1. 子群：非空子集，取逆，乘法封闭

正规子群：子群 H，且 $gHg^{-1}=H$，$\forall g\in G$.

① $G=S_3$. $H=\{(1),(12)\}$.

$(12)^2=(1)$. 所以 H 是子群

$g=(23)$ $gHg^{-1}=\{(1),(13)\}\neq H$

② $G=S_3\times\mathbb{Z}$. $H=\{(1),(12)\}\times\mathbb{Z}$

同 ①

$n=0$ 时 $N_H(G)=G$（没写扣1分）

2. G p-群. $|G|=p^m$. $|H|=p^n$. $m>n\in\mathbb{Z}$

H 的左陪集 gH 全体. G/H.

$|G/H|=p^{n-m}\equiv 0 \mod p$

H 左乘作用于 G/H. 有 $G/H=\bigcup O_i$

其中 $O_1=\{H\}$，$|G/H|=1+\sum_{i\geq 2}|O_i|$

又 $|O_i|\,\big|\,|H|=p^m$

$\Rightarrow$ $|O_i|\equiv 1, 0 \mod p$

所以必有 $i\geq 2$, $|O_i|=\{gH\}$

$\forall h \in H, \quad hgH = gH$

$\Rightarrow \quad g^{-1}hg \in H$

$\Rightarrow \quad g \in N_G(H)$ 且 $g \notin H$

$\Rightarrow \quad N_G(H) \supsetneq H$

3. $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad ad - bc = 1$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} b & -a \\ d & -c \end{bmatrix} = \begin{bmatrix} c & d \\ -a & -b \end{bmatrix}$$

$\Leftrightarrow \quad b = c, \quad d + a = 0$

A, B 共轭 $\Leftrightarrow \exists \begin{bmatrix} a & b \\ -b & -a \end{bmatrix} \in G.$

1. $\det\begin{pmatrix} a & b \\ -b & -a \end{pmatrix} = -a^2-b^2 < 0 < 1$

Since A, B 不共轭.

2. $a^2+b^2=-1$, $p=2$ 有解

$p\geq 3$. 考虑 $X=\{a^2 \mid a\in\mathbb{F}_p\}$

$=\{0\}\cup\{a^2 \mid a\in\mathbb{F}_p^\times\}$

由于 $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. $\Rightarrow |X|=1+\frac{p-1}{2}$

(或者由 $x^2-a^2=0$ 有2个不同根 $a, -a$)

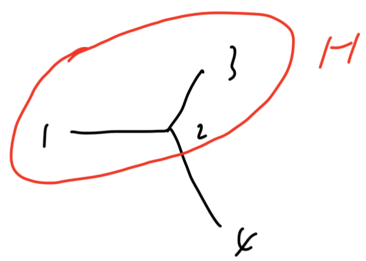
$Y=\{-1-b^2 \mid b\in\mathbb{F}_p\}$. $|Y|=|X|=1+\frac{p-1}{2}$

$|X|+|Y|=p+1 \Rightarrow X\cap Y\neq\emptyset$.

$\Rightarrow \exists\, a, b\in\mathbb{F}_p$. $a^2+b^2=-1$.

$\Rightarrow$ A, B 共轭

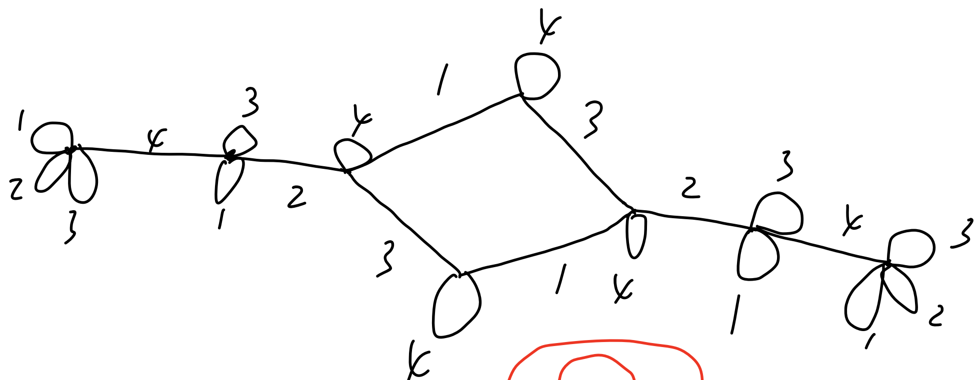
4.



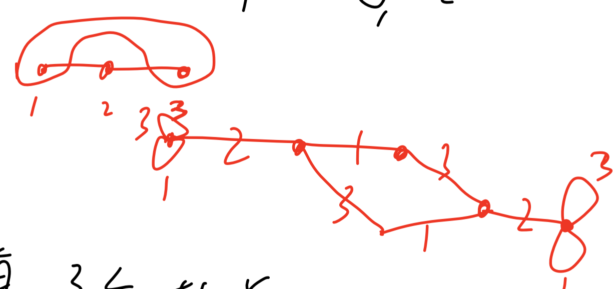
考虑子群 $H \subset G$, $H = \langle s_1, s_2, s_3 \rangle$

则 $|H| \le |S_4| = 4!$. 且 H 是 S_4 的商群.

由 Coxeter-Todd.



$|G/H| = 8$.



$H \curvearrowright G/H$ 有 3个轨道,

其中一个轨道长为 6.

$6 \mid |H|$. 而 S_4 的正规子群有

记这为 V

$\{(1)\}$, $\{(1), (12)(34), (13)(24), (14)(23)\}$, A_4

若为 V，则 $S_4/V \cong H$, $|H| = 6$

H 作用在 O 上 的 任一点，的 $Stab = \{e\}$

而 $S_1, S_3 \in Stab \Rightarrow |H| \leq 2$

$\Rightarrow H = S_4$

$\Rightarrow G = |S_4| \cdot 8 = 24 \cdot 8 = 192$

5. a_9 = # of sylow 3 group

$a_9 \equiv 1 \mod 3$ $\quad a_9 | 2$. $\Rightarrow a_9 = 1$

$|H| = 9$. H 是 G 的正规子群. $|HK| = 18$

$|K| = 2$. $\quad K = \langle x \rangle$ $\quad \Rightarrow HK = G$

① $H \cong C_3 \times C_3$. $\varphi: K \to Aut(C_3 \times C_3)$

1.1 若 φ trivial. then $G \cong (C_3 \times C_3) \times C_2$

1.2 若 φ nontrivial. $\varphi(x) = f$

1.2.1 $\exists\, \alpha \in C_3 \times C_3 | \{e\}$. $f(\alpha) \notin \langle e, \alpha, \alpha^2 \rangle$

则 $\langle \alpha, f(\alpha) \rangle = C_3 \times C_3$. $f(f(\alpha)) = \alpha$.

则 $G = \langle \alpha, \beta, x \mid \alpha^3 = \beta^3 = x^2 = e$
$\alpha\beta = \beta\alpha,$
$x\alpha x^{-1} = \beta$
$x\beta x^{-1} = \alpha \rangle$

即 $(C_3 \times C_3) \rtimes_\varphi C_2$

$(\varphi(x))(\alpha) = \beta$

$(\varphi(x))(\beta) = \alpha$

1.2.2. 若 $\forall$ $\alpha \in C_3 \times C_3 \setminus \{e\}$. $\varphi(x)(\alpha)$
$\in \langle e, \alpha, \alpha^2 \rangle$

$\exists$ α, s.t. $f(\alpha) = \alpha^2$.

取 $\beta \notin \langle e, \alpha, \alpha^2 \rangle$

则 $\langle \alpha, \beta \rangle = H$.

1.2.2.1 $f(\beta) = \beta$, $f(\alpha\beta) = \alpha^2\beta \notin$
$\{e, \alpha\beta, (\alpha\beta)^2\}$
与 1.2.2 假设矛盾

1.2.2.2 $f(\beta) = \beta^2$.
$(C_3 \times C_3) \rtimes_\varphi C_2$, $(\varphi(x))(\alpha) = \alpha^2$

$$(\varphi(x))(\beta)=\beta^2.$$

此时可验证满足 1.2.2 的假设

② $H\cong C_9=\langle\alpha\rangle$. 生成元有 $\alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^7, \alpha^8$

$C_2=\langle x\rangle$

$$\varphi: C_2\to \mathrm{Aut}(C_9)$$

记 $\varphi(x)=f$. 由于 $f^2=id$.

$f(\alpha)=\alpha$ 或者 $f(\alpha)=\alpha^8$.

2.1. $f(\alpha)=\alpha$, $\Rightarrow G\cong C_9\times C_2$

2.2 $f(\alpha)=\alpha^8 \Rightarrow G\cong C_9\rtimes_{\varphi} C_2$

$$(\varphi(x))(\alpha)=\alpha^8.$$

① 与 ② 不同构因为 Sylow-3 子群不一样.

2.1. 2.2 不同, 因为 2.1 交换, 2.2 不交换
同理 1.1 与 1.2 不同构.
改变 Sylow-2 子群的选取不改变 1.2.1 与 1.2.2
中的分类性质, 因为 $HK=G$.
对 $K'=\langle e, x'\rangle$, $x'=h\cdot x$.

而 1-1 对换 $(hx)\alpha(hx)^{-1} = x\alpha x^{-1}$.

所以一共 5 种.

6. $|G| = 72 = 8\cdot 9$.

Sylow 3 子群有 1个, 4个 2种可能

若有1个, 则 G 有 Sylow 3 子群正规

若有4个, $G \curvearrowright \{H_1, H_2, H_3, H_4\}$ 共轭作用

H_i Sylow 3子群

$f: G \to S_4$ 非平凡. $|\mathrm{Im}\, G| \mid 24$

$\Rightarrow \ker f \neq \{e\}$.

7. 1. $\varphi: SL(2,\mathbb{Z}) \to SL(2,\mathbb{F}_2)$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod 2$$

φ 是群同态，$\Rightarrow$ $\ker\varphi$ 正规子群

$\ker\varphi = \Gamma(2)$

$$\begin{pmatrix} 1 & \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ & 1 \end{pmatrix}, \begin{pmatrix} -1 & \\ & -1 \end{pmatrix} \in \Gamma(2)$$

2. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $a \equiv 1 \bmod 2$

$c \equiv 0 \bmod 2$

$ad - bc = 1$, $\Rightarrow$

若 $c \neq 0$，　a, c 互素.

带余引理：$(m,n)=1$. $m, n \in \mathbb{Z}$, $|m|>|n|>1$

$\exists\ q \in \mathbb{Z}$.　$m = n(2q) + r$.

$|r| < |n|$

由带余除法，　$m = nk + r$　$|r|<|n|$

$r \neq 0$

若 k 为奇数，取 $m=(k+1)n+(r-n)$

$m=(k-1)n+(r+n)$

必有一个 $|r-n|<n$ 成立。

$|r+n|<n$

若 $|a|,|c|\geq 2$.

对 $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\in\Gamma(2)$ 可用引理中的辗转相除，

相当于左乘 $\begin{bmatrix} 1 & 0 \\ -2q & 1 \end{bmatrix}$ 或 $\begin{bmatrix} 1 & -2q \\ & 1 \end{bmatrix}$

$=\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}^{-q}$, $=\begin{bmatrix} 1 & 2 \\ & 1 \end{bmatrix}^{-q}$

使得 $\max(|a|,|c|)$ 严格减小

直到 $\min(|a|,|c|)=1$

只能是 $|a|=1$, $|c|=2k$.

再左乘 $\begin{bmatrix} 1 & \\ 2i & 1 \end{bmatrix}$ 或者 $\begin{bmatrix} 1 & \\ -2i & 1 \end{bmatrix}$

得到 $\begin{bmatrix} 1 & 2i \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} -1 & 2i \\ & -1 \end{bmatrix}$

再乘以 $\begin{bmatrix} -1 & \\ & -1 \end{bmatrix}$ 得到 $\begin{bmatrix} 1 & 2i \\ 0 & 1 \end{bmatrix}$

---

3. 考虑 $P(2)/\{\pm I\}$ 在 $\mathbb{R}^2$ 中的所有过原点的直线上的作用 $X=\{y=kx\}\cup\{\infty\}$

$X_1 = \{y=kx,\ |k|<1\}$

$X_2 = X \setminus X_1$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+2y \\ y \end{pmatrix}$$

If $\left|\frac{y}{x}\right| \geq 1$, then $\left|\frac{y}{x+2y}\right| < 1$.

and for $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$

line $x=0$ is mapped to $y = \frac{1}{2}x$

If $\left|\frac{y}{x}\right| < 1$, then $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$

$$= \begin{pmatrix} x \\ 2x+y \end{pmatrix}$$

$$\left|\frac{2x+y}{x}\right| > 1$$

所以 $\begin{bmatrix}1&2\\0&1\end{bmatrix}\cdot X_2 \subset X_1$

$\begin{bmatrix}1&0\\2&1\end{bmatrix}\cdot X_1 \subset X_2$

又 $\begin{bmatrix}1&2\\0&1\end{bmatrix}$ 和 $\begin{bmatrix}1&0\\2&1\end{bmatrix}$ 阶数 $= \infty$.

$\Rightarrow \Gamma(2)/\{\pm I\} \cong \left\langle \begin{bmatrix}1&2\\0&1\end{bmatrix}\right\rangle * \left\langle \begin{bmatrix}1&0\\2&1\end{bmatrix}\right\rangle$

= free group generated by two elements

---

8. $|PSL(2, F_5)| = \dfrac{(5^2-1)(5^2-5)/4}{\#\{\lambda \in F_5^* \mid \lambda^2 = 1\}}$

$= \dfrac{24\cdot 5}{2} = 60$

$PSL(2, F_5) \cong A_5$ 单群.

下证 60 阶单群 G 均同构于 A_5.

$|G| = 60 = 4 \cdot 15 = 4 \cdot 3 \cdot 5$.

Sylow 2-group 有 1, 3, 5, 15 四种可能.

若有 1 个, 与 G 单群矛盾.

若有 3 个, 有 $G \to S_3$ 同态, 非平凡

$|G| > |S_3|$, $\Rightarrow$ ker 非平凡

若有 5 个, 有 $f: G \to S_5$ 同态, 非平凡

$\ker f = \{e\} \Rightarrow f$ 单射

$f(G)$ 是 S_5 的指数为 2 的子群.

下证只能是 A_5. $S_5 / f(G) = \{\pm 1\}$

$s_1 \quad s_2 \quad s_3 \quad s_4$

满同态: $S_5 \xrightarrow{\rho} \{\pm 1\}$

$S_5 = \langle s_i \rangle$

则存在 $\rho(s_i) = -1$.

则 $\rho((s_j s_i)^3) = 1$, $j = i \pm 1$

$(\rho(s_j))^3 = (\rho(s_i))^3 = -1$

$\Rightarrow \rho(s_j) = -1$

$\Rightarrow \rho(s_k) = -1$ for $k = 1, 2, 3, 4$

$\Rightarrow \ker \rho = A_5$

若有 15 个.

则有 6 个 sylow 5 group,

至少 4 个 sylow 3 group

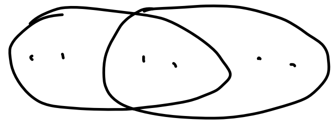
3 阶元素 $\geq 4 \cdot 2 = 8$ 个

5 阶元素 $\geq 6 \cdot 4 = 24$ 个.

15 个 sylow 2-group H_i 若 H_i 为 4 阶循环群, 则

4阶元素 $\geq 2\cdot 15 = 30$. $20+24+30>60$

H_i 的可能为 $C_2\times C_2$. 一定存在两个 $H_i \neq H_j$. $H_i\cap H_j = \{1, g\}$



否则 2阶元计数 $\geq 3\cdot 15 = 30$

考虑 g 的 centralizer. C. $C \supset H_i, H_j$

$|C| \geq 6$. $|H_i| \mid |C|$, $\Rightarrow |C| = 12, 20, 60$.

$|C| = 60 \Rightarrow \{1, g\}$ 正规.

非平凡

$|C| = 20 \Rightarrow G \curvearrowright G/C \Rightarrow G \to S_3$ 矛盾.

$|C| = 12 \Rightarrow G \curvearrowright G/C, \Rightarrow G \to S_5$ 非平凡

$\Rightarrow G \cong A_5$.

$\Rightarrow PSL(2, F_5) \cong A_5$

9. 1. $I \subset R$ 是加法子群，

且 $\forall r \in R,\ s \in I,\ r \cdot s \in I$.

$\mathbb{Z} \subset \mathbb{Q}$，$\mathbb{Q}$ 是域，$\mathbb{Z}$ 不是 $\mathbb{Q}$ 的理想

2. $I \subsetneq R$ 是理想，

且 $\forall J \supsetneq I$ 是理想，

则 $J = R$

$(0) \subset \mathbb{Z}$ 是素理想，不是极大理想

10\. (1) $\forall f \cdot g \in R, g \neq 0$

$\exists b' \neq 0$, $\tilde{s}(g) = s(g \cdot b')$

$b' f = (g \cdot b') \cdot q + r'$

$r' = 0$，即 $f = g \cdot q$

或者 $r' \neq 0$，$s(r') < s(g b')$

取 $r = f - g q$

则 $s(r') = s(r b') \geq \tilde{s}(r)$

$\Rightarrow \tilde{s}(r) \leq s(r') < \tilde{s}(g)$

(2) 若 $a | b$，则 $b = a \cdot c$，$c \neq 0$.

$\forall m \neq 0.\ S(b \cdot m) = S(a \cdot m)$

$\geq \tilde{S}(a)$

$\Rightarrow \quad \tilde{S}(b) \geq \tilde{S}(a)$

11\.

1\. $\left(\mathbb{Z}/6\mathbb{Z}\right)[x] \big/ (3x-1)$

$\cong \mathbb{Z}[x] \big/ (6,\ 3x-1)$

$-2(3x-1) + 6 \cdot x = 2$

$\Rightarrow \mathbb{Z}[x] \big/ (2,\ 6,\ 3x-1)$

$= \mathbb{Z}[x] \big/ (2,\ 3x-1)$

$$= \mathbb{Z}/22\,[x] \,/\, (3x-1)$$

$$= \mathbb{Z}/22\,[x] \,/\, (x+1)$$

$t = x+1$

$$= \mathbb{Z}/22\,[t] \,/\, (t)$$

$$= \mathbb{Z}/22$$

2. $\mathbb{Z}[i]/(5) = \mathbb{Z}[i] \,/\, (1+2i)\cdot(1-2i)$

$I = (1+2i)$, $J = (1-2i)$

$I \cap J = (0)$, $I + J = \mathbb{Z}[i]$

因为 $I = 1+2i$ 极大, $J \not\subset I$

$\Rightarrow \mathbb{Z}[i]/IJ \cong (\mathbb{Z}[i]/I) \times (\mathbb{Z}[i]/J)$

(用 $\mathbb{Z}[i] \to (\mathbb{Z}[i]/I) \times (\mathbb{Z}[i]/J))$

或用中国剩余定理.

$\ker = I \cap J = IJ$, 满射由 $I+J = \mathbb{Z}[i]$)

$\Rightarrow \mathbb{Z}[i]/(5) \cong \mathbb{Z}/(5) \times \mathbb{Z}/(5)$

---

12. $\forall\ x, y \in \mathbb{Z},\ a, b \in \mathbb{Z},\ a^2+b^2 \neq 0,\ \exists\ c, d \in \mathbb{Q}$

$(x+y\sqrt{2}) = (a+b\sqrt{2}) \cdot (c+d\sqrt{2})$

取 $\tilde{c}, \tilde{d} \in \mathbb{Z}$, s.t.

$|\tilde{c} - c| \leq \frac{1}{2}$

$|\tilde{d} - d| \leq \frac{1}{2}$.

$$\Rightarrow \quad (x+y\sqrt{2}) = (a+b\sqrt{2})(\tilde{c}+\tilde{d}\sqrt{2}) + r$$

$$r = (a+b\sqrt{2}) \cdot \left[(\tilde{c}-c) + (\tilde{d}-d)\sqrt{2}\right]$$

由于 $S(\alpha\beta) = S(\alpha)\cdot S(\beta)$. 在最后验证

$$S\left((\tilde{c}-c) + (\tilde{d}-d)\sqrt{2}\right) \le \left|\frac{1}{4}\right| + \left|\frac{1}{4}\right| \cdot 2 < 1.$$

$$\Rightarrow \quad S(r) < S(a+b\sqrt{2})$$

对于 $\mathbb{Q}[\sqrt{2}]$, $S(a+b\sqrt{2}) = |a^2-2b^2|$, $a, b \in \mathbb{Q}$

$\alpha = a + a'\sqrt{2}$. $\quad \beta = b + b'\sqrt{2}$. $\quad a, a', b, b' \in \mathbb{Q}$

$s(\alpha\beta) = s(ab + 2a'b' + \sqrt{2}(ab' + a'b))$

$= |(ab+2a'b')^2 - 2(ab'+a'b)^2|$

$= |a^2b^2 + 4a'^2b'^2 - 2a'^2b^2 - 2a^2b'^2|$

$s(\alpha)s(\beta) = |a^2 - 2a'^2|\,|b^2 - 2b'^2|$

$= |a^2b^2 + 4a'^2b'^2 - 2a'^2b^2$
$\quad - 2a^2b'^2|$

---

13. $P \subset \mathbb{C}[x,y]$. $x^3+y^3-1 \in P$

直接 quote 素理想,
homework, 沒有其他解釋 −1

則 $P \cap \mathbb{C}[x]$ 是 $\mathbb{C}[x]$ 的素理想

如果 $P \cap \mathbb{C}[x] = (0)$. 則

存在 $m = \min\{\deg_y f(x,y) \mid f(x,y) \in P.$

$\deg_y f(x,y) \geq 1$)

m 由 $\deg_y f(x,y) \in P$ 取得.

可假设 $f(x,y)$ 不可约, 相对于系数环 $\mathbb{C}[x]$ primitive. $\Rightarrow$ $f(x,y)$ 在 $\mathbb{C}(x)[y]$ 中不可约

则 $\forall\ h(x,y) \in P$, 有

$$h(x,y) = f(x,y) \cdot G(x,y). \quad G(x,y) \in \mathbb{C}(x)[y]$$

$$R_1(x)\, h(x,y) = f(x,y) \cdot g(x,y) \cdot R_1(x)$$

$g(x,y) \in \mathbb{C}[x,y]$, $R_1(x), R_2(x) \in \mathbb{C}[x]$ | [illegible]

$\mathbb{C}[x][y]$ 中对系数 $R = \mathbb{C}[x]$ primitive

$$\Rightarrow h(x,y) = f(x,y) \cdot g(x,y)$$

$$\Rightarrow P = (f(x,y))$$

又 x^3+y^3-1 不可约.

用 mod $(y-1)$ 的 Eisenstein 判别法

$\Rightarrow P = (x^3+y^3-1)$

与 $P \neq (0)$ 矛盾

所以 $P \cap \mathbb{C}[x] = (x-a)$

$$\Rightarrow \mathbb{C}[x,y]/P$$

$$= \mathbb{C}[x,y]/(P, x-a)$$

$$= \mathbb{C}[y]/\overline{P}$$

又 $\overline{P} \supset (y^3-1+a^3) \Rightarrow \mathbb{C}[y]/\overline{P}$

is a field. $\Rightarrow P$ maximal

14. 1) $ad-bc$ irreducible

若可约. $(ad-bc) = f(a,b,c,d)\cdot g(a,b,c,d)$

$$\deg_a f = 1. \quad \deg_a g = 0$$

$$(a + f_0(b,c,d))\cdot g(b,c,d)$$

$$= a\, g(b,c,d) + f_0(b,c,d)\cdot g(b,c,d)$$

$$\Rightarrow g(b,c,d) = d$$

$$\Rightarrow d \mid bc. \text{ 矛盾.}$$

$\mathbb{Z}[a,b,c,d]$ UFD $\Rightarrow$ $ad-bc$ prime

$\Rightarrow$ $\mathbb{Z}[a,b,c,d]/(ad-bc)$ 整环

2. Claim a irreducible in R

$$a = f(a,b,c,d)\,g(a,b,c,d) + (ad-bc)\cdot h(a,b,c,d)$$

考虑关于 $a.b.c,d$ 的次数之和

有 $f(a,b,c,d) = f_0 + f_1 + f_2 + \cdots + f_k$

$g(a,b,c,d) = g_0 + g_1 + g_2 + \cdots + g_n$.

$h = h_0 + h_1 + h_2 + \cdots + h_m$

If $k+n \geq 2$

.

$f_k g_n = -(ad-bc)\cdot h_m$

$\Rightarrow$ f_k, 或 $g_n \in (ad-bc)$, 可删去

使得 $k+n$ 减小, 所以可假设

$\Rightarrow \quad f = f_0 + f_1$

$g = g_0$

$f_0 g_0 = 0, \quad f_1 g_0 = a.$

$\Rightarrow \quad f_0$ 或 $g_0 = 0$

$\Rightarrow \quad f_0 = 0.$

$g_0 f_1 = a$ 因于 a irreducible in $\mathbb{Z}[a,b,c,d]$

$\Rightarrow \quad g_0 = \pm 1.$

而 $\mathbb{Z}[a,b,c,d]/(ad-bc, a)$

$\cong \mathbb{Z}[b,c,d]/(-bc)$

b, c 是零因子, $\Rightarrow$ a not prime

$\Rightarrow$ R 不是 UFD

(倍角公式)

15. 想法: $x^2+y^2=1$ 有解 $x=\frac{2t}{1+t^2}$, $y=\frac{1-t^2}{1+t^2}$

$$=\frac{2t}{(t-i)(t+i)} \qquad =\frac{1-t^2}{(t-i)(t+i)}$$

取 $s=\frac{t-i}{t+i}$, $\Rightarrow t=\frac{\cancel{2s}\,s+i}{-1+s}$

(将分母化为只含 $\frac{1}{s}$)

$$=i\,\frac{s+1}{s-1}$$

$$x=\frac{2i\,\frac{s+1}{s-1}}{1-\frac{(s+1)^2}{(s-1)^2}}=\frac{2i\,\frac{s+1}{s-1}(s-1)^2}{-4s}$$

$$=-\frac{i}{2}\,\frac{s^2-1^2}{s}$$

$$=-\frac{i}{2}\left(s-\frac{1}{s}\right)$$

$$y=\frac{1+\frac{(s+1)^2}{(s-1)^2}}{1-\frac{(s+1)^2}{(s-1)^2}}$$

$$= \frac{2(s^2+1^2)}{-4s} = -\frac{1}{2}\left(s+\frac{1}{s}\right)$$

定义 $\varphi: \mathbb{C}[x,y] \to \mathbb{C}[s, \frac{1}{s}]$

$$x \mapsto -\frac{i}{2}\left(s-\frac{1}{s}\right)$$

$$y \mapsto -\frac{1}{2}\left(s+\frac{1}{s}\right)$$

则 $$(\varphi(x))^2 + (\varphi(y))^2 = -\frac{1}{4}\left(s-\frac{1}{s}\right)^2 + \frac{1}{4}\left(s+\frac{1}{s}\right)^2 = 1$$

$\Rightarrow$ φ 定义了环同态

$$\mathbb{C}[x,y]/(x^2+y^2-1) \to \mathbb{C}[s, \frac{1}{s}]$$

∴满同态，因为 $\varphi(x), \varphi(y)$ 的线性组合生成 $s, \frac{1}{s}$.

单同态，因为若 $f(\varphi(x), \varphi(y)) = 0$

$\Rightarrow$ 由带余除法

$$f(x,y) = (x^2+y^2-1)\,q(x,y) + r(x,y)$$

$$\deg_x r(x,y) \le 1$$

$$g\left(\tfrac{1}{2}\left(s+\tfrac{1}{s}\right)\right)\left(-\tfrac{i}{2}\left(s-\tfrac{1}{s}\right)\right) + h\left(\tfrac{1}{2}\left(s+\tfrac{1}{s}\right)\right) = 0$$

取 $s \mapsto \frac{1}{s}$，则

$0 = r(\varphi(x), \varphi(y))$ 中 $g\left(\frac{1}{2}\left(s+\frac{1}{s}\right)\right)$ $h\left(\frac{1}{2}\left(s+\frac{1}{s}\right)\right)$ 不变

令 $(s-\frac{1}{s})\ 1 \longrightarrow \frac{1}{s}-s$

$\Rightarrow\ g(\frac{1}{2}(s+\frac{1}{s}))(s-\frac{1}{s})=0$

由于 $s-\frac{1}{s}=\frac{s^2-1}{s}$, $gcd(s^2-1,\ s)=1$

$\Rightarrow\ g(\frac{1}{2}(s+\frac{1}{s}))=0$

$\Rightarrow\ g=0$ (比较 s^i 的系数

i 最高次项)

$\Rightarrow\ h=0$

所以 $f(x,y)=(x^2+y^2-1)\cdot h(x,y)$

$\Rightarrow f(x,y)\in(x^2+y^2-1)$

---

15. 直接用 $x^2+y^2-1=(x+iy)(x-iy)$

-1

$t = x+iy, \quad s = x-iy$

$$\mathbb{C}[x,y] / (x^2+y^2-1)$$

$$\cong \mathbb{C}[t,s] / (ts-1)$$

$$\cong \mathbb{C}[t, \tfrac{1}{t}]$$