答疑

(1) 理解 $|Em_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|$：它是 $\mathbb{E}$ 到 $\overline{\mathbb{F}}$ 的域同态（保持 $\mathbb{F}$ 不动）的个数，是 $\mathbb{E}$ 和 $\overline{\mathbb{F}}$ 的子域的同构（保持 $\mathbb{F}$ 不动）的个数.

例如 $\mathbb{F}\subseteq\mathbb{E}=\mathbb{F}(\alpha)$，$\alpha$ 在 $\mathbb{F}$ 上的极小多项式为 $p(x)\in\mathbb{F}[x]$

$p(x)=c\prod_{i=1}^{s}(x-\alpha_i)^{n_i}$ $\alpha_i\neq\alpha_j$. $c\in\mathbb{F}$，$\alpha_i\in\overline{\mathbb{F}}$. $\alpha_1=\alpha$

因为 $p(x)$ 不可约，$n_1=n_2=\cdots=n_s=\nu$

$\forall\sigma:\mathbb{E}\to\overline{\mathbb{F}}$ 且 $\sigma|_{\mathbb{F}}=id$，则 $\sigma(p(x))=p(x)$，$\sigma(\alpha)$ 在 $\overline{\mathbb{F}}$ 中是 $\sigma(p(x))=p(x)$ 的根，$\sigma(\alpha)=\alpha_1,\alpha_2,\cdots$ 或 α_s.

由上讨论 $\sigma(\mathbb{E})=\mathbb{F}(\alpha_i)$ $i=1,\cdots,s$.

$\mathbb{E}\xrightarrow{\sim}\sigma(\mathbb{E})$

$\Rightarrow|Em_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|=s=p(x)$ 的不同根个数.

另一方面，在 $\overline{\mathbb{F}}[x]$ 中，$p(x)=c\,q^{\nu}(x)$ 其中 $q(x)=\prod_{i=1}^{s}(x-\alpha_i)$

$\Rightarrow\deg p(x)=\nu\cdot\deg q(x)$

$\Rightarrow|Em_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|\cdot\nu=[\mathbb{E}:\mathbb{F}]$ （当 $\nu=1$，$p(x)$ 可分）.

(2) 可分扩张的传递性.

由讲义命题（或(1)的归纳讨论）（讲义上传少了一页，重新上传）

$\mathbb{F}\subseteq\mathbb{E}$ 有限扩张，$\mathbb{E}$ 是 $\mathbb{F}$ 的可分扩张 $\Leftrightarrow|Em_{\mathbb{F}}(\mathbb{E},\overline{\mathbb{F}})|=[\mathbb{E}:\mathbb{F}]$

设$\mathbb{F}\subseteq\mathbb{E}\subseteq K$是域扩张，若$\mathbb{E}$是$\mathbb{F}$的可分扩张，$K$是$\mathbb{E}$的可分扩张，则$K$是$\mathbb{F}$的可分扩张.

证明：设$\alpha\in K$，因为K是$\mathbb{E}$的可分(代数)扩张，存在极小多项式$P_{\mathbb{E}}(x)=\sum_{i=0}^{n}a_i x^i\in\mathbb{E}[x]$，(可分)，$P_{\mathbb{E}}(\alpha)=0$，考虑链：

$$\mathbb{F}\subset\mathbb{F}(a_0)\subseteq\mathbb{F}(a_0,a_1)\subseteq\cdots\subseteq\mathbb{F}(a_0,a_1,\cdots,a_n)\subseteq\underbrace{\mathbb{F}(a_0,\cdots,a_n,\alpha)}_{=\mathbb{L}}$$

因为$\mathbb{E}$是$\mathbb{F}$上可分扩张$\Rightarrow a_i\ \ i=0,\cdots,n$在$\mathbb{F}$上可分

$\Rightarrow a_i$在$\mathbb{F}(a_0,a_1,\cdots,a_{i-1})$上可分，$\alpha$在$\mathbb{F}(a_0,\cdots,a_n)$上可分

$[\mathbb{L}:\mathbb{F}(a_0,\cdots,a_n)]=\mathrm{Em}_{\mathbb{F}(a_0,\cdots,a_n)}(\mathbb{L},\overline{\mathbb{F}(a_0,\cdots,a_n)})$. 令$\mathbb{E}_i=\mathbb{F}(a_0,\cdots,a_i)$

$[\mathbb{L}:\mathbb{E}_{n-1}]=[\mathbb{L}:\mathbb{E}_n][\mathbb{E}_n:\mathbb{E}_{n-1}]$

$|\mathrm{Em}_{\mathbb{E}_{n-1}}(\mathbb{L},\overline{\mathbb{E}_{n-1}})|=|\mathrm{Em}_{\mathbb{E}_n}(\mathbb{L},\overline{\mathbb{E}_n})|\cdot\deg P_n(x)$ (正如(1)). $\left(\overline{\mathbb{E}_n}=\overline{\mathbb{E}_{n-1}}\right)$

其中$P_n(x)$是α_n在$\mathbb{E}_{n-1}$上极小多项式次数.

$\Rightarrow|\mathrm{Em}_{\mathbb{E}_{n-1}}(\mathbb{L},\overline{\mathbb{E}_{n-1}})|=[\mathbb{E}_n:\mathbb{E}_{n-1}][\mathbb{L}:\mathbb{E}_n]=[\mathbb{L}:\mathbb{E}_{n-1}]$

即$\mathbb{L}$是$\mathbb{E}_{n-1}$上可分扩张，递归得，$\mathbb{L}$是$\mathbb{F}$上可分扩张$\Rightarrow\alpha$可分元 (over $\mathbb{F}$)

注：(1) $\mathbb{F}\subseteq\mathbb{E}\subseteq K$不需要有限扩张.

(2) 反之，K是$\mathbb{F}$上可分$\Rightarrow K$在$\mathbb{E}$上可分，$\mathbb{E}$在$\mathbb{F}$上可分