一元五次方程不可解之证明

李浩然

2020/06/27

目录

1 代数基本定理与对称多项式基本定理

引理1.1. 假设f是一个n次多项式，它有根a等价于它可以分解为$f(x)=(x-a)g(x)$

证明. 由多项式除法知$f(x)=(x-a)g(x)+c$，故$f(a)=0$等价于$c=0$ $\square$

例子1.2. 我们有$2x^5+3x^4-x^2-5=(x-2)(2x^4+7x^3+14x^2+27x+54)+103$

$$
\begin{array}{rrrrrrr}
 & 2x^4 & +7x^3 & +14x^2 & +27x & +54 & \\
\cline{2-7}
x-2\big) & 2x^5+3x^4 & & -x^2 & & -5 & \\
 & -2x^5+4x^4 & & & & & \\
\cline{2-2}
 & 7x^4 & & & & & \\
 & -7x^4+14x^3 & & & & & \\
\cline{2-3}
 & & 14x^3 & -x^2 & & & \\
 & & -14x^3+28x^2 & & & & \\
\cline{3-4}
 & & & 27x^2 & & & \\
 & & & -27x^2+54x & & & \\
\cline{4-5}
 & & & & 54x & -5 & \\
 & & & & -54x+108 & & \\
\cline{5-6}
 & & & & & 103 &
\end{array}
$$

Fundamental theorem of algebra

定理1.3 (代数基本定理). *假设$f=z^n+a_1z^{n-1}+\cdots+a_n$是一个复系数$n$次多项式，则它有复数根$z_1$，进而可以分解为$f(z)=(z-z_1)g(z)$，最终将分解为$f(z)=(z-z_1)\cdots(z-z_n)$*

证明. 假设是C_r复平面上以0为心，r为半径的圆,假设$f(z)$恒不为零，可以定义函数$h(z)=\dfrac{f(z)}{|f(z)|}$,它将复平面$\mathbb{C}$映射到复平面的单位圆$C_1$上,令$z=re^{i\theta}$, $f(z)=z^n\left(1+\dfrac{a_1}{z}+\cdots\dfrac{a_n}{z^n}\right)$,记$1+\dfrac{a_1}{z}+\cdots\dfrac{a_n}{z^n}=\rho e^{i\alpha}$,则$f(z)=r^n\rho e^{i(n\theta+\alpha)}$, $h(z)=e^{i(n\theta+\alpha)}$, C_r在h下的像将是一条限制在C_1里连续的闭合路径,注意到C_0在h下的像就是一个点，而当r趋向无穷时, $\rho e^{i\alpha}=1+\dfrac{a_1}{z}+\cdots\dfrac{a_n}{z^n}\approx 1$, α趋于零, C_r的像就变成了一条绕了n圈的路径，而这显然不可能,因为路径是随着r连续变化的 $\square$

定义1.4. n元多项式$f(x_1,\cdots,x_n)$，被称为一个**对称多项式**随意置换$x_1,\cdots,x_n$后f不变，$s_k=\sum\limits_{i_1<\cdots<i_k}x_{i_1}\cdots x_{i_k}$被称为**基础对称多项式**,例如

$$s_1=x_1+\cdots+x_n$$

$$s_2=x_1x_2+x_1x_3+\cdots+x_1x_n+x_2x_3+\cdots+x_2x_n+\cdots+x_{n-1}x_n$$

$$\vdots$$

$$s_n=x_1\cdots x_n$$

我们有**Vièta公式**$(x-x_1)\cdots(x-x_n)=x^n-s_1x^{n-1}+s_2x^{n-2}+\cdots+(-1)^ns_n$

例子1.5.

$$
\begin{aligned}
&(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)\\
=&x^5-(x_1+x_2+x_3+x_4+x_5)x^4\\
&+(x_1x_2+x_1x_3+x_1x_4+x_1x_5+x_2x_3+x_2x_4+x_2x_5+x_3x_4+x_3x_5+x_4x_5)x^3\\
&-(x_1x_2x_3+x_1x_2x_4+x_1x_2x_5+x_1x_3x_4+x_1x_3x_5\\
&\qquad+x_1x_4x_5+x_2x_3x_4+x_2x_3x_5+x_2x_4x_5+x_3x_4x_5)x^2\\
&+(x_1x_2x_3x_4+x_1x_2x_3x_5+x_1x_2x_4x_5+x_1x_3x_4x_5+x_2x_3x_4x_5)x\\
&-x_1x_2x_3x_4x_5\\
=&x^5-s_1x^4+s_2x^3-s_3x^2+s_4x-s_5
\end{aligned}
$$

定义1.6. 我们可以给所有n元单项式以**字典序**$\prec$进行如下排序
对于单项式$x_1^{a_1}\cdots x_n^{a_n}, x_1^{b_1}\cdots x_n^{b_n}$，比较次数，次数大的排在先，如果一样,比较$x_1$的次数$a_1, b_1$，次数大的排在先，如果一样，就比较$x_2$的次数$a_2, b_2$，直到比出先后
不难看出，两个多项式f, g相乘，fg中排在最先的的单项式是f, g中排在最先的的单项式的乘积

例子1.7. 对于3元单项式我们有如下字典序排列

$$\begin{aligned}\cdots &\prec x_3^5 \prec x_1^4 \prec x_1^3x_2 \prec x_1^3x_3 \prec x_1^2x_2^2 \prec x_1^2x_2x_3 \prec x_1^2x_3^2 \prec x_1x_2^3 \prec x_1x_2^2x_3\\ &\prec x_1x_2x_3^2 \prec x_1x_3^3 \prec x_2^4 \prec x_2^3x_3 \prec x_2^2x_3^2 \prec x_2x_3^3 \prec x_3^4 \prec x_1^3 \prec \cdots\end{aligned}$$

`Fundamental theorem of symmetric polynomials`

定理1.8 (对称多项式基本定理). 任何对称多项式可以写作基本对称多项式的多项式,即假如$f(x_1, \cdots, x_n)$是对称多项式，则存在多项式$g(x_1, \cdots, x_n)$使得

$$f(x_1, \cdots, x_n) = g(s_1, \cdots, s_n)$$

证明. 记$x_1^{a_1}\cdots x_n^{a_n}$为$f$中排在最先的的单项式,则必有$a_1 \geq \cdots \geq a_n$
注意到对称多项式$s_1^{a_1-a_2}s_2^{a_2-a_1}\cdots s_{n-2}^{a_{n-2}-a_{n-1}}s_{n-1}^{a_{n-1}-a_n}s_n^{a_n}$中排在最先的单项式是$x_1^{a_1}\cdots x_n^{a_n}$,故$f - s_1^{a_1-a_2}\cdots s_n^{a_n}$也是对称多项式,但其排在最先的单项式排在$x_1^{a_1}\cdots x_n^{a_n}$之后，重复该过程，每次做差后排在最先的单项式排序都会靠后，因此最终一定会终止，所以$f(x_1, \cdots, x_n)$
可以写作$g(s_1, \cdots, s_n)$ □

例子1.9. 对于2元对称多项式$f(x_1, x_2) = x_1^3 + x_2^3$, $s_1 = x_1 + x_2$, $s_2 = x_1x_2$

$$x_1^3 + x_2^3 - s_1^3 = -x_1^2x_2 - x_1x_2^2$$
$$-x_1^2x_2 - x_1x_2^2 + s_1^2s_2 = 0$$

故$f(x_1, x_2) = s_1^3 - s_1^2s_2$

2 群

定义2.1. 我们称对n个对象的所有置换为n阶**置换群**S_n,我们可以定义置换的复合为乘法,记恒等变换为**恒等元**1,记某个变换g的逆变换为**逆**g^{-1},**群**G是某个n阶置换群S_n中关于乘法封闭的非空子集

命题2.2. $G \subseteq S_n$是一个群，则G包含恒等元和逆

证明. 因为S_n只有有限多个置换，考虑$g^0 = 1, g = g^1, g^2, \cdots$，其中必有重复，不妨设$g^i = g^j, i < j$,则有$1 = g^{-i}g^i = g^{-i}g^j = g^{j-i} = g^k$, $k > 0$,故$1 = g^k \in G$, $g^{k-1} = g^{-1} \in G$ □

注2.3. 使得$g^k = 1$的最小正整数k叫做g的**阶**
注意到$ghh^{-1}g^{-1} = 1$，故$(gh)^{-1} = h^{-1}g^{-1}$, $(g_1 \cdots g_m)^{-1} = g_m^{-1} \cdots g_1^{-1}$

定义2.4. 将对象抽象为数字，我们记置换g将i置换到j为$gi = j$
假如一个置换将$1, \cdots, n$变为$j_1, \cdots, j_n$，记这个置换为

$$\begin{pmatrix} 1 & \cdots & n \\ j_1 & \cdots & j_n \end{pmatrix}$$

一个对$1, \cdots, n$的置换就是一个对$1, \cdots, n$的排列,故S_n中共有$n!$个置换
一个置换称为k阶**轮换**如果它将j_1变到j_2, j_2变到j_3, $\cdots$, j_{n-1}变到j_n, j_n变到j_1且保持其他元素不变,引入简化记号$(j_1j_2\cdots j_k)$来记这个轮换,注意到

$$(j_1j_2\cdots j_k) = (j_2j_3\cdots j_kj_1) = (j_3j_4\cdots j_kj_1j_2) = \cdots (j_kj_1j_2\cdots j_{k-1})$$

不难看出S_n中共有$C_n^k \cdot \dfrac{k!}{k} = \dfrac{n!}{k(n-k)!}$个$k$阶轮换,一个轮换称为**对换**如果它仅仅是交换了两个对象

例子2.5. $(513) = (351) = (135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$是$S_5$中的3阶轮换
$(42) = (24) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$是$S_5$中的对换

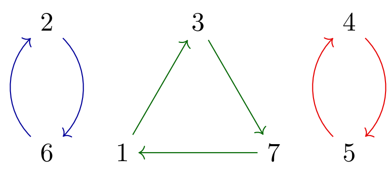
定义2.6. 群乘法一般不满足交换律$gh = hg$，称满足交换律的群为**Abel群**
如果G的子集H也是一个群，我们称H是G的**子群**

例子2.7. 考虑$A_3 = \{1, (123), (132)\}$是$S_3$的子群因为$(123)^2 = (132)$, $(123)^3 = 1$, A_3是Abel群,但S_3不是Abel群，因为$(12)(13) = (132) \neq (123) = (13)(12)$

命题2.8. 每个置换都可以唯一的写作轮换的乘积，且这些轮换所涉及的元素都不相同，故乘积的顺序无关紧要

证明. 我们通过举例来证明

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 5 & 4 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 4 & 5 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 3 & 4 & 5 & 2 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 4 & 6 & 7 \end{pmatrix} \\ &= (137)(26)(47) \end{aligned}$$



我们称(137), (26), (45)为σ的**循环节** $\square$

例子2.9. S_5中的置换有

恒等元$1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

$\dfrac{5!}{5} = 24$个5阶轮换:

(12345), (12354), (12435), (12453), (12534), (12543)
(13245), (13254), (13425), (13452), (13524), (13542)
(14235), (14253), (14325), (14352), (14523), (14532)
(15234), (15243), (15324), (15342), (15423), (15432)

$C_5^4 \cdot \dfrac{4!}{4} = 30$个4阶轮换:

(1234), (1243), (1324), (1342), (1423), (1432)
(1235), (1253), (1325), (1352), (1523), (1532)
(1245), (1254), (1425), (1452), (1524), (1542)
(1345), (1354), (1435), (1453), (1534), (1543)
(2345), (2354), (2435), (2453), (2534), (2543)

$C_5^3 \cdot \dfrac{3!}{3} = 20$个3阶轮换:

(123), (132), (124), (142), (125), (152), (134), (143), (135), (153), (145), (154)
(234), (243), (235), (253), (245), (254), (345), (354)

$C_5^2 = 10$个对换:

(12), (13), (14), (15), (23), (24), (25), (34), (35), (45)

$\dfrac{C_5^2 \cdot C_3^2}{2} = 15$个两个不相交对换的乘积:

(12)(34), (13)(24), (14)(23), (12)(35), (13)(25)
(15)(23), (12)(45), (14)(25), (15)(24), (13)(45)
(14)(35), (15)(34), (23)(45), (24)(35), (25)(34)

$C_5^2 \cdot \dfrac{3!}{3} = 20$个不相交对换与3阶轮换的乘积:

(123)(45), (132)(45), (124)(35), (142)(35), (125)(34), (152)(34)
(134)(25), (143)(25), (135)(24), (153)(24), (145)(23), (154)(23)
(234)(15), (243)(15), (235)(14), (253)(14), (245)(13), (254)(13)
(345)(12), (354)(12)

故总共$1 + 24 + 30 + 20 + 10 + 15 + 20 = 120 = 5!$个置换

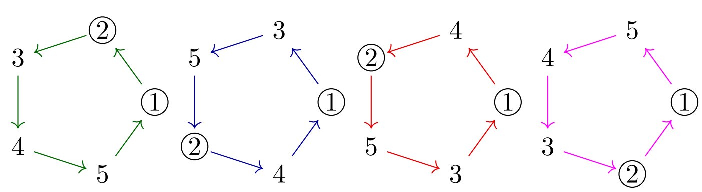
定义2.10. 群$G \subseteq S_n$叫做**传递的**如果对任意两个不相同的对象$k \neq l$，存在$g \in G$使得$gk = l$

例子2.11. S_3的子群$A_3 = \{1, (123), (132)\}$是传递的,因为$1, 2, 3$在恒等置换下不变, $(123)1 = 2, (123)2 = 3, (123)3 = 1$, $(132)1 = 3, (132)2 = 1, (132)3 = 2$
而S_3的子群$S_2 = \{1, (12)\}$则不是传递的,因为3在S_2的置换下不变

`G<=S5 transitive and contains a transposition implies G=S5`

引理2.12. 如果群$G \subseteq S_5$是传递的，且包含一个对换,那么$G = S_5$

证明. 不妨设$\sigma_2 = (12) \in G$
假设G有5阶轮换,则G包含这个轮换生成的5阶循环群,不妨设$\tau = (12345), \tau^2 = (13524), \tau^3 = (14253), \tau^4 = (15432) \in G$



这样假设没问题，因为$1,2$的位置必须得是以上4种情况中的一种，我们可以选择其他3位数字，这只是我们给对象的名字罢了，接着有$\sigma_2\tau^3 = (14)(253) \in G$, $\sigma_4 = \left(\sigma_2\tau^3\right)^3 = (14) \in G$, $\sigma_5 = \left(\sigma_4\tau^4\right)^3 = (15) \in G$, $\sigma_3 = \left(\sigma_5\tau^2\right)^3 = (13) \in G$,然后有$\sigma_2\sigma_3\sigma_2 = (23) \in G$, $\sigma_3\sigma_4\sigma_3 = (34) \in G$, $\sigma_4\sigma_5\sigma_4 = (45) \in G$,进而$G$包含所有的对换，故$G = S_5$
接下来证明任何传递的$G \subseteq S_5$都有5阶轮换
情况I:如果G没有5阶轮换，但有4阶轮换
不妨设$\tau = (1234), \tau^2 = (13)(24), \tau^3 = (1432) \in G$,由于$G$是传递的，故存在$\xi \in G$使得$\xi 4 = 5$
如果$\xi = (45), (45)(12), (45)(13), (45)(123)$,注意到$((45)(123))^3 = (45)$,那么$(45)(1234) = (12354)$, $(1234)(45)(12)(1234) = (12435)$, $(1432)(45)(13)(1234)(45)(13) = (15243)$
如果$\xi = (145), (145)(23)$,注意到$((145)(23))^4 = (145)$,那么$(1234)(145)(1234) = (13524)$,
如果$\xi = (2345), (1345)$,那么$(2345)(1234) = (13524)$, $(1345)(1234) = (12435)$
情况II:如果G没有$4,5$阶轮换，但有3阶轮换
不妨设$\tau = (123), \tau^2 = (132), \in G$,存在$\xi, \eta \in G$使得$\xi 1 = 4$, $\eta 1 = 5$
如果$\xi = (14), (14)(235), (14)(25), (145)$,那么$(14)(123) = (1234)$, $(14)(25)(123) = (15234)$, $(145)(123) = (12345)$
如果$\xi = (14)(23)$
若$\eta = (15)(23), (152)$,那么$(15)(23)(14)(23) = (145)$, $(14)(23)(152) = (15324)$
情况IV:如果G没有$3,4,5$阶轮换，但有$2,3$阶轮换乘积
显然
情况V:如果G没有$3,4,5$阶轮换和$2,3$阶轮换乘积，但有对换乘积
不妨设$\tau = (12)(34) \in G$,存在$\xi \in G$使得$\xi 1 = 5$
如果$\xi = (15), (15)(34), (15)(23)$,那么$(15)(12)(34) = (125)(34)$, $(15)(34)(12)(34) = (125)$, $(15)(23)(12)(34) = (13425)$
情况VI:如果G没有$3,4,5$阶轮换, $2,3$阶轮换乘积和对换乘积,但有对换
不妨设$\tau = (12) \in G$,存在$\xi \in G$使得$\xi 1 = 5$
如果$\xi = (15)$,那么$(15)(12) = (125)$ □

定义2.13. $H \subseteq G$叫做G的**正规子群**如果$\forall g \in G, h \in H$, $ghg^{-1} \in H$, G叫做**单群**如果G的正规子群只有$\{1\}$和G,我们说G中元素g, g'**相似**如果存在$g_1 \in G$使得$g' = g_1 g g_1^{-1}$

例子2.14. S_5的子群S_4不是正规子群,因为$(45)(1234)(45)^{-1} = (1235) \notin S_4$,注意这里$(1234)$和$(1235)$相似

引理2.15. 一个置换不可能同时被写作奇数个对换的乘积又被写作偶数个对换的乘积

证明. 考虑该置换作用在$\delta = \prod_{1 \le i < j \le n} (j - i) \neq 0$上，注意到对换将$\delta$变为$-\delta$,若该置换被写作奇数个置换，那么$\delta$应该变号，若该置换被写作奇数个置换，那么$\delta$应不变号，产生矛盾 □

定义2.16. 由于轮换$(j_1 j_2 \cdots j_k)$可以写作对换的乘积$(j_1 j_2)(j_2 j_3)\cdots(j_{k-1} j_k)$,故每个置换都可以写作对换的乘积，可以被写作奇数个对换乘积的置换称为**奇置换**，可以被写作偶数个对换乘积的置换称为**偶置换**，显然1是偶置换，偶置换的乘积是偶置换，奇置换的乘积是偶置换，偶只换与奇置换的乘积是奇置换，故S_n中所有的偶置换是一个正规子群，记作A_n

`Simplicity of A5`

定理2.17. A_5是单群

证明. 假如$\{1\} \neq G \subseteq A_5$是一个正规子群,接下来证明$G$中包含有一个3阶轮换
若$(12345) \in G$, $(123)(12345)(123)^{-1}(12345)^{-1} = (124) \in G$
若$(12)(34) \in G$, $(123)(12)(45)(123)^{-1}(12)(45) = (132) \in G$
故G中包含有一个3阶轮换,不妨设为(123)，接下来证明G包含A_5中所有3阶轮换
只需证明(123)与(124)相似, (123)与(145)相似
$(12453)(123)(12453)^{-1} = (124)$, $(24)(35)(123)(24)(35) = (145)$
故$G \subseteq A_5$包含所有3阶轮换，接下来证明$G = A_5$
$(123)(145) = (14523)$, $(123)(124) = (13)(24)$ □

3 域

定义3.1. $\mathbb{Q}\subseteq F\subseteq\mathbb{C}$称作域假如它满足加减乘除运算封闭,即如果$a,b\in F$,则$a+b,a-b,ab\in F$,且$\dfrac{b}{a}\in F,a\neq 0$

注3.2. 假如$F\subseteq K$都是域，我们称K为F的**域扩张**

定义3.3. 对于$\alpha_1,\cdots,\alpha_n\in\mathbb{C}$，我们可以定义

$$F(\alpha_1,\cdots,\alpha_n)=\left\{\frac{f(\alpha_1,\cdots,\alpha_n)}{g(\alpha_1,\cdots,\alpha_n)}\middle|f,g\text{为}F\text{上的多项式},g(\alpha_1,\cdots,\alpha_n)\neq 0\right\}$$

我们称这样关于$\alpha_1,\cdots,\alpha_n$的函数$\dfrac{f(\alpha_1,\cdots,\alpha_n)}{g(\alpha_1,\cdots,\alpha_n)}$为关于$\alpha_1,\cdots,\alpha_n$的有理函数
不难看出$F(\alpha_1,\cdots,\alpha_n)$为包含$F,\alpha_1,\cdots,\alpha_n$的最小的域

例子3.4. $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}|a,b\in\mathbb{Q}\}$
$\mathbb{Q}(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2|a,b,c\in\mathbb{Q}\}$
$\mathbb{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}|a,b,c,d\in\mathbb{Q}\}$

`Bezout's theorem`

定理3.5 (**Bézout定理**)**.** $m,n\in\mathbb{Z}$互素当且仅当存在$r,s\in\mathbb{Z}$，使得$rm+sn=1$

证明. 不妨假设$m,n>0$，否则可以考虑$(-r)(-m)+sn=1$当为m负数，$rm+(-s)(-n)=1$当为n负数，$(-r)(-m)+(-s)(-n)=1$当为m,n负数
我们使用归纳法，假设命题对于$m,n\leq N$都成立，现假设$n<m$，我们知道$m=un+v$，其中余数$v<n$与n也互素,由归纳假设知存在$r',s'\in\mathbb{Z}$，使得$r'n+s'v=1$，故有$1=r'n+s'v=r'n+s'(m-un)=(r'-s'u)n+s'm$，令$r=s',s=r'-s'u$即可
反之假设存在$r,s\in\mathbb{Z}$，使得$rm+sn=1$但m,n最大公因子为$d>1$，则有$\mathbb{Z}\ni r\dfrac{m}{d}+s\dfrac{n}{d}=\dfrac{1}{d}$，而这显然不可能 □

推论3.6. $m,n\in\mathbb{Z}$的最大公因子为d当且仅当存在$r,s\in\mathbb{Z}$，使得$rm+sn=d$

证明. $m,n\in\mathbb{Z}$的最大公因子为$d\Leftrightarrow\dfrac{m}{d},\dfrac{n}{d}\in\mathbb{Z}$的最大公因子为$1\Leftrightarrow\dfrac{m}{d},\dfrac{n}{d}$互素$\Leftrightarrow$存在$r,s\in\mathbb{Z}$，使得$r\dfrac{m}{d}+s\dfrac{n}{d}=1\Leftrightarrow rm+sn=d$ □

例子3.7. $m=34$, $n=38$, $d=2$
$38=1\times 34+4$
$34=8\times 4+2$
$4=2\times 2+0$
故$2=34-8\times 4=34-8\times(38-1\times 34)=34-8\times 38+8\times 34=9\times 34-8\times 38=9m-8n$

定义3.8. F是一个域,一个多项式f在F上**可约**如果它可以写作两个次数大于等于1的在F上的多项式g,h的乘积$f=gh$
如同整数分解为素因子一般，F上的多项式f也可以写作**素因式(不可约因式)**的乘积$f=f_1^{r_1}\cdots f_k^{r_k}$

`Bezout's theorem for polynomial`

定理3.9. 假如F是一个域，F上多项式f,g的最大公因式为d，则存在F上多项式r,s，使得$rf+sg=d$，特别的，f,g在任何包含F的域上的最大公因式都是d

证明. 同定理3.5证明一样，对多项式的次数做归纳 □

例子3.10. $f(x)=x^3+x^2+x+1$, $g(x)=2x^2+5x+3$, $d(x)=x+1$

$$
\begin{array}{r}
\frac{1}{2}x \;-\frac{3}{4} \\
2x^2+5x+3\,\overline{\big)\; x^3 \;+x^2 \;\;+x \;\;+1} \\
-x^3-\frac{5}{2}x^2 \;-\frac{3}{2}x \qquad \\
\hline
-\frac{3}{2}x^2 \;-\frac{1}{2}x \;\;+1 \\
\frac{3}{2}x^2+\frac{15}{4}x \;+\frac{9}{4} \\
\hline
\frac{13}{4}x+\frac{13}{4}
\end{array}
$$

$$x^3+x^2+x+1=\left(\frac{1}{2}x-\frac{3}{4}\right)(2x^2+5x+3)+\frac{13}{4}x+\frac{13}{4}$$

$$
\begin{array}{r}
\frac{8}{13}x+\frac{12}{13} \\
\frac{13}{4}x+\frac{13}{4}\,\overline{\big)\; 2x^2+5x \;+3} \\
-2x^2-2x \qquad \\
\hline
3x \;+3 \\
-3x \;-3 \\
\hline
0
\end{array}
$$

$2x^2+5x+3=\left(\frac{8}{13}x+\frac{12}{13}\right)\left(\frac{13}{4}x+\frac{13}{4}\right)+0$

故$\frac{13}{4}x+\frac{13}{4}=x^3+x^2+x+1-\left(\frac{1}{2}x-\frac{3}{4}\right)(2x^2+5x+3)=f(x)-\left(\frac{1}{2}x-\frac{3}{4}\right)g(x)$

两边同时除去$\frac{13}{4}$，有$x+1=\frac{4}{13}f(x)-\left(\frac{2}{13}x-\frac{3}{13}\right)g(x)$

Minimal polynomial

命题3.11 (Galois)**.** 假设F是域，α是F上某个多项式的根，存在唯一一个F上的首项系数为1的多项式$m(x)$，使得所有F上以α为根的多项式都被m整除

证明. 假设F上的多项式f以α为根，$f=f_1^{r_1}\cdots f_k^{r_k}$是$f$的素因式分解，令$m=f_i$为其中一个以$\alpha$为根的素因子,这样任何一个$F$上以$\alpha$为根的多项式$g$与$m$的最大公因式都不是1，否则根据定理3.9知$1=r(\alpha)g(\alpha)+s(\alpha)m(\alpha)=0$,另外我们又知道$m$是素因子，故$g$被$m$整除 □

注3.12. $m(x)$称为α在F上的**最小多项式**，我们称$m(x)$的根为α在F上的**共轭根**

例子3.13. $\sqrt{2}$在$\mathbb{Q}$上的最小多项式为x^2-2, $-\sqrt{2}$是它的共轭根
ω在$\mathbb{Q}$上的最小多项式为x^2+x+1, $\omega^2=\omega^{-1}$是它的共轭根,其中ω是三次单位根
$\sqrt[3]{2}$在$\mathbb{Q}$上的最小多项式为x^3-2, $\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$是它的共轭根,其中$\omega$是三次单位根

Unique expression of elements in F(apha)

命题3.14 (Kummer)**.** 假设m是α在F上的最小多项式, $F(\alpha)$中的元素β都可以表示为一个次数低于n的多项式$f(\alpha)=a_{n-1}\alpha^{n-1}+\cdots+a_0$，且这个表达唯一

证明. 假设$m(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0$, $F(\alpha)$中的元素β都可以表示为一个α的有理函数$\frac{f(\alpha)}{g(\alpha)}$,这里$g(\alpha)\neq 0$，故$m$不整除$g$,由于最小多项式不可约，$m$与$g$互素,根据定理3.9,存在$F$上的多项式$r,s$，使得$rm+sg=1$,故$s(\alpha)g(\alpha)=1$, $\beta=f(\alpha)s(\alpha)$,即$F(\alpha)$中的元素可以写成α的多项式,我们又知道$m(\alpha)=0\Rightarrow\alpha^n=-c_{n-1}\alpha^{n-1}-\cdots-c_1\alpha-c_0$,故$F(\alpha)$中的元素$\beta$都可以表示为一个次数低于$n$的$\alpha$的多项式,接下来证明唯一性
假设$\beta=f(\alpha)=g(\alpha)$,其中$f(\alpha)=a_{n-1}\alpha^{n-1}+\cdots+a_0$, $g(\alpha)=b_{n-1}\alpha^{n-1}+\cdots+b_0$,则$0=f(\alpha)-g(\alpha)=(a_{n-1}-b_{n-1})\alpha^{n-1}+\cdots+(a_0-b_0)$, $h(x)=(a_{n-1}-b_{n-1})x^{n-1}+\cdots+(a_0-b_0)$是一个次数低于$n$的多项式且有为根，故$h=0$ □

例子3.15. $\frac{1}{\sqrt{2}}=\frac{\sqrt{2}}{2}$, $\frac{1}{\sqrt{2}+1}=\sqrt{2}-1$

设ω是三次单位根, $\omega^2+\omega+1=0\Rightarrow 1+\omega=\omega^2\Rightarrow\frac{1}{1+\omega}=\omega^{-2}=\omega$

Irreducible polynomial doesn't have multiple roots

命题3.16 (Galois)**.** 不可约多项式没有重根

证明. 假设f是F上不可约多项式，在$\mathbb{C}$上分解为$f(x)=(x-a_1)^{k_1}(x-a_2)^{k_2}\cdots(x-a_n)^{k_n}$，则

$$\begin{aligned}f'(x)&=k_1(x-a_1)^{k_1-1}(x-a_2)^{k_2}\cdots(x-a_n)^{k_n}\\&+k_2(x-a_1)^{k_1}(x-a_2)^{k_2-1}\cdots(x-a_n)^{k_n}\\&+\cdots\\&+k_n(x-a_1)^{k_1}(x-a_2)^{k_2}\cdots(x-a_n)^{k_n-1}\\&=(k_1(x-a_2)\cdots(x-a_n)+\cdots+k_n(x-a_1)\cdots(x-a_{n-1}))\\&\quad(x-a_1)^{k_1-1}(x-a_2)^{k_2-1}\cdots(x-a_n)^{k_n-1}\end{aligned}$$

仍然是F上的多项式，故f和f'的最大公因式包含$(x-a_1)^{k_1-1}(x-a_2)^{k_2-1}\cdots(x-a_n)^{k_n-1}$ □

定义3.17. 使用$r|n$表示r**整除**n, $r\nmid n$表示r**不整除**n,例如$3|6, 4\nmid 6$
假设p是素数，那么在模p同余的意义下,即$m\equiv n\Leftrightarrow p|m-n$，我们可以对非零数$m$(模$p$不余零)作除法,因为$m,p$互素，存在$r,s\in\mathbb{Z}$使得$rm+sp=1$,故$rm\equiv 1$，如果$r'm\equiv 1$，则$(r-r')m\equiv 0\Rightarrow r\equiv r'$，故可以定义$\dfrac{1}{m}=r$，故$\mathbb{F}_p=\{0,1,\cdots,p-1\}$在加减乘除运算下封闭，且$\mathbb{F}_p$满足加法乘法交换律，结合律，分配率，我们称$\mathbb{F}_p$为**有限$p$域**

定义3.18. 整系数多项式$f(x)=a_mx^m+\cdots+a_0$称作**本原多项式**如果$a_m,\cdots,a_0$的最大公约数为1，换一种说法，对任何素数p，$f(x)$看作$\mathbb{F}_p$上的多项式(系数模p)都不为零

Gauss' lemma

引理3.19 (**Gauss引理**)**.** 本原多项式的乘积还是本原多项式

证明. 假设$f(x)=a_mx^m+\cdots+a_0, g(x)=b_nx^n+\cdots+b_0$是本原多项式,对任何素数$p$，$f(x),g(x)$在$\mathbb{F}_p$上都不为零,故$f(x)g(x)$在$\mathbb{F}_p$上也不为零,故$f(x)g(x)$还是本原多项式 □

定理3.20. 不可约整系数多项式$f(x)$作为有理系数多项式不可约

证明. 注意到任何有理系数多项式$\dfrac{a_n}{b_n}x^n+\cdots+\dfrac{a_0}{b_0}$可以经过通分写作$\dfrac{c_nx^n+\cdots+c_0}{d}$，其中$c_nx^n+\cdots+c_0$是本原多项式假设$f$可以写作两个有理系数多项式的乘积$\dfrac{g}{d_1}\dfrac{h}{d_2}=\dfrac{gh}{d_1d_2}$，其中$g,h$是本原多项式，故$gh$也是本原多项式,故$d_1d_2=\pm1$, $f=\pm gh$变成了在$\mathbb{Z}$上的分解 □

Eisenstein's criterion

定理3.21 (**Eisenstein判别法**)**.** 假设存在素数p使得整系数多项式$f(x)=a_nx^n+\cdots+a_0$满足$p|a_i, 0\le i\le n-1$, $p\nmid a_n$, $p^2\nmid a_0$，则f不可约

证明. 假设$f=gh$可约，其中$g(x)=b_kx^k+\cdots+b_0$, $h(x)=c_lx^l+\cdots+c_0$, $k+l=n$, $a_n=b_kc_l$，将f,g,h看作在$\mathbb{F}_p$上的多项式,则有$f(x)=a_nx^n$,因为$a_0=b_0c_0$, $b_0\equiv 0, c_0\not\equiv 0$或者$b_0\not\equiv 0, c_0\equiv 0$,不妨假设$b_0\not\equiv 0, c_0\equiv 0$，且$c_m\not\equiv 0$是$h$不为零的次数最小项的系数，则有$a_m=b_0c_m\not\equiv 0$,这与$f(x)=a_nx^n$矛盾 □

4 Galois预解式

Lemma for primitive element theorem

引理4.1. 假设$\alpha_1,\cdots,\alpha_m \in F$互不相等, $\beta=\beta_1,\cdots,\beta_n \in F$互不相等,则存在$c \in F$使得$\alpha_i + c\beta_j$也互不相等

证明. 反之假如$\alpha_i + c\beta_j = \alpha_k + c\beta_l$,则$\beta_j \neq \beta_l$否则$\beta_j = \beta_l \Rightarrow \alpha_i = \alpha_k$,故$c = \dfrac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$,而这样的$\dfrac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$只有有限多个，而$F$有无穷多元素，我们自然可以找到$c$使得$c = \dfrac{\alpha_i - \alpha_k}{\beta_l - \beta_j}$永不成立 □

Primitive element theorem

定理4.2 (**本原元定理**)**.** *假设f, g分别是α, β在F上的最小多项式, $\alpha = \alpha_1,\cdots,\alpha_m, \beta=\beta_1,\cdots,\beta_n$分别为$\alpha$和$\beta$的共轭根,根据引理4.1,存在$c \in F$,使得使得$\alpha_i + c\beta_j$互不相等,则$F(\alpha,\beta) = F(\gamma)$,其中$\gamma = \alpha + c\beta$被称作***本原元**

证明. $h(x) = f(\gamma - cx)$是$F(\gamma)$上的多项式, β是h的根,且$\beta_i \neq \beta$都不是h的根,故$g(x)$和$h(x)$的最大公因式为$x-\beta$,因而$x-\beta$是$F(\gamma)$上的多项式, $\beta \in F(\gamma)$, $\alpha = \gamma - c\beta \in F(\gamma)$ □

Lemma for Galois resolvent

引理4.3. 假设f是F上的多项式, $\alpha_1,\cdots,\alpha_n$为f的根, $\gamma = \alpha_1 + c_2\alpha_2 + \cdots + c_k\alpha_k, c_i \in F$,则$\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_k\alpha_{j_k}$包含了所有$\gamma$的共轭根,其中$j_i = 1,\cdots,n$,特别的，如果$k=n$，则$\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_n\alpha_{j_n}$包含了所有$\gamma$的共轭根,其中$j_1,\cdots,j_n$是$1,\cdots,n$的排列

证明. 考虑

$$H(x) = \prod_{1 \leq j_1,\cdots,j_k \leq n} (x - (x_{j_1} + c_2 x_{j_2} + \cdots + c_k x_{j_k}))$$

是以$x_1,\cdots,x_n$为系数的多项式,其中$j_i = 1,\cdots,n$,则$H(x)$在对任意$x_1,\cdots,x_n$的置换下不变,故其系数在对任意$x_1,\cdots,x_n$的置换下亦不变,即为$x_1,\cdots,x_n$的对称多项式,由定理1.8, H可以写作以$s_1,\cdots,s_n$为系数的多项式,现将x_i替换为α_i可知$H(x)$是F上以$\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_k\alpha_{j_k}$为根的多项式,由命题3.11知, H包含了所有γ的共轭根

如果$k=n$,考虑

$$G(x) = \prod_{j_1,\cdots,j_k} (x - (x_{j_1} + c_2 x_{j_2} + \cdots + c_n x_{j_n}))$$

是以$x_1,\cdots,x_n$为系数的多项式,其中$j_1,\cdots,j_n$是$1,\cdots,n$的排列, $G(x)$在对任意$x_1,\cdots,x_n$的置换下不变,故其系数在对任意$x_1,\cdots,x_n$的置换下亦不变,即为$x_1,\cdots,x_n$的对称多项式,由定理1.8, G可以写作以$s_1,\cdots,s_n$为系数的多项式,现将x_i替换为α_i可知$G(x)$是F上以$\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_n\alpha_{j_n}$为根的多项式,由命题3.11知, G包含了所有γ的共轭根 □

Galois resolvent

定理4.4 (Galois预解式)**.** *假设f是F上的多项式, $\alpha_1,\cdots,\alpha_n$为f的不同的根(不计重数),存在$c_2,\cdots,c_n \in F$使得$\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_n\alpha_{j_n}$互不相等,其中$j_i = 1,\cdots,n$,且$F(\alpha_1,\cdots,\alpha_n)$ $= F(\gamma)$,其中$\gamma = \alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$*

证明. 使用归纳法,假设存在$c_2,\cdots,c_{n-1} \in F$使得$\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_{n-1}\alpha_{j_{n-1}}$互不相等,其中$j_i = 1,\cdots,n$,且$F(\alpha_1,\cdots,\alpha_{n-1}) = F(\eta)$,其中$\eta = \alpha_1 + c_2\alpha_2 + \cdots + c_{n-1}\alpha_{n-1}$,根据引理4.1,存在$c_n \in F$使得$\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_n\alpha_{j_n}$互不相等,其中$j_i = 1,\cdots,n$,根据引理4.3, $\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_{n-1}\alpha_{j_{n-1}}$包含了所有$\eta$的共轭根,并且我们知道$\alpha_1,\cdots,\alpha_n$包含$\alpha_i$所有的共轭根,根据定理4.2, $F(\alpha_1,\cdots,\alpha_n) = F(\gamma)$,其中$\gamma = \eta + c_n\alpha_n = \alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$,根据引理4.3, $\alpha_{j_1} + c_2\alpha_{j_2} + \cdots + c_n\alpha_{j_n}$包含了所有$\gamma$的共轭根,其中$j_1,\cdots,j_n$是$1,\cdots,n$的排列 □

注4.5. 称$\gamma = \alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$为**Galois预解式**,记所有$\gamma$的共轭根为$\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = \gamma = \gamma_1 = \alpha_{11} + c_2\alpha_{12} + \cdots + c_n\alpha_{1n}, \cdots, \gamma_m = \alpha_{m1} + c_2\alpha_{m2} + \cdots + c_n\alpha_{mn}$,其中$\alpha_{i1},\cdots\alpha_{in}$是$\alpha_1,\cdots,\alpha_n$的某个排列

5 Galois群

注5.1. 假设$f(x)$是F上的一个多项式，$\alpha_1,\cdots,\alpha_n$是的根,对于有理函数$\beta=\dfrac{f(\alpha_1,\cdots,\alpha_n)}{g(\alpha_1,\cdots,\alpha_n)}$，假如对$\alpha_1,\cdots,\alpha_n$的任意排列不改变表达式，则$\beta\in F$，但$F$中的元素并不一定在$\alpha_1,\cdots,\alpha_n$
的置换下保持不变，例如当$\alpha_1=1,\alpha_2=2,-1=\alpha_1-\alpha_2$时，对$\alpha_1-\alpha_2$置换$\alpha_1,\alpha_2$会变为$\alpha_2-\alpha_1=1$，但对$-1$置换$\alpha_1,\alpha_2$会使$-1$保持不变

`Lemma for Galois group`

引理5.2 (Galois)**.** 假设$f(x)$是F上的一个多项式，以$\alpha_1,\cdots,\alpha_n$为根(不计重数)，$\gamma=\alpha_1+c_2\alpha_2+\cdots+c_n\alpha_n$为Galois预解式，$\gamma$的共轭根为$\gamma=\gamma_1=\alpha_{11}+c_2\alpha_{12}+\cdots+c_n\alpha_{1n},\cdots,\gamma_m=\alpha_{m1}+c_2\alpha_{m2}+\cdots+c_n\alpha_{mn}$,其中$\alpha_{i1},\cdots\alpha_{in}$是$\alpha_1,\cdots,\alpha_n$的某个置换$g_i$，$\alpha_1=h_1(\gamma),\cdots,\alpha_n=h_n(\gamma)$,那么$\alpha_{ij}=h_j(\gamma_i)$
特别的，g_i作用在$F(\alpha_1,\cdots,\alpha_n)$中元素上与其具体表达方式无关

证明. 注意到F上的多项式$(\alpha_1-h_j(x))\cdots(\alpha_n-h_j(x))$有根$\gamma$,故$\gamma_1,\cdots,\gamma_m$都是根，$(\alpha_1-h_j(\gamma_i))\cdots(\alpha_n-h_j(\gamma_i))$仍然为零,故$h_j(\gamma_i)$是某个$\alpha_k$,另一方面，$h_1(x)+c_2h_2(x)+\cdots+c_nh_n(x)-x$有根$\gamma$，故$\gamma_1,\cdots,\gamma_m$都是根，$\alpha_{i1}+c_2\alpha_{i2}+\cdots+c_n\alpha_{in}=\gamma_i=h_1(\gamma_i)+c_2h_2(\gamma_i)+\cdots+c_nh_n(\gamma_i)$,由于$\alpha_{j_1}+c_2\alpha_{j_2}+\cdots+c_n\alpha_{j_n}$互不相同,故$\alpha_{ij}=h_j(\gamma_i)$
假设$F(\alpha_1,\cdots,\alpha_n)$中元素$\beta$有两种表达方式$\dfrac{p(\alpha_1,\cdots,\alpha_n)}{q(\alpha_1,\cdots,\alpha_n)}$，$\dfrac{p'(\alpha_1,\cdots,\alpha_n)}{q'(\alpha_1,\cdots,\alpha_n)}$,则

$$g_i\frac{p(\alpha_1,\cdots,\alpha_n)}{q(\alpha_1,\cdots,\alpha_n)}=\frac{p(\alpha_{i1},\cdots,\alpha_{in})}{q(\alpha_{i1},\cdots,\alpha_{in})}=\frac{p(h_1(\gamma_i),\cdots,h_n(\gamma_i))}{q(h_1(\gamma_i),\cdots,h_n(\gamma_i))}$$

同理有

$$g_i\frac{p'(\alpha_1,\cdots,\alpha_n)}{q'(\alpha_1,\cdots,\alpha_n)}=\frac{p'(h_1(\gamma_i),\cdots,h_n(\gamma_i))}{q'(h_1(\gamma_i),\cdots,h_n(\gamma_i))}$$

简化有理多项式$\dfrac{p(h_1(x),\cdots,h_n(x))}{q(h_1(x),\cdots,h_n(x))}-\dfrac{p'(h_1(x),\cdots,h_n(x))}{q'(h_1(x),\cdots,h_n(x))}$得到$\dfrac{P(x)}{Q(x)}$，则有$\dfrac{P(\gamma)}{Q(\gamma)}=0$,所以$P(\gamma)=0$,故$P(\gamma_i)=0$,所以

$$\frac{p(h_1(\gamma_i),\cdots,h_n(\gamma_i))}{q(h_1(\gamma_i),\cdots,h_n(\gamma_i))}-\frac{p'(h_1(\gamma_i),\cdots,h_n(\gamma_i))}{q'(h_1(\gamma_i),\cdots,h_n(\gamma_i))}=\frac{P(\gamma_i)}{Q(\gamma_i)}=0$$

故g_i作用在$F(\alpha_1,\cdots,\alpha_n)$中元素上与其具体表达方式无关 □

`Galois group`

定理5.3 (**Galois群**)**.** *假设$f(x)$是F上的一个多项式，$\alpha_1,\cdots,\alpha_n$是的根(不计重数)，可以定义f在F上的Galois群G为所有保持F中元素不变的置换，注意这里保持元素不变是指对任意的表达方式，显然G是个群,不仅如此，$F(\alpha_1,\cdots,\alpha_n)$中所有被$G$固定的元素也都在$F$中,且满足这样性质的群也是唯一的*

证明. 假设$\gamma=\alpha_1+c_2\alpha_2+\cdots+c_n\alpha_n$为Galois预解式,设$\gamma$在$F$上最小多项式为$m(x)$，$\gamma$的共轭根为$\gamma=\gamma_1=\alpha_{11}+c_2\alpha_{12}+\cdots+c_n\alpha_{1n},\cdots,\gamma_m=\alpha_{m1}+c_2\alpha_{m2}+\cdots+c_n\alpha_{mn}$,其中$\alpha_{i1},\cdots\alpha_{in}$是$\alpha_1,\cdots,\alpha_n$的某个置换$g_i$,根据引理5.2我们知道$g_i\in G$,而对于$g\in G$，$gm(x)$
$=m(x)$，故g将γ变成某个γ_i,因为Galois预解式在不同置换下都不相同，$g=g_i$,因此$G=\{g_1,\cdots,g_m\}$
根据命题3.14我们知道$F(\alpha_1,\cdots,\alpha_n)=F(\gamma)$中的元素可以唯一的被表示为的一个次数低于的多项式$q(\gamma)$,如果$q(x)$不是常数且$q(\gamma)$被$g_i$固定，即$q(\gamma_i)$都相等,则$F(\gamma)$上多项式$q(x)-\gamma$有个$n$根，而这不可能因为它的次数小于$n$,故$F(\alpha_1,\cdots,\alpha_n)$中所有被$g_i$固定的元素都在$F$中,显然$F(\alpha_1,\cdots,\alpha_n)$中所有被$G$固定的元素也都在$F$中
最后证明Galois群的唯一性,假设G'是另一个满足条件的群,即G'所有保持F中元素不变且所有在G'下不变的元素都在F中,故$G'\subseteq G$,假设G'只是G的一个真子群，$G=\{g_1,g_{j_2},\cdots,g_{j_k}\}$，$k<m$,则多项式$(x-\gamma_1)(x-\gamma_{j_2})\cdots(x-\gamma_{j_k})$在$G'$作用下不变，故是$F$上的多项式，这与$m(x)$是最小多项式矛盾,故$G'=G$ □

`Splitting lemma`

引理5.4 (Galois)**.** f是F上的一个多项式，f的根为$x_1,\cdots,x_n$，记f在F上的Galois群为G,如果F上的多项式g在$F(x_1,\cdots,x_n)$中有根β，则g所有的根都在$F(x_1,\cdots,x_n)$里，G中的元素将β变成其共轭根

证明. 假设$\beta = \dfrac{p(x_1,\cdots,x_n)}{q(x_1,\cdots,x_n)}$是$g$，考虑

$$h(x) = \prod_{j_1,\cdots,j_n}\left(x - \frac{p(x_{j_1},\cdots,x_{j_n})}{q(x_{j_1},\cdots,x_{j_n})}\right)$$

其中$j_1,\cdots,j_n$是$1,\cdots,n$的排列, h在$x_1,\cdots,x_n$的置换下不变，故是F上的多项式，包含β为根,假设$m(x)$是β的最小多项式，则m在G下不变，故G中的元素将β变成其共轭根 □

`Galois group of irreducible polynomial is transitive`

定理5.5. *f是F上一个不可约多项式，$x_1,\cdots,x_n$是f的根,根据命题3.16，我们知道它们互不相同，G是f的$Galois$群，则对任意的x_i,x_j，存在G中的置换g使得$gx_i = x_j$,即G是传递的*

反过来，如果f是F上一个多项式,其$Galois$群G是传递的，那么f在F上不可约

证明. 若不然，不妨设所有置换只是置换$x_1,\cdots,x_q$和置换$x_{q+1},\cdots,x_n$，则$(x-x_1)\cdots(x-x_q)$在G置换下不变，所以是F上的多项式，这与f不可约相矛盾

如果f可约,根据引理5.4, G只能将根置换到它的共轭根，故G不是传递的,产生矛盾 □

6 主要定理

`Main lemma`

引理6.1. $f(x)=(x-\alpha_1)\cdots(x-\alpha_5), g(x)=(x-\beta_1)\cdots(x-\beta_n)$是$F$上没有重根的五次和$n$次多项式,且$K=F(\beta_1)=F(\beta_1,\cdots,\beta_n)$, g在F上的Galois群H是Abel群, f在F上的Galois群G是A_5,那么f在K上的Galois群G'仍然是A_5

证明. 记$L=F(\alpha_1,\cdots,\alpha_5)$, g在L上的Galois群为H', fg在F上的Galois群为$\mathcal{G}$,注意到Galois群之间的关系, $G',G\subseteq S_5$, $H',H\subseteq S_n$, $S_5,S_n,\mathcal{G}\subseteq S_{5+n}$, $S_5\cap S_n=\{1\}$

$$\begin{tikzcd}
K \arrow[r, dash, "G'"] \arrow[d, dash, "H"'] & \Gamma \arrow[d, dash, "H'"] \\
F \arrow[r, dash, "G=A_5"'] \arrow[ur, dash, "\mathcal{G}"] & L
\end{tikzcd}$$

由于G'固定K中的元素，G'当然也固定F中的元素，故$G'\subseteq G$
对于任意的$g\in\mathcal{G}$, $g'\in G'$,有$gg'g^{-1}\beta_l=gg'\beta_k=g\beta_k=\beta_l$,故$gg'g^{-1}$也固定$K$中的元素, G'是$G=A_5$的一个正规子群，根据定理2.17, $G'=\{1\}$或者$G'=A_5$
如果$G'=\{1\}$, $K=\Gamma$, $\alpha_i=h_i(\beta_1)$,由于$f(x)=(x-\alpha_1)\cdots(x-\alpha_5)=(x-h_1(\beta_1))\cdots(x-h_5(\beta_1))$在$H$作用下不变, H通过对β_1作用将α_i变为另一根α_j,另外,判别式$0\neq\Delta=\prod\limits_{i<j}(\alpha_i-\alpha_j)^2=\prod\limits_{i<j}(h_i(\beta_1)-h_j(\beta_1))^2$在$H$作用下仍然为$\Delta$,故$\alpha_1,\cdots,\alpha_5$在$H$中元素变换后仍然互不相等,即$H$中元素通过对$\beta_1$作用而对$\alpha_1,\cdots,\alpha_5$置换,注意这里不同$H$中的元素可能对$\alpha_1,\cdots,\alpha_5$进行了相同的置换
对于$\gamma=\dfrac{p(\alpha_1,\cdots,\alpha_5)}{q(\alpha_1,\cdots,\alpha_5)}\in L$,若$\gamma=\dfrac{p(h_1(\beta_1),\cdots,h_5(\beta_1))}{q(h_1(\beta_1),\cdots,h_5(\beta_1))}\in\Gamma=K$在$H$下不变,根据定理5.3, $\gamma\in F$,同时也说明由H对β_1作用引入对$\alpha_1,\cdots,\alpha_5$的置换正好就是G,因为H是Abel群，
G也得是Abel群，但A_5不是Abel群因为$(12)(13)=(132)\neq(123)=(13)(12)$ □

定义6.2. $F\subseteq K$称为n次**根域扩张**，如果存在$\alpha\in K,\alpha^n\in F$使得$K=F(\alpha)$

例子6.3. $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}\subseteq\mathbb{Q}(\omega)$都是根域扩张，其中$\omega$是三次单位根

`Lemma for main theorem`

引理6.4 (Abel). 假设F包含n次单位根ζ，$F\subseteq F(\alpha)=K$为n次根域扩张, $\alpha^n=\beta\in F$, $x^n-\beta$在F上的Galois群是Abel群
对于n次根域扩张$\mathbb{Q}\subset\mathbb{Q}(\zeta)$, x^n-1在$\mathbb{Q}$上的Galois群是Abel群

证明. $x^n-\beta$的根为$\alpha,\zeta\alpha,\cdots,\zeta^{n-1}\alpha$，考虑其Galois群中置换$g,h$,则一定存在$i,j$使得$g(\alpha)=\zeta^i\alpha$, $h(\alpha)=\zeta^j\alpha$，那么$h(g(\alpha))=h(\zeta^i\alpha)=\zeta^ih(\alpha)=\zeta^i\zeta^j\alpha=\zeta^{i+j}\alpha=g(h(\alpha))$,故$gh=hg$,因为它们对$\alpha$作用是相同的
x^n-1的根为$1,\zeta,\cdots,\zeta^{n-1}$，考虑其Galois群中的置换$g,h$,则一定存在$i,j$使得$g(\zeta)=\zeta^i$, $h(\zeta)=\zeta^j$,那么$h(g(\zeta))=h(\zeta^i)=h(\zeta)^i=\left(\zeta^j\right)^i=\zeta^{ij}=g(h(\zeta))$,故$gh=hg$ □

`S5 to A5`

引理6.5. 假如五次多项式f在F上的Galois群是S_5,记f的根为$x_1,\cdots,x_5$
记**判别式**$\Delta=\prod\limits_{i<j}(x_i-x_j)^2$的一个平方根为$\delta=\prod\limits_{i<j}(x_i-x_j)$，则$f$在$F(\delta)$上的Galois群是$A_5$

证明. 注意到偶置换固定δ而奇置换将δ变为$-\delta$, f在$F(\delta)$上的Galois群G固定δ,故是A_5的子群,另一方面,由于Galois群对F中元素的作用与其表达式无关，$F(\delta)$在A_5作用下不变,由定理5.3中Galois群的唯一性知$G=A_5$ □

`Main theorem`

定理6.6. $f(x)$是F上的五次多项式，其*Galois*群G是A_5或者S_5，则$f(x)=0$不可根式求解

证明. 不妨假设$G = A_5$，如果$G = S_5$,由引理6.5，$f(x)$在$F(\delta)$上的Galois群是A_5
根据定理5.5, f在$K(\zeta)$上不可约,根据定理3.16, f没有重根
反设$f(x) = 0$可由根式求解,则存在一系列根域扩张

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \cdots, \alpha_m) = K$$

$\alpha_i \in F(\alpha_1, \cdots, \alpha_i), \alpha_i^{n_i} \in F(\alpha_1, \cdots, \alpha_{i-1})$,使得$K$包含$f(x)$所有的根,记$n = n_1 \cdots n_m$, ζ为n次单位根，考虑系列根域扩张

$$F \subset F(\zeta) \subset F(\alpha_1, \zeta) \subset F(\alpha_1, \alpha_2, \zeta) \subset \cdots \subset F(\alpha_1, \cdots, \alpha_m, \zeta) = K(\zeta)$$

这里$F(\alpha_1, \cdots, \alpha_{i-1}, \zeta)$包含$n_i$次单位根$\zeta^{\frac{n}{n_i}}$,且$K(\zeta)$仍然包含$f(x)$所有的根,但根据引理6.4以及引理6.1,我们知道f在$K(\zeta)$上的Galois群仍然是A_5,根据定理5.5我们知道f在$K(\zeta)$上不可约，产生矛盾 $\square$

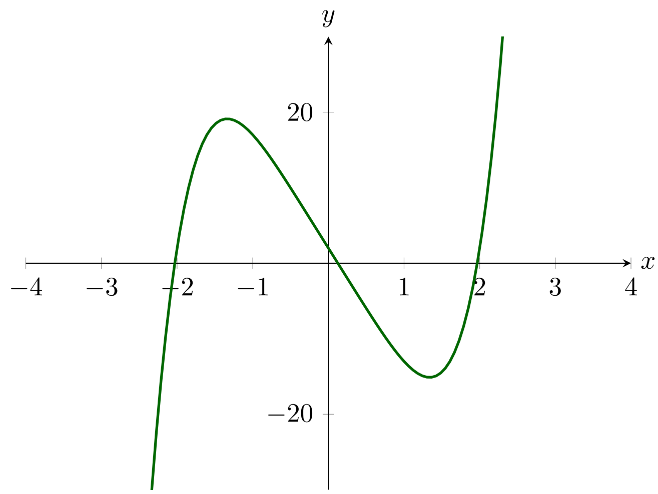
7 不可求解五次方程实例

`Galois group of an irreducible polynomial containing a transposition is S5`

引理7.1. $f(x)$是$\mathbb{Q}$上不可约五次多项式，且恰好有三个互不相同的实根，其Galois群G是S_5

证明. 假设$x_1 < x_2 < x_3$是三个实根，$z, \bar{z}$是一对复数根
考虑共轭引入对根的置换$\tau : x_i \to x_i, z \leftrightarrow \bar{z}$,假设$\dfrac{p(x_1,x_2,x_3,z,\bar{z})}{q(x_1,x_2,x_3,z,\bar{z})} \in \mathbb{Q}$, $\dfrac{p(x_1,x_2,x_3,z,\bar{z})}{q(x_1,x_2,x_3,z,\bar{z})} = \overline{\dfrac{p(x_1,x_2,x_3,z,\bar{z})}{q(x_1,x_2,x_3,z,\bar{z})}} = \dfrac{p(x_1,x_2,x_3,\bar{z},z)}{q(x_1,x_2,x_3,\bar{z},z)} = \tau\dfrac{p(x_1,x_2,x_3,z,\bar{z})}{q(x_1,x_2,x_3,z,\bar{z})}$,故$\mathbb{Q}$在$\tau$的作用下不变,对换$\tau \in G$,另一方面，根据定理5.5,我们知道$G$是传递的,由引理2.12我们知$G = S_5$ □

例子7.2. 根据定理3.21在$p = 2$的时候可知$f(x) = x^5 - 16x + 2$不可约, $x^5 - 16x + 2$有三个实根，因为求导可知f先增再减再增,且$f(-3) = -193 < 0, f(-1) = 17, f(1) = -13, f(2) = 2$



由引理7.1以及定理6.6可知，$x^5 - 16x + 2 = 0$不可用根式求解

8 历史发展

一元二次方程的解法古巴比伦便早已有之，一元高次方程的数值解法也早在中国出现(九章算术)，而直到公元16世纪，意大利的Ferro，Tartaglia，Cardano才发现了一元三次方程的解法

定理8.1 (Cardano公式). 一元三次方程$x^3+bx^2+cx+d=0$的一般求解方法

设$y=x+\frac{b}{3}$,则有$y^3+py+q=0$,其中$p=c-\frac{b^2}{3}$,$q=\frac{2b^3}{27}-\frac{bc}{3}+d$,这一步与解一元二次方程中的“平移”如出一辙,接下来假设y写作$u+v$,则有$u^3+(3uv+p)(u+v)+v^3+q=0$,假如我们令$3uv=-p\Rightarrow v=-\frac{p}{3u}$,这其实相当于我们直接做了变换$y=u-\frac{p}{3u}$,我们得到$u^3+v^3+q=u^3-\frac{p^3}{27u^3}+q=0\Rightarrow(u^3)^2+qu^3-\frac{p^3}{27}=0$,解二次方程我们得到$u^3=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$,
$v^3=-\frac{p^3}{27u^3}=-\frac{q}{2}\mp\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$,注意到$u^3,v^3$其实是方程$X^2+qX-\frac{p^3}{27}=0$的两根,故$u$有6个解

$$\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}},\omega\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}},\omega^2\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}},\omega\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}},\omega^2\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

其中$\omega=e^{\frac{2\pi i}{3}}$是三次单位根,其相对应的$v$则是

$$\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}},\omega^2\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}},\omega\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}},\omega^2\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}},\omega\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$y=u-\frac{p}{3u}=u+v$相应为

$$\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$\omega\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\omega^2\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$\omega^2\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\omega\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$\omega\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\omega^2\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$\omega^2\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\omega\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

注意到后三个根与前三个根重复

而Cardano的学生Ferrari很快又发现了一元四次方程的解法

定理8.2 (Ferrari方法)**.** *一元四次方程$x^4+bx^3+cx^2+dx+e=0$的一般求解方法*
设$y=x+\dfrac{b}{4}$,不难发现有$y^4+py^2+qy+r=0\Rightarrow y^4=-py^2-qy-r$,希望将两边同时配方,考虑$(y^2+m)^2=y^4+2my^2+m^2=(2m-p)y^2+qy+(m^2-r)$,右边可以写作平方如果判别式$q^2-4(2m-p)(m^2-r)=0\Rightarrow m^3-\dfrac{p}{2}m^2-rm+\left(\dfrac{pr}{2}-\dfrac{q^2}{8}\right)=0$,而这是$m$的一元三次方程

接着Descartes，Euler也发现了其他三四次方程的解法，人们自然开始尝试解决一元五次方程，却始终未能成功，因此Lagrange系统研究总结了前人的方法:
假设一元二次方程$x^2+bx+c=0$两根分别为x_1,x_2,做变换$y=x+\dfrac{b}{2}$,我们知道$b=x_1+x_2$,故y相对应的两根为$y_1=\dfrac{x_1-x_2}{2}$, $y_2=\dfrac{x_2-x_1}{2}$
$y_1=\dfrac{x_1-x_2}{2}$被称为Lagrange预解式,虽然解x与解y都是解二次方程，但解y只需要开方
假设一元三次方程$y^3+py+q=0$的根为

$$y_1=\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$y_2=\omega\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\omega^2\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$y_3=\omega^2\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}+\omega\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}$$

那么u的6个解便恰好是

$$\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}=\frac{y_1+\omega y_3+\omega^2y_2}{3}$$

$$\omega\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}=\frac{y_2+\omega y_1+\omega^2y_3}{3}$$

$$\omega^2\sqrt[3]{-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}=\frac{y_3+\omega y_2+\omega^2y_1}{3}$$

$$\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}=\frac{y_1+\omega y_2+\omega^2y_3}{3}$$

$$\omega\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}=\frac{y_3+\omega y_1+\omega^2y_2}{3}$$

$$\omega^2\sqrt[3]{-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}}=\frac{y_2+\omega y_3+\omega^2y_1}{3}$$

注意到这正好是y_1,y_2,y_3的6个排列, u^3的两个解则分别为

$$-\frac{q}{2}+\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}=\left(\frac{y_1+\omega y_3+\omega^2y_2}{3}\right)^3$$

$$-\frac{q}{2}-\sqrt{-\frac{q^2}{4}+\frac{p^3}{27}}=\left(\frac{y_1+\omega y_2+\omega^2y_3}{3}\right)^3$$

它们在偶置换群$A_3=\{1,(123),(132)\}$下不变

$u=\dfrac{y_1+\omega y_3+\omega^2 y_2}{3}$被称为Lagrange预解式,即要求解$y_1,y_2,y_3$，可以预先求解$u$,而要求解$u$，可以预先求解$u^3$,然后开三次方,注意这里$u^3$相较$u$关于根的对称性更高，因为在$A_3$作用下不变,且在$S_3$作用下共有两个取值

可以认为三次方程的解法基本是先将F通过解二次方程（开平方）域扩张为$F(u^3)$,接着通过解三次方程(开三次方)将$F(u^3)$域扩张为$F(u)$,而$y_1,y_2,y_3\in F(u)$因为u是一个Galois预解式

Lagrange定义了一般的Lagrange预解式

定义8.3. 假设f是F上的多项式,根为$x_1,\cdots,x_n$,且F包含n次单位根ζ，定义**Lagrange预解式**为

$$\alpha=x_1+\zeta x_2+\zeta^2 x_3+\cdots+\zeta^{n-1}x_n$$

注8.4. 注意到

$$\begin{aligned}\zeta\alpha&=x_n+\zeta x_1+\zeta^2 x_2+\cdots+\zeta^{n-1}x_{n-1}\\ \zeta^2\alpha&=x_{n-1}+\zeta x_n+\zeta^2 x_1+\zeta^3 x_2+\cdots+\zeta^{n-1}x_{n-2}\\ &\cdots\\ \zeta^{n-1}\alpha&=x_2+\zeta x_3+\zeta^2 x_4+\cdots+\zeta^{n-1}x_1\end{aligned}$$

记S_n的轮换子群$G=\left\{1,(12\cdots n),(12\cdots n)^2,\cdots,(12\cdots n)^{n-1}\right\}$,那么$\zeta^k\alpha=(12\cdots n)^k\alpha$,故$\alpha^n=\alpha\cdot\zeta\alpha\cdots\zeta^{n-1}\alpha=\zeta^{\frac{n(n-1)}{2}}\alpha^n$,故当$n$为奇数时$\alpha^n$在$G$作用下不变,当$n$为偶数时$\alpha^{2n}$在$G$作用下不变, α是一个Galois预解式,故$x_1,\cdots,x_n\in F(\alpha)$，且$\alpha^n,\alpha^{2n}$关于根的对称性更高,而开方就能得到$\alpha$

Lagrange也注意到了解方程与方程根的对称性的关联，总结了Lagrange定理

Lagrange's theorem

定理8.5 (Lagrange定理)**.** *假设$x_1,\cdots,x_n$是方程$f(x)=0$不同的根,$u=u(x_1,\cdots,x_n)$, $v=v(x_1,\cdots,x_n)$分别是的有理函数表达式，那么如果S_n中使得u不变的置换也使得v不变，则v可以写成u的有理函数表达式*

如果S_n中使得u不变的置换在v作用可以得到k个值$v_1,\cdots,v_k$，则$v_1,\cdots,v_k$是一个以u的有理函数为系数的k次方程的解

证明. 我们假设$f(x)$是F上的多项式,记$K=F(x_1,\cdots,x_n)$,那么u,v是K中元素,我们知道$f(x)$在$F(u),F(v)$上的Galois群H_u,H_v满足$H_u\subseteq H_v$,故由Galois群的性质易知$v\in F(u)$,故v可以写成u的有理函数表达式

考虑方程$(x-v_1)\cdots(x-v_k)=0$ □

注8.6. 如果v可以写成u的有理函数表达式,那么显然S_n中使得u不变的置换也使得v不变

假设α是一个Lagrange预解式,依照定理来说，α^n,α^{2n}要比原方程根更好求解，然后再开方，我们便可以得到原方程的根

例子8.7. 求解四次方程$(x-x_1)(x-x_2)(x-x_3)(x-x_4)=0$

首先考虑预解式$x_1x_2+x_3x_4$,方程

$$(x-(x_1x_2+x_3x_4))(x-(x_1x_3+x_2x_4))(x-(x_1x_4+x_2x_3))=0$$

关于x_1,x_2,x_3,x_4对称,先解这个三次方程,接下来在考虑预解式x_1x_2,可以求解方程

$$0=(x-x_1x_2)(x-x_3x_4)=x^2-(x_1x_2+x_3x_4)x+x_1x_2x_3x_4$$

得到x_1x_2,x_3x_4,同理还可以解出$x_1x_3,x_1x_4,x_2x_3,x_2x_4$

再考虑预解式x_1+x_2,可以求解方程

$$0=(x-(x_1+x_2))(x-(x_3+x_4))=x^2-(x_1+x_2+x_3+x_4)x+(x_1x_3+x_2x_4)+(x_1x_4+x_2x_3)$$

得到x_1+x_2,x_3+x_4,同理还可以解出$x_1+x_3,x_1+x_4,x_2+x_3,x_2+x_4$

最终可以求解方程$(x-x_1)(x-x_2)=x^2-(x_1+x_2)x+x_1x_2$得到$x_1,x_2$,同理还可以解出$x_3,x_4$

可以看得出这里解方程便是通过一个不断降低预解式关于根的对称性的过程，直到解出答案

Lagrange对一元五次方程尝试了相同的方法，却未能获得成功，其实根本原因就是A_5是单群,考虑F上的一般一元五次方程$f(x)=(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)=0$, f在F上的Galois群是S_5，每次求解一个预解式其实都是在做根域扩张，即使是解二三四次方程也是不断做根域扩张，如果存在一个预解式$u=u(x_1,x_2,x_3,x_4,x_5)$可以通过多次开根求得，根据引理6.1，f在$F(u)$上的Galois群仍然是S_5或A_5,所以对根的置换也总使得u不变,即u关于根的对称性与那些已知量一样，根据定理8.5，这对解方程并没有帮助

索引