

Kapitel I

Galois theory

§ 1 Algebraic field extensions

Notations 1.1 If k, L are fields and $K \subseteq L$, L/k is called a *field extension*. The *dimension* $[L : k] := \dim_k L$ of L considered as a k -vector space, is called the *degree* of the field extension of L over k . A field extension L/k is called *finite*, if $[L : k] < \infty$. The *polynomial ring* over k is defined as

$$k[X] := \left\{ f = \sum_{i=0}^n a_i X^i \mid n \geq 0, a_i \in k \ \forall i \in \{0, \dots, n\}, a_n \neq 0 \right\} \cup \{0\}.$$

Reminder 1.2 Let L/k a field extension, $\alpha \in L$, $f \in k[X]$.

- (i) $f(\alpha)$ is well defined.
- (ii) $\phi_\alpha : k[X] \rightarrow L$, $f \mapsto f(\alpha)$ is a homomorphism.
- (iii) $\text{im}(\phi_\alpha) := k[\alpha]$ is the smallest subring of L containing k and α .
- (iv) $\ker(\phi_\alpha) = \{f \in k[X] \mid f(\alpha) = 0\} \triangleleft k[X]$ is a prime ideal.
- (v) $\ker(\phi_\alpha)$ is a principle ideal.
- (vi) If $f_\alpha \neq 0$ and the leading coefficient of f_α is 1, f_α is called the *minimal polynomial* of α , i.e. $f_\alpha(\alpha) = 0$ and f_α is the polynomial of smallest degree with this property. In this case, f_α is irreducible and $\ker(\phi_\alpha) = (f_\alpha)$ is a maximal ideal.
- (vii) Then $L_\alpha := k[X] / \ker(\phi_\alpha) = k[X] / (f_\alpha)$ is a field.
- (viii) We have $k[\alpha] = \text{im}(\phi_\alpha) \cong k[X] / \ker(\phi_\alpha) = L_\alpha$, if $f_\alpha \neq 0$. Moreover $k[\alpha] = k(\alpha)$, where $k(\alpha)$ is the smallest field containing k and α . In particular, $\frac{1}{\alpha} \in k[\alpha]$.
- (ix) The degree of the field extension $k[\alpha]/k$ is $[k[\alpha] : k] = \deg(f_\alpha)$.

proof. (ii) For $f, f_1, f_2 \in k[X]$, $\lambda \in k$ we have

$$(f_1 + f_2)(\alpha) = f_1(\alpha) + f_2(\alpha) \text{ and } (\lambda f)(\alpha) = \lambda f(\alpha)$$

(iii) Clear.

(iv) Let $f, g \in k[X]$ such that $f \cdot g \in \ker(\phi_\alpha)$: Then

$$0 = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)$$

and since L has no zero divisors, $f(\alpha) = 0$ or $g(\alpha) = 0$ and hence $f \in \ker(\phi_\alpha)$ or $g \in \ker(\phi_\alpha)$

(v) Remember that the polynomial ring is euclidean. Take $f_\alpha \in \ker(\phi_\alpha)$ of minimal degree. We will show, that $\ker(\phi_\alpha)$ is generated by f_α . Let $g \in \ker(\phi_\alpha)$ arbitrary and write

$$g = q \cdot f_\alpha + r \text{ with } q, r \in k[X], \quad \deg(r) < \deg(f_\alpha) \text{ or } r = 0.$$

Since $r = g - q \cdot f_\alpha \in \ker(\phi_\alpha)$ and the choice of f_α , $\deg(r) < \deg(f_\alpha)$, hence $r = 0 \Rightarrow g \in (f_\alpha)$.

(vi) If $f_\alpha = g \cdot h$, either $g(\alpha) = 0$ or $h(\alpha) = 0$. As above, this implies $g \in k$ or $h \in k^\times$, i.e. f or g is irreducible. Now assume, there is an ideal $I \trianglelefteq k[X]$ satisfying $(f_\alpha) \subsetneq I \subsetneq k[X]$. Let $g \in I \setminus (f_\alpha)$, such that $(g) = I$. Such a g exists by proof of (v). Then $f_\alpha = g \cdot h$, $h \in k[X]$. This implies, that either g or h is a constant polynomial, hence a unit. In the first case, $I = k[X]$ and in the second one $I = (f_\alpha)$, which implies the claim.

(vii) We show the more general argument: If R is a ring, $\mathfrak{m} \triangleleft R$ a maximal ideal, then R/\mathfrak{m} is a field. Let $\bar{a} \in R/\mathfrak{m}$ for some $a \in R$, $\bar{a} \neq 0$. Let $I := (\mathfrak{m}, a)$ the smallest ideal in R containing \mathfrak{m} and a . Since $\bar{a} \neq 0$, hence $a \notin \mathfrak{m}$ we have $\mathfrak{m} \subsetneq I$ and since \mathfrak{m} is a maximal ideal, $I = R$. Hence $1 \in I$, so we can write $1 = x + ab$ for some $x \in \mathfrak{m}$ and $b \in R$. Then we get

$$\bar{1} = \overline{x + ab} = \bar{x} + \bar{a}\bar{b} = \bar{a}\bar{b},$$

hence \bar{a} is invertible in R/\mathfrak{m} .

(viii) Let

$$f_\alpha = \sum_{i=0}^n a_i X^i$$

Note, that $a_n = 1$ and $a_0 \neq 0$, since f_α is irreducible. We get

$$\begin{aligned} \implies 0 &= f_\alpha(\alpha) = \sum_{i=0}^n a_i \alpha^i = a_0 + a_1 \alpha + \cdots + a_n \alpha^n \\ \implies a_0 &= -\alpha \cdot (a_1 + a_2 \alpha + \cdots + a_{n-2} \alpha^{n-2} + \alpha^{n-1}) \\ \implies 1 &= -\alpha \cdot \left(\frac{a_1}{a_0} + \frac{a_2}{a_0} \alpha + \cdots + \frac{a_{n-2}}{a_0} \alpha^{n-2} + \frac{1}{a_0} \alpha^{n-1} \right) \\ \implies \frac{1}{\alpha} &= -\frac{a_1}{a_0} - \frac{a_2}{a_0} \alpha - \cdots - \frac{a_{n-2}}{a_0} \alpha^{n-2} - \frac{1}{a_0} \alpha^{n-1} \end{aligned}$$

Hence $\frac{1}{\alpha} \in k[X]$ and $k[X]$ is a field.

(ix) The family $\{1, \alpha, \dots, \alpha^{n-1}\}$ forms a basis of $k[\alpha]$ as a k -vector space. □

Example 1.3 Let $k = \mathbb{Q}$, $L = \mathbb{C}$, $\alpha = 1 + i$, $\beta = \sqrt{2}$. Then the minimal polynomials of α and β are

$$f_\alpha = (X - 1)^2 + 1, \quad f_\beta = X^2 - 2.$$

Proposition 1.4 (Kronecker) *Let k be a field, $f \in k[X]$, $\deg(f) \geq 1$.*

Then there exists a finite field extension L/k and $\alpha \in L$, such that $f(\alpha) = 0$.

proof. W.l.o.g. we may assume, that f is irreducible, since $f = g \cdot h = 0 \Rightarrow g = 0$ or $h = 0$. Then by 1.2 $(f) = \{f \cdot g \mid g \in k[X]\}$ is a maximal ideal and $L := k/(f)$ is a field.

Clearly k is a subfield of L , since (f) does not contain any constant polynomial, i.e., if

$$\pi : k[X] \longrightarrow k[X]/(f)$$

denotes the residue map, we have $\ker(\pi) \cap k = \{0\}$, hence $\pi|_k$ is injective. Write

$$f = \sum_{i=0}^n a_i X^i.$$

Then we have

$$f(\pi(X)) = \sum_{i=0}^n a_i \pi(X)^i = \sum_{i=0}^n \pi(a_i) \pi(X)^i = \pi \left(\sum_{i=0}^n a_i X^i \right) = \pi(f) = 0,$$

hence $\alpha := \pi(X)$ is a zero of f in L . Moreover L/k is finite with degree $[L : k] = \deg(f) = n$, since $\{1, \alpha, \dots, \alpha^{n-1}\}$ is basis of L as a k -vector space. For the independence write

$$\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0, \quad \lambda_i \in k.$$

Assume, there is $0 \leq j \leq n-1$ with $\lambda_j \neq 0$. Then the polynomial

$$g = \sum_{i=0}^{n-1} \lambda_i X^i$$

satisfies $g(\alpha) = 0$ with $\deg(g) < \deg(f)$, which is not possible by irreducibility of f . It remains to show, that L is generated by the powers of α . We have $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$, hence we write

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0) \in (1, \dots, \alpha^{n-1}).$$

By induction on n , we get $\alpha^k \in (1, \dots, \alpha^{n-1})$ for all $k \geq n$. □

Example 1.5 Let $k = \mathbb{Q}$, $f = X^n - a$ for some $a \in \mathbb{Q}$. For now we assume that f is irreducible (we may be able to prove this later). Then

$$L := \mathbb{Q}[X]/(f) = \mathbb{Q}[X]/(X^n - a) \cong \mathbb{Q}[\sqrt[n]{a}] = \mathbb{Q}(\sqrt[n]{a})$$

and the degree of the extension is equal to n .

Definition 1.6 Let L/k a field extension, $\alpha \in L$.

- (i) α is called *algebraic over k* , if there exists $f \in \mathbb{X}[X] \setminus \{0\}$, such that $f(\alpha) = 0$.
- (ii) Otherwise α is called *transcendental*.
- (iii) L/k is called an *algebraic field extension*, if every $\alpha \in L$ is algebraic over k .

Proposition 1.7 Every finite field extension L/k is algebraic.

proof. Let $\alpha \in L$, $n := [L : k]$ the degree of L/k . Then $1, \alpha, \dots, \alpha^n$ are linearly dependant over k , i.e. there exist $\lambda_0, \dots, \lambda_n \in k$, $\lambda_j \neq 0$ for at least one $0 \leq j \leq n$, such that

$$\sum_{i=0}^n \lambda_i \alpha^i = 0.$$

Hence the polynomial

$$f = \sum_{i=0}^n \lambda_i X^i \neq 0$$

satisfies $f(\alpha) = 0$, thus α is algebraic over k . Since α was arbitrary, L/k is algebraic. \square

Proposition 1.8 Let L/k a field extension, $\alpha, \beta \in L$.

- (i) If α, β are algebraic over k , then $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ are also algebraic over k .
- (ii) If $\alpha \neq 0$ is algebraic over k , then $\frac{1}{\alpha}$ is also algebraic over k .
- (iii) $k_L := \{\alpha \in L \mid \alpha \text{ is algebraic over } k\} \subseteq L$ is a subfield of L .

proof. (i) Since $\alpha \in L$ is algebraic over $k \Rightarrow k[\alpha] = k(\alpha)$ is a finite field extension of k . Since β is algebraic over $k \Rightarrow \beta$ is algebraic over $k[\alpha]$, hence $(k[\alpha])[\beta]/k[\alpha]$ is a finite field extension. Further, we have

$$k \subseteq k[\alpha] \subseteq (k[\alpha])[\beta] = k[\alpha, \beta].$$

Thus $k[\alpha, \beta]/k$ is algebraic with Proposition 1.5. This implies the claim, as $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta \in k[\alpha, \beta]$.

- (ii) If $\alpha \neq 0$, $\frac{1}{\alpha}$ is algebraic over k with part (i).
- (iii) Follows from (i) and (ii). \square

Definition + proposition 1.9 Let k be a field, $f \in k[X]$, $\deg(f) = n$.

- (i) A field extension L/k is called a *splitting field of f* , if L is the smallest field in which f decomposes into linear factors.
- (ii) A splitting field $L(f)$ exists.
- (iii) The field extension $L(f)/k$ is algebraic over k .
- (iv) For the degree we have $[L(f) : k] \leq n!$.

proof.

- (ii) Do this by induction on n .

n=1 Clear.

n>1 Write $f = f_1 \cdots f_r$ with irreducible polynomials $f_i \in k[X]$. Then f splits if and only every f_i splits. Hence we may assume that f is irreducible

Consider $L_1 := k/(f)$. Then f has a zero in L_1 ; say α . Then we have $L_1 = k[\alpha]$. Now we can write $f = (X - \alpha) \cdot g$ for some $g \in k[X]$ with $\deg(g) = n - 1$. By induction hypothesis, there exists a splitting field $L(g)$ for g . Then f splits over $L(g)[\alpha]$.

(iii) Follows by part (iv) and Proposition 1.5

(iv) Do this again by induction.

n=1 Clear.

n>1 In the notation of part (ii) we have $[k[\alpha] : k] = \deg(f) = n$. By the multiplication formula for the degree and induction hypothesis we have

$$[L(f) : k] = [L(g)[\alpha] : k] = [L(g)[\alpha] : L(g)] \cdot [L(g) : k] \leq n \cdot (n - 1)! = n!$$

Definition + proposition 1.10 Let k be a field.

(i) k is called *algebraically closed*, if every $f \in k[X]$ splits over k .

(ii) The following statements are equivalent:

- (1) k is algebraically closed
- (2) Every nonconstant polynomial $f \in k[X]$ has a zero in k .
- (3) There is no proper algebraic field extension of k .
- (4) If $f \in k[X]$ is irreducible, then $\deg(f) = 1$.

proof. '(1) \Rightarrow (2)' Let $f \in k[X]$ be a non-constant polynomial of degree n . Then f splits over k , i.e. we have a presentation

$$f = \prod_{i=1}^n (X - \lambda_i)$$

with $\lambda_i \in k$ for $1 \leq i \leq n$. Every λ_i is a zero. Since $n \geq 1$, we find a zero for any nonconstant polynomial.

'(2) \Rightarrow (3)' Assume L/k is algebraic, $\alpha \in L$. Let f_α be the minimal polynomial of α . By assumption, f_α has a zero in k . Since f_α is irreducible, we must have $f_\alpha = X - \alpha$, hence $\alpha \in k$, since $f \in k[X]$.

'(3) \Rightarrow (4)' Let $f \in k[X]$ irreducible. Then $L := k[X]/(f)$ is an algebraic field extension. By (3), $L = k$, hence $1 = [L : k] = \deg(f)$.

'(4) \Rightarrow (1)' For $f \in k[X]$ write $f = f_1 \cdots f_r$ with irreducible polynomials f_i for $1 \leq i \leq r$.

With (4), $\deg(f_i) = 1$ for any i , hence f splits. □

Lemma 1.11 Let k be a field. Then there exists an algebraic field extension k'/k , such that every $f \in k[X]$ has a zero in k' .

proof. For every irreducible polynomial $f \in k[X]$ introduce a symbol X_f and consider

$$R := k[\{X_f \mid f \in k[X] \text{ irreducible}\}] \supseteq k.$$

Monomials in R look like

$$g = \lambda \cdot X_{f_1}^{n_1} X_{f_2}^{n_2} \cdots X_{f_k}^{n_k}$$

with $\lambda \in k$, $n_i \in \mathbb{N}$. Let $I \trianglelefteq R$ be the ideal generated by the $f(X_f)$, $f \in k[X]$ irreducible. The following claims prove the lemma:

Claim (a) $I \neq R$

Claim (b) There exists a maximal ideal $\mathfrak{m} \trianglelefteq R$ containing I .

Claim (c) $k' = R/\mathfrak{m}$

To finish the proof, it remains to show the claims.

(a) Assume $I = R$. Then $1 \in I$, i.e.

$$1 = \sum_{i=1}^k g_{f_i} f_i(X_{f_i})$$

for suitable $g_{f_i} \in R$. Let L/k be a field extension in which all f_i have a zero α_i . Define a ring homomorphism by

$$\pi : R \longrightarrow L, X_f \mapsto \begin{cases} \alpha_i, & f = f_i \\ 0, & \text{otherwise} \end{cases}$$

Then we obtain

$$1 = \pi(1) = \pi\left(\sum_{i=1}^k g_{f_i} f_i(X_{f_i})\right) = \sum_{i=1}^k \pi(g_{f_i}) f_i(\pi(X_{f_i})) = \sum_{i=1}^k \pi(g_{f_i}) f_i(\alpha_i) = 0,$$

hence our assumption was false and we have $I \neq R$.

(b) Let \mathcal{S} be the set of all proper ideals of R containing I . By claim 2, $I \in \mathcal{S}$. Let now

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \dots$$

be elements of \mathcal{S} . More generally let N be a totally ordered subset of \mathcal{S} and

$$S := \bigcap_{J \in N} J$$

Then $S \in \mathcal{S}$, hence \mathcal{S} is nonempty. By Zorn's Lemma we know that \mathcal{S} contains a maximal element $\mathfrak{m} \neq R$. Then \mathfrak{m} is maximal ideal of R , since an ideal $J \trianglelefteq R$ satisfying $\mathfrak{m} \subsetneq J \subsetneq R$ is contained in \mathcal{S} , which is a contradiction considering the choice of \mathfrak{m} .

(c) Clearly k' is a field extension of k . Let $f \in k[X]$ be irreducible and

$\pi : R \longrightarrow k/\mathfrak{m}$ denote the residue map. Then

$$f(X_f) \in I \subseteq \mathfrak{m}$$

i.e. we have

$$\pi(X_f) = 0$$

and thus $f(\pi(X_f)) = 0$. Hence $\pi(X_f)$ is algebraic over k .

Since k' is generated by the $\pi(X_f)$, k'/k is algebraic, which finishes the proof. \square

Theorem 1.12 *Let k be a field. Then there exists an algebraic field extension \bar{k}/k such that \bar{k} is algebraically closed. \bar{k} is called the algebraic closure of k .*

proof. By Lemma 1.9 there is an algebraic field extension k'/k , such that every $f \in k[X]$ has a zero in k' . Then let

$$k_0 := k, \quad k_1 = k'_0, \quad k_2 = k'_1, \quad k_{i+1} = k'_i \quad \text{for } i \geq 1$$

Clearly k_i is algebraic over k for all $i \in \mathbb{N}_0$ and $k_i \subseteq k_{i+1}$. Define

$$\bar{k} := \bigcup_{i \in \mathbb{N}_0} k_i$$

Then \bar{k}/k is an algebraic field extension. For $f \in \bar{k}[X]$ we find $i \in \mathbb{N}_0$ with $f \in k_i[X]$, hence f has a zero in k_i . With proposition 1.8, \bar{k} is algebraically closed. \square

§ 2 Simple field extensions

Definition 2.1 A field extension L/k is called *simple*, if there exists some $\alpha \in L$ such that $L = k[\alpha]$.

Example 2.2 Let $f \in k[X]$ be irreducible, $L := k[X]/(f)$. Then $L = k[\alpha]$ where $\alpha = \pi(X) = \bar{X}$ and $\pi : k[X] \rightarrow L$ denotes the residue map. Conversely, if L/k is simple and algebraic, then $L = k[\alpha]$ for some algebraic $\alpha \in L$. Let $f \in k[X]$ be the minimal polynomial of α over k , then

$$L = k[\alpha] = k(\alpha) = k[X]/(f).$$

Proposition 2.3 *Let L be a field. Then any finite subgroup G of the multiplicative group L^\times is cyclic.*

proof. Let $\alpha \in G$ be an element of maximal order, $n := \text{ord}(\alpha)$. Define

$$G' := \{\beta \in G : \text{ord}(\beta) \mid n\}$$

We first show $G' = G$ and then $G' = \langle \alpha \rangle$. Let $\beta \in G$, $m := \text{ord}(\beta)$. Then

$$\text{ord}(\alpha\beta) = \text{lcm}(m, n) \leq n$$

by the property of n . Thus $m|n$ and $\beta \in G'$ and hence $G \subseteq G'$. Since $G' \subseteq G$ by definition, we have $G' = G$. Let now $\gamma \in G'$. We have $\gamma^n = 1$, hence γ is zero of

$$f = X^n - 1$$

f has at most n zeros, but since $|\langle \alpha \rangle| = n$, we have $\langle \alpha \rangle = G'$ which finishes the proof. \square

Corollary 2.4 *Let k be a finite field. Then every finite field extension L/k is simple.*

proof. We have $|L| = |k|^{[L:k]}$ and thus L is also finite. With proposition 2.2 there exists some $\alpha \in L$ such that $L^\times = L \setminus \{0\} = \langle \alpha \rangle$, hence $L = k[\alpha]$, which proves the claim. \square

Remark 2.5 *Let L/k be a finite field extension, $f \in k[X]$ and $\alpha \in L$ a zero of f . Let \bar{k} be an algebraic closure of k and $\sigma : L \longrightarrow \bar{k}$ a homomorphism of field such that $\sigma|_k = id_k$. Then $\sigma(\alpha)$ is a zero of f .*

proof. Write

$$f = \sum_{i=0}^n a_i X^i$$

with coefficients $a_i \in k$, hence we have $\sigma(a_i) = a_i$ for $0 \leq i \leq n$. We obtain

$$f(\sigma(\alpha)) = \sum_{i=0}^n a_i (\sigma(\alpha))^i = \sum_{i=0}^n \sigma(a_i) (\sigma(\alpha))^i = \sigma \left(\sum_{i=0}^n a_i \alpha^i \right) = \sigma(f(\alpha)) = \sigma(0) = 0,$$

which finishes the proof. \square

Theorem 2.6 *Let L/k be a finite field extension of degree $n := [L : k]$ and \bar{k} an algebraic closure of k . If there exist n different field homomorphisms $\sigma_1, \dots, \sigma_n : L \longrightarrow \bar{k}$ such that $\sigma_i|_k = id_k$, then L/k is simple.*

proof. Let $L = k[\alpha_1, \dots, \alpha_r]$ for some $r \geq 1$ and $\alpha_i \in L$. Prove the statement by induction on r .

r=1 $L = k[\alpha_1]$, hence L is simple.

r>1 Let now $L' = k[\alpha_1, \dots, \alpha_{r-1}]$. By hypothesis, L'/k is simple, say $L' = k[\beta]$. Then we have

$$L = k[\alpha_1, \dots, \alpha_r] = L'[\alpha_r] = k[\beta, \alpha_r]$$

with $\alpha := \alpha_r$. For $\lambda \in k$ consider

$$\gamma := \gamma_\lambda = \beta + \lambda\alpha.$$

By remark 2.4 it suffices to show

$$\sigma_i(\gamma) \neq \sigma_j(\gamma) \text{ for } i \neq j.$$

Assume there are $i \neq j$ such that $\sigma_i(\gamma) = \sigma_j(\gamma)$. Then

$$\sigma_i(\alpha) + \lambda\sigma_i(\beta) = \sigma_j(\alpha) + \lambda\sigma_j(\beta),$$

so we get

$$\sigma_i(\alpha) - \sigma_j(\alpha) + \lambda(\sigma_i(\beta) - \sigma_j(\beta)) = 0.$$

Consider the polynomial

$$g := \prod_{1 \leq i \neq j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha) + X \cdot (\sigma_i(\beta) - \sigma_j(\beta))).$$

By proposition 2.2 we may assume, that k is infinite. Note that g is not the zero polynomial: If $g = 0$, we find $i \neq j$ such that $\sigma_i(\alpha) = \sigma_j(\alpha)$ and $\sigma_i(\beta) = \sigma_j(\beta)$. Since α, β generate L , σ_i and σ_j must be equal on L , which is a contradiction. Therefore we find $\lambda \in k$, such that $g(\lambda) \neq 0$. Hence the minimal polynomial m_{γ_λ} of $\gamma_\lambda = \alpha + \lambda\beta$ has at least n zeroes, i.e.

$$\deg(m_{\gamma_\lambda}) \geq n \Rightarrow [k[\gamma_\lambda] : k] \geq n$$

and hence $k[\gamma_\lambda] = L$. □

Proposition 2.7 *Let $L = k[\alpha]$ be a simple, finite field extension, \bar{k} an algebraic closure of k . Let $f \in k[X]$ the minimal polynomial of α . Then for every zero β of f in \bar{k} there exists a unique homomorphism of fields $\sigma : L \longrightarrow \bar{k}$ such that $\sigma(\alpha) = \beta$.*

proof. The uniqueness is clear. It remains to show the existence. Define

$$\phi_\beta : k[X] \longrightarrow \bar{k}, \quad g \mapsto g(\beta).$$

We have $f(\beta) = 0$, thus $(f) \subseteq \ker(\phi_\beta)$ and hence ϕ_β factors to a homomorphism

$$\overline{\phi}_\beta : L \cong k[X]/(f) \longrightarrow \bar{k}$$

such that $\phi_\beta = \overline{\phi}_\beta \circ \pi$ where $\pi : k[X] \longrightarrow k[X]/(f)$ denotes the residue map. Let

$$\tau : L \longrightarrow k[X]/(f)$$

be an isomorphism. Then

$$\sigma := \overline{\phi}_\beta \circ \tau : L \longrightarrow \bar{k}$$

satisfies

$$\sigma(\alpha) = (\overline{\phi}_\beta \circ \tau)(\alpha) = \overline{\phi}_\beta(\tau(\alpha)) = \overline{\phi}_\beta(\overline{\alpha}) = \overline{\phi}_\beta(\pi(X)) = \phi_\beta(X) = \beta,$$

thus the claim. □

Corollary 2.8 *Let $f \in k[X]$ be a nonconstant polynomial. Then the splitting field of f over k is unique, i.e. any two splitting fields L, L' of f over k are isomorphic.*

proof. Let $L = k[\alpha_1, \dots, \alpha_n]$, $L' = k[\beta_1, \dots, \beta_m]$.

Assume that f is irreducible. W.l.o.g. we have $f(\alpha_1) = f(\beta_1) = 0$. By Proposition 2.6 we find field homomorphisms

$$\sigma_1 : k[\alpha_1] \longrightarrow k[\beta_1] \text{ such that } \sigma_1|_k = \text{id}_k \text{ and } \alpha_1 \mapsto \beta_1$$

$$\tau_1 : k[\beta_1] \longrightarrow k[\alpha_1] \text{ such that } \tau_1|_k = \text{id}_k \text{ and } \beta_1 \mapsto \alpha_1$$

Hence, since $\sigma_1 \circ \tau_1 = \text{id}_{k[\beta_1]}$ and $\tau_1 \circ \sigma_1 = \text{id}_{k[\alpha_1]}$, σ_1 and τ_1 are isomorphisms, i.e. $k[\alpha_1] \cong k[\beta_1]$. By induction on n the corollary follows. \square

Definition + proposition 2.9 Let L/k , L'/k be field extension.

(i) We define

$$\text{Hom}_k(L, L') := \{\sigma : L \longrightarrow L' \text{ field homomorphism s.t. } \sigma|_k = \text{id}_k\}$$

$$\text{Aut}_k(L) := \{\sigma : L \longrightarrow L \text{ field automorphism s.t. } \sigma|_k = \text{id}_k\}$$

(ii) If L/k is finite, \bar{k} an algebraic closure of k , then

$$|\text{Hom}_k(L, L')| \leq [L : k].$$

proof. Assume first $L = k[\alpha]$ for some algebraic $\alpha \in L$. Let f be the minimal polynomial of α over k , i.e. $f \in k[X]$, $\deg(f) = [L : k]$. By 2.4 and 2.6, the elements of $\text{Hom}_k(L, \bar{k})$ correspond bijectively to the zeroes of f . Then we get

$$|\text{Hom}_k(L, \bar{k})| = |\{\text{zeroes of } f \text{ in } \bar{k}\}| \leq \deg(f) = [L : k].$$

Now consider the general case. Let $L = k[\alpha_1, \dots, \alpha_n]$ and $L' = k[\alpha_1, \dots, \alpha_{n-1}] \subseteq L = L'[\alpha_n]$.

By induction on n we have $|\text{Hom}_k(L', \bar{k})| \leq [L' : k]$. Let now

$$f = \sum_{i=0}^d a_i X^i \in L'[X]$$

with coefficients $a_i \in L'$ be the minimal polynomial of α_n over L' . Let $\sigma \in \text{Hom}_k(L, \bar{k})$ and $\sigma' = \sigma|_{L'} \in \text{Hom}_k(L', \bar{k})$, $f^{\sigma'} := \sum_{i=0}^d \sigma'(a_i) X^i$. Then

$$f^{\sigma'}(\sigma(\alpha_n)) = \sum_{i=0}^d \sigma'(a_i) (\sigma(\alpha_n))^i = \sum_{i=0}^d \sigma(a_i) (\sigma(\alpha_n))^i = \sigma \left(\sum_{i=0}^d a_i \alpha_n^i \right) = 0.$$

Thus

$$|\{\text{Hom}_{L'}(L, \bar{k})\}| = |\{\sigma \in \text{Hom}_k(L, \bar{k}) \mid \sigma|_{L'} = \text{id}_{L'}\}| \leq \deg(f^{\sigma'}) = \deg(f) = [L' : L]$$

So all in all we have

$$|\text{Hom}_k(L, \bar{k})| \leq |\text{Hom}_k(L', \bar{k})| \cdot [L : L'] \leq [L : L'] \cdot [L' : k] = [L : k],$$

which is exactly the assignment. □

Definition 2.10 Let k be a field, $f = \sum_{i=0}^d a_i X^i \in k[X]$, \bar{k} an algebraic closure of k , L/k an algebraic field extension.

- (i) f is called *separable* over k , if f has $\deg(f)$ different roots in \bar{k} , i.e. there are no multiple roots.
- (ii) $\alpha \in L$ is called *separable* over k , if the minimal polynomial of α over k is separable.
- (iii) L/k is called *separable*, if any $\alpha \in L$ is separable over k .
- (iv) We define the *formal derivative* of f by

$$f' := \sum_{i=1}^d i \cdot a_i X^{i-1}$$

We have well known properties of the derivative:

$$(f + g)' = f' + g', \quad 1' = 0, \quad (f \cdot g)' = f \cdot g' + f' \cdot g.$$

Proposition 2.11 *Let*

$$f = \prod_{i=1}^n (X - \alpha_i) \in k[X], \quad \alpha_i \in \bar{k} \text{ for } 1 \leq i \leq n$$

Then the following statements are equivalent:

- (i) f is separable.
- (ii) $(X - \alpha_i) \nmid f'$ for $1 \leq i \leq n$.
- (iii) $\gcd(f, f') = 1$ in $k[X]$.

proof. '(i) \Leftrightarrow (ii)' We have

$$f' = \sum_{i=1}^n \prod_{j \neq i} (X - \alpha_j),$$

thus we get

$$(X - \alpha_i) \mid f' \Leftrightarrow (X - \alpha_i) \mid \prod_{j \neq i} (X - \alpha_j) \Leftrightarrow \alpha_i = \alpha_j \text{ for some } i \neq j.$$

'(ii) \Rightarrow (iii)' Assume $(X - \alpha_i) \nmid f'$ for all $1 \leq i \leq n$. Then

$$\gcd(f, f') = 1 \text{ in } \bar{k}[X] \implies \gcd(f, f') = 1 \text{ in } k[X].$$

'(iii) \Rightarrow (ii)' Let now $\gcd(f, f') = 1$ in $k[X]$. Then we can write

$$1 = af + bf', \quad a, b \in k[X].$$

Since again $k[X] \subseteq \bar{k}[X]$, we can write $1 = af + bf'$ for $a, b \in \bar{k}[X]$ and hence we obtain $\gcd(f, f') = 1$ in $\bar{k}[X]$. This implies

$$(X - \alpha_i) \nmid f' \text{ for all } 1 \leq i \leq n,$$

which was to be shown. \square

Corollary 2.12 (i) *An irreducible polynomial $f \in k[X]$ is separable if and only if $f' \neq 0$.*
(ii) *Any algebraic field extension in characteristic 0 is separable.*

Example 2.13 Let $\text{char}(k) = p > 0$. Then

$$X^p - 1 = (X - 1)^p$$

Let $k = \mathbb{F}_p(t)$ and $f = X^p - t \in \mathbb{F}_p(t)[X]$. Then $f' = 0$, hence f is not separable, but f is irreducible in $\mathbb{F}_p(t)[X]$.

Definition + proposition 2.14 Let L/k be a finite field extension, \bar{k} an algebraic closure of k and L .

- (i) $[L : k]_s := |\text{Hom}_k(L, \bar{k})|$ is called the *degree of separability* of L/k .
- (ii) If $L = k[\alpha]$ for some separable $\alpha \in L$ with minimal polynomial m_α over k , then

$$[L : k]_s = \deg(m_\alpha) = [L : k].$$

- (iii) If $L = k[\alpha]$ for some $\alpha \in L$, $\text{char}(k) = p > 0$, then there exists $n \geq 0$, such that

$$[L : k] = p^n \cdot [L : k]_s$$

- (iv) If $k \subseteq \mathbb{F} \subseteq L$ is an intermediate field extension, then

$$[L : k]_s = [L : \mathbb{F}]_s \cdot [\mathbb{F} : k]_s$$

proof. (i) This follows from Proposition 2.6:

$$[L : k]_s = |\text{Hom}_k(L, \bar{k})| = |\{\text{different zeroes of } f\}| = n = [L : k].$$

(iii) Write

$$f = \sum_{i=0}^n a_i X^i.$$

If α is separable over k , we are done with part (ii). Otherwise by Corollary 2.11 we have

$$f' = \sum_{i=1}^n i \cdot a_i \cdot X^{i-1} \stackrel{!}{=} 0 \iff i \cdot a_i \equiv 0 \pmod{p} \text{ for all } 0 \leq i \leq n$$

Thus we can write $f = g(X^p)$ for some $g \in k[X]$. Continue this way until we can write $f = g(X^{p^n})$ for some $n \in \mathbb{N}_0$ and separable g . Then

$$[k[\alpha] : k]_s = |\{\text{zeroes of } g \text{ in } \bar{k}\}| = \deg(g)$$

and thus we obtain

$$[k[\alpha] : k] = \deg(f) = \deg(g) \cdot p^n = p^n \cdot [k[\alpha] : k]_s.$$

(iv) Consider first the simple case $L = k(\alpha)$. Let

$$f = \sum_{i=0}^n a_i X^i \in \mathbb{F}[X]$$

be the minimal polynomial of α over \mathbb{F} . Let $\tau \in \text{Hom}_k(\mathbb{F}, \bar{k})$ and let

$$f^\tau = \sum_{i=0}^n \tau(a_i) X^i.$$

Given $\sigma \in \text{Hom}_k(L, \bar{k})$ with $\sigma|_{\mathbb{F}} = \tau$, notice that $\sigma(\alpha)$ is a zero of f^τ . Moreover by Proposition 2.6, every zero β of f^τ determines a unique σ such that $\sigma(\alpha) = \beta$. Thus we have

$$\begin{aligned} |\{\sigma \in \text{Hom}_k(L, \bar{k}) \mid \sigma|_{\mathbb{F}} = \tau\}| &= |\{\beta \in \bar{k} \mid f^\tau(\beta) = 0\}| \\ &= |\{\beta \in \bar{k} \mid f(\beta) = 0\}| \stackrel{2.6}{=} [L : \mathbb{F}]_s. \end{aligned}$$

We conclude

$$\begin{aligned} [L : k]_s &= |\text{Hom}_k(L, \bar{k})| = \left| \bigcup_{\tau \in \text{Hom}_k(\mathbb{F}, \bar{k})} \{\sigma \in \text{Hom}_k(L, \bar{k}) \mid \sigma|_{\mathbb{F}} = \tau\} \right| \\ &= |\{\sigma \in \text{Hom}_k(L, \bar{k}) \mid \sigma|_{\mathbb{F}} = \tau\}| \cdot |\text{Hom}_k(\mathbb{F}, \bar{k})| \\ &= [L : \mathbb{F}]_s \cdot [\mathbb{F} : k]_s \end{aligned}$$

For the general case we can write $L = \mathbb{F}(\alpha_1, \dots, \alpha_n)$. Define $L_i := \mathbb{F}(\alpha_1, \dots, \alpha_i)$, $L_0 := \mathbb{F}$

and $L_n = L$. Then L_i/L_{i-1} is simple and by the special case above we get

$$\begin{aligned}
[L : k]_s &= [L_n : L_{n-1}]_s \cdot [L_{n-1} : k]_s \\
&\vdots \\
&= [L_n : L_{n-1}]_s \cdots [L_2 : L_1]_s \cdot [L_1 : L_0]_s \cdot [L_0 : k]_s \\
&= [L_n : L_{n-1}]_s \cdots [L_2 : L_1]_s \cdot [L_1 : \mathbb{F}]_s \cdot [\mathbb{F} : k]_s \\
&= [L_n : L_{n-1}]_s \cdots [L_2 : \mathbb{F}]_s \cdot [\mathbb{F} : k]_s \\
&\vdots \\
&= [L_n : \mathbb{F}]_s \cdot [\mathbb{F} : k]_s \\
&= [L : \mathbb{F}]_s \cdot [\mathbb{F} : k]_s,
\end{aligned}$$

which implies the claim. \square

Proposition 2.15 *A finite field extension L/k is separable if and only if $[L : k] = [L : k]_s$.*

proof. '⇒' Let $L = k[\alpha_1, \dots, \alpha_n]$. Prove this by induction on n .

n=1 This is proposition 12.2(ii)

n>1 Let $L' = k[\alpha_1, \dots, \alpha_{n-1}]$. Then by induction hypothesis $[L' : k]_s = [L' : k]$. Moreover $[L : L']_s = [L : L']$, since L/L' is simple by $L = L'[\alpha_n]$. By proposition 12.2 (iv) we get

$$[L : k]_s = [L : L']_s \cdot [L' : k]_s = [L : L'] \cdot [L' : k] = [L : k].$$

'⇐' Let $\alpha \in L$ and $f = m_\alpha \in k[X]$ its minimal polynomial. If $\text{char}(k) = 0$, f is separable, so α is separable by corollary 2.11. Let now $\text{char}(k) = p > 0$. By proposition 12.2 there exists $n \geq 0$ such that

$$[k[\alpha] : k] = p^n \cdot [k[\alpha] : k]_s$$

We find

$$[L : k] = [L : k[\alpha]] \cdot [k[\alpha] : k] \geq [L : k[\alpha]]_s \cdot p^n [k[\alpha] : k]_s = p^n [L : k]_s = p^n [L : k],$$

Hence we must have $n = 0$, i.e. $[k[\alpha] : k] = [k[\alpha] : k]_s$. Thus α is separable over k . \square

§ 3 Galois extensions

Definition 3.1 A field extension L/k is called *normal*, if there is a subset $\mathcal{F} \subseteq k[X]$ such that L is the smallest field which any $f \in \mathcal{F}$ splits over.

Remark 3.2 Let L/k be a normal field extension, \bar{k} an algebraic closure of k . Then

$$\text{Hom}_k(L, \bar{k}) = \text{Aut}_k(L).$$

proof. '⊇' Clear.

'⊆' Let L be the splitting field of \mathcal{F} . Let

$$f = \sum_{i=0}^d a_i X^i \in \mathcal{F}$$

and $\alpha \in L$ such that $f(\alpha) = 0$. Let $\sigma \in \text{Hom}_k(L, \bar{k})$. Then

$$f(\sigma(\alpha)) = \sum_{i=0}^d a_i \sigma(\alpha)^i = \sum_{i=0}^d \sigma(a_i) \sigma(\alpha)^i = \sigma \left(\sum_{i=0}^d a_i \alpha^i \right) = \sigma(f(\alpha)) = 0,$$

hence $\sigma(\alpha)$ is zero of f . Since f splits over L , i.e. all zeroes of f are in L , we have $\sigma(\alpha) \in L$. Moreover L is generated over k by the zeroes of $f \in \mathcal{F}$, thus $\sigma(L) \subseteq L$ and hence we get $\sigma \in \text{Hom}_k(L, L)$.

It remains to show bijectivity. σ is clearly injective. For the surjectivity consider that σ permutes all the zeroes of any $f \in \mathcal{F}$. Finally $\sigma \in \text{Aut}_k(L)$. \square

Definition 3.3 An algebraic field extension L/k is called *Galois extension* or *Galois*, if it is normal and separable. In this case, the *Galois group* of L/k is defined as

$$\text{Gal}(L, k) := \text{Aut}_k(L).$$

Proposition 3.4 A finite field extension L/k is Galois if and only if $|\text{Aut}_k(L)| = [L : k]$.

proof. '⇒' We have

$$|\text{Aut}_k(L)| = |\text{Hom}_k(L, \bar{k})| = [L : k]_s = [L : k]$$

'⇐' We have to show that L/k is separable and normal. First we see

$$[L : k] = |\text{Aut}_k(L)| \leq |\text{Hom}_k(L, \bar{k})| = [L : k]_s \leq [L : k]$$

Hence we have equality on each inequality, i.e. $[L : k] = [L : k]_s$ and L/k is separable.

By Theorem 2.5 we know that L/k is simple, say $L = k[\alpha]$ for some $\alpha \in L$.

Let $m_\alpha \in k[X]$ be the minimal polynomial of α over k . Moreover let $\beta \in \bar{k}$ be another zero of m_α . Then there exists $\sigma \in \text{Hom}_k(L, \bar{k})$ such that $\sigma(\alpha) = \beta$. By the (in-)equality above we know $|\text{Aut}_k(L)| = |\text{Hom}_k(L, \bar{k})|$, hence $\sigma(\beta) \in L$. Since β was arbitrary, m_α splits over L , i.e. L is the splitting field of f over k . Thus L/k is normal and finally Galois. \square

Example 3.5 All quadratic field extensions are normal. Moreover, if $\text{char}(k) \neq 2$, then all quadratic field extensions of k are Galois.

Remark 3.6 Let L/k be a Galois extension and $k \subseteq K \subseteq L$ an intermediate field.

(i) Then L/K is Galois and

$$\text{Gal}(L/K) \leq \text{Gal}(L/k)$$

(ii) If K/k is Galois, then $\text{Gal}(L/K) \trianglelefteq \text{Gal}(L/k)$ is a normal subgroup and

$$\text{Gal}(L/k) / \text{Gal}(L/K) \cong \text{Gal}(K/k).$$

proof. (i) Clearly L/K is normal, since L is the splitting field for the same polynomials as in L/k . Let now $\alpha \in L$. Then the minimal polynomial m_α of α over K divides the minimal polynomial m'_α of α over k , since $k \subseteq K$. Since m'_α has no multiple roots, m_α does not either and hence L/K is separable and thus Galois.

(ii) Define

$$\rho : \text{Gal}(L/k) \longrightarrow \text{Gal}(K/k), \sigma \mapsto \sigma|_K.$$

ρ is well defined since $\sigma|_K \in \text{Hom}_K k(K, \bar{k}) = \text{Aut}_k(K) = \text{Gal}(K/k)$ as K/k is Galois:

$$[K : k] = |\text{Aut}_k(K)| \leq |\text{Hom}_k(K, \bar{k})| \leq [K : k].$$

Moreover ρ is surjective. For the kernel we get

$$\ker(\rho) = \{\sigma \in \text{Gal}(L/k) \mid \sigma|_K = \text{id}_K\} = \text{Gal}(L/K)$$

and thus we obtain $\text{Gal}(L/k) / \text{Gal}(L/K) \cong \text{Gal}(K/k)$. □

Theorem 3.7 (Main theorem of Galois theory) Let L/k be a finite Galois extension and $G := \text{Gal}(L/k)$. Then the subgroups $H \leq G$ correspond bijectively to the intermediate fields $k \subseteq K \subseteq L$. Explicitly we have inverse maps

$$K \mapsto \text{Gal}(L/K) \leq G$$

$$H \mapsto L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

proof. Clearly L^H is a field for any $H \leq G$. We now have to show

(i) $\text{Gal}(L/L^H) = H$ for any $H \leq G$.

(ii) $L^{\text{Gal}(L/K)} = K$ for any intermediate field $k \subseteq K \subseteq L$.

These prove the theorem.

(i) We show both inclusion.

' \supseteq ' Clear by definition.

' \subseteq ' It suffices to show $|\text{Gal}(L/L^H)| \leq |H|$. By 3.4(i) we have

$$|\text{Gal}(L/L^H)| = [L : L^H].$$

By theorem 2.5 L/L^H is simple, say $L = L^H[\alpha]$. Define

$$f = \prod_{\sigma \in H} (X - \sigma(\alpha))$$

with $\deg(f) = |H|$. Further, since $\text{id} \in H$, we have $f(\alpha) = 0$. Clearly $f \in L[X]$. We want to show that $f \in L^H[X]$. Therefore for $\tau \in H$ define

$$g^\tau := \sum_{i=0}^n \tau(a_i) X^i \text{ for } g = \sum_{i=0}^n a_i X^i$$

Then for f as defined above we have

$$f^\tau = \prod_{\sigma \in H} (X - \tau(\sigma(\alpha))) = \prod_{\sigma \in H} (X - \sigma(\alpha)) = f$$

hence $f \in L^H[X]$. From $f(\alpha) = 0$ we know that the minimal polynomial m_α of α over L^H divides f , thus

$$|\text{Gal}(L/L^H)| = [L : L^H] = \deg(m_\alpha) \leq \deg(f) = |H|$$

(ii) '⊇' Clear by definition.

'⊆' Let $H := \text{Gal}(L/K)$. Since $K \subseteq L^H$ it suffices to show $[L^H : K] = 1$. Since L^H/K is separable, this is equivalent to $[L^H : K]_s = 1$. Let now $\sigma \in \text{Hom}_K(L^H, \bar{k})$. By 2.6 we can extend σ to

$$\tilde{\sigma} : L \longrightarrow \bar{k}$$

with $\tilde{\sigma}|_{L^H} = \sigma$. Explicitly: Let $L = L^H[\alpha]$ and $f \in L^H[X]$ its minimal polynomial. Choose a zero $\beta \in \bar{k}$ of f^σ . Then by 2.6 there exists $\tilde{\sigma} : L \longrightarrow \bar{k}$ with $\tilde{\sigma}(\alpha) = \beta$ and $\tilde{\sigma}|_{L^H} = \sigma$. We get $\tilde{\sigma} \in \text{Gal}(L/K) = H$ and $\sigma = \tilde{\sigma}|_{L^H} = \text{id}_K$ which finally implies $[L^H : K] = 1$. \square

Remark 3.8 *An intermediate field $k \subseteq K \subseteq L$ is Galois over k if and only if $\text{Gal}(L/K) \trianglelefteq \text{Gal}(L/k)$ is a normal subgroup.*

proof. '⇒' If K/k is Galois, then $\text{Gal}(L/K) = \ker(\rho)$ is a normal subgroup by 3.5.

'⇐' Conversely let $\text{Gal}(L/K) =: H \trianglelefteq \text{Gal}(L/k)$ be a normal subgroup. By 3.4 it suffices to show $\text{Hom}_k(K, \bar{k}) = \text{Aut}_k(K)$. Let now $\sigma \in \text{Hom}_k(K, \bar{k})$ and $\alpha \in K$. Extend σ to $\tilde{\sigma} : L \longrightarrow \bar{k}$. Then $\tilde{\sigma} \in \text{Gal}(L/k)$. By the theorem it suffices to show that $\sigma(\alpha) \in L^{\text{Gal}(L/K)} = K$, i.e. $\sigma(K) \subseteq K$. Let $\tau \in \text{Gal}(L/L^H)$. Then, since $\text{Gal}(L/K)$ is normal, we obtain

$$\tau(\sigma(\alpha)) = \tau(\tilde{\sigma}(\alpha)) = (\tilde{\sigma} \circ \tau')(\alpha) = \tilde{\sigma}(\alpha) = \sigma(\alpha),$$

which implies the claim. \square

Example 3.9 Let $k = \mathbb{Q}$, $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$. Further let $L = L(f)$ be the splitting field of f over \mathbb{Q} . What is $\text{Gal}(L/\mathbb{Q})$?

We first want to show that f is irreducible. But this immediately follows by Eisenstein's criterion for irreducibility with $p = 2$.

Thus L is an extension of $\mathbb{Q}/(f)$. Therefore $[L : \mathbb{Q}]$ is multiple of $[\mathbb{Q}/(f)] = 5$, hence $|\text{Gal}(L/\mathbb{Q})|$ is divisible by 5. By Lagrange's theorem we know that $\text{Gal}(L/\mathbb{Q})$ contains an element of order 5. Further note that f has exactly 3 zeroes in \mathbb{R} . With

$$\lim_{x \rightarrow -\infty} f(x) = -\infty < 0, \quad f(0) = 2 > 0, \quad f(1) = -1 < 0, \quad \lim_{x \rightarrow \infty} f(x) = \infty > 0$$

we see by the intermediate value theorem that f has at least 3 zeroes. Moreover

$$f' = 5X^4 - 4 = 5 \cdot \left(X^4 - \frac{4}{5}\right) = 5 \cdot \left(X^2 - \frac{2}{\sqrt{5}}\right) \cdot \left(X^2 + \frac{2}{\sqrt{5}}\right)$$

Obviously, since the second factor has not real zeroes, the derivative of f has 2 zeroes, hence f has at most 3 zeroes. Together we obtain that f has exactly 3 zeroes. Since f splits over \mathbb{C} , f has two more conjugate zeroes in \mathbb{C} , say $\beta, \bar{\beta}$. Hence we know that the conjugation in \mathbb{C} must be an element of $\text{Gal}(L/\mathbb{Q})$.

To sum it up, we know: $\text{Gal}(L/\mathbb{Q})$ is isomorphic to a subgroup of S_5 , contains the conjugation, which corresponds to a transposition and moreover an element of order 5, i.e. a 5-cycle. But these two elements generate the whole group S_5 . Hence we have $\text{Gal}(L/\mathbb{Q}) \cong S_5$.

Proposition 3.10 (Cyclotomic fields) Let k be a field, $n \in \mathbb{N}$, $\text{char}(k) \nmid n$ and L the splitting field of the polynomial $f = X^n - 1$.

Then L/k is Galois and $\text{Gal}(L_n/k)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

proof. We have $f' = nX^{n-1}$ and $f' = 0 \Leftrightarrow X = 0$ but $f(0) \neq 0$, hence f' and f_n are coprime. Thus f is separable. Since L is the splitting field of f by definition, L/k is normal, thus Galois. The zeroes of f form a group $\mu_n(k)$ under multiplication. By proposition 2.3 $\mu_n(k)$ is cyclic. Let ζ_n be a generator of $\mu_n(k)$. Define a map

$$\chi_n : \text{Gal}(L_n/k) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \quad \sigma \mapsto m \text{ if } \sigma(\zeta_n) = \zeta_n^m$$

where m is relatively coprime to n . We obtain that χ_n is a homomorphism of groups since for $\sigma_1, \sigma_2 \in \text{Gal}(L_n/k)$ we have $\sigma_2\sigma_1(\zeta_n) = \sigma_2(\zeta_n^{k_1}) = (\zeta_n^{k_1})^{k_2} = \zeta_n^{k_1 k_2}$ and hence

$$\chi_n(\sigma_1\sigma_2) = k_1 \cdot k_2 = \chi_n(\sigma_1) \cdot \chi_n(\sigma_2).$$

Moreover χ_n is injective, since

$$\chi_n(\sigma) = 1 \Leftrightarrow \sigma(\zeta_n) = \zeta_n \Leftrightarrow \sigma = \text{id}.$$

This proves the proposition. Recall that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ Where ϕ is Euler's ϕ -function. \square

§ 4 Solvability of equations by radicals

Definition + remark 4.1 Let k be a field, $f \in k[X]$ separable.

- (i) Let $L(f)$ be the splitting field of f over k . The *Galois group of the equation* $f = 0$ is defined by

$$\text{Gal}(f) := \text{Gal}(L(f)/k).$$

- (ii) There exists an injective homomorphism of groups $\text{Gal}(f) \longrightarrow S_n$ where $n := \deg(f)$.
 (iii) If L/k is a finite, separable field extension, the $\text{Aut}_k(L)$ is isomorphic to a subgroup of S_n , where $n = [L : k]$.

proof. (ii) Clear, since automorphisms permute the zeroes of f , of which we have at most n .

- (iii) We know L/k is simple, say $L = k[\alpha]$ for some $\alpha \in L$. Let m_α be the minimal polynomial of α over k . Then $\deg(f) = n$. Every $\sigma \in \text{Aut}(L/k)$ maps α to a zero of f and the same for every zero of f . Hence the claim follows. \square

Definition 4.2 (i) A simple field extension $L = k[\alpha]$ of a field k is called an *elementary radical extension* if either

- (1) α is a root of unity, i.e. a zero of the polynomial $X^n - 1$ for some $n \in \mathbb{N}$.
- (2) α is a root of $X^n - \gamma$ for some $\gamma \in k, n \in \mathbb{N}$ such that $\text{char}(k) \nmid n$.
- (3) α is a root of $X^p - X - \gamma$ for some $\gamma \in k$ where $p = \text{char}(k)$.

In the following, we will denote (1), (2) and (3) as the three *types* of elementary radical extensions.

- (ii) A finite field extension L/k is called a *radical extension*, if there is a field extension L'/L and a chain of field extension

$$k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L'$$

such that L_i/L_{i-1} is an elementary radical extension for every $1 \leq i \leq m$.

Example 4.3 Let $k = \mathbb{Q}$, $f = X^3 - 3X + 1$. The zeroes of f (in \mathbb{C}) are

$$\alpha_1 = \zeta + \zeta^{-1} \in \mathbb{R}, \quad \alpha_2 = \zeta^2 + \zeta^{-2} \quad \text{and} \quad \alpha_3 = \zeta^4 + \zeta^{-4}$$

where $\zeta = e^{\frac{2\pi i}{9}}$ is a primitive ninth root of unity. We show this exemplarily for α_1 . We have

$$f(\alpha_1) = (\alpha_1^3 - 3\alpha_1 + 1) = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} - 3\zeta - 3\zeta^{-1} + 1 = \zeta^3 + \zeta^{-3} - 3 + 1 = 0$$

where we use $\zeta^{-3} = \overline{\zeta^3}$ and since $z + \bar{z} = 2 \cdot \Re(z)$ for any $z \in \mathbb{C}$ we have

$$\zeta^3 + \zeta^{-3} = 2 \cdot \Re(\zeta^3) = 2 \cdot \Re\left(e^{\frac{2\pi i}{3}}\right) = 2 \cdot \Re\left(\cos \frac{2\pi}{3} + i \cdot \sin \frac{2\pi}{3}\right) = 2 \cdot \cos \frac{2\pi}{3} = 2 \cdot \left(-\frac{1}{2}\right) = -1.$$

Further we have

$$\alpha_1^2 = \zeta^2 + 2\zeta^{-2} + 2 = \alpha_2 + 2,$$

hence $\alpha_2 \in \mathbb{Q}(\alpha_1)$ and $\alpha_1 + \alpha_2 + \alpha_3 = 0$, hence $\alpha_3 \in \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1)$.

This means that $\mathbb{Q}(\alpha_1)$ contains all the zeroes of f , i.e. is a splitting field of f . We conclude

$$\mathbb{Q}(\alpha_1) \cong \mathbb{Q}/(f), \quad [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3.$$

From the f we see that $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ is not an elementary radical extension, but a radical extension, since for $\mathbb{Q}(\zeta)$ we have $\mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta)/\mathbb{Q}$ is an elementary radical extension.

Definition 4.4 Let k be a field, $f \in k[X]$ a separable, non-constant polynomial. We say f is *solvable by radicals*, if the splitting field $L(f)$ is a radical extension.

Remark 4.5 Let L/k be an elementary field extension, referring to Definition 4.1 of type

- (1) $L = k[\zeta]$ for some root of unity ζ (primitive for some suitable $n \in \mathbb{N}$, $\text{char}(k) \nmid n$). Then L/k is Galois with abelian Galois group

$$\text{Gal}(L/k) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

- (2) $L = k[\alpha]$ where α is a root of $X^n - \gamma$ for some $\gamma \in k$, $n \in \mathbb{N}$, $\text{char}(k) \nmid n$. If k contains the n -th roots of unity, i.e. $\mu_n(\bar{k})$, then L/k is Galois with cyclic Galois group.
- (3) $L = k[\alpha]$, where α is a root of $X^p - X - \gamma$ for some $\gamma \in k^\times$. Then L/k is Galois with Galois group

$$\text{Gal}(L/k) \cong \mathbb{Z}/p\mathbb{Z}.$$

proof. (1) We proved this in proposition 3.9.

- (2) Let $\zeta \in k$ be a primitive n -th root of unity. Then $\zeta^i \cdot \alpha$ is a zero of $X^n - \gamma$, where we assume n to be minimal such that $X^n - \gamma$ is irreducible. Then L contains all roots of $X^n - \gamma$, i.e. L/k is normal and thus Galois with

$$|\text{Gal}(L/k)| = [L : k] = \deg(X^n - \gamma) = n$$

Since the automorphism $\sigma \in \text{Gal}(L/k)$ that maps $\alpha \mapsto \zeta \cdot \alpha$ has order n , $\text{Gal}(L/k)$ is cyclic.

- (3) $f = X^p - X - \gamma$ has p zeroes in $L = k[\alpha]$. Since $f(\alpha) = 0$, we have

$$f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - \gamma = \alpha^p + 1 - \alpha - 1 - \gamma = \alpha^p - \alpha - \gamma = f(\alpha) = 0$$

Hence L is the splitting field of f and L/k is normal. Moreover $f' = -1 \neq 0$, hence L/k is separable and thus Galois with

$$|\text{Gal}(L/k)| = [L : k] = \deg(f) = p$$

Further $\text{Gal}(L/k) \ni \sigma : \alpha \mapsto \alpha + 1$ has order p , hence $\text{Gal}(L/k)$ is cyclic and thus

$$\text{Gal}(L/k) \cong \mathbb{Z}/p\mathbb{Z},$$

which is the claim. \square

Remark 4.6 Let L/k be an elementary radical extension of type (ii), i.e. $L = k[\alpha]$, where α is the root of $f = X^n - \gamma$ for some $\gamma \in k, n \geq 1, \text{char}(k) \nmid n$. $X^n - \gamma$ is irreducible

Let \mathbb{F} be a splitting field of $X^n - 1$ over k and $L\mathbb{F} = k(\alpha, \zeta)$ be the compositum of L and \mathbb{F} , i.e. the smallest subfield of \bar{k} containing L and \mathbb{F} .

$$\begin{array}{ccc} & \tilde{L} = L\mathbb{F} & \\ & \swarrow \quad \searrow & \\ L = k[\alpha] & & k[\zeta] = \mathbb{F} \\ & \swarrow \quad \searrow & \\ & k & \end{array}$$

\tilde{L} is a splitting field of $X^n - \gamma$ over \mathbb{F} , hence \tilde{L}/\mathbb{F} is Galois and by 4.4(ii), $\text{Gal}(\tilde{L}/\mathbb{F})$ is cyclic. Moreover \mathbb{F}/k is Galois and $\text{Gal}(\mathbb{F}/k)$ is abelian. Hence \tilde{L}/k is Galois and

$$\text{Gal}(\tilde{L}/k) / \text{Gal}(\tilde{L}/\mathbb{F}) \cong \text{Gal}(\mathbb{F}/k)$$

i.e. we have a short exact sequence

$$1 \longrightarrow \underbrace{\text{Gal}(\tilde{L}/\mathbb{F})}_{\text{cyclic}} \xrightarrow{\text{inj.}} \text{Gal}(\tilde{L}/k) \xrightarrow{\text{surj.}} \underbrace{\text{Gal}(\mathbb{F}/k)}_{\text{abelian}} \longrightarrow 1.$$

Example 4.7 Let $k = \mathbb{Q}$, $f = X^3 - 2$. Then $L = \mathbb{Q}[\alpha]$ with $\alpha = \sqrt[3]{2}$ and $\mathbb{F} = \mathbb{Q}[\zeta]$ with $\zeta = e^{\frac{2\pi}{3}}$. Then $\tilde{L} = L(f)$ with $[\tilde{L} : \mathbb{Q}] = 6$. We obtain

$$\text{Gal}(\tilde{L}/\mathbb{F}) \cong \mathbb{Z}/3\mathbb{Z}, \text{Gal}(\mathbb{F}/k) \cong \mathbb{Z}/2\mathbb{Z}, \text{Gal}(\tilde{L}/\mathbb{Q}) \cong S_3.$$

Definition 4.8 A group G is called *solvable*, if there exists a chain of subgroups

$$1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$$

where $G_{i-1} \triangleleft G_i$ is a normal subgroup and G_i/G_{i-1} is abelian for all $1 \leq i \leq n$.

Example 4.9 (i) Every abelian group is solvable.

(ii) S_4 is solvable by

$$1 \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

where $V_4 = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$. For the quotients we have

$$V_4/\{1\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}, \quad S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}.$$

(iii) S_5 is not solvable, since A_5 is simple (EAZ 6.6) but the quotient $A_5/\{1\}$ is not abelian.

(iv) If G, H are solvable groups, then the direct product $G \times H$ is solvable.

Proposition 4.10 (i) *Let G be a solvable group. Then*

(1) *Every subgroup $H \leq G$ is solvable.*

(2) *Every homomorphic image of G is solvable.*

(ii) *Let*

$$1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1$$

be a short exact sequence. Then G is solvable if and only if G' and G'' are solvable.

proof. (i) (1) Let G be solvable, i.e. we have a chain $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$. Let $G' \leq G$ a subgroup. Then

$$1 \triangleleft G_1 \cap G' \triangleleft \dots \triangleleft G_n \cap G' = G'$$

is a chain of subgroups of G' and we have $G_i \cap G' \triangleleft G_{i+1} \cap G'$ and moreover

$$(G_{i+1} \cap G') / (G_i \cap G') \cong G_i(G_{i+1} \cap G') / G_i \leq G_{i+1} / G_i.$$

Hence we have abelian quotients and G' is solvable.

(2) Let H be a group and $\phi : G \longrightarrow H$ be a surjective homomorphism of groups. Let

$$1 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G.$$

Let $H_i := \phi(G_i)$. Then H_i is normal in H_{i+1} . It remains to show that the quotients are abelian. Consider

$$\begin{array}{ccccc} G_i & \longrightarrow & G_{i+1} & \xrightarrow{\pi_G} & G_{i+1}/G_i \\ \downarrow \phi & & \downarrow \phi & \searrow \tilde{\phi} & \downarrow \bar{\phi} \\ H_i & \longrightarrow & H_{i+1} & \xrightarrow{\pi_H} & H_{i+1}/H_i \end{array}$$

(We have $G_i \subseteq \ker(\tilde{\phi})$, since $\phi(G_i) = H_i = \ker(\pi_H)$. Hence $\tilde{\phi}$ factors to

$$\bar{\phi} : \underbrace{G_{i+1}/G_i}_{\text{abelian}} \twoheadrightarrow \underbrace{H_{i+1}/H_i}_{\text{abelian!}}$$

and we get $\bar{\phi}(a)\bar{\phi}(b) = \bar{\phi}(ab) = \bar{\phi}(ba) = \bar{\phi}(b)\bar{\phi}(a)$, hence the quotient is abelian and

$H = \phi(G)$ is solvable.

(ii) ' \Rightarrow ' Clear.

' \Leftarrow ' Let

$$1 \triangleleft G_1 \triangleleft \cdots \triangleleft G_m = G', \quad 1 \triangleleft H_{m+1} \triangleleft \cdots \triangleleft H_{m+k} = G''$$

chains of subgroups with abelian quotients. Define

$$G_i := \pi^{-1}(H_i)_{m+1 \leq i \leq m+k}, \quad \pi : G \longrightarrow G''.$$

Then G_i is normal in G_{i+1} and we have

$$G_{m+0} = \pi^{-1}(\{1\}) = G' = G_m.$$

For $m+1 \leq i \leq m+k$ we have

$$G_{i+1}/G_i = \pi^{-1}(H_{i+1}/H_i) \cong H_{i+1}/H_i$$

and hence the chain

$$1 \triangleleft G_1 \triangleleft \cdots \triangleleft G_m = G' \triangleleft G_{m+1} \triangleleft \cdots \triangleleft G_{m+k} = G$$

reveals the solvability of G . □

Lemma 4.11 *A finite separable field extension L/k is a radical extension if and only if there exists a finite Galois extension L'/k , $L \subseteq L'$ such that $\text{Gal}(L'/k)$ is solvable.*

proof. ' \Rightarrow ' Let

$$k = k_0 = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n$$

a chain as in definition 4.7 with $L \subseteq L_n$. we prove the statement by induction.

n=1 This is exactly remark 4.5, 4.6

n>1 By induction hypothesis L_{n-1}/k is solvable. Moreover L_n/L_{n-1} is solvable, too. This is equivalent to the fact, that L_{n-1} is contained in a Galois extension \tilde{L}_{n-1}/k such that $\text{Gal}(\tilde{L}/k)$ is solvable and L_n is contained in a Galois extension \tilde{L}/L_{n-1} such that $\text{Gal}(\tilde{L}/L_{n-1})$ is solvable. We have a diagramm

$$\begin{array}{ccccccc} \tilde{L}_{n-1} & \subseteq & \tilde{L}L_{n-1} & := & \mathbb{M} & & \\ \cup & & & & \cup & & \\ k & \subseteq & L_{n-1} & \subseteq & L_n & \subseteq & \tilde{L} \end{array}$$

We obtain, that \mathbb{M} is Galois over L_{n-1} , since $\tilde{L}, \tilde{L}_{n-1}$ are Galois over L_{n-1} , hence by

$$\iota : \text{Gal}(\mathbb{M}/\tilde{L}_{n-1}) \longrightarrow \text{Gal}(\tilde{L}/L_{n-1}), \quad \sigma \mapsto \sigma|_{\tilde{L}}$$

an injective homomorphism of groups is given, hence

$$\text{Gal}(\mathbb{M}/\tilde{L}_{n-1}) \leq \text{Gal}(\tilde{L}/L_{n-1})$$

is solvable as a subgroup of a solvable group.

Let now $\tilde{\mathbb{M}}/\mathbb{M}$ be a minimal extension, such that $\tilde{\mathbb{M}}/k$ is Galois. Explicitly, $\tilde{\mathbb{M}}$ is defined as the *normal hull* of \mathbb{M} , i.e. the splitting field of the minimal polynomial of a primitive element of \mathbb{M}/k .

Now we want to show that $\text{Gal}(\mathbb{M}/k)$ is solvable. This finishes the proof of the sufficiency of our Lemma. Consider the short exact sequence

$$1 \longrightarrow \text{Gal}(\tilde{\mathbb{M}}/\tilde{L}_{n-1}) \longrightarrow \text{Gal}(\mathbb{M}/k) \longrightarrow \text{Gal}(\tilde{L}_{n-1}/k) \longrightarrow 1.$$

By proposition 4.8 and our induction hypothesis it suffices to show that $\text{Gal}(\tilde{\mathbb{M}}/\tilde{L}_{n-1})$ is solvable. Therefore observe that $\tilde{\mathbb{M}}$ is generated over k by the $\sigma(k)$ for $\sigma \in \text{Hom}_k(\mathbb{M}, \bar{k})$, where \bar{k} denotes an algebraic closure of k . For any $\sigma \in \text{Hom}_k(\mathbb{M}, \bar{k})$, $\sigma(\mathbb{M})/\sigma(L_{n-1}) = \sigma(\mathbb{M})/\tilde{L}_{n-1}$ is Galois. Hence

$$\Phi : \text{Gal}(\tilde{\mathbb{M}}/\tilde{L}_{n-1}) \longrightarrow \prod_{\sigma \in \text{Hom}_k(\mathbb{M}, \bar{k})} \text{Gal}(\sigma(\mathbb{M})/\tilde{L}_{n-1}), \quad \tau \mapsto (\tau|_{\sigma(\mathbb{M})})_{\sigma}$$

is injective. Hence $\text{Gal}(\tilde{\mathbb{M}}/\tilde{L}_{n-1})$ is solvable as a subgroup of a product of solvable groups.

' \Leftarrow ' Let now \tilde{L}/L finite such that $\text{Gal}(\tilde{L}/k)$ is solvable. Let

$$1 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$$

be a chain of subgroups as in definition 4.7. By the main theorem we have bijectively correspond intermediate fields

$$\tilde{L} = L_n \supseteq L_{n-1} \supseteq \dots \supseteq L_0 = k$$

where L_{i+1}/L_i is Galois and $\text{Gal}(L_{i+1}/L_i) \cong \mathbb{Z}/p\mathbb{Z}$ for all $1 \leq i \leq n-1$. We now have to differ between three cases.

case 1 $p_i = \text{char}(k)$. Then L_{i+1}/L_i is an elementary radical extension of type (iii), i.e. L/k is a radical extension.

case 2 $p_i \neq \text{char}(k)$ and L_i contains a primitive p_i -th root of unity. Then L_{i+1}/L_i is an elementary radical extension of type (ii), i.e. L/k is a radical extension.

case 3 $p_i \neq \text{char}(k)$ and L_i does not contain any primitive p_i -th root of unity. Then define

$$d := \prod_{p \in \mathbb{P}, p \mid |G|} p$$

And let \mathbb{F} be the splitting field of $X^d - 1$ over k . Then \mathbb{F}/k is an elementary radical extension of type (i). Let $L' := \tilde{L}\mathbb{F}$ be the composite of \tilde{L} and \mathbb{F} in \bar{k} . Then L'/\mathbb{F} is Galois by remark 4.5. Let $G' = \text{Gal}(L'/\mathbb{F})$. Consider the map

$$\Psi : \text{Gal}(L'/\mathbb{F}) \longrightarrow \text{Gal}(\tilde{L}/k), \sigma \mapsto \sigma|_{\tilde{L}}.$$

Ψ is a well defined injective homomorphism of groups, hence $\text{Gal}(L'/\mathbb{F}) \leq \text{Gal}(\tilde{L}/k)$ is solvable as a subgroup of a solvable group. Let

$$1 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G'$$

a chain of subgroups as in definition 4.7. Let further be

$$k \subseteq \mathbb{F} = L_0 \subseteq L_1 \subseteq \dots \subseteq L_n = L'$$

be the corresponding chain of intermediate fields, i.e. L_i/L_{i-1} is Galois and $\text{Gal}(L_i/L_{i-1}) \cong \mathbb{Z}/p\mathbb{Z}$ for $1 \leq i \leq n$. Hence, L_i/L_{i-1} is a radical extension of type (ii). Thus L/k is a radical extension, which finishes the proof. \square

Theorem 4.12 *Let $f \in k[X]$ be a separable non-constant polynomial. Then f is solvable by radicals if and only if $\text{Gal}(f) = \text{Gal}(L(f)/k)$ is solvable.*

proof. Let f be solvable by radicals, i.e. $L(f)/k$ be a radical field extension.

$\iff L(f)$ is contained in some Galois extension \tilde{L}/k and $\text{Gal}(\tilde{L}/k)$ is solvable.

\iff In $k \subseteq L(f) \subseteq \tilde{L}$ all extensions are Galois.

$\xLeftrightarrow{3.5} \text{Gal}(L(f)/k) \cong \text{Gal}(\tilde{L}/k) / \text{Gal}(\tilde{L}/L(f))$

$\xLeftrightarrow{4.8} \text{Gal}(L(f)/k)$ is solvable. \square

Theorem 4.13 *Let G be a group, k a field. Then the subset $\text{Hom}(G, k^\times) \subseteq \text{Maps}(G, k)$ is linearly independant in the k -vector space $\text{Maps}(G, k)$.*

proof. Suppose $\text{Hom}(G, k^\times)$ is linearly dependant. Then let $n > 0$ minimal, such that there exist distinct elements $\chi_1, \dots, \chi_n \in \text{Hom}(G, k^\times)$ and $\lambda_1, \dots, \lambda_n \in k^\times$ such that

$$\sum_{i=1}^n \lambda_i \chi_i = 0.$$

The χ_i are called *characters*. Clearly we have $n \geq 2$. Choose $g \in G$ such that $\chi_1(g) \neq \chi_2(g)$. For any $h \in G$ we have

$$0 = \sum_{i=1}^n \lambda_i \chi_i(gh) = \sum_{i=1}^n \underbrace{\lambda_i \chi_i(g)}_{=: \mu_i} \chi_i(h) = \sum_{i=1}^n \mu_i \chi_i(h).$$

Then we get

$$0 = \sum_{i=0}^n \mu_i \chi_i(h) = \sum_{i=0}^n \lambda_i \chi_i(g) \chi_i(h) \Rightarrow \sum_{i=0}^n \underbrace{(\mu_i - \lambda_i \chi_1(g))}_{=:\nu_i} \chi_i(h) = 0.$$

Consider

$$\nu_1 = \mu_1 - \lambda_1 \chi_1(g) = \lambda_1 \chi_1(g) - \lambda_1 \chi_1(g) = 0,$$

$$\nu_2 = \mu_2 - \lambda_2 \chi_1(g) = \lambda_2 \chi_2(g) - \lambda_2 \chi_1(g) = \underbrace{\lambda_2}_{\neq 0} \cdot \underbrace{(\chi_2(g) - \chi_1(g))}_{\neq 0} \neq 0.$$

Hence χ_2, \dots, χ_n are linearly dependent. This is a contradiction to the minimality of n . \square

Proposition 4.14 *Let L/k be a Galois extension such that $G := \text{Gal}(L/k) = \langle \sigma \rangle$ is cyclic of order d for some $\sigma \in G$, where $\text{char}(k) \nmid d$. Let $\zeta_d \in k$ be a primitive d -th root of unity.*

Then there exists $\alpha \in L^\times$ such that $\sigma(\alpha) = \zeta \cdot \alpha$.

proof. Let

$$f : L \longrightarrow L, \quad f(X) = \sum_{i=0}^{d-1} \zeta^{-i} \cdot \sigma^i(X).$$

Applying Theorem 4.10 on $G = L^\times$ and $k = L$ shows $f \neq 0$. Then let $\gamma \in L$ such that $\alpha := f(\gamma) \neq 0$. Then we have

$$\begin{aligned} \sigma(\alpha) &= \sigma(f(\gamma)) = \sigma\left(\sum_{i=0}^{d-1} \zeta^{-i} \cdot \sigma^i(\gamma)\right) = \sum_{i=0}^{d-1} \zeta^{-i} \cdot \sigma^{i+1}(\gamma) = \zeta \cdot \sum_{i=0}^{d-1} \zeta^{-(i+1)} \cdot \sigma^{i+1}(\gamma) \\ &= \zeta \cdot \sum_{i=1}^d \zeta^{-i} \cdot \sigma^i(\gamma) = \zeta \cdot \left(\left(\sum_{i=1}^{d-1} \zeta^{-i} \cdot \sigma^i(\gamma) \right) + \gamma \right) \\ &= \zeta \cdot f(\gamma) = \zeta \cdot \alpha. \end{aligned}$$

Remark: The claim follows from Proposition 5.2 by inserting $\beta = \zeta$. \square

Corollary 4.15 *Let L/k be a Galois extension, such that $G := \text{Gal}(L/k) = \langle \sigma \rangle$ is cyclic of order d for some $\sigma \in G$, where $\text{char}(k) \nmid d$. Assume k contains a primitive d -th root of unity.*

Then L/k is an elementary radical extension of type (ii).

proof. Let $\zeta_d \in k$ be a primitive d -th root of unity and $\alpha \in L^\times$ such that $\sigma(\alpha) = \zeta \cdot \alpha$.

We have

$$\sigma^i(\alpha) = \zeta^i \cdot \alpha \quad \text{for } 1 \leq i \leq d.$$

The minimal polynomial of α over k has at least d zeroes, namely $\alpha, \sigma(\alpha), \dots, \sigma^{d-1}(\alpha)$. Thus $L = k[\alpha]$. Moreover we have

$$\sigma(\alpha^d) = (\sigma(\alpha))^d = (\zeta \cdot \alpha)^d = \alpha^d,$$

hence

$$\alpha^d \in L^{(\sigma)} = L^{\text{Gal}(L/k)} = k$$

where the last equation follows by the main theorem. Define $\gamma := \alpha^d$. Then the minimal polynomial of α over k is $X^d - \gamma \in k[X]$, which proves the claim. \square

Proposition 4.16 *Let L/k be a Galois extension of degree $p = \text{char}(k)$ with cyclic Galois group $\text{Gal}(L/k) \cong \mathbb{Z}/p\mathbb{Z} = (\sigma)$. Then there exists $\alpha \in L^\times$ such that $\sigma(\alpha) = \alpha + 1$.*

proof. The proof follows by Proposition 5.4 by setting $\beta = -1$. \square

Corollary 4.17 *Let L/k be a Galois extension of degree $p = \text{char}(k)$ with cyclic Galois group $\text{Gal}(L/k) \cong \mathbb{Z}/p\mathbb{Z} = (\sigma)$. Then L/k is an elementary radical extension of type (iii).*

proof. Let $\alpha \in L^\times$ such that $\sigma(\alpha) = \alpha + 1$. We have

$$\sigma^i(\alpha) = \alpha + i \quad \text{for } 1 \leq i \leq p,$$

thus we have $L = k[\alpha]$. Moreover we have

$$\sigma(\alpha^p - \alpha) = \sigma^p(\alpha) - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha.$$

Thus again we have $\alpha^p \in k$. Define $\gamma := \alpha^p - \alpha$. Then the minimal polynomial of α over k is $X^p - X - \gamma$, which proves the claim. \square

§ 5 Norm and trace

Definition + remark 5.1 Let L/k be a finite separable field extension, $[L : k] = n$. Let $\text{Hom}_k(L, \bar{k}) = \{\sigma_1, \dots, \sigma_n\}$.

(i) For $\alpha \in L$ we define the *norm* of α over k by

$$N_{L/k}(\alpha) := \prod_{i=1}^n \sigma_i(\alpha).$$

(ii) $N_{L/k} \in k$ for all $\alpha \in L$.

(iii) $N_{L/k} : L^\times \longrightarrow k^\times$ is a homomorphism of groups.

proof. (ii) Let $\alpha \in L$. Assume first that L/k is Galois. Then $\text{Hom}_k(L, \bar{k}) = \text{Aut}_k(L) = \text{Gal}(L/k)$.

For $\tau \in \text{Gal}(L/k)$ we have

$$\tau(N_{L/k}) = \tau\left(\prod_{i=1}^n \sigma_i(\alpha)\right) = \prod_{i=1}^n \underbrace{(\tau\sigma_i)}_{\in \text{Gal}(L/k)}(\alpha) = N_{L/k},$$

hence $N_{L/k} \in L^{\text{Gal}(L/k)} = k$. Now consider the general case. Let $\tilde{L} \supseteq L$ be the normal hull of L over k . Recall that \tilde{L} is the composition of the $\sigma_i(L)$, i.e. we have

$$\tilde{L} = \prod_{i=1}^n \sigma_i(L).$$

Then \tilde{L}/k is Galois and for $\tau \in \text{Gal}(\tilde{L}/k)$ we have

$$\tau(N_{L/k}(\alpha)) = \prod_{i=1}^n \underbrace{(\tau\sigma_i)}_{\in \text{Hom}_k(L, \bar{k})}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) = N_{L/k}(\alpha),$$

hence $N_{L/k}(\alpha) \in \tilde{L}^{\text{Gal}(\tilde{L}/k)} = k$.

(iii) We have $N_{L/k}(\alpha) = 0 \iff \sigma_i(\alpha) = 0$ for some $1 \leq i \leq n \iff \alpha = 0$.

Moreover

$$\begin{aligned} N_{L/k}(\alpha \cdot \beta) &= \prod_{i=1}^n \sigma_i(\alpha\beta) = \prod_{i=1}^n \sigma_1(\alpha)\sigma_i(\beta) = \left(\prod_{i=1}^n \sigma_i(\alpha) \right) \cdot \left(\prod_{i=1}^n \sigma_i(\beta) \right) \\ &= N_{L/k}(\alpha) \cdot N_{L/k}(\beta), \end{aligned}$$

which proves the claim. \square

Example 5.2 (i) Let $\alpha \in k$. Then

$$N_{L/k}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) = \prod_{i=1}^n \alpha = \alpha^n.$$

(ii) Let $k = \mathbb{R}$, $L = \mathbb{C}$. Then $\text{Hom}_{\mathbb{R}}(\mathbb{C}, \bar{\mathbb{R}}) = \text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}, z \mapsto \bar{z}\}$ and thus the norm is $N_{L/k}(z) = z\bar{z} = |z|^2$.

(iii) Let $k = \mathbb{Q}$, $L = \mathbb{Q}[\sqrt{d}]$ for $d \in \mathbb{Z}$ squarefree. We have $[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] = 2$ and

$$\text{Gal}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q}) = \{\text{id}, \sqrt{d} \mapsto -\sqrt{d}\} = \{a + b\sqrt{d} \mapsto a + b\sqrt{d}, a + b\sqrt{d} \mapsto a - b\sqrt{d}\}.$$

Then we have

$$N_{\mathbb{Q}[\sqrt{d}]/\mathbb{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

- $d < 0$: $d = -\tilde{d}$, hence $a^2 + \tilde{d}b^2 \stackrel{!}{=} 1 \Rightarrow$ either $a = \pm 1, b = 0$ or $a = 0, b = \pm 1, \tilde{d} = 1$.
- $d > 0$: Infinitely many solutions for $a^2 - bd^2 = 1$.

Proposition 5.3 (*Hilbert's theorem 90 - multiplicative version*) Let L/k a finite Galois extension with cyclic Galois group $\text{Gal}(L/k) = \langle \sigma \rangle$, $n = [L : k]$. Let $\beta \in L$ with $N_{L/k}(\beta) = 1$.

Then there exists $\alpha \in L^\times$ such that $\beta = \frac{\alpha}{\sigma(\alpha)}$.

proof. Define

$$f = \text{id}_L + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \dots + \beta\sigma(\beta)\sigma^2(\beta) \dots \sigma^{n-2}(\beta)\sigma^{n-1} = \sum_{j=0}^{n-1} \sigma^j \prod_{i=1}^j \sigma^{i-1}(\beta).$$

Then by Theorem 4.10 $f \neq 0$. Choose $\gamma \in L$ such that $\alpha := f(\gamma) \neq 0$. Then we have

$$\begin{aligned} \beta \cdot \sigma(\alpha) &= \beta \cdot \sigma(f(\gamma)) = \beta \cdot \left(\sigma \left(\gamma + \beta\sigma(\gamma) + \dots + \prod_{i=0}^{n-2} \sigma^i(\beta)\sigma^{n-1}(\gamma) \right) \right) \\ &= \beta \cdot \left(\sigma(\gamma) + \sigma(\beta)\sigma^2(\gamma) + \dots + \prod_{i=0}^{n-2} \sigma^{i+1}(\beta)\sigma^n(\gamma) \right) \\ &= \beta \cdot \left(\sigma(\gamma) + \sigma(\beta)\sigma^2(\gamma) + \dots + \frac{1}{\beta} N_{L/k}(\beta) \cdot \gamma \right) \\ &= \beta \cdot (\sigma(\gamma) + \sigma(\beta)\sigma^2(\gamma) + \dots + \gamma) \\ &= \gamma + \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \dots + \beta \cdot \prod_{i=1}^{n-2} \sigma^i(\beta)\sigma^{n-1}(\gamma) \\ &= f(\gamma) = \alpha, \end{aligned}$$

which is the claim. \square

Definition + remark 5.4 Let L/k be a finite separable field extension, $[L : k] = n$. Let $\text{Hom}_k(L, \bar{k}) = \{\sigma_1, \dots, \sigma_n\}$.

(i) For $\alpha \in L$,

$$\text{tr}_{L/k}(\alpha) := \sum_{i=0}^n \sigma_i(\alpha)$$

is called the *trace* of α over k .

(ii) $\text{tr}_{L/k}(\alpha) \in k$ for all $\alpha \in L$.

(iii) $\text{tr}_{L/k} : L \longrightarrow k$ is k -linear.

proof. (ii) As in proof 5.1, $\text{tr}_{L/k}(\alpha)$ is invariant under $\text{Gal}(\tilde{L}/k)$.

(iii) Clear. \square

Example 5.5 (i) Let $\alpha \in k$. Then

$$\text{tr}_{L/k}(\alpha) = \sum_{i=0}^n \sigma_i(\alpha) = \sum_{i=0}^n \alpha = n \cdot \alpha.$$

(ii) Let $k = \mathbb{R}$, $L = \mathbb{C}$. Then $\text{tr}_{\mathbb{C}/\mathbb{R}}(z) = z + \bar{z} = 2 \cdot \Re(z)$.

Proposition 5.6 (*Hilbert's theorem 90 - additive version*) Let L/k be a Galois extension with cyclic Galois group $\text{Gal}(L/k) = \langle \sigma \rangle$ and $[L : k] = \text{char}(k) = p \in \mathbb{P}$. Then for every $\beta \in L$ with $\text{tr}_{L/k}(\beta) = 0$ there exists $\alpha \in L$ such that $\beta = \alpha - \sigma(\alpha)$.

proof. Define

$$g = \beta \cdot \sigma + (\beta + \sigma(\beta)) \cdot \sigma^2 + \dots + \left(\sum_{i=0}^{p-2} \sigma^i(\beta) \right) \cdot \sigma^{p-1} = \sum_{i=0}^{p-2} \left(\sum_{j=0}^i \sigma^j(\beta) \right) \cdot \sigma^{i+1}.$$

Let now $\gamma \in L$ such that $\text{tr}_{L/k}(\gamma) \neq 0$ (existing by 4.11). Then for

$$\alpha := \frac{1}{\text{tr}_{L/k}(\gamma)} \cdot g(\gamma)$$

we have

$$\begin{aligned} \alpha - \sigma(\alpha) &= \frac{1}{\text{tr}_{L/k}(\gamma)} \cdot (g(\gamma) - \sigma(g(\gamma))) \\ &= \frac{1}{\text{tr}_{L/k}(\gamma)} \left(\left(\sum_{i=0}^{p-2} \left(\sum_{j=0}^i \sigma^j(\beta) \right) \sigma^{i+1}(\gamma) \right) - \left(\sum_{i=0}^{p-2} \left(\sum_{j=0}^i \sigma^{j+1}(\beta) \right) \sigma^{i+2}(\gamma) \right) \right) \\ &= \frac{1}{\text{tr}_{L/k}(\gamma)} \left(\left(\sum_{i=0}^{p-2} \left(\sum_{j=0}^i \sigma^j(\beta) \right) \sigma^{i+1}(\gamma) \right) - \left(\sum_{i=1}^{p-1} \left(\sum_{j=1}^i \sigma^j(\beta) \right) \sigma^{i+1}(\gamma) \right) \right) \\ &= \frac{1}{\text{tr}_{L/k}(\gamma)} \cdot \left(\sum_{i=0}^{p-1} \beta \cdot \sigma^i(\gamma) \right) = \beta, \end{aligned}$$

and we obtain the claim. □

Proposition 5.7 *Let L/k be a finite separable extension, $\alpha \in L$. Consider the k -linear map*

$$\phi_\alpha : L \longrightarrow L, \quad x \mapsto \alpha \cdot x.$$

Then

$$(i) \quad N_{L/k}(\alpha) = \det(\phi_\alpha).$$

$$(ii) \quad \text{tr}_{L/k}(\alpha) = \text{tr}(\phi_\alpha).$$

proof. Let

$$f = \sum_{i=0}^d a_i X^i$$

be the minimal polynomial of α over k . Then it holds

$$(f \circ \phi_\alpha)(x) = f(\phi_\alpha(x)) = \sum_{i=0}^d a_i \phi_\alpha^i(x) = \sum_{i=0}^d a_i \alpha^i \cdot x = x \cdot \sum_{i=0}^d a_i \alpha^i = x \cdot f(\alpha) = 0$$

For arbitrary $x \in L$, hence $f(\phi_\alpha) = 0$.

case 1.1 Assume first $L = k[\alpha]$ for some $\alpha \in k$. Then $[L : k] = \deg(f) = d$, so $\{1, \alpha, \dots, \alpha^{d-1}\}$ is a k -basis of L . Then we have a transformation matrix of ϕ_α with respect to the basis $\{1, \alpha, \dots, \alpha^{d-1}\}$

$$D = \begin{pmatrix} 0 & 0 & 0 & 0 & a_0 \\ 1 & 0 & & \vdots & -a_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}$$

thus we have $\text{tr}(\phi_\alpha) = -a_{d-1}$ and $\det(\phi_\alpha) = (-1)^d \cdot a_0$. We know that f splits over \bar{k} , say

$$f = \prod_{i=1}^d (X - \lambda_i) = \prod_{i=1}^d (X - \sigma_i(\alpha))$$

Then we easily see

$$\det(\phi_\alpha) = (-1)^d \cdot a_0 = (-1)^d \cdot f(0) = (-1)^d \cdot \prod_{i=1}^d (0 - \sigma_i(\alpha)) = \prod_{i=1}^d \sigma_i(\alpha) = N_{L/k}(\alpha),$$

$$\text{tr}(\phi_\alpha) = -a_{d-1} = \text{tr}_{L/k}(\alpha).$$

case 1.2 For the case $\alpha \in k$, ϕ_α is represented by the diagonal matrix $\begin{pmatrix} \alpha & & 0 \\ & \ddots & \\ 0 & & \alpha \end{pmatrix} \in k^{d \times d}$.

We obtain

$$\text{tr}(\phi_\alpha) = d \cdot \alpha = \text{tr}_{L/k}(\alpha) \quad \det(\phi_\alpha) = \alpha^d = \text{tr}_{L/k}(\alpha).$$

case 2 For the general case we have $k \subseteq k(\alpha) \subseteq L$.

Claim (a) The following is true:

$$N_{L/k}(\alpha) = N_{k(\alpha)/k}(N_{L/k(\alpha)}(\alpha)), \quad \text{tr}_{L/k}(\alpha) = \text{tr}_{k(\alpha)/k}(\text{tr}_{L/k(\alpha)}(\alpha))$$

Claim (b) The following identity holds:

$$\det(\phi_\alpha) = (\det(\phi_\alpha|_{k(\alpha)}))^{[L:k(\alpha)]} \quad \text{tr}(\phi_\alpha) = [L:k(\alpha)] \cdot \text{tr}(\phi_\alpha|_{k(\alpha)}).$$

Assuming Claim (a) and (b), we get

$$\begin{aligned} \det(\phi_\alpha) &= (\det(\phi_\alpha|_{k(\alpha)}))^{[L:k(\alpha)]} \stackrel{1.1}{=} (N_{k(\alpha)/k}(N_{L/k(\alpha)}(\alpha)))^{[L:k(\alpha)]} = N_{k(\alpha)/k}(\alpha^{[L:k(\alpha)]}) \\ &\stackrel{1.2}{=} N_{k(\alpha)/k}(N_{L/k(\alpha)}(\alpha)) \\ &\stackrel{(a)}{=} N_{L/k}(\alpha) \end{aligned}$$

And analogously $\text{tr}(\phi_\alpha) = \text{tr}_{L/k}(\alpha)$.

Let's now proof the claims.

- (b) Let x_1, \dots, x_d be a basis of $k(\alpha)/k$ as a k -vector space and y_1, \dots, y_m a basis of L as a $k(\alpha)$ -vector space. Then the $x_i y_j$ for $1 \leq i \leq d$, $1 \leq j \leq m$ form a k -basis for L . Let now $D \in k^{d \times d}$ be the matrix representing $\phi_\alpha|_{k(\alpha)}$. Then we have

$$\alpha x_i y_j = \underbrace{(\alpha x_i)}_{\in k(\alpha)} y_j = (D \cdot x_i) y_j,$$

hence ϕ_α is represented by

$$\tilde{D} = \begin{pmatrix} A & 0 & \dots & 0 \\ 0 & A & & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A \end{pmatrix}$$

- (a) This is an exercise. □

Definition + remark 5.8 Let L/k be a finite field extension, $r = [L : k]_s = |\text{Hom}_k(L, \bar{k})|$. Let $q = \frac{[L:k]}{[L:k]_s}$.

- (i) For $\alpha \in L$ define

$$N_{L/k}(\alpha) = \det(\phi_\alpha) \quad \text{tr}_{L/k}(\alpha) = \text{tr}(\phi_\alpha).$$

- (ii) Let $\text{Hom}_k(L, \bar{k}) = \{\sigma_1, \dots, \sigma_r\}$. Then

$$N_{L/k}(\alpha) = \left(\prod_{i=1}^r \sigma_i(\alpha) \right)^q, \quad \text{tr}_{L/k}(\alpha) = \left(\sum_{i=1}^r \sigma_i(\alpha) \right) \cdot q.$$

proof. Copy the proof of 5.5. Recall that the minimal polynomial of α over k is given by

$$m_\alpha = \prod_{i=1}^r (X - \sigma_i(\alpha))^q,$$

where q is defined as above. □

§ 6 Normal series of groups

Definition 6.1 Let G be a group.

- (i) A series

$$G = G_0 \supset G_1 \supset \dots \supset G_n$$

of subgroups is called a *normal series* for G , if $G_i \triangleleft G_{i-1}$ is a normal subgroup in G_{i-1} and $G_i \neq G_{i-1}$ for $1 \leq i \leq n$. The groups $H_i := G_{i-1}/G_i$ are called *factors* of the series.

- (ii) A normal series as above is called a *composition series* for G , if all its factors are simple groups and $G_n = \{e\}$.

Example 6.2 (i) For $G = S_4$ we have a composition series

$$G = S_4 \triangleright A_4 \triangleright V_4 \triangleright T_4 \triangleright \{e\}$$

where $T_4 = \{\text{id}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ for some transposition $\sigma \in S_4$. We have quotients

$$S_4/A_4 = \mathbb{Z}/2\mathbb{Z}, \quad A_4/V_4 = \mathbb{Z}/3\mathbb{Z}, \quad V_4/T_4 = \mathbb{Z}/2\mathbb{Z}, \quad T_4/\{e\} = \mathbb{Z}/2\mathbb{Z}$$

- (ii) \mathbb{Z} has no composition series.
 (iii) Every normal series is a composition series.
 (iv) Every finite group has a composition series.

Remark 6.3 If $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{e\}$ is a normal composition series for a finite group G , then the following is clear:

$$|G| = \prod_{i=1}^n |G_{i-1}/G_i|$$

Definition + remark 6.4 Let G be a group.

- (i) For subgroups $H_1, H_2 \leq G$ let $[H_1, H_2]$ denote the subgroup of G generated by all *commutators*

$$[h_1, h_2] = h_1 h_2 h_1^{-1} h_2^{-1} \quad \text{with } h_i \in H_i \text{ for } i \in \{1, 2\}.$$

- (ii) $[G, G] = G'$ is called the *derived* or *commutator subgroup* of G .
 (iii) $G' \triangleleft G$ and $G^{\text{ab}} := G/G'$ is abelian.
 (iv) Let A be an abelian group and $\phi : G \rightarrow A$ a homomorphism of groups. Let $\pi : G \rightarrow G^{\text{ab}}$ denote the residue map. Then $G' \subseteq \ker(\phi)$, thus ϕ factors to a unique homomorphism

$$\bar{\phi} : G^{\text{ab}} \rightarrow A, \quad \text{such that } \phi = \bar{\phi} \circ \pi.$$

- (v) The chain

$$G \triangleright G' \triangleright G'' = [G', G'] \triangleright \dots \triangleright G^{(n+1)} = [G^n, G^n]$$

is called the *derived series* of G .

- (vi) G is solvable if and only if its derived series stops at $\{e\}$.

proof. (iii) For $g \in G$, $a, b \in G$ we have

$$g[ab]g^{-1} = gaba^{-1}b^{-1}g^{-1} = ga \underbrace{g^{-1}g}_{=e} b \underbrace{g^{-1}g}_{=e} a^{-1} \underbrace{g^{-1}g}_{=e} b^{-1}g^{-1} = [gag^{-1}, gbg^{-1}] \in G'.$$

Moreover

$$e = [\bar{a}, \bar{b}] = \overline{[a, b]} = \overline{aba^{-1}b^{-1}} \iff \bar{ab} = \bar{a}\bar{b} = \bar{b}\bar{a} = \overline{ba}.$$

(iv) Let A be an abelian group, $\phi : G \longrightarrow A$ a homomorphism. For $x, y \in G$ we have

$$\phi([x, y]) = \phi(xy x^{-1} y^{-1}) = \phi(x) \phi(y) \phi(x)^{-1} \phi(y)^{-1} = e \implies G' \subseteq \ker(\phi).$$

(vi) ' \Leftarrow ' If the derived series of G stops at $\{e\}$, G has a normal series with abelian factors and is solvable.

' \Rightarrow ' Let now $G = G_0 \supset \dots \supset G_n = \{e\}$ be a normal series with abelian factors. We have to show that $G^{(n)} = \{e\}$.

Claim (a) We have $G^{(i)} \subseteq G_i$ for $0 \leq i \leq n$.

Then we see $G^{(n)} \subseteq G_n = \{e\}$ and hence the derived series of G stops at $\{e\}$. It remains to prove the claim.

(a) We have $\pi_i : G_i \longrightarrow G_i / G_{i+1}$ is a homomorphism from G to an abelian group.

Then by part (iv), we have $G_i^{(1)} = G'_i \subseteq \ker(\pi_i) = G_{i+1}$.

By induction on n we have $G^{(i)} = (G^{(i-1)})' \subseteq G_i$, hence $(G^{(i)})' \subseteq G_i$?

Thus we get

$$G^{(i+1)} = \left(G^{(i)}\right)' \subseteq G'_i \subseteq \ker(\pi_i) = G_{i+1},$$

which finishes the proof. \square

Proposition 6.5 *A finite group G is solvable if and only if the factors of its composition series are cyclic of prime order.*

proof. ' \Rightarrow ' Let

$$G = G_1 \supset G_2 \supset \dots \supset G_m = \{1\}$$

be a normal series of G with abelian quotients G_i / G_{i+1} for $1 \leq i \leq m$. Refine it to a composition series

$$G = G_0 = H_{0,0} \supset H_{0,1} \supset \dots \supset H_{0,d_0} = G_1 = H_{1,0} \supset \dots \supset H_{1,d_1} = G_2 \supset \dots \supset G_m = \{1\}.$$

Then we have

$$H_{i,j} / H_{i,j+1} \cong H_{i,j} / G_{i+1} \Big/ H_{i,j+1} / G_{i+1} \subseteq G_i / G_{i+1} \Big/ H_{i,j+1} / G_{i+1}$$

hence $H_{i,j} / H_{i,j+1}$ is isomorphic to a subgroup of a factor group of an abelian group, thus abelian.

' \Leftarrow ' Since the factor groups of the composition series are isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some primes p , the quotients are abelian, thus G is solvable. \square

Theorem 6.6 (*Jordan - Hölder*) Let G be a group and

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{e\}$$

$$G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_m = \{e\}$$

be two composition series of G . Then $n = m$ and there is $\sigma \in S_n$ such that

$$H_i / H_{i+1} \cong G_{\sigma(i)} / G_{\sigma(i)+1} \quad \text{for } 0 \leq i \leq n-1$$

proof. We prove the statement by induction on n .

n=1 G is simple and thus $H_1 = \{e\}$.

n>1 Let $\overline{G} := G/G_1$ and $\pi : G \rightarrow \overline{G}$ be the residue map.

Then $\overline{H}_i = \pi(H_i) \leq \overline{G}$ is a normal subgroup. Since \overline{G} is simple, hence we have $\overline{H}_i \in \{\{e\}, \overline{G}\}$. If $\overline{H}_1 = \overline{G}$, then \overline{H}_2 is a normal subgroup of $\overline{H}_1 = \overline{G}$, and so on. Hence we find $j \in \{1, \dots, m\}$ such that

$$\overline{H}_i = \overline{G} \text{ for } 0 \leq i \leq j \text{ and } \overline{H}_i = \{e\} \text{ for } j+1 \leq i \leq m.$$

Define $C_i := H_i \cap G_1 < G_1$ for $0 \leq i \leq m$.

Claim (a) If $j \leq m-2$, then we have a composition series for G_1 :

$$G_1 = C_0 \triangleright C_1 \triangleright \dots \triangleright C_j \triangleright C_{j+2} \triangleright \dots \triangleright C_m = \{e\}.$$

If $j = m-1$, we have a composition series for G_1 :

$$G_1 = C_0 \triangleright C_1 \triangleright \dots \triangleright C_{m-1} = \{e\}.$$

Clearly $G_1 \triangleright G_2 \triangleright \dots \triangleright G_n = \{e\}$ is a composition series, too. By induction hypothesis we have $n-1 = m-1$, hence $n = m$. Moreover we have for $i \neq j$

$$\left. \begin{array}{l} C_i / C_{i+1} \cong G_{\sigma(i)} / G_{\sigma(i)+1} \\ C_j / C_{j+2} \cong G_{\sigma(j)} / G_{\sigma(j)+1} \end{array} \right\} (*)$$

For some $\sigma : \{0, 1, \dots, j, j+2, j+3, \dots, n-1\} \rightarrow \{1, \dots, n-1\}$

Claim (b) We have

- (1) $C_{j+1} = C_j$
- (2) $C_i / C_{i+1} \cong H_i / H_{i+1}$ for $i \neq j$.
- (3) $H_j / H_{j+1} \cong \overline{G} = G/G_1$.

By (*) and Claim (a),(b) the theorem is proved.

It remains to show the Claims.

(a) C_{i+1} is a normal subgroup of C_i , $C_{i+1} = H_{i+1} \cap G_1$. Further C_{j+1} is normal in $C_j = C_{j+1}$

by Claim (b)(2) and $C_i/C_{i+1} \cong H_i/H_{i+1}$ for $i \neq j$ is simple by Claim (b)(2). Then $C_j/C_{j+2} = C_j/C_{j+1} = H_j/H_{j+1}$ is simple, too.

(b) (1) We have $H_{j+1} \subseteq G_1$, hence $H_{j+1} \cap G_1 = H_{j+1} = C_{j+1}$. $C_j = H_j \cap G_1$ is normal subgroup of H_j . Thus $H_j \triangleright C_j \triangleright C_{j+1} = H_{j+1}$. Since H_i/H_{i+1} is simple, we must have $C_j = C_{j+1}$.

(2) $i > j$ Then $C_i = H_i \cap G_1 = H_i$ since $H_i \subseteq G_1$.

$i < j$ We have $\overline{H}_i = \overline{G} = G/G_1$. Then we have $G_1 H_i = G$ (*), since:

' \subseteq ' Clear.

' \supseteq ' For $g \in G, \bar{g} \in \overline{G}$ its image there exists $h \in H_i$ such that

$$\bar{h} = \bar{g} \implies \bar{h}^{-1} \bar{g} \in G_1 \iff \bar{h}^{-1} \bar{g} = g_1 \in G_1 \implies g = h g_1 \in H_i G_1.$$

With the isomorphism theorem we obtain

$$C_i/C_{i+1} = C_i/H_{i+1} \cap G_i = C_i/H_{i+1} \cap C_i \cong C_i H_{i+1}/H_{i+1}.$$

Therefore it remains to show that $C_i H_{i+1} = H_i$.

' \subseteq ' Since $C_i, H_{i+1} \subseteq H_i$ we also have $C_i H_{i+1} \subseteq H_i$

' \supseteq ' Let $x \in H_i$. by (*) we have $H_{i+1} G_i = G$. Then there exists $g \in G_1, h \in H_{i+1}$ such that $x = gh$, thus we have $g = x h^{-1} \in H_i H_{i+1} = H_i$, i.e. $g \in G_i \cap H_i = C_1$ and thus $x \in C_i H_{i+1}$.

(3) We have

$$H_i/H_{i+1} = H_i/C_{j+1} = H_j/C_j = H_j/H_j \cap G_1 = G_1 H_j/G_1 \stackrel{(*)}{=} G/G_1,$$

which finishes the proof, paragraph and chapter. □