练习 14.

1. 证明:

(1) $L=F(\alpha_1,\cdots,\alpha_n)$ 为 $f(x)$ 的分裂域，又 K/F 为可分扩张，即有 α 在 F 上可分，$f(x)$ 为可分多项式 $\Rightarrow$ L/F 为 Galois 扩张.

(2) $F(\alpha_1)=K$，$K\subset L$，$K\subset L'$.

$\alpha_1\in L'$，$f(x)\in F[x]$，$f(\alpha_1)=0$

$\Rightarrow$ $f(x)$ 的根均在 L' 中（L'/F 为 Galois 扩张）

$\Rightarrow$ $\alpha_i\in L'$ $\Rightarrow$ $L\subset L'$.

由此知 L 不依赖于 α 的选取.

2. 证明: $G=Gal(K/F)$，$|G|<+\infty$ $\Rightarrow$ G 的子群个数有限

$\Rightarrow$ K/F 的中间域只能有有限个（由 Galois 基本定理，K/F 的 Galois 群与 K/F 的中间域一一对应）.

设 K/F 为任意有限可分扩张，由 1. 知 $\exists$ 它的 Galois 闭包 L/F.

由于 L/F 的中间域有限 $\Rightarrow$ K/F 的中间域有限.

3. 证明: $G=Gal(K/F)$ $|G|<+\infty$，$G=\{\overset{id}{\sigma_1},\cdots,\sigma_n\}$

$$\sigma(f)=\prod_{\substack{\sigma_i\in G\\ 1\le i\le n}}(x-\sigma\sigma_i(\alpha))=\prod_{\substack{\sigma_i\in G\\ 1\le i\le n}}(x-\sigma_i(\alpha))=f$$

$\therefore$ $f\in F[x]$.

设 $g(x)$ 是 α 在 F 上的极小多项式，则 $g(x)\mid f(x)$

又 α 是 $g(x)$ 根，$\sigma(\alpha)$ 也是 $g(x)$ 根，且 $g(x)$ 无重根

故 $g(x)=\prod_{\substack{\sigma\in G\\ \sigma(\alpha)\text{互不相同}}}(x-\sigma(\alpha))$

$G\alpha=\{\sigma_1(\alpha),\cdots,\sigma_n(\alpha)\}$（其中有重复的）$\overset{\text{不妨设}}{=\!=}\{\alpha_1,\cdots,\alpha_m\}$，$\alpha_1,\cdots,\alpha_m$ 互不相同.

$H_i=\{\sigma\in G \mid \sigma(\alpha)=\alpha_i\}$，则 $G=\coprod_{1\le i\le m} H_i$

$H_1=\{\sigma\in G\mid \sigma(\alpha)=\alpha_1=\alpha\}=G_\alpha$

$\forall\ \alpha\in G_\alpha,\ \forall\ \sigma,\tau\in H_i \Rightarrow \sigma^{-1}\tau\in G_\alpha$

$\Rightarrow H_i\subseteq G_\alpha$

又 $\sigma G_\alpha\subseteq H_i \Rightarrow H_i=\sigma G_\alpha$ 故 $|H_i|=|G_\alpha|$

ii $f(x)=g(x)^{|G_\alpha|}$

特别地，若 f 为极小多项式，则 $|G_\alpha|=1$，可知 $|Gal(K/F(\alpha))|=1$

$\Rightarrow K=F(\alpha)$

若 α 为 K/F 的本原根，$K=F(\alpha)$

则 G 中元素完全由 α 在其上作用决定，可知 $|G_\alpha|=1$

$\Rightarrow f(x)=g(x)$

4. (1) E/F，$\mathrm{char}F=0$，$[E:F]=2$

$\forall\alpha\in E$，$\alpha\notin F$，α 在 F 上极小多项式为 $f(x)$

$f(x)=x^2+px+q$，α,β 是 $f(x)$ 根

$\alpha+\beta=-p \Rightarrow \beta=-p-\alpha\in E$

故 $F(\alpha,\beta)=F(\alpha)$，$[F(\alpha):F]=2$

$\Rightarrow E=F(\alpha)$，即 E 为 $f(x)$ 的分裂域，又 $f(x)$ 可分，

$\Rightarrow E/F$ 为 Galois 扩张

(2) $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\omega)$ 也是 3 次 Galois 扩张。

5. 证明

(1) 代入即可

(2) 设 β 是 $f(x)=x^3+x^2-2x-1$ 的第三个根，则由韦达定理

$$\alpha+(\alpha^2-2)+\beta=-1$$

$$\Rightarrow \beta=1-\alpha-\alpha^2$$

故 $E=\mathbb{Q}(\alpha)$ 为 $f(x)$ 的分裂域，又 $f(x)$ 可分

$\Rightarrow E/\mathbb{Q}$ 为 Galois 扩张.

练习 15

1. $\forall f \in \mathbb{Q}[x]$, $\deg f = n$, 则 $Gal(f) \hookrightarrow S_n$, 即 $Gal(f)$ 可看成 S_n 的子群.

(1) $n=2$ 时, 若 f 可约, 则 $f(x)$ 必在 $\mathbb{Q}[x]$ 上可裂, 即 $Gal(f) = \{id\}$.

若 f 不可约, 则 $Gal(f) \cong S_2$

(2) $n=3$ 时, f 可约, 则 f 必有一个有理根, 即 $f(x) = (x-a)g(x)$, $a \in \mathbb{Q}$.

当 $g(x)$ 可约时, 则 $Gal(f) = \{id\}$

当 $g(x)$ 不可约时, 则 $Gal(f) \cong S_2$

2. (1) 令 $\alpha = \sqrt[4]{2}(1+i)$, 则 $\alpha^2 = 2\sqrt{2}i$, $\alpha^3 = 2(\sqrt[4]{2}^3(-1))$, $\alpha^4 = -8$.

又 $f(x) = x^4 + 8$ 是 $\mathbb{Q}[x]$ 上不可约的, 故 α 在 $\mathbb{Q}$ 上的极小多项式为 x^4+8.

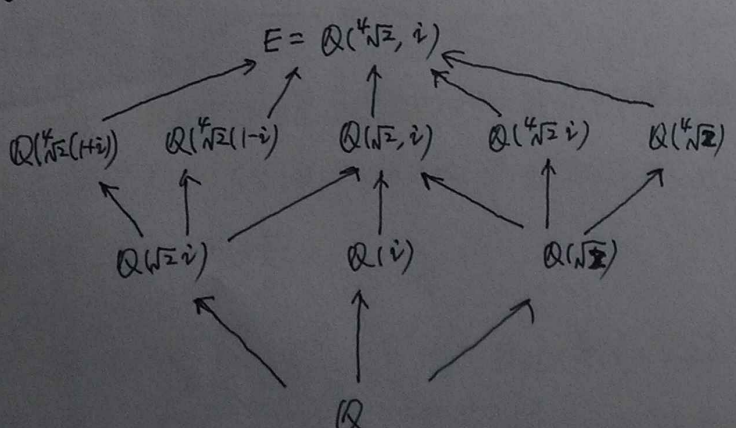
$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. $f(x)$ 的全部根为 $\pm\sqrt[4]{2}(1+i)$, $\pm\sqrt[4]{2}(1-i)$.

但 $\sqrt[4]{2}(1-i) \notin \mathbb{Q}(\alpha)$, 故 $\forall \sigma \in Gal(\mathbb{Q}(\sqrt[4]{2}(1+i))/\mathbb{Q})$, σ 只能把 α 变成 $\pm\alpha$.

因此 $Gal(\mathbb{Q}(\sqrt[4]{2}(1+i))/\mathbb{Q})$ 是 2 阶循环群.

(2) $\mathbb{Q}(\sqrt[4]{2}(1+i))$ 的所有中间域为 $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}i)$, $\mathbb{Q}(\sqrt[4]{2}(1+i))$.

$\mathbb{Q}(\sqrt[4]{2}(1+i))/\mathbb{Q}$ 不是伽罗瓦扩张, 它可以嵌在一个伽罗瓦扩张里.

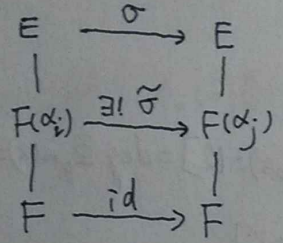


3. 证明：

$\Rightarrow$ 设 $f(x)$ 的根集合为 $X=\{\alpha_1,\cdots,\alpha_n\}$

$\forall \alpha_i, \alpha_j \in X$，$\alpha_i, \alpha_j$ 均是不可约多项式 $f(x)$ 的根，

则 $\exists!\ \tilde{\sigma}: F(\alpha_i)\longrightarrow F(\alpha_j)$, s.t. $\tilde{\sigma}|_F = id$.



然后将 $\tilde{\sigma}$ 延拓成 $f(x)$ 的分裂域 E 上的自同构 σ, s.t. $\sigma(\alpha_i)=\alpha_j$, $\sigma|_F = id$

即 $\exists \sigma \in Gal(f)$, $\sigma(\alpha_i)=\alpha_j$

因此 $Gal(f)$ 在根集合 X 上的作用是传递的.

$\Leftarrow$ 设 α_1 在 F 上的极小多项式为 $f_1(x)$，由于 $Gal(f)$ 在 X 上作用传递，则

$\forall \alpha_1, \alpha_i \in X$, $\exists \sigma_i \in Gal(f)$, s.t. $\sigma_i(\alpha_1)=\alpha_i$

$0=\sigma_i(f_1(\alpha_1)) = f_1(\sigma_i(\alpha_1)) = f_1(\alpha_i)$，因此 X 中元素均为 $f_1(x)$ 根.

故 $f \mid f_1$，因 $f_1(x)$ 在 $F[x]$ 上不可约，所以 $f(x)$ 也不可约.

4. (1). 证明：

$$\Phi_{p^m}(x+1)=\frac{(x+1)^{p^m}-1}{x^{p^{m-1}}-1} \equiv \frac{x^{p^m}}{x^{p^{m-1}}} = x^{p^{m-1}(p-1)} \pmod p$$

由此知，$\Phi_{p^m}(x+1)$ 除首项系数外，其余均被 p 整除，又 $\Phi_{p^m}(1)=p$，即 $\Phi_{p^m}(x+1)$ 的常数项为 p，故由 Eisenstein 判别法可知 $\Phi_{p^m}(x+1)$ 是不可约的，进而 $\Phi_{p^m}(x)$ 是不可约的.

(2) 设 $\sigma_k(\zeta_{p^m}^k)=\zeta_{p^m}^k$, $\forall \sigma \in Gal(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q})$

每个 $\sigma \in Gal(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q})$，它完全由在 ζ_{p^m} 上的取值决定.

因 $\zeta_{p^m}^k$ 也仍然是 p^m 次本原单位根，故 $(k, p^m)=1$.

先构造群同态：

$$\psi: Gal(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}) \longrightarrow (\mathbb{Z}/p^m\mathbb{Z})^\times$$
$$\sigma_k \longmapsto [k]$$

由 $\sigma_j\sigma_i(\zeta_{p^m}) = \sigma_j(\zeta_{p^m}^i) = (\zeta_{p^m}^i)^j = \zeta_{p^m}^{ij} = \zeta_{p^m}^{ji}$

$\therefore \psi(\sigma_j\sigma_i) = [ji] = \psi(\sigma_j)\psi(\sigma_i)$，即这是一个群同态.

单射显然，如果 $[k]=[l]$，即 $k \equiv l \bmod p^m$，则 $\exists q$, s.t $k = q\cdot p^m + l$

$\zeta_{p^m}^k = \zeta_{p^m}^{q\cdot p^m}\cdot\zeta_{p^m}^l = \zeta_{p^m}^l$，即 $\sigma_k = \sigma_l$.

现在说明 ψ 是满同态.

事实上，ζ_{p^m} 在 $\mathbb{Q}$ 的极小多项式为 Φ_{p^m}，故 $[\mathbb{Q}(\zeta_{p^m}):\mathbb{Q}] = \deg \Phi_{p^m}(x) = \varphi(p^m)$

而 $|(\mathbb{Z}/p^m\mathbb{Z})^\times| = \varphi(p^m)$，即 $[\mathbb{Q}(\zeta_{p^m}):\mathbb{Q}] = |(\mathbb{Z}/p^m\mathbb{Z})^\times|$

因此有 $Gal(\mathbb{Q}(\zeta_{p^m}):\mathbb{Q}) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$.

$(\mathbb{Z}/p^m\mathbb{Z})^\times$ 是 $\varphi(p^m) = p^{m-1}(p-1)$ 阶循环群，而 $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$ 也是 $(p-1)p^{m-1}$ 阶循环群，故 $(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$.

(3). 对一般的 n，我们只需说明 $\Phi_n(x)$ 是不可约的，即可得到 $Gal(\zeta_n\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

设 $f(x)$ 是 n 次本原单位根 $\zeta = \zeta_n$ 在 $\mathbb{Q}$ 上的极小多项式.

因为 $f(x) | (x^n-1)$，$f(x) \nmid (x^d-1)$，$\forall d<n$，故 $(f(x), x^d-1) = 1$，$f(x)$ 的根只能是 n 次本原单位根. 下证每个 n 次本原单位根必是 $f(x)$ 的根.

断言：对 $f(x)$ 的任一根 u 和与 n 互素的素数 p，u^p 也是 $f(x)$ 根.

反证：否则设 u^p 在 $\mathbb{Q}$ 上的极小多项式为 $g(x)$，由 $g(x) | (x^n-1)$.

$f(x) | x^n-1$，知 $f(x)g(x) | (x^n-1)$，于是 $x^n-1 = f(x)g(x)h(x)$. 由高斯引理知，$f(x), g(x), h(x)$ 均为整系数多项式，而 $g(x^p)$ 以 u 为根，故

$g(x^p) = g(x)f(x)$，$g(x) \in \mathbb{Z}[x]$.

在 $\mathbb{Z}_p[x]$ 中，我们有 $\overline{(g(x))^p} = \overline{g(x^p)}$

$\therefore \overline{(g(x))^p} = \overline{g(x)}\,\overline{f(x)}$，又 $(p,n)=1$，故 x^n-1 无重根，从而

由 $\overline{x^n-1} = x^n-\bar{1} = \bar{f}(x)\bar{g}(x)\bar{h}(x)$ 知 $(\bar{f}(x), \bar{g}(x)) = 1$，但这与 $\overline{(g(x))^p} = \overline{g(x)}\,\overline{f(x)}$ 式子矛盾. 故断言成立.

我们知道任一 n 次本原单位根形如 ζ_n^i, $(i,n)=1$, 设 $i=p_1\cdots p_s$, 其中 p_j 均为素数, 于是 $(n,p_j)=1$, $\forall j$. 反复使用上述断言, 即知 $\alpha\zeta_n^{p_1}, \cdots, \zeta_n^{p_1\cdots p_s}=\zeta_n^i$ 均是 $f(x)$ 的根, 从而任一 n 次本原单位根均是 $f(x)$ 的根. 由此 $f(x)=\Phi_n(x)$, $\Phi_n(x)$ 是不可约的.

5. 此题有点问题.

6. 参见《近世代数引论》(冯克勤著) 有关可解群部分内容

7. 证明：$|G|=n$. G 同构于 S_n 的子群.

设 K 为任意域，$x_1,\cdots,x_n$ 为 n 个文字，$P_1,\cdots,P_n$ 是它们的初等对称函数，即 $P_1=\sum_{i=1}^{n} x_i$，$P_2=\sum_{1\le i<j\le n} x_i x_j$，$\cdots$，$P_n=x_1\cdots x_n$

则 $K(x_1,\cdots,x_n)/K(P_1,\cdots P_n)$ 是 Galois 扩张且它的 Galois 群为 S_n（此可参见教材）.

设 $\overline{G}\le S_n$，且 $\overline{G}\cong G$.

$K(P_1,\cdots,P_n)\subset M=K(x_1,\cdots,x_n)^{\overline{G}}\subset K(x_1,\cdots,x_n)$

则 $K(x_1,\cdots,x_n)/M$ 为 Galois 扩张，且其 Galois 群恰为 $\overline{G}\cong G$.