G_n$;

(2) $N_1\times N_2\times\cdots\times N_n \lhd G_1\times G_2\times\cdots\times G_n \iff \forall i,\ N_i \lhd G_i$;

(3) 当 $N_1\times\cdots\times N_n \lhd G_1\times\cdots\times G_n$ 时，

$$G_1\times\cdots\times G_n/N_1\times\cdots\times N_n \cong G_1/N_1\times\cdots\times G_n/N_n$$

证明.

(1) $\forall (x_1,\cdots,x_n),(y_1,\cdots,y_n)\in N_1\times N_2\times\cdots\times N_n$

$(x_1,\cdots,x_n)(y_1,\cdots,y_n)^{-1}=(x_1y_1^{-1},\cdots,x_ny_n^{-1})\in N_1\times\cdots\times N_n$

由此 $N_1\times N_2\times\cdots\times N_n \le G_1\times G_2\times\cdots\times G_n$.

(2) $\forall (x_1,\cdots,x_n)\in G_1\times\cdots\times G_n$,

$N_1\times N_2\times\cdots\times N_n \lhd G_1\times G_2\times\cdots\times G_n$

$\iff (x_1,\cdots,x_n)(N_1\times\cdots\times N_n)(x_1,\cdots,x_n)^{-1}$

$= x_1N_1x_1^{-1}\times\cdots\times x_nN_nx_n^{-1}$

$= N_1\times\cdots\times N_n$

$\iff x_iN_ix_i^{-1}=N_i,\ \forall i \iff N_i\lhd G_i,\ \forall i$.

(3) 有自然满同态

$$\pi: G_1\times\cdots\times G_n \longrightarrow G_1/N_1\times\cdots\times G_n/N_n$$
$$(g_1,\cdots,g_n)\longmapsto (g_1N_1,\cdots,g_nN_n)$$

验算 $\ker\pi = N_1\times\cdots\times N_n$.

Ex 8 $\mathbb{Z}^n \cong \langle x_1, \cdots, x_n \mid x_i x_j = x_j x_i,\ 1 \le i < j \le n \rangle$

$= F(x_1, \cdots, x_n) / N(x_i x_j x_i^{-1} x_j^{-1} \mid 1 \le i < j \le n)$

泛性质：有自然满同态

$$\pi : F(x_1, \cdots, x_n) \longrightarrow \mathbb{Z}^n$$

其中 $\pi(x_i) = e_i$. $\pi(x_i x_j x_i^{-1} x_j^{-1}) = e_i + e_j - e_i - e_j = 0$

因此诱导了满同态

$$\pi : F(x_1, \cdots, x_n) / N(x_i x_j x_i^{-1} x_j^{-1} \mid 1 \le i < j \le n) \longrightarrow \mathbb{Z}^n$$

$\forall g \in \ker \pi$, $g = \bar{x}_1^{k_1} \bar{x}_2^{k_2} \cdots x_n^{k_n}$, 且 $\pi(g) = 0$. 则

$$k_1 e_1 + k_2 e_2 + \cdots + k_n e_n = 0.$$

即 $e_1, \cdots, e_n$ 是 $\mathbb{Z}^n$ 的一组基. 因此 $k_1 = \cdots = k_n = 0$. 即 $g = 1$. 因此 π 是单的.

Ex 9. $N \lhd G$, N f.g. G/N f.g. $\Rightarrow G$ f.g.

证明. 设 $X=\{x_1,\cdots,x_m\}$ 是 N 的生成元集, $Y=\{\bar{y}_1,\cdots,\bar{y}_n\}$ 是 G/N 的生成元集. $\forall g\in G$, $\bar{g}=k_1\bar{y}_1+\cdots+k_n\bar{y}_n$

因为 $g-(k_1y_1+\cdots+k_ny_n)\in N$. 从而

$$g-(k_1y_1+\cdots+k_ny_n)=l_1x_1+\cdots+l_mx_m$$

即

$$g=l_1x_1+\cdots+l_mx_m+k_1y_1+\cdots+k_ny_n$$

因此 G 由 $\{x_1,\cdots,x_m,y_1,\cdots,y_n\}$ 生成.

Ex10. $A \in M_n(\mathbb{Z})$. 则 $A \in GL_n(\mathbb{Z}) \Leftrightarrow \phi_A : \mathbb{Z}^n \to \mathbb{Z}^n$ 是同构.

证明. $A \in GL_n(\mathbb{Z}) \Leftrightarrow \exists B \in GL_n(\mathbb{Z})$, s.t. $AB = BA = I$

$\Leftrightarrow \phi_A \phi_B = \phi_B \phi_A = id$.

Ex 11. $\phi_P(\mathrm{Im}\,\phi_B) = \mathrm{Im}\,\phi_A$

Pf. $B = P^{-1}AQ \Rightarrow PB = AQ$

$$\Rightarrow \phi_P\phi_B = \phi_A\phi_Q$$

$$\Rightarrow \phi_P(\mathrm{Im}\,\phi_B) = \phi_A(\mathrm{Im}\,\phi_Q)$$

$$= \phi_A(\mathbb{Z}^n)$$

$$= \mathrm{Im}\,\phi_A$$

Ex1 $2\mathbb{Z}\subseteq\mathbb{Z}$ 没有补.

证明 设 $2\mathbb{Z}\subseteq\mathbb{Z}$ 的补是 U. 由于 $U\leq\mathbb{Z}$, 因此 $U=m\mathbb{Z}$.

而 $m\mathbb{Z}\cap 2\mathbb{Z}=2m\mathbb{Z}=\{0\}$. 因此 $m=0$. 即 $\{0\}+2\mathbb{Z}\neq\mathbb{Z}$.

矛盾. 因此 $2\mathbb{Z}\subseteq\mathbb{Z}$ 没有补. □

Ex2. $G=\mathbb{Z}_2\times\mathbb{Z}$, $t(G)=\mathbb{Z}_2\times\{0\}$, $F_1=\{\bar{0}\}\times\mathbb{Z}$, $F_2=\mathbb{Z}(\bar{1},1)$. 证 $t(G)$ 的补恰为 F_1 或 F_2. (已证 $t(G)\oplus F_i=G$, $i=1,2$).

证明 记 H 是 $t(G)$ 的补. 设 $H\neq F_1$. 现证 $H=F_2$. $(\bar{1},1)\in G$ 且 $(\bar{1},1)=(\bar{0},1)+(\bar{1},0)=(\bar{1},1)+(\bar{0},0)$, 故 $(\bar{1},1)\in H$ 从而 $F_2\subseteq H$. $\forall(\bar{a},b)\in H$, $(\bar{0},b-a)\in H\cap t(G)=0$. 因此 $b-a=0$, 即 $a=b$. 从而 $(\bar{a},b)\in F_2$. 因此 $F_2=H$. □

Ex3. $G=A\oplus B$ 内直和, 则 $B\cong G/A$ 是群同构.

证明 $G=A\oplus B$, 故 $A+B=G$, $A\cap B=\{0\}$, $a+b=b+a$ $\forall a\in A$, $b\in B$. 故 $G\cong A\times B$. 从而 $G/A\cong A\times B/A\times\{0\}$

$\cong A/A\times B/\{0\}\cong B$ (第十二次作业 Ex7).

(可用于证明 Ex1) 用反证法. 若 $2\mathbb{Z}\subseteq\mathbb{Z}$ 有补 U, 则

$$U\cong\mathbb{Z}/2\mathbb{Z}$$

因此 U 中有 2 阶元, 矛盾.

Ex 4. 试证：有限生成 Abel 群 G 是自由 Abel 群 $\Leftrightarrow$ G 的每个非零元素都是无限阶元素.

证明：$\Rightarrow$ $\forall x \in G$, $\langle x \rangle \leq G$. 由定理 1 知 $\langle x \rangle$ 自由 Abel 群，因此 x 是无限阶的.

$\Leftarrow$ G 是有限生成 Abel 群，由定理 3. $G \cong \mathbb{Z}^r \oplus t(G)$. 由于 $t(G)$ 中的元素是有限阶，而每个非零元素都是无限阶元素，因此 $t(G) = 0$，即 $t = 0$. 因此 $G \cong \mathbb{Z}^r$ 是自由 Abel 群.

Ex 5. 设 A 为有限 Abel 群，则对于 $|A|$ 的每个正因子 d，A 均有 d 阶子群和 d 阶商群.

证明：设 A 的初等因子为 $\{p_1^{s_1}, \cdots, p_k^{s_k}\}$. 则 $d = p_1^{t_1} \cdots p_k^{t_k}$ 其中 $0 \leq t_i < s_k$ 且 $t_1 + \cdots + t_k > 0$. 因为 $\mathbb{Z}_{p^{s_i}}$ 一定有 p^{t_i} 阶子群，A 的 d 阶子群存在且其初等因子为 $\{p_{i_1}^{t_{i_1}}, \cdots, p_{i_l}^{t_{i_l}}\}$ 其中 $1 \leq i_1 < i_2 < \cdots < i_l \leq k$. 因此我们有 n/d 阶（正规）子群 H，从而 G/H 是 d 阶商群.

Ex 6. 设 H 是有限 Abel 群 A 的子群，则有 A 的子群同构于 A/H.

证明：设 A 的初等因子为 $\{p_1^{s_1}, \cdots, p_k^{s_k}\}$.

Claim H 的初等因子为 $\{p_1^{t_1}, \cdots, p_k^{t_k}\}$，$t_i \leq s_i$，$t_i = 0$ 时删去.

Pf of claim：由于 H 的 p-子群一定形如 $P \cap H$，其中 P

为A的Sylow p-子群. 因此我们只需说明 $p_i = p$, $\forall i$. 时的Claim (此时不妨设 $s_1 \le \cdots \le s_k$, $t_1 \le \cdots \le t_l$). 由于 $A = \mathbb{Z}^k / K$, $\mathbb{Z}^k$ 的子群最多不大于 k 的自由Abel群. 因此由好定定理知, $H = \mathbb{Z}^l / K$, $l \le k$. 此时将 $t_i = 0$ 考虑进来, 则可设 $l = k$.

1° $k = 1$ 时, 显然 $l = k$, 且 $t_1 \le s_1$.

2° 假设 $k \le n$ 时结论成立.

1) 若 $s_1 = \cdots = s_k = s$. 此时 $t_i \le s$. 否则, 存在阶大于 s 的元素, 矛盾.

2) 取 $a = \max\{ i \mid s_i > s_{i-1}, i > 1 \}$. 令 $A / \mathbb{Z}_{p^{s_a}} \oplus \cdots \oplus \mathbb{Z}_{p^{t_k}} \cong \mathbb{Z}_{p^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{s_{a-1}}}$, 由归纳假设知所有子群同构于 $\mathbb{Z}_{p^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{t_{a-1}}}$, $t_i \le s_i$, $i = 1, \cdots, a-1$. 若 $\exists j \ge a$, s.t. $t_j > s = s_a = \cdots = s_k$, 则存在阶大于 s 的元素, 矛盾. 因此 $\forall j \ge a$, $t_j \le s$.

因此Claim成立.

从而 $A/H \cong \mathbb{Z}_{p_1^{s_1 - t_1}} \oplus \mathbb{Z}_{p_2^{s_2 - t_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k - t_k}}$.

Ex 7 证明有限Abel群 A 不是循环群，则存在素数 p 使得 A 有子群同构于 $\mathbb{Z}_p^2$

证明：设 A 的初等因子为 $\{p_1^{s_1}, \cdots, p_k^{s_k}\}$，则 $\exists i, j$，$i \neq j$，s.t. $p_i = p_j$（否则，$p_1, \cdots, p_k$ 是不同素数，从而

$$A \cong \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_k^{s_k}} \cong \mathbb{Z}_{p_1^{s_1} \cdots p_k^{s_k}}$$

是循环群，矛盾.）不妨设 $i=1$，$j=2$. 取 $\mathbb{Z}_{p_1^{s_1}}$ 和 $\mathbb{Z}_{p_2^{s_2}}$ 的 $p_1 = p_2$ 阶元 x 和 y. 则 A 的子群 $\langle x \rangle \times \langle y \rangle \times \{0\} \times \cdots \times \{0\} \cong \mathbb{Z}_p^2$.

Ex 8 讨论：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：1° $(m,n)=1$ 时，$\mathbb{Z}_m \oplus \mathbb{Z}_n = \mathbb{Z}_{mn}$. 此时不变因子为 mn.

2° $(m,n) \neq 1$ 时，设 $p_1, \cdots, p_k$ 是 (m,n) 中出现的所有素因子. 则可设 $m = p_1^{s_1} \cdots p_k^{s_k} m'$，$n = p_1^{r_1} \cdots p_k^{r_k} n'$. 其中 $(m', p_i) = (n', p_i) = 1$. 则 $(m', n') = 1$.

$$\begin{aligned}
\mathbb{Z}_m \oplus \mathbb{Z}_n &= \mathbb{Z}_{m'n'} \oplus (\mathbb{Z}_{p_1^{s_1}} \oplus \mathbb{Z}_{p_1^{r_1}}) \oplus \cdots \oplus (\mathbb{Z}_{p_k^{s_k}} \oplus \mathbb{Z}_{p_k^{r_k}}) \\
&= [\mathbb{Z}_{m'n'} \oplus (\mathbb{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{a_k}})] \oplus (\mathbb{Z}_{p_1^{b_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{b_k}})
\end{aligned}$$

其中 $a_i = \max\{s_i, t_i\}$，$b_i = \min\{s_i, t_i\}$，$i = 1, \cdots, k$.

因此不变因子是

$$\{p_1^{b_1} \cdots p_k^{b_k},\ p_1^{a_1} \cdots p^{a_k} m'n'\} = \{(m,n), [m,n]\}.$$

Ex 9. 求 $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{35}$ 的初等因子和不变因子.

解. 由 Ex 8 知, 其不变因子为 $\{630\}$. 从而其初等因子为 $\{2, 3^2, 5, 7\}$.

Ex 10. $V = \{v \in K^{n+1} \mid Av = 0\}$. $G \curvearrowright K^{n+1}$ 如下:

$$\tau \cdot v = \tau \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_{n+1} \end{pmatrix} = \begin{pmatrix} \tau(\lambda_1) \\ \vdots \\ \tau(\lambda_{n+1}) \end{pmatrix}$$

证明. $v \in V$, $\tau \in G \Rightarrow \tau \cdot v \in V$.

略 (问过老师, 没听懂这道题在讲什么, 大家忽略掉吧)

Ex 11. $G \leq S_n$, $K = k(t_1, \cdots, t_n)$, n 元有理函数域.

$S_n \curvearrowright K$. 证明: $\forall \sigma \in S_n$, $\exists!$ 域自同构 $T_\sigma : K \to K$,

$t_i \longmapsto t_{\sigma(i)}$.

思路. 由 $S_n \curvearrowright K$ 诱导了群表示 $S_n \hookrightarrow \mathrm{Aut}(K)$. 因此 T_σ 是存在且唯一的.

Ex 12. 写出 $\mathbb{Q}(\sqrt{2},\sqrt{5})$ 的 Galois 对应.

解 $\mathbb{Q}(\sqrt{2},\sqrt{5})$ 是可分多项式 $f(x)=(x^2-2)(x^2-5)$ 的分裂域，因此是有限 Galois 扩张. 因为 $g(x)=x^2-5$ 在 $\mathbb{Q}(\sqrt{2})$ 上不可约，

$$\begin{aligned}|Gal(\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q})| &= [\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] \\ &= 2\times 2=4.\end{aligned}$$

因此 $G=Gal(\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q})$ 是四元群. $\forall \sigma\in G$, $\sigma(\sqrt{2})=\pm\sqrt{2}$ $\sigma(\sqrt{5})=\pm\sqrt{5}$. 因此 G 中有 3 个 2 阶元. 因此 $G=\{1,\sigma,\tau,\sigma\tau\}$ 其中 $\sigma(\sqrt{2})=\sqrt{2}$, $\sigma(\sqrt{5})=-\sqrt{5}$, $\tau(\sqrt{2})=-\sqrt{2}$, $\tau(\sqrt{5})=\sqrt{5}$ 我们有

$Inv((\sigma))=\mathbb{Q}(\sqrt{2})$, $Inv((\tau))=\mathbb{Q}(\sqrt{5})$, $Inv((\sigma\tau))=\mathbb{Q}(\sqrt{10})$

因此有 Galois 对应：