23. Script zur Vorlesung: Algebra (B III)
Prof. Dr. Salma Kuhlmann, Gabriel Lehéricy, Simon Müller
WS 2016/2017: 3. Februar 2017

Useful English/German Vocabulary
Splitting field - Zefällungskörper
Field extension - Körpererweiterung

Definition 0.1. *Let E/F be a field extension. The* ***Galois group****, denoted $Gal(E/F)$, of E/F is the group of automorphisms of E which fix F pointwise i.e. the automorphisms μ of E such that for all $\alpha \in F$, $\mu(\alpha) = \alpha$.*

Definition 0.2. *Let F be a field and G be a subgroup of the group of automorphisms of F. The set*

$$Inv(G) := \{a \in F \mid \sigma(a) = a \text{ for all } \sigma \in G\}$$

*is a subfield of F. We call it the G-**fixed subfield** of F.*

Let E be a field and G the group of automorphisms of E. Let Γ be the set of subgroups of G and Σ the set of subfields of E. The maps

$$\Gamma \to \Sigma, \ H \mapsto \mathrm{Inv}(H)$$

and

$$\Sigma \to \Gamma, \ F \mapsto \mathrm{Gal}(E/F)$$

have the following properties:

(i) $G_1 \subseteq G_2 \Rightarrow \mathrm{Inv}(G_1) \supseteq \mathrm{Inv}(G_2)$

(ii) $F_1 \subseteq F_2 \Rightarrow \mathrm{Gal}(E/F_1) \supseteq \mathrm{Gal}(E/F_2)$

(iii) $\mathrm{Inv}(\mathrm{Gal}(E/F)) \supseteq F$

(iv) $\mathrm{Gal}(E/\mathrm{Inv}(H)) \supseteq H$

Lemma 0.3. *Let E/F be a splitting field of a separable polynomial with coefficients in F. Then*

$$|Gal(E/F)| = [E : F].$$

Proof. What we will actually show is the following:

Let $\tau : F \to F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be a separable. Let E be a splitting field for $p(x)$ and E' be a splitting field for $\tau(p)(x)$. There exist exactly $[E : F]$ extensions of τ to an isomorphism $\sigma : E \to E'$.

We proceed by induction on $[E : F]$. If $[E : F] = 1$ the statement is clear.
Fix α a root of $p(x)$ in $E \backslash F$ with minimal polynomial $m_\alpha(x)$. For each β a root of $\tau(m_\alpha)(x)$, let $\tau_\beta : F(\alpha) \to F'(\beta)$ be the (unique) isomorphism extending τ with $\tau_\beta(\alpha) = \beta$.
For each root β of $\tau(m_\alpha)(x)$ let S_β be the set of isomorphisms $E \to E'$ extending τ_β. If $\beta \neq \beta'$ then $S_\beta \cap S_{\beta'} = \emptyset$.

The field E remains the splitting field of $p(x)$ over $F(\alpha)$ and E' remains the splitting field of $\tau_\beta(p)(x)$ over $F'(\beta)$. Since $[E : F(\alpha)] < [E : F]$, by the induction hypothesis,

$$|S_\beta| = [E : F(\alpha)].$$

Since $m_\alpha(x)$ divides $p(x)$, $m_\alpha(x)$ is separable and thus, so is $\tau(m_\alpha)(x)$. Thus $\tau(m_\alpha)(x)$ has $[F(\alpha) : F]$ distinct roots.
Each isomorphism $\sigma : E \to E'$ extending τ maps α to a root of $\tau(m_\alpha)(x)$. Thus each σ restricts to some τ_β. So each σ is in S_β for some β a root of $\tau(m_\alpha)(x)$.
Thus there are exactly $[E : F(\alpha)][F(\alpha) : F]$ isomorphisms $\sigma : E \to E'$ extending $\tau : F \to F'$. So we have proved our claim.
Setting $E = E'$, $F = F'$ and τ equal to the identity homomorphism we get our lemma as stated.

□

Lemma 0.4. *Let G be a finite group of automorphisms of a field E and let $F = Inv(G)$. Then*

$$[E : F] \leq |G|.$$

Remark/Reminder from linear algebra: A system of n homogeneous linear equations over a field E in m variables with $n < m$ has a non-trivial solution. (See LA I, Korollar 2, 7. Vorlesung am 11.11.11)

proof of lemma. Let $n = |G|$ and $G = \{\mu_1 = 1, \mu_2, ..., \mu_n\}$. We need to show that any $m > n$ elements of E are linearly dependent over F. Let $u_1, ..., u_m \in E$. Consider the system of linear equations in variables $x_1, ..., x_m$

$$\sum_{j=1}^{m} \mu_i(u_j)x_j = 0, \ 1 \leq i \leq n. \tag{1}$$

Let $(b_1, ..., b_m)$ be a non-trivial solution with the least number of $b_i \neq 0$. By permuting the variables x_i we may assume $b_1 \neq 0$ and by multiplying through by b_1^{-1} we may assume $b_1 = 1$.

We now show by contradiction that each $b_i \in F := \text{Inv}(G)$. Without loss of generality we may suppose $b_2 \notin F$ and $1 \leq k \leq n$ is such that $\mu_k(b_2) \neq b_2$.
Applying μ_k to 1 we get that

$$\sum_{j=1}^{m} (\mu_k\mu_i)(u_j)\mu_k(b_j) = 0, \ 1 \leq i \leq n.$$

Since $\mu_k\mu_1, ..., \mu_k\mu_n$ is just a permutation of $\mu_1, ..., \mu_n$,

$$(\mu_k(1), \mu_k(b_2), ..., \mu_k(b_m)) = (1, \mu_k(b_2), ..., \mu_k(b_m))$$

is a solution to 1.
Thus

$$(0, b_2 - \mu_k(b_2), ..., b_m - \mu_k(b_m))$$

is a solution to 1 and is non-trivial since $b_2 - \mu_k(b_2) \neq 0$. But this solutions has more zero entries than our original solution. So we have a contradiction. Thus each $b_i \in F$ and from the first equation in 1:

$$\sum_{j=1}^{m} u_j b_j = 0.$$

Thus $u_1, ..., u_m$ are linearly dependent over F.

□

Definition 0.5. *We say an algebraic field extension E/F is* ***separable*** *if the minimal polynomial of every element of E over F is separable.*

Theorem 0.6. *Let E/F be a field extension. The following are equivalent:*

1. *E is a splitting field of a separable polynomial $p(x) \in F[x]$.*
2. *$F = Inv(G)$ for some finite group of automorphisms of E.*
3. *E is a finite dimensional, normal and separable over F.*

Moreover, if E and F are as in (1) and $G = Gal(E/F)$ then $F = Inv(G)$ and if G and F are as in (2), then $G = Gal(E/F)$.

Proof. (1)⇒(2) Let $F' = \text{Inv}(\text{Gal}(E/F))$ and note $F' \supseteq F$. Clearly E is a splitting field of $p(x)$ over F' and since $\text{Gal}(E/F)$ fixes F' pointwise, $\text{Gal}(E/F) = \text{Gal}(E/F')$.

By lemma 0.3, $[E : F] = |\text{Gal}(E/F)|$ and $[E : F'] = |\text{Gal}(E/F')|$. Thus, since $[E : F] = [E : F'][F' : F]$, $[F' : F] = 1$. Thus $F = F'$. So (2) holds.
Note we have also shown that $F := \text{Inv}(G)$ for $G := \text{Gal}(E/F)$, which is the first part of the moreover.

(2) $\Rightarrow$ (3) E is finite dimensional over F by lemma 0.4. Let $\alpha \in E$. Let $\alpha_1 = \alpha, \alpha_2, ..., \alpha_m$ be the orbit of α under the action of G. Let $g(x) = \prod_{i=1}^{m}(x - \alpha_i)$. For any $\sigma \in G$,

$$\sigma(g)(x) = \prod_{i=1}^{m}(x - \sigma(\alpha_i)) = g(x)$$

since σ just permutes the elements of $\{\alpha_1, ..., \alpha_m\}$. Thus $g(x) \in F[x]$.

Since $g(\alpha) = 0$ and $g(x) \in F[x]$, the minimal polynomial of α over F divides g. Since the α_is are all different, g is separable and thus the minimal polynomial of α is separable. So E/F is separable.
Moreover, all roots of the minimal polynomial of α are in E. Thus E is a normal over F (it is the splitting field of the minimal polynomials over F of all elements $\alpha \in E$).

(3) $\Rightarrow$ (1) Since E/F is normal and finite dimensional, E is the splitting field of a finite number of polynomials $p_1, ..., p_n \in F[x]$. We may as well assume that each of these polynomials is monic, irreducible over F and that no two are equal. Thus, each polynomial p_i is the minimal polynomial of some $\alpha \in E$ over F. Thus, since they are non-equal, they also have no common roots. Therefore, there product $p_1 \cdots p_n$ is separable and E is its splitting field.

We now prove the second part of the "moreover". Suppose $F = \mathrm{Inv}(G)$ for some finite group of automorphisms of E. Then by lemma 0.4, $[E : F] \leq |G|$. Since (1) holds, lemma 0.3 says that $\mathrm{Gal}(E/F) = [E : F]$. So, since G is a subgroup of $\mathrm{Gal}(E/F)$, $G = \mathrm{Gal}(E/F)$.

$\square$

Definition 0.7. *We call a field extension E/F which satisfies any (and hence all) the equivalent conditions of the above theorem a* ***Galois extension****.*

Theorem 0.8 (Fundamental theorem of Galois theory). *Let E/F be a Galois extension with $G := Gal(E/F)$. Let Γ be the set of subgroups of $G := Gal(E/F)$ and let Σ be the set of intermediate fields between E and F. The maps*

$$H \mapsto Inv(H)$$

$$K \mapsto Gal(E/K)$$

are inverse bijective maps. Moreover, we have the following properties:

(i) $H_1 \supseteq H_2 \Leftrightarrow Inv(H_1) \subseteq Inv(H_2)$.

(ii) $|H| = [E : Inv(H)]$, $[G : H] = [Inv(H) : F]$

(iii) *H in G is normal if and only if $Inv(H)$ is normal over F. In this case*

$$Gal(Inv(H)/F) \cong G/H$$