Algebra

lectured by Prof. Dr. Frank Herrlich during fall 2014/2015 at the KIT

 $\textit{Written in } \texttt{IFT}_{E\!X} \textit{ by Arthur Martirosian, arthur.martirosian@student.kit.edu}$

11. März 2017

Inhaltsverzeichnis

Ι $\mathbf{5}$ Galois theory Algebraic field extensions..... § 1 5 $\S 2$ Simple field extensions 11 § 3 § 4 § 5 § 6 Valuation theory \mathbf{II} 41 **ξ**7 § 8 § 9 **III** Rings and modules 63

§ 11	Multilinear Algebra	63
$\S{12}$	Hilbert's basis theorem	74
$\S13$	Integral ring extensions	77
$\S{14}$	Dedekind domains	83

Kapitel I

Galois theory

§ 1 Algebraic field extensions

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

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

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

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

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

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

(iii) Clear.

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

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

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

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

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

Since $r = q \cdot f_{\alpha} \in \ker(\phi_{\alpha})$ and the choice of f_{α} , $\deg(r) \leq \deg(f_{\alpha})$, hence $r = 0 \Rightarrow g \in (f_{\alpha})$.

- (vi) If $f_{\alpha} = g \cdot h$, either $g(\alpha) = 0$ or $h(\alpha) = 0$. As above, this implies $g \in k$ or $h \in k^{\times}$, i.e. f or g is irreducible. Now assume, there is and ideal $I \leq k[X]$ satisfying $(f_{\alpha}) \subsetneq I \subsetneq k[K]$. Let $g \in I \setminus (f_{\alpha})$, such that (g) = I. Such a g exists by proof of (v). Then $f_{\alpha} = g \cdot h$, $h \in k[X]$. This implies, that either g or h is a constant polynomial, hence a unit. In the first case, I = k[X] and in the second one $I = (f_{\alpha})$, which implies the claim.
- (vii) We show the more general argument: If R is a ring, $\mathfrak{m} \triangleleft R$ a maximal ideal, then R/\mathfrak{m} is a field. Let $\overline{a} \in R/\mathfrak{m}$ for some $a \in R$, $\overline{a} \neq 0$. Let $I := (\mathfrak{m}, a)$ 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

$$\implies 0 = f_{\alpha}(\alpha) = \sum_{i=0}^{n} a_{i}\alpha^{i} = a_{0} + a_{1}\alpha + \dots + a_{n}\alpha^{n}$$

$$\implies a_{0} = -\alpha \cdot (a_{1} + a_{2}\alpha + \dots + a_{n-2}\alpha^{n-2} + \alpha^{n-1})$$

$$\implies 1 = -\alpha \cdot \left(\frac{a_{1}}{a_{0}} + \frac{a_{2}}{a_{0}}\alpha + \dots + \frac{a_{n-2}}{a_{0}}\alpha^{n-2} + \frac{1}{a_{0}}\alpha n - 1\right)$$

$$\implies \frac{1}{\alpha} = -\frac{a_{1}}{a_{0}} - \frac{a_{2}}{a_{0}}\alpha - \dots - \frac{a_{n-2}}{a_{0}}\alpha^{n-2} - \frac{1}{a_{0}}\alpha^{n-1}$$

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

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

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

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

Proposition 1.4 (Kronecker) Let k be a field, $f \in k[X]$, $\deg(f) \ge 1$. Then there exists a finite field extension L/k and $\alpha \in L$, such that $f(\alpha) = 0$.

proof. W.l.o.g. we may assume, that f is irreducible, since $f = g \cdot h = 0 \Rightarrow g = 0$ or h = 0. Then by 1.2 $(f) = \{f \cdot g \mid g \in k[X]\}$ is a maximal ideal and L := k/(f) is a field. Clearly k is a subfield of L, since (f) does not contain any constant polynomial, i.e., if

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

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

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

Then we have

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

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

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

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

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

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

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

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

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

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

and the degree of the extension is equal to n.

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

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

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

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

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

Hence the polynomial

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

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

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

- (i) If α, β are algebraic over k, then $\alpha + \beta, \alpha \beta, \alpha \cdot \beta$ are also algebraic over k.
- (ii) If $\alpha \neq 0$ is algebraic over k, then $\frac{1}{\alpha}$ is also algebraic over k.
- (iii) $k_L := \{ \alpha \in L | \alpha \text{ is algebraic over } k \} \subseteq L \text{ is a subfield of } L.$
- proof. (i) Since $\alpha \in L$ is algebraic over $k \Rightarrow k[\alpha] = k(\alpha)$ is a finite field extension of k. Since β is algebraic over $k \Rightarrow \beta$ is algebraic over $k[\alpha]$, hence $(k[\alpha])[\beta]/k[\alpha]$ is a finite field extension. Further, we have

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

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

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

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

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

proof.

(ii) Do this by induction on n.

n=1 Clear.

- **n**>1 Write $f = f_1 \cdots f_r$ with irreducible polynomials $f_i \in k[X]$. Then f splits if and only every f_i splits. Hence we may assume that f is irreducible Consider $L_1 := k/(f)$. Then f has a zero in L_1 ; say α . Then we have $L_1 = k[\alpha]$. Now we can write $f = (X - \alpha) \cdot g$ for some $g \in k[X]$ with $\deg(g) = n - 1$. By induction hypothesis, there exists a splitting field L(g) for g. Then f splits over $L(g)[\alpha]$.
- (iii) Follows by part (iv) and Proposition 1.5
- (iv) Do this again by induction.

n=1 Clear.

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

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

Definition + **proposition 1.10** Let k be a field.

- (i) k is called *algebraically closed*, if every $f \in k[X]$ splits over k.
- (ii) The following statements are equivalent:
 - (1) k is algebraically closed
 - (2) Every nonconstant polynomial $f \in k[X]$ has a zero in k.
 - (3) There is no proper algebraic field extension of k.
 - (4) If $f \in k[X]$ is irreducible, then $\deg(f) = 1$.
- proof. '(1) \Rightarrow (2)' Let $f \in k[X]$ be a non-constant polynomial of degree n. Then f splits over k, i.e. we have a presentation

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

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

- $'(2) \Rightarrow (3)'$ Assume L/k is algebraic, $\alpha \in L$. Let f_{α} be the minimal polynomial of α . By assumption, f_{α} has a zero in k. Since f_{α} is irreducible, we must have $f_{\alpha} = X \alpha$, hence $\alpha \in k$, since $f \in k[X]$.
- $'(3) \Rightarrow (4)'$ Let $f \in k[X]$ irreducible. Then L := k[X]/(f) is an algebraic field extension. By (3), L = k, hence $1 = [L:k] = \deg(f)$.
- $'(4) \Rightarrow (1)'$ For $f \in k[X]$ write $f = f_1 \cdots f_r$ with irreducible polynomials f_i for $1 \le i \le r$. With (4), deg $(f_i) = 1$ for any *i*, hence *f* splits.

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

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

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

Monomials in R look like

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

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

Claim (a) $I \neq R$

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

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

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

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

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

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

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

Then we obtain

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

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

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

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

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

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

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

(c) Clearly k' is a field extension of k. Let $f \in k[X]$ be irreducible and $\pi: R \longrightarrow k/\mathfrak{m}$ denote the residue map. Then

i.e. we have

$$\pi(X_f) = 0$$

and thus $f(\pi(X_f)) = 0$. Hence $\pi(X_f)$ is algebraic over k. Since k' is generated by the $\pi(X_f)$, k'/k is algebraic, which finishes the proof.

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

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

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

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

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

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

§ 2 Simple field extensions

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

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

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

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

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

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

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

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

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

$$f = X^n - 1$$

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

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

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

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

proof. Write

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

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

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

which finishes the proof.

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

proof. Let $L = k[\alpha_1, ..., \alpha_r]$ for some $r \ge 1$ and $\alpha_i \in L$. Prove the statement by induction on r. $\mathbf{r=1} \ L = k[\alpha_1]$, hence L is simple.

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

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

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

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

By remark 2.4 it suffices to show

$$\sigma_i(\gamma) \neq \sigma_j(\gamma)$$
 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

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

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

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

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

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

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

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

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

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

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

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

be an isomorphism. Then

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

satisfies

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

thus the claim.

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

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

 $\sigma_1: k[\alpha_1] \longrightarrow k[\beta_2]$ such that $\sigma_1|_k = \mathrm{id}_k$ and $\alpha_1 \mapsto \beta_1$

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

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

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

(i) We define

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

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

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

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

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

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

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

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

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

So all in all we have

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

which is exactly the assignment.

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

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

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

We have well known properties of the derivative:

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

Proposition 2.11 Let

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

Then the following statements are equivalent:

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

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

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

thus we get

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

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

$$gcd(f, f') = 1$$
 in $\overline{k}[X] \Longrightarrow gcd(f, f') = 1$ in $k[X]$.

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

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

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

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

which was to be shown.

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

Example 2.13 Let char(k) = p > 0. Then

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

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

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

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

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

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

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

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

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

proof. (i) This follows from Propoition 2.6:

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

(iii) Write

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

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

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

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

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

and thus we obtain

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

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

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

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

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

Given $\sigma \in \operatorname{Hom}_k(L, \overline{k})$ 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

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

We conclude

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

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

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

$$[L:k]_{s} = [L_{n}:L_{n-1}]_{s} \cdot [L_{n-1}:k]_{s}$$

$$\vdots$$

$$= [L_{n}:L_{n-1}]_{s} \cdots [L_{2}:L_{1}]_{s} \cdot [L_{1}:L_{0}]_{s} \cdot [L_{0}:k]_{s}$$

$$= [L_{n}:L_{n-1}]_{s} \cdots [L_{2}:L_{1}]_{s} \cdot [L_{1}:\mathbb{F}]_{s} \cdot [\mathbb{F}:k]_{s}$$

$$= [L_{n}:L_{n-1}]_{s} \cdots [L_{2}:\mathbb{F}]_{s} \cdot [\mathbb{F}:k]_{s}$$

$$\vdots$$

$$= [L_{n}:\mathbb{F}]_{s} \cdot [\mathbb{F}:k]_{s}$$

$$= [L:\mathbb{F}]_{s} \cdot [\mathbb{F}:k]_{s},$$

which implies the claim.

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

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

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

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

We find

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

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

§ 3 Galois extensions

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

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

$$\operatorname{Hom}_k(L,\overline{k}) = \operatorname{Aut}_k(L).$$

proof. ' \supseteq ' Clear.

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

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

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

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

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

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

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

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

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

proof. ' \Rightarrow ' We have

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

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

$$[L:k] = |\operatorname{Aut}_{k}(L)| \leq |\operatorname{Hom}_{k}(L,\overline{k})| = [L:k]_{s} \leq [L:k]$$

Hence we have equality on each inequality, i.e. $[L:k] = [L:k]_s$ and L/k is separable. By Theorem 2.5 we know that L/k is simple, say $L = k[\alpha]$ for some $\alpha \in L$.

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

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

Remark 3.6 Let L/k be a Galois extension and $k \subseteq K \subseteq L$ an intermediate field. (i) Then L/K is Galois and

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

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

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

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

$$\rho: \operatorname{Gal}(L/k) \longrightarrow \operatorname{Gal}(K/k), \ \sigma \mapsto \sigma|_{K}$$

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

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

Moreover ρ is surjective. For the kernel we get

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

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

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

$$K \mapsto \operatorname{Gal}(L/K) \leqslant G$$

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

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

- (i) $\operatorname{Gal}(L/L^H) = H$ for any $H \leq G$.
- (ii) $L^{\operatorname{Gal}(L/K)} = K$ for any intermediate field $k \subseteq K \subseteq L$.

Theese prove the theorem.

- (i) We show both inclusion.
 - '⊇' Clear by definition.

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

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

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

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

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

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

Then for f as defined above we have

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

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

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

(ii) ' \supseteq ' Clear by definition.

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

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

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

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

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

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

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

which implies the claim.

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

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

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

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

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 $\operatorname{Gal}(L/\mathbb{Q})$.

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

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

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

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

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

where *m* is relatively coprime to *n*. We obtain that χ_n is a homomorphism of groups since for $\sigma_1.\sigma_2 \in \text{Gal}(L_n/k)$ we have $\sigma_2\sigma_1(\zeta_n) = \sigma_2(\zeta_n^{k_1}) = (\zeta_n^{k_1})^{k_2} = \zeta_n^{k_1k_2}$ and hence

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

Moreover χ_n is injective, since

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

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 k be a field, $f \in k[X]$ separable.

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

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

- (ii) There exists an injective homomorphism of groups $\operatorname{Gal}(f) \longrightarrow S_n$ where $n := \operatorname{deg}(f)$.
- (iii) If L/k is a finite, separable field extension, the Aut_k(L) is isomorphic to a subgroup of S_n , where n = [L:k].
- proof. (ii) Clear, since automorphisms permute the zeroes of f, of which we have at most n.
- (iii) We know L/k is simple, say $L = k[\alpha]$ for some $\alpha \in L$. Let m_{α} be the minimal polynomial of α over k. Then $\deg(f) = n$. Every $\sigma \in \operatorname{Aut}(L/k)$ 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 $L = k[\alpha]$ of a field k is called an *elementary* radical extension if either

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Since the automorphism $\sigma \in \text{Gal}(L/k)$ that maps $\alpha \mapsto \zeta \cdot \alpha$ has order n, Gal(L/k) is cyclic. (3) $f = X^p - X - \gamma$ has p zeroes in $L = k[\alpha]$. Since $f(\alpha) = 0$, we have

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

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

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

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

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

which is the claim.

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

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



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

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

i.e. we have a short exact sequence

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

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

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

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

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

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

Example 4.9 (i) Every abelian group is solvable.

(ii) S_4 is solvable by

$$1 \lhd V_4 \lhd A_4 \lhd S_4$$

where $V_4 = \{ id, (12)(34), (13)(24), (14)(23) \}$. 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 4.10 (i) Let G be a solvable group. Then

- (1) Every subgroup $H \leq G$ is solvable.
- (2) Every homomorphic image of G is solvable.
- (ii) Let

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

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

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

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

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

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

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

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

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

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.

'⇐' Let

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

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

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

and hence the chain

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

reveals the solvability of G.

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

proof. ' \Rightarrow ' Let

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

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

n=1 This is exactly remark 4.5, 4.6

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

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

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

an injective homomorphism of groups is given, hence

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

is solvable as a subgroup of a solvable group.

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

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

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

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

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

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

' \Leftarrow ' Let now \tilde{L}/L finite such that $\operatorname{Gal}(\tilde{L}/k)$ 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

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

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

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

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

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

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

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

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

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

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

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

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

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

proof. Let f be solvable by radicals, i.e. L(f)/k be a radical field extension. $\iff L(f)$ is contained in some Galois extension \tilde{L}/k and $\operatorname{Gal}(\tilde{L}/k)$ is solvable. $\iff \operatorname{In} k \subseteq L(f) \subseteq \tilde{L}$ all extensions are Galois. $\stackrel{3.5}{\iff} \operatorname{Gal}(L(f)/k) \cong \operatorname{Gal}(\tilde{L}/k)/\operatorname{Gal}(\tilde{L}/L(f))$ $\stackrel{4.8}{\iff} \operatorname{Gal}(L(f)/k)$ is solvable.

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

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

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

The χ_i are called *characters*. Clearly we have $n \ge 2$. Choose $g \in G$ such that $\chi_1(g) \ne \chi_2(g)$. 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

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

Consider

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

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

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

Proposition 4.14 Let L/k be a Galois extension such that $G := \operatorname{Gal}(L/k) = (\sigma)$ is cyclic of order d for some $\sigma \in G$, where $\operatorname{char}(k) \nmid d$. Let $\zeta_d \in k$ be a primitive d-th root of unity. Then there exists $\alpha \in L^{\times}$ such that $\sigma(\alpha) = \zeta \cdot \alpha$.

proof. Let

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

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

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

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

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

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

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

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

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

hence

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

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

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

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

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

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

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

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

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

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

§ 5 Norm and trace

Definition + remark 5.1 Let L/k be a finite separable field extension, [L : k] = n. Let $\operatorname{Hom}_{k}(L,\overline{k}) = \{\sigma_{1}, \ldots \sigma_{n}\}.$

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

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

- (ii) $N_{L/k} \in k$ for all $\alpha \in L$.
- (iii) $N_{L/k}: L^{\times} \longrightarrow k^{\times}$ is a homomorphism of groups.

proof. (ii) Let $\alpha \in L$. Assume first that L/k is Galois. Then $\operatorname{Hom}_k(L, \overline{k}) = \operatorname{Aut}_k(L) = \operatorname{Gal}(L/k)$. For $\tau \in \operatorname{Gal}(L/k)$ we have

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

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

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

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

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

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

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

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

which proves the claim.

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

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

- (ii) Let $k = \mathbb{R}$, $L = \mathbb{C}$. Then $\operatorname{Hom}_{\mathbb{R}}(\mathbb{C}, \overline{\mathbb{R}}) = \operatorname{Gal}(\mathbb{C}/\mathbb{R}) = {\operatorname{id}, z \mapsto \overline{z}}$ and thus the norm ist $N_{L/k}(z) = z\overline{z} = |z|^2$.
- (iii) Let $k = \mathbb{Q}, L = \mathbb{Q}[\sqrt{d}]$ for $d \in \mathbb{Z}$ squarefree. We have $[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] = 2$ and

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

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 $a^2 + \tilde{d}b^2 \stackrel{!}{=} 1 \Rightarrow$ either $a = \pm 1, b = 0$ or $a = 0, b = \pm 1, \tilde{d} = 1$.

• d > 0: Infinitely many solutions for $a^2 - bd^2 = 1$.

Proposition 5.3 (Hilbert's theorem 90 - multiplicative version) Let L/k a finite Galois extension with cyclic Galois group $\operatorname{Gal}(L/k) = (\sigma), n = [L:k]$. Let $\beta \in L$ with $N_{L/k}(\beta) = 1$. Then there exists $\alpha \in L^{\times}$ such that $\beta = \frac{\alpha}{\sigma(\alpha)}$.

proof. Define

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

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

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

which is the claim.

Definition + remark 5.4 Let L/k be a finite separable field extension, [L : k] = n. Let $\operatorname{Hom}_{k}(L, \overline{k}) = \{\sigma_{1}, \ldots \sigma_{n}\}.$

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

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

is called the *trace* of α over k.

- (ii) $tr_{L/k}(\alpha) \in k$ for all $\alpha \in L$.
- (iii) $tr_{L/k}: L \longrightarrow k$ is k-linear.

proof. (ii) As in proof 5.1, $tr_{L/k}(\alpha)$ is invariant under Gal(L/k). (iii) Clear.

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

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

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

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

proof. Define

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

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

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

we have

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

and we obtain the claim.

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

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

Then

(i) $N_{L/k}(\alpha) = \det(\phi_{\alpha}).$ (ii) $tr_{L/k}(\alpha) = \operatorname{tr}(\phi_{\alpha}).$

proof. Let

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

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

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

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

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

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

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

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

Then we easily see

$$\det(\phi_{\alpha}) = (-1)^{d} \cdot a_{0} = (-1)^{d} \cdot f(0) = (-1)^{d} \cdot \prod_{i=1}^{d} (0 - \sigma_{i}(\alpha)) = \prod_{i=1}^{d} \sigma_{i}(\alpha) = N_{L/k}(\alpha)$$
$$\operatorname{tr}(\phi_{\alpha}) = -a_{d-1} = tr_{L/k}(\alpha).$$

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

We obtain

$$\operatorname{tr}(\phi_{\alpha}) = d \cdot \alpha = tr_{L/k}(\alpha) \qquad \det(\phi_{\alpha}) = \alpha^{d} = tr_{L/k}(\alpha).$$

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

Claim (a) The following is true:

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

Claim (b) The following identity holds:

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

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

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

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

Let's now proof the claims.

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

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

hence ϕ_{α} is represented by

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

(a) This is an exercise.

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

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

$$N_{L/k}(\alpha) = \det(\phi_{\alpha}) \qquad \operatorname{tr}_{L/k}(\alpha) = \operatorname{tr}(\phi_{\alpha})$$

(ii) Let $\operatorname{Hom}_k(L, \overline{k}) = \{\sigma_1, \ldots, \sigma_r\}$. Then

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

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

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

where q is defined as above.

§ 6 Normal series of groups

Definition 6.1 Let G be a group.

(i) A series

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

of subgroups is called a *normal series* for G, if $G_i \lhd G_{i-1}$ is a normal subgroup in G_{i-1} and $G_i \neq G_{i-1}$ for $1 \le i \le n$. The groups $H_i := G_{i-1}/G_i$ are called *factors* of the series.
(ii) A normal series as above is called a *composition series* for G, if all its factors are simple groups and $G_n = \{e\}$.

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

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

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

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

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

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

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

Definition + **remark 6.4** Let *G* be a group.

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

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

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

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

(v) The chain

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

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

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

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

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

- (vi) ' \Leftarrow ' If the derived series of G stops at $\{e\}$, G has a normal series with abelian factors and is solvable.
 - '⇒' Let now $G = G_0 \triangleright \ldots \triangleright G_n = \{e\}$ be a normal series with abelian factors. We have to show that $G^{(n)} = \{e\}$.
 - Claim (a) We have $G^{(i)} \subseteq G_i$ for $0 \leq i \leq n$.

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

By induction on n we have $G^{(i)} = (G^{(i)}) \subseteq G_i$, hence $(G^{(i)}) \subseteq G_i$. Thus we get

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

which finishes the proof.

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

proof. ' \Rightarrow ' Let

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

be a normal series of G with abelian quotients $G_i - 1/G_i$ for $1 \le i \le m$. 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

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

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

$$G = G_0 \vartriangleright G_1 \vartriangleright \dots \trianglerighteq G_n = \{e\}$$
$$G = H_0 \vartriangleright H_1 \vartriangleright \dots \vartriangleright H_m = \{e\}$$

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

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

proof. We prove the statement by induction on n.

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

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

Then $\overline{H}_i = \pi(H_i) \triangleleft \overline{G}$ 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

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

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

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

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

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

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

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

$$\frac{C_i / C_{i+1} \simeq G_{\sigma(i)} / G_{\sigma(i)+1}}{C_j / C_{j+2} \simeq G_{\sigma(j)} / G_{\sigma(j)+1} }$$
 (*)

For some $\sigma : \{0, 1, \dots, j, j+2, j+3, \dots, n-1\} \longrightarrow \{1, \dots, n-1\}$ Claim (b) We have

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

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

It remains to show the Claims.

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

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

- (b) (1) We have $H_{j+1} \subseteq G_1$, hence $H_{j+1} \cap G_1 = H_{j+1} = C_{j+1}$. $C_j = H_j \cap G_1$ is normal subgroup of H_j . Thus $H_j \rhd C_j \rhd C_{j+1} = H_{j+1}$. Since H_i / H_{i+1} is simple, we must have $C_j = C_{j+1}$.
 - (2) i>j Then C_i = H_i ∩ G₁ = H_i since H_i ⊆ G₁.
 i<j We have H
 _i = G = G/G₁. Then we have G₁H_i = G (*), since: '⊆' Clear.
 '⊇' For g ∈ G, g ∈ G its image there exists h ∈ H_i such that

$$\overline{h} = \overline{g} \Longrightarrow \overline{h}^{-1}\overline{g} \in G_1 \longleftrightarrow \overline{h}^{-1}\overline{g} = g_1 \in G_1 \Longrightarrow g = hg_1 \in H_iG_1$$

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

(3) We have

$$H_i/H_{i+1} = H_i/C_{j+1} = H_j/C_j = H_j/H_j \cap G_1 = G_1H_j/G_1 \stackrel{(*)}{=} G/G_1,$$

which finishes the proof, paragraph and chapter.

Kapitel II

Valuation theory

§ 7 Discrete valuations

Example 7.1 Let $P \in \mathbb{N}$ prime. For $x \in \mathbb{Z} \setminus \{0\}$ let

$$\nu_p(x) = \max\{k \in \mathbb{N} \mid p^k \mid x\}.$$

Then $p^{\nu_p(x)} \mid x$, $p^{\nu_p(x)+1} \nmid x$. Example: $\nu_2(12) = 2$. Write $x = p^{\nu_p(x)} \cdot x'$ where $p \nmid x'$. For $\frac{x}{y} \in \mathbb{Q}^{\times}$ define

$$\nu_p\left(\frac{x}{y}\right) = \nu_p(x) - \nu_p(y)$$

This defines a map $\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z}$, such that

- (i) $v_p(ab) = \nu_p(a) + \nu_p(b)$ (clear)
- (ii) $v_p(a+b) \ge \min\{\nu_p(a), \nu_p(b)\}$, since: Write $a = p^{\nu_p(a)} \cdot a', b = p^{\nu_p(b)} \cdot b'$. Let w.l.o.g $\nu_p(b) \le \nu_p(a)$. Then we have

$$a + b = p^{\nu_p(a)} \cdot a' + p^{\nu_p(b)} \cdot b' = p^{\nu_p(b)} \cdot \left(b' + a' \cdot p^{\nu_p(a) - \nu_p(b)}\right).$$

Hence $p^{\nu_p(b)} \mid a+b$ and thus $\nu_p(a+b) \ge \nu_p(b) = \min\{\nu_p(a), \nu_p(b)\}.$

Definition 7.2 Let k be afield. A *discrete valuation* on k is a surjectove group homomorphism $\nu_k^{\times} \longrightarrow (\mathbb{Z}, +)$ satisfying

$$\nu(x+y) \ge \min\{\nu(x), \nu(y)\} \qquad \text{for all } x, y \in k^{\times}, \ x \neq -y.$$

Remark 7.3 Let R be a factorial domain, $k = \text{Quot}(\mathbb{R})$. Let further be $p \in \mathbb{R} \setminus \{0\}$ be a prime element. Then $\nu_p : k^{\times} \longrightarrow \mathbb{Z}$ can be defined as in Example 7.1: Write

$$x = e \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(x)}, \qquad e \in R^{\times}$$

where \mathbb{P} denotes set of representatives of prime elements of R. Then ν_p is a discrete valuation on k.

Example 7.4 Let k be a field, $a \in k$, R = k[X] and $p_a = X - a \in k[X]$. For $f \in k[X]$ define $\nu_{p_a}(f) = n$ if f has an n-fold root in a, i.e. $f = (X - a)^n \cdot g$ for some $0 \neq g \in k[X]$. Then ν_{p_a} is a discrete valuation on k(X) = Quot(k[X]) satisfying $\nu_p|_k = 0$.

Remark 7.5 There is no discrete valuation on \mathbb{C} .

proof. Assume there exists a discrete valuation on \mathbb{C} , say $\nu : \mathbb{C}^{\times} \longrightarrow \mathbb{Z}$. Since ν is surjective, there exists $z \in \mathbb{C}^{\times}$ such that $\nu(z) = 1$.

Let now $y \in \mathbb{C}^{\times}$ such that $y^2 = z$. Then we have

$$1 = \nu(z) = \nu(y^{2}) = \nu(y \cdot y) = \nu(y) + \nu(y) = 2\nu(y) \iff \nu(y) = \frac{1}{2} \notin \mathbb{Z}$$

which is a contradiction.

Example 7.6 Let $\nu : \mathbb{Q}^{\times} \longrightarrow \mathbb{Z}$ be a nontrivial discrete valuation. Then there exists $a \in \mathbb{Z}$ such that $\nu(a) \neq 0$ and hence we find $p \in \mathbb{P}$: $\nu(p) \neq 0$.

If $\nu(q) = 0$ for all $q \in \mathbb{P}$, then $\nu = \nu_p$.

Assume we have $\nu(p) \neq 0 \neq \nu(q)$ for some $p \neq q \in \mathbb{P}$ and write 1 = ap + bq for suitable $a, b \in \mathbb{Z}$. Then

$$0 = \nu(1) = \nu(ap + bq) \ge \min\{\nu(ap), \nu(bq)\} = \min\{\underbrace{\nu(a)}_{\ge 0 \ (*)} + \nu(p), \underbrace{\nu(b)}_{\ge 0 \ (*)} + \nu(q)\} \ge \min\{\nu(p), \nu(q)\} > 0$$

Hence a contradiction, i.e. we have $\nu(p) \neq 0$ for at most one $p \in \mathbb{P}$, thus $\nu = \nu_p$. (*) obtain that we have $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1) \Rightarrow \nu(1) = 0$ and by induction

$$\nu(a) = \nu(1 + (a - 1)) \ge \min\{\nu(1), \nu(a - 1)\} \ge 0$$

Proposition 7.7 Let k be a field and $\nu : k^{\times} \longrightarrow \mathbb{Z}$ be a discrete valuation on k.

- (i) $\nu(1) = \nu(-1) = 0.$
- (ii) $\mathcal{O}_{\nu} := \{x \in k^{\times} \mid \nu(x) \ge 0\} \cup \{0\}$ is a ring, called the valuation ring of ν .
- (iii) $\mathfrak{m}_{\nu} := \{x \in k^{\times} \mid \nu(x) > 0\} \cup \{0\} \lhd \mathcal{O}_{\nu} \text{ is an ideal in } \mathcal{O}_{\nu}, \text{ called the valuation ideal of } \nu.$ More precisely, \mathfrak{m}_{ν} is the only maximal ideal in \mathcal{O}_{ν} , i.e. \mathcal{O}_{ν} is a local ring.
- (iv) \mathfrak{m}_{ν} is a principal ideal.
- (v) \mathcal{O}_{ν} is a principal ideal domain. More precisely, any ideal $I \neq \{0\}$ in \mathcal{O}_{ν} is of the form $I = (t^d)$ for some $d \in \mathbb{N}$ and $t \in \mathfrak{m}_{\nu}$ with $\nu(t) = 1$.
- (vi) We have $k = \text{Quot}(\mathbf{R})$ and for $x \in k^{\times}$: $x \in \mathcal{O}_{\nu}$ or $\frac{1}{x} \in \mathcal{O}_{\nu}$.

proof. (ii) This is strict calculating, which may be verified by the reader.

(iii) \mathfrak{m}_{ν} is an ideal, since for $x, y \in \mathfrak{m}_{\nu}, \alpha \in \mathcal{O}_{\nu}$ we have

$$\nu(x+y) \ge \min\{\nu(x), \nu(y)\} > 0, \qquad \nu(\alpha x) = \underbrace{\nu(\alpha)}_{\ge 0} + \nu(x) \ge \nu(x) > 0.$$

Let now $x \in \mathcal{O}_{\nu}$ with $\nu(x) = 0$. Then

$$\nu\left(\frac{1}{x}\right) = \nu(1) - \nu(x) = -\nu(x) = 0,$$

hence $x \in \mathcal{O}_{\nu}^{\times}$. Thus we have $\mathfrak{m}_{\nu} = \mathcal{O}_{\nu} \setminus \mathcal{O}_{\nu}^{\times}$ and the claim follows.

(iv) Let $t \in \mathfrak{m}_{\nu}$ such that $\nu(t) = 1$. Then for $x \in \mathfrak{m}_{\nu}$ let $\nu(x) = d > 0$. Then we have

$$\nu\left(x\cdot t^{-d}\right) = \nu(x) + \nu\left(\frac{1}{t^d}\right) = d + 0 - d = 0$$

Define $e := x \cdot t^{-d} \in \mathcal{O}_{\nu}^{\times}$. Then $x = e \cdot t^d$, hence $\mathfrak{m}_{\nu} = (t)$.

- (v) Let $\{0\} \neq I \neq \mathcal{O}_{\nu}$ be an ideal in \mathcal{O}_{ν} . Let $d := \min\{\nu(x) \mid x \in I \setminus \{0\}\} > 0$.
 - '⊇' Let $x \in I$ such that $\nu(x) = d$. By part (iv) we have $x = e \cdot t^d$ for some $e \in \mathcal{O}_{\nu}^{\times}$, hence we have $t^d \in I$; thus $(t^d) \subseteq I$.
 - '⊆' Let now $y \in I \setminus \{0\}$ and write $y = e \cdot t^{\nu(y)}$ for some $e \in \mathcal{O}_{\nu}^{\times}$ and $\nu(y) > d$. Then $y = t^d \cdot e \cdot t^{\nu(y)-d}$, hence $y \in (t^d)$ and thus $I \subseteq (t^d)$.
- (vi) If $\nu(x) \ge 0$, then $x \in \mathcal{O}_{\nu}$. If $\nu(x) < 0$, we have

$$\nu\left(\frac{1}{x}\right) = \nu(1) - \nu(x) = -\nu(x) > 0, \quad \text{hence } \frac{1}{x} \in \mathfrak{m}_{\nu} \subseteq \mathcal{O}_{\nu},$$

which we wanted to show.

Definition 7.8 An integral domain R is called a *discrete valuation ring*, if there exists a discrete valuation ν of $k = \text{Quot}(\mathbf{R})$ such that $R = \mathcal{O}_{\nu}$.

Proposition 7.9 Let R be a lokal integral domain. Then the following statements are equivalent.

- (i) R is a discrete valuation ring.
- (ii) R is a principal ideal domain.
- (iii) There exists $t \in \mathbb{R} \setminus \{0\}$ such that every $x \in \mathbb{R} \setminus \{0\}$ can uniquely be written in the form

$$x = e \cdot t^d$$
 for some $e \in R^{\times}, \ d \ge 0$

proof. '(i) \Rightarrow (ii)' This follows by 7.7.

'(ii) ⇒ (iii)' We know that principal ideal domains are factorial. Let t ∈ R be a generator of the maximal ideal m of R. Then t is prime, since any maximal ideal is also prime. Let now p ∈ R\{0} a prime element. Then p ∉ R[×], hence p ∈ m, thus we can write p = t ⋅ x for some x ∈ R. Since p is prime, hence irreducible, we have x ∈ R[×] ⇒ (p) = (t). Thus we

have p = t and we have only one prime element in R. The unique prime factorization in factorial domains gives us $x = e \cdot t^d$ for some $e \in R^{\times}$ and $d \ge 0$.

'(iii) \Rightarrow (i)' For $x = e \cdot t^d \in R \setminus \{0\}$, $e \in R^{\times}, d \ge 0$ define $\nu(x) = d$. We claim that ν is discrete valuation. We have

$$\nu(xy) = \nu\left(et^d \cdot e't^{d'}\right) = \nu\left(ee't^{d+d'}\right) = \nu\left(e''t^{d+d'}\right) = d+d'.$$

Let w.l.o.g. $d \leq d'$. Then

$$\nu(x+y) = \nu\left(et^d + e't^{d'}\right) = \nu\left(t^d\left(e + e't^{d'-d}\right)\right) \ge d = \min\{d, d'\}$$

which we extend to

$$\nu: k^{\times} \longrightarrow \mathbb{Z}, \qquad \nu\left(\frac{x}{y}\right) = \nu(x) - \nu(y).$$

This is well defined: For $\frac{x}{y} = \frac{x'}{y'}$ we have xy' = x'y and $\nu(x'y) = \nu(x) + \nu(y') = \nu(x') + \nu(y)$, thus

$$\nu\left(\frac{x}{y}\right) = \nu(x) - \nu(y) = \nu(x') - \nu(y') = \nu\left(\frac{x'}{y'}\right).$$

Finally we have $\nu(t) = 1$, hence $\nu : k^{\times} \longrightarrow \mathbb{Z}$ is surjective. Thus ν is a discrete valuation on k and $R = \mathcal{O}_{\nu}$.

Definition + **proposition 7.10** Let R be a local ring with maximal ideal \mathfrak{m} .

- (i) $k := R/\mathfrak{m}$ is called the *residue field* of R.
- (ii) $\mathfrak{m}/\mathfrak{m}^2$ has a structure of a k-vector space.
- (iii) If R is a discrete valuation ring, then $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

proof. (ii) For $a \in R$, $x \in \mathfrak{m}$ define $\overline{ax} = \overline{ax}$, where $\overline{a}, \overline{x}$ are the images of a, x in k.

This is well defined: Let $a' \in R$ with $\overline{a'} = \overline{a}$ and $x' \in \mathfrak{m}$ with $\overline{x'} = \overline{x}$. We have to show that

$$\overline{a'x'} = \overline{ax} \iff a'x' - ax \in \mathfrak{m}^2$$

We have $\overline{a'} = \overline{a}$, hence a' = a + y for some $y \in \mathfrak{m}$. Analogously we have $\overline{x'} = \overline{x}$, hence x' = x + for some $z \in \mathfrak{m}^2$. Thus we have

$$a'x' = (a+y)(b+z) = ax + az + xy + yz \equiv ax \mod \mathfrak{m}^2,$$

which finishes the proof.

§ 8 The Gauß Lemma

Let R be a UFD (unique factorization domain), \mathbb{P} a set of representatives of the primes in R with respect to associateness, i.e. $x \sim y \iff y = u \cdot x$ for some $u \in \mathbb{R}^{\times}$. Every $x \in \mathbb{R} \setminus \{0\}$ has a unique factorization

$$x = u \cdot \prod_{p \in \mathbb{P}} p^{\nu_p(x)}, \qquad \nu_p(x) \ge 0 \text{ for } p \in \mathbb{P}, \, u \in R^{\times}$$

where $\nu_p: k^{\times} \longrightarrow \mathbb{Z}$ is a discrete valuation on $k = \operatorname{Quot}(R)$.

Definition + **proposition 8.1** Let R be a factorial domain, k = Quot(R) and

$$f = \sum_{i=0}^{n} a_i X^i \in k[X] \setminus \{0\}, \qquad a_n \neq 0.$$

- (i) For $p \in \mathbb{P}$ let $\nu_p(f) = \min\{\nu_p(a_i) \mid 0 \leq i \leq n\}.$
- (ii) f is called *primitive*, if $\nu_p(f) = 0$ for all $p \in \mathbb{P}$.
- (iii) If f is primitive, then $f \in R[X]$.
- (iv) If $f \in R[X]$ is monic, i.e. $a_n = 1$, then f is primitive.
- (v) There exists $c \in k^{\times}$ such that $c \cdot f$ is primitive.
- proof. (iii) If f is primitive, we have $\min_{1 \le i \le n} \{\nu_p(a_i)\} = 0$, i.e. $\nu_p(a_i) \ge 0$ for all $1 \le i \le n$. Thus $a_i \in R$ and $f \in R[X]$.
- (iv) If $a_i \in R$ we have $\nu_p(a_i) \ge 0$ for all $1 \le i \le n$. Moreover $\nu_p(a_n) = \nu_p(1) = 0$, hence $\nu_p(f) = \min_{1 \le i \le n} \{\nu_p(a_i)\} = 0$. thus f is primitive.
- (v) For $\nu_p(f) := d$ choose $c := p^{-d} \in k^{\times}$. Then

$$\nu_p(c \cdot f) = \nu_p(c) + \nu_p(f) = \nu_p(p^{-d}) + d = -d + d = 0,$$

thus $c \cdot f$ is primitive.

Proposition 8.2 (Gauß-Lemma) For $f, g \in k[X]$ and $p \in \mathbb{P}$ we have

$$u_p(f \cdot g) = \nu_p(f) + \nu_p(g).$$

proof. Write

$$f = \sum_{i=0}^{n} a_i X^i, \qquad g = \sum_{j=0}^{m} b_j X^j, \qquad f \cdot g = \sum_{k=0}^{m+n} c_k X^k, \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

case 1 Assume m = 0, i.e. $g = b_0 \in k^{\times}$. Then $c_k = a_k \cdot b_0$, hence

$$\nu_p(c_k) = \nu_p(a_k) + \nu_p(b_0).$$

Then we obtain

$$\nu_p(f \cdot g) = \min_{0 \le k \le n} \nu_p(c_k) = \min_{0 \le k \le n} \{\nu_p(a_k) + \nu_p(b_0)\} = \nu_p(b_0) + \min_{0 \le k \le n} \{\nu_p(a_k)\} = \nu_p(g) + \nu_p(f)$$

case 2 Assume $\nu_p(f) = 0 = \nu_p(g)$, i.e. f, g are primitive. Clearly $\nu_p(fg) \ge 0$. We have to show: $\nu_p(fg) = 0$. Let $i_0 := \max\{i \mid \nu_p(a_i) = 0\}$ and $j_0 := \max\{j \mid \nu_p(b_j) = 0\}$. Then

$$c_{i_0+j_0} = \sum_{i=0}^{i_0+j_0} a_i b_{i_0+j_0-i} = \underbrace{\sum_{i=0}^{i_0-1} a_i b_{i_0+j_0-i}}_{(A)} + a_{i_0+j_0} + \underbrace{\sum_{i=i_0+1}^{i_0+j_0} a_i b_{i_0+j_0-i}}_{(B)}$$

We have $\nu_p(a_{i_0}b_{j_0}) = \nu_p(a_{i_0}) + \nu_p(b_{j_0}) = 0$. We have $i_0 + j_0 - i > j_0$, hence $\nu_p(b_{i_0+j_0-i}) \ge 1$ for $0 \le i \le i_0 - 1$. Then

$$\nu_p(A) = \nu_p \left(\sum_{i=0}^{i_0-1} a_i b_{i_0+j_0-i} \right) \ge \min_{0 \le i \le i_0-1} \{ \nu_p(a_i b_{i_0+j_0-1}) \}$$
$$= \min_{0 \le i \le i_0-1} \{ \nu_p(a_i) + \nu_p(b_{i_0+j_0-1}) \}$$
$$\ge \min_{0 \le i \le i_0-1} \{ \nu_p(b_{i_0+j_0-1}) \}$$
$$\ge 1$$
$$\nu_p(B) = \nu_p \left(\sum_{i=i_0+1}^{i_0+j_0} a_i b_{i_0+j_0-i} \right) \ge 1.$$

Since we have

$$0 = \nu_p(a_{i_0}b_{j_0}) \ge \min\{\nu_p(c_{i_0+j_0}), \nu_p(A), \nu_p(B)\} = \nu_p(c_{i_0+j_0}) = 0$$

we get $\nu_p(c_{i_0+j_0}) = 0$. Hence we obtain

$$\nu_p(fg) = \min\{\nu_p(c_i) \mid 0 \le i \le m+n\} = \nu_p(c_{i_0+j_0}) = 0.$$

case 3 Consider now the general case, i.e. f, g are arbitrary. Multiply f and g by suitable constants a and b, such that $\tilde{f} := af$ and $\tilde{g} := bg$ are primitive. Then by the first two cases we have

$$\begin{split} \nu_p(fg) &= \nu_p \left(\frac{1}{a}\frac{1}{b}\tilde{f}\tilde{g}\right) \stackrel{1}{=} \nu_p \left(\frac{1}{a}\frac{1}{b}\right) + \nu_p(\tilde{f}\tilde{g}) \stackrel{2}{=} \nu_p \left(\frac{1}{a}\right) + \nu_p \left(\frac{1}{b}\right) + \underbrace{\nu_p(\tilde{f})}_{=0} + \underbrace{\nu_p(\tilde{g})}_{=0} \\ &= \nu_p \left(\frac{1}{a}\right) + \nu_p(\tilde{f}) + \nu_p \left(\frac{1}{b}\right) + \nu_p(\tilde{g}) = \nu_p \left(\frac{1}{a}\tilde{f}\right) + \nu_p \left(\frac{1}{b}\tilde{g}\right) \\ &= \nu_p(f) + \nu_p(g), \end{split}$$

which finishes the proof.

Theorem 8.3 (*Eisenstein's criterion for irreducibility*) Let R be a factorial domain, $p \in \mathbb{P}$ and

$$f = \sum_{i=0}^{n} a_i X^i \quad \in R[X] \backslash \{0\}$$

Assume that f is primitive and we have

- (i) $\nu_p(a_0) = 1$,
- (ii) $\nu_p(a_i) \ge 1$ or $a_i = 0$ for $1 \le i \le n-1$ and
- (*iii*) $\nu_p(a_n) = 0$
- Then f is irreducible over R[X].

proof. Assume that $f = g \cdot h$ with some $g, h \in R[X]$. Write

$$g = \sum_{i=0}^{r} b_i X^i, \qquad h = \sum_{j=0}^{s} c_i X^j, \qquad \text{with } r+s = n$$

Then we have $a_0 = b_0 c_0$. W.l.o.g. $\nu_p(b_0) = 1$ and $\nu_p(c_0) = 0$. Further $a_n = b_r c_s$, thus we must have $\nu_p(b_r) = \nu_p(c_s) = 0$ for $\nu_p(a_n) = 0$. Let now

$$d := \max\{i \mid \nu_p(b_j) \ge 1 \text{ for } 0 \le j \le i\}$$

Obviously $0 \leq d \leq r - 1$. Consider

$$a_{d+1} = \underbrace{b_{d+1}c_0}_{=:A} + \underbrace{\sum_{i=0}^{d} b_i c_{d+1-i}}_{=:B}$$

We have

$$\nu_p(A) = \nu_p(b_{d+1}) + \nu_p(c_0) = 0 + 0 = 0,$$
$$\nu_p(B) \ge \min_{0 \le i \le d} \{\nu_p(b_i c_{d+1-1}) \ge 1$$

and thus $\nu_p(a_{d+1}) = 0$. But this implies $d + 1 = n \Leftrightarrow n - 1 = d \leqslant r - 1 \Rightarrow n \leqslant r \Rightarrow n = r$. Then we have s = 0, thus $h = c_0$ is constant. Further for $q \in \mathbb{P}$ we have

$$0 = \nu_q(f) = \nu_q(gc_o) = \underbrace{\nu_q(g)}_{\geqslant 0} + \nu_q(c_0)$$

i.e. $\nu_q(c_0) = 0$, hence $c_0 \in \mathbb{R}^{\times}$ and f is irreducible.

Theorem 8.4 (Gauß) Let R be a factorial domain. Then R[X] is factorial.

proof. Let $f \in R[X] \setminus \{0\} \subseteq k[X]$ where k = Quot(R). Since k[X] is factorial, we can write

$$f = c \cdot f_1 \cdots f_n, \quad f_i \in k[X] \text{ prime }, \ c \in k^{\times}$$

W.l.o.g the. f_i are primitive, otherse multiply them by suitable constants. In particular we have $f_i \in R[X]$. Note that $c \in R$: For $p \in \mathbb{P}$, we have

$$0 = \nu_p(f) = \nu_p(c) + \sum_{i=1}^n \nu_p(f_i) = \nu_p(c).$$

Write $c = \epsilon \cdot p_1 \cdots p_r$ with some $\epsilon \in \mathbb{R}^{\times}$ and $p_i \in \mathbb{P}$. Then by

Claim (a) $f_i \in R[X]$ are prime for $1 \leq i \leq n$.

Claim (b) $p_i \in R[X]$ are prime for $1 \leq i \leq r$.

we have found a factorization of f into prime elements and hence R[X] is factorial. Now prove the claims.

(a) Let $g, h \in R[X]$ such that $gh \in (f_i) = f_i R[X]$. May assume that $g \in f_i k[X]$, i.e. $g = f_i \tilde{g}$ for some $\tilde{g} \in k[X]$. For $p \in \mathbb{P}$ we obtain

$$0 \leq \nu_p(g) = \underbrace{\nu_p(f_i)}_{=0} + \nu_p(\tilde{g}) = \nu_p(\tilde{g}).$$

Thus we get $\tilde{g} \in R[X]$, which implies $g = f_i \tilde{g} \in f_i R[X] = (f_i)$.

(b) Since $\pi : R \longrightarrow R/(p)$ induces a map $\psi : R[X] \longrightarrow R/(p)[X]$ with $\ker(\psi) = pR[X]$ we have

$$R[X]/pR[X] \cong R/pR[X].$$

Since R/pR is an integral domain, (p) is prime.

Corollary 8.5 Let k be a field. Then $k[X_1, \ldots, X_n]$ is factorial for any $n \in \mathbb{N}$.

Corollary 8.6 Let R be a factorial domain, k = Quot(R). If $f \in R[X]$ is irreducible over R[X], then f is irreducible over k[X].

proof. Let $0 \neq f = c \cdot f_1 \cdots f_n$ be decomposition of f in k[X], i.e. $c \in k^{\times}$ and $f_i \in k[X]$ irreducible for $1 \leq i \leq n$. We may assume that the f_i are primitive, hence contained in R[X], since we can multiply them by suitable constants. We still have to show $c \in R$. Since $f \in k[X]$, i.e. $\nu_p(f) \geq 0$ we have

$$\nu_p(f) = \nu_p(c \cdot f_1 \cdots f_n) = \nu_p(c) + \sum_{i=1}^n \underbrace{\nu_p(f_i)}_{=0} = \nu_p(c) \stackrel{!}{\geq} 0$$

Thus $c \in R$. Then the decomposition from above is in R - but since f is irreducible in R, we have n = 1 and $c \in R^{\times}$.

§ 9 Absolute values

Definition 9.1 Let k be a field. A map

$$|\cdot|:k\longrightarrow \mathbb{R}_{\geq 0}$$

is called an *absolute value*, if

- (i) positive definiteness: $|x| = 0 \iff x = 0$
- (ii) multiplicativeness: $|xy| = |x| \cdot |y|$ for all $x, y \in k$.
- (iii) triangle inequality: $|x + y| \leq |x| + |y|$ for all $x, y \in k$.

Example 9.2 (i) The 'normal' absolute value $|\cdot|_{\infty}$ on \mathbb{C} and on any of its subfields denotes an absolute value.

(ii) Let $\nu_k^{\times} \longrightarrow \mathbb{Z}$ be a discrete valuation, $\rho \in (0, 1)$. Then

$$|\cdot|_{\nu}: k \longrightarrow \mathbb{R}, \ x \mapsto \begin{cases} \rho^{\nu(x)} & x \neq 0\\ 0 & x = 0 \end{cases}$$

is an absolute value on k, since

- (1) Trivial, since |0| = 0 and $\rho^x \neq 0$ for any $x \in \mathbb{Z}$.
- (2) Clearly $|xy|_{\nu} = \rho^{\nu(xy)} = \rho^{\nu(x)+\nu(y)} = \rho^{\nu(x)}\rho^{\nu(y)} = |x|_{\nu}|y|_{\nu}$.
- (3) Further

$$|x+y|_{\nu} = \rho^{\nu(x+y)} \leqslant \rho^{\min\{\nu(x),\nu(y)\}} = \max\{\rho^{\nu(x)}, \rho^{\nu(y)}\} = \max\{|x|_{\nu}, |y|_{\nu}\} \leqslant |x|_{\nu} + |y|_{\nu}$$

(iii) For the *p*-adic valuation ν_p on \mathbb{Q} we choose $\rho := \frac{1}{p}$. Then $|x|_p = p^{-\nu_p(x)}$ is an absolute value.

Remark + definition 9.3 Let k be a field, $|\cdot|$ an absolute value on k.

- (i) |1| = |-1| = 1 and |x| = |-x| for all $x \in k$.
- (ii) The absolute value is called trivial, if |x| = 1 for all $x \in k$.

proof. We have $|1| = |1 \cdot 1| = |1| \cdot |1|$, hence |1| = 1. Moreover $|-1| = |1 \cdot (-1)| = |1| \cdot |-1|$, hence |-1| = 1. For $x \in k$ we have $|-x| = |(-1) \cdot x| = |-1| \cdot |x| = |x|$.

Proposition + definition 9.4 Let k be a field with char(k) = 0, i.e. $k \supseteq \mathbb{Q}$ and $|\cdot|$ an absolute value on k.

- (i) $|\cdot|$ is called *archimedean*, if |n| > 1 for all $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$.
- (ii) $|\cdot|$ is called *nonarchimedean*, if $|n| \leq 1$ for all $n \in \mathbb{Z}$.
- (iii) $|\cdot|$ is either archimedean or nonarchimedean.
- (iv) The *p*-adic absolute value on \mathbb{Q} is nonarchimedean.

proof of (iii). Since |n| = |-n|, it suffices to check $n \in \mathbb{N}$. Let $a \in \mathbb{N} \subseteq k$ with |a| > 1. Assume there exists $b \in \mathbb{N}_{>1}$ with $|b| \leq 1$. Write

$$a = \sum_{i=0}^{N} \alpha_i b^i \qquad \alpha_i \in \{0, \dots b - 1\}, \ |N| = \lfloor \log_b(a) \rfloor.$$

Then we have

$$|a| \leq \sum_{i=0}^{\lfloor \log_b(a) \rfloor} |\alpha_i| |b|^i \leq \log_b(a) \cdot \max_{0 \leq i \leq \lfloor \log_b(a) \rfloor} \{ |\alpha_i| \} =: \log_b(a) \cdot c,$$
$$|a^n| \leq \log_b(a^n) \cdot c = n \cdot \log_b(a) \cdot c$$

and $|a^n|$ grows linearly in n. Likewise we get for $n \in \mathbb{N}$

$$a^{n} = \sum_{i=0}^{\lfloor \log_{b}(a^{n}) \rfloor} \alpha_{i}^{(n)} b^{i}, \qquad \alpha_{i}^{(n)} \in \{0, \dots b-1\},$$

$$|a^n| = |a|^n \leq (\log_b(a) \cdot c)^n$$

which grows exponentially in n, which is a contradiction. Hence the claim follows.

Remark 9.5 An absolute value $|\cdot|$ on a field k induces a metric

$$d(x,y) := |x-y|, \qquad x, y \in k$$

Therefore, k as a topology and aspects as 'convergence' and 'cauchy sequences' are meaningful.

- **Definition** + **remark 9.6** (i) Two absolute values $|\cdot|_1, |\cdot|_2$ on k are called *equivalent*, if there exists $s \in \mathbb{R}$, such that $|x|_1 = |x|_2^s$ for all $x \in k$. In this case, we write $|\cdot|_1 \sim |\cdot|_2$.
 - (ii) Two absolutes values $|\cdot|_1, |\cdot|_2$ are equivalent if and only if the induce the same topology on k.

proof. Is left for the reader as an exercise.

Example 9.7 The *p*-adic absolute values on \mathbb{Q} are not equivalent for $p \neq q \in \mathbb{P}$. Consider

$$|p^n|_p = p^{-n} \xrightarrow{n \to \infty} 0, \qquad |p^n|_q = 1 \text{ for all } n \in \mathbb{N}$$

Moreover we have $|\cdot|p \neq |\cdot|_{\infty}$, since by the transittivity of equivalence of absolute values, we have

$$|\cdot|_p \sim |\cdot|_{\infty} \sim |\cdot|_q$$

which is not true.

Theorem 9.8 (Ostrowski) Any nontrivial absolute value $|\cdot|$ on \mathbb{Q} is equivalent either to the standard absolute value $|\cdot|_{\infty}$ on \mathbb{Q} or to a p-adic absolute value $|\cdot|_p$ for some $p \in \mathbb{P}$.

proof. case 1 Assume $|\cdot|$ is nonarchimedean. We want to show, that in this case $|\cdot| \sim |\cdot|_p$ for some $p \in \mathbb{P}$. Since $|\cdot|$ is non-trivial, there exists $x \in \mathbb{N}$ such that

$$|x| = \left| \prod_{p \in \mathbb{P}} p^{\nu_p(x)} \right| = \prod_{p \in \mathbb{P}} |p|^{\nu_p(x)} \neq 1$$

for at least one $x \in \mathbb{Q}$, hence, we have $|p| \neq 1$ for at least one $p \in \mathbb{P}$, i.e. |p| < 1. Assume there is another prime $q \neq p$ with |q| < 1. Then we find $N \in \mathbb{N}$, such that

$$|p|^N \leq \frac{1}{2}, \qquad |q|^N \leq \frac{1}{2}$$

Moreover, since p^N, q^N are coprime, we can write

$$1 = a \cdot p^N + b \cdot q^N \qquad \text{for suitable } a, b \in \mathbb{Z}.$$

So the contradiction follows by

$$1 = |1| = \left|ap^N + bq^N\right| \leqslant \underbrace{|a|}_{\leqslant 1} \underbrace{\left|p^N\right|}_{<\frac{1}{2}} + \underbrace{|b|}_{\leqslant 1} \underbrace{\left|q^N\right|}_{<\frac{1}{2}} < 1,$$

hence we have |q| = 1 for any $q \neq p \in \mathbb{P}$. Let now $s := -\log_p |p|$. For $x \in \mathbb{Q}^{\times}$ we obtain

$$|x| = \left| \prod_{\tilde{p} \in \mathbb{P}} \tilde{p}^{\nu_{\tilde{p}}(x)} \right| = \prod_{\tilde{p} \in \mathbb{P}} |\tilde{p}|^{\nu_{\tilde{p}}(x)} = |p|^{\nu_{p}(x)} = p^{-s \cdot \nu_{p}(x)} = \left(p^{-\nu_{p}(x)} \right)^{s} = |x|_{p}^{s}$$

thus we have $|\cdot| \sim |\cdot|_p$.

case 2 Let now $|\cdot|$ be archimedean. We now have to show $|\cdot| \sim |\cdot|_{\infty}$. For $n \in \mathbb{N}_{\geq 2}$ we have

$$1 < |n| = \left|\sum_{i=1}^{n} 1\right| \le \sum_{i=1}^{n} |1| = n.$$

For any $a \in \mathbb{N}_{\geq 2}$ we find $s := s(a) \in \mathbb{R}_{<0}$ such that

$$|a| = |a|_{\infty}^{s} = a^{s}$$

namely

$$s = \log_a(|a|) = \frac{\log(|a|)}{\log(a)}.$$

Claim (a) We have

$$\frac{\log(|a|)}{\log(a)} = \frac{\log(|2|)}{\log(2)}.$$

Since now s is independent of a, we have $|\cdot| \sim |\cdot|_{\infty}$. Prove now the claim:

(a) For $n \in \mathbb{N}$ write

$$2^{n} = \sum_{i=0}^{N} \alpha_{i} a^{i} \text{ with } \alpha_{i} \in \{0, \dots, a-1\} \text{ and } N \leq \log_{a} 2^{n} = n \cdot \frac{\log(2)}{\log(a)}.$$

Then we have

$$|2|^n = |2^n| \leq \sum_{i=0}^N \underbrace{|\alpha_i|}_{\leq \alpha_i < a} \overbrace{|a|^i} \leq |a|^N \leq (N+1)^{\cdot} a \cdot |a|^N,$$

hence we get

$$n \cdot \log(|2|) \leq \log(N+1) + \log(a) + N \log(|a|)$$

$$\leq \log\left(n \cdot \frac{\log(2)}{\log(a)} + 1\right) + \log(a) + n \cdot \frac{\log(2)}{\log(a)} \cdot \log(|a|).$$

Multiplying the equation by $\frac{1}{n} \cdot \frac{1}{\log(2)}$ gives us

$$\frac{\log(|2|)}{\log(2)} \leqslant \frac{1}{n} \cdot \log\left(n \cdot \frac{\log(2)}{\log(a)} + 1\right) + \frac{\log(|a|)}{\log(a)}$$

and thus

$$\frac{\log(|2|)}{\log(2)} \leqslant \frac{\log(|a|)}{\log(a)}.$$

Swapping the roles of a and 2 in the equation above gives us the other inequality. Hence we have equality, which proves the claim.

Proposition 9.9 Let $|\cdot|$ be a nonarchimedean absolute value on a field k.

- (i) $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in k$.
- (ii) If $|x| \neq |y|$, then equality holds in (i).

proof. (i) If x = 0, we have $|y + x| = |y| \le \max\{0, |y|\} = \max\{|x|, |y|\}$. Thus assume $x \ne 0$. We have $|x + y| = |x| \left| 1 + \frac{y}{x} \right|$. It suffices to show $|x + 1| \le \max\{1, |x|\}$. Then we get

$$|x+y| = |y| \cdot \left|1 + \frac{x}{y}\right| \le |y| \cdot \max\left\{\left|\frac{x}{y}\right|, |1|\right\} \le \max\{|x|, |y|\}$$

For $n \in \mathbb{N}$ we have

$$(x+1)^n = \sum_{k=0}^n \binom{n}{k} x^k.$$

Then we have

$$|x+1|^{n} = |(x+1)^{n}| = \left|\sum_{k=0}^{n} \binom{n}{k} x^{k}\right| \leq \sum_{k=0}^{n} \left|\underbrace{\binom{n}{k}}_{\leq 1}\right| \underbrace{|x|}_{\leq 1}^{k} \leq n+1,$$

hence

$$|x+1| \leq \sqrt[n]{n+1}$$
 for all $n \in \mathbb{N}$.

Thus $|1 + x| \leq 1$. Since we clearly have $|x + 1| \leq |x|$, we all in all have

$$|x+1| \le \max |\{|x|, 1\}.$$

(ii) Let z = x + y and assume |x| < |y|. We have to show |z| = |y|. Assume |z| < |y|. Then

$$|y| = |z - x| \stackrel{(i)}{\leq} \max\{|z|, |-x|\} < |y| \quad \notin$$

and the proof is done.

Proposition 9.10 Let $|\cdot|$ be an a nonarchimedean absolute value on a field k. Then

(i) We have a local ring

$$\overline{\mathcal{B}}_1(0) := \{ x \in k | |x| \le 1 \} =: \mathcal{O}_k$$

with maximal ideal

$$\mathcal{B}_1(0) := \{ x \in k | |x| < 1 \} =: \mathfrak{m}_k$$

- (ii) Every point in ball is its center.
- (iii) Balls are either disjoint or one of them is contained in the other one.
- (iv) All triangles are isosceles.

proof. (i) By 9.8(i), $\mathcal{B}_1(0)$ is closed under Addition. The remaining is calculating.

(ii) Let $z \in \overline{\mathcal{B}}_r(x)$. To show: $\overline{\mathcal{B}}_r(z) = \overline{\mathcal{B}}_r(x)$.

' \subseteq ' Let $y \in \overline{\mathcal{B}}_r(z)$, i.e. we have $|y - z| \leq r$. Then

$$|y-x| = |y-z+z-x| \leq \max\{|y-z|, |z-x|\} \leq r \quad \Rightarrow \quad y \in \mathcal{B}_r(x).$$

Thus we have $\overline{\mathcal{B}}_r(z) \subseteq \overline{\mathcal{B}}_r(x)$.

 \supseteq Follows by symmetry.

(iii) Let $\mathcal{B} := \overline{\mathcal{B}}_r(x), \, \mathcal{B}' := \overline{\mathcal{B}}_{r'}(x')$ and $y \in \mathcal{B} \cap \mathcal{B}'$. W.l.o.g. $r \leq r'$.

Then for $z \in \mathcal{B}$ we have

$$|z - x'| = |z - x + x - y + y - x'| \le \max\{|z - x|, |x - y|, |y - x'|\} = \max\{r, r, r'\} = r'$$

which implies $z \in \mathbb{B}'$. Hence we have $\mathcal{B} \subseteq \mathcal{B}'$.

(iv) Follows from 9.8(ii).

Corollary 9.11 Let k be a field, $|\cdot|$ a nonarchimedean absolute value on k.

- (i) All balls are closed and open, considering the topology on k induced by the metric d(x, y) = |x y|.
- (ii) k is totally disconnected, i.e. no subset of k containing more than on element is connected.
- proof. (i) Let $\mathcal{B} := \overline{\mathcal{B}}_r(x)$ be a closed ball for some $x \in k, r \in \mathbb{R}_{\geq 0}$. Then \mathcal{B} topologically clearly is closed. Let now $y \in \mathcal{B}$. Then $\mathcal{B}_r(y) \subseteq \mathcal{B}$ by 9.9(ii), i.e. \mathcal{B} is open. Let now $\mathcal{B} := \mathcal{B}_r(x)$ be an open ball and $y \in k$ a boundary point. Thus for all s > 0 we find $z \in \mathcal{B}_s(x) \cap \mathcal{B}_r(x)$. Choose $s \leq r$. Then

$$d(x, y) \leq \max\{d(y, z), d(x, z)\} < \max\{s, r\} = r.$$

Thus $y \in \mathcal{B}_r(x)$, hence $\mathcal{B}_r(x)$ is contains its boundary and is closed.

(ii) Let $X \subseteq k$ be a subset with $x \neq y \in X$. Then for r := |x - y| > 0 we get

$$X = \left(\overline{\mathcal{B}}_{\frac{r}{2}}(x) \cap X\right) \cup \left(X \setminus \overline{\mathcal{B}}_{\frac{r}{2}}(x)\right)$$

which is a decomposition of X into two nonempty, disjoint open subset, i.e. the claim follows.

Example 9.12 (*Geometry on* $(\mathbb{Q}, |\cdot|_p)$) The unit disc in $(\mathbb{Q}, |\cdot|_p)$ is

$$\left\{\frac{a}{b} \in \mathbb{Q} \ \big| \ p \nmid b\right\} =: \mathbb{Z}_{(p)}$$

The maximal ideal is

$$\left\{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b, p \mid a\right\} = p \cdot \mathbb{Z}_{(p)} = \overline{\mathcal{B}}_{\frac{1}{p}}(0)$$

We have

$$\left\{x \in \mathbb{Q} \mid |x|_p < 1\right\} = \left\{x \in \mathbb{Q} \mid |x|_{\infty} < \frac{1}{p}\right\}$$

Moreover

$$\mathbb{Z}_{(p)} / p\mathbb{Z}_{(p)} \cong \mathbb{Z} / p\mathbb{Z} = \mathbb{F}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$$

 $\overline{\mathcal{B}}_1(0)$ is the disjoint union of the $\overline{\mathcal{B}}_{\frac{1}{p}}(i)$ for $0 \leq i \leq p-1$, where $\overline{\mathcal{B}}_{\frac{1}{p}}(i) = i + p\mathbb{Z}_{(p)}$.

§ 10 Completions, *p*-adic numbers and Hensel's Lemma

Remark 10.1 Let $|\cdot|$ be an absolute value on a field k. Let

$$\mathcal{C} := \{ (a_n)_{n \in \mathbb{N}} \mid (a_n) \text{ is Cauchy sequence in } (k, |\cdot|) \}$$

be th ring (!) of Cauchy sequences in k and

$$\mathcal{N} := \left\{ (a_n)_{n \in \mathbb{N}} \mid \lim_{n \to \infty} a_n = 0 \right\} \triangleleft \mathcal{C}$$

the ideal (!) of Cauchy sequences converging to 0. Then

- (i) \mathcal{N} is a maximal ideal.
- (ii) k' := C / N is a field extension of k.
- (iii) $|\overline{(a_n)_{n\in\mathbb{N}}}| := \lim_{n\to\infty} (a_n) \in \mathbb{R}_{\geq 0}$ is an absolute value on k' extending $|\cdot|$.
- (iv) k' is complete with respect to $|\cdot|$.

Remark 10.2 If $|\cdot|$ is nonarchimedean, for every Cauchy sequence $(a_n)_{n\in\mathbb{N}} \notin \mathcal{N}$ we have $|a_m| = |a_n|$ for all $m, n \gg 0$.

proof. Since $(a_n) \notin \mathcal{N}$, 0 is not an accumulation point of $(a_n) \Longrightarrow |a_n| \ge \epsilon$ for some $\epsilon > 0$ and all $n \ge n_0(\epsilon) =: n_0$. Thus for $n, m \ge n_0$ we have $|a_n - a_m| < \epsilon$. This implies by 9.8 (ii)

$$|a_n - a_m| \leq \max\{|a_n|, |a_m|\} \implies |a_n| = |a_m|,$$

which was the claim.

Definition 10.3 Let $k = \mathbb{Q}$, $|\cdot| = |\cdot|_p$ for some $p \in \mathbb{P}$. Then the field k' on 10.1 is called the field of *p*-adic numbers and denoted by \mathbb{Q}_p . The valuation ring is called the ring of *p*-adic integers and is denoted by \mathbb{Z}_p .

Remark 10.4 (i) $\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Z}_p$.

- (ii) The maximal ideal in \mathbb{Z}_p is $p\mathbb{Z}_p$.
- (iii) $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{Z} / p\mathbb{Z} = \mathbb{F}_p$.
- (iv) \mathbb{Z}_p is a discrete valuation ring.

proof. (i) The first inclusion is clear. For the second one consider $x = \frac{r}{s} \in \mathbb{Z}_{(p)}$. Then by definition of localization we have $p \nmid s$ and hence

$$|x| = \left|\frac{r}{s}\right| = \frac{|r|}{|s|} = |r| \leqslant 1$$

and thus $x \in \mathbb{Z}_p$. Now prove that \mathbb{Z} is dence in \mathbb{Z}_p : Let $x \in \mathbb{Z}_p$ with p-adic expansion

$$x = \sum_{i=0}^{\infty} a_i p^i, \qquad a_i \in \{0, 1, \dots, p-1\}.$$

Define a sequence $(x_n)_{n \in \mathbb{N}}$ by

$$x_n := \sum_{i=0}^n a_i p^i \in \mathbb{Z}$$

Then we have

$$|x - x_n| = \Big|\sum_{i=n+1}^{\infty}\Big| = \max_{i \ge n+1}\{|p^i|\} = |p^{n+1}| = p^{-(n+1)} \xrightarrow{n \to \infty} 0$$

and hence \mathbb{Z} is dence in \mathbb{Z}_p .

(ii) Recall that the maximal ideal is given by

$$\mathfrak{m} = \{ x \in \mathbb{Z}_p \mid |x| < 1 \} \stackrel{!}{=} p\mathbb{Z}_p$$

'⊆' Let $x \in \mathfrak{m}$, i.e. |x| < 1. Thus we have $|x| < \left|\frac{1}{p}\right|$. This implies

$$|p^{-1}x| \leqslant 1 \iff p^{-1}x \in \mathbb{Z}_p.$$

and thus $p^{-1}x = y$ for some $y \in \mathbb{Z}_p$. Then we have $x = py \in p\mathbb{Z}_p$.

- '⊇' Let $x \in p\mathbb{Z}_p$, i.e. we can write x = py for some $y \in \mathbb{Z}_p$. Then |x| = |py| = |p||y| < 1and hence $x \in \mathfrak{m}$.
- (iii) Consider the surjective homomorphism

$$\psi_p : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad x = \sum_{i=0}^n a_i p^i \mapsto a_0$$

We have

$$\ker(\psi_p) = \{ x \in \mathbb{Z}_p \mid a_0 \equiv 0 \mod p \} = p\mathbb{Z}_p$$

thus we get $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{Z} / p\mathbb{Z}$ by homomorphism theorem.

(iv) The absolute value $|\cdot| = |\cdot|_p$ on \mathbb{Q}_p induces a discrete valuation ν on \mathbb{Q}_p^{\times} . With respect to this valuation we have

$$\mathcal{O}_{\nu} = \{ x \in \mathbb{Q}_p \mid \nu(x) \ge 0 \} \cup \{ 0 \} = \{ x \in \mathbb{Q}_p \mid |x| \le 1 \} = \mathbb{Z}_p$$

which finishes the proof.

Proposition 10.5 (i) Any $x \in \mathbb{Z}_p$ can uniquely be written in the form

$$x = \sum_{i=0}^{\infty} a_i p^i, \qquad a_i \in \{0, 1, \dots, p-1\}.$$

(ii) Any $x \in \mathbb{Q}_p$ can uniquely be written in the form

$$x = \sum_{i=-m}^{\infty} a_i p^i, \qquad m \in \mathbb{Z}, \ a_i \in \{0, 1, \dots, p-1\}, \ a_m \neq 0.$$

proof. (i) We first obtain, that any series

$$\sum_{i=0}^{\infty} a_i p^i, \qquad a_i \in \{0, \dots, p-1\}$$

converges, since for n > m we have

$$\left|\sum_{i=0}^{n} a_{i} p^{i} - \sum_{i=0}^{m} a_{i} p^{i}\right| = \left|\sum_{i=n+1}^{m} a_{i} p^{i}\right| = |p^{m+1}| \underbrace{\left|\sum_{i=n+1}^{m} a_{i} p^{i-(m+1)}\right|}_{\leqslant 1} \leqslant |p^{m+1}|$$

uniqueness Let

$$x = \sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} b_i p^i, \qquad a_i, b_i \in \{0, 1, \dots, p-1\}$$

representations of $x \in \mathbb{Q}_p$. Assume them to be different and define $i_o := \min\{i \in \mathbb{N}_0 \mid a_i \neq b_i\}$. Then

$$0 = \left| \sum_{i=0}^{\infty} a_i p^i - \sum_{i=0}^{\infty} b_i p^i \right| = \left| \underbrace{p^{i_0}(a_{i_0} - b_{i_0})}_{=:A} + p^{i_0 + 1} \cdot \underbrace{\left(\sum_{i=i_0+1}^{\infty} a_i p^{i-(i_0+1)} - \sum_{i=i_0+1}^{\infty} b_i p^{i-(i_0+1)} \right)}_{=:B} \right|.$$

We obtain $\nu_p(A) = p^{-i_0}$ and

$$B \in \mathbb{Z}_p, \quad \nu_p\left(p^{i_0+1} \cdot B\right) = \nu_p\left(p^{i_0+1}\right) \underbrace{\nu_p(B)}_{\leqslant 1} \leqslant \nu_p\left(p^{i_0+1}\right) = p^{-(i_0+1)},$$

so all in all

$$0 = |A + p^{i_0 + 1} \cdot B| \stackrel{9.8(ii)}{=} \max\{p^{-i_0}, p^{-(i_0 + 1)}\} = p^{-i_0} \notin.$$

existence Look at $\overline{x} \in \mathbb{Z}_p / p\mathbb{Z}_p = \mathbb{F}_p$.

Let a_0 be the representative of x in $\{0, 1, \ldots, p-1\}$. Then we have

$$|x-a_0| < 1 \iff |x-a_0| \leqslant \frac{1}{p}.$$

In the next step, let a_1 be the representative of $\frac{1}{p}(x-a_0)$ in $\{0, 1, \ldots, p-1\}$. Then

$$\left|\frac{1}{p}(x-a_0)-a_1\right| = \left|\frac{1}{p}\right||x-a_0-a_1p| \le \frac{1}{p}$$

and thus $|x - a_0 - a_1 p| \leq \frac{1}{p^2}$. Inductively we let a_n be the representative of

$$\frac{1}{p^n}(x-a_0-a_1p-\ldots-a_{n-1}p^{n-1}) = \frac{1}{p^n}\left(x-\sum_{i=0}^{n-1}a_ip^i\right)$$

in $\{0, 1, ..., p - 1\}$. Then we have

$$\left|x - \sum_{i=0}^{n-1} a_i p^i\right| \leq \frac{1}{p^{n+1}}.$$

and finally

$$\lim_{n \to \infty} \left| x - \sum_{i=0}^{n-1} a_i p^i \right| \le \lim_{n \to \infty} \frac{1}{p^{n+1}} = 0 \implies x = \sum_{i=0}^{\infty} a_i p^i.$$

(ii) If $|x| = p^m$ for some $m \in \mathbb{Z}$, we have

$$|x \cdot p^m| = |d| \cdot |p^m| = p^m \cdot p^{-m} = 1,$$
 i.e. $x \cdot p^m \in \mathbb{Z}_p^{\times}$

By part (i) we conclude

$$x \cdot p^m = \sum_{i=0}^{\infty} a_i p^i, \quad a_0 \neq 0$$

Thus we have

$$x = \frac{1}{p^m} \cdot x \cdot p^m = \frac{1}{p^m} \cdot \sum_{i=0}^{\infty} a_i p^i = \sum_{i=-m}^{\infty} a_{i+m} p^i,$$

which was the assertion.

Remark 10.6 What is -1 in \mathbb{Q}_p ? We have $a_0 = p - 1$, since $\overline{p-1} - \overline{(-a)} = \overline{p} = 0$. a_1 is the representative of $\frac{1}{p}(-1 - (p-1)) = -1$, i.e. $a_1 = p - 1$. a_2 is the representative of $\frac{1}{p^2}(-1 - (p-1) - (p-1)p) = -1$, i.e. $a_2 = p - 1$. Inductively we have $a_n = p - 1$ for all $n \in \mathbb{N}_0$, so we get

$$-1 = \sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{\infty} (p-1)p^i$$

Moreover we obtain

$$\sum_{i=0}^{\infty} (p-1)p^{i} = (p-1)\sum_{i=0}^{\infty} p^{i} = (p-1) \cdot \frac{1}{1-p} = \frac{p-1}{1-p} = -1.$$

Remark 10.7 Let

$$x = \sum_{i=0}^{\infty} a_i p^i, \qquad y = \sum_{i=0}^{\infty} b_i p^i$$

p-adic integers. Then

$$x + y = \sum_{i=0}^{\infty} c_i p^i$$

with coefficients

$$c_0 = \begin{cases} a_0 + b_0 & \text{if } a_0 + b_0$$

$$c_{1} = \begin{cases} a_{1} + b_{1} & \text{if } a_{0} + b_{0}$$

Inductively let

$$\epsilon_0 := 0, \qquad \epsilon_i := \begin{cases} 0 & \text{if } a_i + b_i + \epsilon_{i-1}$$

Then we have

$$c_i = \begin{cases} a_i + b_i + \epsilon_i & \text{if } a_i + b_i + \epsilon_i$$

Remark 10.8 (i) $\sqrt{p} \notin \mathbb{Q}_p$, since $|\sqrt{p}| = \sqrt{|p|} = \sqrt{\frac{1}{p}} \in (\frac{1}{p}, 1)$, which is not possible. (ii) Let $a \in \mathbb{Z}_p^{\times}$ with image $\overline{a} \in \mathbb{F}_p^{\times} \setminus \mathbb{F}_p^{\times^2}$, where

$$\mathbb{F}_p^{\times^2} = \{ x \in \mathbb{F}_p \mid \text{ there exists } y \in \mathbb{F}_p : y^2 = x \}$$

denotes the set of squares. Then $\sqrt{a} \notin \mathbb{Q}_p$. Assume a is a aquare, i.e. $b^2 = a$. Then

$$|b| = \sqrt{|a|} = 1 \quad \Rightarrow \quad b \in \mathbb{Z}_p^{\times}$$

But then $\overline{b} \in \mathbb{F}_p$ satisfies $\overline{b}^2 \equiv a$, which is a contradiction, since $a \notin \mathbb{F}_p^{\times^2}$.

- (iii) Let now $\overline{\mathbb{Q}}_p$ be the algebraic closure of \mathbb{Q}_p with valuation ring $\overline{\mathbb{Z}}_p$ and maximal ideal $\overline{\mathfrak{m}}_p$. Then $\overline{\mathbb{Z}}_p/\overline{\mathfrak{m}}$ is algebraically closed. Moreover \mathbb{Q}_p is complete with respect to $|\cdot|_p$. The completion \mathbb{C}_p of $\overline{\mathbb{Q}}_p$ is complete and algebraically closed, but:
 - (1) $|\cdot|_p$ is not a discrete valuation.
 - (2) $\overline{\mathbb{Z}}_p$ is not a discrete valuation ring.
 - (3) $\overline{\mathfrak{m}}_p$ is not a principal ideal.

Theorem 10.9 (Hensel's Lemma) Let

$$f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}_p[X], \qquad \overline{f} = \sum_{i=0}^{n} \overline{a_i} X^i \in \mathbb{F}[X]$$

where \overline{f} is the reduction of f in $\mathbb{F}[X]$. Suppose that $\overline{f} = f_1 \cdot f_2$ with $f_1, f_2 \in \mathbb{F}_p[X]$ relatively prime. Then there exist $g, h \in \mathbb{Z}_p[X]$, such that

$$f = g \cdot h$$
, $\overline{g} = f_1, h = f_2$, $\deg(f_1) = \deg(g)$

proof. Let $d := \deg(f), m := \deg(f_1)$. Then $\deg(f_2) \leq d - m$. Choose $g_0, h_0 \in \mathbb{Z}_p[X]$ such that $\overline{g_0} = f_1, \overline{h_0} = f_2, \deg(g_0) = m, \deg(h_0) = d - m$. Strategy: Find $g_1 = g_0 + pc_1, h_1 = h_0 + pd_1$ with some $c_1, d_1 \in \mathbb{Z}_p[X]$, such that

$$f - g_1 h_1 \in p^2 \mathbb{Z}_p[X].$$

Therefore we have a

Claim (a) For $n \ge 1$ there exists $c_n, d_n \in \mathbb{Z}_p[X]$ with $\deg(c_n) \le m, \deg(d_n) \le d - m$ and

$$f - g_n h_n \in p^{n+1} \mathbb{Z}_p[X],$$
 where $g_n = g_{n-1} + p^n c_n, \quad h_n = h_{n-1} + p^n d_n$

Assuming (a), write

$$g_n = \sum_{i=0}^m g_{n,i} X^i, \qquad h_n = \sum_{i=0}^{d-m} h_{n,i} X^i.$$

By construction, the $(g_{n,i})$ converge to some $\alpha_i \in \mathbb{Z}_p$ and the $(h_{n,i})$ converge to some $\beta_i \in \mathbb{Z}_p$. Let

$$g := \sum_{i=0}^{m} \alpha_i X^i, \qquad h := \sum_{i=0}^{d-m} \beta_i X^i.$$

Observe, that $\deg(g) = m$, $\deg(h) = d - m$. Obviously we have

$$f = g \cdot h.$$

It remains to show the claim.

(a) c_n, d_n have to satisfy

$$f - g_n h_n = f - (g_{n-1} + p^n c_n) \cdot (h_{n-1} + p^n d_n)$$

= $f - g_{n-1} h_{n-1} - p^n \cdot (g_{n-1} d_n + h_{n-1} c_n + p^n c_n d_n)$
 $\stackrel{!}{\in} p^{n+1} \mathbb{Z}_p[X]$

where $f - g_{n-1}h_{n-1} \in p^n \mathbb{Z}_p[X]$ by hypothesis. We get

$$\tilde{f}_n := \frac{1}{p^n} (f - g_{n-1}h_{n-1}) \equiv c_n h_{n-1} + d_n g_{n-1} \mod p \ (*)$$

Since f_1, f_2 are relatively prime and $g_j \equiv g_k \mod p$ for any j, k, we find integers $a, b \in \mathbb{Z}$, such that

$$af_1, bf_2 = 1 \implies ag_{n-1} + bh_{n-1} \equiv 1 \mod p.$$

Multiplying the equation by \tilde{f}_n gives us

$$\tilde{f}_n \equiv \underbrace{a\tilde{f}_n}_{=:\tilde{d}_n} g_{n-1} + \underbrace{b\tilde{f}_n}_{=:\tilde{c}_n} h_{n-1} \mod p \; (**).$$

Further $\mathbb{Z}_p[X]$ is euclidean, thus we can choose $q_n, r_n \in \mathbb{Z}_p[X]$, deg $(r_n) < m$ such that

$$bf_n = q_n g_{n-1} + r_n.$$

By (**) we have

$$g_{n-1}\left(a\tilde{f}_n + q_nh_{n-1}\right) + r_n \equiv \tilde{f}_n \mod p_n$$

Let now $c_n = r_n, d_n = a\tilde{f}_n + q_n h_{n-1}$. All the terms are divisible by p. Then

$$d_n \equiv a\tilde{f}_n + q_n h_{n-1} \mod p.$$

Thus (*) holds and we have

$$\deg(d_n) = \deg(\overline{d_n}) \leqslant \deg\left(\underbrace{\overbrace{\tilde{f}_n}^{\leqslant d}}_{\leqslant d} - \underbrace{\overline{c_n}}_{\leqslant d} \underbrace{\overline{\tilde{h}_{n-1}}}_{=m}\right) - \underbrace{\deg(\overline{g}_{n-1})}_{=m} \leqslant d - m$$

since $\overline{d}_n \overline{g}_{n-1} = \overline{\tilde{f}}_n - \overline{c}_n \overline{h}_{n-1}$. Thus, the claim is proved.

Corollary 10.10 Let $p \in \mathbb{P}$ odd. Then $a \in \mathbb{Z}_p^{\times}$ is a square if and only if $\overline{a} \in \mathbb{F}_p^{\times}$ is a square.

Proposition 10.11 $a \in \mathbb{Q}$ is a square if and only if a > 0 and a is a square in \mathbb{Q}_p for all $p \in \mathbb{P}$. Remark: This is a special case of the 'Hasse-Minkowski-Theorem'.

Kapitel III

Rings and modules

§ 11 Multilinear Algebra

In this section, R will always be a commutative, unitary ring.

Reminder 11.1 (i) An *R*-module is an abelian group (M, +) together with a scalar multiplication

$$\cdot: R \times M \longrightarrow M$$

with the usual properties of a vector space, i.e. for any $m, n \in M, r, s \in R$ we have

- (1) $r \cdot (s \cdot m) = (rs) \cdot m$
- (2) $(r+s) \cdot m = r \cdot m + s \cdot m$
- (3) $r \cdot (m+n) = r \cdot m + r \cdot n$

(4)
$$1_R \cdot m = m$$

(ii) A map $\phi: M \longrightarrow M'$ of *R*-modules M, M' is called *R*-linear or *R*-module homomorphism, if

$$\phi(r \cdot m + s \cdot n) = r \cdot \phi(m) + s \cdot \phi(n) \qquad \text{for all } r, s \in R, m, n \in M.$$

- (iii) A subset $S \subseteq M$ of an R-module is called an *R*-submodule of M, if S is an *R*-module.
- (iv) R itself is an R-module, the submodules are the ideals of R.
- (v) If $\phi: M \longrightarrow M'$ is *R*-linear, then

$$\ker(\phi) = \{ m \in M \mid \phi(m) = 0 \},\$$

$$\operatorname{im}(\phi) = \{m' \in M' \mid \phi(m) = m' \text{ for some } m \in M\}$$

are R-submodules.

(vi) If $M \subseteq M'$ is a submodule, then the factor group M/M' is an *R*-module via

$$a \cdot \overline{m} = \overline{a \cdot m}.$$

(vii) For an *R*-linear map $\phi: M \longrightarrow M''$, we have

$$\operatorname{im}(\phi) \cong M / \operatorname{ker}(\phi).$$

(viii) An *R*-module *M* is called *free*, if there exists a subset $X \subseteq M$, such that every $m \in M$ has a unique representation

$$m = \sum_{x \in X} a_x \cdot x, \qquad a_x \in R, \ a_x \neq 0 \text{ only for finitely many } x \in X.$$

In this case, X is called the rank of M.

(ix) Not every *R*-module is free: Indeed let $0 \leq I \leq R$ be a proper ideal. Then R/I is not free: Let $X \subseteq R$, such that $\overline{X} \subseteq R/I$ generates the *R*-module R/I. Let $x \in X$ and $a \in I \setminus \{0\}$. Then we have

$$x \cdot \overline{x} = \overline{a \cdot x} = 0 = 0 \cdot x = 0 \cdot \overline{x},$$

hence we have found two different reapersentations of 0. Thus R/I is not free.

- (x) For any $n \in \mathbb{N}$, $n\mathbb{Z}$ is a free module
- (xi) If $I \leq R$ is not a principle ideal, then I is not a free R-module., since for $x, y \in I$ with $y \notin (x)$ we have xy yx = 0. Again we have a nontrivial representation of 0 and I is not free.

Definition + **proposition 11.2** Let R be a ring, M, M' R-modules.

(i) The set of *R*-module homomorphisms

$$\operatorname{Hom}_R(M, M') = \{\phi : M \longrightarrow M' \mid \phi \text{ is } R\text{-linear } \}$$

is again an R-module.

(ii) $M^* = \operatorname{Hom}_R(M, R)$ is called the *dual module* of M.

Let now

$$0 \longrightarrow M' \stackrel{\alpha}{\longrightarrow} M \stackrel{\beta}{\longrightarrow} M'' \longrightarrow 0$$

be a short exact sequence of R-modules M, M', M'', i.e. α is injective and β is surjective.

(iii) Then we have a short exact sequence

$$0 \longrightarrow \operatorname{Hom}_{R}(N, M') \xrightarrow{\alpha_{*}} \operatorname{Hom}_{R}(N, M) \xrightarrow{\beta_{*}} \operatorname{Hom}_{R}(N, M'')$$

$$\phi \longmapsto \alpha \circ \phi, \ \psi \longmapsto \beta \circ \psi$$

(iv) We have s short exact sequence

$$0 \longrightarrow \operatorname{Hom}_{R}(M'', N) \xrightarrow{\beta^{*}} \operatorname{Hom}_{R}(M, N) \xrightarrow{\alpha^{*}} \operatorname{Hom}_{R}(M', N)$$

$$\phi \mapsto \phi \circ \beta, \quad \psi \mapsto \psi \circ \alpha$$

(v) N is called a *projective* module, if β_* is surjective for all short exact sequences as in (iii).

(vi) N is called an *injective* module, if α^* is surjective for all short exact sequences an in (iv).

proof. (i) This is clear: For all $\phi, \phi_1, \phi_2 \in \operatorname{Hom}_R(M, M')$ and $a \in R$ we have

$$(\phi_1 + \phi_2)(x) = \phi_1(x) + \phi_2(x), \qquad (a \cdot \phi)(x) = a \cdot \phi(x)$$

(iii) α_* is *R*-linear: For any $\phi_1, \phi_2 \in \operatorname{Hom}_R(N, M')$ and $x \in N$ we have

$$\alpha_*(\phi_1 + \phi_2)(x) = (\alpha \circ (\phi_1 + \phi_2))(x) = \alpha (\phi_1(x) + \phi_2(x)) = \alpha (\phi_1(x)) + \alpha (\phi_2(x))$$

and thus

$$\alpha_*(\phi_1 + \phi_2)(x) = \alpha_*(\phi_1)(x) + \alpha_*(\phi_2)(x) = (\alpha_*(\phi_1) + \alpha_*(\phi_2))(x)$$

Moreover, α_* is injective: Since α is injective we have $\alpha_*(\phi)(x) = \alpha(\phi(x)) = 0$ if and only if $\phi(x) = 0$ for all $x \in N$, thus $\phi = 0$. Now we still have to show ker $(\beta_*) = \operatorname{im}(\alpha_*)$.

- ' \supseteq ' For $\phi \in \operatorname{Hom}_R(N, M')$ we have $\beta_*(\alpha \circ \phi) = \beta \circ \alpha \circ \phi = 0 \circ \phi = 0$, i.e. $\alpha \circ \phi = \alpha_*(\phi) \in \ker(\beta_*)$.
- ' \subseteq ' Let $\phi : N \longrightarrow M$, $\phi \in \ker(\beta_*)$, i.e. $\beta \circ \phi = 0$. We have to show, that there exists $\phi' \in \operatorname{Hom}_R(N, M')$ such that $\phi = \alpha_*(\phi') = \alpha \circ \phi'$. Let $x \in N$. Then $\phi(x) \in \ker(\beta) = \operatorname{im}(\alpha)$. Then there exists $z \in M'$ such that $\phi(x) = \alpha(z)$ and z is unique, since α is injective. Define $\phi'(x) := z$. Then we have $\alpha \circ \phi' = \phi$. It remains to show that ϕ' is *R*-linear. We have $\phi'(x_1 + x_2) = z$ and with $\alpha(z) = \phi(x_1 + x_2) = \phi(x_1) + \phi(x_2)$ we again have $\alpha(z) = \phi(z_1) + \phi(z_2)$ for some suitable, but unique $z_1, z_2 \in M'$. Since we have

$$\alpha(z) = \phi(x_1 + x_2) = \phi(x_1) + \phi(x_2) = \alpha(z_1) + \alpha(z_2) = \alpha(z_1 + z_2)$$

and α is injective, we have $z = z_1 + z_2$, thus

$$\phi'(x_1 + x_2) = z = z_1 + z_2 = \phi'(x_1) + \phi'(x_2).$$

Moreover for $a \in R$ we have $\phi'(ax) = w$ with $\alpha(w) = \phi(ax) = a \cdot \phi(x) = a \cdot \alpha(z)$. Thus $\alpha(\phi'(ax)) = \alpha(w) = \phi(ax) = a \cdot \phi(x) = a \cdot \alpha(z) = a \cdot \alpha(\phi'(x)) \xrightarrow{\alpha \text{ inj.}} \phi'(ax) = a \cdot \phi'(x),$ which proves the claim.

Remark 11.3 (i) An R-module N is projective if and only if for every surjective R-linear map $\beta : M \longrightarrow M''$ and every R-linear map $\phi : N \longrightarrow M''$ there is an R-linear map $\tilde{\phi}: N \longrightarrow M$, such that the diagram below commutes, i.e. $\phi = \beta \circ \tilde{\phi}$.



(ii) Free modules are projective.

Definition 11.4 Let M, M_1, M_2 be *R*-modules. A map

$$\Phi: M_1 \times M_2 \longrightarrow M$$

is called *bilinear*, if the maps

$$\Phi_{x_0}: M_2 \longrightarrow M, \quad y \mapsto \Phi(x_0, y), \qquad \Phi_{y_0}: M_1 \longrightarrow M, \quad x \mapsto \Phi(x, y_0)$$

are linear for all $x_0 \in M_1$ and $y_0 \in M_2$.

Definition 11.5 Let M_1, M_2 be *R*-modules. A *tensor prodect* of M_1 and M_2 is an *R*-module *T* together with a bilinear map

$$\tau: M_1 \times M_2 \longrightarrow T,$$

such that for every bilinear map $\Phi: M_1 \times M_2 \longrightarrow M$ for any *R*-module *M* there is a unique linear map $\phi: T \longrightarrow M$, such that the following diagram becomes commutative.



Remark 11.6 Let (T, τ) and (T', τ') be tensor products of *R*-modules M_1 and M_2 . Then there exists a unique isomorphism $h: T \longrightarrow T'$, such that

$$\tau' = h \circ \tau.$$

proof. Consider



Existence and uniqueness of the linear maps g and h come from Definition 11.5. It remains to show, that $h \circ g = \operatorname{id}_{T'}$ and $g \circ h = \operatorname{id}_T$.

In order to do this, consider the following diagramm.



We have $(g \circ h)\tau = g \circ (h \circ \tau) = g \circ \tau' = \tau$. By the uniqueness we get $\mathrm{id}_T = g \circ h$. Analogously we get $\mathrm{id}_{T'} = h \circ g$ which finishes the proof.

Corollary 11.7 The tensor product (T, τ) of *R*-modules M_1 , M_2 is unique up to isomorphism. The standard notation is

$$T = M_1 \otimes_R M_2, \qquad \tau(x, y) = x \otimes y$$

Example 11.8 Let M_1, M_2 be free *R*-modules with bases $\{e_i\}_{i \in I}, \{f_j\}_{j \in J}$. Let *T* be the free *R*-module with basis $\{g_{ij}\}_{(i,j)\in I\times J}$ and

$$\tau: M_1 \times M_2 \longrightarrow T, \ (e_i, f_j) \mapsto g_{ij} \quad \text{for all } (i, j) \in I \times J,$$

i.e. for elements in M_1, M_2 we have

$$\tau\left(\sum_{i\in I}a_ie_i,\ \sum_{j\in J}b_jf_j\right) = \sum_{(i,j)\in I\times J}a_ib_jg_{ij}$$

Then (T, τ) is the tensor product of M_1, M_2 , since: Let $\Phi: M_1 \times M_2 \longrightarrow M$ be bilinear. Define

$$\phi: T \longrightarrow M, \ g_{ij} \mapsto \Phi(e_i, f_j).$$

Obviously ϕ is linear and satisfies $\Phi = \phi \circ \tau$. Now consider a special case and let |I| = n, |J| = m. Identify M_1 via $(e_1, \ldots e_n)$ with \mathbb{R}^n and M_2 via $(f_1, \ldots f_m)$ with \mathbb{R}^m . Then T is identified with $\mathbb{R}^{n \times m}$ via

$$g_{ij} = E_{ij} = \begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ \vdots & & 1 & & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}$$

where the only nonzero entry is in the *i*-th row and *j*-th column. Then $\tau : \mathbb{R}^n \times \mathbb{R}^m \longrightarrow \mathbb{R}^{n \times m}$ is given by

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} a_1 b_1 & \dots & a_1 b_m \\ \vdots & & \vdots \\ a_n b_1 & \dots & a_n b_m \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 & \dots & b_m \end{pmatrix},$$

where the last multiplication is the usual multiplication of matricees.

Theorem 11.9 For any two *R*-modules M_1, M_2 there exists a tensor product $(T, \tau) = (M_1 \otimes_R M_2, \otimes)$.

proof. Let F be the free R-module with basis $M_1 \times M_2$ and Q be the submodule generated by all the elements

$$(x + x', y) - (x, y) - (x', y), \quad (x, y + y') - (x, y) - (x, y'), \quad (ax, y) - a(x, y), \quad (x, ay) - a(x, y)$$

for $a \in R, x, x' \in M_1, y, y' \in M_2$. Define

$$T := F/Q, \qquad \tau : M_1 \times M_2 \longrightarrow T, \ (x, y) \mapsto \overline{(x, y)}.$$

Then by the construction of Q, τ is bilinear. Let now be M a further R-module and $\Phi: M_1 \times M_2 \longrightarrow M$ a bilinear map. Define

$$\phi: F \longrightarrow M, \quad (x, y) \mapsto \Phi(x, y).$$

Clearly $\tilde{\phi}$ is linear. Moreover we have $Q \subseteq \ker(\phi)$, since Φ is bilinear. By the isomorphism theorem, $\tilde{\phi}$ factors to a linear map $\phi: T \longrightarrow M$ satisfying $\phi\left(\overline{(x,y)}\right) = \Phi(x,y)$. The uniqueness of ϕ follows by the fact that T is generated by the $\overline{(x,y)}$ for $x \in M_1, y \in M_2$.

Example 11.10 We want to find out what is

$$\mathbb{Z}/2\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/3\mathbb{Z}.$$

Let $\Phi: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \longrightarrow A$ bilinear for some \mathbb{Z} -module A. Then we see

$$\Phi(\overline{1},\overline{1}) = \Phi(\overline{3},\overline{1}) = \Phi\left(3\cdot(\overline{1},\overline{1})\right) = 3\cdot\Phi(\overline{1},\overline{1}) = \Phi(\overline{1},\overline{3}) = \Phi(\overline{1},\overline{0}) = 0\cdot\Phi(\overline{1},\overline{1}) = 0$$

Hence $\Phi = 0$, since $(\overline{1}, \overline{1})$ generates $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Thus $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$.

Proposition 11.11 For *R*-modules M, M_1, M_2, M_3 we have the following properties.

- (i) $M \otimes_R R \cong M$.
- (*ii*) $M_1 \otimes_R M_2 \cong M_2 \otimes_R M_1$.
- (*iii*) $(M_1 \otimes_R M_2) \otimes_R M_3 \cong M_1 \otimes_R (M_2 \otimes_R M_2).$
- proof. (i) Let $\tau : M \times R \longrightarrow M$, $(x, a) \mapsto a \cdot x$. Then τ is bilinear. We now can verify the universal property of the tensor product. Let N be an arbitrary R-module and $\Phi : M \times R \longrightarrow N$ be bilinear a bilinear map. Define

$$\phi: M \longrightarrow N, \quad x \mapsto \Phi(x, 1)$$

Then ϕ is *R*-linear: For $x, y \in M, \alpha \in R$ we have

$$\phi(\alpha \cdot x) = \Phi(\alpha \cdot x, 1) = \alpha \cdot \Phi(x, 1) = \alpha \cdot \phi(x),$$

$$\phi(x+y) = \Phi(x+y, 1) = \Phi(x, 1) + \Phi(y, 1) = \phi(x) + \phi(y)$$

and thus

$$\phi(\tau(x,a)) = \phi(a \cdot x) = a \cdot \Phi(x,1) = \Phi(x,a)$$

(ii) The isomorphism

$$M_1 \times M_2 \xrightarrow{\cong} M_2 \times M_1, \quad (x, y) \mapsto (y, x)$$

induces an isomorphism $M_1 \otimes_R M_2 \cong M_2 \otimes_R M_1$.

(iii) For fixed $z \in M_3$ define

$$\Phi_z: M_1 \times M_2 \longrightarrow M_1 \otimes_R (M_2 \otimes_R M_3), \quad (x, y) \mapsto x \otimes (y \otimes z) = \tau_{1(23)} (\tau_{23}(x, y)).$$

Then Φ_z is bilinear and induces a linear map

$$\phi_z: M_1 \otimes_R M_2 \longrightarrow M_1 \otimes_R (M_2 \otimes_R M_3)$$

Define

$$\Psi: (M_1 \otimes_R M_2) \times M_3 \longrightarrow M_1 \otimes_R (M_2 \otimes_R M_3), \quad (x \otimes y, z) \mapsto \phi_z(x \otimes y).$$

 Ψ is bilinear and induces a linear map

$$\psi: (M_1 \otimes_R M_2) \otimes_R M_3 \longrightarrow M_1 \otimes_R (M_2 \otimes_R M_3)$$

Doing this again the other way round we find a linear map

$$\tilde{\psi}: M_1 \otimes_R (M_2 \otimes_R M_3) \longrightarrow (M_1 \otimes_R M_2) \otimes_R M_3$$

By the uniqueness we obtain as in Remark 11.6 that $\psi \circ \tilde{\psi} = \tilde{\psi} \circ \psi = id$, hence the claim follows.

Definition + remark 11.12 Let M, M_1, \ldots, M_n be *R*-modules.

(i) A map

$$\Phi: M_1 \times \ldots \times M_n = \prod_{i=1}^n M_i \longrightarrow M$$

is called *multilinear*, if for any $1 \leq i \leq n$ and all choices of $x_j \in M_j$ for $j \neq i$ the map

$$\Phi_i: M_i \longrightarrow M, \quad x \mapsto \Phi(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n)$$

is linear.

(ii) The map

$$\tau_{M_1,\dots,M_n}:\prod_{i=1}^n M_i\longrightarrow \bigotimes_{i=1}^n M_i, \qquad (x_1,\dots,x_n)\mapsto x_1\otimes\dots\otimes x_n$$

is multilinear.

(iii) For every multilinear map

$$\Phi:\prod_{i=1}^n M_i \longrightarrow M$$

there exists a unique linear map

$$\phi:\bigotimes_{i=1}^n M_i \longrightarrow M$$

such that $\Phi = \phi \circ \tau_{M_1,\dots,M_n}$.

Definition 11.13 Let M, N be R-modules, $\Phi : M^n = \prod_{i=1}^n M \longrightarrow N$ a multilinear map.

(i) Φ is called *symmetric*, if for any $\sigma \in S_n$ we have

$$\Phi(x_1,\ldots x_n) = \Phi(x_{\sigma(1)},\ldots x_{\sigma(n)}).$$

(ii) Φ is called *alternating*, if

$$x_i = x_j$$
 for some $i \neq j \implies \Phi(x_1, \dots, x_n) = 0.$

If $char(R) \neq 2$, this is equivalent to

$$\Phi(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n) = -\Phi(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n).$$

Proposition 11.14 Let M be an R-module, $n \ge 1$.

(i) There exists an R-module $S^n(M)$, called the n-th symmetric power of M and a symmetric multilinear map

$$\sigma_M^n: M^n \longrightarrow S^n(M)$$

such that for all symmetric, multilinear maps $\Phi : M^n \longrightarrow N$ for any *R*-module *N* there exists a unique linear map $\phi : S^n(M) \longrightarrow N$ satisfying $\Phi = \phi \circ \sigma_M^n$.

(ii) There exists an R-module $\Lambda^n(M)$, called the n-th exterior power of M and an alternating multilinear map

$$\lambda_M^n: M^n \longrightarrow \Lambda^n(M)$$

such that for all alternating, multilinear maps $\Phi : \Lambda^n(M) \longrightarrow N$ for any *R*-module *N* there exists a unique linear map $\phi : \Lambda^n(M) \longrightarrow N$ satisfying $\Phi = \phi \circ \lambda_M^n$.

proof. (i) Let $T^n(M) = M \otimes_R \ldots \otimes_R M$.

Let now $J_n(M)$ be the submodule of $T^n(M)$ generated by all elements

$$(x_1 \otimes \ldots \otimes x_n) - (x_{\sigma(1)} \otimes \ldots \otimes x_{\sigma(n)}), \quad x_i \in M, \sigma \in S_n$$

Define

$$S^n(M) := T^n(M) / J_n(M), \qquad \sigma^n_M := \operatorname{proj} \circ \tau_{\mathrm{M},\dots\mathrm{M}}$$

Then σ_M^n is multilinear and symmetric by construction. Given a multilinear and symmetric map $\Phi: M^n \longrightarrow N$, define ϕ as follows: Let $\tilde{\phi}: T^n(M) \longrightarrow N$ be the linear map induced by Φ and observe that $J_n(M) \subseteq \ker(\tilde{\phi})$. Hence $\tilde{\phi}$ factors to a linear map

$$\phi: S^n(M) = S^n(M) / J_n(M) \longrightarrow N$$

satisfying $\phi \circ \sigma_M^n = \Phi$.

(ii) Similarly let $I_n(M)$ be the submodule of $T^n(M)$ generated by all the elements

$$x_1 \otimes \ldots \otimes x_n, \qquad x_i \in M \text{ with } x_i = x_j \text{ for some } i \neq j$$

Analogously we define

$$\Lambda^{n}(M) := T^{n}(M) / I_{n}(M), \qquad \lambda^{n}_{M} := \operatorname{proj} \circ \tau_{\mathrm{M}, \dots, \mathrm{M}}$$

and obtain the required properties.

Proposition 11.15 Let M be a free R-module of rank r and $\{e_1, \ldots, e_r\}$ a basis of M. Then $\Lambda^n(M)$ is a free R-module with basis

$$proj(e_{i_1} \otimes \ldots \otimes e_{i_n}) =: e_{i_1} \wedge \ldots \wedge e_{i_n}, \qquad 1 \leqslant i_1 < \ldots < i_n \leqslant r$$

In particular, $\Lambda^n(M) = 0$ for n > r and rank $(\Lambda^r(M)) = 1$.

proof. By definition we have $e_{i_1} \wedge \ldots \wedge e_{i_n} = 0$ if $i_k = i_j$ for some $k \neq j$, hence we have $\Lambda^n(M) = 0$ for n > r, as at least on of the e_k must appear twice.

generating: Clearly the $e_{i_1} \wedge \ldots \wedge e_{i_n}, i_k \in \{1, \ldots, r\}$ generate $\Lambda^n(M)$. We have to show that we can leave out some of them. Obviously $e_{i_{\sigma(1)}} \wedge \ldots \wedge e_{i_{\sigma(n)}}$ is a multiple by ± 1 of $e_{i_1} \wedge \ldots \wedge e_{i_n}$. Thus the $e_{i_1} \wedge \ldots \wedge e_{i_n}$ with $1 \leq i_1 < i_2 < \ldots < i_n \leq r$ generate $\Lambda^n(M)$. linear independence: Assume

$$\sum_{1 \leq i_1 < \dots < i_n \leq r} a_{i_1,\dots,i_n} e_{i_1} \wedge \dots \wedge e_{i_n} = 0. \qquad (*)$$

For fixed $j := (j_1, \ldots, j_n), 1 \leq j_1 < \ldots < j_n \leq r$ choose $\sigma_j \in S_r$, such that $\sigma_j(k) = j_k$ for

 $1 \leq k \leq n$. Then we obtain

$$e_{i_1} \wedge \ldots \wedge e_{i_n} \wedge e_{\sigma_j(n+1)} \wedge \ldots \wedge e_{\sigma_j(r)} = \begin{cases} \pm e_1 \wedge \ldots \wedge e_r, & \text{if } i_k = j_k \text{ for all } k \\ 0 & \text{otherwise} \end{cases}$$

By (*) we get

$$0 = \left(\sum_{1 \leq i_1 < \dots < i_n \leq r} a_{i_1, \dots, i_n} e_{i_1} \land \dots \land e_{i_n}\right) \land e_{\sigma_j(n+1)} \land \dots \land e_{\sigma_j(r)} = a_j e_{j_1} \land \dots \land e_{j_r}$$

and thus $a_j = 0$.

Example 11.16 Let $M = R^n$. Then $\Lambda^k(M)$ is the free *R*-module with basis

$$e_{i_1} \wedge \ldots \wedge e_{i_k}, \quad 1 \leq i_1 < \ldots < i_k \leq n$$

and we have $e_1 \wedge e_2 = -e_2 \wedge e_1$. What is $\Lambda^n(\mathbb{R}^n) = \Lambda^n(M)$? And what is λ_k^M ? First we obtain $\Lambda^n(\mathbb{R}^n) = (e_1 \wedge \ldots \wedge e_n)\mathbb{R} \cong \mathbb{R}$. Then

$$M^{n} = (R^{n})^{n} = R^{n \times n}, \quad (a_{1}, \dots a_{n}) = A \in R^{n \times n}, \quad a_{i} = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} = \sum_{j=1}^{n} a_{ji}e_{j} \in R^{n} = M.$$

For λ_n^M we get

$$\lambda_n^M = \lambda_n^{R^n} = \lambda_n(A) = \lambda_n \left(\sum_{j=1}^n a_{j1} e_j, \dots, \sum_{j=1}^n a_{jn} e_j \right)$$

$$= \sum_{j=1}^n a_{j1} e_j \wedge \dots \wedge \sum_{j=1}^n a_{jn} e_j$$

$$= \sum_{j=1}^n a_{j1} \left(e_1 \wedge \sum_{j=1}^n a_{j2} e_j \wedge \dots \wedge \sum_{j=1}^n a_{jn} e_j \right)$$

$$= \sum_{j=1}^n a_{j1} \cdots \sum_{j=1}^n a_{jn} (e_1 \wedge \dots \wedge e_n)$$

$$= \sum_{\sigma \in S_n} a_{\sigma(1)1} \cdots a_{\sigma(n)n} \cdot e_1 \wedge \dots \wedge e_n \cdot \operatorname{sgn}(\sigma)$$

$$= \det(A) \cdot e_1 \wedge \dots \wedge e_n,$$

which is well-known tu us.

Definition 11.17 Let M be a R-module. Then we define

$$T(M) := \bigoplus_{n=0}^{\infty} T^n(M), \qquad T^0(M) := R, \ T(M) := M$$
$$S(M) := \bigoplus_{n=0}^{\infty} S^n(M). \qquad S^0(M) := R, \ S(M) := M$$
$$\Lambda(M) := \bigoplus_{n=0}^{\infty} \Lambda^n(M), \qquad \Lambda^0(M) := R, \ \Lambda(M) := M$$

On T(M) define a multiplication

Similarly do it for S(M) and $\Lambda(M)$. Then we have R-algebra-structures and feel free to define

- (i) the tensor algebra T(M),
- (ii) the symmetric algebra S(M)
- (iii) the exterior algebra $\Lambda(M)$.

Definition 11.18 Let R be an arbitrary ring.

- (i) An *R*-algebra is a ring R' together with a ring homomorphism $\alpha : R \longrightarrow R'$. In particular R' is an *R*-module. If α is injective, R'/R is called a ring extension.
- (ii) A homomorphism of *R*-algebras R', R'' is an *R*-linear map $\phi : R' \longrightarrow R''$, which is a ring homomorphism.

Example 11.19 (i) $R[X_1, \ldots, X_N]$ is an *R*-algebra for every $n \in \mathbb{N}$.

(ii) If R' is an R-algebra and $I \leq R'$ an ideal, then R'/I is an R-algebra.

Remark 11.20 Let R' be an R-algebra, F a free R-module. Then $F' := F \otimes_R R'$ is a free R'-module.

proof. Let $\{e_i\}_{i\in I}$ be basis of F. Let us show, that $\{e_1 \otimes 1\}_{i\in I}$ is basis of F' as an R-module, where F' is an R' module by

$$b \cdot (x \otimes a) := x \otimes b \cdot a, \qquad a, b \in R, \ x \in F$$

Check the universal property of the free R'-module with basis $\{e_i \otimes 1\}_{i \in I}$ for $F \otimes_R R'$. Let M' be an R-module and $f : \{e_i \otimes 1\}_{i \in I} \longrightarrow M'$ be a map. We have to show: There exists an R'-linear map $\phi : F' \longrightarrow M'$ with $\phi(e_i \otimes 1) = f(e_i \otimes 1)$. Note that the $\{e_i \otimes 1\}$ generate F' as an R'-module, since $e_i \otimes a = a \cdot (e_i \otimes a)$ for $a \in R'$. Let $\tilde{\phi} : F \longrightarrow M'$ be the unique R-linear map satisfying $\tilde{\phi}(e_i) = f(e_i \otimes 1)$. Then define

$$\phi: F \otimes_R R' \longrightarrow M', \quad x \otimes a \mapsto a \cdot \phi(x).$$

Then ϕ is R'-linear an we have

$$\phi(e_i \otimes 1) = 1 \cdot \tilde{\phi}(e_i) = \tilde{\phi}(e_i) = f(e_i \otimes 1),$$

which gives us the desired structure of an R'-module.

Proposition 11.21 Let R be a ring, R', R'' two R-algebras.

(i) $R' \otimes_R R''$ is an R-algebra with multiplication

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) := (a_1 a_2) \otimes (b_1 b_2)$$

- (ii) There are R-algebra homomorphisms
 - $\sigma': R' \longrightarrow R' \otimes_R R'', \qquad a \mapsto a \otimes 1$ $\sigma'': R'' \longrightarrow R'' \otimes_R R'', \qquad b \mapsto 1 \otimes b$
- (iii) For any R-algebra A and R-algebra homomorphisms $\phi': R' \longrightarrow A, \phi'': R'' \longrightarrow A$, there is a unique R-algebra homomorphism

$$\phi: R' \otimes_R R'' \longrightarrow A$$

satisfying $\phi' = \phi \circ \sigma'$ and $\phi'' = \phi \circ \sigma''$, i.e. making the following diagram commutative



proof. Defining

$$\tilde{\phi}: R' \times R'' \longrightarrow A, \qquad (x, y) \mapsto \phi'(x) \cdot \phi''(y)$$

gives us ϕ , which satisfies the required properties.

§ 12 Hilbert's basis theorem

Definition 12.1 Let R be a ring, M and R-module.

(i) M is called *noetherian*, if any ascending chain of submodules $M_0 \subset M_1 \subset \ldots$ becomes stationary.

 (ii) R is called *noetherian*, if R is noetherian as an R-module, i.e. if every ascending chain of ideals becomes stationary.

Example 12.2 (i) Let k be a field. A k-vector space is notherian if and only if $\dim(V) < \infty$.

- (ii) \mathbb{Z} is noetherian.
- (iii) Principle ideal domains are noetherian.

Proposition 12.3 Let

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$$

be a short exact sequence. Then M is noetherian if and only if M' and M'' are noetherian.

proof. ' \Rightarrow ' Let M be noetherian. Let first $M'_0 \subset M'_1 \subset \ldots$ be an ascending chain of submodules in M'. Then $\alpha(M'_0) \subset \alpha(M'_1) \subset \ldots$ is an ascending chain in M. Since M is noetherian, there exists some $n \in \mathbb{N}$, such that $\alpha(M'_i) = \alpha(M'_n)$ for all $i \ge n$. Since α is injective, we have $M'_i = M'_n$ for $i \ge n$, hence M' is noetherian. Let now $M''_0 \subset M''_1 \subset \ldots$ be an ascending chain of submodules in M''. Then $\beta^{-1}(M_0)'' \subset \beta^{-1}(M''_1) \subset \ldots$ is an ascending chain in M, hence becomes stationary. Since β is surjective, $\beta(\beta^{-1}(M''_i)) = M''_i$ and thus $M''_0 \subset M''_1 \subseteq \ldots$ becomes stationary.

' \Leftarrow ' Let $M_0 \subset M_1 \subset \ldots$ be an ascending chain in M. Let $M'_i := \alpha^{-1}(M_i) \cong M_i \cap M'$ and $M''_i := \beta(M_i)$. By assumption, there exists $n \in \mathbb{N}$, such that $M'_i = M'_n$ and $M''_i = M''_n$ for all $i \ge n$. Then for $i \ge n$ we have



Where γ is injective as an embedding. It remains to show that γ is surjective. Let $z \in M_i$. Since β is surjective, there exists $x \in M_n$, such that $\beta(x) = \beta(z)$. Then $\beta(\gamma(x) - z) = 0 \Rightarrow \gamma(x) - z = \alpha(y)$ for some $y \in M'_i = M'_n$. Let $\tilde{x} := x - \alpha(y)$. Then

$$\gamma(\tilde{x}) = \gamma(x) - \gamma(\alpha(y)) = \gamma(x) - \gamma(x) + z = z$$

hence γ is surjective, thus bijective and we have $M_i = M_n$ for $i \ge n$.

Corollary 12.4 Let R be a noetherian ring.

- (i) Any free R-module F of finite rank n is noetherian.
- (ii) Any finitely generated R-module M is noetherian.

proof. (i) Prove this by induction on n.

n = 1 Clear.

n > 1 Let $e_1, \ldots e_n$ be a basis of F and le F' be the submodule generated by $e_1, \ldots e_{n-1}$. Then F' is free of rank n - 1, thus noetherian by induction hypothesis. Moreover F/F' is free with generator e_n . Thus we have a short exact sequence

 $0 \longrightarrow F' \longrightarrow F \longrightarrow F/F' \longrightarrow 0$

with F', F/F' noetherian, hence by 12.2, F is noetherian.

(ii) If M is generated by $x_1, \ldots x_n$, there is a surjective, R-linear map $\phi : F \longrightarrow M$, sending the e_i to x_i , where F is the free R-module with basis $e_1, \ldots e_n$. Again by 12.2, M is noetherian which finishes the proof.

Proposition 12.5 For an *R*-module *M* the following statements are equivalent:

- (i) M is noetherian.
- (ii) Any nonempty family of submodules of M has a maximal element with respect to ' \subseteq '.
- (iii) Every submodule of M is finitely generated.
- proof. '(i) \Rightarrow (ii)' Let $\mathcal{M} \neq \emptyset$ be a set of submodules of M. Let $M_0 \in \mathcal{M}$. If M_0 is not maximal, there is $M_1 \in \mathcal{M}$ with $M_0 \subsetneq M_1$. If M_1 is not maximal, there is $M_2 \in \mathcal{M}$ with $M_1 \subsetneq M_2$. Since M is noetherian, we come to a maximal submodule M_n after finitely many step.
- '(ii) \Rightarrow (iii)' Let $N \subseteq M$ be a submodule. Let \mathcal{M} be the set of finitely generated submodules of N. Since $(0) \in \mathcal{M}$, we have $\mathcal{M} \neq \emptyset$ and thus there exists a maximal element $N_0 \in \mathcal{M}$. If $N_0 \neq N$, let $x \in N \setminus N_0$ and $N' := N_0 + (x)$ be the submodule generated by N_0 and x. Then clearly $N' \in \mathcal{M}$, which is a contradiction to the maximality of N_0 . Hence $N_0 = N$ and N is finitely generated.
- '(iii) \Rightarrow (i)' Let $M_0 \subseteq M_1 \subseteq \ldots$ be an ascending chain of submodules in M. Let $N := \bigcup_{n \in \mathbb{N}_0} M_n$. By assumption, N is finitely generated, say by $x_1, \ldots x_n$. Then there exists $i_0 \in \mathbb{N}$, such that $x_k \in M_{i_0}$ for all $1 \leq k \leq n$. Thus we have $M_i = M_{i_0}$ for $i \geq i_0$, i.e. th chain becomes stationary and M is noetherian.

Corollary 12.6 *R* is noetherian if and only if every ideal $I \leq R$ can be generated by finitely many elements. In particular, every principle ideal domain is noetherian.

proof. Follows from Proposition 12.4.

Theorem 12.7 (Hilbert's basis theorem) If R is noetherian, R[X] is also noetherian.

proof. Let $J \leq R[X]$ be an ideal. Assume that J is not finitely generated. Let f_1 be an element of $J \setminus \{0\}$ of minimal degree. Then $(f_1) \neq J$. Inductively let $J_i := (f_1, \ldots, f_i)$ and pick $f_{i+1} \in J \setminus J_i$ of minimal degree. Let a_i be the leading coefficient of f_i , i.e. we have

$$f_i = a_i X^{\deg(f_i)} + \sum_{j=1}^{\deg(f_i)-1} b_j X^j$$

The ideal $I \leq R$ generated by the a_i for $i \in \mathbb{N}$, is finitely generated by assumption. Then we find $n \in \mathbb{N}$ such that $a_{n+1} \in (a_1, \ldots, a_n)$, i.e. we have

$$a_{n+1} = \sum_{i=1}^{n} \lambda_i a_i$$

for suitable $\lambda_i \in R$. Let $d_i := \deg(f_i)$. Note, that $d_{i+1} \ge d_i$ for all $1 \le i \le n$. Let now

$$\rho := \sum_{i=1}^{n} \lambda_i f_i X^{d_{n+1}-d_i}$$

Then the leading coefficient of ρ is

$$a_{d_{n+1}} = \sum_{i=1}^{n} \lambda_i a_i$$

Hence $\deg(\rho - f_{n+1}) < d_{n+1}, \rho - f_{n+1} \notin J_n$, since $\rho \in J_n$, so f_{n+1} would be in J_n . This contradicts the choice of f_{n+1} . Hence our assumption was false and J is finitely generated and by Corollary 12.5 R[X] is noetherian.

Corollary 12.8 Let R be noetherian. Then

- (i) $R[X_1, \ldots, X_n]$ is noetherian for any $n \in \mathbb{N}$.
- (ii) Any finitely generated R-algebra is noetherian.

§ 13 Integral ring extensions

Definition 13.1 Let R be ring, S an R-algebra.

- (i) If $R \subseteq S$, S/R is called a ring extension.
- (ii) If $R \subseteq S$, $b \in S$ is called *integral over* S, if there exists a monic polynomial $f \in R[X] \setminus \{0\}$ such that f(b) = 0.
- (iii) S/R is called an *integral ring extension*, if every $b \in S$ is integral over R.

Example 13.2 (i) If R = k is a field, then *integral* is equivalent to *algebraic*.

(ii) $\sqrt{2}$ is integral over \mathbb{Z} , since $f = X^2 - 2$ is monic with $f(\sqrt{2}) = 0$.

(iii) $\frac{1}{2}$ is not integral over \mathbb{Z} . Assume $\frac{1}{2}$ is integral over \mathbb{Z} . Then there exists some monic $f \in R[X]$, such that $f(\frac{1}{2}) = 0$, i.e. we have

$$\left(\frac{1}{2}\right)^n + g\left(\frac{1}{2}\right) = 0 \;(*)$$

for some $g \in \mathbb{Z}[X]$. Then $2^{n-1} \cdot g\left(\frac{1}{2}\right) \in \mathbb{Z}$. Multiplying (*) by 2^{n-1} gives us

$$2^{n-1} \cdot \left(\left(\frac{1}{2}\right)^n + g\left(\frac{1}{2}\right) \right) = 0$$

and hence

$$\frac{1}{2} = -2^{n-1} \cdot g\left(\frac{1}{2}\right) \in \mathbb{Z}$$

Thus $\frac{1}{2}$ is not integral over \mathbb{Z} . More generally, we easily see that any $q \in \mathbb{Q} \setminus \mathbb{Z}$ is not integral over \mathbb{Z} .

Lemma 13.3 Let S/R be a ring extension, $b \in S$. If R[b] is contained in a subring $S' \subseteq S$ which is finitely generated as an R-module, then b is integral over R.

proof. Let s_1, \ldots, s_n be generators of S'. Since $b \cdot s_i \in S$ (we have $b \in R[b] \subseteq S$), we find $a_{ik} \in R$, such that

$$b \cdot s_i = \sum_{k=1}^n a_{ik} s_k \iff 0 = \sum_{k=1}^n (a_i k - \delta_{ik}) s_k. \quad (*)$$

Claim (a) Let A be the coefficient matrix of (*). Then det(A) = 0

Since the determinant is a monic polynomial in b of degree n with coefficients in R, b is integral over R. It remains to show the claim.

(a) Let $A^{\#}$ be the adjoint matrix

$$A_{ji}^{\#} = \det(A_{ij} \cdot (-1)^{i+j})$$

where A_{ij} is obtained from A by deleting the *i*-the row and *j*-th column. Recall

$$A^{\#}A = \det(A) \cdot E_n.$$

By (*) we have

$$A \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = 0$$

hence we have

$$A^{\#} \cdot A \cdot \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = 0 \implies \det(A) \cdot s_i = 0 \quad \text{for all } 1 \le i \le n$$

Since S' is a subring of S, we have $1 \in S'$, hence there exist $\lambda_1, \ldots, \lambda_n \in R$ with

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

Finally

$$\det(A) = \det(A) \cdot 1 = \det(A) \cdot \sum_{i=1}^{n} \lambda_i s_i = \sum_{i=1}^{n} \det(A) \cdot \lambda_i \cdot s_i = 0$$

Proposition 13.4 Let S/R be a ring extension. Define

$$\overline{R} := \{ b \in S \mid b \text{ is integral over } R \} \supseteq R$$

Then \overline{R} is a subring of S, called the integral closure of R in S.

proof. Let $b_1, b_2 \in \overline{R}$. We have to show, that $b_1 \pm b_2 \in \overline{R}$, $b_1b_2 \in \overline{R}$. Let $R[b_1]$ be the smallest subring of S containing R and b_1 . Then R is finitely generated as an R-module by $1, b_1, b_1^2, \ldots, b_1^{n-1}$, where n denotes the degree of the 'minimal polynomial' of f. Thus $R[b_1, b_2] = (R[b_1])[b_2]$ is also finitely generated as an $R[b_1]$ -module. This implies, that $R[b_1, b_2]$ is also finitely generated as an R-module and by Lemma 13.2, $R[b_1, b_2]/R$ is an integral ring extension. In particular, $b_1 \pm b_2$ and b_1b_2 are integral over R.

Definition 13.5 Let S/R be a ring extension, \overline{R} the integral closure of R in S.

- (i) R is called *integrally closed* in S, if $\overline{R} = R$.
- (ii) Let R be an integral domain. The integral closure of R in Quot(R) is called the *normalization* of R. R is called *normal*, if it agrees with its normalization.

Proposition 13.6 Any factorial domain is normal.

proof. Let R be a domain and $x = \frac{a}{b} \in \text{Quot}(R), a, b \in R, b \neq 0$ relatively prime. Suppose, x is integral over R, i.e. there exist $\alpha_0, \ldots, \alpha_{n-1} \in R$, such that

$$x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1x + \alpha_0 = 0$$

Multiplying by b^n gives us

$$a^{n} + \alpha_{n-1}a^{n-1}b + \ldots + \alpha_{1}ab^{n-1} + \alpha_{0}b^{n} = 0$$

and hence

$$a^{n} = b \cdot \underbrace{\left(-\alpha_{n-1}a^{n-1} - \ldots - \alpha_{1}ab^{n-2} - \alpha_{0}b^{n-1}\right)}_{\in \mathbb{R}} \quad \Longleftrightarrow \quad b \mid a^{n}$$

Since a and b are coprime, we have $b \in R^{\times}$. Thus $x = \frac{a}{b} = ab^{-1} \in R$ and R is normal.

Definition 13.7 Let R be a ring.

(i) For a prime ideal $\mathfrak{p} \leq R$ we define

$$ht(\mathfrak{p}) := \sup\{n \in \mathbb{N}_0 \mid \text{ there exist prime ideals } \mathfrak{p}_0, \mathfrak{p}_1, \dots, \mathfrak{p}_n, \text{ with } \mathfrak{p}_n = \mathfrak{p} \text{ and } \mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_n\}$$

to be the *height* of \mathfrak{p} .

(ii) The Krull-dimension of R is

$$\dim(R) := \dim_{\mathrm{Krull}}(R) = \sup\{ht(\mathfrak{p}) \mid \mathfrak{p} \leqslant R \text{ prime }\}$$

Example 13.8 (i) Since $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n)$, we have dim $(k[X_1, \ldots, X_n]) \ge n$.

- (ii) $\dim(k) = 0$ for any field k, since (0) is the only prime ideal.
- (iii) dim(\mathbb{Z}) = 1, since (0) \subsetneq (p) is a maximal chain of prime ideals for $p \in \mathbb{P}$.
- (iv) $\dim(R) = 1$ for any principle ideal domain which is not a field: Assume p, q are prime element with $(p) \subseteq (q)$. Then $p = q \cdot a$ for some $a \in R$. Since p is irreducible, we have $a \in R^{\times}$ and hence (p) = (q).
- (v) $\dim(k[X]) = 1$ for any field k:

Theorem 13.9 (Going up theorem) Let S/R be an integral ring extension and

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

a chain of prime ideals in R. Then there exists a chain of prime ideals

$$\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \ldots \subsetneq \mathfrak{P}_n$$

in S, such that $\mathfrak{p}_i = \mathfrak{P}_i \cap R$.

proof. Do this by induction on n.

n=0 Let $\mathfrak{p} \triangleleft R$ be a prime ideal. We have to find a prime ideal $\mathfrak{P} \triangleleft S$ with $\mathfrak{P} \cap R = \mathfrak{p}$. Let

$$\mathcal{P} := \{ I \lhd S \text{ ideal } | I \cap R = \mathfrak{p} \}$$

Claim (a) $\mathfrak{p}S \in \mathcal{P}$.

```
Then \mathcal{P} is nonempty. Zorn's lemma provides us then a maximal element \mathfrak{m} \in \mathcal{P}.
Claim (b) \mathfrak{m} \lhd S is a prime ideal.
```

This proves the claim. It remains to show the Claims.

(b) Suppose $b_1, b_2 \in S$ with $b_1b_2 \in \mathfrak{m}$. Assume $b_1, b_2 \in S \setminus \mathfrak{m}$.

Then $\mathfrak{m} + (b_i) \notin \mathcal{P}$, hence $(\mathfrak{m} + (b_i)) \supseteq \mathfrak{p}$ for $i \in \{1, 2\}$. \Longrightarrow Thus there exists $p_i \in \mathfrak{m}, s_i \in S$ such that $r_i := p_i + b_i s_i \in R \setminus \mathfrak{p}$. Then we have

$$r_1r_2 = (p_1 + b_1s_1)(p_2 + b_2s_2) = \underbrace{p_1p_2 + p_1b_2s_2 + b_1s_1p_2}_{\in \mathfrak{m}} + \underbrace{b_1b_2}_{\in \mathfrak{m} \text{ by ass.}} s_1s_2 \in \mathfrak{m}$$

Clearly $r_1r_2 \in R$, hence $r_1r_2 \in \mathfrak{m} \cap R = \mathfrak{p}$, which is a contradiction, since \mathfrak{p} is prime. (a) We have to show $\mathfrak{p}S \cap R = \mathfrak{p}$. We prove both inclusions.

'⊇' This is clear by definition.

'⊆' Let now

$$b = \sum_{i=0}^{n} p_i t_i, \qquad p_{\in} \mathfrak{p}, \ t_i \in S$$

Since the t_i are integral over R, $R[t_1, \ldots t_n] =: S'$ is finitely generated. Let

 s_1, \ldots, s_m be generators of S' as an R-module. Since $b \in \mathfrak{p}S'$, we have

$$bs_i = \sum_{k=0}^m a_{ki} s_k$$

for suitable $a_{ik} \in \mathfrak{p}$. Then as in lemma 13.3 we have $\det(a_{ik} - \delta_{ik}b) = 0$ and thus b is a zero of monic polynomial with coefficients in \mathfrak{p} , i.e. b satisfies an equation

$$b^{n} + a_{n-1}b^{n-1} + \ldots + a_{1}b + a_{0} = 0$$
 with $a_{i} \in \mathfrak{p}$,

Write

$$b^n = -\sum_{i=0}^{n-1} a_i b^i \in \mathfrak{p},$$

since $b^i \in \mathfrak{p}$. Since \mathfrak{p} is prime, we must have $b \in \mathfrak{p}$ and hence the required inclusion.

n > 1 By induction hypothesis we have a chain

$$\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \ldots \subsetneq \mathfrak{P}_{n-1}$$

satisfying $\mathfrak{P}_i \cap R = \mathfrak{p}_i$. Moreover we find $\mathfrak{P}_n \triangleleft S$ such that $\mathfrak{P}_n \cap R = \mathfrak{p}_n$. It remains to show $\mathfrak{P}_{n-1} \subsetneq \mathfrak{P}_n$. For $x \in \mathfrak{P}_{n-1}$ we have $x \in R \cap \mathfrak{p}_{n-1}$, i.e. $x \in \mathfrak{p}_{n-1} \subset \mathfrak{p}_n$. Thus $x \in \mathfrak{p}_n \cap R = \mathfrak{P}_n$. Assume now $\mathfrak{P}_{n-1} = \mathfrak{P}_n$. Let $x \in \mathfrak{p}_n$. Then

$$x \in \mathfrak{p}_n \in \mathfrak{p}_n \cap R = \mathfrak{P}_n = \mathfrak{P}_{n-1} = \mathfrak{p}_{n-1} \cap R, \implies x \in \mathfrak{p}_{n-1}$$

and thus $\mathfrak{p}_n \subseteq \mathfrak{p}_{n-1}$, hence $\mathfrak{p}_n = \mathfrak{p}_{n-1}$, a contradiction.

Theorem 13.10 Let S/R be an integral ring extension. Then $\dim(R) = \dim(S)$.

proof. ' \leq ' Follows from Proposition 13.7

'>' Let $\mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \ldots \subsetneq \mathfrak{P}_n$ be chain of prime ideals in S and define $\mathfrak{p}_i := \mathfrak{P}_i \cap R$. Then \mathfrak{p}_i is prime and we have $\mathfrak{p}_i \subseteq \mathfrak{p}_{i+1}$. It remains to show, that $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$. Define $S' := S/\mathfrak{P}_i$ and $R' := R/\mathfrak{p}_i$. Then S'/R' is integral (!). We have to show that $\overline{\mathfrak{P}}_{i+1} \cap R = \overline{\mathfrak{p}}_{i+1} :=$ image of \mathfrak{p}_{i+1} in S' is not (0). Let $b \in \mathfrak{P}_{i+1} \setminus \{0\}$. Since b is integral over R', there exist $a_0, \ldots, a_{n-1} \in R$, such that

$$b^{n} + a_{n-1}b^{n-1} + \ldots + a_{1}b + a_{0} = 0$$

Let further n be minimal with this property. Write

$$a_0 = -b \cdot \underbrace{\left(a_1 + a_2b + \ldots + a_{n-1}b^{n-2} + b^{n-1}\right)}_{=:c} \in \overline{\mathfrak{P}}_{i+1} \cap R = \overline{\mathfrak{p}}_{i+1}$$

But $c \neq 0$ by the choice of n and $b \neq 0$. Since $R' = R/\mathfrak{p}$ is an integral domain, we have $\overline{0} \neq a_0 \in \overline{\mathfrak{p}}_{i+1}$ and thus $\overline{\mathfrak{p}}_{i+1} \neq (0)$, which proves the claim.

Theorem 13.11 (Noether normalization) Let k be a field. Then every finitely generated kalgebra is an integral extension of a polynomial ring over k[X].

proof. Let $a_1, \ldots a_n$ be generators of A as a k-algebra. Prove the theorem by induction.

- **n=1** If a_1 is transcendental over k, then $A \cong k[X]$. Otherwise $A \cong k[X]/(f)$, where f denotes the minimal polynomial of a_1 over k. Thus A is integral over k.
- n>1 If $a_1, \ldots a_n$ are algebraically independent, $A \cong k[X_1, \ldots X_n]$. Otherwise there exists some polynomial

 $F \in k[X_1, \ldots, X_n] \setminus \{0\}$ such that $F(a_1, \ldots, a_n) = 0$.

case 1 Assume we have

$$F = X_n^m + \sum_{i=1}^{m-1} g_i X_n^i$$

with $g_i \in k[X_1, \ldots, X_n]$. Then $F(a_1, \ldots, a_n) = 0$, hence a_n is integral over $A' := k[a_1, \ldots, a_{n-1}]$. By induction hypothesis, A' is integral over some polynomial ring, so is A.

case 2 For the general case write

$$F = \sum_{i=0}^{m} F_i,$$

where F_i is homogenous of degree *i*, i.e. the sum of the exponents of any monomial in f_i is equal to *i*. Then replace a_i by $b_i := a_i - \lambda a_n$ (*) with suitable $\lambda_i \in k, 1 \leq i \leq n-1$. Then $A \cong k[b_1, \ldots, b_{n-1}, a_n]$. For any monomial $a_1^{d_1} \cdots a_n^{d_n}$ we find

$$a_1^{d_1} \cdots a_n^{d_n} = (b_1 + \lambda_1 a_n)^{d_1} \cdots (b_{n-1} + \lambda_{n-1} a_n)^{d_{n-1}} \cdot a_n^{d_n} = \left(\prod_{i=1}^{n-1} \lambda_i^{d_i}\right) \cdot a_n^{\sum_{i=1}^n d_i} + \mathcal{O}(a_n)$$

where $\mathcal{O}(a_n)$ denotes terms of lower degree in a_n . Then for $d := \sum_{i=1}^n d_i$ we obtain

$$F_d(a_1, \dots a_n) = a_n^d \cdot F_d(\lambda_1, \dots \lambda_{n-1}, 1) + \mathcal{O}(a_n)$$

and thus

$$F(a_1,\ldots,a_n) = a_n^m F_m(\lambda_1,\ldots,\lambda_{n-1},1) + \mathcal{O}(a_n)$$

Choose now $\lambda_1, \ldots, \lambda_{n-1} \in k$, such that $F_m(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. If k is infinite, this is always possible. In the finite case, go back to (*) and use $b_i := a_i + a_n^{\mu_i}$ instead and repeat the procedure. Then by the first case and induction hypothesis the claim follows.

§ 14 Dedekind domains

Definition 14.1 A noetherian integral domain R of dimension 1 is called a *Dedekind domain*, if every nonzero ideal $I \lhd R$ has a unique representation as a product of prime ideals

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

Definition + remark 14.2 Let R be a noetherian integral domain, k := Quot(R) and $(0) \neq I \subseteq k$ an R-module.

- (i) I is called a *fractional ideal*, if there exists $a \in R \setminus \{0\}$, such that $a \cdot I \subseteq R$.
- (ii) I is a fractional ideal if and only if I is finitely generated as an R-module.
- (iii) For a fractional ideal I let

$$I^{-1} := \{ x \in k | x \cdot I \subseteq R \}$$

Then I^{-1} is a fractional ideal.

- (iv) I is called *invertible*, if $I \cdot I^{-1} = R$, where $I \cdot I^{-1}$ denotes the R-module generated by all products $x \cdot y$ with $x \in I, y \in I^{-1}$.
- proof. (ii) ' \Rightarrow ' If $a \cdot I \subseteq R$, then $a \cdot I$ is an ideal in R. since R is noetherian, $a \cdot I$ is finitely generated, say by x_1, \ldots, x_n . Then I is generated by $\frac{x_1}{a}, \ldots, \frac{x_n}{a}$.

' \Leftarrow ' Let y_1, \ldots, y_m be generators of *I*. Write $y_i = \frac{r_i}{a_i}$ with $r_i, a_i \in R \setminus 0$. Define

$$a := \prod_{i=1}^{n} a_i$$

Then for any generator we have $a \cdot y_i = r \cdot a_1 \cdot \ldots \cdot a_{i-1} \cdot a_{i+1} \cdot \ldots \cdot a_m \in R$, hence $a \cdot I \subseteq R$.

Example 14.3 Every principle ideal $I \neq (0)$ is invertible: Let $I = (a) \leq R$. Then $I^{-1} = \frac{1}{a}R$, since we have

$$I \cdot I^{-1} = (a) \cdot \frac{1}{a}R = aR \cdot \frac{1}{a}R = R$$

Proposition 14.4 Let R be a Dedekind domain. Then every nonzero ideal $I \leq R$ is invertible. proof. Let $(0) \neq I \lhd R$ be a proper ideal. Then by assumption we can write

$$I = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r$$

with prime ideal $\mathfrak{p}_i \lhd R$.

If each \mathfrak{p}_i is invertible, then we have

$$I \cdot \mathfrak{p}_r^{-1} \cdots \mathfrak{p}_1^{-1} = R,$$

hence I is invertible. Thus we may assume that $I = \mathfrak{p}$ is prime. Let $a \in \mathfrak{p} \setminus \{0\}$ and write

$$(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_m$$

with prime ideals $\mathfrak{p}_i \lhd R$. Then $(a) \subseteq \mathfrak{p}$, i.e. $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some $1 \leq i \leq m$, say i = 1. Since the ideals were proper and $\dim(R) = 1$, we have $\mathfrak{p}_1 = \mathfrak{p}$ and $\mathfrak{p}^{-1} = \mathfrak{p}_1^{-1} = \frac{1}{a} \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_m$, since $\mathfrak{p}_1 \mathfrak{p}_1^{-1} = \frac{1}{a}(a) = (1) = R$.

Corollary 14.5 The fractional ideals in a Dedekind domain R form a group.

proof. Let $(0) \neq I \subseteq k = \text{Quot}(R)$ be a fractional ideal. Choose $a \in R$ such that $a \cdot I \subseteq R$. By Proposition 14.3, $a \cdot I$ is invertible, i.e. there exists a fractional ideal I', such that

$$(a \cdot I) \cdot I' = R \implies I \cdot (a \cdot I') = R$$

where R is neutral element of the group.

Proposition 14.6 Every Dedekind domain R is normal.

proof. Let $x \in k := \text{Quot}(\mathbf{R})$ be integral over R, i.e. we can write

$$x^{n} + a_{n-1}X^{n-1} + \dots a_{1}x + a_{0} = 0, \qquad a_{i} \in R$$

By the proof of Proposition 13.3, R[x] is a finitely generated *R*-module, hence R[x] is a fractional ideal by Remark 14.2. Further by Corollary 14.4 R[x] is invertible, i.e. we can find $I \leq k$, such that $I \cdot R[x] = R$.

On the other hand R[x] is a ring, i.e. $R[x] \cdot R[x] = R[x]$. Multiplying the equation by I gives us $x \in R$. In particular we have

$$R = I \cdot R[x] = I \cdot (R[x] \cdot R[x]) = (I \cdot R[x]) \cdot R[x] = R \cdot R[x] = R[x]$$

which implies the claim.

Proposition 14.7 Let R be noetherian integral domain of dimension 1. Then R is a Dedekind domain if and only if R is normal.

proof. ' \Rightarrow ' This is Proposition 14.5

'⇐' We claim

claim (a) For every prime ideal (0) $\neq \mathfrak{p} \triangleleft R$ the localization $R_{\mathfrak{p}}$ is a discrete valuation ring.

claim (b) Every nonzero ideal in R is invertible.

Then let $(0) \neq I \neq R$ be an ideal in R. Then $I \subseteq \mathfrak{m}_0$ for a maximal ideal $\mathfrak{m}_0 \triangleleft R$. By claim (b), \mathfrak{m}_0 is invertble. Define $I_1 := \mathfrak{m}_0^{-1} \cdot I$. Then $I_1 \subseteq \mathfrak{m}_0^{-1} \cdot \mathfrak{m}_0 = R$ is an ideal. If $I_1 = R$, then

 $I = \mathfrak{m}_0$. Otherwise let \mathfrak{m}_1 be a maximal ideal containing I_1 and define $I_2 := \mathfrak{m}_1^{-1} \cdot I_1 \leq R$. If $I_1 = I$, then $\mathfrak{m}_0^{-1} \cdot I = I \xrightarrow{\text{invert.}} \mathfrak{m}_0^{-1} = R$, which is a contradiction. By this way we obtain a chain of ideals

$$I \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_n$$

Since R is noetherian, there exists $n \in \mathbb{N}$; such that $I_n = R$. Then

$$R = I_n = \mathfrak{m}_{n-1}^{-1} \cdot I_{n-1} = \mathfrak{m}_{n-1}^{-1} \cdot \mathfrak{m}_{n-1}^{-1} \cdot I_{n-2} = \mathfrak{m}_{n-1}^{-1} \cdot \cdot \cdot \mathfrak{m}_0^{-1} \cdot I_{n-2}$$

Thus

$$I = \mathfrak{m}_0 \cdot \mathfrak{m}_1 \cdots \mathfrak{m}_{n-2} \cdot \mathfrak{m}_{n-1}$$

with maximal, thus prime ideals \mathfrak{m}_i . Hence R is a Dedekind domain.

It remains to show the claims.

- (b) Let $(0) \neq I \leq R$ be an ideal. We have to show $I \cdot I^{-1} = R$ for $I^{-1} = \{x \in k \mid x \cdot I \subseteq R\}$. ' \subseteq ' Clear.
 - '⊇' Assume $I \cdot I^{-1} \neq R$. Then there exists a maximal ideal $\mathfrak{m} \lhd R$ such that $I \cdot I^{-1} \subseteq \mathfrak{m}$. By claim (a), $R_{\mathfrak{m}}$ is a principal ideal domain, thus $I \cdot R_{\mathfrak{m}}$ is generated by one element, say $\frac{a}{s}$ for some $a \in I, s \in R \setminus \mathfrak{m}$. Let now b_1, \ldots, b_n be generators of I as an ideal in R. Then

$$\frac{b_i}{1} = \frac{a}{s} \cdot \frac{r_i}{s_i}, \quad r_i \in R, s_i \in R \backslash \mathfrak{m}, \text{ for } 1 \leqslant i \leqslant n$$

Define $t := s \cdot s_1 \cdots s_n \in R \setminus \mathfrak{m}$. We have $\frac{t}{a} \in I^{-1}$, since

$$\frac{t}{a} \cdot b_i = \frac{t}{a} \cdot \frac{a}{s} \cdot \frac{r_i}{s_i} = r_i \cdot s_1 \cdots s_{i-1} \cdot s_{i+1} \cdots s_n \in R$$

for $1 \leq i \leq n$. But then

$$t = \frac{t}{a} \cdot a \in I^{-1} \cdot I \subseteq \mathfrak{m} \quad \notin$$

(a) We will only give a proof sketch. The strategy is as follows:

- (i) Ot suffices to show, that $\mathfrak{m} := \mathfrak{p}R_{\mathfrak{p}}$ is a principal ideal.
- (ii) Show that $\mathfrak{m}^n \neq \mathfrak{m}$.
- (iii) Show that \mathfrak{m} is invertible.

Then pick $t \in \mathfrak{m}^2 \setminus \mathfrak{m}$ and obtain $t \cdot \mathfrak{m}^{-1} = R_{\mathfrak{m}}$. This is true, since otherwise, as \mathfrak{m} is the only maximal ideal in $R_{\mathfrak{p}}$, we would have $t \cdot \mathfrak{m}^{-1} \subseteq \mathfrak{m}$ and thus $t \in \mathfrak{m}^2$, which implies $\mathfrak{m} = \mathfrak{m}^2$. Then we have

$$(t) = t \cdot R = t \cdot (\mathfrak{m} \cdot \mathfrak{m}^{-1}) = R_{\mathfrak{p}} \cdot \mathfrak{m} = \mathfrak{m},$$

which will gives us the claim.

		L

Theorem 14.8 Let R be a Dedekind domain, L/k a finite separable field extension of k := Quot(R) and S the integral closure of R in L. Then S is a Dedekind domain.

proof. We will show all the required properties of a Dedekind domain.

integral domain. This is clear.

dimension 1. We know that S/R is integral and Proposition 13.7 gives us $\dim(S) = 1$.

normal. If $x \in L$ is integral over S, x is integral over R, thus $x \in S$.

noetherian. This is the only hard work in the proof. Let N := [L : k]. Since L/k is separable, there exists $\alpha \in L$ such that $L = k(\alpha)$. Moreover we have $|\operatorname{Hom}_k(L, \overline{k})| = n$, say $\operatorname{Hom}_k(L, \overline{k}) = \{\operatorname{id} = \sigma_1, \ldots, \sigma_n\}$.

claim (a) α can be chosen in S.

Then let

$$D := \begin{pmatrix} 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \sigma_2(\alpha) & \dots & \sigma_2(\alpha^{n-1}) \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\alpha) & \dots & \sigma_n(\alpha^{n-1}) \end{pmatrix} = (\sigma_i(\alpha^j))_{(i,j)\in\{1,\dots,n\}\times\{0,\dots,n-1\}}$$

and $d := (\det(D))^2$. $d := d_{L/k}(\alpha)$ is called the discriminant of L/k with respect to α . claim (b) We have

(i) $d \neq 0$

(ii) S is contained in the R-module generated by $\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^{n-1}}{d}$.

Then S is submodule of a finitely generated R-module, and since R is noetherian, S is noetherian as an R-module, thus also as an S-module. This proves *noetherian*. Now prove the claims.

(a) Let $\tilde{\alpha} \in L$ be a primitive element, i.e. $L = k(\tilde{\alpha})$. Let

$$f = X^n - \sum_{i=0}^{n-1} c_i X^i$$

be the minimal polynomial of $\tilde{\alpha}$ over k. Writr $c_i = \frac{a_i}{b_i}$ for suitable $a_i, b_i \in R, b_i \neq 0$. Now define

$$b := \prod_{i=0}^{n-1} b_i, \qquad \alpha := b \cdot \tilde{\alpha}.$$

Since we have

$$\alpha^n = b^n \tilde{\alpha}^n = b^n \cdot \sum_{i=0}^{n-1} c_i \tilde{\alpha}^i = \sum_{i=0}^{n-1} c_i \cdot \frac{\alpha^i}{b^i} b^n$$

we obtain

$$\alpha^n = b^n \cdot \tilde{\alpha}^n = \sum_{i=0}^{n-1} c_i ? \alpha^i, \quad c'_i = c_i \cdot b^{n-i} \in R.$$

Thus α is integral over R, i.e. $\alpha \in S$. We easily see $k(\alpha) = k(\tilde{\alpha})$, hence the claim is proved.

(b) (i) We have

$$d = (\det(D))^2 = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \neq 0,$$

since otherwise we would have $\sigma_i(\alpha) = \sigma_j(\alpha)$, i.e. $\sigma_i = \sigma_j$, which is not possible. (ii) Let $\beta \in S$. Write

$$\beta = \sum_{i=0}^{n-1} c_{i+1} \alpha^i, \quad c_i \in k.$$

We have to show: $c_i \in \frac{1}{d}R$ for all $1 \leq i \leq n$. Therefore we need **claim (c)** There is a matrix $A \in R^{n \times n}$ and $b \in R^n$, such that

$$A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = b$$
 and $\det(A) = d$.

Then by Cramer's rule and Claim (c) we have

$$c_i = \frac{\det(A_i)}{\det(A)} = \frac{\det(A_i)}{d} \in \frac{1}{d} \in R$$

where A_i is obtained by replacing the *i*-th column of A by b. This proves claim (b). (c) Recall that

$$tr_{L/k}: L \longrightarrow k, \quad \beta \mapsto \sum_{i=1}^{n} \sigma_i(\beta)$$

is a k-linear map. For β as above we find for $1\leqslant i\leqslant n$

$$(*) tr_{L/k}(\underbrace{\alpha^{i-1}\beta}_{\in S}) = \sum_{j=1}^{n} tr_{L/k}(\alpha^{i-1}\alpha^{j-1}c_j) = \sum_{j=1}^{n} tr_{L/k}(\alpha^{i-1}\alpha^{j-1})c_j \in k \cap S = R$$

where the last equality holds since R is normal and by Proposition 14.5. Let now

$$A = (a_{ij})_{(i,i)\in\{1,\dots,n\}\times\{1,\dots,n\}}, \quad a_{ij} = tr_{L/k}(\alpha^{i-1}, \alpha^{j-1})$$

and

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \quad b_i = Tr_{L/k}(\alpha^{i-1}\beta).$$

Then by (*) we have

$$A \cdot \begin{pmatrix} c_1 \\ \cdots \\ c_n \end{pmatrix} = b,$$

i.e. the first part of the claim. Moreover we have $D^T D = (\tilde{a}_{ij})$, where

$$\tilde{a}_{ij} = \sum_{k=1}^{n} \sigma_k(\alpha^{i-1}) \sigma_k(\alpha^{j-1}) = \sum_{k=1}^{n} \sigma_k(\alpha^{i-1}\alpha^{j-1}) = tr_{L/k}(\alpha^{i-1}, \alpha^{j-1}) = a_{ij}$$

Hence $D^T D = A$ and by $det(D) = det(D^T)$ we have

$$\det(D)^2 = \det(D \cdot D) = \det(D \cdot D^T) = \det(A) = d.$$

We have now shown that S is an integral domain, of dimension 1, noetherian and normal. By Proposition 14.6 the theorem is proved. $\hfill \Box$