LESSON 9 - SPLITTING FIELDS

ERAN ASSAF

1. Introduction

Last lesson we have learned how to apply basic ideas from field theory to constructions with straight-edge and compass, and solved some very difficult problems. Remember that we still need to figure out which regular polygons are constructible. For that we need to develop some more theory, related to roots of unity. In addition, progressing towards solvability of equations, we want to be able to talk about symmetries of roots. For that, it's easier to take as a starting point a field in which we can see all the roots of the polynomial. These are called splitting fields, and will be our topic today.

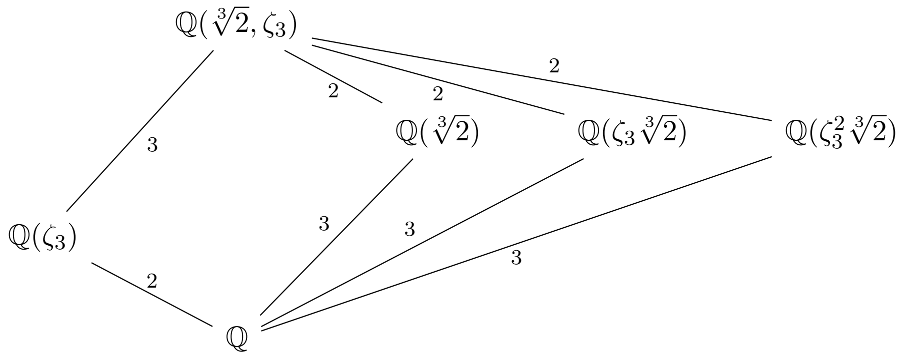
2. Definition and examples

Definition 1. *An extension K/F is called a* **splitting field** *for $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (* **splits completely** *) in $K[x]$ and $f(x)$ does not split completely over any proper subfield of K.*

Example 2. *The splitting field for $(x^2-5)(x^2+1)$ over $\mathbb{Q}$ is the field $\mathbb{Q}(\sqrt{5}, i)$. Clearly $[\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}] = 4$, and we have the following diagram of subfields.*

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{5}, i) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{-5}) \arrow[d, dash, "2"] & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Example 3. *The splitting field of x^3-2 over $\mathbb{Q}$ is not just $Q(\sqrt[3]{2}) \subseteq \mathbb{R}$, as this field only includes one of the roots. We have to adjoin also ζ_3, and obtain $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. We have seen that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$, and we have the following diagram of subfields.*



Example 4. *The splitting field of x^4+4 over $\mathbb{Q}$ is $\mathbb{Q}(i)$, and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Indeed, the roots are $\pm 1 \pm i$.*

Example 5. *Assume $\mathrm{ch}(F) = p \neq 0$, and let $f(x) = x^p - x - a \in F[x]$. Let α be a root of $f(x)$ in some extension of F. Then the other roots are $\alpha + 1, \dots, \alpha + p - 1$, so the splitting field of f is $F(\alpha)$.*

Example 6. *Let $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$, and let $\alpha = \sqrt{b^2 - 4ac} \in \mathbb{C}$. Then $\mathbb{Q}(\alpha) \subseteq \mathbb{C}$ is a splitting field of $f(x)$.*

Example 7. *Let $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ be irreducible, and let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ its complex roots. Then $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_1, \alpha_2)$ is a splitting field for $f(x)$. Note that $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)] \in \{1, 2\}$, so $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] \in \{3, 6\}$.*

3. Existence of a splitting field

Theorem 8. *For any $f(x) \in F[x]$, there exists a splitting field K_f for $f(x)$, and if $\deg f(x) = n$, then*

$$[K_f : F] \leq n!.$$

Proof. We first show the existence of an extension K/F where $f(x)$ splits completely, with $[K : F] \leq n!$ by induction on n. If $n = 1$, then $K = F$. Assume $n > 1$, and write $f(x) = \prod f_i(x)$ with $f_i(x) \in F[x]$ irreducible. If $\deg f_i(x) = 1$ for all i, then $K = F$. Otherwise, there exists i with $\deg f_i(x) \geq 2$. Consider $K_1 = F[x]/f_i(x)$, and write α for the image of x, then $f_i(\alpha) = 0$ hence $f_i(x)$ (and a fortriori $f(x)$) has a linear factor $x - \alpha$ in $K_1[x]$. Write $f(x) = p(x)(x - \alpha)$ in $K_1[x]$. Then $\deg p(x) = n - 1$, and by induction there is an extension K/K_1 where $p(x)$ splits completely, with $[K : K_1] \leq (n-1)!$. Then $f(x)$ also splits completely in K, and by the tower law

$$[K : F] = [K : K_1][K_1 : F] \leq (n-1)! \cdot n = n!.$$

Let K_f be the intersection of all the subfields of K in which $f(x)$ splits completely. □

Example 9. *Let $f(x) = x^n - 1$. If $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ is a primitive n-th root of unity, then the other roots of unity are $\zeta_n^2, \dots, \zeta_n^{n-1}$, so the splitting field of $x^n - 1$ is $\mathbb{Q}(\zeta_n)$. This field is called the* **cyclotomic field** *of n-th root of unity.*

When $n = p$ is a prime, we already know that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. In a few lessons we will also compute the degree of $\mathbb{Q}(\zeta_n)$ for n composite.

Example 10. *Let p be a prime. The splitting field of $x^n - p$ is $\mathbb{Q}(\zeta_n, \sqrt[n]{p})$. If $n = q$ is also prime, then $[\mathbb{Q}(\zeta_q) : \mathbb{Q}] = q - 1$ and $[\mathbb{Q}(\sqrt[q]{p} : \mathbb{Q}] = q$, so $[\mathbb{Q}(\zeta_q, \sqrt[q]{p}) : \mathbb{Q}] = q(q-1)$. This shows also that $x^q - p$ remains irreducible in $\mathbb{Q}(\zeta_q)$.*

Our next goal would be to show that the splitting field is in fact unique (up to isomorphism).

4. Extensions and Uniqueness

In order to prove uniqueness of the splitting field, the idea will be to proceed by induction. However, for the argument to work, we need to prove something slightly more general. (e.g. as in proving by induction that $\sum 2^{-n} < 2$).

Recall that when we have an isomorphism of fields $\varphi : F_1 \to F_2$, it can be extended to an isomorphism $\widetilde{\varphi} : F_1[x] \to F_2[x]$. In particular, if $p_1(x) \in F[x]$ is an irreducible polynomial, and $p_2(x) = \widetilde{\varphi}(p_1(x)) \in F_2[x]$, we have an isomorphism

$$F_1[x]/(p_1(x)) \xrightarrow{\simeq} F_2[x]/(p_2(x)).$$

If α is a root of $p_1(x)$ and β is a root of $p_2(x)$, we obtain an isomorphism $\varphi_\alpha : F_1(\alpha) \to F_2(\beta)$ extending $\varphi : F_1 \to F_2$. We represent it by the following diagram.

$$\begin{tikzcd} \varphi_\alpha : F_1(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & F_2(\beta) \arrow[d, dash] \\ \varphi : F_1 \arrow[r, "\sim"] & F_2 \end{tikzcd}$$

We use this idea to prove the following theorem.

Theorem 11. *Let $\varphi : F_1 \to F_2$ be an isomorphism of fields. Let $f_1(x) \in F_1[x]$, and let $f_2(x) = \widetilde{\varphi}(f_1(x)) \in F_2[x]$. Let E_1 be a splitting field for $f_1(x)$ over F_1 and let E_2 be a splitting field for $f_2(x)$ over F_2. Then the isomorphism φ extends to an isomorphism $\varphi_E : E_1 \to E_2$, i.e. $\varphi_E|_{F_1} = \varphi$.*

$$\begin{tikzcd} \varphi_E : E_1 \arrow[r, "\sim"] \arrow[d, dash] & E_2 \arrow[d, dash] \\ \varphi : F_1 \arrow[r, "\sim"] & F_2 \end{tikzcd}$$

Proof. We proceed by induction on $n = \deg f(x)$. If $f_1(x)$ splits completely in F_1, then $f_2(x)$ splits completely in F_2, so that $E_1 = F_1$ and $E_2 = F_2$ and we can set $\varphi_E = \varphi$. Otherwise, $f_1(x)$ has an irreducible factor $p_1(x)$ with $\deg p_1(x) \geq 2$. Let $\alpha \in E_1$ be a root of $p_1(x)$, and let $\beta \in E_2$ be a root of $p_2(x) = \widetilde{\varphi}(p_1(x))$. Then we can extend φ to an isomorphism $\varphi_\alpha : F_1(\alpha) \to F_2(\beta)$. We now apply the induction step to φ_α and $f_1(x)/p_1(x)$, noting that E_1, E_2 remain their splitting fields. $\square$

Corollary 12. *Any two splitting fields for $f(x) \in F[x]$ over a field F are F-isomorphic.*

5. SUMMARY

We have seen the definition of a splitting field, and exhibited (plenty of) examples. We have seen that there exists a unique (up to F-isomorphism) splitting field for every polynomial. Next lesson we will talk about separability, and use these two notions to find all finite fields.