Chapter I

Galois theory

§ 1 Algebraic field extensions

Notations 1.1

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

$$\mathbb{K}[X] := \left\{ f = \sum_{i=0}^{n} a_i X^i \;\middle|\; n \geqslant 0, a_i \in \mathbb{K}\ \forall i \in \{0, ..., n\}, a_n \neq 0 \right\} \cup \{0\}$$

Reminder 1.2

Let $\mathbb{L}/\mathbb{K}$ a field extension, $\alpha \in \mathbb{L}$, $f \in \mathbb{K}[X]$.

(i) $f(\alpha)$ is well defined.
(ii) $\phi_\alpha : \mathbb{K}[X] \to \mathbb{L}$, $f \mapsto f(\alpha)$ is a homomorphism.
(iii) $\mathrm{im}(\phi_\alpha) := \mathbb{K}[\alpha]$ is the smallest subring of $\mathbb{L}$ containing $\mathbb{K}$ and α.
(iv) $\ker(\phi_\alpha) = \left\{ f \in \mathbb{K}[\alpha] \;\middle|\; f(\alpha) = 0 \right\} \triangleleft \mathbb{K}[X]$ 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 $\ker(\phi_\alpha) = \langle f_\alpha \rangle$ is a maximal ideal.
(vii) Then $L_\alpha := \mathbb{K}[X] \,/\ker(\phi_\alpha) = \mathbb{K}[X] \,/\langle f_\alpha \rangle$ is a field.
(viii) We have $\mathbb{K}[\alpha] = \mathrm{im}(\phi_\alpha) \cong \mathbb{K}[X] \,/\ker(\phi_\alpha) = \mathbb{L}_\alpha$, if $f_\alpha \neq 0$. Moreover $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$, where $\mathbb{K}(\alpha)$ is the smallest field containing $\mathbb{K}$ and α. In particular, $\frac{1}{\alpha} \in \mathbb{K}[\alpha]$.
(ix) The degree of the field extension $\mathbb{K}[\alpha]/\mathbb{K}$ is $[\mathbb{K}[\alpha] : \mathbb{K}] = \deg(f_\alpha)$.

proof.

(ii) For $f, f_1, f_2 \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$ we have

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

(iii) Clear.

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

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

and since $\mathbb{L}$ 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

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

Since $r = q \cdot f_\alpha \in \ker(\phi_\alpha)$ and the choice of f_α, $\deg(r) \not< \deg(f_\alpha)$, hence $r = 0 \Rightarrow g \in \langle f_\alpha \rangle$.

(vi) If $f_\alpha = g \cdot h$, either $g(\alpha) = 0$ or $h(\alpha) = 0$. As above, this implies $g \in \mathbb{K}$ or $h \in \mathbb{K}^\times$, i.e. f or g is irreducible.

Now assume, there is and ideal $I \trianglelefteq \mathbb{K}[X]$ satisfying $\langle f_\alpha \rangle \subsetneq I \subsetneq \mathbb{K}[K]$.

Let $g \in I \setminus \langle f_\alpha \rangle$, such that $\langle g \rangle = I$. Such a g exists by proof of (v). Then $f_\alpha = g \cdot h$, $h \in \mathbb{K}[X]$. This implies, that either g or h is a constant polynomial, hence a unit. In the first case, $I = \mathbb{K}[X]$ and in the second one $I = \langle f_\alpha \rangle$, 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 $\overline{a} \in R/\mathfrak{m}$ for some $a \in R$, $\overline{a} \neq 0$. Let $I := \langle \mathfrak{m}, a \rangle$ the smallest ideal in R containing $\mathfrak{m}$ and a. Since $\overline{a} \neq 0$, 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
$\overline{1} = \overline{x + ab} = \overline{x} + \overline{a}\overline{b} = \overline{a}\overline{b}$, hence $\overline{a}$ 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

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

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

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

Example

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

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

Proposition 1.3 *(Kronecker)*

Let $\mathbb{K}$ be a field, $f \in \mathbb{K}[X]$, $\deg(f) \geqslant 1$.

Then there exists a finite field extension $\mathbb{L}/\mathbb{K}$ and $\alpha \in \mathbb{L}$, 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 $\langle f \rangle = \left\{ f \cdot g \;\middle|\; g \in \mathbb{K}[X] \right\}$ is a maximal ideal and $\mathbb{L} := \mathbb{K} \big/ \langle f \rangle$ is a field.

Clearly $\mathbb{K}$ is a subfield of $\mathbb{L}$, since $\langle f \rangle$ does not contain any constant polynomial, i.e., if

$$\pi : \mathbb{K}[X] \longrightarrow \mathbb{K}[X] \big/ \langle f \rangle$$

denotes the residue map, we have $\ker(\pi) \cap \mathbb{K} = \{0\}$, hence $\pi|_{\mathbb{K}}$ is injective.

Write

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

Then we have

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

Hence $\alpha := \pi(X)$ is a zero of f in $\mathbb{L}$.

Moreover $\mathbb{L}/\mathbb{K}$ is finite with degree $[\mathbb{L} : \mathbb{K}] = \deg(f) = n$, since $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is basis of $\mathbb{L}$ as a $\mathbb{K}$-vector space.

For the independence write

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

Assume, there is $0 \leqslant j \leqslant n-1$ 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 $\mathbb{L}$ is generated by the powers of α. We have $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, hence we write

$$\alpha^n = -\left(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\right) \in \langle 1, \ldots, \alpha^{n-1} \rangle$$

By induction on n, we get $\alpha^k \in \langle 1, \ldots, \alpha^{n-1} \rangle$ for all $k \geqslant n$.

Example

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

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

Definition 1.4

Let $\mathbb{L}/\mathbb{K}$ a field extension, $\alpha \in \mathbb{L}$.

(i) α is called *algebraic over* $\mathbb{K}$, if there exists $f \in \mathbb{X}[X] \setminus \{0\}$, such that $f(\alpha) = 0$.

(ii) Otherwise α is called *transcendental*.

(iii) $\mathbb{L}/\mathbb{K}$ is called an *algebraic field extension*, if every $\alpha \in \mathbb{L}$ is algebraic over $\mathbb{K}$.

Proposition 1.5

Every finite field extension $\mathbb{L}/\mathbb{K}$ is algebraic.

proof.

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

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

Hence the polynomial

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

satifies $f(\alpha) = 0$, thus α is algebraic over $\mathbb{K}$. Since α was arbitrary, $\mathbb{L}/\mathbb{K}$ is algebraic.

Proposition 1.6

Let $\mathbb{L}/\mathbb{K}$ a field extension, $\alpha, \beta \in \mathbb{L}$.

(i) If α, β are algebraic over $\mathbb{K}$, then $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ are also algebraic over $\mathbb{K}$.

(ii) If $\alpha \neq 0$ is algebraic over $\mathbb{K}$, then $\frac{1}{\alpha}$ is also algebraic over $\mathbb{K}$.

(iii) $\mathbb{K}_{\mathbb{L}} := \left\{ \alpha \in \mathbb{L} \middle| \alpha \text{ is algebraic over } \mathbb{K} \right\} \subseteq \mathbb{L}$ is a subfield of $\mathbb{L}$.

proof.

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

$$\mathbb{K} \subseteq \mathbb{K}[a] \subseteq (\mathbb{K}[\alpha])[\beta] = \mathbb{K}[\alpha, \beta]$$

$\Rightarrow \mathbb{K}[\alpha, \beta]/\mathbb{K}$ is algebraic with Proposition 1.5. This implies the claim, as $\alpha+\beta$, $\alpha-\beta$, $\alpha\cdot\beta \in \mathbb{K}[\alpha, \beta]$.

(ii) If $\alpha \neq 0$, $\frac{1}{\alpha}$ is algebraic over $\mathbb{K}$ with part (i).

(iii) Follows from (i) and (ii).

Definition + Proposition 1.7

Let $\mathbb{K}$ be a field, $f \in \mathbb{K}[X]$, $\deg(f) = n$.

(i) A field extension $\mathbb{L}/\mathbb{K}$ is called a *splitting field of* f, if $\mathbb{L}$ is the smallest field in which f decomposes into linear factors.

(ii) A splitting field $\mathbb{L}(f)$ exists.

(iii) The field extension $\mathbb{L}(f)/\mathbb{K}$ is algebraic over $\mathbb{K}$.

(iv) For the degree we have $[\mathbb{L}(f) : \mathbb{K}] \leqslant n!$.

proof.

(ii) Do this by induction on n.

n=1 Clear.

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

Consider $\mathbb{L}_1 := \mathbb{K}\big/\langle f \rangle$. Then f has a zero in $\mathbb{L}_1$; say α. Then we have $\mathbb{L}_1 = \mathbb{K}[\alpha]$. Now we can write $f = (X - \alpha) \cdot g$ for some $g \in \mathbb{K}[X]$ with $\deg(g) = n - 1$. By induction hypothesis, there exists a splitting field $\mathbb{L}(g)$ for g. Then f splits over $\mathbb{L}(g)[\alpha]$.

(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 $[\mathbb{K}[\alpha] : \mathbb{K}] = \deg(f) = n$. By the multiplication formula for the degree and induction hypothesis we have

$$[\mathbb{L}(f) : \mathbb{K}] = [\mathbb{L}(g)[\alpha] : \mathbb{K}] = [\mathbb{L}(g)[\alpha] : \mathbb{L}(g)] \cdot [\mathbb{L}(g) : \mathbb{K}] \leqslant n \cdot (n-1)! = n!$$

Definition + Proposition 1.8

Let $\mathbb{K}$ be a field.

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

(ii) The following statements are equivalent:

(1) $\mathbb{K}$ is algebraically closed

(2) Every nonconstant polynomial $f \in \mathbb{K}[X]$ has a zero in $\mathbb{K}$.

(3) There is no proper algebraic field extension of $\mathbb{K}$.

(4) If $f \in \mathbb{K}[X]$ is irreducible, then $\deg(f) = 1$.

proof.

'(1) $\Rightarrow$ (2)' Let $f \in \mathbb{K}[X]$ be a non-constant polynomial of degree n. Then f splits over $\mathbb{K}$, i.e.

$$f = \prod_{i=0}^{n} (X - \lambda_i)$$

with $\lambda_i \in \mathbb{K}$ for $1 \leqslant i \leqslant n$. Every λ_i is a zero. Since $n \geqslant 1$, we find a zero for any nonconstant polynomial.

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

'(3) ⇒ (4)' Let $f \in \mathbb{K}[X]$ irreducible. Then $\mathbb{L} := \mathbb{K}[X] \,/ \langle f \rangle$ is an algebraic field extension. By (3), $\mathbb{L} = \mathbb{K}$, hence $1 = [\mathbb{L} : \mathbb{K}] = \deg(f)$.

'(4) ⇒ (1)' For $f \in \mathbb{K}[X]$ write $f = f_1 \cdots f_r$ with irreducible polynomials f_i for $1 \leqslant i \leqslant r$. With (4), $\deg(f_i) = 1$ for any i, hence f splits.

Lemma 1.9

Let $\mathbb{K}$ be a field. Then there exists an algebraic field extension $\mathbb{K}'/\mathbb{K}$, such that every $f \in \mathbb{K}[X]$ has a zero in $\mathbb{K}'$.

proof.

For every irreducible polynomial $f \in \mathbb{K}[X]$ introduce a symbol X_f and consider

$$R := \mathbb{K}[\{X_f \big| f \in \mathbb{K}[X] \text{ irreducible}\}] \supseteq \mathbb{K}$$

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 $\lambda \in \mathbb{K}$, $n_i \in \mathbb{N}$. Let $I \trianglelefteqslant R$ be the ideal generated by the $f(X_f)$, $f \in \mathbb{K}[X]$ irreducible.

The following claims prove the lemma:

Claim (a) $I \neq R$

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

Claim (c) $\mathbb{K}? = R \,/ \mathfrak{m}$

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

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

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

for suitable $g_{f_i} \in R$.

Let $\mathbb{L}/\mathbb{K}$ be a field extension in which all f_i have a zero α_i. Define a ring homomorphism

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

Then we obtain

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

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

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \ldots$$

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 $\mathbb{K}'$ is a field extension of $\mathbb{K}$. Let $f \in \mathbb{K}[X]$ be irreducible and $\pi : R \longrightarrow \mathbb{K}/\mathfrak{m}$ 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 $\mathbb{K}$.
Since $\mathbb{K}?$ is generated by the $\pi(X_f)$, $\mathbb{K}?/\mathbb{K}$ is algebraic, which finishes the proof.

Theorem 1.10

Let $\mathbb{K}$ be a field. Then there exists an algebraic field extension $\overline{\mathbb{K}}/\mathbb{K}$ such that $\overline{\mathbb{K}}$ is algebraically closed. $\overline{\mathbb{K}}$ is called the *algebraic closure* of $\mathbb{K}$.

proof.

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

$$\mathbb{K}_0 := \mathbb{K}, \mathbb{K}_1 = \mathbb{K}_0', \mathbb{K}_2 = \mathbb{K}_1', \mathbb{K}_{i+1} = \mathbb{K}_i' \qquad \text{for } i \geqslant 1$$

Clearly $\mathbb{K}_i$ is algebraic over $\mathbb{K}$ for all $i \in \mathbb{N}_0$ and $\mathbb{K}_i \subseteq \mathbb{K}_{i+1}$. Define

$$\overline{\mathbb{K}} := \bigcup_{i \in \mathbb{N}_0} \mathbb{K}_i$$

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

§ 2 Simple field extensions

Definition 2.1

A field extension $\mathbb{L}/\mathbb{K}$ is called *simple*, if there exists some $\alpha \in \mathbb{L}$ such that $\mathbb{L} = \mathbb{K}[\alpha]$

Example

Let $f \in \mathbb{K}[X]$ be irreducible, $\mathbb{L} := \mathbb{K}[X] \big/ \langle f \rangle$.
Then $\mathbb{L} = \mathbb{K}[\alpha]$ where $\alpha = \pi(X) = \overline{X}$ and $\pi : \mathbb{K}[X] \longrightarrow \mathbb{L}$ denotes the residue map.
Conversely, if $\mathbb{L}/\mathbb{K}$ is simple and algebraic, then $\mathbb{L} = \mathbb{K}[\alpha]$ for some algebraic $\alpha \in \mathbb{L}$. Let $f \in \mathbb{K}[X]$ be the minimal polynomial of α over $\mathbb{K}$, then

$$\mathbb{L} = \mathbb{K}[\alpha] = \mathbb{K}(\alpha) = \mathbb{K}[X] \big/ \langle f \rangle$$

Proposition 2.2

Let $\mathbb{L}$ be a field. Then any finite subgroup G of the multiplicative group $\mathbb{L}^\times$ is cyclic.
proof.
Let $\alpha \in G$ be an element of maximal order, $n := \mathrm{ord}(\alpha)$. Define

$$G' := \{\beta \in G : \mathrm{ord}(\beta) \big| n\}$$

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

$$\mathrm{ord}(\alpha\beta) = \mathrm{lcm(m, n)} \leqslant \mathrm{n}$$

by the property of n. Thus $m \big| n$ 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.

Corollary 2.3

Let $\mathbb{K}$ be a finite field. Then every finite field extension $\mathbb{L}/\mathbb{K}$ is simple.
proof.
We have $|\mathbb{L}| = |\mathbb{K}|^{[\mathbb{L}:\mathbb{K}]}$ and thus $\mathbb{L}$ is also finite. With proposition 2.2 there exists some $\alpha \in \mathbb{L}$ such that $\mathbb{L}^\times = \mathbb{L} \setminus \{0\} = \langle \alpha \rangle$, hence

$$\mathbb{L} = \mathbb{K}[\alpha]$$

Remark 2.4

Let $\mathbb{L}/\mathbb{K}$ be a finite field extension, $f \in \mathbb{K}[X]$ and $\alpha \in \mathbb{L}$ a zero of f. Let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$ and $\sigma : \mathbb{L} \longrightarrow \overline{\mathbb{K}}$ a homomorphism of field such that $\sigma|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$.
Then $\sigma(\alpha)$ is a zero of f.

proof.
Write

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

with coefficients $a_i \in \mathbb{K}$, hence we have $\sigma(a_i) = a_i$ for $0 \leqslant i \leqslant n$. We obtain

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

Theorem 2.5

Let $\mathbb{L}/\mathbb{K}$ be a finite field extension of degree $n := [\mathbb{L} : \mathbb{K}]$ and $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$.
If there exist n different field homomorphisms $\sigma_1, \ldots \sigma_n : \mathbb{K} \longrightarrow \mathbb{L}$ such that
$\sigma_i|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$, then $\mathbb{L}/\mathbb{K}$ is simple.
proof.
Let $\mathbb{L} = \mathbb{K}[\alpha_1, ..., \alpha_r]$ for some $r \geqslant 1$ and $\alpha_i \in \mathbb{L}$. Prove the statement by induction on r.

r=1 $\mathbb{L} = \mathbb{K}[\alpha_1]$, hence $\mathbb{L}$ is simple.

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

$$\mathbb{L} = \mathbb{K}[\alpha_1, \ldots \alpha_r] = \mathbb{L}'[\alpha_r] = \mathbb{K}[\alpha, \beta]$$

with $\alpha := \alpha_r$.
For $\lambda \in \mathbb{K}$ consider

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

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

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

Consider the polynomial

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

By proposition 2.2 we may assume, that $\mathbb{K}$ 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 $\mathbb{L}$, σ_i and σ_j must be equal on $\mathbb{L}$, which is a contradiction.

Therefore we find $\lambda \in \mathbb{K}$, 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.

$$\deg(m_{\gamma_\lambda}) \geqslant n \Rightarrow [\mathbb{K}[\gamma_\lambda] : \mathbb{K}] \geqslant n$$

and hence $\mathbb{K}[\gamma_\lambda] = \mathbb{L}$.

Proposition 2.6

Let $\mathbb{L} = \mathbb{K}[\alpha]$ be a simple, finite field extension, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$. Let $f \in \mathbb{K}[X]$ the minimal polynomial of α. Then for every zero β of f in $\overline{\mathbb{K}}$ there exists a unique homomorphism of fields

$$\sigma : \mathbb{L} \longrightarrow \overline{\mathbb{K}}$$

such that $\sigma(\alpha) = \beta$

proof.

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

Define

$$\phi_\beta : \mathbb{K}[X] \longrightarrow \overline{\mathbb{K}}, \qquad g \mapsto g(\beta)$$

We have

$$f(\beta) = 0 \implies \langle f \rangle \subseteq ker(\phi_\beta)$$

hence ϕ_β factors to a homomorphism

$$\overline{\phi_\beta} : \mathbb{L} \cong \mathbb{K}[X] \big/ \langle f \rangle \longrightarrow \overline{\mathbb{K}}$$

such that $\phi_\beta = \overline{\phi_\beta} \circ \pi$ where $\pi : \mathbb{K}[X] \longrightarrow \mathbb{K}[X] \big/ \langle f \rangle$ denotes the residue map. Let

$$\tau : \mathbb{L} \longrightarrow \mathbb{K}[X] \big/ \langle f \rangle$$

be an isomorphism. Then

$$\sigma := \overline{\phi_\beta} \circ \tau : \mathbb{L} \longrightarrow \overline{\mathbb{K}}$$

satisfies

$$\sigma(\alpha) = \left(\overline{\phi_\beta} \circ \tau\right)(\alpha) = \overline{\phi_\beta}\left(\tau(\alpha)\right) = \overline{\phi_\beta}(\overline{X}) = \overline{\phi_\beta}\left(\pi(X)\right) = \phi_\beta(X) = \beta$$

Corollary 2.7

Let $f \in \mathbb{K}[X]$ be a nonconstant polynomial. Then the splitting field of f over $\mathbb{K}$ is unique, i.e. any two splitting fields $\mathbb{L}, \mathbb{L}'$ of f over $\mathbb{K}$ are isomorphic.

proof.

Let $\mathbb{L} = \mathbb{K}[\alpha_1, \ldots \alpha_n]$, $\mathbb{L}' = \mathbb{K}[\beta_1, \ldots \beta_m]$.

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

$$\sigma_1 : \mathbb{K}[\alpha_1] \longrightarrow \mathbb{K}[\beta_2] \text{ such that } \sigma_1|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}} \text{ and } \alpha_1 \mapsto \beta_1$$

$$\tau_1 : \mathbb{K}[\beta_1] \longrightarrow \mathbb{K}[\alpha_1] \text{ such that } \tau_1|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}} \text{ and } \beta_1 \mapsto \alpha_1$$

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

Definition + Proposition 2.8
Let $\mathbb{L}/\mathbb{K}$, $\mathbb{L}'/\mathbb{K}$ be field extension.

(i) We define

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

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

(ii) If $\mathbb{L}/\mathbb{K}$ is finite, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, then

$$|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L}')| \leqslant [\mathbb{L} : \mathbb{K}]$$

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

$$|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = |\{\text{zeroes of f in } \overline{\mathbb{K}}\}| \leqslant \deg(\mathrm{f}) = [\mathbb{L} : \mathbb{K}]$$

Now consider the general case. Let $\mathbb{L} = \mathbb{K}[\alpha_1, \dots \alpha_n]$ and $\mathbb{L}' = \mathbb{K}[\alpha_1, \dots \alpha_{n-1}] \subseteq \mathbb{L} = \mathbb{L}'[\alpha_n]$.
By induction on n we have $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}', \overline{\mathbb{K}}) \leqslant [\mathbb{L}' : \mathbb{K}]$. Let now

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

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

$$|\{\mathrm{Hom}_{\mathbb{L}'}(\mathbb{L}, \overline{\mathbb{K}})\}| = |\{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) \big| \sigma|_{\mathbb{L}'} = \mathrm{id}_{\mathbb{L}'}\}| \leqslant \deg(\mathrm{f}^{\sigma'}) = \deg(\mathrm{f}) = [\mathbb{L}' : \mathbb{L}]$$

So all in all we have

$$|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| \leqslant |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}', \overline{\mathbb{K}})| \cdot [\mathbb{L} : \mathbb{L}'] \leqslant [\mathbb{L} : \mathbb{L}'] \cdot [\mathbb{L}' : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]$$

Definition 2.9

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

(i) f is called *separable* over $\mathbb{K}$, if f has $\deg(f)$ different roots in $\overline{\mathbb{K}}$, i.e. there are no multiple roots.

(ii) $\alpha \in \mathbb{L}$ is called *separable* over $\mathbb{K}$, if the minimal polynomial of α over $\mathbb{K}$ is separable.

(iii) $\mathbb{L}/\mathbb{K}$ is called *separable*, if any $\alpha \in \mathbb{L}$ is separable over $\mathbb{K}$.

(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:

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

Proposition 2.10

Let

$$f = \prod_{i=1}^{n} (X - \alpha_i) \in \mathbb{K}[X], \qquad a_i \in \overline{\mathbb{K}} \text{ for } 1 \leqslant i \leqslant n$$

Then the following statements are equivalent:

(i) f is separable.

(ii) $(X - \alpha_i) \nmid f'$ for $1 \leqslant i \leqslant n$.

(iii) $\gcd(f, f') = 1$ in $\mathbb{K}[X]$.

proof.

'(i) $\Leftrightarrow$ (ii)' We have

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

Then 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 $1 \leqslant i \leqslant n$. Then

$$\gcd(f, f') = 1 \text{ in } \overline{\mathbb{K}}[X] \Longrightarrow \gcd(f, f') = 1 \text{ in } \mathbb{K}[X]$$

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

$$1 = af + bf', \ a, b \in \mathbb{K}[X]$$

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

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

Corollary 2.11

(i) An irreducible polynomial $f \in \mathbb{K}[X]$ is separable if and only if $f' \neq 0$.

(ii) Any algebraic field extension in characteristic 0 is separable.

Example

Let $\mathrm{char}(\mathbb{K}) = \mathrm{p} > 0$. Then

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

Let $\mathbb{K} = \mathbb{F}_p(t)$ 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 2.12

Let $\mathbb{L}/\mathbb{K}$ be a finite field extension, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$ and $\mathbb{L}$.

(i) $[\mathbb{L} : \mathbb{K}]_s := |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})|$ is called the *degree of separability* of $\mathbb{L}/\mathbb{K}$.

(ii) If $\mathbb{L} = \mathbb{K}[\alpha]$ for some separable $\alpha \in \mathbb{L}$ with minimal polynomial m_α over $\mathbb{K}$, then

$$[\mathbb{L} : \mathbb{K}]_s = \deg(m_\alpha) = [\mathbb{L} : \mathbb{K}]$$

(iii) If $\mathbb{L} = \mathbb{K}[\alpha]$ for some $\alpha \in \mathbb{L}$, $\mathrm{char}(\mathbb{K}) = \mathrm{p} > 0$, then there exists $n \geqslant 0$, such that

$$[\mathbb{L} : \mathbb{K}] = p^n \cdot [\mathbb{L} : \mathbb{K}]_s$$

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

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

proof.

(i) This follows from Propoition 2.6:

$$[\mathbb{L} : \mathbb{K}]_s = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = |\{ \text{ different zeroes of } f\}| = n = [\mathbb{L} : \mathbb{K}]$$

(iii) Write

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

If α is separable over $\mathbb{K}$, we are done with part (ii). Otherwise by Corollary 2.11 we have

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

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

$$[\mathbb{K}[\alpha] : \mathbb{K}]_s = |\{ \text{ zeroes of } g \text{ in } \overline{\mathbb{K}}\}| = \deg(g)$$

and thus we obtain

$$[\mathbb{K}[\alpha] : \mathbb{K}] = \deg(f) = \deg(g) \cdot p^n = p^n \cdot [\mathbb{K}[\alpha] : \mathbb{K}]_s$$

(iv) Consider first the simple case $\mathbb{L} = \mathbb{K}(\alpha)$. Let

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

be the minimal polynomial of α over $\mathbb{F}$. Let $\tau \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{F}, \overline{\mathbb{K}})$ and let

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

Given $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ 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

$$\begin{aligned} \big|\{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) \ \mid \ \sigma|_{\mathbb{F}} = \tau\}\big| &= \big|\{\beta \in \overline{\mathbb{K}} \ \mid \ f^\tau(\beta) = 0\}\big| \\ &= \big|\{\beta \in \overline{\mathbb{K}} \ \mid \ f(\beta) = 0\}\big| \overset{2.6}{=} [\mathbb{L} : \mathbb{F}]_s \end{aligned}$$

We conclude

$$\begin{aligned} [\mathbb{L} : \mathbb{K}]_s &= \big|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})\big| = \Big| \bigcup_{\tau \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{F}, \overline{\mathbb{K}})} \big\{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) \ \mid \ \sigma|_{\mathbb{F}} = \tau\big\} \Big| \\ &= \big|\big\{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) \ \mid \ \sigma|_{\mathbb{F}} = \tau\big\}\big| \cdot \big|\mathrm{Hom}_{\mathbb{K}}(\mathbb{F}, \overline{\mathbb{K}})\big| \\ &= [\mathbb{L} : \mathbb{F}]_s \cdot [\mathbb{F} : \mathbb{K}]_s \end{aligned}$$

For the general case we can write $\mathbb{L} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. Define $\mathbb{L}_i := \mathbb{F}(\alpha_1, \ldots, \alpha_i)$, $\mathbb{L}_0 := \mathbb{F}$ and $\mathbb{L}_n = \mathbb{L}$. Then $\mathbb{L}_i / \mathbb{L}_{i-1}$ is simple and by the special case above we get

$$\begin{aligned} [\mathbb{L} : \mathbb{K}]_s &= [\mathbb{L}_n : \mathbb{L}_{n-1}]_s \cdot [\mathbb{L}_{n-1} : \mathbb{K}]_s \\ &\ \ \vdots \\ &= [\mathbb{L}_n : \mathbb{L}_{n-1}]_s \cdots [\mathbb{L}_2 : \mathbb{L}_1]_s \cdot [\mathbb{L}_1 : \mathbb{L}_0]_s \cdot [\mathbb{L}_0 : \mathbb{K}]_s \\ &= [\mathbb{L}_n : \mathbb{L}_{n-1}]_s \cdots [\mathbb{L}_2 : \mathbb{L}_1]_s \cdot [\mathbb{L}_1 : \mathbb{F}]_s \cdot [\mathbb{F} : \mathbb{K}]_s \\ &= [\mathbb{L}_n : \mathbb{L}_{n-1}]_s \cdots [\mathbb{L}_2 : \mathbb{F}]_s \cdot [\mathbb{F} : \mathbb{K}]_s \\ &\ \ \vdots \\ &= [\mathbb{L}_n : \mathbb{F}]_s \cdot [\mathbb{F} : \mathbb{K}]_s \\ &= [\mathbb{L} : \mathbb{F}]_s \cdot [\mathbb{F} : \mathbb{K}]_s \end{aligned}$$

Proposition 2.13

A finite field extension $\mathbb{L}/\mathbb{K}$ is separable if and only if $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_s$.

proof.

'⇒' Let $\mathbb{L} = \mathbb{K}[\alpha_1, \dots \alpha_n]$. Prove this by induction on n.

n=1 This is proposition 12.2(ii)

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

$$[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{L}']_s \cdot [\mathbb{L}' : \mathbb{K}]_s = [\mathbb{L} : \mathbb{L}'] \cdot [\mathbb{L}'.\mathbb{K}] = [\mathbb{L} : \mathbb{K}]$$

'⇐' Let $\alpha \in \mathbb{L}$ and $f = m_\alpha \in \mathbb{K}[X]$ its minimal polynomial. If $\mathrm{char}(\mathbb{K}) = 0$, f is separable, so α is separable by corollary 2.11. Let now $\mathrm{char}(\mathbb{K}) = p > 0$.

By proposition 12.2 there exists $n \geqslant 0$ such that

$$[\mathbb{K}[\alpha] : \mathbb{K}] = p^n \cdot [\mathbb{K}[\alpha] : \mathbb{K}]_s$$

We find

$$[\mathbb{L} : \mathbb{K}] \;=\; [\mathbb{L} : \mathbb{K}[\alpha]] \;\cdot\; [\mathbb{K}[\alpha] : \mathbb{K}] \;\geqslant\; [\mathbb{L} : \mathbb{K}[\alpha]]_s \;\cdot\; p^n\, [\mathbb{K}[\alpha] : \mathbb{K}]_s \;=\; p^n\, [\mathbb{L} : \mathbb{K}]_s = \; p^n\, [\mathbb{L} : \mathbb{K}]$$

Hence we must have $n = 0$, i.e. $[\mathbb{K}[\alpha] : \mathbb{K}] = [\mathbb{K}[\alpha] : \mathbb{K}]_s$. Thus α is separable over $\mathbb{K}$.

§ 3 Galois extensions

Definition 3.1

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

Remark 3.2

Let $\mathbb{L}/\mathbb{K}$ be a normal field extension, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$. Then

$$\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) = \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$$

proof.

'⊇' Clear.

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

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

and $\alpha \in \mathbb{L}$ such that $f(\alpha) = 0$. Let $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$. Then

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

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

Definition 3.3

An algebraic field extension $\mathbb{L}/\mathbb{K}$ is called *Galois extension* or *Galois*, if it is normal and separable. In this case, the *Galois group* of $\mathbb{L}/\mathbb{K}$ is defined as

$$\mathrm{Gal}(\mathbb{L}, \mathbb{K}) := \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$$

Proposition 3.4

A finite field extension $\mathbb{L}/\mathbb{K}$ is Galois if and only if $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})| = [\mathbb{L} : \mathbb{K}]$.

proof.

'$\Rightarrow$' We have

$$|\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})| = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = [\mathbb{L} : \mathbb{K}]_{\mathrm{s}} = [\mathbb{L} : \mathbb{K}]$$

'$\Leftarrow$' We have to show that $\mathbb{L}/\mathbb{K}$ is separable and normal. First we see

$$[\mathbb{L} : \mathbb{K}] = |\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})| \leqslant |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = [\mathbb{L} : \mathbb{K}]_{\mathrm{s}} \leqslant [\mathbb{L} : \mathbb{K}]$$

Hence we have equality on each inequality, i.e. $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_s$ and $\mathbb{L}/\mathbb{K}$ is separable.
By Theorem 2.5 we know that $\mathbb{L}/\mathbb{K}$ is simple, say $\mathbb{L} = \mathbb{K}[\alpha]$ for some $\alpha \in \mathbb{L}$.
Let $m_\alpha \in \mathbb{K}[X]$ be the minimal polynomial of α over $\mathbb{K}$. Moreover let $\beta \in \overline{\mathbb{K}}$ be another zero of m_α. Then there exists $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ such that $\sigma(\alpha) = \beta$. By the (in-)equality above we know $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L}) = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$, hence $\sigma(\beta) \in \mathbb{L}$. Since β was an arbitrary zero of m_α, f splits over $\mathbb{L}$, i.e. $\mathbb{L}$ is the splitting field of f over $\mathbb{K}$. Thus $\mathbb{L}/\mathbb{K}$ is normal and finally Galois.

Example

All quadratic field extensions are normal. Moreover, if $\mathrm{char}(\mathbb{K}) \neq 2$, then all quadratic field extensions of $\mathbb{K}$ are Galois.

Remark 3.5

Let $\mathbb{L}/\mathbb{K}$ be a Galois extension and $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$ an intermediate field.

(i) Then $\mathbb{L}/\mathbb{E}$ is Galois and

$$\mathrm{Gal}(\mathbb{L}/\mathbb{E}) \leqslant \mathrm{Gal}(\mathbb{L}/\mathbb{K})$$

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

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \,/ \mathrm{Gal}(\mathbb{L}/\mathbb{E}) \cong \mathrm{Gal}(\mathbb{E}/\mathbb{K})$$

proof.

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

(ii) Define

$$\rho : \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \longrightarrow \mathrm{Gal}(\mathbb{E}/\mathbb{K}),\ \sigma \mapsto \sigma|_{\mathbb{E}}$$

ρ is well defined since $\sigma|_{\mathbb{E}} \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{E}, \overline{\mathbb{K}}) = \mathrm{Aut}_{\mathbb{K}}(\mathbb{E}) = \mathrm{Gal}(\mathbb{E}/\mathbb{K})$ as $\mathbb{E}/\mathbb{K}$ is Galois:

$$[\mathbb{E} : \mathbb{K}] = |\mathrm{Aut}_{\mathbb{K}}(\mathbb{E})| \leqslant |\mathrm{Hom}_{\mathbb{K}}(\mathbb{E}, \overline{\mathbb{K}})| \leqslant [\mathbb{E} : \mathbb{K}]$$

Moreover ρ is surjective. For the kernel we get

$$\ker(\rho) = \{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \mid \sigma|_{\mathbb{E}} = \mathrm{id}_{\mathbb{E}}\} = \mathrm{Gal}(\mathbb{L}/\mathbb{E})$$

$$\Longrightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \,/ \mathrm{Gal}(\mathbb{L}/\mathbb{E}) \cong \mathrm{Gal}(\mathbb{E}/\mathbb{K})$$

Theorem 3.6 *(Main Theorem of Galois theory)*
Let $\mathbb{L}/\mathbb{K}$ be a finite Galois extension and $G := \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Then the subgroups $H \leqslant G$ correspond bijectively to the intermediate fields $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$. Explicitly we have inverse maps

$$\mathbb{E} \mapsto \mathrm{Gal}(\mathbb{L}/\mathbb{E}) \leqslant G$$

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

proof.
Clearly $\mathbb{L}^H$ is a field for any $H \leqslant G$. We now have to show

(i) $\mathrm{Gal}(\mathbb{L}/\mathbb{L}^H) = H$ for any $H \leqslant G$.

(ii) $\mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{E})} = \mathbb{E}$ for any intermediate field $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$.

Theese prove the theorem.

(i) We show both inclusion.
'$\supseteq$' Clear by definition.
'$\subseteq$' It suffices to show $|\mathrm{Gal}(\mathbb{L}/\mathbb{L}^H)| \leqslant |H|$. By 3.4(i) we have

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

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

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

with $\deg(f) = |H|$. Further, since $\mathrm{id} \in H$, we have $f(\alpha) = 0$. Clearly $f \in \mathbb{L}[X]$. We want to

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

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

(ii) Again we show both inclusions.

'$\supseteq$' Clear by definition.

'$\subseteq$' Let $H := \mathrm{Gal}(\mathbb{L}/\mathbb{E})$. Since $\mathbb{E} \subseteq \mathbb{L}^H$ it suffices to show $[\mathbb{L}^H : \mathbb{E}] = 1$. Since $\mathbb{L}^H/\mathbb{E}$ is separable, this is equivalent to $[\mathbb{L}^H : \mathbb{E}]_s = 1$.
Let now $\sigma \in \mathrm{Hom}_{\mathbb{E}}(\mathbb{L}^H, \overline{\mathbb{K}})$. By proposition 2.6 we can extend σ to some

$$\tilde{\sigma} : \mathbb{L} \longrightarrow \overline{\mathbb{K}}$$

with $\tilde{\sigma}|_{\mathbb{L}^H} = \sigma$. Explicitly: Let $\mathbb{L} = \mathbb{L}^H[\alpha]$ and $f \in \mathbb{L}^H[X]$ its minimal polynomial. Choose a zero $\beta \in \overline{\mathbb{K}}$ of f^σ. Then by 2.6 there exists $\tilde{\sigma} : \mathbb{L} \longrightarrow \overline{\mathbb{K}}$ with $\tilde{\sigma}(\alpha) = \beta$ and $\tilde{\sigma}|_{\mathbb{L}^H} = \sigma$.
We get $\tilde{\sigma} \in \mathrm{Gal}(\mathbb{L}/\mathbb{E}) = H$ and $\sigma = \tilde{\sigma}|_{\mathbb{L}^H} = \mathrm{id}_{\mathbb{E}}$ and hence $[\mathbb{L}^H : \mathbb{E}] = 1$.

Remark 3.7

An intermediate field $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$ is Galois over $\mathbb{K}$ if and only if $\mathrm{Gal}(\mathbb{L}/\mathbb{E}) \trianglelefteq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is a normal subgroup.

proof.

'$\Rightarrow$' If $\mathbb{E}/\mathbb{K}$ is Galois, then $\mathrm{Gal}(\mathbb{L}/\mathbb{E}) = \ker(\rho)$ is a normal subgroup by 3.5.

'$\Leftarrow$' Conversely let $\mathrm{Gal}(\mathbb{L}/\mathbb{E}) =: H \trianglelefteq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ be a normal subgroup. By 3.4 it suffices to show $\mathrm{Hom}_{\mathbb{K}}(\mathbb{E}, \overline{\mathbb{K}}) = \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$. Let now $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{E}, \overline{\mathbb{K}})$ and $\alpha \in \mathbb{E}$. Extend σ to $\tilde{\sigma} : \mathbb{L} \longrightarrow \overline{\mathbb{K}}$. Then $\tilde{\sigma} \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. By the theorem it suffices to show that $\sigma(\alpha) \in \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{E})} = \mathbb{E}$, i.e. $\sigma(\mathbb{E}) \subseteq \mathbb{E}$. Let $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{L}^{\mathrm{H}})$. Then by using the properties of normal subgroups we obtain

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

Example 3.8

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

We first want to show that f is irreducible. But this immediately follows by By Eisenstein's criterion for

irreducibility with $p = 2$.
Thus $\mathbb{L}$ is an extension of $\mathbb{Q}/\langle f\rangle$. Therefore $[\mathbb{L} : \mathbb{Q}]$ is multiple of $[\mathbb{Q}/\langle f\rangle] = 5$, hence $|\mathrm{Gal}(\mathbb{L}/\mathbb{Q})|$ is divisible by 5. By Lagrange's theorem we know that $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ contains an element of order 5.
Further note that f has exactly 3 zeroes in $\mathbb{R}$. With

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

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 $\beta, \overline{\beta}$. Hence we know that the conjugation in $\mathbb{C}$ must be an element of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.
To sum it up, we know: $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ 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 $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \cong \mathrm{S}_5$.

Proposition 3.9 *(Cyclotomic fields)*
Let $\mathbb{K}$ be a field, $n \in \mathbb{N}$, $\mathrm{char}(\mathbb{K}) \nmid \mathrm{n}$ and $\mathbb{L}_n$ the splitting field of the polynomial $f = X^n - 1$.
Then $\mathbb{L}_n/\mathbb{K}$ is Galois and $\mathrm{Gal}(\mathbb{L}_\mathrm{n}/\mathbb{K})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.
proof.
We have $f_n? = nX^{n-1}$ and $f? = 0 \Leftrightarrow X = 0$ but $f_n(0) \neq 0$, hence $f_n?$ and f_n are coprime. Thus f_n is separable. Since $\mathbb{L}_n$ is the splitting field of f_n by definition, $\mathbb{L}_n/\mathbb{K}$ is normal, thus Galois.
The zeroes of f_n form a group $\mu_n(\mathbb{K})$ under multiplication. By proposition 2.3 $\mu_n(\mathbb{K})$ is cyclic. Let ζ_n be a generator of $\mu_n(\mathbb{K})$. Define a map

$$\chi_n : \mathrm{Gal}(\mathbb{L}_\mathrm{n}/\mathbb{K}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \ \ \sigma \mapsto \mathrm{k} \text{ if } \sigma(\zeta_\mathrm{n}) = \zeta_\mathrm{n}^\mathrm{k}$$

where k is relatively coprime to n. We obtain that χ_n is a homomorphism of groups since for $\sigma_1.\sigma_2 \in \mathrm{Gal}(\mathbb{L}_\mathrm{n}/\mathbb{K})$ we have $\sigma_2\sigma_1(\zeta_n) = \sigma_2\left(\zeta_n^{k_1}\right) = \left(\zeta_n^{k_1}\right)^{k_2} = \zeta_n^{k_1k_2}$ and hence

$$\chi_n\left(\sigma_1\sigma_2\right) = k_1 \cdot k_2 = \chi_n(\sigma_1) \cdot \chi_n(\sigma_2)$$

Moreover χ_n is injective, since

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

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

§ 4 Solvability of equations by radicals

Definition + Remark 4.1

Let $\mathbb{K}$ be a field, $f \in \mathbb{K}[X]$ separable.

(i) Let $\mathbb{L}(f)$ be the splitting field of f over $\mathbb{K}$. The *Galois group of the equation* $f = 0$ is defined by

$$\mathrm{Gal(f)} := \mathrm{Gal}(\mathbb{L}(\mathrm{f})/\mathbb{K})$$

(ii) There exists an injective homomorphism of groups $\mathrm{Gal(f)} \longrightarrow \mathrm{S_n}$ where $n := \deg(f)$.

(iii) If $\mathbb{L}/\mathbb{K}$ is a finite, separable field extension, the $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ is isomorphic to a subgroup of S_n, where $n = [\mathbb{L} : \mathbb{K}]$.

proof.

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

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

Definition 4.2

(i) A simple field extension $\mathbb{L} = \mathbb{K}[\alpha]$ of a field $\mathbb{K}$ 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 $\gamma \in \mathbb{K}, n \in \mathbb{N}$ such that $\mathrm{char}(\mathbb{K}) \nmid \mathrm{n}$.
   (3) α is a root of $X^p - X - \gamma$ for somme $\gamma \in \mathbb{K}$ where $p = \mathrm{char}(\mathbb{K})$.
   In the following, we will denote (1), (2) and (3) as the three *types* of elementary radical extensions.

(ii) A finite field extension $\mathbb{L}/\mathbb{K}$ is called a *radical extension*, if there is a field extension $\mathbb{L}'/\mathbb{L}$ and a chain of field extension

$$\mathbb{K} = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \cdots \subseteq \mathbb{L}_m = \mathbb{L}'$$

such that $\mathbb{L}_i/\mathbb{L}_{i-1}$ is an elementary radical extension for every $1 \leqslant i \leqslant m$.

Example 4.3

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

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

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

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

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

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

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

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

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 $\mathbb{K}$ be afield, $f \in \mathbb{K}[X]$ a separable, non-constant polynomial. We say *f is solvable by radicals*, if the splitting field $\mathbb{L}(f)$ is a radical extension.

Remark 4.5
Let $\mathbb{L}/\mathbb{K}$ be an elementary field extension, referring to Definition 4.1 of type

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

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong (\mathbb{Z}\,/n\mathbb{Z})^\times$$

(ii) $\mathbb{L} = \mathbb{K}[\alpha]$ where α is a root of $X^n - \gamma$ for some $\gamma \in \mathbb{K}, n \in \mathbb{N}, \mathrm{char}(\mathbb{K}) \nmid$ n. If $\mathbb{K}$ contains the n-th roots of unity, i.e. $\mu_n(\overline{\mathbb{K}})$, then $\mathbb{L}/\mathbb{K}$ is Galois with cyclic Galois group.

(iii) $\mathbb{L} = \mathbb{K}[\alpha]$, where α is a root of $X^p - X - \gamma$ for some $\gamma \in \mathbb{K}^\times$. Then $\mathbb{L}/\mathbb{K}$ is Galois with Galois group

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \mathbb{Z}\,/p\mathbb{Z}$$

proof.

(i) We proved this in proposition 3.9.

(ii) Let $\zeta \in \mathbb{K}$ 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 sucht that $X^n - \gamma$ is irreducible. Then $\mathbb{L}$ contains all roots of $X^n - \gamma$, i.e. $\mathbb{L}/\mathbb{K}$ is normal and thus Galois with

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

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

(iii) $f = X^p - X - \gamma$ has p zeroes in $\mathbb{L} = \mathbb{K}[\alpha]$. Since $f(\alpha) = 0$, we have

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

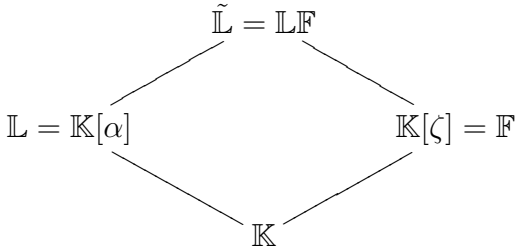
Hence $\mathbb{L}$ is the splitting field of f and $\mathbb{L}/\mathbb{K}$ is normal. Moreover $f' = -1 \neq 0$, hence $\mathbb{L}/\mathbb{K}$ is separable and thus Galois with

$$|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}] = \deg(f) = p$$

Further we obtain that $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \ni \sigma : \ \alpha \mapsto \alpha + 1$ has order p, hence $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is cyclic and thus

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \mathbb{Z}/p\mathbb{Z}$$

Remark 4.6
Let $\mathbb{L}/\mathbb{K}$ be an elementary radical extension of type (ii), i.e. $\mathbb{L} = \mathbb{K}[\alpha]$, where α is the root of $f = X^n - \gamma$ for some $\gamma \in \mathbb{K}, n \geqslant 1, \mathrm{char}(\mathbb{K}) \nmid \mathrm{n}$. $X^n - \gamma$ is irreducible
Let $\mathbb{F}$ be a splitting field of $X^n - 1$ over $\mathbb{K}$ and $\mathbb{L}\mathbb{F} = \mathbb{K}(\alpha, \zeta)$ be the *compositum* of $\mathbb{L}$ and $\mathbb{F}$, i.e. the smallest subfield of $\overline{\mathbb{K}}$ containing $\mathbb{L}$ and $\mathbb{F}$.



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

$$\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{K}) \,/\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{F}) \cong \mathrm{Gal}(\mathbb{F}/\mathbb{K})$$

i.e. we have a short exact sequence

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

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

$$\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{F}) \cong \mathbb{Z}/3\mathbb{Z}, \ \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \cong \mathbb{Z}/2\mathbb{Z}, \ \mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{Q}) \cong \mathrm{S}_3$$

Definition 4.7
A group G is called *solvable*, if there exists a chain of subgroups

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

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

Example

(i) Every abelian group is solvable.

(ii) S_4 is solvable by

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

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

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

(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 4.8

(i) Let G be a solvable group. Then

(1) Every subgroup $H \leqslant G$ 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 $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$. Let $G' \leqslant G$ a subgroup. Then

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

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

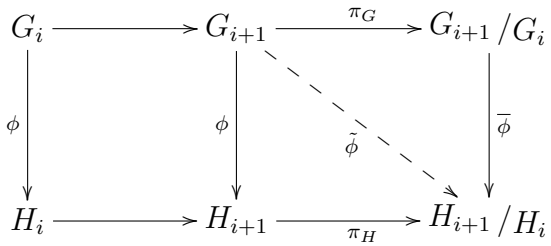
$$(G_{i+1} \cap G') / (G_i \cap G') \cong G_i (G_{i+1} \cap G') / G_i \leqslant G_{i+1} / G_i$$

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

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

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



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

$$\overline{\phi} : \underbrace{G_{i+1}/G_i}_{abelian} \underbrace{\longrightarrow}_{\Rightarrow} \underbrace{H_{i+1}/H_i}_{abelian!}$$

And we get $\overline{\phi}(a)\overline{\phi}(b) = \overline{\phi}(ab) = \overline{\phi}(ba) = \overline{\phi}(b)\overline{\phi}(a)$, hence the quotient is abelian and $H = \phi(G)$ is solvable.

(ii) '$\Rightarrow$' Clear.

'$\Leftarrow$' Let

$$1 \lhd G_1 \lhd \cdots \lhd G_m = G'$$

and

$$1 \lhd H_{m+1} \lhd \cdots \lhd H_{m+k} = G''$$

chains of subgroups with abelian quotients. Define

$$G_i := \pi^{-1}\left(H_i\right)_{m+1 \leqslant i \leqslant m+k}\,,\ \pi : G \longrightarrow G''$$

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

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

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

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

and hence the chain

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

reveals the solvability of G.

Lemma 4.9

A finite separable field extension $\mathbb{L}/\mathbb{K}$ is a radical extension if and only if there exists a finite Galois extension $\mathbb{L}'/\mathbb{K}$, $\mathbb{L} \subseteq \mathbb{L}'$ such that $\mathrm{Gal}(\mathbb{L}'/\mathbb{K})$ is solvable.

proof.

'$\Rightarrow$' Let

$$\mathbb{K} = \mathbb{K}_0 = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \cdots \subseteq \mathbb{L}_n$$

a chain as in definition 4.7 with $\mathbb{L} \subseteq \mathbb{L}_n$. we prove the statement by induction.

n=1 This is exactly remark 4.5, 4.6

n>1 By induction hypothesis $\mathbb{L}_{n-1}/\mathbb{K}$ is solvable. Moreover $\mathbb{L}_n/\mathbb{L}_{n-1}$ is solvable, too. This is equivalent to the fact, that

$\mathbb{L}_{n-1}$ is contained in a Galois extension $\tilde{\mathbb{L}}_{n-1}/\mathbb{K}$ such that $\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{K})$ is solvable and $\mathbb{L}_n$ is contained in a Galois extension $\tilde{\mathbb{L}}/\mathbb{L}_{n-1}$ such that $\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{L}_{\mathrm{n-1}})$ is solvable.
We have a diagramm

$$\begin{array}{ccccccc} & & \tilde{\mathbb{L}}_{n-1} & \subseteq & \tilde{\mathbb{L}}\mathbb{L}_{n-1} & := & \mathbb{M} \\ & & \cup| & & & & \cup| \\ \mathbb{K} & \subseteq & \mathbb{L}_{n-1} & \subseteq & \mathbb{L}_n & \subseteq & \tilde{\mathbb{L}} \end{array}$$

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

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

an injective homomorphism of groups is given, hence

$$\mathrm{Gal}(\mathbb{M}/\tilde{\mathbb{L}}_{\mathrm{n-1}}) \leqslant \mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{L}_{\mathrm{n-1}})$$

is solvable as a subgroup of a solvable group.
Let now $\tilde{\mathbb{M}}/\mathbb{M}$ be a minimal extension, such that $\tilde{\mathbb{M}}/\mathbb{K}$ 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 $\mathbb{M}/\mathbb{K}$.
Now we want to show that $\mathrm{Gal}(\mathbb{M}/\mathbb{K}$ is solvable.This finishes the proof of the sufficiency of our Lemma. Consider the short exact sequence

$$1 \longrightarrow \mathrm{Gal}(\tilde{\mathbb{M}}/\tilde{\mathbb{L}}_{\mathrm{n-1}}) \longrightarrow \mathrm{Gal}(\mathbb{M}/\mathbb{K}) \longrightarrow \mathrm{Gal}(\tilde{\mathbb{L}}_{\mathrm{n-1}}/\mathbb{K}) \longrightarrow 1$$

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

$$\Phi : \mathrm{Gal}(\tilde{\mathbb{M}}/\tilde{\mathbb{L}}_{\mathrm{n-1}}) \longrightarrow \prod_{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{M}, \overline{\mathbb{K}})} \mathrm{Gal}\left(\sigma(\mathbb{M})/\tilde{\mathbb{L}}_{\mathrm{n-1}}\right),\ \tau \mapsto \left(\tau|_{\sigma(\mathbb{M})}\right)_{\sigma}$$

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

'⇐' Let now $\tilde{\mathbb{L}}/\mathbb{L}$ finite such that $\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{K})$ is solvable. Let

$$1 \lhd\ G_1\ \lhd\ \ldots\ \lhd\ G_n\ =\ G$$

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

$$\tilde{\mathbb{L}} = \mathbb{L}_n \supseteq \mathbb{L}_{n-1} \supseteq \cdots \supseteq \mathbb{L}_0 = \mathbb{K}$$

where $\mathbb{L}_{i+1}/\mathbb{L}_i$ is Galois and $\mathrm{Gal}(\mathbb{L}_{\mathrm{i+1}}/\mathbb{L}) \cong \mathbb{Z}/p\mathbb{Z}$ for all $1 \leqslant i \leqslant n-1$. We now have to differ between three cases.

case 1 $p_i = \mathrm{char}(\mathbb{K})$. Then $\mathbb{L}_{i+1}/\mathbb{L}_i$ is an elementary radical extension of type (iii), i.e. $\mathbb{L}/\mathbb{K}$ is a radical extension.

case 2 $p_i \neq \mathrm{char}(\mathbb{K})$ *and* $\mathbb{L}_i$ contains a primitive p_i-th root of unity. Then $\mathbb{L}_{i+1}/\mathbb{L}_i$ is an elementary radical extension of type (ii), i.e. $\mathbb{L}/\mathbb{K}$ is a radical extension.

case 3 $p_i \neq \mathrm{char}(\mathbb{K})$ *and* $\mathbb{L}_i$ does not contain any primitive p_i-th root of unity. Then define

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

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

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

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

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

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

$$\mathbb{K} \subseteq \mathbb{F} = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \cdots \subseteq \mathbb{L}_n = \mathbb{L}'$$

be the corresponding chain of intermediate fields, i.e $\mathbb{L}_i/\mathbb{L}_{i-1}$ is Galois and $\mathrm{Gal}(\mathbb{L}_\mathrm{i}/\mathbb{L}_{\mathrm{i}-1}) \cong \mathbb{Z}/p\mathbb{Z}$ for $1 \leqslant i \leqslant n$. Hence, $\mathbb{L}_i/\mathbb{L}_{i-1}$ is a radical extension of type (ii). Thus $\mathbb{L}/\mathbb{K}$ is a radical extension, which finishes the proof.

Theorem 4.10

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

proof.

Let f be solvable by radicals, i.e. $\mathbb{L}(f)/\mathbb{K}$ be a radical field extension.

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

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

$\overset{3.5}{\iff}$ $\mathrm{Gal}(\mathbb{L}(\mathrm{f})/\mathbb{K}) \cong \mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{K})\,/\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{L}(\mathrm{f}))$

$\overset{4.8}{\iff}$ $\mathrm{Gal}(\mathbb{L}(\mathrm{f})/\mathbb{K})$ is solvable.

Theorem 4.11

Let G be a group, $\mathbb{K}$ a field. Then the subset $\mathrm{Hom}(\mathrm{G}, \mathbb{K}^\times) \subseteq \mathrm{Maps}(\mathrm{G}, \mathbb{K})$ is linearly independant in the $\mathbb{K}$-vector space $\mathrm{Maps}(\mathrm{G}, \mathbb{K})$.

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

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

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

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

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 $\chi_2, \dots \chi_n$ are linearily dependent. This is a contradiction to the minimality of n.

Proposition 4.12

Let $\mathbb{L}/\mathbb{K}$ be a Galois extension such that $G := \mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \langle \sigma \rangle$ is cyclic of order d for some $\sigma \in G$, where $\mathrm{char}(\mathbb{K}) \nmid \mathrm{d}$. Let $\zeta_d \in \mathbb{K}$ be a primitive d-th root of unity.
Then there exsits $\alpha \in \mathbb{L}^\times$ such that $\sigma(\alpha) = \zeta \cdot \alpha$.
proof.
Let

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

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

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

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

Corollary 4.13

Let $\mathbb{L}/\mathbb{K}$ be a Galois extension, such that $G := \mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \langle\sigma\rangle$ is cyclic of order d for some $\sigma \in G$, where $\mathrm{char}(\mathbb{K}) \nmid \mathrm{d}$. Assume $\mathbb{K}$ contains a primitive d-th root of unity.
Then $\mathbb{L}/\mathbb{K}$ is an elementary radical extension of type (ii).
proof.
Let $\zeta_d \in \mathbb{K}$ be a primitive d-th root of unity and $\alpha \in \mathbb{L}^\times$ such that $\sigma(\alpha) = \zeta \cdot \alpha$.
We have

$$\sigma^i(\alpha) = \zeta^i \cdot \alpha \qquad \text{for } 1 \leqslant i \leqslant d$$

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

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

hence

$$\alpha^d \in \mathbb{L}^{\langle\sigma\rangle} = \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} = \mathbb{K}$$

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

Proposition 4.14

Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of degree $p = \mathrm{char}(\mathbb{K})$ with cyclic Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \mathbb{Z}/p\mathbb{Z} = \langle\sigma\rangle$.
Then there exists $\alpha \in \mathbb{L}^\times$ such that $\sigma(\alpha) = \alpha + 1$.
proof.
The proof follows by Proposition 5.4 by setting $\beta = -1$.

Corollary 4.15

Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of degree $p = \mathrm{char}(\mathbb{K})$ with cyclic Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong \mathbb{Z}/p\mathbb{Z} = \langle\sigma\rangle$.
Then $\mathbb{L}/\mathbb{K}$ is an elementary radical extension of type (iii).
proof.
Let $\alpha \in \mathbb{L}^\times$ such that $\sigma(\alpha) = \alpha + 1$.
We have

$$\sigma^i(\alpha) = \alpha + i \qquad \text{for } 1 \leqslant i \leqslant p$$

Thus we have $\mathbb{L} = \mathbb{K}[\alpha]$.
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 $\alpha^p \in \mathbb{K}$. Define $\gamma := \alpha^p - \alpha$. Then the minimal polynomial of α over $\mathbb{K}$ is $X^p - X - \gamma$, which proves the claim.

§ 5 Norm and trace

Definition + Remark 5.1

Let $\mathbb{L}/\mathbb{K}$ be a finite separable field extension, $[\mathbb{L}:\mathbb{K}] = n$. Let $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) = \{\sigma_1, \dots \sigma_n\}$.

(i) For $\alpha \in \mathbb{L}$ we define the *norm* of α over $\mathbb{K}$ by

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

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

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

proof.

(ii) Let $\alpha \in \mathbb{L}$. Assume first that $\mathbb{L}/\mathbb{K}$ is Galois. Then $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) = \mathrm{Aut}_{\mathbb{K}}(\mathbb{L}) = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. For $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ we have

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

Hence $N_{\mathbb{L}/\mathbb{K}} \in \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} = \mathbb{K}$. Now consider the general case. Let $\tilde{\mathbb{L}} \supseteq \mathbb{L}$ be the normal hull of $\mathbb{L}$ over $\mathbb{K}$. Recall that $\tilde{\mathbb{L}}$ is the composition of the $\sigma_i(\mathbb{L})$, i.e.

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

Then $\tilde{\mathbb{L}}/\mathbb{K}$ is Galois an for $\tau \in \mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{K})$ we have

$$\tau\left(N_{\mathbb{L}/\mathbb{K}}(\alpha)\right) = \prod_{i=1}^{n} \underbrace{(\tau\sigma_i)}_{\in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = N_{\mathbb{L}/\mathbb{K}}(\alpha)$$

Hence $N_{\mathbb{L}/\mathbb{K}}(\alpha) \in \tilde{\mathbb{L}}^{\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{K})} = \mathbb{K}$.

(iii) We have $N_{\mathbb{L}/\mathbb{K}}(\alpha) = 0 \Longleftrightarrow \sigma_i(\alpha) = 0$ for some $1 \leqslant i \leqslant n \Leftrightarrow \alpha = 0$.
Moreover

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

Example

(i) Let $\alpha \in \mathbb{K}$. Then

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

(ii) Let $\mathbb{K} = \mathbb{R}$, $\mathbb{L} = \mathbb{C}$. Then
$\Rightarrow \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \overline{\mathbb{R}}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \mathrm{z} \mapsto \overline{\mathrm{z}}\}$ And thus $N_{\mathbb{L}/\mathbb{K}}(z) = z\overline{z} = |z|^2$.

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

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

Then we have

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

- $d < 0$: $d = -\tilde{d}$, hence $a^2 + \tilde{d}b^2 \overset{!}{=} 1 \Rightarrow$ 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 5.2 *(Hilbert's theorem 90 - multiplicative version)*
Let$\mathbb{L}/\mathbb{K}$ a finite Galois extension with cyclic Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \langle\sigma\rangle$, $n = [\mathbb{L} : \mathbb{K}]$. Let $\beta \in \mathbb{L}$ with $N_{\mathbb{L}/\mathbb{K}}(\beta) = 1$.
Then there exists $\alpha \in \mathbb{L}^\times$ such that $\beta = \frac{\alpha}{\sigma(\alpha)}$.
proof.
Define

$$f = \mathrm{id}_{\mathbb{L}} + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \ldots + \beta\sigma(\beta)\sigma^2(\beta)\cdots\sigma^{\mathrm{n}-2}(\beta)\sigma^{\mathrm{n}-1} = \sum_{\mathrm{j}=0}^{\mathrm{n}-1}\sigma^{\mathrm{j}}\prod_{\mathrm{i}=1}^{\mathrm{j}}\sigma^{\mathrm{i}-1}(\beta)$$

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

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

Definition + Remark 5.3
Let $\mathbb{L}/\mathbb{K}$ be a finite separable field extension, $[\mathbb{L} : \mathbb{K}] = n$. Let $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) = \{\sigma_1, \ldots \sigma_{\mathrm{n}}\}$.

(i) For $\alpha \in \mathbb{L}$,

$$tr_{\mathbb{L}/\mathbb{K}}(\alpha) := \sum_{i=0}^{n}\sigma_i(\alpha)$$

is called the *trace* of α over $\mathbb{K}$.

(ii) $tr_{\mathbb{L}/\mathbb{K}}(\alpha) \in \mathbb{K}$ for all $\alpha \in \mathbb{L}$.

(iii) $tr_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \longrightarrow \mathbb{K}$ is $\mathbb{K}$-linear.

proof.

(ii) As in proof 5.1, $tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ is invariant under $\mathrm{Gal}(\tilde{\mathbb{L}}/\mathbb{K})$.

(iii) Clear.

Examples

(i) Let $\alpha \in \mathbb{K}$. Then

$$tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=0}^{n} \sigma_i(\alpha) = \sum_{i=0}^{n} \alpha = n \cdot \alpha.$$

(ii) Let $\mathbb{K} = \mathbb{R}$, $\mathbb{L} = \mathbb{C}$. Then $tr_{\mathbb{C}/\mathbb{R}}(z) = z + \overline{z} = 2 \cdot \mathfrak{Re}(z)$.

Proposition 5.4 *(Hilbert's theorem 90 - additive version)*

Let $\mathbb{L}/\mathbb{K}$ be a Galois extension with cyclic Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \langle\sigma\rangle$ and $[\mathbb{L} : \mathbb{K}] = \mathrm{char}(\mathbb{K}) = p \in \mathbb{P}$.

Then for every $\beta \in \mathbb{L}$ with $tr_{\mathbb{L}/\mathbb{K}}(\beta) = 0$ there exists $\alpha \in \mathbb{L}$ such that $\beta = \alpha - \sigma(\alpha)$.

proof.

Define

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

Let now $\gamma \in \mathbb{L}$ such that $tr_{\mathbb{L}/\mathbb{K}}(\gamma) \neq 0$ (existing by 4.11). Then for

$$\alpha := \frac{1}{tr_{\mathbb{L}/\mathbb{K}}(\gamma)} \cdot g(\gamma)$$

we have

$$\begin{aligned}
\alpha - \sigma(\alpha) &= \frac{1}{tr_{\mathbb{L}/\mathbb{K}}(\gamma)} \cdot (g(\gamma) - \sigma\left(g(\gamma)\right)) \\
&= \frac{1}{tr_{\mathbb{L}/\mathbb{K}}(\gamma)} \left(\left(\sum_{i=0}^{p-2} \left(\sum_{j=0}^{i} \sigma^j(\beta) \right) \sigma^{i+1}(\gamma) \right) - \left(\sum_{i=0}^{p-2} \left(\sum_{j=0}^{i} \sigma^{j+1}(\beta) \right) \sigma^{i+2}(\gamma) \right) \right) \\
&= \frac{1}{tr_{\mathbb{L}/\mathbb{K}}(\gamma)} \left(\left(\sum_{i=0}^{p-2} \left(\sum_{j=0}^{i} \sigma^j(\beta) \right) \sigma^{i+1}(\gamma) \right) - \left(\sum_{i=1}^{p-1} \left(\sum_{j=1}^{i} \sigma^j(\beta) \right) \sigma^{i+1}(\gamma) \right) \right) \\
&= \frac{1}{tr_{\mathbb{L}/\mathbb{K}}(\gamma)} \cdot \left(\sum_{i=0}^{p-1} \beta \cdot \sigma^i(\gamma) \right) \;=\; \beta
\end{aligned}$$

Proposition 5.5

Let $\mathbb{L}/\mathbb{K}$ be a finite separable extension, $\alpha \in \mathbb{L}$. Consider the $\mathbb{K}$-linear map

$$\phi_\alpha : \mathbb{L} \longrightarrow \mathbb{L}, \quad x \mapsto \alpha \cdot x$$

Then

(i) $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \det(\phi_\alpha)$.
(ii) $tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \mathrm{tr}(\phi_\alpha)$.

proof.
Let

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

be the minimal polynomial of α over $\mathbb{K}$. Then

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

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

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

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

So we have $\mathrm{tr}(\phi_\alpha) = -a_{d-1}$ and $\det(\phi_\alpha) = (-1)^d \cdot a_0$.
We know that f splits over $\overline{\mathbb{K}}$, say

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

Then we easily see

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

$$\mathrm{tr}(\phi_\alpha) = -a_{d-1} = tr_{\mathbb{L}/\mathbb{K}}(\alpha)$$

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

We obtain

$$\mathrm{tr}(\phi_\alpha) = d \cdot \alpha = tr_{\mathbb{L}/\mathbb{K}}(\alpha) \qquad \det(\phi_\alpha) = \alpha^d = tr_{\mathbb{L}/\mathbb{K}}(\alpha$$

case 2 For the general case we have $\mathbb{K} \subseteq \mathbb{K}(\alpha) \subseteq \mathbb{L}$.

Claim (a) We have

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = N_{\mathbb{K}(\alpha])\mathbb{K}}\left(N_{\mathbb{L}/\mathbb{K}(\alpha)}(\alpha)\right), \qquad tr_{\mathbb{L}/\mathbb{K}}(\alpha) = tr_{\mathbb{K}(\alpha)/\mathbb{K}}\left(tr_{\mathbb{L}/\mathbb{K}(\alpha)}(\alpha)\right)$$

Claim (b) We have

$$\det(\phi_\alpha) = \left(\det\left(\phi_\alpha|_{\mathbb{K}(\alpha)}\right)\right)^{[\mathbb{L}:\mathbb{K}(\alpha)]} \qquad \mathrm{tr}(\phi_\alpha) = [\mathbb{L}:\mathbb{K}(\alpha)] \cdot \mathrm{tr}\left(\phi_\alpha|_{\mathbb{K}(\alpha)}\right).$$

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

$$\begin{aligned}\det(\phi_\alpha) &= \left(\det\left(\phi_\alpha|_{\mathbb{K}(\alpha)}\right)\right)^{[\mathbb{L}:\mathbb{K}(\alpha)]} \overset{1.1}{=} \left(N_{\mathbb{K}(\alpha)/\mathbb{K}}\right)^{[\mathbb{L}:\mathbb{K}(\alpha)]} = N_{\mathbb{K}(\alpha)/\mathbb{K}}\left(\alpha^{[\mathbb{L}:\mathbb{K}(\alpha)]}\right) \\ &\overset{1.2}{=} N_{\mathbb{K}(\alpha)/\mathbb{K}}\left(N_{\mathbb{L}/\mathbb{K}(\alpha)}(\alpha)\right) \\ &\overset{(a)}{=} N_{\mathbb{L}/\mathbb{K}}(\alpha)\end{aligned}$$

And analogously $\mathrm{tr}(\phi_\alpha) = tr_{\mathbb{L}/\mathbb{K}}(\alpha)$.

Let's now proof the claims.

(b) Let $x_1, \dots x_d$ be a basis of $\mathbb{K}(\alpha)/$ as a $\mathbb{K}$-vector space and $y_1, \dots y_m$ a basis of $\mathbb{L}$ as a $\mathbb{K}(\alpha)$-vector space.

Then the $x_i y_j$ for $1 \leqslant i \leqslant d,\ 1 \leqslant j \leqslant m$ form a $\mathbb{K}$-basis for $\mathbb{L}$.

Let now $D \in \mathbb{K}^{d\times d}$ be the matrix representing $\phi_\alpha|_{\mathbb{K}(\alpha)}$. Then we have

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

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 5.6

Let $\mathbb{L}/\mathbb{K}$ be a finite field extension, $r = [\mathbb{L}:\mathbb{K}]_s = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})|$. Let $q = \frac{[\mathbb{L}:\mathbb{K}]}{[\mathbb{L}:\mathbb{K}]_s}$.

(i) For $\alpha \in \mathbb{L}$ define

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \det(\phi_\alpha) \qquad tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \mathrm{tr}(\phi_\alpha)$$

(ii) Let $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) = \{\sigma_1, \dots, \sigma_r\}$. Then

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \left(\prod_{i=1}^{r} \sigma^i(\alpha)\right)^q, \qquad tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \left(\sum_{i=1}^{r} \sigma_i(\alpha)\right) \cdot q$$

proof.
Copy the proof of 5.5. Recall that the minimal polynomial of α over $\mathbb{K}$ is

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

§ 6 Normal series of groups

Defintion 6.1

Let G be a group.

(i) A series

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_n$$

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 $1 \leqslant i \leqslant n$. 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

(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 $T_4 = \{\mathrm{id}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ 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 6.2

If $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_n = \{e\}$ is a normal composition series for a finite group G, then we have

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

Definition + Remark 6.3

Let G be a group.

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

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

(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 $\phi : G \longrightarrow A$ a homomorphism of groups. Let $\pi : G \longrightarrow G^{\text{ab}}$ denote the residue map. Then $G' \subseteq \ker(\phi)$, thus ϕ factors to a unique homomorphism

$$\overline{\phi} : G^{\text{ab}} \longrightarrow A \qquad \text{such that } \phi = \overline{\phi} \circ \pi$$

(v) The chain

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

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

$$e = [\overline{a}, \overline{b}] = \overline{[a, b]} = \overline{aba^{-1}b^{-1}} \quad \Longleftrightarrow \quad \overline{ab} = \overline{a}\overline{b} = \overline{b}\overline{a} = \overline{ba}$$

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

$$\phi([x, y]) = \phi(xyx^{-1}y^{-1}) = \phi(x) = \phi(y)\phi(x)^{-1}\phi(y)^{-1} = e \quad \Longrightarrow \quad G' \subseteq \ker(\phi)$$

(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 $G = G_0 \rhd \ldots \rhd G_n = \{e\}$ 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 $0 \leqslant i \leqslant n$.

Then we see $G^{(n)} \subseteq G_n = \{e\}$ an 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 $\left(G^{(i)}\right)' \subseteq G_i$?.

Thus we get

$$G^{(i+1)} = \left(G^{(i)}\right)' \subseteq G_i' \subseteq \ker(\pi_I) = G_{i+1}$$

Proposition 6.4

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

'⇒' Let

$$G \;=\; G_1 \;\triangleright\; G_2 \;\triangleright\; \ldots \;\triangleright\, G_m \;=\; \{1\}$$

be a normal series of G with abelian quotients $G_i - 1 \,/G_i$ for $1 \leqslant i \leqslant m$. Refine it to a composition series

$$G \;=\; G_0 \;= H_{0,0} \triangleright H_{0,1} \triangleright \ldots \triangleright H_{0,d_0} = \; G_1 \;= H_{1,0} \triangleright \ldots \triangleright H - 1, d_1 = G_2 \;\triangleright\; \ldots \;\triangleright\; G_m = \{1\}$$

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.

'⇐' 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.

Theorem 6.5 *(Jordan-HÃ¶lder)*

Let G be a group and

$$G = G_0 \;\triangleright\; G_1 \;\triangleright\; \ldots \;\triangleright\; G_n = \{e\}$$

$$G = H_0 \;\triangleright\; H_1 \;\triangleright\; \ldots \;\triangleright\; H_m = \{e\}$$

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

$$H_i \,/H_{i+1} \;\cong\; G_{\sigma(i)} \,\Big/ G_{\sigma(i)+1} \qquad \text{for } 0 \leqslant i \leqslant n-1$$

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 $\pi : G \longrightarrow \overline{G}$ be the residue map.
Then $\overline{H}_i = \pi(H_i) \trianglelefteq \overline{G}$ 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 $\overline{H}_1 = \overline{H}$, and so on. Hence we find $j \in \{1, \ldots m\}$ such that

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

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

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

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

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

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

Clearly $G_1 \triangleright G_2 \triangleright \ldots \triangleright G_n = \{e\}$ is a composition series, too.

By induction hypothesis we have $n-1 = m-1$, hence $n = m$. Moreover we have for $i \neq j$

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

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

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, $C_{i+1} = H_{i+1} \cap G_1$.

C_{j+1} is normal in $C_j = C_{j+1}$ by Claim (b)(2).

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

$C_j \,/C_{j+2} = C_j \,/C_{j+1} = H_j \,/H_{j+1}$ 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 $g \in G, \overline{g} \in \overline{G}$ its image there exists $h \in H_i$ such that

$$\overline{h} = \overline{g} \Longrightarrow \overline{h}^{-1}\overline{g} \in G_1 \Longleftarrow \overline{h}^{-1}\overline{g} = g_1 \in G_1 \Longrightarrow g = hg_1 \in H_i G_1$$

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 $H_{i+1} G_i = G$.

Hence there exists $g \in G_1, h \in H_{i+1}$ such that $x = gh$.

Then we have $g = xh^{-1} \in H_i H_{i+1} = H_i$, i.e. $g \in G_i \cap H_i = C_1$ and thus $x \in C_i H_{i+1}$.

(3) We have

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