13. Fundamental theorem of Galois theory (Chapter 17.2)

Theorem 13.1. (FTGT) Let $F \subseteq E$ be a Galois field extension. Then there are mutually inverse bijections

$$\{\text{subgroups } H \leq G(E/F)\} \longleftrightarrow \{\text{intermediate fields } F \subseteq k \subseteq E\}$$
$$H \longmapsto E_H$$
$$G(E/k) \longmapsto k,$$

that is

(1) If $F \subseteq k \subseteq E$ is an intermediate field, then $k = E_{G(E/k)}$.

(2) If $H \leq G(E/F)$ is a subgroup, then $H = G(E/E_H)$.

Moreover, if $F \subseteq k \subseteq E$ is an intermediate field, then

(3) $[E:k] = |G(E/k)|$ and $[k:F] = |G(E/F)| / |G(E/k)|$.

(4) If $G(E/k)$ is a normal subgroup of $G(E/F)$, then for every $\sigma \in G(E/F)$, we have $\sigma(k) = k$.

(5) $G(E/k)$ is a normal subgroup of $G(E/F)$ if and only if $F \subseteq k$ is normal.

(6) If $F \subseteq k$ is normal, then $G(k/F) \cong G(E/F)/G(E/k)$.

Proof. First note that if $F \subseteq k \subseteq E$, then $G(E/k) \leq G(E/F)$. Moreover, $F \subseteq E$ Galois $\Rightarrow$ $F \subseteq E$ finite, normal, separable and

$F \subseteq E$ finite $\Rightarrow$ $F \subseteq k$, $k \subseteq E$ finite $\Rightarrow F \subseteq k$, $k \subseteq E$ algebraic

$F \subseteq E$ separable $\Rightarrow$ every $\alpha \in E$ is separable over F

$\Rightarrow$ every $\alpha \in E$ is separable over $k \supseteq F$ $\Rightarrow$ $F \subseteq k$, $k \subseteq E$ separable
every $\alpha \in k \subseteq E$ is separable over F

$F \subseteq E$ normal $\Rightarrow$ E is the splitting field of some polynomials in $F \subseteq k \Rightarrow k \subseteq F$ normal

So $k \subseteq E$ is also Galois, while $F \subseteq k$ is finite and separable.

(1) Since $k \subseteq E$ is Galois, the claim follows by Theorem 12.12.

(2) This follows by Theorem 12.11.

(3) By Theorem 12.12, and since $F \subseteq E$, $k \subseteq E$ are Galois, we have $|G(E/F)| = [E:F]$ and $|G(E/k)| = [E:k]$. Since $F \subseteq E$ is finite,

we have $[E:F]=[E:K][K:F]$. Hence
$$[K:F]=[E:F]/[E:K]=|G(E/F)|/|G(E/K)|.$$
(4) Let $\theta\in G(E/K)$ and $\sigma\in G(E/F)$. Since $G(E/K)\triangleleft G(E/F)$, we have that $\sigma^{-1}\theta\sigma\in G(E/K)$. Hence if $k\in K$ we have $\sigma^{-1}\theta\sigma(k)=k$. Applying σ in both sides we obtain $\theta(\sigma(k))=\sigma(k)$. Then $\forall k\in K$ we have
$$\sigma(k)\in\{\alpha\in E\mid\theta(\alpha)=\alpha\ \forall\theta\in G(E/K)\}=:E_{G(E/K)}\overset{(1)}{=}K.$$
Hence $\sigma(K)\subseteq K$ and since σ is an automorphism of E we conclude that $\sigma(K)=K$.
(5)($\Rightarrow$): Let $\sigma:K\longrightarrow\bar{F}$ be an embedding with $\sigma|_F=id_F$. By Theorem 8.5 to show that $F\subseteq K$ is normal it is enough to show that $\sigma(K)=K$. By Theorem 6.5 we have that σ can be extended to an embedding $\sigma^*:E\longrightarrow\bar{F}$. Since $F\subseteq E$ is normal, we have that $\sigma^*(E)=E$ by Theorem 8.5. In particular we have $\sigma^*\in G(E/F)$. Then by (4) we have that $\sigma^*(K)=K$. Since $\sigma^*|_K=\sigma$, we have $\sigma(K)=K$ as required.
($\Leftarrow$): Assume $F\subseteq K$ is normal. Let $\theta\in G(E/K)$ and $\sigma\in G(E/F)$ and we need to show that $\sigma\theta\sigma^{-1}\in G(E/K)$. Since $\sigma\in G(E/F)$, $\sigma:E\longrightarrow E$ is an automorphism with $\sigma|_F=id_F$. Since $E\subseteq\bar{F}$, we may extend σ to an embedding $\bar{\sigma}:E\longrightarrow\bar{F}$ with $\bar{\sigma}|_E=\sigma$. Since $F\subseteq K$ is normal, the embedding $\bar{\sigma}|_K:K\longrightarrow\bar{F}$ is an F-automorphism of K by Theorem 8.5. To show that $\sigma\theta\sigma^{-1}\in G(E/K)$, we need to show that $\sigma\theta\sigma^{-1}(\alpha)=\alpha$ for all $\alpha\in K$. If $\alpha\in K$, then $\sigma^{-1}(\alpha)=\bar{\sigma}|_K^{-1}(\alpha)\in K$ since $\bar{\sigma}|_K$ is an F-automorphism of K. Since $\theta\in G(E/K)$, we have
$$\sigma\theta\sigma^{-1}(\alpha)=\bar{\sigma}|_K(\theta(\bar{\sigma}^{-1}|_K(\alpha)))=\bar{\sigma}|_K(\bar{\sigma}^{-1}|_K(\alpha))=\alpha,$$
as required
(6) Since $F\subseteq K$ is normal, we have that $G(E/K)\triangleleft G(E/F)$ and so $G(E/F)/G(E/K)$ makes sense. We define a map
$$\psi:G(E/F)\longrightarrow G(K/F)$$

by $\psi(\sigma) = \sigma|_K$. We check the following properties.
(i) ψ is well-defined: Since $(\sigma|_K)|_F = \sigma|_F = id_F$, we only need to show that if $\sigma \in G(E/F)$, then $\sigma(K) = K$. But this follows from (4).
(ii) ψ is a group homomorphism: $\psi(\tau\circ\sigma) = (\tau\circ\sigma)|_K \overset{(i)}{=} \tau|_K \circ \sigma|_K = \psi(\tau)\circ\psi(\sigma)$.
(iii) $\ker\psi = G(E/K)$: We have

$$\ker\psi = \{\sigma \in G(E/F) \mid \sigma|_K = id|_K\} = G(E/K).$$

Then we have

$$\mathrm{Im}\,\psi \cong {}^{G(E/F)}/_{\ker\psi} = {}^{G(E/F)}/_{G(E/K)}.$$

And so we have

$$|\mathrm{Im}\,\psi| = {}^{|G(E/F)|}/_{|G(E/K)|} \overset{(3)}{=} [K:F] \overset{\text{Theorem 11.12}}{=} |G(K/F)|.$$

Since $\mathrm{Im}\,\psi \subseteq G(K/F)$, we conclude that $\mathrm{Im}\,\psi \cong G(K/F)$ and the claim follows. □

Example 13.2. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ is a Galois extension (it is finite by Example 5.5, normal by Example 8.3, and separable since $\mathbb{Q}$ is a perfect field). In particular if $E = \mathbb{Q}(\sqrt{2},\sqrt{3})$, then

$$E = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\}.$$

If $\sigma \in G(E/\mathbb{Q})$, then

$$2 = \sigma(2) = \sigma(\sqrt{2}\cdot\sqrt{2}) = \sigma(\sqrt{2})\,\sigma(\sqrt{2}) = \sigma(\sqrt{2})^2 \Rightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$$

and similarly $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Hence $G(E/\mathbb{Q}) = \{\sigma_{++}, \sigma_{+-}, \sigma_{-+}, \sigma_{--}\}$ where

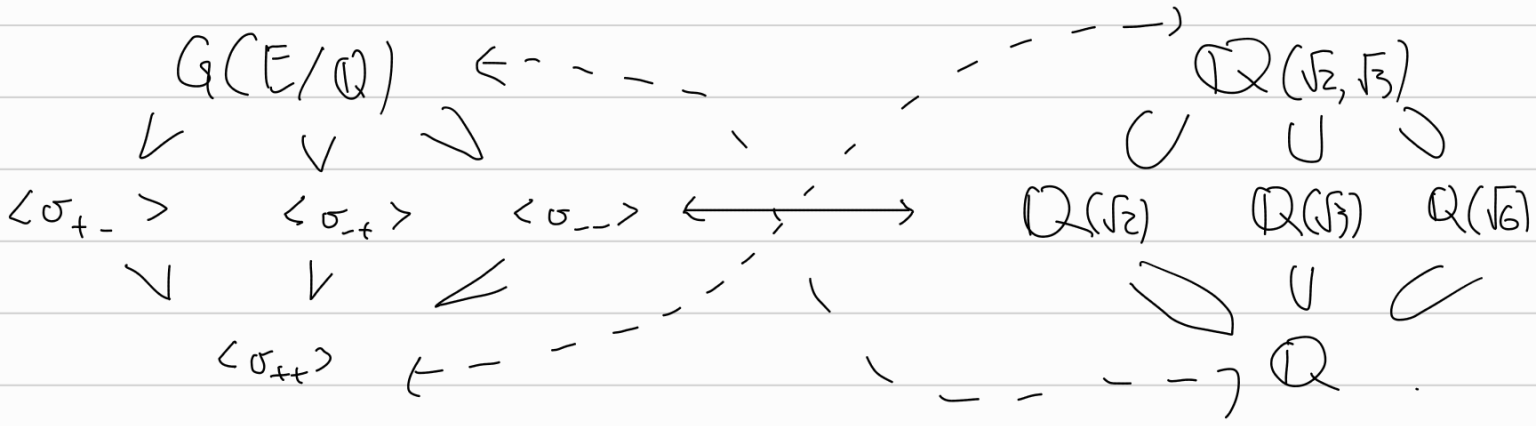
$$\sigma_{++} = id_E$$

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \begin{cases} \xrightarrow{\sigma_{+-}} a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\ \xrightarrow{\sigma_{-+}} a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\ \xrightarrow{\sigma_{--}} a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \end{cases}$$

Since $\sigma^2 = id_E$ for all $\sigma \in G(E/\mathbb{Q})$ and $|G(E/\mathbb{Q})| = 4$, we conclude that $G(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Then

$$E_{\langle\sigma_{+-}\rangle} = \{\alpha \in E \mid \sigma_{+-}(\alpha) = \alpha\} = \mathbb{Q}(\sqrt{2}),$$
$$E_{\langle\sigma_{-+}\rangle} = \{\alpha \in E \mid \sigma_{-+}(\alpha) = \alpha\} = \mathbb{Q}(\sqrt{3}),$$
$$E_{\langle\sigma_{--}\rangle} = \{\alpha \in E \mid \sigma_{--}(\alpha) = \alpha\} = \mathbb{Q}(\sqrt{6}),$$

and we have the correspondence


$G(E/\mathbb{Q})$
$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$\langle \sigma_{+-} \rangle$
$\langle \sigma_{-+} \rangle$
$\langle \sigma_{--} \rangle$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(\sqrt{3})$
$\mathbb{Q}(\sqrt{6})$
$\langle \sigma_{++} \rangle$
$\mathbb{Q}$