不可约性

2023 年 12 月 2 日

目录

1 引言 **2**

1.1 定理：有理根式判别法 2

1.2 定义：代数整数(algebra integer) 2

1.3 引理 3

1.4 定义：本原多项式 3

1.5 高斯引理 3

1.6 引理 4

1.7 定义：容度(content) 4

1.8 引理 4

1.9 引理 5

1.10 定理：高斯 5

1.11 定理 6

1.11.1 例子 6

1.11.2 例子2 7

1.11.3 例子3 7

1.12 引理 8

1.13 艾森斯坦森准则(Eisenstein Criterion) 8

1.14 定义：割圆多项式 8

1.15 引理2：高斯 9

2 习题 **9**

1 引言

尽管我们可以使用一些技术来帮助我们确定整数是否是素数，但对很大的整数坐因式分解仍然是非常困难的问题。

同样的，我们也很难去判断一个多项式是否是不可约的，但现在我们给出一些非常有用技巧：

我们知道若$f(x) \in k[x]$且r是$f(x)$在域k中的根，则有一个因式分解$f(x) = (x-r)g(x \in k[x])$得到$f(x)$并非是不可约的。并且拓展了，若$f(x)$没有根的时候，它们是不可约的多项式。

1.1 定理：有理根式判别法

令$f(x) = a_0 + a_1x + \cdots + a_nx^n \in Z[x] \subseteq Q[x]$。则每个$f(x)$的有理根$r$形如$r = b/c$，其中$b \mid a_0$且$c \mid a_n$

证明： 我们设$r = b/c$是最简形式，那么$(b, c) = 1$.

带入r到$f(x)$则有

$$0 = f(b/c) = a_0 + a_1(b/c) + \cdots + a_n(b/c)^n$$

两端乘上c^n得到

$$0 = a_0c^n + a_1c^{n-1} + \cdots + a_nb^n$$

因此$a_0c^n = b(-a_1c^{n-1} - \cdots - a_nb^{n-1})$可知$b \mid a_0c^n$，但$b, c$互素，由欧拉引理可知$b \mid a_0$，类似的，$a_nb^n = c(-a_{n-1}b^{n-1} - \cdots - a_0c^{n-1})$可得$c \mid a_n$

1.2 定义：代数整数(algebra integer)

一个复数α被称为代数整数，指的是α是$f(x) \in Z[x]$中首一多项式的根。

1.3 引理

有理数z是代数整数则必须在Z中，更准确的来说，若$f(x) \in Z[x] \subseteq Q[x]$是首一的，则每个$f(x)$的有理根是整除常数项的整数。

证明： 设$f(x) = a_0 + a_1x + \cdots + a_nx^n$是首一的，则$a_n = 1$，利用定理1.1可知，整除1的整数只有1，所以有理根都是整数。

例如：考虑$f(x) = x^3 + 4x^2 - 2x - 1 \in Q[x]$，它不可约当且仅当$f(x)$没有根。利用定理1.1，可能存在的根只有±1，但$f(1) = 2$，$f(-1) = 4$，所以$f(x)$在$Q[x]$中是不可约的。

1.4 定义：本原多项式

多项式$f(x) = a_0 + a_1x + \cdots + a_nx^n \in Z[x]$是本原多项式，当且仅当其系数最大公因子为1。

□

显而易见的是，每个首一的多项式都是本原的。若$f(x)$的首系数是d，那么$(1/d)f(x)$就是$Z[x]$中的本原多项式。
另一个事情是，若$f(x)$不是本原的，则存在一个素数p可以整除每个系数。
若gcd是$d > 1$，则p可以取d的任何素因子。

1.5 高斯引理

若$f(x), g(x) \in Z[x]$是两个本原多项式，则$f(x)g(x)$也是本原的。

证明： 设$f(x) = \sum a_ix^i$，$g(x) = b_jx^j$，那么$f(x)g(x) = \sum c_kx^k$。若$f(x)g(x)$不是本原的，则存在一些素数p整除每个c_k，由于$f(x)$是本原的，那么至少存在一个系数是不被p整除的，不妨设a_i和b_j是第一个不能被整除的数，由多项式的乘法定义我们有：

$$a_ib_j = c_{i+j} - (a_0b_{i+j} + \cdots + a_{i-1}b_{j+1} + a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0)$$

右侧的每项都可以被整除，但左边是不行的，矛盾。

1.6 引理

每个非零$f(x) \in Q[x]$都有唯一分解

$$f(x) = c(f)f^{\#}(x)$$

其中$c(f) \in Q$是正数而$f^{\#}(x) \in Z[x]$是本原多项式。

证明：取一些正数a_i和b_j使得

$$f(x) = (a_0/b_0) + (a_1/b_1)x + \cdots + (a_n/b_n)x^n \in Q[x]$$

定义$B = b_0b_1 \cdots b_n$，使得$g(x) = Bf(x) \in Z[x]$。我们再定义$D = \pm d$，其中d是$g(x)$的系数的gcd。我们再选取一些符号使得D/B这个有理数为正。现在$(B/D)f(x) = (1/D)g(x) \in Z[x]$，并且是一个首一多项式。再定义$c(f) = D/B$和$f^{\#} = (B/D)f(x)$则$f(x) = c(f)f^{\#}(x)$就是我们描述的因式分解。
现在证明唯一性，设$f(x) = eh(x)$是另一个分解，那么e是一些正有理数和$h(x) \in Z[x]$是本原的。现在有$f(x) = c(f)f^{\#}(x) = eh(x)$，那么$f^{\#} = (e/c(f))h(x)$，记$e/c(f)$的既约形式为$u/v$，其中$u, v$是互素的正整数，等式可以改写为$vf^{\#}(x) = uh(x) \in Z[x]$。那么$v$是等式$uh(x)$中的公因子，但由$(u, v) = 1$可知$v \mid h(x)$。由于$h(x)$是本原的，那么$v = 1$。类似的结论可知$u = 1$，那么我们有$e/c(f) = u/v = 1$得到$h(x) = f^{\#}(x)$。

1.7 定义：容度(content)

引理1.6中的$c(f)$我们称作容度。

1.8 引理

若$f(x) \in Z[x]$，则$c(f) \in Z$

证明：若d是$f(x)$的系数的gcd，那么$(1/d)f(x) \in Z[x]$是本原的。因此$d[(1/d)f(x)]$是$f(x)$的因式分解，像一些正有理数d和本原多项式的乘积。由引理1.6的唯一性可知$c(f) = d \in Z$。

1.9 引理

若$f(x) \in Q[x]$的分解像$f(x) = g(x)h(x)$，则

$$c(f) = c(g)c(h),\ f^{\#}(x) = g^{\#}(x)h^{\#}(x)$$

证明：我们有

$$\begin{aligned} f(x) =& g(x)h(x) \\ c(f)f^{\#}(x)3 =& [c(g)g^{\#}(x)][c(h)h^{\#}(x)] = \quad c(g)c(h)g^{\#}(x)h^{\#}(x) \end{aligned}$$

因此$g^{\#}(x)h^{\#}(x)$是本原的。利用定理1.6可知这种分解是唯一的。。

1.10 定理：高斯

令$f(x) \in Z[x]$，若

$$f(x) = G(x)H(x) \in Q[x]$$

则有因式分解

$$f(x) = g(x)h(x) \in Z[x]$$

其中$\deg(g) = \deg(G)$和$\deg(h) = \deg(H)$。因此，若$f(x)$在$Z[x]$不能分解为次数更低的因式分解，则$f(x)$在$Q[x]$中是不可约的。

证明：利用引理1.9，这里有一个因式分解

$$f(x) = c(G)c(H)G^{\#}(x)H^{\#}(x) \in Q[x]$$

其中$G^{\#}(x), H^{\#}(x) \in Z[x]$是本原多项式由于$f(x) \in Z[x]$。综上所述$c(f) = c(G)c(H) \in Z$。则
有$g(x) = c(f)G^{\#}(x), h(x) = c(h)H^{\#}(x)$是$f(x)$在$Z[x]$中的因式分解。

1.11 定理

令$f(x) = a_0 + a_1x + a_2x^2 + \cdots + x^n \in Z[x]$是首一的，再令$p$是素数。若$f^*(x) = [a_0] + [a_1]x + \cdots + x^n \in F_p[x]$是不可约的，则$f(x)$在$Q[x]$中也不可约。

证明： 引入如下定理：

> 设R, S是交换环，则$\varphi : R \to S$是同态。若$s_1, s_2, \cdots, s_n \in S$，则存在一个唯一的同态
> $$\widetilde{\varphi} : R[x_1, \cdots, x_n] \to S$$
> 满足对所有i存在$\widetilde{\varphi}(x_i) = s_i$且对所有$r \in R$有$\widetilde{\varphi}(r) = \varphi(r)$

那么自然映射$\varphi : Z \to F_p$定义一个同态$\varphi^* : Z[x] \to F_p[x]$为

$$\varphi^*(b_0 + b_1x + \cdots) = [b_0] + [b_1]x + \cdots$$

若$g(x) \in Z[x]$，我们则记$\varphi^*(g(x)) \in F_p[x]$为$g^*(x)$。设$f(x)$在$Z[x]$中是可分解的，记为$f(x) = g(x)h(x)$，其中$\deg(g) < \deg(f)$。由于$\varphi^*$是环同态，那么$f^*(x) = g^*(x)h^*(x)$。那么$\deg(f^*) = \deg(h^*) + \deg(g^*)$。又由于$f(x)$是首一的，那么$f^*(x)$是首一的[1]。因此$\deg(f^*) = \deg(f)$，由题可知若$f^*$是不可约的，但$g^*$和$h^*$的次数严格小于$f^*$表示是一个矛盾。因此$f(x)$在$Z[x]$中实际上是不可约的。利用定理1.10可知在$Q[x]$中是不可约的。

注意： 定理1.11的逆命题不成立，它不总是奏效的。不难找出一个多项式$f(x) \in Z[x] \subseteq Q[x]$是不可约的。但对某个素数$p$有$f^*(x) \in F_p[x]$是可分解的。例如$x^4 + 1$在$Q[x]$中不可约，但在$F_p[x]$中可约，其中$p$是任意素数。

由于$F_p[x]$的元素书写冗杂，在下面的叙述中我们描述F_p的元素时不加中括号。

1.11.1 例子

我们来确定$F_2[x]$中的最小次数不可约的多项式。

首先肯定的是，线性多项式x和$x + 1$是不可约的

[1] 环同态把0映射到0，1映射到1

其次，对于二次方程$x^2, x^2+x, x^2+1, x^2+x+1$有四个，但前三个在$F_2[x]$中有根，真正不可约的多项式只有一个。

一般来说，在$F_p[x]$中，n次的多项式有p^n个。这是因为对于n个系数中每个系数$a_0, \cdots, a_{n-1}$都存在p种选法。

对于三次多项式，则存在8个，而这8个种真正可约的只有4个，因为其他四个的常数项是0。它们是：

$$x^3+1,\ x^3+x+1,\ x^3+x^2+1,\ x^3+x^2+x+1$$

其中1是第一个方程和第四个方程的根，所以不可约的元素有2个(注：$-1 \in [1]_2$，因为$1-(-1) \mid 2$)

现在给出一些不可约多项式的表格

n次不可约多项式

$\deg = 2$	x^2+x+1		
$\deg = 3$	x^3+x+1	x^3+x^2+1	
$\deg = 4$	x^4+x^3+1	x^4+x+1	$x^4+x^3+x^2+x+1$

1.11.2 例子2

现在我们来检验一下$f(x) = x^4 - 5x^3 + 2x + 3$是$Q[x]$中的不可约多项式。利用引理1.3。唯一值得考虑的有理根只可能是$1, -1, 3, -3$。带入后实际上发现不是根，但还有另一种可能，$f(x)$可能是两个不可约多项式的乘积，那么让我们试试定理1.11。由于$f^*(x)$在$F_2[x]$中是不可约的多项式，所以$f(x)$在$Q[x]$中是不可约的。

1.11.3 例子3

令$f(x) = x^4 + x^3 + x^2 + x + 1 \in Q[x]$。由于$f^*(x)$在$F_2[x]$中是不可约多项式，因此$f(x) \in Q[x]$是不可约的。

1.12 引理

令$g(x) \in Z[x]$。若这里有$c \in Z$使得$g(x+c)$在$Z[x]$中不可约，则$g(x)$在$Q[x]$中不可约。

证明： 我们利用在定理1.1引入的定理。利用$f(x) \to f(x+c)$定义函数$\varphi : Z[x] \to Z[x]$，则它是一个同构。若$g(x) = s(x)t(x)$，那么$g(x+c) = \varphi(g(x)) = \varphi(st) = \varphi(s)\varphi(t)$，这与我们的假设$g(x+c)$是不可约的矛盾。因此$g(x)$在$Z[x]$中不可约。由高斯定理可知$g(x)$在$Q[x]$中不可约。

1.13 艾森斯坦森准则(Eisenstein Criterion)

令$f(x) = a_0 + a_1x + \cdots + a_nx^n \in Z[x]$。若存在一个素数$p$整除$a_i$，其中$i < n$使得$p \nmid a_n$和$p^2 \nmid a_0$。则$f(x)$在$Q[x]$中不可约。

证明： 我们来用反证法，设

$$f(x) = (b_0 + b_1x + \cdots + b_mx^m)(c_0 + c_1x + \cdots + c_kx^k)$$

是两个分解。其中$m < n$且$k < n$。由定理1.10我们可以假设两个因子都在$Z[x]$中，那么$p \mid a_0 = b_0c_0$，由欧几里得引理可知$p \mid b_0$或者$p \mid c_0$，由于$p^2 \nmid a_0$。因此b_0, c_0只能有一个倍p整除，不妨设为$p \mid c_0$。根据题设，首系数$a_n = b_mc_k$不被p整除，所以$p \nmid c_k, b_m$。设c_r是第一个不被p整除的系数，那么$p \mid c_0, \cdots, c_{r-1}$。设$r < n$。则$p \mid a_r$有$b_0c_r = a_r - (b_1c_{r-1} + \cdots + b_rc_0)$被$p$整除，有$p \mid b_0c_r$，但由假设，$p$不能整除这两个因子，是一个矛盾。因此$r = n$，$n \geq k \geq r = n$有$k = n$，所以$k < n$矛盾，因此$f(x)$在$Q[x]$中不可约。

1.14 定义：割圆多项式

若p是素数，则p次割圆多项式定义为

$$\Phi(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

1.15 引理2：高斯

每个割圆多项式$\Phi_n(x)$对$n \geq 1$（不一定是素数）都在$Q[x]$中不可约。

证明： 由定义有

$$\Phi_p(x) = (x^p - 1)/(x - 1)$$

那么

$$\begin{aligned}\Phi_p(x+1) =&((x+1)^p - 1)/x \\ =&x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p\end{aligned}$$

由于p是素数，我们利用爱森斯坦森准则。和下列定理：

> 若p是素数，则$p \mid \binom{p}{j}, 0 < j < p$

那么可以得到$Q[x]$中$\Phi_n(x+1)$是不可约的，最后利用引理1.12，可知$\Phi_n(x)$在$Q[x]$中不可约。

2 习题

> 判断下列多项式在$Q[x]$是否可约
>
> 1. $f(x) = 3x^2 - 7x - 5$
> 2. $f(x) = 350x^3 - 25x^2 + 34x + 1$
> 3. $f(x) = 2x^3 - x - 6$
> 4. $f(x) = 8x^3 - 6x - 1$

证明 利用定理1.1，则根的选择有$b = \pm 5, \pm 1$，而$c = \pm 3, \pm 1$，但带入后都不存在$f(b/c) = 0$，因此$f(x)$在$Q[x]$上不可约

对于第二个多项式，可能的因子有$\pm 1, \pm 35, \pm 10, \pm 1, 2, 5, 7, 14, 25, 35, 50, 70, 175, 350$检查后发现$f(1/35) = 0$，因此是可约的。

对于第三个多项式如法炮制

对第四个多项式，如果想用定理1.13，我们先配合引理1.12。令$x = x-1$带入得到

$$f(x-1) = 8x^3 - 24x^2 + 18x - 3$$

选择$p=3$。$3^2 \nmid 3$且$3 \nmid 8$，因此该多项式在$Q[x]$中也是不可约的。

若p是素数，证明在$F_p[x]$中有$\frac{1}{3}(p^3-p)$个首一的不可约三次多项式

证明： 对于一个一般首一三次方程，它形如$x^3+[a]x^2+[b]x+[c]$，其中a,b,c各有p种选法，因此可能的三次方程一共有p^3种。可约的多项式形如$(x-a)(x-b)(x-c)$，我们利用伯恩赛德引理，首先因子可能的置换就存在六种，$\mid S_3 \mid = 6$。现在我们利用伯恩赛德引理，对这六种置换分别计算，恒等置换存在p^3个元素，对置换$(a\ b)(c)$和$(b\ c)(a)$和$(c\ a)(b)$来说是$3p^2$，还剩下两个置换，即$(a\ b\ c),(a\ c\ b)$各有p种可能。利用伯恩赛德引理，形如$(x-a)(x-b)(x-c)$的置换有

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

其次，考虑到二次不可约多项式和一次的乘积$(x+a)(x^2+bx+c)$也是一种有$(p^3-p^2)/2$可能的多项式，$x+a$有p种可能，x^2+bx+c的可能就是$\frac{p^2-p}{2}$种，因为形如$(x-a)(x-b)$的可能为$1/2(p(p-1))-p$。合起来一共的可能就是

$$\begin{aligned}&p^3-\frac{1}{6}(p^3+3p^2+2p)-\frac{1}{2}(p^3-p^2)\\=&\frac{1}{3}(p^3-p)\end{aligned}$$

设k是一个域，$f(x) = a_0 + a_1x + \cdots + a_nx^n \in k[x]$的次数为$n$，若$f(x)$是不可约的，则$a_n + a_{n-1}x + \cdots + a_0x^n$也是不可约的。

证明： 设$\varphi : k[x] \to k[x]$由函数$\varphi(f(x)) \to a^n f(1/x)$定义，则

$$\varphi(f) = x^n(a_0+a_1(1/x)+\cdots+a_n(1/x)^n) = x_n\sum_{i=0}^{n}\frac{a_i}{x^i} = a_n+a_{n-1}x+\cdots+a_0x^n$$

由于$f(x)$不可约，所以$f(1/x)$也是不可约的，不妨设$x^nf(1/x)$存在因式分解，则

$$x^nf(1/x) = (s_r+s_{r-1}x+\cdots+s_0x^r)(t_k+t_{k-1}x+\cdots+t_0x^k) = x^rs(1/x)x^kt(1/x)$$

其中$s(x) = s_0+s_1x+\cdots+s_rx^r$，$t(x) = t_0+t_1x+\cdots+t_kx^k$ 其中$\deg(s), \deg(t) < \deg(f)$,由于$f(x)$不可约，而根据我们的假设有

$$x^nf(1/x) = x^rs(1/x)x^kt(1/x) = x^ns(1/x)t(1/x)$$

意味着$s \mid f$或者$t \mid f$这是一个矛盾，因此$x^nf(1/x)$是不可约的。