1.

$$\begin{pmatrix} 10 & 4 & 6 \\ 4 & 4 & 4 \\ 2 & 8 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 8 & 8 \\ 4 & 4 & 4 \\ 10 & 4 & 6 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & -4 & -4 \\ 2 & 8 & 8 \\ 10 & 4 & 6 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & -4 & -4 \\ 0 & 12 & 12 \\ 0 & 24 & 26 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 12 \\ 0 & 24 & 26 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 24 & 2 \end{pmatrix}$$

7分

$$\longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & & \\ & 2 & \\ & & 12 \end{pmatrix}$$

G 是 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ 的直积

3分：G 可能为 10个：$(\mathbb{Z}/2\mathbb{Z})$，$(\mathbb{Z}/3\mathbb{Z})$，$(\mathbb{Z}/6\mathbb{Z})$，$(\mathbb{Z}/2\mathbb{Z})^2$，$(\mathbb{Z}/2\mathbb{Z})^3$，$(\mathbb{Z}/4\mathbb{Z})$，$(\mathbb{Z}/12\mathbb{Z})$，$(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/6\mathbb{Z})$，$(\mathbb{Z}/2\mathbb{Z})^2\times(\mathbb{Z}/12\mathbb{Z})$，$(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/12\mathbb{Z})$，$(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/4\mathbb{Z})$，$(\mathbb{Z}/2\mathbb{Z})^2\times(\mathbb{Z}/4\mathbb{Z})$

(多一个扣0.5分，少一个扣0.5分)

3分扣完为止

2. 1. $f(x) = (x^5 - 14x^2 + 6)\, q(x) + r(x)$

$\deg r(x) \le 4. \Rightarrow f(\alpha) = r(\alpha)$

(5分) 所以 $\mathbb{Z}[\alpha]$ 由 5 个元素

$1, \alpha, \alpha^2, \alpha^3, \alpha^4$ 生成

2. 作业: α 代数整数 当且仅当 $\mathbb{Z}[\alpha]$ 作为 Abel 群有限生成.

(5分)

若 $\mathbb{Z}[\alpha^{-1}]$ 有限生成. α^{-1} 是代数整数.

α^{-1} 满足 $\underbrace{6x^5 - 14x^3 + 1}_{``h(x)"} = 0$

由 Eisenstein criterion $x^5 - 14x^2 + 6$ 在 $\mathbb{Q}[x]$ 中不可约

$\Rightarrow$ $h(x)$ 在 $\mathbb{Q}[x]$ 中不可约

(因为 若 $h(x) = h_1(x) \cdot h_2(x)$.

则 $x^5 h(\frac{1}{x}) = x^{(\deg h_1)} h_1(\frac{1}{x})\, x^{(\deg h_2)} h_2(\frac{1}{x})$)

$h(x)$ primitive in $\mathbb{Z}[x]$ $\Rightarrow$ $h(x)$ 在 $\mathbb{Z}[x]$ 中不可约

若 $g(\alpha)=0$ 且 g 首一

$g(x)\in\mathbb{Z}[x]$,

则 $g.c.d(h(x), g(x))$ in $\mathbb{Q}[x]$ $\neq 1$

所以 $h(x) \mid g(x)$. 与 $g(x)$ 首1矛盾.
in $\mathbb{Z}[x]$

所以 $\mathbb{Z}[\alpha^{-1}]$ 不是有限生成 abel 群.

3. $f: \mathbb{R} \to \mathbb{R}$

3分

① 先证明: $f|_{\mathbb{Q}}: \mathbb{Q} \to \mathbb{Q}$ 是恒等

$\forall n \in \mathbb{Z}_{\geq 0}$ $f(n) = f(1+\cdots+1) = f(1)+\cdots+f(1)$

$= n$

$f(-n) = -f(n) = -n$

$\forall \frac{p}{q} \in \mathbb{Q}$, $p, q \in \mathbb{Z}$, $q > 0$

$q f(\frac{p}{q}) = f(q \frac{p}{q}) = f(p) = p$

$\Rightarrow f(\frac{p}{q}) = \frac{p}{q}$.

(假设]连续条件这一部分不给分)

② 7分 $\forall x > 0$. $f(x) = f((\sqrt{x})^2)$

$= (f(\sqrt{x}))^2 > 0$

$\Rightarrow \forall x > y$, $f(x-y) = f(x) - f(y) > 0$

$f(x) > f(y)$

$\forall\ \alpha \in \mathbb{R}$, 取 $\alpha_1 \cdots \alpha_n \cdots \in \mathbb{Q}$, $\alpha_i < \alpha_{i+1} < \alpha$

$\beta_1 \cdots \beta_n \cdots \in \mathbb{Q}$ $\beta_i > \beta_{i+1} > \alpha$

$$\lim_{n \to \infty} \alpha_n = \lim_{n \to \infty} \beta_n = \alpha$$

则 $\alpha_n = f(\alpha_n) < f(\alpha) < f(\beta_n) = \beta_n$

Take $\lim_{n \to \infty}$ $\alpha \le f(\alpha) \le \alpha$

$\Rightarrow f(\alpha) = \alpha$

4. 1. $\alpha = a + b\frac{1+\sqrt{-3}}{2}$ $a, b \in \mathbb{Z}$.

5(1)
p

$\alpha \cdot \alpha^{-1} = 1. \Rightarrow N(\alpha) \cdot N(\alpha^{-1}) = 1$

$\Rightarrow N(\alpha) \mid 1 \Rightarrow N(\alpha) = 1$

$\Rightarrow (a + \frac{b}{2})^2 + \frac{3}{4}b^2 = a^2 + ab + b^2$
$= 1$

$a, b \in \mathbb{Z}. \Rightarrow |a|, |b| \leq \frac{2}{\sqrt{3}}$

$\Rightarrow a, b = \pm 1, 0$

代入检验, $\Rightarrow \alpha = \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}$, 6个.

$w = \frac{1+\sqrt{-3}}{2}$, 则 α为 $1, w, w^2, w^3, w^4, w^5$.

所以 $R^\times \cong \mathbb{Z}/6\mathbb{Z}$

2. $\rho: R \to \mathbb{C}[t]$

$x \mapsto t^2$

5分

$y \mapsto t^3$

Claim: ρ 单同态，因为 $\rho(f(x,y))=0$

由 DNR，$f(x,y) = a_1(x) + y\, a_2(x)$

$\rho(f) = a_1(t^2) + t^3 a_2(t^2)$

由 t 的奇偶次项 $\Rightarrow a_1 = a_2 = 0$

(2) $R^\times \hookrightarrow \mathbb{C}[t]^\times$

而 $\mathbb{C}[t]^\times = \mathbb{C}^\times$

由于 $\deg(f_1 f_2) = \deg f_1 + \deg f_2$

$\Rightarrow R^\times = \mathbb{C}^\times$

即 $R^\times = \{a \mid a \in \mathbb{C},\ a \neq 0\}$

5. 1. 存在标准正交基，使得 Q 的矩阵为对角阵 $A = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$ 且 $\lambda_i \in \mathbb{R}$.

7分

又由于 $1-\sqrt{-1}\lambda_i \neq 0$，$\Rightarrow$ $I_n - A$ 可逆.

$\Rightarrow$ $I - AQ$ 可逆

$\Rightarrow$ U 的矩阵 $B = \begin{bmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{bmatrix}$

且 $\mu_i = \dfrac{1+\lambda_i\sqrt{-1}}{1-\lambda_i\sqrt{-1}}$

$\Rightarrow$ $|\mu_i| = 1$

$\Rightarrow$ $\overline{B}^T B = I_n$

$\Rightarrow$ U 是 unitary.

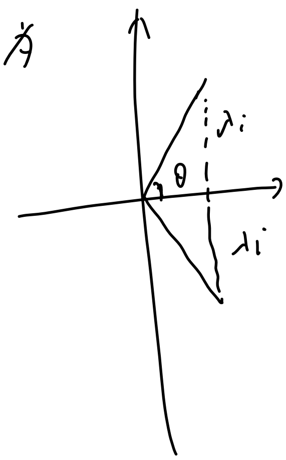
2. 由以上讨论，若 U 在某一组标准正交基下为对角阵 $\begin{pmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{pmatrix}$ $|\mu_i| = 1$

3分

令 $\mu_i = \dfrac{1+\lambda_i\sqrt{-1}}{1-\lambda_i\sqrt{-1}}$ $(*)$ $\lambda_i \in \mathbb{R}$

则 $(*)$ 有解 $\lambda_i \in \mathbb{R}$ 当且仅当 $\mu_i \neq -1$

因为



$\tan\theta = \lambda_i$，μ_i 的辐角为 2θ.

存在这样的 Q 当且仅当 U 没有 -1 为特征值.

$d=-19 \equiv 1 \pmod 4$

6\. 1. $\lfloor \mu \rfloor = \lfloor \sqrt{\frac{|d|}{3}} \rfloor = 2$

5分 检验 $x^2 - x + \frac{1-d}{4}$

$= x^2 - x + 5 \mod 2$

是否不可约. $x^2 - x + 1 \mod 2$ ✓

$\Rightarrow R$ PID $\Rightarrow R$ UFD

2\. $22 = 2 \cdot 11 = (1+\sqrt{-21})(1-\sqrt{-21})$

5分 2 不可约. 因为 若, $a, b, c, d \in \mathbb{Z}$

$2 = (a+b\sqrt{-21})(c+d\sqrt{-21})$

$4 = (a^2+21b^2)(c^2+d^2 21)$

$\Rightarrow b = d = 0$

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

$\cong \mathbb{F}_2[x]/(x+1)^2$

非整环

$\Rightarrow$ 2 不是素元

$\Rightarrow$ R 不是 UFD

G

7. 1. $f: (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2$

4分 $(a, (b, c))$

$x = f(1, (0,0))$ 是 G 中的4阶元

有 $4 \cdot 2^2 - 2^3 = 16 - 8 = 8$ 种.

$y = f(0, (1,0))$ 是 G 中2阶元

且不在 $\langle x \rangle$ 中,

有 $2^3 - 2 = 6$ 种

$z = f(0, (0,1))$ 是 G 中2阶元

且不在 $\langle x, y \rangle$ 中

$2^3 - 2^2 = 4$ 种

$8 \cdot 6 \cdot 4 = 3 \cdot 2^6$

2. 考虑素数 p，以及 $G_0 = \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p^{n_2}\mathbb{Z}$

(6分)

(a, b)

$n_1 \geq n_2 \geq 1$

构造

$f \in Aut(G_0)$

$g \in Aut(G_0)$

$$f(1,0) = (1,1)$$

$$f(0,1) = (0,1)$$

$$g(1,0) = (x,0) \quad . \quad x \in (\mathbb{Z}/p^{n_1}\mathbb{Z})^\times$$

$$g(0,1) = (p^{n_1-n_2}, 1)$$

则 $fg(1,0) = (x, x)$

$gf(1,0) = (x+p^{n_1-n_2}, 1)$

$$f\cdot g \neq gf \quad in \quad Aut(G_0)$$

若 G 为有限非循环交换群，则有 $G \cong G_1 \times G_0$ 某个 p, n_1, n_2

$(id, f), (id, g) \in Aut(G)$，且不交换

8. "1 ⇒ 2" 考虑 $n=1$.

"8分" R 的理想 $I \cong R^m$.

若 $m \geq 2$, 存在 $a, b \in I$, $a, b \neq 0$

s.t. a, b 对应 R^m 中某一组基的

不同两个元素

而 $ba - ab = 0$, 与 a, b

R 线性无关矛盾, ⇒ $I \cong R$

即 $I = (a)$ 主理想 4分

若对 $\forall a \neq 0, a \in R$, 有 $b \neq 0$, $b \cdot a = 0$, 则

$b \cdot (a) = 0$. 与 (a) 为自由模矛盾

⇒ R 是整环, ⇒ R 是PID

整环 4分

" $2 \Rightarrow 1$ " 由于 R noether. R^n 的子模 M 有限生成.

R^n 的子模 torsion free $\Rightarrow$ M torsion free

R 上有限生成模定理.

$\Rightarrow$ M 自由. $\cong R^m$ 2分

9. $1 \Rightarrow 2.$ $\quad e: W(K) \to \mathbb{Z}/2\mathbb{Z}$

$\langle 1 \rangle$ 是 $W(K)$ 中非平凡元素（非零）

$\forall a \neq 0 \in K$

$\begin{bmatrix} 1 & \\ & -a \end{bmatrix}$ 是 isotropic. 否则

反例 $\begin{bmatrix} 1 & \\ & -a \end{bmatrix}$ 是 $W(K)$ 中与 $\langle 1 \rangle$ 不同的非平凡元素（非零）

$\Rightarrow \exists\, x, y \in K, \quad x^2 - ay^2 = 0$

$\Rightarrow \quad a = \left(\frac{x}{y}\right)^2$

"$2 \Rightarrow 1$" $\quad \forall$ $a_1, \dots, a_n \neq 0 \in K.$ $\langle a_1, \dots, a_n \rangle \cong$

反例 $\langle 1, \dots, 1 \rangle$

$\langle 1, 1 \rangle \cong \langle 1, -1 \rangle$

If n odd $\Rightarrow \langle 1, \dots, 1 \rangle$

$\cong \langle 1 \rangle \perp (\langle 1, -1 \rangle)^{\perp \frac{n-1}{2}}$

If n even $\langle 1, \dots, 1 \rangle \cong (\langle 1, -1 \rangle)^{\perp \frac{n}{2}}$

$\Rightarrow$ $W(K)$ has two elements.

$W(K) \cong \mathbb{Z}/2\mathbb{Z}$.

---

10. 由于 T 可对角化，则 T 的 minimal polynomial irreducible $f(x)$ 无重根.

而 $T|_W$ 时 $f(T|_W)=0$

(10分)

$\Rightarrow$ $T|_W$ 的 minimal polynomial 无重根

$\Rightarrow$ $T|_W$ 可对角化.

即 $V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$

$$V_{\lambda_i} = \ker(T-\lambda_i I)$$

$$W = W_{\lambda_1} \oplus \cdots \oplus W_{\lambda_s}$$

$$W_{\lambda_i} = \ker(T|_W - \lambda_i I)$$

所以 $W_{\lambda_i} = V_{\lambda_i} \cap W$

对 $W_{\lambda_i} \subset V_{\lambda_i}$ $\quad T|_{V_{\lambda_i}} = \lambda_i I$

所以 存在 $U_{\lambda_i} \subset V_{\lambda_i}$ $\quad T|_{U_{\lambda_i}}$ 不变

s.t. $U_{\lambda_i} \oplus W_{\lambda_i} = V_{\lambda_i}$

取 $U = U_{\lambda_1} \oplus \cdots \oplus U_{\lambda_s}$. T-不变

有 $W \oplus U = V$.

11. $F^4 = V \perp W$, $W = \ker g$

1. 1.1 $\dim V = 4$. $\langle 1, 1, 1, 1 \rangle$ 一种

5种 1.2. $\dim V = 3$. $\langle 1, 1, 1 \rangle$ 一种

1.3 $\dim V = 2$. $\langle 1, 1 \rangle$

1.4 $\dim V = 1$ $\langle 1 \rangle$

1.5. $\dim V = 0$

5分

$\langle 1, 1, 1, 1 \rangle$, $\langle 1, 1, 1, 0 \rangle$

$\langle 1, 1, 0, 0 \rangle$, $\langle 1, 0, 0, 0 \rangle$

$\langle 0, 0, 0, 0 \rangle$

2. 2.1 $\dim V = 4$. $\langle 1, 1, 1, 1 \rangle$, $\langle 1, 1, 1, -1 \rangle$

$\langle 1, 1, -1, -1 \rangle$, $\langle 1, -1, -1, -1 \rangle$

$\langle -1, -1, -1, -1 \rangle$

5种.

5分

2.2. $\dim V = 3$. $\langle 1, 1, 1\rangle$, $\langle 1, 1, -1\rangle$

$\langle 1, -1, -1\rangle$, $\langle -1, -1, -1\rangle$

4 种

2.3 $\dim V = 2$. $\langle 1, 1\rangle$, $\langle 1, -1\rangle$, $\langle -1, -1\rangle$

3 种

2.4 $\dim V = 1$ $\langle 1\rangle$, $\langle -1\rangle$ 2 种

2.5. $\dim V = 0$

10 种

3. 3.1 $\dim V = 4$, $V \cong \langle 1, -1\rangle \perp \langle 1, a\rangle$

(3 维 isotropic) $\Rightarrow$

因此由 case 3.3 $\langle 1, a\rangle$ 2 种

$p \equiv 3 \pmod 4$ $\{1, -1\} = \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ $\langle 1, -1\rangle$, $\langle 1, 1\rangle$

$\langle 1, 1, -1, -1\rangle$. $\langle 1, -1, 1, 1\rangle$

3.2 $\dim V = 3$. $\langle 1, -1, a\rangle$. $a = \pm 1$ 2 种

$\langle 1, -1, 1\rangle$

$\langle 1, -1, -1\rangle$

5 分

3.3 $\dim V = 2$. $\langle 1, a \rangle$. $a = \pm 1$ 2种.

3.4 $\dim V = 1$ $\langle a \rangle$ $a = \pm 1$ 2种

3.5 $\dim V = 0$

9种.

12. 1. $|G| = (p^3-1)(p^3-p)(p^3-p^2)$ 1分

$|H| = \dfrac{|G|}{p-1}$ 1分

2. G 中一个 Sylow 3- subgroup

5分 是 $U = \left\{ \begin{pmatrix} 1 & x & x \\ & 1 & x \\ & & 1 \end{pmatrix} \right\}$

下证 U 的 normaliter 是 B = {上三角阵}

设 $A \in GL(3, \mathbb{F}_p)$

$AU = UA$

$\Rightarrow A \cdot \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \cdot A$

$A \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a & b \\ & 0 & c \\ & & 0 \end{pmatrix} \cdot A$

$$\Rightarrow \begin{pmatrix} 0 & a_{11} & 0 \\ 0 & a_{21} & 0 \\ 0 & a_{31} & 0 \end{pmatrix} = \begin{pmatrix} & * & \\ 0 & 0 & 0 \end{pmatrix}$$

$a_{31} = 0$. 同理 $A \cdot \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix} A^{-1} \in U$

$$\Rightarrow \quad a_{32} = 0$$

$$A \cdot \begin{pmatrix} 0 & d & e \\ & 0 & f \\ & & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ & 0 & 0 \\ & & 0 \end{pmatrix} \cdot A$$

$$\Rightarrow \begin{pmatrix} 0 & & \\ 0 & * & \\ 0 & & \end{pmatrix} = \begin{pmatrix} a_{21} & a_{22} & a_{23} \\ & * & \end{pmatrix}$$

$$\Rightarrow \quad a_{21} = 0$$

故 $A \in B$.

若 $A \in B$, 则 $A = \begin{pmatrix} a & & * \\ & b & \\ & & c \end{pmatrix}$

$$A^{-1} = \begin{pmatrix} a^{-1} & & \\ & b^{-1} & * \\ & & c^{-1} \end{pmatrix}$$

$$A \cdot \begin{pmatrix} 1 & & \\ & 1 & * \\ & & 1 \end{pmatrix} \cdot A^{-1} = \begin{pmatrix} 1 & & * \\ & 1 & \\ & & 1 \end{pmatrix} \in U$$

所以 B 是 U 在 G 中的 normalizer

$\Rightarrow$ Sylow p-subgroup 个數 $= \dfrac{|G|}{|B|}$

$$= \frac{(p^3-1)(p^3-p)(p^3-p^2)}{(p-1)^3 \cdot p^3}$$

$$= (p^2+p+1)(p+1)$$

以上也推出 $B \cap SL(3, \mathbb{F}_p)$ 是 U 在 H 中的 normalizer

所以 H 的 Sylow p-group 也有 $(p^2+p+1)(p+1)$ 个

8分　(8个数) 一类 一分

③ $\mathbb{F}_p[x]$ 中 不可约多项式

$\deg = 1$, x, $x-a$　$a \in \mathbb{F}_p^*$

$\deg = 2$, x^2+ax+b, 有 $p^2 - \left(\binom{p}{2} + p\right)$

$\deg = 3$,　$= p^2 - \frac{p(p+1)}{2}$

x^3+ax^2+bx+c　$= \frac{p(p-1)}{2}$

有 $p^3 - p\cdot\left(\frac{p(p-1)}{2}\right)$

$- \left(\binom{p}{3} + p(p-1) + p\right)$

$p^3 - \left(\frac{p^3}{2} - \frac{p^2}{2} + \frac{p(p-1)(p-2)}{6} + p^2\right)$

$= p^3 - \left(\frac{p^3}{2} - \frac{p^2}{2} + \frac{p^3-3p^2+2p}{6} + p^2\right)$

$= p^3 - \left(\frac{2}{3}p^3 + \frac{p}{3}\right)$

$= \frac{1}{3}(p^3 - p)$

$A \in GL(3, \mathbb{F}_p)$ 的初等因子

一个 3 次，$\frac{1}{3}(p^3-p) + (p-1)$

一个 2 次，一个 1 次 $\frac{1}{2}(p^2-p) \times (p-1)$

$+ (p-1)(p-2) + (p-1)$

3个 1 次，$\binom{p-1}{3} + \binom{p-1}{2} \cdot 2 + (p-1)$

加起来 $p^3 - p$

附加题　　8种　一种一分.

	类型	个数	Normalizer	size
1	一个3次不可约 $f(x)$	$\frac{1}{3}(p^3-p)$	$(F_p[x]/f(x))^\times$ p^3-1	$(p^3-p)(p^3-p^2)$
2	一个 $(x-a)^3$	$p-1$	$(F_p[x]/(x-a)^3)^\times$ p^3-p^2	$(p^3-1)(p^3-p)$
3	一个2次不可约 $f(x)$ 一个 $(x-a)$	$\frac{p(p-1)^2}{2}$	$(F_p[x]/(f(x)))^\times$ $\times\ (F_p)^\times$ $(p^2-1)(p-1)$	$p^3(p^3-1)$
4	一个 $(x-a)^2$ 一个 $(x-b)$, $a\neq b$	$(p-1)(p-2)$	$(F_p[x]/(x-a)^2)^\times$ $\times\ (F_p)^\times$ $(p^2-p)(p-1)$	$(p^2+p+1)(p+1)(p-1)$ p^2
5	一个 $(x-a)^2$ 一个 $(x-a)$	$(p-1)$	(p^3-p^2) (p^2-p)	$(p^2+p+1)(p^2-1)$
6	$(x-a)$ $(x-b)$ $(x-c)$ a, b, c distinct	$\binom{p}{3}$	$(p-1)^3$	$p^3(p+1)$ (p^2+p+1)
7	$(x-a)$, $(x-a)$ $(x-b)$ $a\neq b$	$\binom{p}{2}$	$(p^2-1)(p^2-p)$ $\cdot(p-1)$	$p^2(p^2+p+1)$
8	$(x-a)$, $(x-a)$ $(x-a)$	$(p-1)$	$\|G\|$	1

个数统计 wiki 上写反了.