0.1 有理系数多项式

定理 0.1 (整数系数多项式有有理根的必要条件)

设有 n 次整系数多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, \tag{1}$$

则有理数 $\dfrac{q}{p}$ 是 $f(x)$ 的根的必要条件是 $p\mid a_n, q\mid a_0$, 其中 p,q 是互素的整数.

证明 将 $\dfrac{q}{p}$ 代入(1)式得

$$a_n\left(\frac{q}{p}\right)^n+a_{n-1}\left(\frac{q}{p}\right)^{n-1}+\cdots+a_1\left(\frac{q}{p}\right)+a_0=0,$$

将上式两边乘以 p^n 得

$$a_nq^n+a_{n-1}q^{n-1}p+\cdots+a_1qp^{n-1}+a_0p^n=0.$$

从而

$$q\left(a_nq^{n-1}+a_{n-1}q^{n-2}p+\cdots+a_1p^{n-1}\right)=-a_0p^n.$$

于是 $q\mid a_0p^n$, 又因为 $(q,p)=1$, 所以 $q\mid a_0$. 同理可得 $p\mid a_n$.

□

定义 0.1 (本原多项式)

设多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

是整系数多项式, 若 $a_n,a_{n-1},\cdots,a_1,a_0$ 的最大公约数等于 1, 则称 $f(x)$ 为**本原多项式**.

引理 0.1 (Gauss 引理)

两个本原多项式之积仍是本原多项式.

证明 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_1x+b_0$$

是两个本原多项式. 若

$$f(x)g(x)=c_{m+n}x^{m+n}+c_{m+n-1}x^{m+n-1}+\cdots+c_1x+c_0$$

不是本原多项式, 则 $c_0,c_1,\cdots,c_{m+n}$ 必有一个公约素因子 p. 因为 $f(x)$ 是本原多项式, 故 p 不能整除 $f(x)$ 的所有系数, 可设 $p\mid a_0, p\mid a_1,\cdots,p\mid a_{i-1}$, 但 p 不能整除 a_i. 同理, 可设 $p\mid b_0,p\mid b_1,\cdots,p\mid b_{j-1}$, 但 p 不能整除 b_j. 注意到

$$c_{i+j}=\cdots+a_{i-2}b_{j+2}+a_{i-1}b_{j+1}+a_ib_j+a_{i+1}b_{j-1}+\cdots,$$

p 可整除 c_{i+j},p 也能整除右式除 a_ib_j 以外的所有项. 但 p 不能整除 a_i 和 b_j, 故 p 不能整除 a_ib_j, 引出矛盾.

□

定理 0.2

若整系数多项式 $f(x)$ 在有理数域上可约, 则它必可分解为两个次数较低的整系数多项式之积.

证明 假设整系数多项式 $f(x)$ 可以分解为两个次数较低的有理系数多项式之积:

$$f(x) = g(x)h(x),$$

$g(x)$ 的各项系数为有理数, 必有一个公分母记为 c, 于是 $g(x) = \frac{1}{c}(cg(x))$, 其中 $cg(x)$ 为整系数多项式. 若把 $cg(x)$ 中所有系数的最大公因数 d 提出来, 则

$$g(x) = \frac{d}{c}\left(\frac{c}{d}g(x)\right),$$

$\frac{c}{d}g(x)$ 是一个本原多项式. 这表明 $g(x) = ag_1(x)$,a 为有理数,$g_1(x)$ 为本原多项式. 同理,$h(x) = bh_1(x)$, 其中 b 为有理数,$h_1(x)$ 为本原多项式. 于是我们得到

$$f(x) = g(x)h(x) = abg_1(x)h_1(x).$$

由Gauss 引理知,$g_1(x)h_1(x)$ 是本原多项式. 若 ab 不是一个整数, 则 $abg_1(x)h_1(x)$ 将不是整系数多项式, 这与 $f(x)$ 是整系数多项式相矛盾. 因此 ab 必须是整数, 于是 $f(x)$ 可以分解为两个次数较小的整系数多项式之积.

□

定义 0.2 (整系数多项式在整数环上可约)

我们通常称一个整系数多项式 $f(x)$ **在整数环上可约**, 若它可以分解为两个次数较低的整系数多项式之积. ♣

命题 0.1

整系数多项式 $f(x)$ 若在整数环上不可约, 则在有理数域上也不可约. ♠

证明 由定理 0.2即得.

□

例题 0.1 $f(x)$ 是次数大于零的首一整系数多项式, 若 $f(0), f(1)$ 都是奇数, 求证:$f(x)$ 没有有理根.

证明 若 c 是偶数, 则上述左边为奇数, 不可能等于零. 若 c 是奇数, 令 $c = 2b+1$, 其中 b 是整数, 可得

$$(2b+1)^n + a_{n-1}(2b+1)^{n-1} + \cdots + a_1(2b+1) + a_0 = 0.$$

用二项式定理展开后将看到, 上式左边是一个偶数加上 $1 + a_{n-1} + \cdots + a_1 + a_0$, 故必是奇数, 也不可能等于零. 因此 $f(x)$ 没有有理根.

□

命题 0.2

设 $f(x)$ 是实系数多项式, 若对任意的有理数 c,$f(c)$ 总是有理数, 求证:$f(x)$ 是有理系数多项式. ♠

注 证明与命题**??**

证明 设 $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, 分别令 $x = 0, 1, 2, \cdots, n$, 得到一个以 $a_n, a_{n-1}, \cdots, a_1, a_0$ 为未知数, 由 $n+1$ 个方程式组成的实系数线性方程组. 该方程组的系数行列式是一个非零的 Vandermonde 行列式, 故方程组必有唯一解, 且解为有理数. 因此 $f(x)$ 是有理系数多项式.

□

例题 0.2 设 $f(x)$ 是有理系数多项式,a, b, c 是有理数, 但 $\sqrt{c}$ 是无理数. 求证: 若 $a + b\sqrt{c}$ 是 $f(x)$ 的根, 则 $a - b\sqrt{c}$ 也是 $f(x)$ 的根.

证明 设 $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, 则

$$f(a+b\sqrt{c}) = a_n(a+b\sqrt{c})^n + a_{n-1}(a+b\sqrt{c})^{n-1} + \cdots + a_1(a+b\sqrt{c}) + a_0 = 0.$$

将 $(a+b\sqrt{c})^k$ 用二项式定理展开, 可设

$$f(a+b\sqrt{c}) = A + B\sqrt{c} = 0,$$

其中 A, B 都是有理数. 因为 $\sqrt{c}$ 是无理数, 故 $A = B = 0$. 因此

$$f(a-b\sqrt{c}) = A - B\sqrt{c} = 0,$$

即 $a-b\sqrt{c}$ 也是 $f(x)$ 的根.

□

例题 0.3 设 $f(x)$ 是有理系数多项式,a,b,c,d 是有理数, 但 $\sqrt{c},\sqrt{d},\sqrt{cd}$ 都是无理数. 求证: 若 $a\sqrt{c}+b\sqrt{d}$ 是 $f(x)$ 的根, 则下列数也是 $f(x)$ 的根:

$$a\sqrt{c}-b\sqrt{d},-a\sqrt{c}+b\sqrt{d},-a\sqrt{c}-b\sqrt{d}.$$

证明 令

$$g(x)=(x-(a\sqrt{c}+b\sqrt{d}))(x-(a\sqrt{c}-b\sqrt{d}))(x-(-a\sqrt{c}+b\sqrt{d}))(x-(-a\sqrt{c}-b\sqrt{d})),$$

则经计算可得

$$g(x)=x^4-2(a^2c+b^2d)x^2+(a^2c-b^2d)^2.$$

注意到 $g(x)$ 是一个有理数首一多项式, 只要证明它不可约, 便可由极小多项式式的充要条件得到 $g(x)$ 是 $a\sqrt{c}+b\sqrt{d}$ 的极小多项式, 从而由极小多项式的基本性质可知 $g(x)\mid f(x)$, 于是结论成立. 显然 $g(x)$ 没有有理系数的一次因式, 只要证明它没有有理系数的二次因式即可. 经过简单的计算可知, 在 $g(x)$ 的一个一次因式中任取一个一次因式相乘都不是有理系数多项式, 因此 $g(x)$ 没有有理系数的二次因式.

□

例题 0.4 求以 $\sqrt{2}+\sqrt[3]{3}$ 为根的次数最小的首一有理系数多项式.

注 确定 f(x) 的 6 个根的方法: 原方程 $x-\sqrt{2}=\sqrt[3]{3}$ 的解为 $x=\sqrt{2}+\sqrt[3]{3}$. 但三次方程 $y^3=3$ 的所有根为 $y=\sqrt[3]{3},\sqrt[3]{3}\omega,\sqrt[3]{3\omega^2}$(其中 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ 是三次单位根), 因此原方程对应三个解:

$$x=\sqrt{2}+\sqrt[3]{3},\quad \sqrt{2}+\sqrt[3]{3\omega},\quad \sqrt{2}+\sqrt[3]{3\omega^2}.$$

在消去 $\sqrt{2}$ 的平方步骤中, 方程 $x^3+6x-3=(3x^2+2)\sqrt{2}$ 的两边平方后, 原方程中的 $\sqrt{2}$ 可以被替换为 $-\sqrt{2}$, 从而产生另一组解:

$$x=-\sqrt{2}+\sqrt[3]{3},\quad -\sqrt{2}+\sqrt[3]{3\omega},\quad -\sqrt{2}+\sqrt[3]{3\omega^2}.$$

解 本题即求 $\sqrt{2}+\sqrt[3]{3}$ 的极小多项式. 令 $x-\sqrt{2}=\sqrt[3]{3}$, 两边立方得到 $(x-\sqrt{2})^3=3$. 整理可得 $x^3+6x-3=(3x^2+2)\sqrt{2}$, 再两边平方可得,$\sqrt{2}+\sqrt[3]{3}$ 适合下列多项式:

$$f(x)=x^6-6x^4-6x^3+12x^2-36x+1.$$

由 $f(x)$ 的构造过程,不难看出 $f(x)$ 的 6 个根分别为 $\pm\sqrt{2}+\sqrt[3]{3},\pm\sqrt{2}+\sqrt[3]{3}\omega,\pm\sqrt{2}+\sqrt[3]{3}\omega^2$. 其中 $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$. 因此, 我们有

$$f(x)=\left(x-\sqrt{2}-\sqrt[3]{3}\right)\left(x+\sqrt{2}-\sqrt[3]{3}\right)\left(x-\sqrt{2}-\sqrt[3]{3}\omega\right)\left(x+\sqrt{2}-\sqrt[3]{3}\omega\right)\left(x-\sqrt{2}-\sqrt[3]{3}\omega^2\right)\left(x+\sqrt{2}-\sqrt[3]{3}\omega^2\right).$$

通过简单的验证可知, 任取 $f(x)$ 的 2 个一次因式相乘都不是有理系数多项式; 任取 $f(x)$ 的 3 个一次因式相乘也都不是有理系数多项式, 因此 $f(x)$ 是有理数域上的不可约多项式, 从而由极小多项式式的充要条件可知,$f(x)$ 是 $\sqrt{2}+\sqrt[3]{3}$ 的极小多项式. □

例题 0.5 求证: 有理系数多项式 x^4+px^2+q 在有理数域上可约的充要条件是或者 $p^2-4q=k^2$, 其中 k 是一个有理数; 或者 q 是某个有理数的平方, 且 $\pm2\sqrt{q}-p$ 也是有理数的平方.

证明 必要性: 若多项式 x^4+px^2+q 在有理数域上可约, 考虑下列两种情况:

(1) x^4+px^2+q 有有理数根 t, 这时 t^2 是 x^2+px+q 的有理根, 因此其判别式 p^2-4q 必是一个有理数的完全平方.

(2) x^4+px^2+q 无有理数根, 则 x^4+px^2+q 在有理数域上可分解为两个二次多项式的积. 设 $x^4+px^2+q=(x^2+ax+b)(x^2+cx+d)$, 展开后比较系数可得

$$\begin{cases} a+c=0, \\ ad+bc=0. \end{cases}$$

若 $a=0$, 则 $c=0$, 这时将有 $p=b+d$, $q=bd$, 因此 $p^2-4q=(b-d)^2$. 若 $a\neq 0$, 则 $b=d$, 比较系数后可知 $p=2b-a^2$, $q=b^2$, 因此 $\pm 2\sqrt{q}-p=a^2$.

充分性: 若 $p^2-4q=k^2$, 则

$$x^4+px^2+q=x^4+px^2+\frac{1}{4}(p+k)(p-k)=\left(x^2+\frac{1}{2}(p+k)\right)\left(x^2+\frac{1}{2}(p-k)\right).$$

因此多项式可约.

若 $q=b^2$, $\pm 2\sqrt{q}-p=\pm 2b-p=a^2$, 则 $p=-a^2\pm 2b$. 于是

$$x^4+px^2+q=x^4+(-a^2\pm 2b)x^2+b^2=(x^2\pm b)^2-a^2x^2$$

也可约.

□

定理 0.3 (Eisenstein 判别法)

设多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

是整系数多项式,$a_n\neq 0, n\geqslant 1, p$ 是一个素数. 若 $p\mid a_i(i=0,1,\cdots,n-1)$, 但 $p\nmid a_n$ 且 $p^2\nmid a_0$, 则 $f(x)$ 在有理数域上不可约.

♡

证明 只需证明 $f(x)$ 在整数环上不可约即可. 设 $f(x)$ 可分解为两个次数较低的整系数多项式之积:

$$f(x)=(b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0)(c_tx^t+c_{t-1}x^{t-1}+\cdots+c_0),$$

其中 $m+t=n$. 显然 $a_0=b_0c_0, a_n=b_mc_t$. 由假设 $p\mid a_0$, 故 $p\mid b_0$ 或 $p\mid c_0$. 又 $p^2\nmid a_0$, 故 p 不能同时整除 b_0 及 c_0. 不妨设 $p\mid b_0$ 但 $p\nmid c_0$. 又由假设,p 不能整除 $a_n=b_mc_t$, 故 p 既不能整除 b_m 又不能整除 c_t. 因此不妨设 $p\mid b_0, p\mid b_1,\cdots,p\mid b_{j-1}$ 但 p 不能整除 b_j, 其中 $0<j\leqslant m<n$. 而

$$a_j=b_jc_0+b_{j-1}c_1+\cdots+b_0c_j,$$

根据假设,$p\mid a_j$, 又 p 可整除上述右端除 b_jc_0 外的其余项, 而不能整除 b_jc_0 这一项, 引出矛盾.

□

例题 0.6 设 $p_1,\cdots,p_m$ 是 m 个互不相同的素数, 求证: 对任意的 $n\geqslant 1$, 下列多项式在有理数域上不可约:

$$f(x)=x^n-p_1\cdots p_m.$$

证明 用 Eisenstein 判别法即可证明.(取 $p=p_i$ 即可)

□

例题 0.7 证明:x^8+1 在有理数域上不可约.

证明 作代换 $x=y+1$, 得

$$x^8+1=(y+1)^8+1=y^8+8y^7+28y^6+56y^5+70y^4+56y^3+28y^2+8y+2.$$

显然 2 可整除除第一项外的所有系数, 但 4 不能整除常数项. 用 Eisenstein 判别法可知 $(y+1)^8+1$ 不可约, 故 x^8+1 也不可约.

□

例题 0.8 设 $f(x)$ 是有理系数多项式, 已知 $\sqrt{2}$ 是 $f(x)$ 的根, 证明:$\sqrt{2}\varepsilon, \sqrt{2}\varepsilon^2,\cdots,\sqrt{2}\varepsilon^{n-1}$ 也是 $f(x)$ 的根, 其中 $\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ 是 1 的 n 次根.

证明 显然 $\sqrt{2}$ 适合多项式 x^n-2, 由 Eisenstein 判别法可知,x^n-2 在有理数域上不可约, 因此它是 $\sqrt{2}$ 的极小多项式. 最后由极小多项式的基本性质可得 $(x^n-2)\mid f(x)$, 从而结论得证.

□

例题 0.9 设 $f(x)$ 是次数大于 1 的奇数次有理系数不可约多项式, 求证: 若 x_1,x_2 是 $f(x)$ 在复数域内两个不同的根,

则 x_1+x_2 必不是有理数.

证明 不妨设 $f(x)$ 为首一多项式, 我们用反证法来证明结论. 设 $x_1+x_2=r$ 为有理数, 则有理系数多项式 $f(x)$ 与 $f(r-x)$ 有公共根 x_1. 因为 $f(x)$ 在有理数域上不可约, 故 $f(x)$ 是 x_1 的极小多项式, 从而由极小多项式的基本性质可得 $f(x)\mid f(r-x)$. 注意到 $f(x)$ 与 $f(r-x)$ 次数相同, 首项系数相同, 从而有 $f(r-x)=-f(x)$. 令 $x=\frac{r}{2}$, 则可得 $f\left(\frac{r}{2}\right)=0$, 即 $\frac{r}{2}$ 是 $f(x)$ 的一个有理根, 这与 $f(x)$ 在有理数域上不可约相矛盾.

□

例题 0.10 设 $a_1,a_2,\cdots,a_n\in\mathbb{Z}$ 两两不同, 证明:

1. $f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)-1$ 在 $\mathbb{Q}$ 上不可约;
2. $f(x)=(x-a_1)^2(x-a_2)^2\cdots(x-a_n)^2+1$ 在 $\mathbb{Q}$ 上不可约.

证明

1. 若 f 在 $\mathbb{Q}$ 上可约, 则由定理 0.2知, 存在 $p,q\in\mathbb{Z}[x]$ 使得
$$f=pq, 1\le\deg p<\deg f, 1\le\deg q<\deg f.$$
于是由 $f(a_i)=p(a_i)q(a_i)=-1, i=1,2,\cdots,n$ 及 $p,q\in\mathbb{Z}[x]$ 知
$$p(a_i)+q(a_i)=0, i=1,2,\cdots,n.$$
但是
$$\deg(p+q)\le\max\{\deg p,\deg q\}<\deg f=n,$$
我们有 $p+q=0$. 但是 f 首系数为 1, 所以 p,q 首系数符号相同, 这就是一个矛盾! 至此我们证明了 f 在 $\mathbb{Q}$ 上不可约.
2. 证法一:若 f 在 $\mathbb{Q}$ 上可约, 则由定理 0.2知, 存在 $p,q\in\mathbb{Z}[x]$ 使得
$$f=pq, 1\le\deg p<\deg g, 1\le\deg q<\deg f.$$
由 $f(a_i)=p(a_i)q(a_i)=1, i=1,2,\cdots,n, f\ge 1$ 和 $p,q\in\mathbb{Z}[x]$ 及介值定理知
$$p(a_i)=1,\forall i=1,2,\cdots,n\text{或者}p(a_i)=-1,\forall i=1,2,\cdots,n.$$
不妨设前者发生, 此时 $q(a_i)=1,\forall i=1,2,\cdots,n$.
注意到 $\deg f=2n, f'(a_i)=0, i=1,2,\cdots,n$, 故由 $f'=p'q+pq'=p'+q'$ 知
$$p'(a_i)+q'(a_i)=0, i=1,2,\cdots,n.$$
又
$$\deg(p+q)<2n,\begin{cases}p(a_i)+q(a_i)=2\\p'(a_i)+q'(a_i)=0\end{cases}, i=1,2,\cdots,n,$$
又因为 $p+q$ 和 $H\equiv 2$ 都是多项式且都满足上述插值条件, 所以由 Hermite 插值多项式的唯一性就有 $p+q\equiv 2$. 现在有 $1\le f=p(2-p)\le 1$, 故 $f=1$ 而矛盾! 至此我们证明了 f 在 $\mathbb{Q}$ 上不可约.
证法二:由命题 0.1可知, 只要证明 $f(x)$ 在整数环上不可约即可. 用反证法, 设 $f(x)=u(x)v(x)$, 其中 $u(x),v(x)$ 都是次数小于 $2n$ 的首一整数系数多项式. 注意到 $f(x)$ 没有实根, 故 $u(x),v(x)$ 也都没有实根, 从而由实系数多项式虚根成对可知,$u(x),v(x)$ 作为实数域上的函数都恒大于零. 由于 $f(x)$ 是 $2n$ 次多项式, 故 $u(x)$ 和 $v(x)$ 的次数至少有一个不超过 n, 不妨设 $u(x)$ 的次数不超过 n.
若 $u(x)$ 的次数小于 n, 则由 $f(a_i)=1$ 可得 $u(a_i)v(a_i)=1$, 因此 $u(a_i)=1$. 考虑非零多项式 $u(x)-1$, 由上面的分析可知它有 n 个不同的根 $a_1,a_2,\cdots,a_n$, 这与它的次数小于 n 矛盾.
因此 $u(x)$ 只能是 n 次首一多项式, 于是 $v(x)$ 也是 n 次首一多项式. 另一方面, 由于 $u(a_i)v(a_i)=1$, 故 $u(a_i)=v(a_i)=\pm1(1\leqslant i\leqslant n)$. 注意到 $u(x)-v(x)$ 的次数小于 n 并且它有 n 个不同的根 $a_1,a_2,\cdots,a_n$, 因此 $u(x)=v(x)$ 或 $u(x)=-v(x)$. 令设 $u(x)=v(x)$, 则 $f(x)=u(x)^2+1$, 即
$$(u(x)+h(x))(u(x)-h(x))=1.$$

因为 $u(x), h(x)$ 都是整数系数多项式, 故或者 $u(x)+h(x)=1, u(x)-h(x)=1$; 或者 $u(x)+h(x)=-1, u(x)-h(x)=-1$, 于是作差可得 $h(x)=0$, 矛盾. 因此结论得证.

□

例题 0.11 设 $f\in\mathbb{Z}[x]$ 是首 1 不可约的, 若 $|f(0)|$ 不是完全平方数, 则 $f(x^2)$ 不可约.

注 $g(-x)g(x)$ 的奇数次项恰好抵消了.

证明 假设 $f(x^2)$ 可约, 则存在首 1 不可约 $g\in\mathbb{Z}[x], 1\le\deg g<2\deg f$ 使得 $g(x)|f(x^2)$, 显然 $g(-x)|f(x^2)$. 若 $g(x)=g(-x)$, 则 g 的每一项都是偶数次方, 因此 $g(x)=h(x^2), h\in\mathbb{Z}[x]$. 现在 $h(x)|f(x)$ 且 $1\le\deg h<\deg f$, 这就和 f 不可约矛盾! 故 $g(x)\ne g(-x)$. 我们知道 $g(-x), g(x)$ 都是不可约的, 所以 $g(-x)g(x)|f(x^2)$. 同样的再由 f 不可约可得

$$g(-x)g(x)=t(x^2)|f(x^2)\implies t|f\implies\deg t=\deg f\implies\deg g=\deg f,$$

故 $f(x^2)=\pm g(x)g(-x)$, 从而 $|f(0)|=|g(0)|^2$, 这就是一个矛盾! 至此我们证明了 $f(x^2)$ 不可约.

□

例题 0.12 设 $n\in\mathbb{N}$, 证明多项式 $f(x)=\prod_{k=1}^{n}(x^2+k^2)+1$ 在 $\mathbb{Q}$ 上不可约.

证明 设 $f(0)=n!^2+1=m^2, m\in\mathbb{N}$, 则有 $(m-n!)(m+n!)=1$, 故由 $m+n!=1, m-n!=1\implies m=\frac{1}{2}$ 知矛盾! 因此我们由例题 0.11知只需证明 $g(x)=\prod_{k=1}^{n}(x+k^2)+1$ 在 $\mathbb{Q}$ 上不可约. 若 $g=pq, p,q\in\mathbb{Z}[x], 1\le\deg p,\deg q\le n-1$. 注意到

$$1=g(-k^2)=p(-k^2)q(-k^2), k=1,2,\cdots,n,$$

我们有

$$p(-k^2)-q(-k^2)=0, k=1,2,\cdots,n.$$

现在我们知道 $p=q$. 但是 $g=p^2\ge 0$ 显然是个矛盾! 因此我们证明了 f 在 $\mathbb{Q}$ 上不可约.

□