方程&根式的可解性

2024 年 4 月 5 日

目录

1 根的可解性 **2**

1.1 定义： 2

1.2 定义：根式可解 2

1.2.1 例子 2

2 用群论语言的叙述 **4**

2.1 定理 4

2.2 引理 4

2.3 引理 6

2.4 定理 6

2.5 定义：正规子群列和可解 7

2.6 定理： 8

2.7 定理：迦罗瓦 8

2.8 定理：阿贝尔-鲁费妮 9

现在，我们来用分裂域讨论多项式根的存在性公式。

1 根的可解性

1.1 定义：

型 m的纯扩张是扩张$k(u)/k$，其中$u^m \in k$对某个$m \geq 1$成立。而扩张K/k被称为根式扩张，若存在一个域的塔

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t = K$$

成立，每个K_{i+1}/K_i都是型m_i的纯扩张。这个扩张也被称为根式塔。

◦

每个次数为$[K : k] \leq 2$的域扩张K/k都是纯扩张。因为复数z可构作当且仅当其是多重二次的。那么就存在一个域的塔$\mathbb{Q}(i) = F_0 \subseteq \cdots \subseteq F_n$使得$z \in F_n$且$[F_i : F_{i-1}] \leq 2$对所有$i$成立，在后面，我们要来证明$\mathbb{Q}(i, z)$是根式扩张。

1.2 定义：根式可解

令$f(x) \in k[x]$的分裂域是E，我们说$f(x)$是根式可解的，若这里存在一根式扩张

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

使得$E \subseteq K_t$

1.2.1 例子

对每个$m \geq 1$和域k。我们来证明$f(x) = x^m - 1 \in k[x]$是根式可解的。回忆集合Γ_m的所有m次单位根在$f(x)$的分裂域E/k内是循环群。生成元ζ称为本原单位根。注意$\mid \Gamma \mid= m$，除非k是特征为$p > 0$且$p \mid m$。此时$\mid \Gamma_m \mid= m'$，其中$m = p^e m'$，且$p \nmid m'$。记$E = k(\zeta)$，所以E是k的纯扩张，并且E/k可以是一个根式扩张，注意E/k中的元素可以写为$a_0 + a_1\zeta + \cdots + a_{m-1}\zeta^{m-1}$的形式。容易得到$1, \zeta, \cdots, \zeta^{m-1}$是一组基。

二次根式

令$f(x)=x^2+bx+c\in\mathbb{Q}[x]$。定义$K_1=\mathbb{Q}(u)$，其中$u=\sqrt{b^2-4c}$。对$u^2\in\mathbb{Q}$，则$K_1$是根式扩张。这是因为$Q=K_0\subseteq K_1$是一个根式塔。更多的，该二次公式可以推出$K_1$是$f(x)$的分裂域，因此$f(x)$是根式可解的。

三次根式

令$f(X)=X^3+bX^2+cX+d\in\mathbb{Q}[x]$。令$X=x-\frac{1}{3}b$替换变量就得到新的多项式$f(\tilde{x})=x^3+qx+r\in\mathbb{Q}[x]$，新的多项式与原来的具有相同的分裂域。这是因为若$u$是$f(\tilde{x})$的根，则$u-\frac{1}{3}b$是$f(\tilde{x})$的根。

现在定义$K_1=\mathbb{Q}(\sqrt{D})$，其中$D=r^2+\frac{4}{27}q^3$。然后再定义$K_2=K_1(\alpha)$，其中$\alpha^3=\frac{1}{2}(-r+\sqrt{D})$。该三次方程证明了$K_2$包含$\tilde{f}(x)$的根$\alpha+\beta$，因为$\beta-q/3\alpha$。最后，定义$K_3=K_2(\omega)$，其中$\omega^3=1$。则我们得到了再上个章节讲的三个根。他们俩俩再$K_3$中。因此$E\subseteq K_3$

四次方程

令$f(x)=x^4+bx^3+cx^2+dx+c\in\mathbb{Q}[x]$，做变量替换$x=x-\frac{1}{4}b$，则我们得到新的多项式$\tilde{f}(x)=x^4+qx^2+rx+s\in\mathbb{Q}[x]$，更多的$f(x)$的分裂域也等于$\tilde{f}(x)$的分裂域，和上面一样若$u$是$\tilde{f}(x)$的根，容易得到$u-\frac{1}{4}b$也是$f(x)$的根。回想

$$\tilde{f}(x)=x^4+qx^2+rx+s=(x^2+jx+l)(x^2-jx+m)$$

所以j^2是一个三次方程的根，则我们可以得到一个式子

$$(j^2)^3+2q(j^2)^2+(q^2-4s)j^2-r^2$$

定义纯扩张

$$\mathbb{Q}=K_0\subseteq K_1\subseteq K_2\subseteq K_3$$

那么$j^2\in K_3$。只需要定义$K_4=K_3(j)$，就可以把系数l,m包含在K_4中。最后，定义$K_5=K_4(\sqrt{j^2-4l})$和$K_6=K_5(\sqrt{j^2-4m})$，则四次方程给出$E\subseteq K_6$

所以，我们看到二次到四次方程是根式可解的，反过来。如果$f(x)\in\mathbb{Q}[x]$是一个根式可解的多项式，则存在一个我们想得到的那种公式，他能用$f(x)$的系数表示出$f(x)$的根。设

$$Q=K_0\subseteq K_1\subseteq\cdots\subseteq K_t$$

是根式扩张使得$E \subseteq K_t$。令z是$f(x)$的根。有$K_t = K_{t-1}(u)$，其中u是$a \in K_{t-1}$的m次单位根。那么z就可以用u和K_{t-1}中的元素表示但$K_{t-1} = K_{t-2}(v)$，其中v的某次方幂属于K_{t-2}，因此z就可以用u, v以及K_{t-2}中的元素表示。一直循环下去最终我们可以找到一个类似于经典公式的公式表示。

2 用群论语言的叙述

这个阶段我们来研究$f(x)$的根式可解性对它的迦罗瓦群的影响。

设$k(u)/k$是型6的纯扩张，那么$u^6 \in k$。那么就有型2的纯扩张$k(u^3)/k$，这是因为$(u^3)^2 = u^6 \in k$。而$k(u)/k(u^3)$是型为3的纯扩张。那么$k(u)/k$可以被重写为型2和3的纯扩张塔$k \subseteq k(u^3) \subseteq k(u)$。一般来书，我们可以假设，给定一个纯扩张的塔，其中的每个域关于它的前一个域的扩张是素数型的。例如，若$k \subseteq k(u)$是型m的，其中$m = p_1 \cdots p_q$，且p_i是素数。那么我们就可以做塔的替换有

$$k \subseteq k(u^{m/p_1}) \subseteq k(u^{m/p_1 p_2}) \subseteq \cdots \subseteq k(u)$$

在下一个定理，我们将得到一个关键的结论。它告诉我们如何将根式可解转化为迦罗瓦群的语言。并告诉我们正规扩张一词是怎么来的。

2.1 定理

令$k \subseteq K \subseteq E$是域的塔，其中$K/k$和$E/k$是正规扩张。则$\mathrm{Gal}(E/K)$是$\mathrm{Gal}(E/k)$的正规子群，且

$$\mathrm{Gal}(E/k)/\mathrm{Gal}(E/K) \cong \mathrm{Gal}(K/k)$$

证明： 由于K/k是正规扩张，那么它就是某个多项式$f(x) \in k[x]$的分裂域。因此若$\sigma \in \mathrm{Gal}(E/k)$，则$\sigma(K) = K$成立。我们定义$\rho : \mathrm{Gal}(E/k) \to \mathrm{Gal}(K/k)$由$\sigma \to \sigma \mid K$给出。容易得到$\rho$是一个同态，且$\ker \rho = \mathrm{Gal}(E/K)$，那么他就是一个正规子群。其次，$\rho$是一个满射，若$\tau \in \mathrm{Gal}(K/k)$，我们可以知道有一个拓展$\tau$的$\sigma \in \mathrm{Gal}(E/k)$，即$\rho(\sigma) = \sigma \mid K = \tau$，再利用第一同构定理我们就完成证明。

2.2 引理

令B是域k的有限扩张，则

1. 这里有个有限扩张F/B使得F/k是正规扩张
2. 若B是k的根式扩张，则这里存在域的塔$k \subseteq B \subseteq F$使得$F/k$是正规扩张也是根式扩张。更多的，在$F/k$的根式塔中出现的纯扩张的型的集合与在$B/k$的根式塔的型的集合是相同的。

证明： 由于B是有限扩张，则对每个i有$B = k(z_1, \cdots, z_l)$，有z_i是某个不可约多项式$p(x) \in k[x]$的根。定义$f(x) = p_1(x) \cdots p_l(x) \in k[x] \subseteq B[x]$。在定义$F$是$f(x)$在$B$上的分裂域。由于$f(x) \in k[x]$，我们有$F/k$是$k$上的分裂域。则$F/k$是正规扩张。

证明2： 现在，定义

$$F = k(z_1, z_1'.z_1'', \cdots; z_2, z_2', z_2'', \cdots; \cdots; z_l, z_l', \cdots)$$

其中$z_i, z_i', \cdots$是$p_i(x)$的根。我们说

$$F = k(\{\sigma(z_1), \cdots, \sigma(z_l) : \sigma \in \mathrm{Gal}(F/k)\})$$

则要来证明F被等号右边的记号包含，因为k的扩域被F包含是明显的。实际上，这足以证明$z_i' = \sigma(z_i)$。注意这里存在固定k的同构$\gamma : k(z_i) \to k(z_i')$且$z_i$映射到$z_i'$。且每个$\gamma$都是扩张$\sigma \in \mathrm{Gal}(F/k)$来的。因此$z_i' = \sigma(z_i)$.

由于B是k的根式扩张，这这里有$u_1, \cdots, u_t \in B$和根式塔

$$k \subseteq k(u_1) \subseteq k(u_1, u_2) \subseteq \cdots \subseteq k(u_1, \cdots, u_t) = B$$

其中$k(u_1, \cdots, u_{i+1})$都是$k(u_1, \cdots, u_i)$的纯扩张。我们现在证明F是k的根式塔。令$\mathrm{Gal}(F/k) = \{1 = \sigma_1, \sigma_2, \cdots, \sigma_n\}$。定义

$$B_1 = k(u_1, \sigma_2(u_1), \cdots \sigma_n(u_1))$$

则存在根式塔

$$B_1 \subseteq B_1(u_2) \subseteq B_1(u_1, \sigma_1(u_2)) \subseteq B_1(u_1, \sigma_1(u_2), \cdots, \sigma_n(u_2)) \subseteq \cdots \subseteq B_2$$

所以B_2是B_1的根式扩张。若$\sigma_j(u_2^q) = \sigma_j(u_2)^q \in \sigma_j(B_1) \subseteq B_1 \subseteq B_1(u_2, \sigma(u_2) \cdots \sigma_{j-1}(u_2))$，那么他们的型是一样的，因为同构给出他们的型就是q。因为B_1是k的根式扩张，我们在B_1添加元素可以得到B_2也是B_1的一个根式扩张，所以B_2是k的根式扩域。对每个$i \geq 2$，我们对B_{i+1}是B_i通过添加$u_1, \sigma_1(u_1), \cdots, \cdots$得到的。那么$B_{i+1}$其实也是$k$的一个根式扩张。由定义，$F = B_i$，那么我们证明$F$是$k$上的一个根式扩张，且是单纯扩张的型论断也成立。

2.3 引理

令$k(u)/k$是素型p的纯扩张，且与k的特征不同，若k包含p次单位根且$u \notin k$，则$\mathrm{Gal(k(u)/k)} \cong \mathbb{I}_p$

证明： 用G作为$\mathrm{Gal}(k(u)/k)$的记号。令$a = u^p \in k$。若ω是p次单位根，则根$1, \omega, \cdots, \omega^{p-1}$是互异的。因此，$f(x) = x^p - a$的根是$u, \omega u, \cdots, \omega^{p-1}u$。由于$\omega \in k$，可以推出$k(u)$是$k$上$f(x)$的一个分裂域。若$\sigma \in G$，则$\sigma(u) = \omega^i u$对某个$i$成立。那么我们定义$\varphi : G \to \mathbb{I}_p$由函数$\varphi(\sigma) = [i]$给出。$[i]$是$i \bmod p$的同余类。容易验证$\varphi$是一个同态。设$\tau \in G$和$\varphi(\tau) = [j]$。则$\sigma\tau(u) = \sigma(\omega^j u) = \omega^{i+j}u$，因此$\varphi(\sigma\tau) = [i+j] = [i]+[j] = \varphi(\sigma)+\varphi(\tau)$。现在$\ker \varphi = \{1\}$。若$\varphi(\sigma) = [0]$，则$\sigma(u) = u$。由于$\sigma$固定$k$，利用一开始的定义，则$\sigma = 1$。最后，我们来证明$\varphi$是满射，因为$u \notin k$。则自同构使得$u \to \omega u$不是恒等映射。因此$\mathrm{im}\varphi \notin \{[0]\}$。但$\mathbb{I}_p$的阶为$p$，除了自身和$\{[0]\}$之外没有子群。因此$\mathrm{im}\varphi = \mathbb{I}_p$。所以$\varphi$是同构.

2.4 定理

令$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$是$k$的根式扩张。设对每个$i$，则每个$K_i$是在$K_{i-1}$上型$p_i$的纯扩张，其中$p_i \neq char(k)$，并且$k$包含所有的$p_i$次单位根。

1. 若K_i是k上的分裂域，则这里存在一子群的序列

$$\mathrm{Gal}(K_t/k) = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_t = \{1\}$$

   其中每个G_{i+1}都是G_i的正规子群。并且使得G_i/G_{i+1}是循环的素数阶群。

2. 若$f(x)$是根式可解的，则它的迦罗瓦群$\mathrm{Gal}(E/k)$是可解群的商群。

证明： 我们定义$G_i = \mathrm{Gal}(K_t/K_i)$给出$\mathrm{Gal}(K_t/k)$的子群序列。由于$K_1 = k(u)$，其中$u^{p_i} \in k$。我们设$k$包含所有$p$次单位根以便证明$K_1$是$x^{p_1} - u^{p_1}$的分裂域。利用引理2.1，则$G_0 = \mathrm{Gal}(K_t/k)$，得到$G_0/G_1 \cong \mathrm{Gal}(K_t/K_1)$是$G_0$的正规子群。以此类推我们重复上述过程就得到了要证明的东西，其次每个$G_0/G_1 \cong \mathbb{I}_{p_i}$。我们就证明完毕了。

证明2： 若$f(x)$根式可解，那么存在一个根式塔

$$k=K_0\subseteq K_1\subseteq\cdots\subseteq K_t$$

其中每个K_i/K_{i+1}是素型的纯扩张，且使得$E\subseteq K_t$。利用引理2.2，我们可以扩充这个塔，变成这个样子：

$$k=K_0\subseteq K_1\subseteq\cdots\subseteq K_t\subseteq\cdots\subseteq F$$

使得F/k是正规扩张（实际上和原来的一样，只是我们做了点延长）利用命题1，k包含所有的单位根表明了$\mathrm{Gal}(F/k)$是可解群。

其次，若E是分裂域，且$\sigma\in\mathrm{Gal}(F/k)$，则做限制$\sigma\mid E\in\mathrm{Gal}(E/k)$。由于$F$也是分裂域，我们可以把每个限制$\sigma\mid E$做拓展变成某个$\sigma\in\mathrm{Gal}(F/k)$，只需要定义$\rho:\sigma\to\sigma\mid E$即可，这是一个满射。

2.5 定义：正规子群列和可解

群G的正规子群列指的是如下形式的子群列

$$G=G_0\geq G_1\geq G_2\geq\cdots\geq G_t=\{1\}$$

其中G_{i+1}是G_i的正规子群；此子群列的商群如下：

$$G_0/G_1,G_1/G_2,\cdots.G_{t-1}/G_t$$

有限群G称为可解群，若$G=\{1\}$或者G有一个使得每个商群阶均为素数的正规子群列

现在我们重新翻译定理2.4，它是在说，$\mathrm{Gal}(K_t/k)$是可解群当K_t是k的根式扩张且k包含一些适当的单位根。

例子： 考虑子群列

$$S_4\geq A_4\geq V\geq W\geq\{1\}$$

其中V是一个4元素群，且W是V的任意二阶群。这是一个正规列，首先，它从S_4开始，结束于$\{1\}$。其次，每个其中的元素都是上一个元素的正规子群：$A_4\lhd S_4,V\lhd A_4,W\lhd V$。因为$V$是阿贝尔群，现在不妨计算一下他们的阶，$\mid S_4/A_4\mid=24/12=2$，$\mid A_4/V\mid=12/4=3$，$\mid V/W\mid=4/2=2$。因此每个商群都是素数阶，那么$S_4$是可解的。

2.6 定理：

每个可解群G的商群本身就是可解群

注意： 我们也可以证明可解群的每个子群都是可解的。

证明： 利用群的第一同构定理，商群和其同态的像同构。因此，我们只需要证明函数$f : G \to H$中，f是满射即可。则H就是可解群。

令$G = G_0 \geq G_1 \geq \cdots \geq G_t = \{1\}$是定义中可解的子群列。那么

$$H = f(G_0) \geq f(G_1) \geq \cdots \geq f(G_t) = \{1\}$$

是H的子群列。若$f(x_{i+1}) \in f(G_{i+1})$且$u_i \in f(G_i)$，那么$u_i f(x_{i+1}) u_i^{-1} = f(x_i)f(x_{i+1})f(x_i)^{-1} = f(x_i x_{i+1} x_i^{-1}) \in f(G_i)$。因为$G_{i+1} \lhd G_i$，那么$f(G_{i+1})$就是$f(G_i)$的正规子群。由$x \to f(x_i)f(G_{i+1})$定义的函数$\varphi : G_i \to f(G_i)/f(G_{i+1})$是一个满射，因为它是满射$G_i \to f(G_i)$和自然映射$f(G_i) \to f(G_i)/f(G_{i+1})$的复合。所以$G_{i+1} \leq \ker \varphi$，该映射诱导了一个满射同态

$$G_i/G_{i+1} \to f(G_i)/f(G_{i+1})$$

也就是$x_i G_{i+1} \to f(x_i)f(G_{i+1})$。其中$G_i/G_{i+1}$为素数阶循环群可知其映射得到的商群也是素数阶的或者1阶的，重复上述过程就可以得到所有商群都是素数阶的，H是可解的。

2.7 定理：迦罗瓦

设k是一个域，$f(x) \in k[x]$，若k包含了全部p次单位根，则$f(x)$是根式可解的，它的迦罗瓦群$\mathrm{Gal}(E/k)$是一个可解群。

证明： 利用定理2.4，迦罗瓦群是某个可解群的商群。其次，利用定理2.6我们知道，可解群G的商群本身是可解群。

若特征为0，则上面的定理的逆也成立，但是当p为特征时，逆是不对的。例如$f(x) = x^p - x - t \in k[x]$，其中$k = F_p(t)$，则$f(x)$在$k$上的迦罗瓦群是$p$阶循环群，但它不是根式可解的。

若$f(x)$的次数为n，则它的迦罗瓦群同构于一个S_n的群。为此利用刚才的例子，我们知道S_2, S_3, S_4是可解的可以得到$f(x) \leq 4$都是可解的。也就是说二三、次四次多项式的迦罗瓦群是可解群。利用迦罗瓦定理，若特征为0，则他们是根式可解的。

2.8 定理：阿贝尔-鲁费妮

对所有$n \geq 5$，一般n次多项式

$$f(x) = (x - y_1)(x - y_2) \cdots (x - y_0)$$

是根式不可解的。

证明： 若F是一个域，其中$E = F(y_1, \cdots, y_n)$是在n个变量中所有有理函数组成的域，其中系数在F中。且设$k = F(a_0, \cdots, a_n)$，其中a_i是$f(x0)$的系数。则E是$f(x)$在k上的分裂域。若我们选择$F = C$，则它包含所有单位方根。我们断言，S_n同构$\mathrm{Gal}(E/k)$的一个子群。其次，若A, R是整环，$\varphi : A \to R$是同构，则商环$a/b \to \varphi(a)/\varphi(b)$是$\mathrm{Farc}(A) \to \mathrm{Frac}(R)$的同构映射。其次，我们可以把一个整环$R$的自同构扩张为$\mathrm{Frac}(A)$的自同构。特别的$\tilde{\sigma}$可以拓展为$E = \mathrm{Frac}(C[y_1, \cdots, y_n])$的一个自同构$\sigma^*$。因此$\sigma^* \in \mathrm{Gal}(E/k)$。那么映射$\sigma \to \sigma^*$可以看得出是一个单射，那么有$n! \leq| \mathrm{Gal}(E/k) |$，其次，逆也是成立的，因为迦罗瓦群同构于$S_n$的一个群。因此$n! =| \mathrm{Gal}(E/k) |$且$\mathrm{Gal}(E/k)$同构于$S_n$，当$n \geq 5$时，它的商群不是素数阶，所以不可解。利用定理迦罗瓦可知当$n \geq 5$时，不存在根式可解的多项式$f(x)$出现，因此是根式不可解的。