迦罗瓦理论的基本定理 分卷2

2024 年 10 月 23 日

目录

1 基本定理

接着讲基本定理的剩下部分。

迦罗瓦的可解性可以让我们推导出运用根式可解。

1.1 定义：范数

若E/k伽罗瓦扩张，且$u \in E^\times$，定义u的范数$N(u)$为

$$N(u) = \prod_{\sigma \in \mathrm{Gal}(E/k)} \sigma(u)$$

接着我们给出一些初等性质：

1. 若$u \in E^\times$，则$N(u) \in k^\times$
2. $N(uv) = N(u)N(v)$，从而$N : E^\times \to k^\times$是同态。
3. 若$a \in k$，则$N(a) = a^n$，其中$n = [E : k]$
4. 若$\sigma \in G$且$u \in E^\times$，则$N(\sigma(u)) = N(u)$

1.2 希尔伯特定理：

设E/k是伽罗瓦扩张，它的伽罗瓦群$G = \mathrm{Gal}(E/k)$是n阶循环群，记生成元为σ，若$u \in E^\times$，则$N(u) = 1$当且仅当存在$v \in E^\times$使得$u = v\sigma(v^{-1})$

证明： 选取$u = v\sigma(v)^{-1}$，就有

$$\begin{aligned} N(u) =& N(v)\sigma(v)^{-1}) \\ =& N(v)N(\sigma(v))^{-1} \\ =& 1 \end{aligned}$$

反之，设$N(u) = 1$，在$E^\times$中定义偏范数：

$$\begin{aligned} \delta_0 =& u \\ \delta_1 =& u\sigma(u) \\ \vdots& \\ \delta_{n-1} =& u\sigma(u)\cdots\sigma^{n-1}(u) \end{aligned}$$

注意范数就是一个特征标。现在$\sigma_{n-1} = N(u) = 1$，那么可以推导出：

$$\text{for all } 0 \leq i \leq n-2, u\sigma(\delta) = \delta_{i+1}$$

由特征标的线性无关性，则我们知道存在$y \in E$使得

$$\delta_0(y) + \delta_1\sigma(y) + \cdots + \delta_{n-2}\sigma^{n-2}(y) + \delta^{n-1}(y) \neq 0$$

不妨把上述和记为z，然后应用$u\sigma$在等式两边，做一下变换则有

$$\begin{aligned}
\sigma(z) &= \sigma(\delta_0)\sigma(y) + \sigma(\delta_1)\sigma^2(y) + \cdots + \sigma(\delta_{n-2})\sigma^{n-1}(y) + \sigma^n(y) \\
&= u^{-1}\delta_1\sigma(y) + u^{-1}\delta_2\sigma^2(y) + \cdots + u^{-1}\delta_{n-1}\sigma^{n-1}(y) + y \\
&= u^{-1}\Big(\delta_1\sigma(y) + \delta_2\sigma^2(y) + \cdots + \delta_{n-1}\sigma^{n-1}(y)\Big) + u^{-1}\delta_0 y \\
&= u^{-1}z.
\end{aligned}$$

1.3 推论：

设E/k是素数p次伽罗瓦扩张，若k包含一个p次单位原根ω，则$E = k(z)$，其中$z^p \in k$，从而E/k是p型纯扩张。

证明： 伽罗瓦群$G = \mathrm{Gal}(E/k)$的阶为p，因此是循环群，我们令σ是生成元，由于$w \in k$，从而$N(\omega) = w^p = 1$。利用希尔伯特定理，对某个$z \in E$使得$w = z\sigma(z)^{-1}$。从而有$\sigma(z) = w^{-1}z$，余式$\sigma(z^p) = (w^{-1}z)^p = z^p$。由于$\sigma$生成$G$，所以$z^p \in E^G$。由于$E/k$是伽罗瓦扩张，因此$E^G = k$，从而$z^p \in k$。其次，$z \notin k$，否则$z^p = 1$。从而$k(z) \neq k$是一个中间域，但是$[E : k] = p$是素数，所以不存在任何中间域。就有$E = k(z)$是$p$型纯扩张。

1.4 定理：伽罗瓦

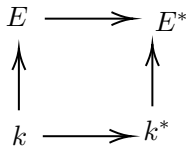
设k是特征为0的域，E/k是伽罗瓦扩张，并设$G = \mathrm{Gal}(E/k)$是可解群，则E可嵌入一个k的根式扩张。由此可得：特征0的域上一个多项式的伽罗瓦群是可解群当且仅当该多项式是运用根式可解的。

证明： 由于G是可解群，则有一正规子群H，设指数为p，令w是p次单位原根，由于k特征为0，则w必定在某个扩域中，则我们有两种情况。

1. 情况1：$w \in k$ 首先对$[E:k]$使用归纳法证明，当$n=1$时，$E=k$，而这是它自己的根式扩张。对归纳步骤，考虑中间域E^H，由推论1.3，E/E^H是伽罗瓦扩张，且$\mathrm{Gal}(E/E^H)$是可解的，它是可解群G的子群。由于$[E:E^H]<[E:k]$，由归纳假设这里存在根式扩张塔$E^H \subseteq R_1 \subseteq \cdots \subseteq R_t$。其中$E \subseteq R_t$。由于$H \lhd G$，所以$E^H/k$是伽罗瓦群。利用基本定理，则$[G:H]=[E^H:k]=p$。利用推论1.3，$E^H=k(z)$，并且$E^H/k$是纯扩张。最后，由根式扩张的定义，我们把$k \subseteq E^H$添加到根式扩张列中即可得到$R_t/k$是根式扩张。

2. 情况2：设$k^*=k(w)$，并定义$E^*=E(w)$，我们假定E^*/k是伽罗瓦扩张，现在，由于E/k是伽罗瓦扩张，那么它应该是某个可分多项式$f(x) \in k[x]$的分裂域，从而E^*是$f(x)(x^p-1) \in k$上的分裂域。但k是特征0的域，因此x^p-1是可分的，从而E^*/k确实是伽罗瓦扩张。则E^*/k^*也是伽罗瓦扩张，令$G^*=\mathrm{Gal}(E^*/k^*)$

   接着我们引入一个习题：

> 定理：配连无理性：设E/k是$f(x) \in k[x]$的分裂域，且伽罗瓦群$G=\mathrm{Gal}(E/k)$。证明，若k^*/k是域扩张，且E^*是$f(x)$在k^*上的分裂域，则$\sigma \to \sigma \mid E$是单同态
>
> $$\mathrm{Gal}(E^*/k^*) \to \mathrm{Gal}(E/k)$$
>
> 
>
>
> **证明：** 这个证明比较简单，由于E是k上的分裂域，且k^*/k是一个域扩张，并且E^*是关于$f(x)$在k^*上的分裂域，则若$\sigma \in \mathrm{Gal}(E^*/k^*)$，那么它置换$f(x)$的所有根，因此$\sigma \mid E \in \mathrm{Gal}(E/k)$是一个单射。

现在，利用配连无理性，那就存在一个单射$\psi : G^* \to G = \mathrm{Gal}(E/k)$，从而$G^*$是可解的（可解群的子群也是可解的）。从而它应该与一个子群同构。现在，因为$w \in k^*$，则利用第一种情况我们可以得到根式塔$R_1^* \subseteq \cdots \subseteq R_m^*$，它有$E \subseteq E^* \subseteq R_m^*$。但是$k^* = k(w)$是纯扩张，那么就可以加进前面的根式塔继续扩张，因而R_M^*/k就是一个根式扩张。

现在我们给出一个经典公式的证明：

1.5 命题

若k是特征为0的域，则每个次数$\deg(f) \leq 4$的$f(x) \in k[x]$都是根式可解的。

证明： 设G是$f(x)$的伽罗瓦群，则G同构于S_4的某个子群，但S_4是可解的，因此S_4的子群都是可解群，利用定理伽罗瓦，则$f(x)$是运用根式可解的。

接着我们讲判别式

1.6 定义：判别式

若$f(x) = \prod_i (x - a_i) \in k[x]$，其中$k$是域，我们定义

$$\Delta = \prod_{i<j} (a_i - a_j)$$

并定义判别式为$D = D(f) = \Delta^2 = \prod_{i<j}(a_i - a_j)$

显然，有重根当且仅当判别式为0

注意 在某些域中$a_i - a_j$是可能变号的。所以我们选择Δ^2作为判别式是恰当的，使用Δ不仅仅要依赖于$f(x)$的根，还依赖于根的排列。而取平方则没这些要求。

1.7 命题：

若$f(x) \in k[x]$是可分多项式，则它的判别式D在k中。

证明： 设E/k是$f(x)$的分裂域，由于$f(x)$可分，所以E/k是伽罗瓦扩张，每个$\sigma \in \mathrm{Gal}(E/k)$置换$f(x)$的根。现在$\sigma(\Delta) = \pm\Delta$。

那么

$$\sigma(D) = \sigma(\Delta^2) = \sigma(\Delta)^2 = (\pm\Delta)^2 = D$$

从而$D \in E^G = k$。

接下来我们讲讲如何用判别式计算伽罗瓦群：

1.8 命题：

设k是特征$\neq 2$的域，其中$f(x) \in k[x]$是无重根的n次多项式，且$D = \Delta^2$是它的判别式，设E/k是$f(x)$的分裂域，并把$G = \mathrm{Gal}(E/k)$看作是S_n的子群，

1. 若$H = A_n \cap G$，则$E^H = k(\Delta)$
2. G是A_n的子群当且仅当$\sqrt{D} \in k$

证明： 利用第二同构定理，则$H = (G \cap A_n) \lhd G$且

$$[G : H] = [G : A_n \cap G] = [A_nG : A_n] \leq [S_n : A_n] = 2$$

利用伽罗瓦基本定理，$[E^H : k] = [G : H]$，因此$[E^H : k] \leq 2$。接着我们继续讨论，首先$\sigma \in G$则会有$\sigma(\Delta) = \pm\Delta$。其次，若$\sigma \in A_n$，则对所有的$\sigma\Delta = \Delta$。则$k(\Delta) \subseteq E^{A_n}$。从而$k(\Delta) \subseteq E^H$，就有

$$[E^H : k] = [E^H : k(\Delta)][k(\Delta) : k] \leq 2$$

现在有两种情况，若$[E^H : k] = 1$，则结果显而易见。有$E^H = k(\Delta)$。其次，若$[E^H : k = 2]$。则$[G : H] = 2$且存在$\sigma \in G$且$\sigma \notin A_n$，从而有$\sigma(\Delta) = -\Delta$。另外，因为$f(x)$是无重根的，因此$\Delta \neq 0$。又有k特征不为2，所以$-\Delta \neq \Delta$。从而$\Delta \notin E^G = k$，就有$[k(\Delta) : k] > 1$。所以$[E^H : k(\Delta)] = 1$且$E^H = k(\Delta)$

对于第二个命题，现在$G \leq A_n$，有$H = G \cap A_n = G$，$E^H = E^G = k$三个命题是等价的，由命题1，则$E^H = k(\Delta)$，因此$E^H = k$等价于$k(\Delta) = k$，也就是$\sqrt{D} \in k$

例子1： 设$f(x) \in Q[x]$是二次多项式，它的伽罗瓦群阶是1或者2，若分裂，则阶为1，否则$f(x)$不可约，阶为2。

1.9 命题

设$f(x) \in \mathbb{Q}[x]$是三次不可约多项式，其伽罗瓦群为G，而判别式为D。

1. $f(x)$恰好有一个实根当且仅当$D < 0$，此时$G \cong S_3$
2. $f(x)$有三个实根当且仅当$D > 0$，或者此时$\sqrt{D} \in \mathbb{Q}$且$G \cong I_3$，或者$\sqrt{D} \notin \mathbb{Q}$且$G \cong S_3$

证明： 首先$D \neq 0$，由于$\mathbb{Q}$特征为0，则$\mathbb{Q}$上的不可约多项式是无重根的，若$f(x)$存在三个实根，则$\sqrt{\Delta}$是实数，且$D = \Delta^2 > 0$。另一种可能是，$f(x)$有一个实根a和两个复根$\beta = u + iv$和$\hat{\beta} = u - iv$。在这种情况下，$a = \hat{a}$

$$\begin{aligned}\Delta =&(a-\beta)(a-\hat{\beta})(\beta-\hat{\beta})\\ =&(a-\beta)(\overline{a-\beta})(\beta-\hat{\beta})\\ =&\mid a-\beta \mid^2 (2iv)\end{aligned}$$

那么$D = \Delta^2 = -4v^2 \mid a-\beta \mid^4 < 0$

另外，设$E/\mathbb{Q}$是$f(x)$的分裂域。若$f(x)$有一实根a，则$E \neq \mathbb{Q}(a)$。那么$\mid G \mid > 3$。因此，只有一个答案，$G \cong S_3$。反过来，若$f(x)$存在三个实根，则$D > 0$且$\sqrt{D}$是实数，则利用命题1.8的第二个命题，若$\sqrt{D}$是有理数，则$G \cong A_3 \cong I_3$，反之$\sqrt{D}$是无理数则有$G \cong S_3$

例子 多项式$x^3 - 2 \in \mathbb{Q}[x]$是不可约的，现在，他的判别式为$D = -108$，则有一个实根，其次，$\sqrt{-109} \notin \mathbb{Q}$，所以$G \cong S_3$.

例子2 多项式$f(x) = x^3 - 4x + 2 \in \mathbb{Q}[x]$是不可约的，他的判别式为$2^{12}3^4$，从而有3个实根，现在$\sqrt{D}$是有理数，则$G \cong A_3 \cong I_3$