Section X.50. Splitting Fields

Note. In this section, we start with a field F and a set of polynomials. We extend F so that it includes all zeros of the polynomials in the set. The smallest such extension field is the "splitting field" of the set of polynomials. (When we say "smallest," we mean in terms of subset inclusion, not in the sense of cardinality.) We then tie splitting fields to automorphisms of fields.

Definition 50.1. Let F be a field with algebraic closure $\overline{F}$. Let $\{f_i(x) \mid i \in I\}$ be a set of polynomials in $F[x]$. A field $E \leq \overline{F}$ is the *splitting field of* $\{f_i(x) \mid i \in I\}$ *over* F if E is the smallest subfield of $\overline{F}$ containing F and all the zeros in $\overline{F}$ of each of the $f_i(x)$ for $i \in I$. A field $K \leq \overline{F}$ is a *splitting field over* F if it is the splitting field of some set of polynomials in $F[x]$.

Note. When we say "smallest field" we specifically mean the intersection of all subfields of $\overline{F}$ which contain F and all zeros in $\overline{F}$ of each $f_i(x)$.

Example 50.2. The splitting field of $\{x^2-2, x^2-3\}$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (notice that x^2-2 and x^2-3 are irreducible over $\mathbb{Q}$). This is also the splitting field of $\{(x^2-2)(x^2-3)\} = \{x^4-5x^2+6\}$ over $\mathbb{Q}$ (notice that x^4-5x^2+6 is not irreducible over $\mathbb{Q}$).

Note. We now see that an extension field E of F is a splitting field if and only if every automorphism of $\overline{F}$ satisfies certain properties.

Theorem 50.3. A field E, where $F \leq E \leq \overline{F}$, is a splitting field over F if and only if every automorphism of $\overline{F}$ leaving F fixed maps E onto itself (and this induces an automorphism of E leaving F fixed).

Note. Theorem 50.3 finally clearly ties together the factoring of polynomials and permutations of the zeros of the polynomial. This is summarized in Exercise 50.22(a). Recall that an automorphism is a permutation and we see in the proof that the induced automorphism permutes the zeros of the relevant irreducible polynomials in F (since $\sigma(\alpha_j)$ is a zero of $\text{irr}(\alpha_j, F)$ as given by Corollary 48.5 which states that such an automorphism must map a zero of an irreducible polynomial to a conjugate of the zero).

Definition 50.4. Let E be an extension field of a field F. A polynomial $f(x) \in F[x]$ *splits in* E if $f(x)$ factors into a product of linear factors in $E[x]$. (Notice that E must contain all zeros of $f(x)$.)

Example 50.5. The polynomial $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ factors as $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$. $f(x)$ factors in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$, but $f(x)$ does not split in these fields. $f(x)$ splits in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ where $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$.

Corollary 50.6. If $E \leq \overline{F}$ is a splitting field over F, then every irreducible polynomial in $F[x]$ having a zero in E splits in E.

Corollary 50.7. If $E \leq \overline{F}$ is a splitting field over F, then every isomorphic mapping of E onto a subfield of $\overline{F}$ leaving F fixed is actually an automorphism of E. In particular, if E is a splitting field of finite degree over F, then $\{E : F\} = |G(E/F)|$, where $G(E/F)$ is the group of automorphisms of E having F fixed.

Note. In the next section we will see that if E is a splitting field over F then $|G(E/F)| = \{E : F\} = [E : F]$.

Example 50.9. Polynomial $f(x) = x^3 - 2$ is irreducible in $\mathbb{Q}[x]$. The only real zero is $\sqrt[3]{2}$ and $f(x)$ factors in $\mathbb{Q}(\sqrt[3]{2})[x]$, but this is not the splitting field of $f(x)$. The other two zeros of $f(x)$ are $\sqrt[3]{2}\left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right)$ and $\sqrt[3]{2}\left(\frac{-1}{2} - i\frac{\sqrt{3}}{2}\right)$. The splitting field of $f(x)$ is $E = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. We have

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = (2)(3) = 6$$

or equivalently (by the previous note)

$$\{E : \mathbb{Q}\} = \{E : \mathbb{Q}(\sqrt[3]{2})\}\{\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}]\} = (2)(3) = 6.$$

So the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is of degree 6. This example is further explored in the exercises.