广义五次方程的不可解性

若$f(x)\in k[x]$是首一多项式，其中k是包含其根$z_1,z_2,\cdots,z_n$作为元素的域，则

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=(x-z_1)\cdots(x-z_n)$$

我们对如下命题进行推广和证明：

练习 1. 设$f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n\in k[x]$，其中$k$是域，并假设$f(x)=(x-r_1)(x-r_2)\cdots(x-r_n)\in E[x]$，其中$E$是包含$k$的域，证明：

$$a_{n-1}=-(r_1+r_2+\cdots+r_n)\text{和}a_0=(-1)^nr_1r_2\cdots r_n$$

并以此得到$f(x)$所有根的和，积都在k中。

证明. 不妨对$n\geq 1$进行归纳。当$n=1$时，$f(x)=x+a_0=(x-a_0)$，基础步骤成立。现在假设对$n-1$成立，那么设$f(x)=a_0+a_2+\cdots+a_{n-2}x^{n-2}+x^{n-1}=(x-r_1)(x-r_2)\cdots(x-r_{n-1})$。则我们要证明的是$(x-r_n)f(x)$成立由归纳假设，现在我们知道$a_{n-2}=-(r_1+\cdots+r_{n-1})$，且 $a_0=(-1)^nr_1\cdots r_{n-1}$。那么$(x-r_n)f(x)$ 中的a_{n-1}项是$-(x-r_n)(r_1+\cdots+r_{n-1})x^{n-2}+(x-r_n)x^{n-1}$，提取出其中的$x^{n-1}$项带有的系数，正是$a_{n-1}=-(r_1+r_2+\cdots+r_n)$。同样的方法能够证明$a_0$。不做过多叙述。因此，由于系数在$k$中，且是根的和与积，所以$k$对根的和、积运算封闭。 □

由上述习题，我们可以得到的事实就是：

$$\begin{aligned}
a_{n-1} &= -\sum_i z_i \\
a_{n-2} &= \sum_{i<j} z_iz_j \\
&\vdots \\
a_0 &= (-1)^n z_1z_2\cdots z_n
\end{aligned} \tag{1}$$

其中$-a_{n-1}$是所有根的和，且a_0是所有根的乘积。给定$f(x)$的系数，则我们可以找到他的根，因此，给定a，我们是否能够解出带有n个变量的n个方程组(1)？若$n=2$，我们的回答是“可以的”若$n=3,4$，勉强可以。但$n\geq 5$，我们会看到没有类似的解存在。

注意的是，我们不是说不存在解，而是说不存在像一开始所谓的“经典公式”这种形状的解。

让我们稍微的回忆前几章的一些定义和命题，若k是一个域K的子域，则K是k的一个扩张，简记为:K/k。若K/k是一个扩展，则K可以视为k上的向量空间，我们说K是有闲扩张，若K是k上的有限向量空间，则K的维度记为$[K:k]$，是K/k的次数。

例 1. 令$p(x)\in k[x]$是n次不可约多项式，其中k是域，再令$k(z)/k$是通过添加$p(x)$的根z得到的扩张，则$k(z)$的每个元素都有形如$b_0+b_1z+\cdots+b_{n-1}z^{n-1}$的表示，其中$b_i\in k$，因此，表$1,z,z^2,\cdots,z^{n-1}$是$k(z)/k$中的基，且$\dim(k(z))=n=\deg(p)$

定理 2. 令$k\subseteq K\subseteq E$是域，其中K是k的有限扩张，且E是K的有限扩张。我们有

$$[E:k]=[E:K][K:k]$$

定义（正规扩张） 3. 设K/k是扩张，且$z\in K$。我们说z是k上的代数元，若存在以z为根的非零多项式$f(x)\in k[x]$。否则z是k上的超越元。

定义（正规扩张） 4. 令k是K的子域和令$\{z_1,\cdots,z_n\}$是K的子集。通过添加$z_1,\cdots,z_n$到k作为K的子域，记为$k(z_1,\cdots,z_n)$。是K包含k和$z_1,\cdots,z_n$的子域的交。

命题 5. 若K/k是一个有限扩张，则每个$z\in K$是k中的代数元，反之，若$K=k(z_1,\cdots,z_n)$且对每个z_i是k上的代数元，则K/k是一个有限扩张。

定义（正规扩张） 6. 令k是K的子域，再令$f(x)\in k[x]$，我们说$f(x)$在K上分裂，这是在说：

$$f(x)=a(x-z_1)\cdots(x-z_n)$$

其中$z_1,\cdots,z_n$在K中且$a\in k$非零。

一个扩张E/k称为$f(x)$的分裂域，当且$f(x)$在E上分裂，但$f(x)$不在E的任何真子域中分裂、

命题 7. 若$f(x)\in k[x]$，其中k是域，则$f(x)$的分裂域E/k存在。

证明. 由克罗内克定理，这里存在某个域扩张K/k使得$f(x)=a(x-z_1)\cdots(x-z_n)$在$K[x]$中。

若我们定义$E=k(z_1,\cdots,z_n)$，其中$z_1,\cdots,z_n$是$f(x)$的根。则$f(x)$在E中分裂。若$B\subsetneq E$是E的真子域，则$z_i\notin B$对某个i成立。那么$f(x)$就不在B中分裂，因此E是$f(x)$的分裂域、 □

定义（自同构） 8. 我们设E是包含k作为子域的域，E的自同构指的是同构映射$\boldsymbol{\sigma}: E\rightarrow E$。我们说$\sigma$固定$k$当且$\sigma(a)=a$对每个$a\in k$成立。

注记 9. 若E/k是域扩张，则E是k上的向量空间。若$\sigma: E\rightarrow E$是固定k的自同构，则σ是一个线性变换。不妨说的更清楚点，注意$z,z'\in E$有$\sigma(z+z')=\sigma(z)+\sigma(z')$。但$\sigma$也对乘法保留，若a∈ k，则

$$\sigma(\mathrm{az})=\sigma(a)\sigma(z)=a\sigma(z)$$

这是因为，σ固定k

命题 10. 令k是K的子域，设

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in k[x]$$

再设$E=k(z_1,\cdots,z_n)$是分裂域，若$\sigma: E\rightarrow E$是固定k的自同构，则σ是f(x)的根$z_1,\cdots,z_n$上的置换。

证明. 若z是$f(x)$的根，那么

$$0=f(z)=z^n+\cdots+a_1z+a_0$$

应用σ在$f(x)$上我们有

$$0\ =\ \sigma(z)^n+\cdots+a\sigma(z)+a_0$$

因为σ固定k，那么$f(x)$的根也是$\sigma(z)$。若Z是所有根的集合，则σ': $Z\to Z$，其中σ'做了限制$\sigma|\, Z$。但σ'是单射，由鸽笼原理，单射+有限元素等价于满射和双射。因此σ是一个置换。 $\square$

推论 11. 令$k\subseteq B\subseteq F$是域的塔，其中B是某个多项式$f(x)\in k[x]$的分裂域。若σ: $F\to F$是固定k的自同构，则$\sigma(B)=B$

证明. 由命题10，σ是关于f(x)根的一个置换，那么$\sigma(B)\subseteq B$作为k上的线性空间。由于$[B{:}\,k]<\infty$，且$B\cong\sigma(B)$，那么这俩都是有限扩域，且$\dim(B)=\dim(\sigma(B))$，那么B =σ(B) $\square$

命题 12. 令$E=k(z_{1,}\cdots,z_n)$。若σ: $E\to E$是固定k的自同构且如果$\sigma(z_i)=z_i$，则σ是恒等变换。

证明. 我们对$n\geq 1$进行归纳来证明，若$n=1$，则每个$u\in E$都形如$f(z_1)\,/\,g(z_1)$，其中$f,g\in k[x]$

由于σ固定每个z_1，也固定多项式的系数，因此σ固定所有的$u\in E$.

现在，我们记$K=k(z_1\cdots,z_{n-1})$，并记$E=K(z_n)$。只需要重复$n=1$的情况即可证明。 $\square$

定义（迦罗瓦群） 13. 令E是包含k作为子域的域。 一个E在k上的迦罗瓦群记为$\mathrm{Gal}(E/k)$是E中所有固定k的自同构构成的集合。若$f(x)\in k[x]$，且$E=k(z_{1,}\cdots,z_n)$是分裂域，则$f(x)$在k上的迦罗瓦群规定为$\mathrm{Gal}(E/k)$

若$f(x)=x^2+1\in\mathbb{Q}[x]$，则其复共轭$\sigma$是其分裂域$\mathbb{Q}[i]$的自同构，其固定$\mathbb{Q}$，因为自同构只是在交换$i,-i$， 因此$\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q})$是置换群$S_2$的子群。 它的阶为2， 藉此推导出$\mathrm{Gal}(E/k)=\langle\sigma\rangle\cong\mathbb{I}_2$。我们应当将$\mathrm{Gal}(E/k)$视为复共轭的推广。

定理 14. 若$f(x)\in k[x]$是n次的，则其迦罗瓦群Gal(E/k)同构于S_n的一个子群。

证明. 令E/k是$f(x)$在k上的分裂域， 令$X=\{z_1,\cdots,z_n\}$是$f(x)$在E中的所有根的集合。若$\sigma\in\mathrm{Gal}(E/k)$， 则跟命题10证明一样， 我们依然对映射做限制$\sigma|\,X$。 它是$X$的置换； 因此σ|X∈$S_X$。定义映射$\varphi$: $\mathrm{Gal}(E/k)\to S_X$由φ: $\sigma\to\sigma|\,X$决定。为了证明φ是同态。注意$\varphi(\sigma\tau)$和$\varphi(\sigma)\varphi(\tau)$都是$X\to X$的函数。因此，如果他们对每个$z_i$的作用一致，那么它们就是相等的。这很容易证明，对任意$z_i\in X$，有$\varphi(\sigma\tau)$: $z_i\to(\sigma\tau)(z_i)=\varphi(\sigma)\varphi(\tau)$: z_i。

φ的像是$S_X\cong S_m$的一个子群，其中$m=|\,X|\leq n$，若$f(x)$有重根，则$m<n$。φ的核由所有X上的恒等置换构成，即σ固定每一个根z_i，利用命题12，而且迦罗瓦群规定其元素σ固定k。因此$\ker\varphi=\{1\}$，因此φ是一个单射，那么$\mathrm{Gal}(E/k)$同构于S_m的一个子群。另一种情况，若$m=n$则直接证明完毕。其次，若有重根，注意S_m是S_n的子群。我们有S_m同构于固定$m+1,\cdots,n$的所有置换构成的子群，因此$f(x)$有重根，定理也是成立的。 $\square$

我们现在来比较给定域k上不同多项式的分裂域。$f(x)\in k[x]$的分裂域E的定义是由某些扩域K/k给出的，其中$f(x)$是某些线性因子的乘积。但是，若K一开始就没给出来会怎么样？例如，设$k=\mathbb{C}(x)$和$f(y)=y^2-x$，或者$k=\mathbb{F}_3$和$f(x)=x^9-x\in\mathbb{F}_3[x]$。由克罗内克定理，它给出一个$\mathbb{C}(x)/\mathbb{C}$包含$\sqrt{x}$的域扩张，且给出包含所有$f(x)$的域扩张$K/\mathbb{F}_3$。但这些域扩张并不是唯一的。接下来我们要来讲一下，在同构上看来，分裂域并不依赖扩域K的选择。

下一个结论，我们来构造$\mathrm{Gal}(E/k)$中的自同构，并且计算当k特征为0时他们的数量，首先回忆定理

定理. 若R,S是交换环，且$\varphi\colon R\to S$是同态，则

$$\varphi^*\colon f(x)=r_0+r_1x+\cdots\mapsto\varphi(r_0)+\varphi(r_1)x+\cdots=f^*(x)$$

命题 15. 令$f(x)\in k[x]$，再令E是$f(x)$在k上的分裂域。设$\varphi\colon k\to k'$是一个域同构。设$\varphi^*\colon k[x]\to k'[x]$是上述定理给出的同构$g(x)\mapsto g^*(x)$且$E'$为$f^*(x)$在$k'$的分裂域，则

1. 存在一个扩张φ的同构$\Phi\colon E\to E'$

$$\begin{tikzcd} E \arrow[r, dashed, "\Phi"] \arrow[d, dash] & E' \arrow[d, dash] \\ k \arrow[r, "\varphi"'] & k' \end{tikzcd}$$

2. 若k特征为0，则正好有$[E:k]$个扩张φ的同构$\Phi\colon E\to E'$

证明. 我们通过对$[E:k]$归纳进行证明。若$[E:K]=1$，则$f(x)$是$k[x]$中一些线性因子的乘积，并且这也比较简单的看出$f^*(x)$也是$k'[x]$中的线性因子的乘积，因此。我们可以设$\Phi=\varphi$

接着，对归纳步骤，我们选择在E中 $f(x)$的根z，并令$p(x)$是$k[x]$中的不可约多项式，且以z为根。由于$z\notin k$，则$\deg(p)>1$。更多的，若$[k(z):k]=\deg(p)$，令$p^*(x)\in k'[x]$是对应的多项式。并用z作为其在E'中的根。注意该多项式不可约，因为$k[x]\to k'[x]$是一个同构。

接着我们引入一个习题：

练习 2. 设$\varphi\colon k\to k'$是域之间的同构，E/k和E'/k'是扩张。$p(x)\in k[x]$和$p^*(x)$都是不可约多项式，并设$z\in E$和$z'\in E'$是两个多项式的根，则存在一个同构$\tilde{\varphi}\colon k(z)\to k'(z')$，满足$\tilde{\varphi}(z)=z'$以及$\tilde{\varphi}$扩张了$\varphi$

$$\begin{tikzcd} k(z) \arrow[r, dashed, "\tilde{\varphi}"] \arrow[d, dash] & k'(z') \arrow[d, dash] \\ k \arrow[r, "\varphi"'] & k' \end{tikzcd}$$

解答. 设同态$\tilde{\varphi}\colon k(z)\to k'(z')$由函数$\tilde{\varphi}(z)=z'$定义。由于$p(x)$和$p^*(x)$都以$z,z'$作为不可约多项式。那么这里存在一个同构

$$f\colon k[x]/(p(x))\to k(z)\text{和}f\colon k'[x]/(p^*(x))\to k'(z')$$

满足$f(x+(p(x))=z$和对所有的$a\in k$都有$\varphi(a)=a$，并且对另一个映射有同样的效果。而$p(x)=\sum a_ix^i$，由φ有$p^*(x)=\sum\varphi(a_i)x^i$。现在剩下一个问题，我们只需要有$k[x]/(p(x))\to k'[x]/p^*(x)$是同构就证明完毕了。

它俩的同态核是p和p^*。那么对同态$k[x]/(p(x))\to k'[x]/p^*(x)$，我们只需要把$k[x]/(p(x))$中的元素$x+(p(x))$映射到$x+(p^*(x))$即可。这是一个满射的同态，因此是同构。再由同构$f$即可得到我们要证明的东西。

那么我们就得到一个扩张了φ的同构$\tilde{\varphi}\colon k(z)\to k'(z')$使得$\tilde{\varphi}(z)=z'$。我们现在把$f(x)$看做$k(z)$中的多项式。由归纳假设有$E$是$f(x)$在$k(z)$上的分裂域，那么我们证明有

$$E=k(z)(z_1,\cdots,z_n)$$

其中$z_1,\cdots z_n$是$f(x)$的根。显然

$$E=k(z_1,\cdots,z_n)\subseteq k(z)(z_1,\cdots,z_n)$$

对于反包含，由于$z\in E$，则

$$k(z)(z_1,\cdots,z_n)\subseteq k(z_1,\cdots,z_n)=E$$

由于$[E{:}k(z)]<[E{:}k]$，由归纳假设，同构$\tilde{\varphi}{:}k(z)\to k'(z')$使得$\tilde{\varphi}(z)=z'$就存在一个同构$\Phi{:}E\to E'$，它是$\tilde{\varphi}$的拓展。从而是$\varphi$的拓展[1] □

证明2. 这部分的证明又是对$[E{:}k]$做归纳，若$[E{:}k]=1$，$E=k$成立，则这里只存在一个唯一的扩张。因此，$\Phi=\varphi$。若$[E{:}k]>1$，令$f(x)=p(x)g(x)\in k[x]$。其中$p(x)$是最大次数不可约多项式，记为d。我们可以假设$d>1$。否则$f(x)$在k上分裂并且$[E{:}k]=1$。

选择$p(x)$的根$z\in E$。由第一部分，多项式$p^*(x)\in k'[x]$不可约，存在某个$z'\in E'$做为$p^*(x)$的根。现在，由于k的特征为0。注意，特征为0的不可约多项式无重根，那么p,p^*都是无重根的多项式。因此他们都有d个互异的根。由命题1中的习题，存在d个同构$\tilde{\varphi}{:}\,k(z)\to k'(z')$扩张$\varphi$。对其中每个扩张，他都必须把$z$映射到某个$z'$。所以，命题12表明了他就是众多$\tilde{\varphi}$中的某个。现在，和命题1一样，$E$就是$f(x)$在$k(z)$上的分裂域，而$E'$看做是$f^*(x)$在$k'(z')$上的分裂域。由于$[E{:}k]=[E{:}\,k(z)][k(z):k]=[E'{:}\,k(z)]d$。那么$[E{:}\,k(z)]<[E{:}\,k]$。由归纳假设，每个$\tilde{\varphi}$都恰好有$[E{:}\,k(z)]$个扩张，因此$[E{:}\,k(z)][k(z):k]=[E{:}\,k]$个扩张恰好就是所有扩张的数量。 □

定理 16. 若k是域且$f(x)\in k[x]$，则任意两个$f(x)$在k上的分裂域是同构的。

证明. 令E,E'是$f(x)$在k上的分裂域。取φ是恒等恒等置换，则利用定理15的命题1，就证明完毕。 □

推论 17. 具有E作为分裂域的多项式$f(x)\in k[x]$的迦罗瓦群只依赖k和$f(x)$的选择，而不依赖域E的选择。

证明. 若$\varphi{:}E\to E'$是固定k的同构，则$\varphi\sigma\varphi^{-1}$是一个在E'的同构复合。只需要定义$\mathrm{Gal}(E/k)\to\mathrm{Gal}(E'/k)$由函数$o\rightarrowtail\varphi\sigma\varphi^{-1}$即可。 □

推论(E.H.Moore) 18. 任意两个拥有p^n个元素的有限域是同构的。

证明. 若E是有$q=p^n$个元素的域，则我们由拉格朗日定理可知其乘法群$E^\times$对每个$a\in E^\times$都有$a^{q-1}=1$。由此可见，每个E中的元素，再加上0，是方程$f(x)=x^q-x=x(x^{q-1}-1)\in F_p[x]$上的根。利用迦罗瓦定理，这里就存在一个$f(x)$在$F_p$上分裂的分裂域$E$ □

若$h(x),g(x)\in F_p$是n次不可约多项式，则我们可以得到一个同构$F_p[x]/g(x)\cong F_p[x]/h(x)$。这是因为两个域都是存在$p^n$个元素的。

现在我们来计算特征为0的域k的迦罗瓦群$\mathrm{Gal}(E/k)$阶数。

定理 19. 若E/k是某个多项式$k[x]$的分裂域，其中k是特征为0的域，则$|\mathrm{Gal}(E/k)|=[E{:}k]$

证明. 令$k=k'$，$E=E'$，还有$\varphi=1_k$。将他们带入命题15的第二个小命题中。那么刚刚好存在$[E{:}k]$个到自身的自同构，这些自同构构成其迦罗瓦群的数量$|\mathrm{Gal}(E/k)|$ □

推论 20. 令$f(x)\in k[x]$是n次不可约多项式，其中k是特征为0的域。若E/k是$f(x)$在k上的分裂域，则n是$|\mathrm{Gal}(E/k)|$的因子

1. 上面习题的证明有一个非常漂亮的结论，但我不想写。

证明. 若$z\in E$是$f(x)$的根， 则对于每个$k(z)$中的元素， 都可以唯一的表示为$a_0+a_1z+\cdots+a_{n-1}z^{n-1}$， 因此这就是$k(z)$中的一组基， 则$[k(z):k]=n$。 但$[E:k]=[E:k(z)][k(z):k]$。 所以$n|[E:k]$。由定理19，它给出$[E:k]=|\mathrm{Gal}(E/k)|$ $\square$

若k是域，则其在$k[x]$中的不可约多项式可以随着域k的扩大而改变

引理 21. 令B/k是某个多项式$g(x)\in k[x]$的分裂域。若$p(x)\in k[x]$不可约，且如果

$$p(x)=q_1(x)\cdots q_t(x)$$

是$p(x)$在$B[x]$中的因式分解，则每个$q_i(x)$都具有相同的次数

证明. 我们把$p(x)$看做是$B[x]$的一个多项式，然后设$E=B(z_1,\cdots,z_n)$是$p(x)$的一个分裂域。其中$z_1,\cdots,z_n$是$p(x)$的根。若p在$B[x]$中不能分解，则我们就证明完了。不然，我们取$q_1(x)$的一个根z_1，对每个$j\neq1$，取$q_j(x)$的根z_j。那么会存在一个同构$\varphi_j: k(z_1)\to k(z_j)$使得$\varphi_j(z_1)=z_j$且$\varphi_j$固定$k$。利用命题15，这里就存在一个$E$上的自同构$\Phi$由$\varphi_j$扩张得到。利用推论11，则有$\Phi_j(B)=B$

因此我们就知道$\Phi_j': B[x]\to B[x]$是一个同构，只需要让Φ_j作用在多项式系数上即可。

那么我们立马得到

$$p'(x)=q_1'(x)\cdots q_t'(x)$$

其中$p'=\Phi_j'(p)$，且$q_j'=\Phi_j'(q_j)$对所有i成立， 由于p的分解为不可约多项式，则同构保证q'中的也是不可约多项式的乘积。因为Φ_j固定k，$B[x]$中的唯一分解定理我们有$q_1'=q_\ell$对某个ℓ成立，为此$q'=q$。但$z_j=\Phi_j(z_1)$是一个根。 从而$q_1'(x)=q_j(x)$。 则$\deg(q_1)=\deg(q_1')=\deg(q_j)$。 因此每个$q_i(x)$都具有相同次数。 $\square$

定理 22. 令E/k是有限域扩张。 则E/k是$k[x]$中某个多项式的分裂域当且仅当$k[x]$中每一个在E中有一个根的不可约多项式在$E[x]$中可分裂。

证明. 设E/k是$k[x]$中某个多项式的分裂域， 且$p(x)\in k[x]$是不可约的。 且设$p(x)=q_1(x)\cdots q_t(x)$是它在$E[x]$中的不可约因式分解。若$p(x)$在E中有一个根，则在$E[x]$中就有一个线性因式。利用引理21，所有的$q_i(x)$是线性的，因此$p(x)$在E中分裂。

反过来，设$k[x]$中每一个在E中有一个根的不可约多项式在$E[x]$中分裂，取$\beta_1\in E$使得$\beta_1\notin k$。由于E/k是有限的，则存在一个以β_1为根的不可约多项式$p_1(x)\in k[x]$。由假设，$p_1(x)$在E中分裂，设$B_1\subseteq E$是$p_1(x)$的一个分裂域，若$B_1=E$，则证明完毕。不然，我们取$\beta_2\in E$且$\beta_2\notin B_1$，然后重复上面的步骤得到$p_2(x)\in k[x]$，然后定义$B_2\subseteq E$是$p_1(x)p_2(x)$的分裂域，这样子就存在一个根式塔$k\subseteq B_1\subseteq B_2\subseteq E$。由于$E/k$是有限的，该过程最后会停止，即存在$r\geq1$使得$E=B_r$。 $\square$

定义（正规扩张） 23. 一个域扩张被称为正规扩张，若每个在E中有一个根的不可约多项式$p(x)\in k[x]$在$E[x]$中分裂。