有趣的题

求证：$f(x)=x^5+x^3+1$ 在 $\mathrm{Q}[x]$中不可约。

证：若$f(x)$在 $\mathrm{Q}[x]$中可约，则$\bar{f}(x)$在$\mathrm{Z}_2[x]$中可约。

因为$f(0)=f(1)=1\ (\mathrm{mod}\ 2)$，故$\bar{f}(x)$只有二次因子，

且只能为x^2+x+1

由带余除法得$\bar{f}(x)=(x^2+x+1)(x^3+x^2+x)+x+1$

因此$\bar{f}(x)$在$\mathrm{Z}_2[x]$中不可约，即$f(x)$在 $\mathrm{Q}[x]$中不可约。

求证：$\mathrm{Z}\left[\sqrt{-2}\right]=\{a+b\sqrt{-2}|a,b\in\mathrm{Z}\}$是欧几里得环

证：范数$N(\alpha)=a^2+2b^2$，设 $\alpha,\beta\in\mathrm{Z}\left[\sqrt{-2}\right]$

在 $\mathrm{Q}\left[\sqrt{-2}\right]$中，$\alpha\beta^{-1}$可表为$m_1+n_1\sqrt{-2},m_1,n_1\in\mathrm{Q}$

m_1,n_1又可分别表为$m+u,n+v,$其中$m,n\in\mathrm{Z},|u|\le\frac{1}{2},|v|\le\frac{1}{2}$

因此$\alpha=\beta\left(m+n\sqrt{-2}\right)+\beta\left(u+v\sqrt{-2}\right)$

$\because\alpha,\beta\in\mathrm{Z}\left[\sqrt{-2}\right],\left(m+n\sqrt{-2}\right)\in\mathrm{Z}\left[\sqrt{-2}\right]$

$\therefore\beta\left(u+v\sqrt{-2}\right)\in\mathrm{Z}\left[\sqrt{-2}\right]$

取$q=m+n\sqrt{-2}$，$r=\beta\left(u+v\sqrt{-2}\right)$

则有熟悉的形式$\alpha=q\beta+r$

取范数为尺度函数，要证$N(r)<N(\beta)$

即证$N\left(\beta\left(u+v\sqrt{-2}\right)\right)=N(\beta)N\left(u+v\sqrt{-2}\right)<N(\beta)$

只需证$N\left(u+v\sqrt{-2}\right)<1$

即证$u^2+2v^2<1$

因为$u^2\le\frac{1}{4},v^2\le\frac{1}{4}$

$u^2+2v^2<1$ 易得。

设G为有限群，有二阶自同构$f\left(f^2\text{为恒等映射}\right)$，

没有非平凡的不动点，即$a\ne e\Rightarrow f(a)\ne a$

证明G为阿贝尔群。

证：考虑映射$k:G\to G,a\to f(a)a^{-1}$是否为单射

若$f(a)a^{-1}=f(b)b^{-1},$则$f(b)^{-1}f(a)=b^{-1}a$

即$f(b^{-1}a)=b^{-1}a$，从而$b^{-1}a=e$，$b=a$

因而k为单射，由G有限可得k为双射。

设$g=f(a)a^{-1}$,则$f(g)=f(f(a)a^{-1})=f^2(a)f(a^{-1})$

$=af(a)^{-1}=(f(a)a^{-1})^{-1}=g^{-1}$

即映射f为$g\to g^{-1}$

于是$ab=f(a^{-1})f(b^{-1})=f(a^{-1}b^{-1})=(a^{-1}b^{-1})^{-1}=ba$

即G为阿贝尔群。

设F是K的扩域，$u\in F$且u是K上的代数元，

求证$F[u]$是域。

证：设u的极小多项式为$P(x)$，则$P(x)$不可约。

$\forall f(x)\in K[x]$,若$f(u)\neq 0$,则存在$s(x),t(x)$,

使得$s(x)f(x)+t(x)P(x)=1$

$\therefore s(u)f(u)=1$

$\therefore f(u)$有逆$s(u)$

重要结论

凯莱定理：任意 n 阶有限群同构于对称群S_n的某个子群。

同构映射：$(a\in G)\ L: a\to L_a\in H, H\subset S_n$

其中 $L_a: G\to G, g\to ag$

如果$\ker f=\{e\}$,则$f: G\to \operatorname{Im} f$是一个同构。

有单位元的非平凡交换环 R 是整环，当且仅当在 R 中消去律成立。

即对$\forall a,b,c\in R, ab=ac, a\neq 0\Rightarrow b=c$

域上的一元多项式环是欧几里得整环。

$$\{\text{域}\}\subset\{\text{欧几里得整环}\}\subset\{\text{主理想整环}\}$$
$$\subset\left\{\begin{matrix}\{\text{诺特环}\}\\ \{\text{唯一因子分解整环}\}\subset\{\text{整环}\}\end{matrix}\right\}\subset\{\text{交换环}\}$$

唯一因子分解环上的多项式环还是唯一因子分解整环。

整环上的多项式环还是整环。

域上的多项式环是欧几里得整环。

正常情况：当 $S\subseteq T$ 时

f在 $S[x]$中可约 $\Rightarrow f$在 $T[x]$中可约

f在 T$[x]$中不可约 $\Rightarrow f$在 S$[x]$中不可约

特殊：

f在 Z$[x]$中不可约 $\Leftrightarrow f$在 Q$[x]$中不可约

f在$\mathrm{Z_p}[x]$中不可约 $\Leftrightarrow f$在 Z$[x]$中不可约

p 为素数且 p 不整除首项系数

设R是一个整环，其中每一个元素都有素因子分解，

则R为唯一因子分解环当且仅当

对每一个整除ab的素元$p \in R, p|a$或$p|b$

拉格朗日插值公式

$$f(X) = \sum_{k=0}^{n} b_k \frac{(X - c_0) \dots (X - c_{i-1})(X - c_{i+1}) \dots (X - c_n)}{(c_i - c_0) \dots (c_i - c_{i-1})(c_i - c_{i+1}) \dots (c_i - c_n)}$$

牛顿插值公式

$$f(X) = u_0 + u_1(X - c_0) + \cdots + u_n(X - c_0)(X - c_1) \dots (X - c_{n-1})$$

拉格朗日公式

$$\frac{f}{g} = \sum_{k=1}^{n} \frac{f(c_k)}{g'(c_k)(x - c_k)}$$

给定非零实系数多项式$f(x)$和闭区间$[a, b]$

$f_0(x) = f(x), f_1(x), \dots, f_s(x)$

称为$f(x)$在闭区间$[a, b]$上的斯图姆序列，

如果这些多项式都是实系数多项式且满足

末式无根：$f_s(x)$在$[a, b]$上没有根；

端非首式根：$f(a)f(b) \neq 0$

中式相邻变号：对$c \in [a, b], 1 \leq k \leq s - 1$，

若$f_k(c) = 0$，则$f_{k-1}(c)f_{k+1}(c) < 0$

首二式根处递增：若$f(c) = 0$, 则$f_0(x)f_1(x)$在c附近是递增的。

由$f_0(x) = f(x), f_1(x) = f'(x)$辗转相除法生成的序列

！注意要取负号

称为标准斯图姆序列。

斯图姆定理

正次数的实系数多项式在开区间(a,b)上的根的个数

（不计重数）等于V_a-V_b，

V_a,V_b分别为a,b处任一斯图姆序列变号数。

笛卡尔定理

实多项式的正根个数（计重数）不超过系数序列的变号数，

且两者有相同的奇偶性。若没有虚根，则两者相等。

设有理数$\frac{p}{q}(p,q$互素)为多项式

$f=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\in \mathrm{Z}[x]$的根

则分子整除末项，分母整除首项：$p|a_n,q|a_0$

之差整除$f(1)$,之和整除$f(-1)$: $q-p|f(1),q+p|f(-1)$

三次方程$x^3+px+q=0$ 的判别式为$D=-4p^3-27q^2$

$D>0\Rightarrow f$有三个相异实根

$D<0\Rightarrow f$有一个实根，两个虚根

$D=0\Rightarrow f$有三个实根，其中一个是重根

卡尔丹公式：

$$c_i=\omega^{i-1}\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{D}{108}}}+\omega^{1-i}\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{D}{108}}}$$

Res 大行列式：

f 的系数写(g 的次数)行，g 的系数写(f 的次数)行

$f(x)=a_0(x-\alpha_1)\ldots(x-\alpha_n)$

$g(x)=b_0(x-\beta_1)\ldots(x-\beta_m)$

$\mathrm{Res(f,g)}=a_0^m b_0^n\prod_{i,j}(\alpha_i-\beta_j)$

注意a_0跟m次，b_0跟n次

多项式f判别式$D(f)=(-1)^{\frac{n(n-1)}{2}}a_0^{-1}\mathrm{Res}(f,f')$

方法

艾森斯坦既约性判别法

设$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$

是 Z 上的首一多项式，

如果$a_1, \ldots, a_n$都能被某个素数p整除，但a_n不能被p^2整除

则$f(X)$在 Q 上是既约的。

霍纳法

$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$

$= (x - c)(b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-2}x + b_{n-1}) + r$

$$\begin{array}{cccccccc} & a_0 & a_1 & a_2 & \ldots & a_{n-1} & a_n \\ c & b_0 & b_1 & b_2 & \ldots & b_{n-1} & b_n = r \end{array}$$

$b_{k+1} = b_k \cdot c + a_{k+1} \qquad b_k = 左 \times c + 上$

反复作霍纳法

$$\begin{array}{cccccccc} & a_0 & a_1 & a_2 & \ldots & a_{n-1} & a_n \\ c & b_0 & b_1 & b_2 & \ldots & b_{n-1} & b_n = r_0 \\ & \ldots & \ldots & \ldots & \ldots & r_1 & \\ & \ldots & & & & & \\ & r_n & & & & & \end{array}$$

则$r_k = \dfrac{f^{(k)}(c)}{k!}, f(x) = \sum_{k=0}^{n} r_k(x - c)^k$