

1. LECTURE 1: ALGEBRAIC CLOSURE AND SPLITTING FIELDS

Definition 1. A field C is algebraically closed if any $h \in C[X]$ has a root in C . Equivalently any irreducible polynomial $f \in C[X]$ is linear, since f has a root α in C , whence $(X - \alpha) | f$, i.e. $f = X - \alpha$.

Proposition 1. Let $\sigma: K \rightarrow K'$ be an isomorphism of fields and $E/K, E'/K'$ algebraic extension fields. Let $f = \sum_{i=0}^n a_i X^i \in K[X]$ be irreducible and $f' = \sum_{i=0}^n \sigma(a_i) X^i \in K'[X]$. Suppose further that f and f' have roots α and α' , respectively. Then there exists an isomorphism $\hat{\sigma}: K(\alpha) \rightarrow K'(\alpha')$ such that

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\hat{\sigma}} & K'(\alpha') \\ \downarrow & & \downarrow \\ K & \xrightarrow{\sigma} & K' \end{array}$$

is commutative.

Proof. We define

$$\hat{\sigma}(g(\alpha)) = g'(\alpha')$$

and prove that $\hat{\sigma}$ is well defined. Indeed, suppose we have in $K(\alpha)$ $g_1(\alpha) = g_2(\alpha)$ i.e. $(g_1 - g_2)(\alpha) = 0$. We conclude that in $K[X]$: $(g_1 - g_2) = fh$ holds and consequently we have in $K'[X]$, $(g'_1 - g'_2) = f'h'$. Therefore we derive $(g'_1 - g'_2)(\alpha') = 0$. But this is equivalent to $g_1(\alpha') = g_2(\alpha')$ which shows that $\hat{\sigma}$ is well defined. $K'(\alpha')$ is generated by all elements of the form $g'(\alpha')$ with $g' \in K'[X]$, $\deg(g') < \deg(f')$. Therefore, for any $h'(\alpha') = \sum_{i=0}^m b_i \alpha'^i$, $\sum_{i=0}^m \sigma^{-1}(b_i) \alpha^i$ is a preimage of $h'(\alpha')$ which proves that $\hat{\sigma}$ is surjective. \square

Theorem 1. (Steinitz) Any field K has an algebraic extension field $C(K)$ that is algebraically closed. $C(K)$ is unique upto isomorphisms of fields.

Proof. Let Ω be a set of strictly higher cardinality than K . W.l.o.g. we may assume $K \subset \Omega$. Let Γ be the set of all triples $(E, +, \cdot)$, where $K \subset E \subset \Omega$ and $(E, +, \cdot)$ is an algebraic extension field of K . We partially order the set

$$\mathcal{A} = \{(E, +, \cdot) \mid K \subset E \subset \Omega, (E, +, \cdot)/K \text{ is algebraic}\}$$

by setting $(E_1, +, \cdot) < (E_2, +, \cdot)$ iff $E_1 \subset E_2$. We next claim:

Any linearly ordered subcollection $\{(E_i, +, \cdot) \mid i \in I\}$ of elements of \mathcal{A} has an upper bound in \mathcal{A} , $(E^*, +, \cdot)$.

We set $E^* = \bigcup_{i \in I} E_i$. Then for any two elements, $\alpha, \beta \in E^*$ there exists, due to the linear ordering of the $(E_i, +, \cdot)$ some index $i \in I$ such that $\alpha, \beta \in E_i$. In E_i , we can formulate the compositions $\alpha + \beta$ and $\alpha \cdot \beta$. These are well defined, since for any $j > i$ E_j is an extension field of E_i . In particular, α and β are algebraic since they are elements of some $(E_i, +, \cdot)$ which is by definition an algebraic extension of K and the claim follows.

We next apply Zorn's lemma, which gives a maximal element $(A, +, \cdot) \in \mathcal{A}$ and claim:
 $(A, +, \cdot)$ is algebraically closed.

We prove the claim by contradiction. Suppose $(B, +, \cdot)$ is a proper algebraic extension field of A . W.l.o.g. we can assume that B has the same cardinality (if not take one element $b \in B$ which is algebraic over K and consider the field $A(b)$ which is of finite dimension over A), i.e. $|B| = |A|$. Hence we have $|B| < \Omega$ and there exists a bijection φ from B into Ω such that

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & \Omega \\ \downarrow & & \downarrow \\ A & \xrightarrow{\text{id}} & \Omega \end{array}$$

The goal is now to equip $\varphi(B)$ with the structure of a field. For this purpose we define

$$\begin{aligned} \varphi(b_1) +_{\varphi} \varphi(b_2) &= \varphi(b_1 + b_2) \\ \varphi(b_1) \cdot_{\varphi} \varphi(b_2) &= \varphi(b_1 \cdot b_2) \end{aligned}$$

and we derive that $(\varphi(B), +, \cdot)$ is an extension field of A (for instance $\varphi(a)(\varphi(b) +_{\varphi} \varphi(c)) = \varphi(a)(\varphi(b + c)) = \varphi(a(b + c)) = \varphi(ab + ac) = \varphi(ab) +_{\varphi} \varphi(ac) = \varphi(a)\varphi(b) +_{\varphi} \varphi(a)\varphi(c)$). By construction $(\varphi(B), +, \cdot)$ is algebraic and contained in Ω , contradicting the maximality of A . We have consequently proved that A is an algebraically closed field over K . \square

Definition 2. Let $\Phi \subset K[X]$, i.e. an arbitrary subset of polynomials and E/K a field extension. Then E/K is a **splitting field** for Φ or **normal** over K if and only if E/K is a minimal field such that

$$(1.1) \quad \forall f \in \Phi, \exists \alpha_1, \dots, \alpha_n \in E; \quad f(X) = \prod_{i=1}^n (X - \alpha_i) \in E[X].$$

Proposition 2. For any $\Phi \subset K[X]$ there exists a splitting field E/K .

Proof. Let C/K be an algebraic closure of K . Then we have for any $f \in \Phi$

$$f(X) = \prod_{i=1}^n (X - \alpha_i) \in C[X].$$

We can form the field $K < K(\{\alpha_j \mid \exists f \in \Phi; f(\alpha_j) = 0\}) < C$. Clearly, $F = K(\{\alpha_j \mid \exists f \in \Phi; f(\alpha_j) = 0\})$ is a splitting field for Φ . \square

Theorem 2. *Let $\sigma: K \longrightarrow K'$ be an isomorphism of fields and $\sigma_1: K[X] \longrightarrow K'[X]$, $f \mapsto f^\sigma$, its extension to $K[X]$. Let furthermore $\Phi \subset K[X]$ and $\Phi^\sigma \subset K'[X]$ subsets of polynomials such that $\sigma_1(\Phi) = \Phi^\sigma$. Then the splitting fields $E = E(\Phi)$ and $E' = E'(\Phi^\sigma)$ are isomorphic.*

Proof. Let Σ be the set of isomorphisms of $K < F < E$ into $K' < F' < E'$ such that

$$\begin{array}{ccc} F & \xrightarrow{\tilde{\sigma}} & F' \\ \downarrow & & \downarrow \\ K & \xrightarrow{\sigma} & K' \end{array}$$

is commutative. We partially order $\{\tilde{\sigma}\}$ setting $\tilde{\sigma}_i \leq \tilde{\sigma}_j$ iff $\tilde{\sigma}_j$ is an extension of $\tilde{\sigma}_i$. Every linearly ordered subset of $(\{\tilde{\sigma}\}, \leq)$ has a maximum which is contained in $\{\tilde{\sigma}\}$ and we can apply Zorn's lemma. Let τ be a maximal element. τ is an isomorphism from F/K into F'/K and if there exists some $\alpha \in E \setminus F$, then there exists an extension field $K < F(\alpha) < E$ and by Proposition 1 an isomorphism such that

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\tilde{\tau}} & F'(\alpha') \\ \downarrow & & \downarrow \\ F & \xrightarrow{\tau} & F' \\ \downarrow & & \downarrow \\ K & \xrightarrow{\sigma} & K' \end{array}$$

is commutative. Since E is a splitting field for Φ , $\alpha \in E$ is then the root of some irreducible polynomial $m_\alpha \in \Phi$. Let $p \in F[X]$ be the irreducible polynomial with root α and α' be a root of $p^\tau \in F'[X]$. According to Proposition 1 the isomorphism $\tilde{\tau}$ is defined via

$$\tilde{\tau}(g(\alpha)) = g^\tau(\alpha')$$

and hence maps α into α' . Clearly we have $p \mid m_\alpha$. Since $\tau|_K = \sigma$, $p \mid m_\alpha$ implies $p^\tau \mid m^\sigma$. Obviously, $m^\sigma \in \Phi^\sigma$ and in view of $p^\tau \mid m^\sigma$ we derive $m^\sigma(\alpha') = 0$, whence $\alpha' \in E'$. Accordingly we have proved $F'(\alpha') \subset E'$ which contradicts the maximality of τ , i.e. E is isomorphic to E' . \square