第二次习题课（9.25）

一、有限域 $\mathbb{F}_p$ （p 是素数）

我们知道 $\mathbb{Z}$ 上有 $(\mathrm{mod}\ p)$ 运算

- $a \equiv b \pmod p \iff p \mid a-b \quad (\forall a,b\in\mathbb{Z})$
- 若 $p\nmid c$ 则 $ac \equiv bc \pmod p \Rightarrow a\equiv b \pmod p$
- 若 $a\equiv b \bmod p$ 则 $a+c \equiv b+c \pmod p$

不难发现，$\forall n\in\mathbb{Z}$，其会唯一对应于 $\{0,1,\cdots,p-1\}$ 中的一个元素

记 $\bar{a} = \{n\in\mathbb{Z} : a\equiv n \pmod p\}$，$a$ 为 $\bar{a}$ 的代表元、

（常取 $\bar{0},\bar{1},\cdots,\overline{p-1}$ 为代表元）

Prop、(1) 若 $a\equiv b \pmod p$ 则 $\bar{a}=\bar{b}$

(2) 若 $a\not\equiv b \pmod p$ 则 $\bar{a}\cap\bar{b}=\phi$.

pf. (1). $\forall n\in\bar{a}$. 有 $n\equiv a \bmod p$.

又由 $a\equiv b \pmod p \Rightarrow n\equiv a\equiv b \pmod p \Rightarrow n\in\bar{b}$

反之同理

(2) 若 $n\in\bar{a}\cap\bar{b}$，则 $\begin{cases} n\equiv a \bmod p \\ n\equiv b \bmod p\end{cases}$ 这与 $a\not\equiv b \bmod p$ 矛盾. $\square$

我们对 $\{\bar{0},\cdots,\overline{p-1}\}$ 定义运算 $(+,\cdot)$

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

Prop: 这样定义的运算不依赖代表元选取.

pf. (1) 只需证明. 若 $\begin{cases} a\equiv a' \bmod p \\ b\equiv b' \bmod p\end{cases}$ $\overline{a+b}=\overline{a'+b'}$

而这等价于证明 $a+b\equiv a'+b' \pmod p$. 而这由条件立得.

(2) Ex. $\square$

令 $\mathbb{F}_p=\{\bar{0},\cdots,\overline{p-1}\}$. 我们实际上定义了上面的乘法与加法、

·(定义). 域 $(k,+,\cdot)$ 称为域，如果

(1) $\exists\ 0, 1 \in k$. 使得 $\forall\ a \in k$

$a = a+0 = 0+a = a\cdot 1 = 1\cdot a$

0，1 为加法"零元"与乘法"幺元"

(2) 加法、乘法均满足交换律，结合律，分配律

i.e. $\forall\ a, b, c \in k$

(i) $a+b = b+a$, $a\cdot b = b\cdot a$

(ii) $a+(b+c) = (a+b)+c$.

$a\cdot(b\cdot c) = (a\cdot b)\cdot c$

(iii) $a\cdot(b+c) = a\cdot b + a\cdot c$

$(a+b)\cdot c = a\cdot c + b\cdot c$

(3) $\forall$ 元素均有加法"负元"，$\forall$ 非零元素有乘法"逆元".

即. $\forall\ a\in k$. $\exists\ b\in k$ $a+b=0$

$\forall\ a \in k^* = k\setminus\{0\}$. $\exists\ b\in k$ $a\cdot b = 1$.

注 在一般的"环""域"上，0, 1 一般不为 $\mathbb{Z}$ 上的 0, 1.

· Ex.（比较有趣的抽象练习）

(1) $\forall\ a\in k$. $a\cdot 0 = 0\cdot a = 0$

(2) 记 $1\in k$ 的负元为 $(-1)_{\in k}$，$a\in k$ 的负元为 $(-a)\in k$

则 $(-1)\cdot a = (-a)$

· Prop $(\mathbb{F}_p, +, \cdot)$ 定义了一个域

Pf. Ex.

· Example. $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$.

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Ex. 写出 $\mathbb{F}_5$, $\mathbb{F}_7$ 的乘法，加法表.

二. $\mathbb{F}_p[x]$ 及其上不可约多项式.

· $\mathbb{F}_p[x] = \{ a_n x^n + \cdots + a_0 \mid a_i \in \mathbb{F}_p,\ a_n \neq \bar{0} \}$

以 $\mathbb{F}_5[x]$ 为例　$x+\bar{1}$, $\bar{2}x^2+\bar{3}x+\bar{1}$ $\in \mathbb{F}_5[x]$.

(注意: $x+\bar{1} \in \mathbb{F}_3[x]$.　$x+\bar{1} \in \mathbb{F}_5[x]$.　两者并不相等!

x^p 与 x 在 $x=\bar{0},\bar{1},\cdots,\overline{p-1}$ 时均有一样的值，但两者不是同一多项式!)

· $\mathbb{F}_p[x]$ 上的不可约多项式

Def. $f \in \mathbb{F}_p[x]$ 称为不可约多项式

如果 $\forall\ gh = f$.　$g, h \in \mathbb{F}_p[x]$.

g, h 中有一个为单位.

(也即 g 或 $h \in \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$)

反之. f 称为可约多项式

如果 $\exists\ g, h$ 均不为单位. 且 $gh = f$. 也即 f 分解为两次数 ≥ 1 的多项式.

Example.　$\mathbb{F}_3[x]$ 中

次数为 1 的多项式　x, $x+\bar{1}$, $x+\bar{2}$, $\bar{2}x$, $\bar{2}x+\bar{1}$, $\bar{2}x+\bar{2}$

均为不可约多项式

次数为 2 的多项式为

x^2, $\underline{x^2+\bar{1}}$, $x^2+\bar{2}$, x^2+x, $x^2+x+\bar{1}$, $\underline{x^2+x+\bar{2}}$,

$x^2+\bar{2}x$, $x^2+\bar{2}x+\bar{1}$, $\underline{x^2+\bar{2}x+\bar{2}}$,

$\bar{2}x^2$, $\bar{2}x^2+\bar{1}$, $\underline{\bar{2}x^2+\bar{2}}$, $\bar{2}x^2+x$, $\underline{\bar{2}x^2+x+\bar{1}}$, $\bar{2}x^2+x+\bar{2}$

$\bar{2}x^2+\bar{2}x$, $\underline{\bar{2}x^2+\bar{2}x+\bar{1}}$, $\bar{2}x^2+\bar{2}x+\bar{2}$

其中 $\boxed{}$ 为不可约多项式

三 $\mathbb{Z}[x]$ 的模 p 约化.

$$\pi: \mathbb{Z} \to \mathbb{F}_p$$
$$n \mapsto \bar{n}$$

该映射诱导了 $\pi: \mathbb{Z}[x] \to \mathbb{F}_p[x]$.
$$f(x) \mapsto \overline{f(x)}$$

令 $f(x) = \sum_{i=1}^{n} a_i x^i$ 则 $\pi(f(x)) = \sum_{i=0}^{n} \bar{a_i} x^i$

Ex. $\pi(f(x)\cdot g(x)) = \pi(f(x))\cdot\pi(g(x))$

(左边 $f\cdot g$ 在 $\mathbb{Z}[x]$ 中进行、右边 $\pi(f(x))\cdot\pi(g(x))$ 在 $\mathbb{F}_p[x]$ 中进行.

应用一、证明 Eisenstein 判别法.

Thm. (Eisenstein). 若 $f(x) = a_n x^n + \cdots a_0 \in \mathbb{Z}[x]$.

且 $\exists$ p 素数 $p \nmid a_n$, $p \mid a_i$ $0 \le i < n$. $p^2 \nmid a_0$.

则 $f(x)$ 在 $\mathbb{Q}[x]$ 上不可约.

Pf. 反证 若 $f(x)$ 在 $\mathbb{Q}[x]$ 上可约

由 Thm 5.5.3. $f(x) = g(x)\, h(x)$. 其中 $g(x)$. $h(x) \in \mathbb{Z}[x]$.

$\deg g(x)$, $\deg h(x) \ge 1$

由 $x^n = \pi(f(x)) = \pi(g(x)\, h(x)) = \pi(g(x))\ \pi(h(x))$

即 $\overline{g(x)} \cdot \overline{h(x)} = x^n$ ($\mathbb{F}_p[x]$ 意义下)

则. $\overline{g(x)} = x^l$. $\overline{h(x)} = x^{n-l}$ $(0 < l < n)$ (想想为什么)

也即 设 $g(x) = b_l x^l + \cdots b_0$,

$h(x) = c_{n-l} x^{n-l} + \cdots + c_0$ 则. $p \mid b_0$, $p \mid c_0$

但 $a_0 = b_0 c_0 \Rightarrow p^2 \mid a_0$ 矛盾. $\square$

应用二. 一种非常有价值的判断不可约多项式的办法.

☆ Thm. $f(x) \in \mathbb{Z}[x]$. p 素, $p \nmid LC(f)$. 首项系数

如果 $\overline{f(x)} = \pi(f(x))$ 在 $\mathbb{F}_p[x]$ 上不可约

则 $f(x)$ 在 $\mathbb{Q}[x]$ 上不可约

pf. (反证) 若 $f(x)$ 在 $\mathbb{Q}[x]$ 上可约.

由 thm 5.5.3, $f(x) = g(x)\,h(x)$.

其中 $\deg g(x), \deg h(x) \geq 1$. 且 $g(x)$, $h(x) \in \mathbb{Z}[x]$.

则 $\overline{f(x)} = \pi(f(x)) = \pi(g(x)h(x)) \overset{EX}{=\!=} \pi(g(x)) \cdot \pi(h(x))$

注意到 $p \nmid LC(f) \Rightarrow \deg \overline{g(x)}, \deg \overline{h(x)} \geq 1$

这与 $\overline{f(x)}$ 不可约矛盾. $\square$

注: 其"否命题"不对. 反例为 x^4+1

$x^4+\bar{1}$ 在 $\mathbb{F}_p[x]$. $\forall p$ 素 上可约

但 x^4+1 不可约 in $\mathbb{Q}[x]$.

$x^4+\bar{1}$ 在 $\forall\ \mathbb{F}_p[x]$ 可约 留作思考题!

Example $x^3+2x+1 \in \mathbb{Z}[x]$. 不可约.

理由. $x^3+\bar{2}x+\bar{1} \in \mathbb{F}_3[x]$. 取 $x=\bar{0}, \bar{1}, \bar{2}$ 均不是解.

故 不可约 in $\mathbb{F}_3[x]$. $\Rightarrow f(x)$ 不可约 in $\mathbb{Z}[x]$.

优点: 在 $\mathbb{F}_p[x]$ 中 系数选择有限. 待定系数/求根 更方便

缺点: p 的选取.

第二次作业解答.

2. 证明：如果$(x^2+x+1)\mid(f_1(x^3)+xf_2(x^3))$，则$(x-1)$同时整除$f_1(x)$与$f_2(x)$.

证明. 法一: 取 ω 为 $x^2+x+1=0$ 的解.

观察到 ω^2 也是解 且 $\omega^3=1$

由于 $x-\omega,\ x-\omega^2 \mid x^2+x+1$

$\Rightarrow$ 令 $g(x)=f_1(x^3)+xf_2(x^3)$. $g(\omega)=g(\omega^2)=0$.

$$\Rightarrow \begin{cases} f_1(\omega^3)+\omega f_2(\omega^3)=0. \\ f_1(\omega^6)+\omega^2 f_2(\omega^6)=0 \end{cases}$$

由于 $\det\begin{pmatrix}1&\omega\\1&\omega^2\end{pmatrix}\neq0 \Rightarrow f_1(1)=f_2(1)=0$

故 $x-1\mid f_1(x)$, $x-1\mid f_2(x)$

另证 设 $f_1(x)=\sum_{i=0}^{n}a_i(x-1)^i$. $f_2(x)=\sum_{i=0}^{m}b_i(x-1)^i$

注意到 $x^2+x+1\mid x^3-1$

故 $f_1(x^3)+xf_2(x^3)=(a_0+b_0x)+\sum_{i\geq1}a_i(x^3-1)+\sum b_i(x^3-1)$

故 $a_0=b_0=0$.

即 $x-1\mid f_1(x)$, $x-1\mid f_2(x)$, □

5. a，b都是有理数且$b\neq0$，$a+b\sqrt{2}$是有理系数多项式$f(x)$的根，求证：$a-b\sqrt{2}$一定也是$f(x)$的根.

证. 法一. 首先 $g(x)=(x-a)^2-2b^2$ 是次数最小的首一的 以 $a+b\sqrt{2}$ 为根的 Q系数多项式

设 $f(x)=q(x)g(x)+r(x)$

则有 $f(a+b\sqrt{2})=q(a+b\sqrt{2})g(a+b\sqrt{2})+r(a+b\sqrt{2})$

$\Rightarrow r(a+b\sqrt{2})=0$

而 $r(x)\in\mathbb{Q}[x]$. 若 $r(x)\neq0 \Rightarrow \deg r<\deg g=2$

$$\begin{cases} r(a+b\sqrt{2})=0 \\ r(x)\in\mathbb{Q}[x]. \end{cases} \Rightarrow$$ 这与 $g(x)$ 次数最小矛盾.

法二、 设 $f(x)=\sum_{i=0}^{n} a_i x^i$

考虑映射 $\sigma:\ \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, $\quad (\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\})$

$a+b\sqrt{2} \longmapsto a-b\sqrt{2}$.

可验证 $\forall\ a,b,c,d\in\mathbb{Q}$

i $\sigma(a\cdot(b+c\sqrt{2})) = a\ \sigma(b+c\sqrt{2})$

ii $\sigma((a+b\sqrt{2})\cdot(c+d\sqrt{2})) = \sigma(a+b\sqrt{2})\cdot\sigma(c+d\sqrt{2})$

则 由于 $f(a+b\sqrt{2})=0$. 即 $\sum a_i (a+b\sqrt{2})^i=0$

两边作用 σ 利用性质 i, ii

即 $\sum a_i (a-b\sqrt{2})^i=0$

故 $f(a-b\sqrt{2})=0$ $\square$

7. 证明：多项式 $1+x+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}$ 没有重根.

Pf. $f(x)=\sum_{i=0}^{n}\frac{x^i}{i!}$

无重根 $\Leftrightarrow$ $\gcd(f(x), f'(x))=1$

而 $f'(x)=\sum_{i=0}^{n-1}\frac{x^i}{i!}$

故 $\gcd(f,f')=\gcd(f-f', f')$

$=\gcd\left(\frac{x^n}{n!},\ 1+x+\cdots+\frac{x^{n-1}}{(n-1)!}\right)$

因为 $\gcd\left(x,\ 1+x+\cdots+\frac{x^{n-1}}{(n-1)!}\right)=\gcd(x,1)=1$

故 $\gcd\left(x^n,\ 1+x+\cdots+\frac{x^{n-1}}{(n-1)!}\right)=1$ $\square$

9. 设 a，b，c 是方程 $x^3+qx+r=0$ 的根．写出根为 $\frac{b+c}{a^2}$，$\frac{c+a}{b^2}$，$\frac{a+b}{c^2}$ 的三次方程．

解. 由韦达定理. $a+b+c=0 \Rightarrow \frac{b+c}{a^2}=-\frac{1}{a}$

因为 a 满足 $x^3+px+r=0$

令 $t=-\frac{1}{a} \Rightarrow a=-\frac{1}{t} \Rightarrow (-\frac{1}{t})^3+p\cdot(-\frac{1}{t})+r=0$

整理后. 即为 $rt^3-pt^2-1=0$

11. 分别在复数域、实数域上将下列多项式分解为不可约多项式的乘积：

(1) x^4+4;　　　　(2) $(x-1)^n+(x+1)^n$;

(3) $x^{12}-1$;　　　　(4) $x^{2n}+x^n+1$.

解. (1). $x^4+4 = x^4+4x^2+4-4x^2 = (x^2+2)^2-(2x)^2$

$= (x^2+2x+2)(x^2-2x+2)$　　$(\mathbb{R})$

$= (x+1+i)(x-1+i)(x+1-i)(x-1-i)$　　$(\mathbb{C})$

(2) 先考虑方程 $(x+1)^n+(x-1)^n=0$

显然 $x=1$ 不是根.

故 $\left(\frac{x+1}{x-1}\right)^n = -1$

令 $w = e^{\frac{2\pi}{2n}i}$，则 w 为 $2n$ 次本原单位根

故 $\frac{x+1}{x-1} = w^{2k-1}$.　　$1 \le k \le n$

故 $x = \frac{1+w^{2k-1}}{w^{2k-1}-1}$

记 $\theta = \frac{\pi}{n}$. 则 $x = \frac{1+\cos(2k-1)\theta + i\sin(2k-1)\theta}{\cos(2k-1)\theta - 1 + i\sin(2k-1)\theta}$

$= \frac{2\cos^2\frac{2k-1}{2}\theta + 2i\sin\frac{2k-1}{2}\theta\cos\frac{2k-1}{2}\theta}{-2\sin^2\frac{2k-1}{2}\theta + 2i\sin\frac{2k-1}{2}\theta\cos\frac{2k-1}{2}\theta}$

$= \cot\frac{2k-1}{2}\theta \cdot \frac{\cos\frac{2k-1}{2}\theta + i\sin\frac{2k-1}{2}\theta}{-\sin\frac{2k-1}{2}\theta + i\cos\frac{2k-1}{2}\theta}$

$= -i\cot\frac{2k-1}{2}\theta$

故 $(x+1)^n+(x-1)^n = 2\prod_{k=1}^{n}\left(x+i\cot\frac{2k-1}{2}\cdot\frac{\pi}{n}\right)$　　$(\mathbb{C})$

$\cot\frac{2k-1}{2}\cdot\frac{\pi}{n} = -\cot\frac{2(n+1-k)-1}{2}\cdot\frac{\pi}{n}$

i 对 $n=2m$ 偶数　可以两两配对

$(x+1)^n+(x-1)^n = 2\prod_{k=1}^{\frac{n}{2}}\left[x^2+\left(\cot\frac{2k-1}{2n}\pi\right)^2\right]$　　$(\mathbb{R})$

ii 对 $n=2m+1$ 奇数

中间出现一项 x，其余两两配对

$(x+1)^n+(x-1)^n = 2x\prod_{k=1}^{\frac{n-1}{2}}\left[x^2+\left(\cot\frac{2k-1}{2n}\pi\right)^2\right]$　　$(\mathbb{R})$

□

注意 系数 2.

(3) $x^{12}-1=\prod_{i=0}^{11}(x-w^i)$ $(\mathbb{C})$ $w=e^{\frac{2\pi}{12}i}=e^{\frac{\pi}{6}i}$

$w^2=e^{\frac{\pi}{3}i}=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}=\frac{1}{2}+\frac{\sqrt{3}}{2}i$

$w^3=e^{\frac{\pi}{2}i}=i$

$w^4=e^{\frac{2}{3}\pi i}=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$

$w^5=\cos\frac{5}{6}\pi+i\sin\frac{5}{6}\pi=-\frac{\sqrt{3}}{2}+\frac{1}{2}i$, $w^6=-1$

故 $x^{12}-1=(x-w^0)\cdot[(x-w^1)(x-w^{11})]\cdot[(x-w^2)(x-w^{10})]$

$\cdot[(x-w^3)(x-w^9)]\cdot[(x-w^4)(x-w^8)]$

$\cdot[(x-w^5)(x-w^7)]\cdot(x-w^6)$

$=(x-1)(x+1)\cdot(x^2-2\mathrm{Re}\,w^1x+1)(x^2-2\mathrm{Re}\,w^2x+1)$

$(x^2-2\mathrm{Re}\,w^3x+1)(x^2-2\mathrm{Re}\,w^4x+1)(x^2-2\mathrm{Re}\,w^5x+1)$

$=(x-1)(x+1)(x^2-\sqrt{3}x+1)(x^2-x+1)(x^2+1)(x^2+x+1)(x^2+\sqrt{3}x+1)$

$(\mathbb{R})$

(4) $(x^{2n}+x^n+1)(x^n-1)=x^{3n}-1$.

考虑 $w=e^{\frac{2\pi}{3n}i}$ 为 $3n$ 次本原单位根

则 $x^{2n}+x^n+1$ 的所有根为 w^{3k+1} 及 w^{3k+2} 型.

$0\le k\le n-1$

故 $x^{2n}+x^n+1=\prod_{k=0}^{n-1}(x-w^{3k+1})(x-w^{3k+2})$

注意到 $\overline{w^{3k+1}}=\frac{1}{w^{3k+1}}=w^{3n-(3k+1)}=w^{3(n-k-1)+2}$

故 k 从 0 到 $n-1$

$(x-w^{3k+1})$ 与 $(x-w^{3(n-1-k)+2})$ —— 对应

故 $x^{2n}+x^n+1=\prod_{k=0}^{n-1}(x-w^{3k+1})\overline{(x-w^{3k+1})}$

$=\prod_{k=0}^{n-1}(x^2-2\mathrm{Re}\,w^{3k+1}x+1)$

$=\prod_{k=0}^{n-1}(x^2-2x\cos\frac{2(3k+1)}{3n}\pi+1)$ $(\mathbb{R})$.

习题 5.5.3 (2)

$a_1, \cdots, a_n$ 为两两不同的整数，求证 $(x-a_1)^2 \cdots (x-a_n)^2+1$ 不可约

pf. 设 $f(x) = \prod_{i=1}^{n}(x-a_i)^2+1$ 可约 $= g(x)\, h(x)$.

其中 g, h 可设为 $\mathbb{Z}[x]$ 多项式 首一.

注意到 $g(a_i)\, h(a_i) = f(a_i) = 1 \quad \forall i$

故 $g(a_i) = h(a_i) = \pm 1$.

注意到 $f(x) \geq 1 > 0$ 恒成立.

故，若 $\exists\ i, j$. $g(a_i) = 1$, $g(a_j) = -1$

则 (a_i, a_j) 或 (a_j, a_i) 间存在 g 的零点 x_0

$\Rightarrow f(x_0) = g(x_0)\, h(x_0) = 0$ 矛盾

由 g 首项为 1，故 $\lim_{x\to\infty} g(x) \to \infty$

故 $g(x) > 0$ 恒成立.

$\Rightarrow \forall i \quad g(a_i) = h(a_i) = 1$

由于 $\deg g + \deg h = 2n$

不妨 $\deg g \geq n \geq \deg h$

$h(x) - 1 = 0$ 有 $a_1, \cdots, a_n$ n 个不同零点.

$\Rightarrow \prod_{i=1}^{n}(x-a_i) \mid h(x) - 1$

又 $\deg h \leq n$. 且 h 首一

$\Rightarrow h(x) = \prod_{i=1}^{n}(x-a_i) + 1$

则 $\deg g = n$ 且 $\prod_{i=1}^{n}(x-a_i) \mid g(x) - 1$

$\Rightarrow g(x) = h(x)$

$\Rightarrow \prod_{i=1}^{n}(x-a_i)^2 + 1 = \left(\prod_{i=1}^{n}(x-a_i) + 1\right)^2$

这显然不对. $\square$

6. 下列多项式在有理数域上是否可约？并说明理由.

（1）x^6+x^3+1　　（2）x^4+4k+1，k 为整数；

（3）x^p+px+1，p 为奇素数.

Pf. (1). 令 $x=y+1$. 则 $(y+1)^6+(y+1)^3+1=y^6+6y^5+15y^4+21y^3+18y^2+9y+3$

取 $p=3$，利用 Eisenstein 判别法，即可.

(2) 令 $x=y+1$，则 $(y+1)^4+4k+1=y^4+4y^3+6y^2+4y+4k+2$

取 $p=2$. Eisenstein.

(3) 令 $x=y-1$. 则 $(y-1)^p+p(y-1)+1$

$$=y^p+\sum_{j=1}^{p-1}C_p^j\,y^j(-1)^{p-j}+py-p$$

注意到 对 $1\le j\le p-1$ $p\mid C_p^j$.

故 取 p. 验证 Eisenstein 即可

一个细节说明：

证明 $f(x)\in\mathbb{Q}[x]$ 不可约时，不能由已存在的一组出现无理数系数的多项式分解来判断 $\mathbb{Q}[x]$ 不可约.

错误示范. x^4-5x^2+6

证明. 因为 $f(x)$ 无 $\mathbb{Q}$ 解 $\Rightarrow$ 无一次因式

又 $f(x)=(x^2-(\sqrt{2}+\sqrt{3})x+\sqrt{6})(x^2+(\sqrt{2}+\sqrt{3})x+\sqrt{6})$

为两个二次因式乘积，且两个因子均 $\notin\mathbb{Q}[x]$

故由唯一分解定理知. $f(x)\in\mathbb{Q}[x]$ 上不可约多项式□

而实际上. $f(x)=(x^2-2)(x^2-3)\in\mathbb{Q}[x]$ 可约.

注：出现错误的地方在 唯一分解定理

要证 $\mathbb{Q}[x]$ 不可约. 要分解为 $\mathbb{R}[x]$（或 $\mathbb{C}[x]$）不可约多项式，再通过配凑 $\mathbb{R}[x]$ 的不可约因子说明 $\mathbb{Q}[x]$ 上不可约！