12. Galois groups (Chapter 17.1)

$F \subseteq E$ – field extension

<u>Notation 12.1.</u> (1) A map $\sigma: E \to E$ is called an <u>automorphism</u> if σ is a ring isomorphism. We denote

$$Aut(E) = \{\sigma: E \to E \mid \sigma \text{ is an automorphism}\}.$$

Note that $Aut(E)$ is a group under composition:

$$\sigma, \theta \in Aut(E) \Rightarrow \sigma \circ \theta \in Aut(E)$$

$$1_E \in Aut(E)$$

$$\sigma \in Aut(E) \Rightarrow \sigma^{-1} \in Aut(E).$$

(2) An automorphism $\sigma: E \to E$ is called an <u>F-automorphism</u> if $\sigma|_F = id_F$. We denote

$$G(E/F) = \{\sigma: E \to E \mid \sigma \text{ is an } F\text{-automorphism}\}$$
$$= \{\sigma \in Aut(E) \mid \sigma|_F = id_F\}.$$

It is easy to see that $G(E/F) < Aut(E)$.

<u>Definition 12.2.</u> (1) $F \subseteq E$ is called a <u>Galois extension</u> if it is finite, normal and separable.

(2) If $F \subseteq E$ is a Galois extension, then $G(E/F)$ is called the <u>Galois group</u> of the extension.

(3) If $F \subseteq E$ is a Galois extension, by Proposition 8.4 E is the splitting field of some polynomial $f(x) \in F[x]$. In this case the Galois group $G(E/F)$ is also called the <u>Galois group of $f(x)$ over F</u>.

<u>Remark 12.3.</u> Galois extensions can more generally be defined as field extensions which are algebraic, normal and separable (finite $\Rightarrow$ algebraic, but the opposite is not tru in general). Also other sources may call $G(E/F)$ a

Galois group without $F \subseteq E$ being Galois.

Main idea of Galois theory: study a Galois extension $F \subseteq E$ through studying the Galois group $G(E/F)$.

Example 12.4. (1) $\mathbb{R} \subseteq \mathbb{C}$ is finite since $[\mathbb{C}:\mathbb{R}]=2$. Moreover, $\mathbb{C}$ is the splitting field of $x^2+1 \in \mathbb{R}[x]$ and so $\mathbb{R} \subseteq \mathbb{C}$ is normal. Since $x^2+1=(x+i)(x-i)$ in $\mathbb{C}[x]$, the extension is also separable and hence Galois. By Example 5.13 we have

$$G(\mathbb{C}/\mathbb{R}) = \{\sigma, \bar{\sigma} : \mathbb{C} \longrightarrow \mathbb{C} \mid \sigma = id_{\mathbb{C}},\ \bar{\sigma}(a+bi)=a-bi\}.$$

Note that $|G(\mathbb{C}/\mathbb{R})| = 2 = [\mathbb{C}:\mathbb{R}]$; this is not a coincidence and we will see that this is always the case.

(2) Let E be the splitting field of a collection of polynomials $\{f_1(x), \dots, f_n(x)\} \subseteq F[x]$. Then $F \subseteq E$ is finite and normal by Proposition 8.4. If $char(F)=0$ or F is finite, then F is perfect and so $F \subseteq E$ is also separable. Hence in this case $F \subseteq E$ is Galois.

(3) From (2) it follows that if E is the splitting field of a polynomial $f(x) \in \mathbb{Q}[x]$, then $\mathbb{Q} \subseteq E$ is Galois.

We now proceed with the study of $G(E/F)$. We first define the set

$$Emb_F(E) = \{\sigma : E \longrightarrow E \mid \sigma|_F = id_F\}.$$

Lemma 12.5. Let $E=F(\alpha)$ with α algebraic over F. Let $p_\alpha(x)$ be the minimal polynomial of α over F. Then

$$|Emb_F(E)| = |\{r \in E \mid p_\alpha(r)=0\}| \le deg(p_\alpha) = [E:F].$$

Proof. By Lemma 6.4 $\exists$ ring homomorphism $\sigma^* : E \to E^*$ making the diagram

$$\begin{tikzcd} F \arrow[r, hook, "\iota_{\bar{E}}"] \arrow[d, hook, "\iota_E"'] & \bar{E} \\ F(\alpha)=E' \arrow[ur, "\sigma^*"'] & \end{tikzcd}$$

$\iota_{\bar{E}}$ = inclusion of F to $\bar{E}$

ι_E = inclusion of F to E

commute and there are as many such σ^* as there are distinct roots of $p_\alpha(x)$. The claim follows. $\square$

<u>Theorem 12.6</u> (1) If $F \subseteq E$ is finite, then $|G(E/F)| \leq [E:F]$.
(2) If $E \subseteq F$ is finite and separable, then $[E:F] = |\mathrm{Emb}_F(E)|$. Moreover, in this case, $|G(E/F)| = [E:F]$ if and only if $F \subseteq E$ is normal

<u>Proof</u>. (1) Since $F \subseteq E$ is finite, it follows that $F \subseteq E$ is finitely generated and algebraic. Hence $\exists$ algebraic elements $\alpha_1, \dots, \alpha_n \in E$ such that $E = F(\alpha_1, \dots, \alpha_n)$. Since $E \subseteq \bar{E}$, we have $G(E/F) \subseteq \mathrm{Emb}_F(E)$. We show that $|\mathrm{Emb}_F(E)| \leq [E:F]$ using induction on n.

For the case $n=1$ we have $E = F(\alpha)$. Let $p_\alpha(x)$ be the minimal polynomial of α over F. By Lemma 12.5 we have

$$|\mathrm{Emb}_F(E)| \leq \deg(p_\alpha) = [E:F],$$

as claimed.

Now let $n \geq 2$ and let $E' = F(\alpha_1, \dots, \alpha_{n-1})$. Then

$$F \subseteq E' \subseteq E \subseteq \bar{E}$$

and $E = E'(\alpha_n)$. Let $p_{\alpha_n}(x) \in E'[x]$ be the minimal polynomial of α over E'. Moreover, let $\{r_1, \dots, r_d\}$ be the set of roots of $p_{\alpha_n}(x)$. We claim that $|\mathrm{Emb}_F(E)| = |\mathrm{Emb}_F(E')| \cdot d$. By Lemma 6.4 we have that for each $\sigma \in \mathrm{Emb}_F(E')$ there exists $\sigma^*: E \to \bar{E}$ such that the diagram

$$\begin{tikzcd} E' \arrow[r, hook, "\sigma"] \arrow[d, hook, "\iota_E"'] & \bar{E} \\ E=E'(\alpha_n) \arrow[ur, "\sigma^*"'] & \end{tikzcd}$$

ι_E = inclusion of E' to E

commutes. Moreover we know that there exist d different such σ^*, say $\{\sigma_1, \dots, \sigma_d\}$. In particular we have

$$\sigma_i = \sigma_j \implies i = j \qquad \forall\, i,j \in \{1, \dots, d\} \qquad (1).$$

Then the map

$$\begin{aligned} \mathrm{Emb}_F(E') \times \{1, \dots, d\} &\longrightarrow \mathrm{Emb}_F(E) \\ (\sigma, i) &\longmapsto \sigma_i \end{aligned}$$

is well-defined. Moreover it is injective since if $\sigma_i = r_j$, then $\sigma_i|_{E'} = r_j|_{E'} \implies \sigma = r$ and so $\sigma_i = \sigma_j \overset{(1)}{\implies} i = j$. It is also surjective since if $\sigma \in \mathrm{Emb}_F(E)$, then $\sigma|_{E'} \in \mathrm{Emb}_F(E')$ and so $\sigma = (\sigma|_{E'})_i$ for some $1 \le i \le j$. Hence $|\mathrm{Emb}_F(E)| = |\mathrm{Emb}_F(E')| \cdot d$ as claimed. Since $d \le \deg(P_{\alpha_n}(x))$ and since $|\mathrm{Emb}_F(E')| \le [E':F]$ by induction assumption, we have $|\mathrm{Emb}_F(E)| \le |\mathrm{Emb}_F(E')| \cdot \deg(P_{\alpha_n}) = [E':F][E:E'] = [E:F]$.

(2) By Theorem 11.3 we have that $E = F(\alpha)$. Let $P_\alpha(x)$ be the minimal polynomial of α over F. Then, since $F \subseteq E$ is separable, we have $|\{r \in E \mid P_\alpha(r) = 0\}| = \deg(P_\alpha)$ and it follows by Lemma 12.5 that $|\mathrm{Emb}_F(E)| = [E:F]$.

Now Theorem 8.5. says that $F \subseteq E$ is normal if and only if $\mathrm{Emb}_F(E) = G(E/F)$. Since $|\mathrm{Emb}_F(E)| = [E:F]$ and $G(E/F) \subseteq \mathrm{Emb}_F(E)$, this is equivalent to $|G(E/F)| = [E:F]$. $\square$

<u>Corollary 12.7.</u> If $F \subseteq E$ is Galois, then $|G(E/F)| = [E:F]$. In particular, Galois groups are finite.

<u>Proof.</u> Follows immediately from Theorem 12.6(2). $\square$

<u>Lemma 12.8.</u> Let $\sigma_1, \dots, \sigma_n : F \to E$ be distinct embeddings. Then $\sigma_1, \dots, \sigma_n$ are linearly independent, that is, if

$$a_1\sigma_1(\alpha) + \dots + a_n\sigma_n(\alpha) = 0 \qquad \forall\, \alpha \in F,$$

then $a_1 = \dots = a_n = 0$.

Proof. We use induction on n. For $n=1$ we have $a_1\sigma_1(\alpha)=0\ \forall \alpha\in F$ $\Rightarrow a_1=0$ since $\sigma(1_F)\neq 0$. Let $n>1$ and assume that

$$a_1\sigma_1(\alpha)+\cdots+a_n\sigma_n(\alpha)=0 \qquad \forall \alpha\in F. \qquad (1)$$

Assume to a contradiction that $a_n\neq 0$. Set $b_i:=a_n^{-1}a_i$ and multiply (1) by a_n^{-1} to obtain

$$b_1\sigma_1(\alpha)+\cdots+b_{n-1}\sigma_{n-1}(\alpha)+\sigma_n(\alpha)=0 \qquad \forall \alpha\in F. \quad (2)$$

Let $\beta\in F$ be such that $\sigma_1(\beta)\neq\sigma_n(\beta)$ and $\sigma_n(\beta)\neq 0$. Then (2) gives

$$b_1\sigma_1(\beta\alpha)+\cdots+b_{n-1}\sigma_{n-1}(\beta\alpha)+\sigma_n(\beta\alpha)=0 \qquad \forall \alpha\in F$$

$$\Rightarrow b_1\sigma_1(\beta)\sigma_1(\alpha)+\cdots+b_{n-1}\sigma_{n-1}(\beta)\sigma_{n-1}(\alpha)+\sigma_n(\beta)\sigma_n(\alpha)=0 \qquad \forall \alpha\in F$$

$$\Rightarrow b_1\sigma_n(\beta)^{-1}\sigma_1(\beta)\sigma_1(\alpha)+\cdots+b_{n-1}\sigma_n(\beta)^{-1}\sigma_{n-1}(\beta)\sigma_{n-1}(\alpha)+\sigma_n(\alpha)=0 \qquad \forall \alpha\in F \quad (3)$$

Subtracting (3) from (2) we obtain

$$(1-\sigma_n(\beta)^{-1}\sigma_1(\beta))b_1\sigma_1(\alpha)+\cdots+(1-\sigma_n(\beta)^{-1}\sigma_{n-1}(\beta))b_{n-1}\sigma_{n-1}(\alpha)=0 \qquad \forall \alpha\in F$$

and so by induction assumption $1-\sigma_n(\beta)^{-1}\sigma_1(\beta)=0$. This implies $\sigma_1(\beta)=\sigma_n(\beta)$, a contradiction. Hencen $a_n=0$. By induction assumption on (1) we also obtain $a_1=\cdots=a_{n-1}$, as required. □