迦罗瓦理论的基本定理 分卷1

2024 年 10 月 13 日

目录

1 基本定理

迦罗瓦理论主要分析了域k的代数扩张E和相应的迦罗瓦群$\mathrm{Gal}(E/k)$之间的联系，这种联系能够使我们证明迦罗瓦定理的逆定理：若k是特征为0的域，且$f(x) \in k[x]$有可解的迦罗瓦群，则$f(x)$是根式可解的。接着就能得到代数基本定理。

设E是域，令$\mathrm{Aut}(E)$表示E的上一切自同构形成的群，若k是E的任一子域，则$\mathrm{Gal}(E/k)$是$\mathrm{Aut}(E)$的子群

1.1 定义：固定域

若E是域且H是$\mathrm{Aut}(E)$的子集，则定义H的**固定域**为：

$$E^H = \{a \in E; \text{For all } \sigma \in H, \sigma(a) = a\}$$

固定域E^H的最重要一个实例是当H是$\mathrm{Aut}(E)$的子群时形成的，但也会遇到H仅仅作为一个子集的情况。

若$\sigma \in \mathrm{Aut}(E)$，则$E^\sigma = \{a \in E; \sigma(a) = a\}$是$E$的子域，因为

$$E^H = \bigcap_{\sigma \in H} E^\sigma$$

我们就得到E^H也是E的子域。

1.2 定义：对称函数

有理函数$g(x_1, \cdots, x_n)/h(x_1, \cdots, x_n) \in k(x_1, \cdots, x_n)$称为对称函数，若置换它的变量保持函数不变；对每个$\sigma \in S_n$，有$g(x_{\sigma_1}, \cdots, x_{\sigma_n})/h(x_{\sigma_1}, \cdots, x_{\sigma_n}) = g(x_1, \cdots, x_n)/h(x_1, \cdots, x_n)$

1.3 命题：

设E是域，则从$\mathrm{Aut}(E)$ 的子集H到E的子域的函数$H \to E^H$是反序的：即$H \le L \le \mathrm{Aut}(E)$，则$E^L \subseteq E^H$

证明： 若$a \in E^L$，则有a对所有$\sigma \in L$有$\sigma(a) = a$,但$H \le L$，则同样对$\sigma \in H$也有$\sigma(a) = a$，因此$E^L \subseteq E^H$

例子： 我们设k是E的子域且$G=\mathrm{Gal}(E/k)$，则有$k\subseteq E^G$，因为$\mathrm{Gal}(E/k)$只是置换除k以外的所有其他元，而对k都是固定域，所以k是E^G包含的固定域。

例子2： 设$E=\mathbb{Q}(\sqrt[3]{2})$，我们设$\sigma\in G=\mathrm{Gal}(E/\mathbb{Q})$，则$\sigma$必定固定$\mathbb{Q}$，从而置换方程$f(x)=x^3-2$的根。但$f(x)$的另外两个根不是实数，因此$\sigma(\sqrt[3]{2})=\sqrt[3]{2}$，所以$\sigma$是恒等函数。有$E^G=E$。但$E$不是$f(x)$的分裂域

我们接着的目标是确定次数$[E:E^G]$，其中$G\leq \mathrm{Aut}(E)$，为此我们特意引入特征标的概念。

1.4 定义：特征标

群G在域E中的特征标指的是：（群）同态$\sigma:G\to E^\times$，其中$E^\times$是E中的非零元素的乘法群。

若$\sigma\in\mathrm{Aut}(E)$，则它的限制$\sigma\mid E^\times:E^\times\to E^\times$是$E$的一个特征标

1.5 定义：无关

若E是域且$G\leq\mathrm{Aut}(E)$，则G在E中的特征标的一个表$\sigma_1,\cdots,\sigma_n$称为无关的，若对任意的$c_1,\cdots,c_n\in E$且对一切$x\in G$有

$$\sum_r c_i\sigma_i(x)=0$$

可以推出$c_i=0$对所有$i=1,2,\cdots,n$成立。

1.6 戴德金

群G在域E中的不同特征标的每个表$\sigma_1,\cdots,\sigma_n$都是无关的。

证明： 对$n\geq 1$使用归纳法，但$n=1$时步骤成立，$c\sigma(x)=0$要么$c=0$要么$\sigma(x)=0$，但$\mathrm{im}\sigma\subseteq E^\times$，因此只有$c=0$

设$n>1$，若特征标不是无关的，则存在不完全为0的$c_i\in E$使得对一切$x\in G$有

$$c_1\sigma(x)+\cdots+c_n\sigma_n(x)=0 \tag{1}$$

若对任意i，$c_i \neq 0$，根据归纳法可以得到这是矛盾，所以我们假设一切的$c_i \neq 0$。若有必要，我们可以乘上c_n^{-1}，从而我们可以先假定$c_n = 1$，由于$\sigma_n \neq \sigma_1$，就有$\sigma_1(y) \neq \sigma_n(y)$。用$yx$做替换$x$，因为$\sigma_i(yx) = \sigma_i(y)\sigma_i(x)$。就有

$$c_1\sigma_1(y)\sigma_1(x) + \cdots + c_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(y)\sigma_n(x) = 0$$

现在我们乘上$\sigma_n^{-1}(y)$有：

$$c_1\sigma_n(y)^{-1}\sigma_1(y)\sigma_1(x) + \cdots + \sigma_n(x) = 0$$

将1式减去上方式子可以得到一个剩下$n-1$个项的和：

$$c_1[1 - \sigma_n^{-1}(y)\sigma_1(y)]\sigma(x) + \cdots = 0$$

由归纳假设，因为系数$c_i[1 - \sigma_n(y)\sigma_i(y)] = 0$，且$c_i \neq 0$。那么所有的$\sigma_n(y)\sigma_i(y) = 1$，得到$\sigma_n(y) = \sigma_i(y)$，这与我们的假设矛盾。

1.7 引理

若$G = \{\sigma_1, \cdots, \sigma_n\}$是域$E$上$n$个不同自同构的集合，则

$$[E : E^G] \geq n$$

证明： 假设$[E : E^G] = r < n$，并设$a_1, \cdots, a_r$是E/E^G的基，考虑E上的n个未知数r个方程的齐次线性方程组：

$$\begin{aligned}
\sigma_1(a_1)x_1 + \cdots + \sigma_n(a_1)x_n = 0 \\
\sigma_1(a_2)x_1 + \cdots + \sigma_n(a_2)x_n = 0 \\
\sigma_1(a_r)x_1 + \cdots + \sigma_n(a_r)x_n = 0.
\end{aligned}$$

由于$r \leq n$，那么E^n中是有非平凡解的$(c_1, \cdots, c_n)$

现在我们证明对任意$\beta \in E^\times, \sigma_1(\beta)c_1 + \cdots + \sigma_n(\beta)c_n = 0$和特征标$\sigma_1 \mid E^\times, \cdots, \sigma_n \mid E^\times$的无关性是矛盾的。

由于$a_1, \cdots, a_n$是E在E^G上的基，则每个$\beta \in E$可以写为：

$$\beta = \sum b_i a_i$$

其中$b_i \in E^G$，方程组的第i行乘以$\sigma_1(b_i)$得到

$$\sigma_1(b_i)\sigma_1(a_i)c_1 + \cdots + \sigma_1(b_i)\sigma_n(a_i)c_n = 0$$

但$b_i \in E^G$，这意味着对所有$\sigma \in G$有$\sigma_1(b_i) = b_i = \sigma_j(b_i)$。那么第$i$行成为：

$$\sigma_1(b_i a_i)c_1 + \cdots + \sigma_n(b_i a_i)c_n = 0$$

然后把所有行加在一起就有

$$\sigma_1(\beta)c_1 + \cdots + \sigma_n(\beta)c_n = 0$$

这是个矛盾。因为$c_1, \cdots, c_n$是非平凡解，这与特征标的无关性矛盾。

1.8 命题：

若$G = \{\sigma_1, \cdots, \sigma_n\}$是$\mathrm{Aut}(E)$的子群，则

$$[E : E^G] =| G |$$

证明： 根据引理1.7，我们证明$[E : E^G] \leq | G |$。由于$[E : E^G] \geq n$。我们设$\{w_1, \cdots, w_{n+1}\}$是E^G上的向量空间E中的线性无关向量表，接着考虑$n+1$个变量组成的n个方程组。

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_{n+1})x_{n+1} &= 0. \end{aligned}$$

那么就存在一组E上的非平凡解$a_1, \cdots, a_{n+1}$，不妨将其正规化，选择具有最少非零分量的解$(\beta_1, \cdots, \beta_r, 0, \cdots, 0)$，其长度为$r$。注意的是$r \neq 1$，以免出现$\sigma_1(w_1)\beta = 0$得到$\beta_1 = 0$，如果有必要不妨乘以$\beta_r$的逆，现在我们假定$\beta_r = 1$，注意的是$\beta_i$并不是全都在$E^G$中，以免出现$\sigma = 1_E$使得$\{w_1, \cdots, w_{n+1}\}$是线性相关的。因此最后的一个假设是$\beta_1$不在$E^G$中，那么就存在$\sigma_k$使得$\sigma_k(\beta_1) \neq \beta_1$

现在，由于$\beta_r = 1$，那么方程组的第j行是：

$$\sigma_j(w_1)\beta_1 + \cdots + \sigma_j(w_{r-1})\beta_{r-1} + \sigma_j(w_r) \tag{2}$$

现在作用σ_k到这个方程上就有

$$\sigma_k\sigma_j(w_1)\sigma_k(\beta_1) + \cdots + \sigma_k\sigma_j(w_r)$$

注意G是群，则$\sigma_k\sigma_1, \cdots, \sigma_k\sigma_n$实际上就是$\sigma_1, \cdots, \sigma_n$的一个置换，不妨设$\sigma_k\sigma_j = \sigma_i$。接着根上一个定理的证明一样，用等式2减去上式得到：

$$\sigma_i(w_1)[\beta_1 - \sigma_k(\beta_1)] + \cdots + \sigma_i(w_{r-1})[\beta_{r-1} - \sigma_k(\beta_{r-1})] = 0$$

由于$\beta_i - \sigma_k(\beta_i) \neq 0$，所以这里有非平凡解，意味着非零分量的个数少于$r$，这与我们的假设矛盾。

那么这给出迦罗瓦定理的基本定理中证明需要的一个结果：

1.9 定理：

若G和H是$\mathrm{Aut}(E)$的有限子群且满足$E^G = E^H$，则$G = H$

证明： 我们来证明，若$\sigma \in \mathrm{Aut}(E)$，则$\sigma$固定$E^G$当且仅当$\sigma \in G$。左推右是简单的，现在，我们假定$\sigma$固定$E^G$但$\sigma \notin G$。若$| G |= n$，根据命题1.8就有

$$n =| G |= [E : E^G]$$

因为σ固定E^G，就有$E^G \subseteq E^{G\cup\{\sigma\}}$，但利用命题1.3，反过来的不等式是恒成立的。因此$E^G = E^{G\cup\{\sigma\}}$

然后利用引理1.7就有

$$n = [E : E^G] = [E : E^{G\cup\{\sigma\}}] \geq| G \cup \{\sigma\} |= n + 1$$

矛盾

若$\sigma \in H$由假设，σ固定$E^H = E^G$，因此$\sigma \in G$得到$H \leq G$。我们可以反过来继续证明反包含关系，因此$H = G$

1.10 定理

若E/k是有限扩张，它具有迦罗瓦群$G = \mathrm{Gal}(E/k)$，则下列陈述是等价的：

1. E是某个可分多项式$f(x) \in k[x]$的分裂域
2. $k = E^G$
3. 每个有根在E中的不可约多项式$p(x) \in k[x]$在$E[x]$中是可分和分裂的。

证明： 由$1 \to 2$，首先$|\ G\ | = [E : k]$，然后命题1.9 给出$|\ G\ | = [E : E^G]$，因此

$$[E : k] = [E : E^G]$$

由于$k \leq E^G$，那么就有$[E : k] = [E : E^G][E^G : k]$得到$[E^G : k] = 1$。因此$k = E^G$

由$2 \to 3$，设$p(x) \in k[x]$是以E中a为根的不可约多项式，再设集合$\{\sigma(a) : \sigma \in G\}$的不同元素为$a_1, \cdots, a_n$。定义$g(x) \in E[x]$为

$$g(x) = \Pi(x - a_i)$$

注意σ置换每个a_i，从而σ固定$g(x)$的系数，那么$g(x)$的系数在$E^G = k$中，所以$g(x)$实际上是$k[x]$中无重根的多项式，现在p, g在E中有一个公共根，所以在$E[x]$中，这俩的$\mathrm{gcd} \neq 1$，由于$p(x)$是不可约的，那么$p(x) \mid g(x)$，所以$p(x)$是无重根的，因而可分且在E上分裂。

最后。由$3 \to 1$。选取$a_1 \in E$且$a_1 \notin k$，因为E/k是有限扩张，那么a_1是k上的代数元，不妨设$p_1(x) = \mathrm{irr}(a_1, k)$[1]是$a_1$的极小多项式，由假设，$p_1(x)$是可分且在$E$上分裂的，令$K_1 \subseteq E$是其分裂域。若$K_1 = E$，则证明完成。否则选取$a_2 \in E$且$a_2 \notin K_1$，根据假设，就存在不可约多项式$p_2(x)$以$a_2$为根，令$K_2$是多项式$p_1(x)p_2(x)$的分裂域，若$K_2 = E$，则证明完成，否则重复上述步骤知道$K_m$满足$K_m = E$。这种过程是有限的，则$E$一定是某个多项式$p_1(x) \cdots p_m(x)$的分裂域

[1] a_1在k上的极小多项式

1.11 定义：迦罗瓦扩张

域扩张E/k称为是迦罗瓦扩张，如果它满足定理1.10上的任意一个等价条件。

1.12 推论：

若E/k是迦罗瓦扩张，B是中间域，满足$k \subseteq B \subseteq E$，则$E/B$是迦罗瓦扩张。

证明： E是某个可分多项式$p(x) \in k[x]$的分裂域，即$E = k(a_1, \cdots, a_n)$，其中$a_1, \cdots, a_n$是$f(x)$的根，由于$k \subseteq B \subseteq E$，就存在$f(x) \in B[x]$且有$E = B(a_1, \cdots, a_n)$。

现在，回想n变量的初等函数对称函数，它是多项式：

$$e_j(x_1, \cdots, x_n) = \sum_{i_1 < \cdots < i_j} x_{i_1} \cdots x_{i_j}$$

其中$j = 1, \cdots, n$

1.13 定理：对称函数的基本定理

若k是域，则$k(x_1, \cdots, x_n)$中的每个对称函数都是初等对称函数$e_1, \cdots, e_n$中的有理函数

证明： 我们设F是$E = k(x_1, \cdots, x_n)$的包含初等对称函数的最小子域。那么E是一个n次一般多项式$f(t)$的分裂域，其中

$$f(t) = \prod_{i=1}^{n} (t - x_i)$$

由于$f(t)$是可分多项式，所以E/F是迦罗瓦扩张，利用阿贝尔-鲁非尼定理，我们知道迦罗瓦群同构于置换群S_n的一个子群$\mathrm{Gal}(E/F) \cong S_n$，利用定理1.10，则$E^{S_n} = F$。但是若$\theta(x) = g(x_1, \cdots, x_n)/h(x_1, \cdots, x_n)$在$F$中，这说明他在变量的置换下是完全不变的，因此$\theta(x)$是对称函数。

1.14 定义：复合域

设A和B是域E的子域，他们的复合域记为$A \vee B$，指E的一切包含$A \cup B$的子域的交。

容易知道，$A \vee B$是包含A, B的最小子域，例如，若E/k是一个具有中间域$A = k(a_1, \cdots, a_n)$和$B = k(b_1, \cdots, b_m)$的扩张。则他们的复合域

$$A \vee B = k(a_1, \cdots, a_n) \vee k(b_1, \cdots, b_m) = k(a_1, \cdots, a_n, b_1, \cdots, b_m)$$

1.15 命题：

1. 每个伽罗瓦扩张E/k都是k的分裂扩张
2. 若E/k是代数扩张且$S \subseteq E$是任意一个可分元素的集合，它可以是无限的，则$k(S)/k$是可分扩张。
3. 设E/k是代数域扩张，其中k是域，且B, C都是中间域。若B/k和C/k都是可分扩张。则他们的复合域$B \vee C$也是k的可分扩张。

证明：

1. 如果$\beta \in E$，则$p(x) = \mathrm{irr}(\beta, k) \in k[x]$是$k[x]$中有一个根在$E$中的不可约多项式。由定理1.10的3，每个不可约多项式都是可分的。所以$p(x)$是可约多项式。则β在k上可分，就有E/k是可分扩张。
2. 首先考虑S是有限的情况，即，$B = k(a_1, \cdots, a_n)$是有限扩张，其中每个a_i在k上是可分的，那么我们知道，E是B的分裂域，存在扩张E/B，他是某个可分多项式$f(x) \in k[x]$的分裂域。由定理1.10的1，该扩张是伽罗瓦扩张。利用刚刚证明的第一个命题，该扩张也是可分扩张，即对于一切的$a \in E$，多项式$\mathrm{irr}(a, k)$无重根，特别的，对于一切的$a \in B$，$\mathrm{irr}(a, k)$是无重根的，这样我们就得到B/k是可分扩张。

   接着考虑一般情况，我们引入如下命题：

   > 设K/k是域扩张，若$A \subseteq K$和$u \in k(A)$,证明存在$a_1, \cdots, a_n \in A$使得$u \in k(a_1, \cdots, a_n)$

证明： 设$u \in k(A)$但不存在$a_1, \cdots, a_n \in A$使得$u \in k(a_1, \cdots, a_n)$，那么这是一个超越元，因为我们假设表明了该元不可能是有限生成的，即$u \notin A$矛盾。

回到证明上来，若$a \in k(S)$，则上述命题告诉我们，存在有限个元素$a_1, \cdots, a_n \in S$使得$a \in B = k(a_1, \cdots, a_n)$，那么$B/k$是可分扩张，从而$a$在$k$上可分，由$a$的任意性，则$k(S)/k$是可分扩张

3. 由于$B \vee C = k(B \cup C)$，我们定义$S = B \cup C$，则S是一个可分元素的集合，由命题2我们知道$k(S)/k = k(B \cup C)/k$是可分扩张。

问题： 若E/k是伽罗瓦扩展且B是中间域，那么B/k是伽罗瓦扩张吗？答案是否定的，在刚才的上述例子2，令$E = Q(\sqrt[3]{2}, w)$是$\mathbb{Q}$上多项式$x^3 - 2$的分裂域，其中w是三次本原根，它的中间域是$B = \mathbb{Q}(\sqrt[3]{2})$，但$x^3 - 2$在$B$中有不可约的根，因此在$B[x]$中是不可约的。

那么我们来判断中间域B在什么时候是伽罗瓦扩张。

1.16 定义：共轭

若E/k是伽罗瓦扩张，B是中间域，则对某个$\sigma \in \mathrm{Gal}(E/k)$，中间域

$$B^\sigma = \{\sigma(b) : b \in B\}$$

称为B的一个共轭

1.17 命题：

若E/k是伽罗瓦扩张，且B是中间域，则B除了自身以外没有其他共轭当且仅当B/k是伽罗瓦扩张。

证明： 设对一切的$\sigma \in G$，$B^\sigma = B$，其中$G = \mathrm{Gal}(E/k)$。再令$p(x) \in k[x]$是在B中有根β的不可约多项式。由于$B \subseteq E$且E/k是伽罗瓦扩张，所以$p(x)$在$E[x]$中分裂且是可分多项式。现在设存在另一个根β'，那么同构将β映射为$\sigma(\beta) = \beta' \in B^\sigma$，由于共轭$B^\sigma = B$，因此$\beta' \in B$使得$p(x)$在$B[x]$中分裂，所以$B/k$是伽罗瓦扩张

反之由于B/k是k上某个多项式$f(x)$的分裂域，就有$B=k(a_1,\cdots,a_n)$，其中$a_1,\cdots,a_n$是$f(x)$所有的根，所以每个$\sigma\in\mathrm{Gal}(E/k)$必置换$f(x)$的根，从而$\sigma$将$B$映射到自身。

1.18 定义：格

格指的是偏序集$\mathcal{L}$，其中每对元素$a,b\in\mathcal{L}$都有最大下界$A\wedge B$和最小上界$A\vee B$。

1.19 反序

若$\mathcal{L}$和$\mathcal{L}'$是格，函数$f:\mathcal{L}\to\mathcal{L}'$称为反序的，若在$\mathcal{L}$中有$a\preceq b$可以推导出在$\mathcal{L}'$中有$f(b)\preceq f(a)$

1.20 引理：

设$\mathcal{L}$和$\mathcal{L}'$是格，$\varphi:\mathcal{L}\to\mathcal{L}'$是使得$\varphi$和$\varphi^{-1}$都是反序的双射。则

$$\varphi(a\wedge b)=\varphi(a)\vee\varphi(b),\varphi(a\vee b)=\varphi(a)\wedge\varphi(b)$$

证明： 由于$a,b\preceq a\vee b$，所以有$\varphi(a\vee b)\prec\varphi(a),\varphi(b)$，即$\varphi(a\vee b)$是$\varphi(a),\varphi(b)$的下界。从而$\varphi(a\vee b)\preceq\varphi(a)\wedge\varphi(b)$

反过来，由φ的满射性给出$c\in\mathcal{L}$使得$\varphi(a)\wedge\varphi(b)=\varphi(c)$ 现在$\varphi(c)=\varphi(a)\wedge\varphi(b)\preceq\varphi(a),\varphi(b)$，将$\varphi^{-1}$作用在两边，因为$\varphi^{-1}$是反序的，就有$a,b\preceq c$，所以$c$是$a,b$的上界。有

$$\varphi(a\vee b)\succeq\varphi(c)=\varphi(a)\vee\varphi(b)$$

用同样的方法可以证明另一个公式。

我们引入一些定义：

1. Int：指中间域的集族
2. Sub指商群组成的组

1.21 定理：伽罗瓦理论的基本定理

设E/k是有限伽罗瓦扩张，它具有伽罗瓦群$G=\mathrm{Gal}(E/k)$

1. 定义函数$\gamma:\mathrm{Sub}(\mathrm{Gal}(E/k))\to\mathrm{Int}(E/k)$为
$$\gamma:H\to E^H$$
则 γ是反序双射。它的逆$\delta:\mathrm{Int}(E/k)\to\mathrm{Sub}(\mathrm{Gal}(E/k))$是反序双射

2. 对每个$B\in\mathrm{Int}(E/k)$和$H\in\mathrm{Sub}(\mathrm{Gal}(E/k))$
$$E^{\mathrm{Gal}(E/B)}=B\text{且}\mathrm{Gal}(E/E^H)=H$$

3. 对每个$H,K\in\mathrm{Sub}(\mathrm{Gal}(E/k))$和$B,C\in\mathrm{Int}(E/k)$
$$\begin{aligned}E^{H\vee K}=&E^H\cap E^K\\E^{H\cap K}=&E^H\vee E^k\\\mathrm{Gal}(E/(B\vee C))=&\mathrm{Gal}(E/B)\cap\mathrm{Gal}(E/C)\\\mathrm{Gal}(E/(B\cap C))=&\mathrm{Gal}(E/B)\vee\mathrm{Gal}(E/C)\end{aligned}$$

4. 对每个$B\in\mathrm{Int}(E/k)$和$H\in\mathrm{Sub}(\mathrm{Gal}(E/k))$
$$[B:k]=[G:\mathrm{Gal}(E/B)]\text{且}[G:H]=[E^H:k]$$

5. 若$B\in\mathrm{Int}(E/k)$，则B/k是伽罗瓦群当且仅当$\mathrm{Gal}(E/B)$是G的正规子群

证明：

1. 命题1.3告诉我们γ是反序的，定理1.9告诉我们γ是单射，现在我们证明的事情只有一个，即$\gamma\delta:\mathrm{Int}(E/k)\to\mathrm{Int}(E/k)$是恒等函数，由此即可导出$\gamma$是具有逆$\delta$的双射。若不是双射，不妨看定义，对中间域$B$有$\gamma\delta:\mathrm{Int}(E/k)\to E^{\mathrm{Gal}(E/B)}$。由于$E/k$是迦罗瓦扩张，利用推论1.12。$E/B$是迦罗瓦扩张，所以$E^{\mathrm{Gal}(E/B)}=B$

2. 利用命题1，我们发现这只是$\gamma\delta$和$\delta\gamma$的另一种表述。

3. 引入引理1.20和命题1，答案就出来了。

4. 由于E/B是迦罗瓦扩张，则

$$[B:k]=[E:k]/[E:B]=\mid G\mid/\mid \mathrm{Gal}(E/B)\mid=[G:\mathrm{Gal}(E/B)]$$

因此，B/k的次数就是G中迦罗瓦群的次数。对于第二个等式，我们取$B=E^H$，命题2给出$\mathrm{Gal}(E/E^H)=H$就有

$$[E^H:k]=[G:\mathrm{Gal}(E/E^H)]=[G:H]$$

5. 当B/k是迦罗瓦扩张时，有$\mathrm{Gal}(E/B)\lhd G$。反过来，我们设$H=\mathrm{Gal}(E/B)$且有$H\lhd G$。根据命题2，有$E^H=E^{\mathrm{Gal}(E/B)}=B$。为了证明是迦罗瓦群，我们利用命题1.17证明对$\sigma\in G$都有$(E^H)^\sigma=E^H$就行了。设$a\in E^H$，则对一切$\eta\in H$有$\eta(a)=a$，由于$H\lhd G$，则对$\eta\in H$和$\sigma\in G$，那么就存在共轭$\eta'=\sigma^{-1}\eta\sigma\Rightarrow\eta\sigma=\sigma\eta'$。由于$\eta'(a)=a$那么：

$$\eta\sigma(a)=\sigma\eta'(a)=\sigma(a)$$

因此$B/k=E^H/k$是迦罗瓦扩张，具有迦罗瓦群$\mathrm{Gal}(B/k)$

接下来我们给几个推论：

1.22 定理

若E/k是迦罗瓦扩张且它的迦罗瓦群是阿贝尔群，则每个中间域都是迦罗瓦扩张。

证明： 阿贝尔群的子群都是阿贝尔群。利用基本定理的命题5即可得到。

1.23 推论：

有限群$\mathrm{Gal}(E/k)$只有有限个中间域

证明： 有限群只有有限个子群。

1.24 定义：单扩张

域扩张E/k称为单扩张，若存在$u\in E$使得$E=k(u)$

1.25 定理：Steinitz

有限扩张E/k是单扩张当且仅当他只有有限个中间域

证明： 我们假定E/k是单扩张，于是$E=k(u)$，再令$\mathrm{irr}(u,k)\in k[x]$是它的极小多项式，若$B$是任意一中间域，令

$$q(x)=\mathrm{irr}(u,B)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}+x^n\in B[x]$$

是u在B上的一个不可约多项式，定义：

$$B'=k(b_0,\cdots,b_{n-1})\subseteq B$$

其中$q(x)$是较小域B'上的多项式那么

$$E=k(u)\subseteq B'(u)\subseteq B(u)\subseteq E$$

从而有$B'(u)=E=B(u)$，其次，我们有$[E:B]=[B(u):B]$和$[E:B']=[B'(u):B']$，为了得到$[B:B']$，B'是由多项式$q(x)$得到的，那么$[E:B]=\deg(q)=[E:B']$，又因为$B'\subseteq B$，所以$[B:B']=1$，也就是

$$B=B'=k(b_0,\cdots,b_{n-1})$$

另一方面，我们用$q(x)$的系数刻画了B，$q(x)$是$p(x)$在$E[x]$中的首一多项式，n个因式，至多有2^n个排列，这意味着中间域B是由不可约多项式$q(x)$的系数唯一决定的，不存在两个不同的中间域对应同一个$q(x)$。由于排列是有限的，因此我们知道中间域的数量也是有限的。

反之，设E/k是只有有限个中间域的，若k是有限域，则我们知道E/k是单扩张，取u为本原元即可。所以我们假定k是无限的，由于E/k是有限扩张，则存在元素$u_1,\cdots,u_n$使得$E=k(u_1,\cdots,u_n)$。我们对$n\geq 1$使用归纳法，我们只需要证明$E=k(a,b)$是单扩张的，但由于k是无限的，那么就存在无限个元素$c\in E$形如$c=a+tb$，其中$t\in k$。由于只有有限个中间域，则只有有限个形如$k(c)$的域，由鸽笼原理，那就存在不同的元素$t,t'\in k$使得$k(c)=k(c')$，其中$c'=a+t'b$。那么有$k(c)\subseteq k(a,b)$，对于反包含，$k(c)=k(c')$包含$c-c'=(t-t')b$，从而$b\in k(c)$就有$a=c-tb\in k(c)$。从而$k(c)=k(a,b)$

利用这个定理，我们可以很快的得到伽罗瓦扩张都是单扩张。

1.26 定理：本原元定理

若B/k是有限可分扩张，则存在$u \in B$使得$B = k(u)$，特别的，若k特征0，则每个有限扩张B/k都是单扩张。

证明： 这其实是Steintz定理的后半部分证明，若是有限域，则选取一个本原元u即可，若是无限域，则存在$\mathrm{B} = k(a,b)$有$B = k(c) = k(a,b)$，其中$c = a + tb, t \in k$。然后使用归纳法即可推广到任意有限多的中间域上。也就是说我们在无限域中得到了一个本原元。

1.27 定理

有限域$\mathbb{F}_q$（其中$q = p^n$）对n的每个因子d恰好有一个阶为p^d的子域，而且不存在除此之外其他子域。

证明： 由于$\mathbb{F}_q/\ \mathbb{F}_p$是$x^q - x$的分裂域，所以它是迦罗瓦扩张。那么$G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$是$n$阶循环群，由于$n$阶循环群的因子$d$唯一对应一个子群，从而$G$也有这样的子群$H$，指数为$n/d$，所以他只有一个中间域$E^H$。满足$[E^H : \mathbb{F}_p] = [G : H] = n/d$和$E^H = \mathbb{F}_{p^{n/d}}$

接下来我们证明代数基本定理，在我的博客中已经用刘维尔定理证明了复数域上的定理，这里我们用伽罗瓦基本理论来证明。

1.28 推论：

首先我们假定R满足弱形式的中值定理，若$f(x) \in R[x]$，且存在$a, b \in R$，那么有$f(a) > 0$和$f(b) < 0$，则$f(x)$存在实根。那么下面是一些推论

每个非常数的多项式$f(x) \in \mathbb{C}[x]$是有复根的。

1. 每个正实数r都有一个实平方根：

   例如若$f(x) = x^2 - r$，则

   $$f(1 + r) = (1 + r)^2 - r = 1 + r + r^2 > 0$$

   且$f(0) = -r < 0$。存在一个实平方根。

2. 每个二次多项式$g(x) \in \mathbb{C}[x]$都有一个复根。若有二次扩张，则这和第二个推论矛盾

3. 域$\mathbb{C}$没有二次扩张。

4. 每个奇数次多项式$f(x) \in \mathbb{R}[x]$都有实根。

   设$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \in \mathbb{R}[x]$，定义$t = 1 + \sum \mid a_i \mid$，则对一切$i$，$\mid a_i \mid \leq t - 1$。设$h(x) = f(x) - x^n$，则

   $$\begin{aligned} \mid h(t) \mid = &\mid a_0 + \cdots + a_{n-1} t^{n-1} \mid \\ &\leq (t-1)(1 + t + \cdots + t^{n-1}) \\ \leq t^n - 1 \leq t^n \end{aligned}$$

   所以$-t^n < h(t)$，那么$f(t) > h(t) + t^n > t^n - t^n = 0$

   其次，$f(t) = h(-t) + (-t^n) < t^n + (-t^n)$ 当n是奇数的时候，$f(-t) < 0$而$f(t) > 0$。因此有实根

5. 不存在次数> 1的奇数次域扩张$E/\mathbb{R}$

1.29 代数基本定理

每个非常数的多项式$f(x) \in \mathbb{C}[x]$都有复根

证明： 我们要证明每个非常数的$f(x) \in \mathbb{R}[x]$都有复根。设$E/\mathbb{R}$是包含$\mathbb{C}$的$(x^2 + 1)f(x)$的分裂域，由于$\mathbb{R}$特征0，所以$E/\mathbb{R}$是伽罗瓦扩张，令$\mathrm{Gal}(E/\mathbb{R}) = G$为它的伽罗瓦群，现在，由于每个整数能表达成$2^m k$，其中$m \geq 0$,$k$是奇数。则$\mid \mathrm{Gal}(E/\mathbb{R}) \mid = 2^m k$，利用西罗定理，存在阶为$2^m$的子群$H$，令$B = E^H$是相应的中间域。利用伽罗瓦的基本定理，次数$[B : \mathbb{R}] = [G : H] = k$，利用推论1.28的5。不存在大于1的奇数次的扩张，因此$k = 1$并且G是$2-$群。其次，$E/\mathbb{C}$也是伽罗瓦扩张，利用上述思路，$\mathrm{Gal}(E/\mathbb{C}) \leq G$也是$2-$群。若该群不是平凡群，那么他就是指数为2的子群$K$。单由1.28的3和伽罗瓦基本定理，这是矛盾，不存在次数为2的扩张。矛盾，因此$[E : \mathbb{C}] = 1$，并且$E = \mathbb{C}$。但E是$f(x)$在$\mathbb{C}$上的分裂域。所以$f(x)$有复根