第三周习题课

——多项式不可约性的判定

一. 整系数多项式在$\mathbb{Z}[x]$和$\mathbb{Q}[x]$中可约性的等价性(定理5.32)

定理 设$f(x)\in\mathbb{Z}[x]$，则$f(x)$在$\mathbb{Q}[x]$可约当且仅当$f(x)$在$\mathbb{Z}[x]$可约

该命题右推左是显然的，因为如果$f(x)=f_1(x)f_2(x)$，$\deg f_1>0$，$\deg f_2>0$，且$f_1,f_2\in\mathbb{Z}[x]$，则由$\mathbb{Z}[x]\subseteq\mathbb{Q}[x]$，我们自然有$f_1,f_2\in\mathbb{Q}[x]$，所以$f(x)$在$\mathbb{Q}$上可约.

现在问题是如果$f(x)=f_1(x)f_2(x)$，$f_1,f_2\in\mathbb{Q}[x]$，$\deg f_1>0$，$\deg f_2>0$，为什么可以保证$f(x)$在$\mathbb{Z}$上可约?

例 设 $f(x)=20x^3+30x^2-16x-2=(15x-\frac{15}{2})(\frac{4}{3}x^2+\frac{8}{3}x+\frac{4}{15})$在$\mathbb{Q}$上可约，如何得到$f(x)$在$\mathbb{Z}$上可约? 我们可以作以下操作:

$$
\begin{aligned}
f(x)&=(15x-\tfrac{15}{2})\cdot(\tfrac{4}{3}x^2+\tfrac{8}{3}x+\tfrac{4}{15})\\
&=\tfrac{1}{2}(30x-15)\cdot\tfrac{1}{15}(20x^2+40x+4)\\
&=\tfrac{15}{2}\underbrace{(2x-1)}_{\text{本原}}\cdot\tfrac{4}{15}\underbrace{(5x^2+10x+1)}_{\text{本原}}\\
&=\tfrac{15}{2}\cdot\tfrac{4}{15}(2x-1)(5x^2+10x+1)\\
&=2\cdot\underbrace{(2x-1)(5x^2+10x+1)}_{10x^3+15x^2-8x-1}\\
&=(4x-2)(5x^2+10x+1)
\end{aligned}
$$

设$f(x)=2x^3+16x^2+28x+24=(\frac{3}{10}x^2+\frac{9}{5}x+\frac{3}{5})(\frac{20}{3}x+40)$

$$
\begin{aligned}
&=\tfrac{3}{10}(x^2+6x+2)\cdot\tfrac{20}{3}(x+6)\\
&=\tfrac{3}{10}\cdot\tfrac{20}{3}(x^2+6x+2)(x+6)\\
&=2(x^2+6x+2)(x+6)=(2x^2+12x+4)(x+6)
\end{aligned}
$$

证. 设 $f(x)=f_1(x)f_2(x)$, $f_1, f_2 \in \mathbb{Q}[x]$, $\deg f_1>0$, $\deg f_2>0$. 则

f_1 可以写为 $f_1(x)=\frac{t_1}{s_1}g_1(x)$, $\frac{t_1}{s_1}\in\mathbb{Q}$, $g_1(x)$ 为本原多项式.

f_2 可以写为 $f_2(x)=\frac{t_2}{s_2}g_2(x)$, $\frac{t_2}{s_2}\in\mathbb{Q}$, $g_2(x)$ 为本原多项式.

所以

$$\begin{aligned} f(x) &= f_1(x)f_2(x) \\ &= \frac{t_1}{s_1}\cdot\frac{t_2}{s_2}g_1(x)g_2(x) \end{aligned}$$

设 $\frac{t_1}{s_1}\cdot\frac{t_2}{s_2}=\frac{p}{q}$, $\gcd(p,q)=1$, 则

$$f(x)=\frac{p}{q}g_1(x)g_2(x)$$

由 Guass 引理可得 $g_1(x)g_2(x)$ 为本原多项式. 由于 $f(x)$ 为整系数的, 所以 $q=\pm1$, 所以 $\frac{p}{q}\in\mathbb{Z}$. 则

$$f(x)=\left(\frac{p}{q}g_1(x)\right)g_2(x),\quad \frac{p}{q}g_1(x)\in\mathbb{Z}[x],\ g_2(x)\in\mathbb{Z}[x].$$

□

(有理)

2. 判断整系数多项式不可约的几种方法.

1. 试根法: 用于判断多项式是否有一次因式

命题 设 $f(x)\in\mathbb{Z}[x]$, 若 $\alpha=\frac{a}{b}$ 是 $f(x)$ 的根, $\gcd(a,b)=1$, 则 a 整除 f 的常数项, b 整除 f 的首项系数.

推论 $f(x)$ 可能的有理根只有有限多个.

推论 次数小于3次的多项式 $f(x)\in\mathbb{Z}[x]$ 不可约当且仅当 $f(x)$ 无有理根.

例 设 $f(x)=3x^3+x+5$, 则3的因子有 $\pm1, \pm3$, 而5的因子有有 $\pm1, \pm5$, 所以可能的有理根有

$$\left\{\pm1, \pm\frac{1}{3}, \pm5, \pm\frac{5}{3}\right\}$$

习题3 (1) x^2+4，可能的有理根有 $\{\pm1, \pm2, \pm4\}$，代入均不是 x^2+4 的根，所以 x^2+4 不可约.

(或者 $x^2+4=(x-2i)(x+2i)$，所以 x^2+4 没有有理根，则 x^2+4 不可约)

(2) x^3+4 可能的有理根为 $\{\pm1, \pm2, \pm4\}$，代入均不是 x^3+4 的根，所以 x^3+4 不可约.

(或者 $x^3+4=x^3+(4^{\frac{1}{3}})^3=(x+4^{\frac{1}{3}})(x^2-4^{\frac{1}{3}}x+4^{\frac{2}{3}})$，因为 $x^2-4^{\frac{1}{3}}x+4^{\frac{2}{3}}$ 的判别式 $\Delta<0$，所以 x^3+4 无有理根).

(3) $x^4+4=x^4+4x^2-4x^2+4$
$=(x^2+2)^2-4x^2$ 所以 x^4+4 可约
$=(x^2-2x+2)(x^2+2x+2)$，

2. 艾森斯坦判别法：设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，若素数 p 整除 $a_{n-1}, a_{n-2}, \cdots, a_1, a_0$，但 $p\nmid a_n$，$p^2\nmid a_0$，则 $f(x)$ 不可约.

注：① 艾森斯坦判别法只是判断不可约的一个充分条件.

② 当用不了艾森斯坦判别法时，可以考虑 $f(x+1)$，$f(x-1)$ 是否可以用艾森斯坦判别法. (例5.35)

$$\phi_p: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$
$$\sum_i a_ix^i \mapsto \sum_i \bar{a}_ix^i$$

3. 模 p 法，p 为素数.

命题 若 p 不整除 $f(x)$ 的首项系数，而且 $f(x)$ 模 p 后不可约，则 $f(x)$ 在 $\mathbb{Z}$ 上不可约.

证明 反证，假设 $f(x)$ 在 $\mathbb{Z}$ 上可约，设

$$f(x)=f_1(x)f_2(x),\quad \deg f_1>0,\ \deg f_2>0.$$

因为 $lc(f)=lc(f_1)lc(f_2)$，$p\nmid lc(f)$，所以 $p\nmid lc(f_1)$ 且 $p\nmid lc(f_2)$，所以 $\deg(\phi_p(f_1))=\deg(f_1)>0$，$\deg(\phi_p(f_2))=\deg(f_2)>0$，等式两边模 p，得

$$\phi_p(f) = \phi_p(f_1)\phi_p(f_2)$$

与 $\phi_p(f)$ 在 $\mathbb{Z}_p$ 上不可约矛盾. □

例 已知 $f(x) = x^p - x - 1$ 在 $\mathbb{Z}_p[x]$ 中不可约，p 为素数. 证明：$f(x) = x^p - x - 1$ 与 $g(x) = x^p + (p-1)x + p - 1$ 在 $\mathbb{Q}[x]$ 上不可约.

证 因为 $\phi_p(x^p - x - 1) = x^p - x - 1$，$\phi_p(x^p + (p-1)x + p - 1) = x^p - x - 1$.

所以由 $x^p - x - 1$ 在 $\mathbb{Z}_p$ 上不可约，和 $p \nmid lc(x^p - x - 1)$，$p \nmid lc(x^p + (p-1)x + p - 1)$.

得 $x^p - x - 1$，$x^p + (p-1)x + p - 1$ 在 $\mathbb{Z}$ 上不可约.

□

例 证明 $x^5 + x^3 + 2x + 1$ 在 $\mathbb{Q}[x]$ 中不可约.

证 设 ϕ_2：
$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x]$$
$$\sum_i a_i x^i \longmapsto \sum_i \overline{a_i} x^i$$

则 $\phi_2(f) = x^5 + x^3 + 1 \in \mathbb{Z}_2[x]$. 因为 1，0 都不是 $\overline{f}$ 的根，所以 $\overline{f}$ 没有一次因式. 则 $\overline{f}$ 只可能分解为 1 个 3 次不可约多项式乘以一个 2 次不可约多项式. 在 $\mathbb{Z}_2[x]$ 中 2 次不可约多项式只有 $x^2 + x + 1$，3 次不可约多项式只有 $x^3 + x + 1$，$x^3 + x^2 + 1$，而 $(x^2 + x + 1)(x^3 + x + 1)$ 和 $(x^2 + x + 1)(x^3 + x^2 + 1)$ 均不等于 $\overline{f}$，所以 f 也不可能分解为 1 个 3 次不可约多项式乘以一个 2 次不可约多项式，则 f 不可约.

□

4 待定系数法

例 证明 x^5+x^3+1 在 $\mathbb{Z}_2[x]$ 中不能分解为1个2次多项式乘以一个3次多项式.

证 设 $x^5+x^3+1=(x^2+ax+1)(x^3+cx^2+dx+1)$

$$=x^5+(a+c)x^4+(d+ac+1)x^3+(ad+c+1)x^2+(a+d)x+1$$

比较系数可得

$$\begin{cases} a+c=0 \\ d+ac+1=1 \\ c+ad+1=0 \\ a+d=0 \end{cases} \quad \text{得} \quad \begin{cases} a=d=c \\ a^2+a+1=1 \\ a^2+a+1=0 \end{cases} \Rightarrow \text{无解}$$

所以 x^5+x^3+1 在 $\mathbb{Z}_2[x]$ 中不能分解为1个2次多项式乘以一个3次多项式.

□

三. 作业讲解

1. 设 $x^3-7x+\lambda=(x-x_1)(x-2x_1)(x-x_2)$, 得方程组

$$\begin{cases} -2x_1^2x_2=\lambda \\ 2x_1^2+2x_1x_2+x_1x_2=-7 \\ 0=-x_1-2x_1-x_2 \end{cases}$$

解得 $\lambda=\pm 6$. ($x_1=\pm 1$, $x_1x_2=-3$)

2. 反证, 若 $\gcd(a,b_1\cdots b_n)=d\neq 1$, 设 $p\mid d$ 且 p 不可约. 因为在UFD中不可约元都是素元, 所以 p 为素元. 由 $\gcd(a,b_1\cdots b_n)=d$, $p\mid d$ 得

$$p\mid a, \quad p\mid b_1\cdots b_n$$

由 p 为素元得 $p\mid b_i$, $\exists i\in\{1,\cdots,n\}$. 则 $\gcd(a,b_i)=p\neq 1$, 矛盾.

□

5. (选做).

m \ n	1	2	3	4	...
1	$T_{1,1}$	$T_{1,2}$	$T_{1,3}$	$T_{1,4}$	
2	$T_{2,1}$	$T_{2,2}$	$T_{2,3}$	$T_{2,4}$	
3	$T_{3,1}$	$T_{3,2}$	$T_{3,3}$	$T_{3,4}$	
4	$T_{4,1}$	$T_{4,2}$	$T_{4,3}$	$T_{4,4}$	
⋮					

当 $n=1$, $m\in\mathbb{Z}$ 时, 全次数为 m 的 1 元单项式只有 1 个,

即 $\binom{m+n-1}{m}=1$, 所以命题成立.

当 $m=1$, $n\in\mathbb{Z}$ 时, 全次数为 1 的 n 元单项式有 n 个,

即 $\binom{m+n-1}{m}=n$, 所以命题成立.

考虑 $n=k>1$, $m=s>1$, 假设命题对于 $n=k-1$, $m=s$ 及 $n=k$, $m=s-1$ 都成立. 对于 $n=k$, $m=s$ 时, 设

$$A=\{x_1^0 x_2^{i_2}\cdots x_n^{i_n} \mid i_2+\cdots+i_n=m\}$$

$$B=\{x_1\cdot x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} \mid i_1+i_2+\cdots+i_n=m-1\}$$

则 $A\cup B$ 为所有 m 次 n 变元的单项式, 而 A 中元素个数恰好等于 m 次 $n-1$ 变元单项式个数, B 中元素个数恰好等于 $m-1$ 次 n 变元单项式个数, 所以由归纳假设

$$|A|=\binom{m+(n-1)-1}{m},\quad |B|=\binom{(m-1)+n-1}{m-1}$$

则 $|A\cup B|=\binom{m+(n-1)-1}{m}+\binom{(m-1)+n-1}{m-1}\overset{\text{帕斯卡恒等式}}{=\!=}\binom{m+n-1}{m}$

则命题对于 $n=k$, $m=s$ 也成立.