LESSON 6 (X-HOUR) - FIELD EXTENSIONS

ERAN ASSAF

1. Introduction

Last lesson we discussed criteria for irreducibility of polynomials, such as Eisenstein's criterion and Gauss's Lemma. Today we will start learning field theory and field extensions.

2. Field Extensions

Let F be a field.

Definition 1. *The* **prime subfield** *of F is the subfield of F generated by 1_F.*

Since F is an integral domain, it either has a subring isomorphic to $\mathbb{Z}$, or a subring isomorphic to $\mathbb{F}_p$ for a prime p. If the former, then F contains $\mathbb{Q}$, as it is a field. In this case, we say that the **characteristic** of $\mathbb{F}$ is 0 and $\mathbb{Q}$ is the **prime subfield** of F. In the latter case, we say that the **characteristic** of $\mathbb{F}$ is p and $\mathbb{F}_p$ is the **prime subfield** of F.

Definition 2. *If F is a subfield of K, we say that K is an* **extension field** *(or a* **field extension** *or an* **extension***) of F, denoted K/F or as follows.*

$$\begin{array}{c} K \\ | \\ F \end{array}$$

The field F is called the **base field**.

Definition 3. *The* **degree** *of a field extension K/F, denoted $[K : F]$ is $\dim_F K$, the dimension of K as a vector space over F. The extensions is* **finite** *if $[K : F]$ is finite, and* **infinite** *otherwise.*

What field extensions do we already know?

Example 4. *$\mathbb{C}/\mathbb{R}$ is a finite extension of degree 2, $\mathbb{R}/\mathbb{Q}$ is an infinite extension, $F(t)$ is an infinite extension of F.*

Definition 5. *Let K/F be an extension and let $\{\alpha_i\}_{i\in I}$ be elements in K. Then the smallest subfield of K containing F and the elements $\{\alpha_i\}_{i\in I}$ is denoted $F(\alpha_i)$ and called the field* **generated by** $\{\alpha_i\}_{i\in I}$ **over** F.

3. Simple Extensions

Definition 6. *If $K = F(\alpha)$ is generated by a single element α over F, then K is a* **simple extension** *of F and α is a* **primitive element** *for the extension.*

Example 7. $\mathbb{C} = \mathbb{R}(i)$.

Example 8. *Consider the element $\sqrt{2} \in \mathbb{R}$ in the extension $\mathbb{R}/\mathbb{Q}$. Then $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Indeed, we have seen that the RHS is a field, it contains $\mathbb{Q}$ and $\sqrt{2}$, and any field containing $\mathbb{Q}$ and $\sqrt{2}$ clearly contains the RHS. Note that we can also form $\mathbb{Q}(-\sqrt{2})$, which turns out to be the same. In particular, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.*

Example 9. *With some more work, one can show that $\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$ is also a subfield of $\mathbb{R}$, hence it is $\mathbb{Q}(\sqrt[3]{2})$, and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. In this case, the equation $x^3 - 2 = 0$ has no other solutions in $\mathbb{R}$, but there are two additional solutions in $\mathbb{C}$ given by $\zeta_3\sqrt[3]{2}$ and $\zeta_3^2\sqrt[3]{2}$. The fields they generate are subfields of $\mathbb{C}$ that are isomorphic to $\mathbb{Q}(\sqrt[3]{2})$.*

Theorem 10. *Let $p(x) \in F[x]$ be irreducible. Assume K/F is an extension containing a root α of $p(x)$, i.e. $p(\alpha) = 0$. Then*

$$F(\alpha) \simeq {}^{F[x]}\!/_{(p(x))}.$$

Proof. The evaluation map $\mathrm{ev}_\alpha : F[x] \to F(\alpha)$ sending $f(x) \mapsto f(\alpha)$ is a ring homomorphism. By assumption $\mathrm{ev}_\alpha(p(x)) = p(\alpha) = 0$, so $p(x) \in \ker \mathrm{ev}_\alpha$. But $p(x)$ is irreducible, hence $(p(x))$ is maximal and we obtain $(p(x)) = \ker \mathrm{ev}_\alpha$. (Note that $\mathrm{ev}_\alpha(1) = 1$, so $\ker \mathrm{ev}_\alpha \neq F[x]$). Thus, ev_α induces a field extension ${}^{F[x]}\!/_{(p(x))} \hookrightarrow F(\alpha)$. Since $\mathrm{ev}_\alpha(x) = \alpha$, the image is a subfield of K containing both F and α, hence by minimality of $F(\alpha)$, the map is surjective, and we obtain an isomorphism. □

Example 11. *Consider $p(x) = x^2 + 1 \in \mathbb{R}[x]$. $\mathbb{C}/\mathbb{R}$ contains $\alpha = i$. Then $\mathbb{C} = \mathbb{R}(i) \simeq {}^{\mathbb{R}[x]}\!/_{(x^2+1)}$. Indeed, one can check that $a + bi \mapsto a + bx$ is an isomorphism.*

Example 12. *Similarly, $\mathbb{Q}(i) \simeq {}^{\mathbb{Q}[x]}\!/_{(x^2+1)}$, $\mathbb{Q}(\sqrt{2}) \simeq {}^{\mathbb{Q}[x]}\!/_{(x^2-2)}$ and $\mathbb{Q}(\sqrt[3]{2}) \simeq {}^{\mathbb{Q}[x]}\!/_{(x^3-2)}$.*

Corollary 13. *Under these hypotheses $[F(\alpha) : F] = \deg p(x)$.*

Proof. Let $n = \deg p(x)$, we will show that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F. Indeed, by the theorem it's enough to show that $\{1, \overline{x}, \ldots, \overline{x}^{n-1}\}$ is a basis for $F(x)/(p(x))$ over F. If $f(x) \in F[x]$, we can write $f(x) = q(x)p(x) + r(x)$ for some $q(x), r(x) \in F[x]$ with $\deg r(x) < n$ or $r(x) = 0$. Therefore, $\overline{f(x)} = \overline{r(x)}$ is a linear combination of $\{1, \overline{x}, \ldots, \overline{x}^{n-1}\}$, showing that it is a spanning set. Also, if $\sum_{i=0}^{n-1} a_i\overline{x}^i = 0$, then $f(x) = \sum_{i=0}^{n-1} a_i x^i \in (p(x))$, which implies $f(x) = 0$ since $\deg f(x) < n$. Therefore, they are also linearly independent, hence a basis. □

Example 14. *The polynomial $p(x) = x^n - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Therefore $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.*

Example 15. *We have seen that the polynomial $p(x) = x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$, hence for any root α of $p(x)$, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$.*

Theorem 16 (The Tower Law)**.** *Let $F \subseteq K \subseteq L$ be fields. Then*

$$[L : F] = [L : K][K : F].$$

Proof. Write $m = [K : F]$ and $n = [L : K]$, and let $\alpha_1, \ldots, \alpha_m$ be a basis for K over F, $\beta_1, \ldots, \beta_n$ a basis for L over K. We will show that $\{\alpha_i\beta_j\}_{i,j=1,1}^{m,n}$ is a basis for L over F. Indeed, if $\sum_{i.j} a_{ij}\alpha_i\beta_j = 0$, then since the β_j are linearly independent over K, we have $\sum_i a_{ij}\alpha_i = 0$ for all j. But the α_i are linearly independent over F, hence all the a_{ij} vanish, showing that $\alpha_i\beta_j$ are linearly independent over F. Moreover, if $\gamma \in L$, as the β_j span L over K, we can write $\gamma = \sum_j b_j\beta_j$ for some $b_j \in K$. But the α_i span K over F, hence for each j there are a_{ij} such that $b_j = \sum a_{ij}\alpha_i$, thus $\gamma = \sum a_{ij}\alpha_i\beta_j$, showing that $\alpha_i\beta_j$ span L over F. □

Corollary 17. *If L/F is a finite extension, and $F \subseteq K \subseteq L$ is a subfield containing F, then $[K : F]$ divides $[L : F]$.*

Example 18. *Let α be the real root of $x^3 - 3x - 1$ in the interval $[0, 2]$. The element $\sqrt{2}$ is not contained in the field $\mathbb{Q}(\alpha)$, since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.*

4. SUMMARY

We have seen the construction of simple field extensions, and discussed some of the properties of field extensions. We have seen how the complex numbers are an example of such a construction, and found a basis for the extension as a vector space. We have used it to compute the degree of an extensions, and to prove the tower law, and have seen an example of how the tower law can be used to obtain interesting results about field extensions.