Höhere Algebra (Säule II)

Übung, LVA 405.450
C. Fuchs

Inhalt der Vorlesung vom 03.12., WS 2013/14 — 02.12.2013

3.3.3 Let K be a field and let Ω be an extension field of K. The set $\overline{K} := \{\alpha \in \Omega;\ \alpha$ algebraic over $K\}$ is called the *algebraic closure of* K *in* Ω. It is a subfield of Ω and we have $\Omega \supseteq \overline{K} \supseteq K$. (*Proof*: Clearly, $K \subseteq \overline{K}$. We have to show that $\overline{K}$ is closed under the operations: $\alpha, \beta \in \overline{K} \Rightarrow K(\alpha,\beta) \supseteq K(\alpha \pm \beta), K(\alpha\beta^{-1}) \supseteq K$ (in the last case if $\beta \neq 0$); therefore $\alpha \pm \beta, \alpha\beta^{-1}$ lie in a finite extension of K and are therefore algebraic.)
If $\overline{K}$ is algebraically closed, then it is called an *algebraic closure of* K. If Ω is algebraically closed, so is $\overline{K}$:
Proof: Let $f \in \overline{K}[T]$ be a non-constant polynomial. Then $f \in E[T]$ for a finite extension E of K (generated by the coefficients of f). Since Ω is algebraically closed, $\exists \alpha \in \Omega$: $f(\alpha) = 0$. We have to show: $\alpha \in \overline{K}$, i.e. α is algebraic over K. We have $E(\alpha) \supseteq E$ is finite, hence $E(\alpha) \supseteq K$ is finite, hence also $K(\alpha)(\subseteq E(\alpha))$ is a finite extension of K. This means that α is indeed algebraic over K.

Example: The algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ is denoted by $\overline{\mathbb{Q}}$. It is not equal to $\mathbb{C}$ because of $e, \pi, \ldots$, which are not algebraic over $\mathbb{Q}$.

3.3.4 **Theorems** of Steinitz

a) Steinitz extension theorem (Fortsetzungssatz für Körperhomomorphismen): Let $\varphi : K \to L$ be a homomorphism of fields and $K' \supseteq K$. Then there is an extension $L' \supseteq L$ and a homomorphism $\varphi' : K' \to L'$ which extends φ, i.e. $\varphi'|_K = \varphi$.
b) Steinitz existence theorem of algebraic closures: Every field K has an algebraically closed extension field; in particular it hence has an algebraic closure.

Proof: We do not prove 3.3.4. Instead we just show a) in the case $K' = K(\alpha)$ (by induction the statement follows for finitely generated extensions). The full statement depends on the axiom of choice and is proved by Zorn's lemma. If α is transcendental over K, then $K(\alpha) \cong K(T)$. By setting $\varphi'(T) = T$, φ extends to $\varphi' : K(\alpha) \cong K(T) \to L(T) =: L'$. Now assume that α is algebraic over K and let $f \in K[T]$ be its minimal polynomial. Let h be an over L irreducible factor of $f^\varphi \in L[T]$. Let $L' := L[T]/(h)$ and denote by $\beta = T + (h) \in L'$ the root of h in L'. Canonically, we get the map $K[T] \to L[T] \to L'$. Since by construction the kernel of this map contains (f), the homomorphism theorem for rings gives $\varphi' : K(\alpha) \cong K[T]/(f) \to L' \cong L(\beta)$, which is an extension of φ as wanted. By construction $L(\beta)$ is a field and therefore φ' a homomorphism between the fields $K(\alpha)$ and L'. //

3.3.5 We have the following consequences: a) Let $\varphi : K \to \Omega$ be a homomorphism of fields with Ω algebraically closed and let $K' \supseteq K$ be an algebraic extension. Then there exits an extension $\varphi' : K' \to \Omega$ of φ. b) Two algebraic closures of a field K are isomorphic.

Proof: a) By 3.3.4 a) there is an extension $\Omega' \supseteq \Omega$ and an extension $\varphi' : K' \to \Omega'$ of φ. Let $\alpha \in K'$. Since K' is algebraic over K, $\varphi'(\alpha)$ is algebraic over Ω (φ' turns an algebraic relation of α over K into an algebraic relation of $\varphi'(\alpha)$ over Ω; it cannot become trivial since field homomorphisms are injective). Hence $\varphi'(K')$ is algebraic over Ω, hence contained in Ω.
b) Let Ω_1, Ω_2 be two algebraic closures of K. The identity $K \to \Omega_2$ can by extended to a (injective) homomorphism $\psi : \Omega_1 \to \Omega_2$. Hence, $\psi' : \Omega_1 \to \psi(\Omega_1) \subseteq \Omega_2$ is an isomorphism. If ψ is not surjective, then there is $\alpha \in \Omega_2 \backslash \psi(\Omega_1)$. But we can extend ψ'^{-1} to a (injective) homomorphism $\psi'' : \Omega_2 \to \Omega_1$. Then $\psi'(\psi''(\alpha)) = \beta \in \psi'(\Omega_1) = \psi(\Omega_1)$ would have the same image under $\psi' \circ \psi''$ as α (observe that $\psi' \circ \psi''|_{\psi(\Omega_1)} = \psi' \circ \psi'^{-1}|_{\psi(\Omega_1)} = \mathrm{id}_{\psi(\Omega_1)}$) in contradiction to the injectivity of this map. Hence ψ is surjective, hence an isomorphism.//

3.3.6 Let K be a field an $\overline{K}$ be an algebraic closure of K. There is an injective map $\iota : \mathrm{Hom}(K, \overline{K}) \to \mathrm{Aut}(\overline{K})$. This map is not unique in general.

3.4 Conjugate extensions

3.4.1 Let K be a field and Ω an algebraically closed extension of K. Each non-constant polynomial $f \in K[T]$ decomposes into linear factors over Ω, i.e. $f = f_0(T - \alpha_1) \cdots (T - \alpha_n)$ with $f_0 \in K, \alpha_1, \ldots, \alpha_n \in \Omega, n = \deg(f)$. In particular this is true for irreducible f. In this case we call $\alpha_1, \ldots, \alpha_n$ to be *conjugate over* K (or K-conjugate). The fields $K(\alpha_1), \ldots, K(\alpha_n)$ are called *conjugate fields over* K. Observe that conjugate fields are (canonically) isomorphic: $K(\alpha_i) \cong K[T]/(f) \cong K(\alpha_j)$ induced by $\alpha_i \mapsto \alpha_j$.

Examples: a) Let $K = \mathbb{R}, \Omega = \mathbb{C}$ and $f = T^2 + 1 = (T - i)(T + i)$. Hence $\pm i$ are conjugate and $\mathbb{R}(i) = \mathbb{R}(-i) = \mathbb{C}$ are the corresponding conjugate fields. The isomorphism $i \mapsto -i$ is an automorphism of $\mathbb{C}$. b) Again $K = \mathbb{R}, \Omega = \mathbb{C}$, but now $f = (T - z)(T - \overline{z}) \in \mathbb{R}[T], z \in \mathbb{C}$, where $\overline{z} = a - ib$ denotes the complex conjugate of $z = a + ib \in \mathbb{C}$. Then $z, \overline{z}$ are conjugate. c) Let $K = \mathbb{Q}, \Omega = \overline{\mathbb{Q}}$ and $f = T^2 - 2$. Hence $\pm\sqrt{2}$ are conjugate and $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{-2})$ are the corresponding conjugate fields.

A further example: Let $K = \mathbb{Q}, \Omega = \mathbb{C}$ and $f = T^3 - 2$. The complex roots of f are $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \zeta\sqrt[3]{2}, \alpha_3 = \zeta^2\sqrt[3]{2}$, where $\zeta = \exp(2\pi i/3)$ denotes the primitive 3rd root of unity. Hence $\alpha_1, \alpha_2, \alpha_3$ are conjugate over $\mathbb{Q}$ and the conjugate fields are $K_1 = \mathbb{Q}(\alpha_1), K_2 = \mathbb{Q}(\alpha_2), K_3 = \mathbb{Q}(\alpha_3)$. Observe that all three fields are pairwise different: K_1 is a subfield of $\mathbb{R}$, but K_2, K_3 are not. If $K_2 = K_3$, then $\zeta = \alpha_3/\alpha_2 \in K_2$, hence $\sqrt[3]{2} = \alpha_2/\zeta \in K_2$, hence $K_1 \subseteq K_2 = K_3$. But $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = 3$, hence $K_1 = K_2 = K_3$ which is clearly not possible.

3.4.2 Let E, F be extension fields of K. A homomorphism $\varphi : E \to F$ is called a *K-homomorphism*, if $\varphi|_K = \mathrm{id}_K$. We denote by $\mathrm{Hom}_K(E, F)$ the K-homomorphisms from E to F. Observe that K-homomorphisms are K-linear maps between the K-vector spaces E, F (*Proof*: $\varphi(\lambda\alpha) = \varphi(\lambda)\varphi(\alpha) = \lambda\varphi(\alpha)$ for all $\alpha \in E, \lambda \in K$.) Polynomial equations over K are transformed into polynomial equations over K with the same coefficients by a K-homomorphism!

<u>3.4.3</u> **Theorem** Let $\Omega \supseteq E \supseteq K$ be a tower of fields with Ω an algebraic closure of K and $\varphi : E \to \Omega$ a K-homomorphism. Then a) $\varphi(E) \subseteq E \Rightarrow \varphi(E) = E$. b) φ extends to K-automorphism φ' of Ω.

Proof: b) follows at once from 3.3.5. a) Let $\alpha \in E$. We have to show that $\alpha \in \varphi(E)$ to be done. Denote by Σ the roots in E of the minimal polynomial f of α over K. Clearly, $\alpha \in \Sigma$. Since φ is a K-homomorphism we have $0 = \varphi(0) = \varphi(f(x)) = f^\varphi(\varphi(x)) = f(\varphi(x))$ for every $x \in \Sigma$ and thus $\varphi(\Sigma) \subseteq \Sigma$ (observe that we have used $\varphi(E) \subseteq E$). Since Σ is finite and φ injective, we have $\varphi(\Sigma) = \Sigma$. Hence $\alpha \in \Sigma = \varphi(\Sigma) \subseteq \varphi(E)$. //

<u>3.4.4</u> Let $\Omega \supseteq K$ be an extension with Ω algebraically closed. We say that two intermediate fields E, F are *conjugate over* K (or K-conjugate), if there is $\varphi \in \mathrm{Aut}_K(\Omega)$ with $\varphi(E) = F$. We say that $x, y \in \Omega$ are *conjugate over* K (or K-conjugate), if there is $\varphi \in \mathrm{Aut}_K(\Omega)$ with $\varphi(x) = y$.

<u>3.4.5</u> We have the following properties: a) Let E, F be conjugate over K, then $\varphi|_E$ is a K-isomorphism and hence E, F are K-isomorphic. b) Conversely, let E, F be K-isomorphic intermediate fields. By 3.3.5 this isomorphism can be extended to a K-automorphism of $\Omega = \overline{K}$ which sends E to F. Hence E, F are K-conjugate. c) Let x, y be K-conjugate (with $\varphi \in \mathrm{Aut}_K(\Omega)$ and $\Omega = \overline{K}$) and let f be the minimal polynomial of x over K. Then $0 = \varphi(0) = \varphi(f(x)) = f^\varphi(\varphi(x)) = f(\varphi(x)) = f(y)$ shows that y is also a root of f and hence has the same minimal polynomial as x over K (the polynomial f has coefficients in K, is irreducible and has y as a root). The different K-conjugate elements are hence the different roots of the minimal polynomial f (in agreement with the definition in 3.4.1).