LESSON 7 - ALGEBRAIC EXTENSIONS

ERAN ASSAF

1. Introduction

Last lesson we defined field extensions, and constructed simple extensions. We have seen how to construct a basis and used it to compute the degree of an extension and to prove the tower law. Today, we will look at larger classes of extensions, namely algebraic extensions, and classify which algebraic extensions are finite.

2. Algebraic Extensions

Definition 1. *Let K/F be a field extension. $\alpha \in K$ is* **algebraic** *over F if there exists a $0 \neq f(x) \in F[x]$ such that $f(\alpha) = 0$. If not, α is* **transcendental** *over F. The extension K/F is* **algebraic** *if every element of K is algebraic over F.*

Proposition 2. *Let $\alpha \in K$ be algebraic over F. There exists a unique monic irreducible $m_{\alpha,F}(x) \in F[x]$ with $m_{\alpha,F}(\alpha) = 0$. For $f(x) \in F[x]$, $f(\alpha) = 0$ iff $m_{\alpha,F}(x) \mid f(x)$.*

Proof. Consider the map $\mathrm{ev}_\alpha : F[x] \to K$. Since α is algebraic, it has a nontrivial kernel I, and $F[x]/I \hookrightarrow K$ is a subring. In particular, as K is a field, it is an integral domain, implying that I is a prime ideal. But $F[x]$ is a PID, so $I = (m_{\alpha,F}(x))$ for some irreducible monic polynomial. □

Corollary 3. *If α is algebraic over F and L/F is a field extension, then it is algebraic over L and $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$.*

Definition 4. *The polynomial $m_\alpha(x) = m_{\alpha,F}(x)$ is the* **minimal polynomial** *for α over F. The* **degree** *of α is $\deg \alpha = \deg m_\alpha(x)$.*

Example 5. *Over $\mathbb{Q}$ the minimal polynomial of $\sqrt[n]{2}$ is $x^n - 2$, but over $\mathbb{R}$ it is $x - \sqrt[n]{2}$.*

Corollary 6. *If α is algebraic, $[F(\alpha) : F] = \deg \alpha$. In particular, $F(\alpha)$ is finite.*

In fact, also the converse holds.

Proposition 7. *If $F(\alpha)/F$ is finite, then α is algebraic.*

Proof. Assume $[F(\alpha) : F] = n$, then the elements $1, \alpha, \ldots, \alpha^n$ are linearly dependent, so there exists $a_i \in F$ such that $\sum a_i \alpha^i = 0$, hence α is algebraic over F. □

Corollary 8. *If K/F is finite, it is algebraic.*

Proof. For any $\alpha \in K$, $F(\alpha) \subseteq K$, hence $[F(\alpha) : F] \leq [K : F] < \infty$, so $F(\alpha)$ is finite, hence α is algebraic. □

We would like to characterize finite extensions. Note that there are infinite algebraic extensions, for example $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots, \sqrt[n]{2}, \ldots)$. Indeed, for any n it contains the degree n extension $\mathbb{Q}(\sqrt[n]{2})$, showing it is infinite, and if we have some linear combination of $x = \sum a_i \sqrt[n_i]{2^{e_i}}$, taking $n = \operatorname{lcm}(n_i)$, we see that $x \in \mathbb{Q}(\sqrt[n]{2})$ is algebraic. Therefore, we need something more subtle.

Definition 9. *An extension K/F is* **finitely generated** *if there are elements $\alpha_1, \ldots, \alpha_k \in K$ such that $K = F(\alpha_1, \ldots, \alpha_k)$.*

Lemma 10. $F(\alpha, \beta) = F(\alpha)(\beta)$.

Proof. The field $F(\alpha, \beta)$ contains $F(\alpha)$ and β hence $F(\alpha)(\beta) \subseteq F(\alpha, \beta)$. Conversely, the field $F(\alpha)(\beta)$ contains F, α and β, hence it contains $F(\alpha, \beta)$. □

Theorem 11. *K/F is finite iff K is generated by finitely many algebraic elements over F. More precisely, if $K = F(\alpha_1, \ldots, \alpha_m)$ with $n_i = \deg \alpha_i$ then $[K : F] \leq \prod n_i$.*

Proof. If $[K : F] = n$, let $\alpha_1, \ldots, \alpha_n$ be a basis. Then the α_i are algebraic over F, and $K = F(\alpha_1, \ldots, \alpha_n)$. Conversely, if $K = F(\alpha_1, \ldots, \alpha_m)$, write $F_i = F(\alpha_1, \ldots, \alpha_i)$ so that

$$F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_m = K.$$

and by the lemma $F_i = F_{i-1}(\alpha_i)$ are simple algebraic extensions, so $[F_i : F_{i-1}] = \deg_{F_{i-1}} \alpha_i \leq \deg_F \alpha_i = n_i$. By the tower law, $[K : F] = \prod [F_i : F_{i-1}] \leq \prod n_i$. □

Corollary 12. *Let K/F be a field extension. The elements of K algebraic over F form a subfield of K.*

Proof. Let $\alpha, \beta \in K$ be algebraic over F with $\beta \neq 0$. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta)$. Since $F(\alpha, \beta)$ is generated by finitely many algebraic elements over F, it is finite, hence algebraic. It follows that the algebraic elements are closed under these operations, showing that it is a subfield. □

Example 13. *Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the subfield of all elements in $\mathbb{C}$ algebraic over $\mathbb{Q}$. It is an infinite algebraic extension of $\mathbb{Q}$, the field of* **algebraic numbers**.

Example 14. *Note that $\mathbb{Q}$ is countable, hence so is $\mathbb{Q}[x]$, showing that $\overline{\mathbb{Q}}$ is countable. In particular, since $\mathbb{R}$ is uncountable, there are elements in $\mathbb{R}$ that are not algebraic over $\mathbb{Q}$.*

Theorem 15. *If K/F is algebraic and L/K is algebraic, then L/F is algebraic.*

Proof. Let $\alpha \in L$. Then it is algebraic over K, so there exist $a_0, \ldots, a_n \in K$ such that

$$a_n \alpha^n + \ldots + a_1 \alpha + a_0 = 0.$$

The a_i are all in K, hence algebraic over F. It follows that the field $F(a_0, \ldots, a_n)$ is generated by a finite number of algebraic elements over F, hence is a finite extension of F. But α is algebraic over $F(a_0, \ldots, a_n)$, hence

$$[F(a_0, \ldots, a_n, \alpha) : F] = [F(a_0, \ldots, a_n, \alpha) : F(a_0, \ldots, a_n)][F(a_0, \ldots, a_n) : F] < \infty$$

is finite, hence algebraic. In particular, α is algebraic over F. □

Definition 16. *Let K_1, K_2 be subfields of K. The* **composite field** *of K_1 and K_2, denoted K_1K_2 is the smallest subfield of K containing both K_1 and K_2.*

3. SUMMARY

We have discussed algebraic and transcendental extensions, introduced the minimal polynomial, and looked at finitely generated extension. We have seen that an algebraic extension of an algebraic extension is still algebraic, and considered the construction of composite fields. Finally, we have reminded ourselves what we need to know to construct things with straight-edge and compass.