# 答疑

1. 设$\mathbb{F}$是域，$\alpha\notin\mathbb{F}$，在$\mathbb{F}$上极小多项式为$p(x)$，则单扩张$\mathbb{E}=\mathbb{F}(\alpha)$可能不含$p(x)=0$其余根.

例如 $x^3-2\in\mathbb{Q}[x]$ $\quad\mathbb{E}=\mathbb{Q}(\sqrt[3]{2})$ 不含另两根$\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$

但是若$\mathbb{E}$是$\mathbb{F}$上一多项式的分裂域，从而正规扩张，

$\Rightarrow$ $\mathbb{E}$包含$p(x)$全部根.

2. $\mathbb{F}$域，$\mathbb{E}$是$f(x)$在$\mathbb{F}$上分裂域，以下陈述错误：

$\forall\alpha,\beta$是$f(x)$的两根，则存在$\sigma\in Aut_{\mathbb{F}}(\mathbb{E})$，$\sigma(\alpha)=\beta$.

例如 $f(x)=(x^2-2)(x^2-3)$，不存在$\sigma\in Aut_{\mathbb{F}}(\mathbb{E})$，使$\sigma(\sqrt{2})=\sqrt{3}$

$\mathbb{F}=\mathbb{Q}$，$\mathbb{E}=\mathbb{Q}(\sqrt{2},\sqrt{3})$

否则 $\sigma(x^2-2)=x^2-2$ 有根$\sigma(\sqrt{2})=\sqrt{3}$.

一般地，若$f(x)=f_1(x)f_2(x)$ $\quad(f_1(x),f_2(x))=1$，则不存在

$\sigma\in Aut_{\mathbb{F}}(\mathbb{E})$，$\sigma$将$f_1(x)$的某一根映成$f_2(x)$的某一根.

这是因为：若$f_1(\alpha)=0$，$f_2(\beta)=0$，$\sigma\in Aut_{\mathbb{F}}(\mathbb{E})$，$\sigma(\alpha)=\beta$.

则$\sigma[f_1(x)]=f_1(x)$有根$\sigma(\alpha)=\beta$ 即在$\mathbb{E}[x]$中，$f_1(x),f_2(x)$

有公因式$x-\beta$. 矛盾

以下陈述正确：若$f(x)$不可约，

$\forall\alpha,\beta$是两根，则存在$\sigma\in Aut_{\mathbb{F}}(\mathbb{E})$，$\sigma(\alpha)=\beta$.

3. 分裂域唯一性

一般地，分裂域同构意义下唯一. 例如 $x^2+1\in\mathbb{Q}[x]$

$\mathbb{Q}[i]$，$\dfrac{\mathbb{Q}[x]}{(x^2+1)}$ 均可以看成 $x^2+1$ 在 $\mathbb{Q}$ 上分裂域，它们有同构：

$$\mathbb{Q}[i]=\mathbb{Q}(i)\xrightarrow{\sim}\frac{\mathbb{Q}[x]}{(x^2+1)}$$

但是，如果限制到 $\overline{\mathbb{F}}$（$\mathbb{F}$的代数闭包）中，分裂域唯一

设 $\mathbb{F}$ 是域，$\mathbb{E}_1,\mathbb{E}_2$ 均是 ~~$\mathbb{F}$~~ $f(x)$ 在 $\mathbb{F}$ 上分裂域，且 $\mathbb{E}_1\subseteq\overline{\mathbb{F}}$，$\mathbb{E}_2\subseteq\overline{\mathbb{F}}$，则 $\mathbb{E}_1=\mathbb{E}_2$（不仅仅同构）

设 $f(x)$ 在 $\overline{\mathbb{F}}$ 中的根为 $\alpha_1,\cdots,\alpha_n$. 则

$$\mathbb{E}_1=\mathbb{E}_2=\mathbb{F}(\alpha_1,\cdots,\alpha_n).$$

4. 设 $\mathbb{F}\subseteq K$ 域扩张，$\operatorname{char}\mathbb{F}=p$，$\alpha\in K$，则 $\alpha$ 在 $\mathbb{F}$ 上可分元 $\Leftrightarrow \mathbb{F}(\alpha)=\mathbb{F}(\alpha^p)$.

证明："$\Rightarrow$"设 $\alpha$ 可分，若 $\alpha\notin\mathbb{F}(\alpha^p)$，则极小多项式 $p(x)\mid x^p-\alpha^p$

$\alpha$ 在 $\mathbb{F}$ 上极小多项式被 $p(x)$ 整除 $x^p-\alpha^p=(x-\alpha)^p$，$p(x)$ 只有根 $\alpha$，由于 $\alpha$ 可分，在 $\mathbb{F}$ 上极小多项式无重根 $\Rightarrow p(x)=x-\alpha$

$\Rightarrow \alpha\in\mathbb{F}(\alpha^p)$

"$\Leftarrow$"因为 $\mathbb{F}(\alpha)=\mathbb{F}(\alpha^p)$，$\alpha,\alpha^p$ 在 $\mathbb{F}$ 上极小多项式次数相同.

设 $p(x)$，$q(x)$ 分别是它们极小多项式. $\deg p(x)=\deg q(x)$.

~~但是~~ $p(\alpha)=0=q(\alpha^p)$

即 $q(x^p)=0$ 有根 $\alpha$. 令~~$q(x)$ 否~~

若 $p(x)$ 不可分, 则存在 $r(x)$ $p(x)=r(x^p)$. $\deg r(x)<\deg p(x)$

$r(\alpha^p)=0$ 这与 $q(x)$ 是 $\alpha^p$ 的极小多项式矛盾!

应用这个结论, 可以展示: 若 $\alpha$ 是 $\mathbb{F}$ 上可分元, 则 $\mathbb{F}(\alpha)$ 是可分扩张 (over $\mathbb{F}$).

证明: 设 $\beta\in\mathbb{F}(\alpha)$. 需证 $\beta$ 是 $\mathbb{F}$ 上可分元. 即证 $\mathbb{F}(\beta)=\mathbb{F}(\beta^p)$

已知 $\mathbb{F}(\beta,\alpha)=\mathbb{F}(\alpha)(\beta)=\mathbb{F}(\alpha)=\mathbb{F}(\beta^p,\alpha)=\mathbb{F}(\beta^p)(\alpha)$

设 $\alpha$ 在 $\mathbb{F}(\beta)$ 上极小多项式为 $P_1(x)\in\mathbb{F}(\beta)[x]$

在 $\mathbb{F}(\beta^p)$ 上 ———— $P_2(x)\in\mathbb{F}(\beta^p)[x]$

在 $\mathbb{F}$ 上 ———— $P_3(x)\in\mathbb{F}[x]$

因为 $(P_1(x))^p\in\mathbb{F}(\beta^p)[x]$ 且 $(P_1(\alpha))^p=0 \Rightarrow P_2(x)\mid P_1^p(x)$

因为 $\mathbb{F}(\beta^p)[x]\subseteq\mathbb{F}(\beta)[x]$, $P_1(x)\mid P_2(x)$.

在 $\mathbb{F}(\beta)[x]$ 中, $P_1(x)\mid P_2(x)\mid P_1^p(x) \Rightarrow P_2(x)=P_1^l(x)$ $l\le p$.

但 $\alpha$ 在 $\mathbb{F}$ 上可分元 $\Rightarrow$ $\alpha$ 在 $\mathbb{F}(\beta)$ 上可分 $\Rightarrow l=1$

即 $[\mathbb{F}(\beta)(\alpha):\mathbb{F}(\beta)]=\deg P_1(x)=\deg P_2(x)=[\mathbb{F}(\beta^p)(\alpha):\mathbb{F}(\beta^p)]$

$\Rightarrow \mathbb{F}(\beta)=\mathbb{F}(\beta^p)$.