SECTION 50 – SPLITTING FIELDS

Our main object of study is an algebraic field extension $F \leq E$, and the group $G(E/F)$ of automorphisms of E over F. The isomorphism extension theorem tells us that E is always isomorphic to a subfield of $\overline{F}$, so we will assume that $E \leq \overline{F}$. Last time we looked at the set of $\tau\colon E \to \overline{F}$ such that τ fixes F. Such a homomorphism may or may not define an automorphism of E:

Example. The conjugates $\sqrt{2}, -\sqrt{2}$ have the property that $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, so $\psi_{\sqrt{2},-\sqrt{2}}\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ is an element of $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Example. The conjugates of $\sqrt[3]{2}$ in $\overline{\mathbb{Q}}$ are the zeros of $\operatorname{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, namely

$$\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2},$$

where $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Since $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$ and $\omega^i\sqrt[3]{2} \notin \mathbb{R}$ for $i = 1, 2$, the homomorphisms $\psi_{\sqrt[3]{2},\omega^i\sqrt[3]{2}}$ do not give automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ for $i = 1, 2$.

Example. Let $\alpha, \beta \in \overline{F}$ be conjugate and of degree n over F, and consider $\psi_{\alpha,\beta}\colon F(\alpha) \to F(\beta)$. If $\beta \in F(\alpha)$, then $\psi_{\alpha,\beta}$ defines a map $F(\alpha) \to F(\alpha)$, since for $a_0, \ldots, a_{n-1} \in F$

$$\psi_{\alpha,\beta}(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1} \in F(\alpha).$$

One can check that $\psi_{\alpha,\beta}\colon F(\alpha) \to F(\alpha)$ is an isomorphism,[1] so that $\psi_{\alpha,\beta} \in G(F(\alpha)/F)$. On the other hand, if $\beta \notin F(\alpha)$, then $\psi_{\alpha,\beta}(\alpha) = \beta \notin F(\alpha)$, so $\psi_{\alpha,\beta}$ does not give an automorphism of $F(\alpha)$.

Today we study the field extensions $F \leq E$ such that every homomorphism $\tau\colon E \to \overline{F}$ gives an automorphism of E.

Definition. Let F be a field, and let $\{f_i(x) \mid i \in I\}$ be a set of polynomials in $F[x]$. The **splitting field** of the $f_i(x)$ over F is the smallest field $E \leq \overline{F}$ such that every zero of $f_i(x)$ in $\overline{F}$ lies in E.

Definition. A field $E \leq \overline{F}$ is **a splitting field** if there exists some set of polynomials for which it is the splitting field.

If the set $\{f_i(x) \mid i \in I\}$ is finite, the splitting field can then be described as follows.

Lemma. *Let $f_1(x), \ldots, f_n(x) \in F[x]$ be polynomials, and let E be the splitting field of the $f_i(x)$. Then E is also the splitting field of $f(x) = \prod_{i=1}^n f_i(x)$. If $\alpha_1, \ldots, \alpha_m \in \overline{F}$ are all the zeros of all the $f_i(x)$, we have*

$$E = F(\alpha_1, \ldots, \alpha_m).$$

---

[1] We know that $\psi_{\alpha,\beta}\colon F(\alpha) \to F(\beta)$ is an isomorphism. We have $F(\beta) = \psi_{\alpha,\beta}[F(\alpha)] \leq F(\alpha)$. Therefore

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

so $[F(\alpha) : F(\beta)] = 1$. Then $F(\beta) = F(\alpha)$, and $\psi_{\alpha,\beta}$ is an automorphism of $F(\alpha)$.

Proof. An element $\alpha \in \overline{F}$ is a zero of some $f_i(x)$ if and only if it is a zero of $f(x)$. Since E is the smallest field containing every zero of some $f_i(x)$, it's also the smallest field containing every zero of $f(x)$. This is by definition the same thing as $F(\alpha_1, \ldots, \alpha_m)$. □

Example. The splitting field of x^2-2 over $\mathbb{Q}$ is the smallest subfield of $\overline{\mathbb{Q}}$ containing $\sqrt{2}$ and $-\sqrt{2}$, which is $\mathbb{Q}(\sqrt{2})$.

We can also show that $\mathbb{Q}(\sqrt{2})$ is a splitting field in other ways,. The polynomial $(x^2-2)^2$ also has zeros $\pm\sqrt{2}$, so its splitting field is $\mathbb{Q}(\sqrt{2})$. The polynomial x^2-8 has splitting field

$$\mathbb{Q}(\sqrt{8}, -\sqrt{8}) = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(2\sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

Example. Let's compute the splitting field E of $x^3 - 2$ over $\mathbb{Q}$. The zeros of the polynomial are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, so we have $E = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$.

It is easy to see that

$$1 + \omega + \omega^2 = 0$$

which gives that

$$\omega^2\sqrt[3]{2} = -\sqrt[3]{2} - \omega\sqrt[3]{2},$$

so $\omega^2\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2})$. Hence $E = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2})$.

Let us compute the degree $[E : \mathbb{Q}]$. We have $\mathbb{Q} < \mathbb{Q}(\sqrt[3]{2}) \leq E$, and since $\deg(\sqrt[3]{2}, \mathbb{Q}) = 3$, we have

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3[E : \mathbb{Q}(\sqrt[3]{2})].$$

Now observe that

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2} + (\sqrt[3]{2})^2)$$

Letting $f(x) = x^2 + \sqrt[3]{2} + (\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})[x]$, we see that the zeros of $f(x)$ are $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. Since $f(x)$ has no real zeros and is of degree 2, $f(x)$ is irreducible over $\mathbb{R}$ and so irreducible over $\mathbb{Q}(\sqrt[3]{2})$. Since $\omega\sqrt[3]{2}$ is a zero of $f(x)$, we must then have that $\operatorname{irr}(\omega\sqrt[3]{2}, \mathbb{Q}(\sqrt[3]{2})) = f(x)$. It follows that

$$[E : \mathbb{Q}(\sqrt[3]{2})] = \deg(\omega\sqrt[3]{2}, \mathbb{Q}(\sqrt[3]{2})) = \deg f(x) = 2,$$

so

$$[E : \mathbb{Q}] = 6.$$

One basis for E over $\mathbb{Q}$ is given by

$$1, \sqrt[3]{2}, \sqrt[3]{2}^2, \omega\sqrt[3]{2}, \omega\sqrt[3]{2}^2, 2\omega$$

Example. The field $\overline{F}$ is the splitting field for the set $\{f_i(x) \mid i \in I\}$ of *all* polynomials in $F[x]$. Indeed, every element of α is a zero of $\operatorname{irr}(\alpha, F)$, so the splitting field of this set must contain every $\alpha \in \overline{F}$.

Theorem. *Let $F \leq E \leq \overline{F}$ be a tower of fields. The following conditions are equivalent*

1. *The field E is a splitting field over F*
2. *Every automorphism $\psi\colon \overline{F} \to \overline{F}$ fixing F gives an automorphism of E.*
3. *Every homomorphism $\tau\colon E \to \overline{F}$ fixing F gives an automorphism of E.*

Proof. (1) ⇒ (2): We assume for simplicity that E is a splitting field for a finite set of polynomials $f_1(x), \ldots, f_m(x) \in F[x]$, and so it is the splitting field of a single polynomial $f(x) = \prod_{i=1}^{m} f_i(x) \in F[x]$. Let $\alpha_1, \ldots, \alpha_m \in \overline{F}$ be the zeros of $f(x)$ so that we have $E = F(\alpha_1, \ldots, \alpha_n)$.

Let $\tau\colon \overline{F} \to \overline{F}$ be an automorphism of $\overline{F}$ fixing F. Then for each $i = 1, \ldots, n$, we have that

$$f(\tau(\alpha_i)) = \tau(f(\alpha_i)) = \tau(0) = 0,$$

Since $\tau(\alpha_i)$ is a zero of $f(x)$, we must have $\tau(\alpha_i) = \alpha_j$ for some j. Therefore τ sends $F(\alpha_1, \ldots, \alpha_n)$ to $F(\alpha_1, \ldots, \alpha_n)$.

It remains to see that $\tau\colon F(\alpha_1, \ldots, \alpha_n) \to F(\alpha_1, \ldots, \alpha_n)$ is an isomorphism. Since τ is a field homomorphism, it is automatically injective, and it remains to see that it is surjective.

The same argument as above applied to $\tau^{-1}\colon \overline{F} \to \overline{F}$ shows that τ^{-1} sends $F(\alpha_1, \ldots, \alpha_n)$ to $F(\alpha_1, \ldots, \alpha_n)$. Therefore, for every $\beta \in F(\alpha_1, \ldots, \alpha_n)$, we have

$$\beta = \tau(\tau^{-1}(\beta))$$

with $\tau^{-1}(\beta) \in F(\alpha_1, \ldots, \alpha_n)$, so τ is surjective.

(2) ⇒ (3): If $\tau\colon E \to \overline{F}$ is a homomorphism fixing F, the isomorphism extension theorem says there is an automorphism $\psi\colon \overline{F} \to \overline{F}$ such that $\psi(b) = \tau(b)$ for $b \in E$. Assumption (2) says that ψ induces an automorphism of E, and therefore τ gives an automorphism of E.

(3) ⇒ (1): Omitted.

□

Example. We saw above that $\psi_{\sqrt[3]{2},\omega\sqrt[3]{2}}\colon \mathbb{Q}(\sqrt[3]{2}) \to \overline{\mathbb{Q}}$ does not map $\mathbb{Q}(\sqrt[3]{2})$ to $\mathbb{Q}(\sqrt[3]{2})$ so $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field.

Corollary. *If $E \leq \overline{F}$ is a splitting field such that $E \leq F$ is finite, we have*

$$|G(E/F)| = \{E : F\}$$

Proof. The left hand side counts automorphisms of E fixing F. The right hand side counts homomorphisms $\tau\colon E \to \overline{F}$ fixing F. In general, every automorphism of E is a homomorphism $E \to \overline{F}$. Since E is a splitting field, the above theorem says that every homomorphism $E \to \overline{F}$ is an automorphism of E. □

Example. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field over $\mathbb{Q}$ of $x^2 - 2, x^2 - 3$. We have previously seen that $|G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}| = 4$ and that $\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\} = 4$.

1. Splitting polynomials

Definition. Let $F \leq E$ be a field extension, and let $f(x) \in F[x]$. We say that $f(x)$ splits in E if and only if $f(x)$ is a product of linear factors in $E[x]$.

Example. $x^2 + 1 \in \mathbb{R}[x]$ splits in $\mathbb{C}$, since $x^2 + 1 = (x + i)(x - i)$.

Example. The polynomial $x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ splits in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as

$$x^4 - 5x^2 + 6 = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3}).$$

Example. Every nonconstant polynomial $f(x) \in F[x]$ splits in $\overline{F}$.

Theorem. *Let E be a splitting field over F, and let $f(x) \in F[x]$ be irreducible. Then the following are equivalent*

(1) $f(x)$ *has a zero in* E.
(2) $f(x)$ *splits in* E.

Proof. (2) $\Rightarrow$ (1): If $f(x) = (a_1x + b_1)\dots(a_nx + b_n)$ with $a_i, b_i \in E$, then $-\frac{b_1}{a_1} \in E$ is a zero of $f(x)$.

(1) $\Rightarrow$ (2): Let $\alpha \in E$ be a zero of $f(x)$. Multiplying by a constant, we can assume $f(x)$ is monic, so $f(x) = \operatorname{irr}(\alpha, F)$. In $\overline{F}[x]$, we have a splitting

$$f(x) = c(x - \alpha)(x - \alpha_2)(x - \alpha_3)\cdots(x - \alpha_n),$$

where $c \in F$ and the $\alpha_i \in \overline{F}$. Since $f(x)$ is irreducible, we have $f(x) = \operatorname{irr}(\alpha_i, F)$ for all i, and so the α_i are conjugates of α over F.

Consider now $\psi_{\alpha,\alpha_i} \colon F(\alpha) \to F(\alpha_i)$. We may extend this to an automorphism $\tau \colon \overline{F} \to \overline{F}$ fixing F. Since E is a splitting field, τ induces an automorphism of E, and in particular $\tau(\alpha) = \psi_{\alpha,\alpha_i}(\alpha) = \alpha_i \in E$. Hence the above splitting is actually a splitting in E. $\square$