答疑

1. $\mathbb{F}\subseteq\mathbb{E}$ 有限(域)扩张，我们知道：有限可分扩张是单扩张. 若去掉"可分"条件，结论不成立.

例如：$\mathbb{F}=\mathbb{Z}_p(x^p,y^p)$ p素数，$\mathbb{E}=\mathbb{Z}_p(x,y)$

(1) $\mathbb{F}\subseteq\mathbb{E}$ 是有限扩张 $[\mathbb{E}:\mathbb{F}]=[\mathbb{E}:\mathbb{Z}_p(x,y^p)]\cdot[\mathbb{Z}_p(x,y^p):\mathbb{Z}_p(x^p,y^p)]=p\cdot p=p^2$

(2) $\mathbb{F}\subseteq\mathbb{E}$ 不是可分扩张，因为 $x,y\in\mathbb{E}$ 均不是 $\mathbb{F}$ 中元素的 p 次幂，但 $t^p-x^p\in\mathbb{F}[t]$ 是不可分多项式

(3) $\mathbb{F}$ 和 $\mathbb{E}$ 之间有无限个中间域：令 $\mathbb{L}_b=\mathbb{F}(x+by)$, $b\in\mathbb{F}$

若 $\mathbb{L}_b=\mathbb{L}_{b'}$, $b\neq b'\in\mathbb{F}$，则 $x+by\in\mathbb{F}(x+b'y)\Rightarrow x\in\mathbb{F}(x+b'y)$
$\Rightarrow y\in\mathbb{F}(x+b'y)$ 即 $\mathbb{F}(x,y)=\mathbb{F}(x+b'y)$

但是 $[\mathbb{F}(x+b'y):\mathbb{F}]=p$，因为 $(x+b'y)^p=x^p+(b')^py^p\in\mathbb{F}$

2. 设 $\mathbb{F}\subseteq\mathbb{E}$ 有限扩张，$\alpha\in\mathbb{E}$，$\forall\sigma\in Aut_{\mathbb{F}}(\mathbb{E})=Gal(\mathbb{E}/\mathbb{F})$
$\sigma(\alpha)$ 仍是 α 在 $\mathbb{F}$ 上极小多项式 $p(x)$ 的根. 令 A 是根集合 互异

情形1. $\mathbb{E}$ 是 $p(x)$ 在 $\mathbb{F}$ 上分裂域. 则

$$\begin{array}{ccc} Aut_{\mathbb{F}}(\mathbb{E}) & \longrightarrow & S_{|A|} \\ \sigma & \longmapsto & \sigma|_A \end{array}$$

对称群

$A=\{r_1,\cdots,r_k\}$, $r_1=\alpha$

$\textcircled{b}$ $Aut_{\mathbb{F}}(\mathbb{E})$ 在 A 上作用忠实：

$\forall \sigma \in Aut_{\mathbb{F}}(\mathbb{E})$，若 $\sigma|_A = id$，即 $\sigma(r_i) = r_i \quad i=1,\cdots,k$

则 $\sigma = id_{\mathbb{E}}$

$Aut_{\mathbb{F}}(\mathbb{E})$ 在 A 上作用可迁：($\Leftrightarrow P(x)$ 不可约)

$\forall r_i, r_j \in A$. $\exists \sigma \in Aut_{\mathbb{F}}(\mathbb{E}) \quad \sigma(r_i) = r_j$.

情形2. 设 $Aut_{\mathbb{F}}(\mathbb{E}) = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ $(|Aut_{\mathbb{F}}(\mathbb{E})| \le [\mathbb{E}:\mathbb{F}])$

$\alpha \in \mathbb{E}$，$\{\sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_n(\alpha)\}$ 是 α 的轨道. 则有可能 $\sigma_1 \neq \sigma_2$，但 $\sigma_1(\alpha) = \sigma_2(\alpha)$

例如：$f(x) = 3x^5 - 15x + 5 \in \mathbb{Q}[x]$，在 $\mathbb{Q}$ 上分裂域为 $\mathbb{E}$.

$Gal(\mathbb{E}/\mathbb{F}) = S_p = S_5$

$f(x) = 3(x-r_1)(x-r_2)(x-r_3)(x-r_4)(x-r_5) \quad r_i \in \mathbb{E}$.

它有3个实根，两个共轭复根，不妨设 r_1, r_2 共轭，$r_3, r_4, r_5 \in \mathbb{R}$. 则 $\sigma = (12) \in Gal(\mathbb{E}/\mathbb{F})$，$\sigma' = (1)$ 均满足 $\sigma(r_5) = \sigma'(r_5) = r_5$.

3. 143页习题9. 推广

考虑 $\mathbb{Z}_p$ 上 $f(x) = x^3 + bx + c$ 的分裂域 $\mathbb{E}$.（不可约）

设 r 是 $f(x)$ 在 $\mathbb{E}$ 中的一个根. 另两根为 $r_1, r_2 \in \mathbb{E}$.

在 $\mathbb{E}[x]$ 中，$f(x)=(x-r)(x-r_1)(x-r_2)$

$r_1+r_2=-r\in\mathbb{Z}_p(r)$ 　　令 $\delta=(r-r_1)(r-r_2)(r_2-r_1)$

$$r_1-r_2=-\frac{\delta}{(r-r_1)(r-r_2)}=-\frac{\delta}{r^2-(r_1+r_2)r+r_1r_2}=-\frac{\delta}{r^2+r^2+\frac{(-c)}{r}}=\frac{r\delta}{c-2r^3}$$

另一方面 $\delta^2=\cancel{-4a^3-27b^2}\ -(4b^3+27c^2)$ (判别式)

$\Rightarrow r_1,r_2\in\mathbb{Z}_p(r)\Leftrightarrow r_1-r_2\in\mathbb{Z}_p(r)\Leftrightarrow\delta\in\mathbb{Z}_p(r)\Leftrightarrow\sqrt{-4b^3-27c^2}\in\mathbb{Z}_p(r)$

① $\sqrt{-4b^3-27c^2}\in\mathbb{Z}_p(r)$，则 $[\mathbb{E}:\mathbb{Z}_p]=3$ 　$\mathrm{Gal}(\mathbb{E}/\mathbb{Z}_p)\simeq A_3$

② $\sqrt{-4b^3-27c^2}\notin\mathbb{Z}_p(r)$，则 $[\mathbb{E}:\mathbb{Z}_p]=6$ 　$\mathrm{Gal}(\mathbb{E}/\mathbb{Z}_p)\simeq S_3$

注：r,r_1,r_2 互异，因为 $f(x)$ 不可约，故在 $\mathbb{Z}_p$ 上可分.

例如：$x^3+2x+1=f(x)$ 　$b=2,\ c=1\Rightarrow\delta^2=1\Rightarrow\delta\in\mathbb{Z}_3(r)$

$(p=3)$

当 $p=3$ 时，若 $-4b^3-27c^2\neq 2$ (在 $\mathbb{Z}_3(r)$ 中)，则 $\delta\in\mathbb{Z}_3(r)$.