Algebraic Number Theory

Franz Halter-Koch

Contents

CHAPTER 1

Supplements to Field Theory

1.1. Normal field extensions

Definition 1.1.1. Let K be a field, $f \in K[X] \setminus K$, $c \in K^\times$ the leading coefficient of f and $L \supset K$ an extension field. We say that f *splits* in L if there exist $\alpha_1, \ldots, \alpha_n \in L$ such that

$$f = c\prod_{i=1}^{n}(X - \alpha_i)\,,$$

and if $L = K(\alpha_1, \ldots, \alpha_n)$, then L is called a *splitting field* of f.

Remark 1.1.2. Let K be a field and $f \in K[X] \setminus K$. Then f possesses a spitting field, and for any two splitting fields L, L' of f there exists a K-isomorphism $L \overset{\sim}{\to} L'$.

Proof. Let $c \in K^\times$ be the leading coefficient of f and $\overline{K}$ an algebraic closure of K. There exist $\alpha_1, \ldots, \alpha_n \in \overline{K}$ such that $f = c(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$, and then $L = K(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f. To prove uniqueness, let L' be another splitting field of f and $\overline{L}'$ an algebraic closure of L'. Since L'/K is algebraic, it follows that $\overline{L}'$ is an algebraic closure of K, and therefore there exists a K-isomorphism $\phi\colon \overline{K} \overset{\sim}{\to} \overline{L}'$. Let $\phi_1\overline{K}[X] \to \overline{L}'[X]$ be the trivial extension of ϕ to the polynomial rings. Then

$$f = \phi_1(f) = c\prod_{i=1}^{n}(X - \phi(\alpha_i))\,.$$

Since f splits in L', it follows that $\phi(\alpha_i) \in L'$ for all $i \in [1, n]$, hence $L' = K(\phi(\alpha_1), \ldots, \phi(\alpha_n)) = \phi(L)$, and $\varphi = \phi \,|\, L\colon L \overset{\sim}{\to} L'$ is the desired K-isomorphism. □

Theorem and Definition 1.1.3. *Let L/K be an algebraic field extension and $\overline{K} \supset L$ and algebrically closed extension field.*

1. *The following statements are equivalent:*
   - (a) *For every K-homomorphism $\varphi\colon L \to \overline{K}$ we have $\varphi(L) \subset L$.*
   - (b) *Every irreducible polynomial $f \in K[X] \setminus K$ which has a zero in L already splits in L.*

   If $[L\!:\!K] < \infty$, then there is also equivalent:
   - (c) *L is the splitting field of some polynomial $f \in K[X] \setminus K$.*

   If these conditions are fulfilled, then the extension L/K is called *normal.* If L/K is normal and separable, then L/K is called *galois.*

2. *L/K is a finite galois extension if and only if L is the splitting field of a separable polynomial $f \in K[X] \setminus K$.*
3. The fields $\varphi(L)$ for $\varphi \in \operatorname{Hom}_K(L, \overline{K})$ are called the *conjugate fields* of L (over K in $\overline{K}$), and its compositum

$$\widetilde{L} = \prod_{\varphi \in \operatorname{Hom}_K(L,\overline{K})} \varphi(L) = K\Big(\bigcup_{\varphi \in \operatorname{Hom}_K(L,\overline{K})} \varphi(L)\Big)$$

is called the *normal closure* of L/K (inside $\overline{K}$). If L/K is separable, then $\widetilde{L}$ is called that *galois closure* of L/K (inside $\overline{K}$).

$\widetilde{L}$ is the smallest subfield of $\overline{K}$ such that $L \subset \widetilde{L}$ and $\widetilde{L}/K$ is normal. If L/K is separable, then $\widetilde{L}/K$ is galois, and if $[L:K] < \infty$, then $[\widetilde{L}:K] < \infty$.

Proof. 1. (a) $\Rightarrow$ (b) Let $f \in K[X] \setminus K$ be irreduzible, $\alpha \in L$ and $f(\alpha) = 0$. Then

$$f = c\prod_{i=1}^{n}(X - \alpha_i)\,, \quad \text{where } c \in K^\times \text{ is the leading coefficient of } f \text{ and } \alpha = \alpha_1, \ldots, \alpha_n \in \overline{K}.$$

For $i \in [2, n]$, let $\alpha_i \colon K(\alpha) \to \overline{K}$ be the unique K-homomorphism such that $\varphi(\alpha) = \alpha_i$, and let $\phi_i \colon L \to \overline{K}$ be a homomorphism such that $\phi_i \,|\, K(\alpha) = \varphi_i$. By assumption, we have $\phi_i(L) \subset L$ and thus $\alpha_i = \phi_i(\alpha_i) \in L$ for all $i \in [2, n]$. Hence f splits in L.

(b) $\Rightarrow$ (a) Let $\varphi \colon L \to \overline{K}$ be a K-homomorphism, $\alpha \in L$ and $f \in K[X]$ the minimal polynomial of α over K. Then f splits in K, and since $f(\varphi(\alpha)) = 0$, we obtain $\varphi(\alpha) \in L$

(b) $\Rightarrow$ (c) Since $[L : K] < \infty$, we obtain $L = K(\alpha_1, \ldots, \alpha_m)$ for some $m \in \mathbb{N}$ and $\alpha_1, \ldots, \alpha_m \in L$. For $j \in [1, m]$, let $f_j \in K[X]$ be the minimal polynomial of α_j over K, and $f = f_1 \cdot \ldots \cdot f_m$. By assumption, every f_j splits in L. Hence f splits in L, and as L arises from K be adjoining zeros of f, it is a splitting field of f.

(c) $\Rightarrow$ (a) Let L be a splitting field of some $f \in K[X] \setminus K$, say

$$f = c\prod_{i=1}^{n}(X - \alpha_i)\,, \quad \text{where } c \in K^\times \text{ and } L = K(\alpha_1, \ldots, \alpha_n).$$

Let $\varphi \in \operatorname{Hom}_K(L, \overline{K})$ and $\varphi_1 \colon L[X] \to \overline{K}[X]$ its trivial extension to polynomial rings. Then

$$f = \varphi_1(f) = c\prod_{i=1}^{n}(X - \varphi(\alpha_i)) = c\prod_{i=1}^{n}(X - \alpha_i)\,,$$

hence $\{\varphi(\alpha_1), \ldots, \varphi(\alpha_n)\} = \{\alpha_1, \ldots, \alpha_n\}$, and $\varphi(L) = K(\varphi(\alpha_1), \ldots, \varphi(\alpha_n)) = K(\alpha_1, \ldots, \alpha_n) = L$.

2. If L is the splitting field of a separable polynomial, then L/K is separabel and normal, hence galois. Assume now that L/K is a finite galois extension. By 1., L is the splitting field of some polynomial $f \in K[X] \setminus K$. Let $f = f_1^{e_1} \cdot \ldots \cdot f_r^{e_r}$, where $r \in \mathbb{N}$, $f_1, \ldots, f_r \in K[X] \setminus K$ are distinct irreducible polynomials, and $e_1, \ldots, e_r \in \mathbb{N}$. Then $L = K(C)$, where C is the set of all zeros of $f_1 \cdot \ldots \cdot f_r$ in L. Hence L is the splitting field of $f^* = f_1 \cdot \ldots \cdot f_r$, each f_i is separable, and thus f^* is separable, too.

3. $\widetilde{L}/K$ is normal: Let $\phi \in \mathrm{Hom}_K(\widetilde{L}, \overline{K})$. If $\varphi \in \mathrm{Hom}_K(L, \overline{K})$, then it follows that $\varphi(L) \subset \widetilde{L}$, hence $\phi\circ\varphi \in \mathrm{Hom}_K(L, \overline{K})$, and therefore $\phi(\varphi(L)) = \phi\circ\varphi(L) \subset \widetilde{L}$. Consequently,

$$\phi(\widetilde{L}) = K\Big(\bigcup_{\varphi \in \mathrm{Hom}_K(L,\overline{K}} \phi(\varphi(L)\Big) \subset \widetilde{L}\,, \quad \text{and thus } \widetilde{L}/K \text{ is normal.}$$

Let now $L' \subset \overline{K}$ any subfield such that $L \subset L'$ and L'/K is normal. For every $\varphi \in \mathrm{Hom}_K(L, \overline{K})$, there is some $\varphi' \in \mathrm{Hom}_K(L', \overline{K})$ such that $\varphi' \,|\, L = \varphi$, and since $\varphi'(L') \subset L'$, it follows that $\varphi(L) \subset L'$. Hence

$$\widetilde{L} = K\Big(\bigcup_{\varphi \in \mathrm{Hom}_K(L,\overline{K})} \varphi(L)\Big) \subset L'\,.$$

If L/K is separable and $\varphi \in \mathrm{Hom}_K(L, \overline{K})$, then $\varphi(L)/K$ is separable, say $\varphi(L) = C_\varphi$, where $C_\varphi \subset \overline{K}$ is a set of separable elements over K. Then it follows that

$$\widetilde{L} = K\Big(\bigcup_{\varphi \in \mathrm{Hom}_K(L,\overline{K})} \varphi(L) = K\Big(\bigcup_{\varphi \in \mathrm{Hom}_K(L,\overline{K})} C_\varphi\Big) \quad \text{is separable over } K.$$

If L/K is finite, then $\mathrm{Hom}_K(L, \overline{K}) = [L\!:\!K]_{\mathsf{s}} \le [L\!:\!K] < \infty$, and therefore $\widetilde{L}/K$ is finite. $\square$

`iveselement`

Theorem 1.1.4 (Primitive Element Theorem)**.** *Let L/K be a finite field extension, $n \in \mathbb{N}$, and $L = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_2, \ldots, \alpha_n$ are separable over K. Then there exists some $\alpha \in L$ such that $L = K(\alpha)$.*

Proof. If K is finite, then L is finite. Hence $L^\times$ is cyclic, and if $L^\times = \langle\omega\rangle$, then $L = K(\omega)$.

Thus let K be infinite, and proceed by induction on n. For $n = 1$, there is nothing to do. Thus suppose that $n \ge 2$. By the induction hypothesis, there exists some $\alpha \in L$ such that $K(\alpha_1, \ldots, \alpha_{n-1}) = K(\alpha)$, and we set $\beta = \alpha_n$. Then $L = K(\alpha, \beta)$, β is separable over K, and we shall prove that there exists some $c \in K$ such that $L = K(\alpha + c\beta)$.

Let $\overline{K} \supset L$ be an algebraically closed extension field, let $f \in K[X]$ be the minimal polynomial of α and $g \in K[X]$ the minimal polynomial of β. Suppose that

$$f = \prod_{i=1}^{r} (X - \alpha_i) \in \overline{K}[X] \quad \text{and} \quad g = \prod_{j=1}^{s} (X - \beta_j) \in \overline{K}[X]\,,$$

where $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$, $\beta = \beta_1, \beta_2, \ldots, \beta_s$, and $\beta_1, \ldots, \beta_s$ are distinct. Since K is infinite, there exists some $c \in K$ such that $\alpha_i + c\beta_k \ne \alpha + c\beta$ for all $i \in [1, r]$ and $k \in [2, s]$, and we set $\vartheta = \alpha + c\beta$. Then $g(\beta) = 0$, $f(\vartheta - c\beta) = 0$, and β is the unique common zero of g and $f(\vartheta - cX) \in K(\vartheta)[X]$, since $\vartheta - c\beta_k = \alpha + c\beta - c\beta_k \notin \{\alpha_1, \ldots, \alpha_r\}$ for all $k \in [2, s]$. since β is a simple zero of g, it follows that $X - \beta = \gcd(g, f(\vartheta - cX)) \in K(\vartheta)[X]$ (note that the gcd of two polyomials can be calculated by the eucidean algorithm). Hence $\beta \in K(\vartheta)$, and consequently $K(\alpha, \beta) = K(\vartheta)$. $\square$

1.2. Roots of unity

Remarks and Definitions 1.2.1. Let K be a commutative ring and $n \in \mathbb{N}$.

1. An element $\zeta \in K$ is called an *n-th root of unity* if $\zeta^n = 1$. We denote by $\mu_n(K)$ the set of all n-th roots of unity in K. For $\zeta \in \mu_n(K)$ and $\kappa = k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, we define $\zeta^\kappa = \zeta^k$. If K is a field, then $\mu_n(K) \subset K^\times$ is a cyclic subgroup and $|\mu_n(K)|$ divides n.
2. An n-th root of unity $\zeta \in \mu_n(K)$ is called *primitive* if $\operatorname{ord}(\zeta) = n$. We denote by $\mu_n^*(K)$ the set of all primitive n-th roots of unity. Then
$$\mu_n(\mathbb{C}) = \{\mathsf{e}^{2\pi \mathsf{i} k/n} \mid k \in [1, n]\,,\ (k, n) = 1\}\,,$$
and $\zeta_n = \mathsf{e}^{2\pi\mathsf{i}/n}$ is called the *normalized* primitive n-th root of unity.

   Let K be a field. If $\zeta \in \mu_n^*(K)$, then $|\mu_n(K)| = n$, $\operatorname{char}(K) \nmid n$, $X^n - 1 \in K[X]$ is separable, $\mu_n^*(K) = \{\zeta^\kappa \mid \kappa \in (\mathbb{Z}/n\mathbb{Z})^\times\}$, and $|\mu_n^*(K)| = \varphi(n)$.

   In particular, if K is algebraically closed and $\operatorname{char}(K) \nmid n$, then $|\mu_n(K)| = n$ and $|\mu_n^*(K)| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

lotomicpoly

Theorem and Definition 1.2.2. *Let K be a field, $\overline{K} \supset K$ and algebraically closed extension field, $n \in \mathbb{N}$, $\operatorname{char}(K) \nmid n$ and F the prime ring of K ($F = \mathbb{Z}$ if $\operatorname{char}(K) = 0$, and $F = \mathbb{F}_p$ if $\operatorname{char}(K) = p > 0$).*

1. *If $\zeta \in \mu_n^*(\overline{K})$, then $K(\zeta)$ is the splitting field of $X^n - 1$,*
$$\Phi_n = \prod_{\zeta \in \mu_n^*(\overline{K})} (X - \zeta) \in F[X]\,, \quad \text{and} \quad X^n - 1 = \prod_{d \,|\, n} \Phi_d\,.$$
The polynomial $\Phi_n \in F[X]$ is called the *n-th cyclotomic polynomial* in characteristic $\operatorname{char}(K)$.
2. *In characteristic 0, the polynomial $\Phi_n \in \mathbb{Z}[X]$ is irreducible.*

Proof. 1. By definition,
$$X^n - 1 = \prod_{\xi \in \mu_n(\overline{K})} (X - \xi) = \prod_{d \,|\, n} \prod_{\substack{\xi \in \mu_n(\overline{K}) \\ \operatorname{ord}(\xi) = d}} (X - \xi) = \prod_{d \,|\, n} \Phi_d\,,$$
since, for $d \,|\, n$, $\mu_d(\overline{K}) = \{\xi \in \mu_n(\overline{K}) \mid \operatorname{ord}(\xi) = d\}$. If $\zeta \in \mu_n^*(\overline{K})$, then $\mu_n(\overline{K}) = \langle \zeta \rangle$, and therefore $K(\zeta)$ is the splitting field of $X^n - 1$.

Now we prove $\Phi_n \in F[X]$ by induction on n. Clearly, $\Phi_1 = X - 1 \in F[X]$. Suppose that $n > 1$ and $\Phi_d \in F[X]$ for all $d < n$. Then
$$\Phi_n = \frac{X^n - 1}{\prod_{\substack{d \,|\, n \\ d < n}} \Phi_d} \in F[X]$$
since the polynomial division of monic polynomials can be performed in $F[X]$.

2. Let $\zeta \in \mu_n^*(\mathbb{C})$ and $f \in \mathbb{Q}[X]$ the minimal polynomial of ζ over $\mathbb{Q}$. Then $X^n - 1 = fh$ for some monic polyomial $h \in \mathbb{Q}[X]$, and by Gauß' Lemma we obtain $f,\, h \in \mathbb{Z}[X]$. It suffices to prove:

A. If $p \in \mathbb{P}$ is a prime, $p \nmid n$, $\xi \in \mathbb{C}$ and $f(\xi) = 0$, then $f(\xi^p) = 0$.

B. $f(\xi) = 0$ for all $\xi \in \mu_n^*(\mathbb{C})$.

Indeed, by **B** if follows that $\Phi_n \mid f$, and as f is irreducible, we obtain $\Phi_n = f$.

Proof of **A.** Assume to the contrary that there is some prime $p \in \mathbb{P}$ such that $p \nmid n$, and there is some $\xi \in \mathbb{C}$ such that $f(\xi) = 0$ and $f(\xi^p) \ne 0$. Then ξ and ξ^p are zeros of $X^n - 1$, and therefore $h(\xi^p) = 0$. Hence ξ is a zero of $h(X^p)$, and as f is the minimal polynomial of ξ, we obtain $h(X^p) = fg$ for some polynomial $g \in \mathbb{Z}[X]$ (again by Gauß' Lemma). For a polynomial $q \in \mathbb{Z}[X]$, let $\overline{q} \in \mathbb{F}_p[X]$ be the residue class polynomial. Since $\overline{a}^p = \overline{a}$ for all $a \in \mathbb{Z}$, we obtain $\overline{h(X^p)} = \overline{h}^p = \overline{f}\,\overline{g}$, and therefore $\gcd(\overline{f}, \overline{h}) = \psi \in \mathbb{F}_p[X] \setminus \mathbb{F}_p$. Since $X^n - \overline{1} = \overline{f}\,\overline{h}$, this implies $\psi^2 \mid X^n - \overline{1}$, a contradition, since $X^n - \overline{1} \in \mathbb{F}_p[X]$ is separable.

Proof of **B.** Assume the contrary and observe that $\mu_n^*(\mathbb{C}) = \{\zeta^q \mid q \in \mathbb{N},\ (q,n) = 1\}$. Let $q \in \mathbb{N}$ be minimal such that $(q,n) = 1$ and $f(\zeta^q) \ne 0$. By **A**, q is not a prime, and thus $q = rp$ for some prime p and $r \ge 2$. Then $f(\zeta^r) = 0$, and by **A** also $f(\zeta^q) = 0$, a contradiction. $\square$

Remarks and Definitions 1.2.3. Let $n \in \mathbb{N}$.

1. $\mathbb{Q}^{(n)} \subset \mathbb{C}$ denotes the splitting field of $X^n - 1$ over $\mathbb{Q}$. If $\zeta \in \mu_n^*(\mathbb{C})$, then $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta)$. $\mathbb{Q}^{(n)}$ is called the *n-th cyclotomic field*, $[\mathbb{Q}^{(n)} : \mathbb{Q}] = \varphi(n)$.
2. If $a \in \mathbb{Q}^\times$ and $\alpha \in \mathbb{C}$ is such that $\alpha^n = a$, then
$$X^n - a = \prod_{\zeta \in \mu_n(\mathbb{C})} (X - \zeta\alpha) = \prod_{i=0}^{n-1} (X - \zeta_n^i \alpha)\,,$$
and $\mathbb{Q}^{(n)}(\alpha) = \mathbb{Q}(\zeta, \sqrt[n]{a}\,)$ is the splitting field of $X^n - a$ (on account of ambiguity we usually avoid the notation $\sqrt[n]{a}$).

1.3. Galois theory

igkeitssatz

Theorem 1.3.1 (Dedekind's Independence Theorem)**.** *Let K be a field, $(M, \cdot)$ a monoid and $\sigma_1, \ldots, \sigma_n \colon H \to K^\times$ distince monoid homomorphisms. Then $(\sigma_1, \ldots, \sigma_n) \in \mathrm{Map}(M, K)$ is linearly independent over K.*

Proof. By induction on n.

$n = 1$: $\sigma_1 \ne 0$ is linearly independent.

$n \ge 2$, $n - 1 \to n$: Let $\lambda_1, \ldots, \lambda_n \in K$ be such that $\lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n = 0 \colon M \to K$. By definition,
$$\sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0 \quad \text{for all } x \in M.$$
Let $y \in M$ be such that $\sigma_1(y) \ne \sigma_n(y)$. Then it follows that
$$0 = \sum_{i=1}^{n} \lambda_i \sigma_i(xy) = \sum_{i=1}^{n} \lambda_i \sigma_i(x) \sigma_i(y) \quad \text{and} \quad 0 = \sum_{i=1}^{n} \lambda_i \sigma_i(x) \sigma_n(y) \quad \text{for all } x \in M\,,$$
hence also
$$0 = \sum_{i=1}^{n-1} \lambda_i \,[\,\sigma_i(y) - \sigma_n(y)\,]\, \sigma_i(x)\,, \quad \text{and therefore} \quad 0 = \sum_{i=1}^{n-1} \lambda_i \,[\,\sigma_i(y) - \sigma_n(y)\,]\, \sigma_i\,.$$

By the induction hypothesis, $\lambda_i\,[\,\sigma_i(y)-\sigma_n(y)\,] = 0$ for all $i\in[1,n-1]$, hence $\lambda_1=0$, and consequently $\lambda_2\sigma_2+\ldots+\lambda_n\sigma_n=0$. Again by the induction hypothesis, it follows that also $\lambda_2=\ldots=\lambda_n=0$. □

Remark and Definition 1.3.2.

1. For a field extension L/K, we denote by $\operatorname{Hom}_K(L,L)$ the set of all K-homomorphisms $L\to L$, and by $\mathsf{Gal}(L/K)\subset\mathsf{Aut}(L)$ the set of all K-automorphisms of L. If L/K is algebraic, then $\operatorname{Hom}_K(L,L)=\mathsf{Gal}(L/K)$.
2. Let $H\subset\operatorname{Aut}(L)$ a subgroup. Then it is easily checked that

$$L^H=\{x\in L\mid\sigma(x)=x \text{ for all } \sigma\in H\}\subset L$$

is a subfield. It is called that *fixed field* of H.

`artin` **Theorem 1.3.3** (Artin's Theorem)**.** *Let L be a field and $G<\mathsf{Aut}(L)$ a finite subgroup. Then L/L^G is a finite galois field extension satisfying $[L\colon L^G]=|G|$ and $\mathsf{Gal}(L/L^G)=G$.*

Proof. We set $K=L^G$, $n=|G|$, $G=\{\sigma_1,\ldots,\sigma_n\}$, and we denote by $\overline{K}\supset L$ an algebraically closed extension field. It suffices to prove that $[L:K]\le n$. Indeed, since $G\subset\mathsf{Gal}(L/K)$, this implies

$$n=|G|\le|\mathsf{Gal}(L/K)|\le|\operatorname{Hom}_K(L,\overline{K})|=[L\colon K]_{\mathsf{s}}\le[L\colon K]\le n\,,$$

hence $[L\colon K]=|G|$, $\mathsf{Gal}(L/K)=G$, L/K is normal since $\operatorname{Hom}_K(L,\overline{K})=\mathsf{Gal}(L/K)$, and L/K is separable since $[L\colon K]_{\mathsf{s}}=[L\colon K]$.

The map $S=\sigma_1+\ldots+\sigma_n\colon L\to L$ is K-linear, by Theorem `unabhaengigkeitssatz` 1.3.1 we obtain $S\ne0$, and we assert that $S(L)=K$. Indeed, for all $x\in L$ and $\tau\in G$ we have $\tau S(x)=\tau\sigma_1(x)+\ldots+\tau\sigma_n=S(x)$, since $\{\tau\sigma_1,\ldots,\tau\sigma_n\}=\{\sigma_1,\ldots,\sigma_n\}$, and therefore $S(x)\in L^G=K$. Hence $S(L)\subset K$, and therefore $S(L)=K$. It is now sufficient to prove that any $n+1$ elements of L are linearly dependent over K.

Let $y_1,\ldots,y_{n+1}\in L$. Then the system of linear homogeneous equations

$$\sum_{\nu=1}^{n+1}\sigma_i^{-1}(y_\nu)\,a_\nu=0 \quad\text{for}\quad i\in[1,n] \quad \text{has a non-trivial solution} \quad (a_1,\ldots,a_{n+1})\in L^{n+1}\setminus\mathbf{0}\,.$$

After renumbering $\sigma_1,\ldots,\sigma_n$ if necessary, we may assume that $a_1\ne0$. As $S(a_1L)=S(L)=K$, there exists some $z\in L$ such that $S(a_1z)\ne0$, and we obtain

$$0=\sum_{i=1}^{n}\sigma_i\Big(\sum_{\nu=1}^{n+1}\sigma_i^{-1}(y_\nu)a_\nu z\Big)=\sum_{\nu=1}^{n+1}\sum_{i=1}^{n}\sigma_i(a_\nu z)y_\nu=\sum_{\nu=1}^{n+1}S(a_\nu z)y_\nu\,,$$

which shows the liner dependence of $(y_1,\ldots,y_{n+1})$ over K. □

`galoismain` **Theorem 1.3.4** (Main Theorem of finite Galois Theory)**.** *Let L/K be a finite field extension and $G=\mathsf{Gal}(L/K)$.*

1. *The following assertions are equivalent:*

   (a) L/K *is galois;* (b) $[L\colon K]=|G|$; (c) $K=L^G$.

2. *Let L/K be galois, $\mathcal{Z}(L/K)$ the set of all intermediate fields of L/K and $\mathcal{U}(G)$ the set of all subgroups of G. Then the maps*

$$\begin{cases} \mathcal{Z}(L/K) & \to \quad \mathcal{U}(G) \\ \quad M & \mapsto \ \mathsf{Gal}(L/M) \end{cases} \quad \textit{and} \quad \begin{cases} \mathcal{U}(G) & \to \ \mathcal{Z}(L/K) \\ \quad H & \mapsto \quad L^H \end{cases}$$

are mutually inverse inclusion-reversing bijections. In particular, if M and M' are intermediate fields of L/K, $H = \mathsf{Gal}(L/M)$ and $H' = \mathsf{Gal}(L/M')$, then:

- $M \subset M' \iff H \supset H'$.
- $MM' = L^{H \cap H'}$ *and* $H \cap H' = \mathsf{Gal}(L/MM')$.
- $M \cap M' = L^{\langle H, H' \rangle}$ *and* $\langle H, H' \rangle = \mathsf{Gal}(L/M \cap M')$.

3. *Let $K \subset M \subset L$ be an intermediate field and $H = \mathsf{Gal}(L/M)$.*
   (a) *For all $\sigma \in G$, we have $\mathsf{Gal}(L/\sigma M) = \sigma H \sigma^{-1}$.*
   (b) *Let L/K be galois. Then M/K is galois if and only if $H \lhd G$, and then there is an isomorphism $G/H \xrightarrow{\sim} \mathsf{Gal}(M/K)$, given by $\sigma H \mapsto \sigma \,|\, M$ for all $\sigma \in G$.*

Proof. Let $\overline{K} \supset L$ be an algebraically closed extension field.

1. (a) $\Leftrightarrow$ (b) Note that $|G| \le |\mathrm{Hom}_K(L, \overline{K})| = [L\!:\!K]_{\mathsf{s}} \le [L\!:\!K]$. Here the first inequality is an equality if and only if L/K is normal, and the second inequality is an equality if and only if L/K is separable. Hence L/K is galois if and oly if $[L\!:\!K] = |G|$.

(b) $\Leftrightarrow$ (c) Since $K \subset L^G \subset L$, Theorem 1.3.3 implies $[L\!:\!K] = [L\!:\!L^G]\,[L^G\!:\!K] = |G|\,[L^G\!:\!K]$, and therefore $K = L^G$ if and only if $[L\!:\!K] = |G|$.

2. Assume that $M \in \mathcal{Z}(L/K)$ and $H = \mathsf{Gal}(L/M)$. Since L/K is galois, L is the splitting field of some separable polynomial $f \in K[X] \setminus K$. But then L also the splitting field of f over M, and therefore L/M is normal. Hence L/M galoissch, and $M = L^H$ by 1.

If $H < G$ is a subgroup and $M = L^H$, then $\mathsf{Gal}(L/L^H) = H$ by Theorem 1.3.3. Hence the maps described in the Theorem are mutually inverse bijections, and obviously they are inclusion-reversing. From this the extra assertions follow. Indeed, MM' is the smallest field containing both M and M', and $M \cap M'$ is the largest field contained in both M and M'. On the other hand, $H \cap H'$ is the largest subroup contained in both H and H', and $\langle H, H' \rangle$ is the smallest subgroup containing both H and H'.

3. (a) Let $\sigma \in G$. Then we obtain, for all $\tau \in G$: $\tau \in \mathsf{Gal}(L/\sigma M) \iff (\forall x \in M)\ \tau\sigma x = \sigma x \iff (\forall x \in M)\ \sigma^{-1}\tau\sigma(x) = x \iff \sigma^{-1}\tau\sigma \in H \iff \tau \in \sigma H \sigma^{-1}$. Hence $\mathsf{Gal}(L/\sigma M) = \sigma H \sigma^{-1}$.

(b) By definition, M/K is galois if and only if $\varphi(M) \subset M$ for all $\varphi \in \mathrm{Hom}_K(M, \overline{K})$. Since L/K is galois, the map $G \to \mathrm{Hom}_K(M, \overline{K})$, defined by $\sigma \mapsto \sigma \,|\, M$, is surjective. Hence M/K is galois if and only if $\sigma M \subset M$ (and then $\sigma M = M$) for all $\sigma \in G$. By 2., this holds if and only if $\mathsf{Gal}(L/\sigma M) = \mathsf{Gal}(L/M)$, and, by (a), this is equivalent to $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, and thus to $H \lhd G$.

Assume now that $H \lhd G$. Then the map $G \to \mathsf{Gal}(M/K)$, defined by $\sigma \mapsto \sigma \,|\, M$, is a group epimorphism with kernel $H = \mathsf{Gal}(L/M)$, and therefore it defines an isomorphism $G/H \xrightarrow{\sim} \mathsf{Gal}(M/K)$, given by $\sigma H \mapsto \sigma \,|\, M$ for all $\sigma \in G$. □

`oisshifting` **Theorem 1.3.5** (Shifting Theorem of Galois Theory)**.** *Let $K \subset L$, $M \subset \overline{K}$ be fields.*

1. *Let L/K be a finite galois extension. Then LM/M is also a finite galois extension, and the map*
$$\rho\colon \mathsf{Gal}(LM/M) \xrightarrow{\sim} \mathsf{Gal}(L/L\cap M) \subset \mathsf{Gal}(L/K)\,, \quad \textit{defined by} \quad \rho(\sigma) = \sigma\,|\,L\,,$$
is an isomorphism. In particular, $[LM\colon M] = [L\colon L\cap M] \,|\, [L\colon K]$.
2. *Let L/K and M/K be finite galois extensions and $L\cap M = K$. Then LM/K is a finite galois extension, and the map*
$$\rho\colon \mathsf{Gal}(LM/K) \xrightarrow{\sim} \mathsf{Gal}(L/K)\times\mathsf{Gal}(M/K)\,, \quad \textit{defined by} \quad \rho(\sigma) = (\sigma\,|\,L, \sigma\,|\,M)$$
is an isomorphism.

Proof. 1. We may assume that $\overline{K}$ is algebraically closed. L is the splitting field of some separable polynomial $f \in K[X]\setminus K$, and LM is the splitting field of f over M. Hence LM/M is finite galois. If $\sigma \in \mathsf{Gal}(LM/M)$, then $\sigma\,|\,L \in \mathrm{Hom}_K(L,\overline{K})$ and $\sigma\,|\,L\cap M = \mathrm{id}_{L\cap M}$, hence $\sigma\,|\,L \in \mathsf{Gal}(L/LM)$, and the map $\rho\colon \mathsf{Gal}(LM/M) \to \mathsf{Gal}(L/L\cap M)$, defined by $\sigma \mapsto \sigma\,|\,L$, is a group homomorphism. If $\sigma \in \ker(\rho)$, then $\sigma\,|\,L = \mathrm{id}_L$, and as $\sigma\,|\,M = \mathrm{id}_M$ it follows that $\sigma = \mathrm{id}_{LM}$. Hence ρ is a monomorphism. If $H = \rho\big(\mathsf{Gal}(LM/M)\big)$, then $L\cap M \subset L^H$, and if $z \in L^H$, then $\sigma(z) = z$ for all $\sigma \in \mathsf{Gal}(LM/M)$, and therefore $z \in M$. Hence $L^H = L\cap M$, and $H = \mathsf{Gal}(L/L\cap M)$.

2. Let L be the splitting fiels of a separable polynomial $f \in K[X]\setminus K$ and M the splitting field of a separable polynomial $g \in K[X]\setminus K$. If $q = \gcd(f,g)$, then LM is the splitting field of the separable polynomial $q^{-1}fg$, and therefore it is a finite galois extension. Obviously, ρ is a group monomorphism, and we must prove that it is surjective. Thus let $(\tau_1,\tau_2) \in \mathsf{Gal}(L/K)\times\mathsf{Gal}(M/K)$. By 1., there are isomorphisms $\mathsf{Gal}(LM/L) \xrightarrow{\sim} \mathsf{Gal}(M/K)$, given by $\tau \mapsto \tau\,|\,M$, and $\mathsf{Gal}(LM/M) \xrightarrow{\sim} \mathsf{Gal}(L/K)$, given by $\tau \mapsto \tau\,|\,L$. Hence there exists some $(\sigma_1,\sigma_2) \in \mathsf{Gal}(LM/M)\times\mathsf{Gal}(LM/L) \subset \mathsf{Gal}(LM/K)\times\mathsf{Gal}(LM/K)$ such that $\sigma_1\,|\,L = \tau_1$ and $\sigma_2\,|\,M = \tau_2$. Hence $\rho(\sigma_1\circ\sigma_2) = (\tau_1,\tau_2)$. □

Theorem 1.3.6 (Cyclotomic extensions). *Let K be a field, $n \in \mathbb{N}$, $\mathrm{char}(K) \nmid n$, L a splitting field of $X^n - 1$ over K, $G = \mathsf{Gal}(L/K)$ and $\zeta \in \mu_n^*(L)$. For every $\sigma \in G$, there is a unique $\kappa = \theta(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sigma(\zeta) = \zeta^\kappa$. The map $\theta\colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$ is a group monomorphism, and for all $\xi \in \mu_n(L)$ and $\sigma \in G$ we have $\sigma(\xi) = \xi^{\theta(\sigma)}$. In particular, θ does not depend on ζ. If $K = \mathbb{Q}$, then θ is an isomorphism.*

Proof. If $\zeta \in \mu_n^*(L)$ and $\sigma \in G$, then $\sigma(\zeta) \in \mu_n^*(G)$, and thus there exists a unique $\theta(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sigma(\zeta) = \zeta^{\theta(\sigma)}$. If $\sigma, \tau \in G$, then $\zeta^{\theta(\sigma\tau)} = \sigma\tau(\zeta) = \sigma(\zeta^{\theta(\tau)}) = \sigma(\zeta)^{\theta(\tau)} = \zeta^{\theta(\sigma)\theta(\tau)}$, and therefore $\theta\colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$ is a group homomorphism. If $\sigma \in \ker(\theta)$, then $\sigma(\zeta) = \zeta^{\theta(\sigma)} = \zeta^{1+n\mathbb{Z}} = \zeta$, and thus $\sigma = \mathrm{id}$. Hence σ is a monomorphism, and if $K = \mathbb{Q}$, then it is an isomorphism by Theorem `cyclotomicpoly` 1.2.2. If $\xi \in \mu_n(L)$, then there is some $\lambda \in \mathbb{Z}/n\mathbb{Z}$ such that $\xi = \zeta^\lambda$, and we obtain, for all $\sigma \in G$, $\sigma(\xi) = \sigma(\zeta)^\lambda = \zeta^{\theta(\sigma)\lambda} = \xi^{\theta(\sigma)}$. Hence $L^H = L\cap M$, and therefore $H = \mathsf{Gal}(L/L\cap M)$. □

Theorem 1.3.7 (Cyclic extensions). *Let K be a field, $n \in \mathbb{N}$ and $\mu_n^*(K) \neq \emptyset$.*

1. *Let $a \in K^\times$, L a splitting field of $X^n - a$ over K, $G = \mathsf{Gal}(L/K)$ and $\alpha \in L$ such that $\alpha^n = a$. Then*
$$X^n - a = \prod_{\zeta \in \mu_n(K)} (X - \zeta\alpha)\,, \quad \text{and} \quad \chi\colon G \to \mu_n(K)\,, \quad \text{defined by} \quad \chi(\sigma) = \frac{\sigma(\alpha)}{\alpha} \ \text{for all } \sigma \in G,$$
is a group monomorphism which does not depend on the choice of α.
2. *Let L/K be a cyclic field extension such that $[L:K] \,|\, n$. Then there is some $\alpha \in L$ such that $\alpha^n \in K$ and $L = K(\alpha)$.*

Proof. 1. The factorization of $X^n - 1$ in L is obvious, and therefore it follows that, for every $\sigma \in G$, there is some $\zeta \in \mu_n(K)$ such that $\sigma(\alpha) = \zeta\alpha$. Therefore there is a map $\chi\colon G \to \mu_n(K)$ such that
$$\chi(\sigma) = \frac{\sigma(\alpha)}{\alpha}\,.$$
If $\alpha_1 \in L$ is another element satisfying $\alpha_1^n = a$, then $\alpha_1 = \xi\alpha$ for some $\xi \in \mu_n(K)$, and therefore
$$\frac{\sigma(\alpha_1)}{\alpha_1} = \frac{\sigma(\xi\alpha)}{\xi\alpha} = \frac{\xi\sigma(\alpha)}{\xi\alpha} = \frac{\sigma(\alpha)}{\alpha}\,.$$
Hence χ does not depend on α, and if σ, $\tau \in G$, then $(\tau\alpha)^n = a$, and therefore
$$\chi(\sigma\tau) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma\tau(\alpha)}{\tau(\alpha)}\,\frac{\tau(\alpha)}{\alpha} = \chi(\sigma)\chi(\tau)\,.$$
Hence χ is a group homomorphism. If $\sigma \in \ker(\chi)$, then $\sigma(\alpha) = \alpha$, and thus $\sigma = \mathrm{id}$. Therefore σ is a monomorphism.

2. Let $G = \mathsf{Gal}(L/K) = \langle\sigma\rangle$, and $[L:K] = m \,|\, n$. If $\zeta \in \mu_n^*(K)$, then $\xi = \zeta^{n/m} \in \mu_m^*(K)$, by Theorem `unabhaengigkeitssatz` 1.3.1 we obtain
$$\Bigl(\sum_{j=0}^{m-1} \xi^{-j}\sigma^j \colon L \to L\Bigr) \ne 0\,, \quad \text{and thus there is some } \beta \in L \text{ such that} \quad \sum_{j=0}^{m-1} \xi^{-j}\sigma^j(\beta) = \alpha \in L^\times\,.$$
We find
$$\sigma(\alpha) = \sum_{j=0}^{m-1} \xi^{-j}\sigma^{j+1}(\beta) = \sum_{j=1}^{m} \xi^{-j+1}\sigma^j(\beta) = \xi\alpha\,, \quad \text{hence} \quad \sigma(\alpha^m) = \alpha^m\,, \quad \text{and thus} \quad \alpha^m \in K\,.$$
By definition, $K(\alpha) \subset L$, we assert that $K(\alpha) = L$, and for this we prove that $\mathsf{Gal}(L/K(\alpha)) = \{\mathrm{id}\}$. Let $d \in [0, m-1]$ be such that $\sigma^d \in \mathsf{Gal}(L/K(\alpha))$. Then $\alpha = \sigma^d(\alpha) = \xi^d\alpha$, and therefore $d = 0$. □

1.4. Norms, traces and discriminants

Definition 1.4.1. Let K be a field, A a commuatative K-algebra and $\dim_K(A) = n \in \mathbb{N}$. For $a \in A$ let $\mu_a\colon A \to A$ be defined by $\mu_a(x) = ax$ for all $x \in A$. μ_a is a K-linear map, and we define the *norm* $\mathsf{N}_{A/K}(a)$ and the *trace* $\mathsf{Tr}_{A/K}(a)$ of a for A/K by
$$\mathsf{N}_{A/K}(a) = \det(\mu_a) \quad \text{and} \quad \mathsf{Tr}_{A/K}(a) = \operatorname{trace}(\mu_a)\,.$$

Remarks 1.4.2. Let K be a field, A a commutative K-algebra und $\dim_K(A) = n \in \mathbb{N}$.

1. Let $\boldsymbol{u} = (u_1, \ldots, u_n) \in A^n$ be a K-basis of A. For $a \in A$, let $M_a \in \mathsf{M}_n(K)$ be the matrix of μ_a with respect to $\boldsymbol{u}$. Then $a\boldsymbol{u} = \boldsymbol{u}M_a$, $\mathsf{N}_{A/K}(a) = \det(M_a)$ and $\mathsf{Tr}_{A/K}(a) = \operatorname{trace}(M_a)$.
2. If $a, b \in A$ and $\lambda \in K$, then $\mu_{ab} = \mu_a \circ \mu_b$, $\mu_{\lambda a} = \lambda \mu_a$ and $\mu_{a+b} = \mu_a + \mu_b$. Consequently,
$$\mathsf{N}_{A/K}(ab) = \mathsf{N}_{A/K}(a)\mathsf{N}_{A/K}(b)\,, \quad \mathsf{N}_{A/K}(\lambda a) = \lambda^n \mathsf{N}_{A/K}(a)\,, \quad \mathsf{N}_{A/K}(\lambda 1_A) = \lambda^n\,, \quad \text{and}$$
$$\mathsf{Tr}_{A/K}(a+b) = \mathsf{Tr}_{A/K}(a) + \mathsf{Tr}_{A/K}(b)\,, \quad \mathsf{Tr}_{A/K}(\lambda a) = \lambda \mathsf{Tr}_{A/K}(a)\,, \quad \mathsf{Tr}_{A/K}(\lambda 1_A) = n\lambda\,.$$
3. Let $r \in \mathbb{N}$ and $A = A_1 \times \ldots \times A_r$ the direct product of commutative algebras $A_1, \ldots, A_r$ (A is the external direct product of the vector spaces $A_1, \ldots, A_r$, equipped with the component-wise multiplication).

   For $a = (a_1, \ldots, a_r) \in A$, we obtain $\mu_a = (\mu_{a_1}, \ldots, \mu_{a_r}) \colon A_1 \times \ldots \times A_r \to A_1 \times \ldots \times A_r$, and therefore
$$\mathsf{N}_{A/K}(a) = \prod_{i=1}^{r} \mathsf{N}_{A_i/K}(a_i) \quad \text{and} \quad \mathsf{Tr}_{A/K}(a) = \sum_{i=1}^{r} \mathsf{Tr}_{A_i/K}(a_i)\,.$$

`normspur`

Theorem 1.4.3. *Let L/K be a finite field extension, $[L:K] = n$, $q = [L:K]_{\mathsf{i}}$ the degree of inseparability of L/K (hence $[L:K] = [L:K]_{\mathsf{s}}[L:K]_{\mathsf{i}}$) and $\overline{K} \supset L$ an algebraically closed extension field.*

1. *Let $x \in L$, $[K(x):K] = d$, $g = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in K[X]$ the minimal polynomial of x over K and $[L:K(x)] = m$ (hence $n = md$). Then*
$$\mathsf{N}_{L/K}(x) = (-1)^n a_0^m \quad \textit{and} \quad \mathsf{Tr}_{L/K}(x) = -ma_{d-1}\,.$$
2. *If $x \in L$, then*
$$\mathsf{N}_{L/K}(x) = \prod_{\sigma \in \operatorname{Hom}_K(L,\overline{K})} \sigma(x)^q \qquad \textit{and} \qquad \mathsf{Tr}_{L/K}(x) = q \sum_{\sigma \in \operatorname{Hom}_K(L,\overline{K})} \sigma(x)\,.$$
   In particular:
   - (a) *If L/K is inseparable, then $\mathsf{Tr}_{L/K} = 0$.*
   - (b) *If L/K is galois and $G = \mathsf{Gal}(L/K)$, then*
$$\mathsf{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \qquad \textit{and} \qquad \mathsf{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)\,.$$
3. *If $K \subset M \subset L$ is an intermediate field, then*
$$\mathsf{N}_{L/K} = \mathsf{N}_{M/K} \circ \mathsf{N}_{L/M} \quad \textit{and} \quad \mathsf{Tr}_{L/K} = \mathsf{Tr}_{M/K} \circ \mathsf{Tr}_{L/M}\,.$$

PROOF. 1. $\boldsymbol{u} = (1, x, \ldots, x^{d-1})$ is a K-basis of $K(x)$, and
$$x\,(1, x, \ldots, x^{d-1}) = (1, x, \ldots, x^{d-1})\,T\,, \quad \text{where} \quad T = \begin{pmatrix} 0 & 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & \ldots & 0 & -a_2 \\ . & . & \ldots & \ldots & . & . \\ 0 & 0 & \ldots & \ldots & 1 & -a_{d-1} \end{pmatrix},$$
$\operatorname{trace}(T) = -a_d$ and $\det(T) = (-1)^d a_0$. Let now $(v_1, \ldots, v_m)$ be a $K(x)$-basis of L. Then it follows that $(v_1\boldsymbol{u}, \ldots, v_m\boldsymbol{u})$ is a K-Basis of L, and $x\,(v_1\boldsymbol{u}, \ldots, v_m\boldsymbol{u}) = (v_1\boldsymbol{u}, \ldots, v_m\boldsymbol{u})\,T^{(m)}$, where

$T^{(m)} = \mathrm{diag}(T, \ldots, T)$ is a diagonal box matrix with $\det(T^{(m)} = \det(T)^m$ and $\mathrm{trace}(T^{(m)} = m\,\mathrm{trace}(T)$. Hence we obtain

$$\mathsf{N}_{L/K}(x) = \det(T^{(m)}) = ((-1)^d a_0)^m = (-1)^n a_0^m \quad \text{and} \quad \mathsf{Tr}_{L/K}(x) = \mathrm{trace}(T^{(m)}) = -m a_{d-1}\,.$$

2. Let $x \in L$, $g = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in K[X]$ the minimal polynomial of x over K, $q_0 = [K(x):K]_{\mathsf{i}}$ the degree of inseparability of x over K and $[L:K(x)] = m$ (hence $d = [K(x):K]$ and $n = md$). Let $H = \mathrm{Hom}_K(K(x), \overline{K})$. Then $|H| = [K(x):K]_{\mathsf{s}}$, $q_0|H| = d$, and

$$\frac{q}{q_0}\,[L:K(x)]_{\mathrm{s}} = [L:K(x)]_{\mathrm{s}}\,\frac{[L:K]\,[K(x):K]_{\mathrm{s}}}{[L:K]_{\mathrm{s}}\,[K(x):K]} = [L:K(x)] = m\,.$$

Now we obtain

$$g = \prod_{\varphi \in H} (X - \varphi(x))^{q_0}\,,$$

hence

$$a_{d-1} = -q_0 \sum_{\varphi \in H} \varphi(x) \quad \text{and} \quad a_0 = \prod_{\varphi \in H} (-\varphi(x))^{q_0} = (-1)^d \prod_{\varphi \in H} \varphi(x)^{q_0}\,.$$

Now it follows that

$$\begin{aligned}\prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(x)^q &= \prod_{\varphi \in H} \prod_{\substack{\sigma \in \mathrm{Hom}_K(L,\overline{K}) \\ \sigma \,|\, K(x) = \varphi}} \sigma(x)^q = \prod_{\varphi \in H} \varphi(x)^{q\,[L:K(x)]_{\mathrm{s}}} = [(-1)^d a_0]^{[L:K(x)]_{\mathrm{s}} q/q_0} \\ &= (-1)^n a_0^m = \mathsf{N}_{L/K}(x)\end{aligned}$$

and

$$\begin{aligned} q \sum_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(x) &= q \sum_{\varphi \in H} \sum_{\substack{\sigma \in \mathrm{Hom}_K(L,\overline{K}) \\ \sigma \,|\, K(x) = \varphi}} \sigma(x) = q\,[L:K(x)]_{\mathrm{s}} \sum_{\varphi \in H} \varphi(x) = -\frac{q}{q_0}[L:K(x)]_{\mathrm{s}} a_{d-1} \\ &= -m a_{d-1} = \mathsf{Tr}_{L/K}(x)\,.\end{aligned}$$

3. Let $K \subset M \subset L$ be an intermediate field, $x \in L$, $q_1 = [M:K]_{\mathsf{i}}$ and $q_2 = [L:M]_{\mathsf{i}}$. Then $q = q_1 q_2$, and

$$\mathsf{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} \sigma(x)^q = \prod_{\varphi \in \mathrm{Hom}_K(M,\overline{K})} \prod_{\substack{\sigma \in \mathrm{Hom}_K(L,\overline{K}) \\ \sigma \,|\, M = \varphi}} \sigma(x)^q\,.$$

If $\widetilde{L} \subset \overline{K}$ is a normal closure of L/K, then $\mathrm{Hom}_K(M, \overline{K}) = \mathrm{Hom}_K(M, \widetilde{L})$, $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(L, \widetilde{L})$ and $\mathrm{Hom}_M(L, \overline{K}) = \mathrm{Hom}_M(L, \widetilde{L})$. Let now $\varphi \in \mathrm{Hom}_K(M, \widetilde{L})$ and $\widetilde{\varphi} \in \mathsf{Gal}(\widetilde{L}/K)$ such that $\widetilde{\varphi}\,|\,M = \varphi$.

If $\sigma \in \mathrm{Hom}_K(L, \widetilde{L})$ and $\sigma\,|\,M = \varphi$, then $\widetilde{\varphi} \circ \sigma\,|\,M = \mathrm{id}_M$, and therefore $\psi = \widetilde{\varphi}^{-1} \circ \sigma \in \mathrm{Hom}_M(L, \widetilde{L})$. Conversely, if $\psi \in \mathrm{Hom}_M(L, \widetilde{L})$, then $\sigma = \widetilde{\varphi} \circ \psi \in \mathrm{Hom}_K(L, \widetilde{L})$ and $\sigma\,|\,M = \varphi$. Hence the assignment $\sigma \mapsto \psi = \widetilde{\varphi}^{-1} \circ \sigma$ defines a bijective map $\{\sigma \in \mathrm{Hom}_K(L, \overline{K}) \mid \sigma\,|\,M = \varphi\} \to \mathrm{Hom}_M(L, \overline{K})$, and therefore we obtain

$$\prod_{\substack{\sigma \in \mathrm{Hom}_K(L,\overline{K}) \\ \sigma \,|\, M = \varphi}} \sigma(x)^q = \prod_{\psi \in \mathrm{Hom}_M(L,\overline{K})} \widetilde{\varphi} \circ \psi(x)^{q_2 q_1} = \widetilde{\varphi}\Big(\prod_{\psi \in \mathrm{Hom}_M(L,\overline{K})} \psi(x)^{q_2} \Big)^{q_1} = \varphi(\mathsf{N}_{L/M}(x))^{q_1}\,,$$

hence

$$\mathsf{N}_{L/K}(x) = \prod_{\varphi\in\operatorname{Hom}_K(M,\overline{K})} \varphi(\mathsf{N}_{L/M}(x)^{q_1} = \mathsf{N}_{M/K}\circ\mathsf{N}_{L/M}(x)\,.$$

The assertion concerning the trace is proved in the same way. □

skriminante

Remark and Definition 1.4.4. Let K be a field, $g \in K[X]$ a monic polynomial, $n = \deg(g) \in \mathbb{N}$, $L \supset K$ an extension field and $\alpha_1, \ldots, \alpha_n \in L$ such that $g = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$. Then the *discriminant* $\Delta(g)$ of g is defined by

$$\Delta(g) = \prod_{1\le i<j\le n} (\alpha_j-\alpha_i)^2 = (-1)^{\binom{n}{2}} \prod_{\substack{i,\,j=1\\ i\ne j}}^{n} (\alpha_j-\alpha_i)$$

By definition, $\Delta(g) = 0$ if and only if g is inseparable. We assert that $\Delta(g) \in K$, and $\Delta(g)$ is independent of the field L used for the definition.

Proof. Let g separable, L a splitting field of g and $G = \mathsf{Gal}(L/K)$. Every $\sigma \in G$ induces a permutation of $\{\alpha_1, \ldots, \alpha_n\}$, hence $\sigma(\Delta(g)) = \Delta(g)$, and therefore $\Delta(g) \in L^G = K$. Let now L' be any extension field of K such that g splits in L', and let $L_1 \supset L$ be any algebraically closed field. Then there exists some $\varphi \in \operatorname{Hom}_K(L, L_1)$, $g = (X-\varphi(\alpha_1))\cdot\ldots\cdot(X-\varphi(\alpha_n))$, and

$$\prod_{1\le i<j\le n} \bigl(\varphi(\alpha_j)-\varphi(\alpha_i)\bigr)^2 = \varphi(\Delta(g)) = \Delta(g)\,. \quad \square$$

Suppose that $f = X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$. Then

$$\Delta(f) = a_1^2 - 4a_2 \ \text{ if } \ n = 2, \quad \text{and} \quad \Delta(f) = -4a_1^3a_3 + a_1^2a_2^2 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2 \ \text{ if } \ n = 3\,.$$

Definition 1.4.5. Let L/K be a finite field extension and $n = [L:K]$. For an n-tuple $(u_1, \ldots, u_n) \in L^n$ we define its *discriminant* $\Delta(u_1, \ldots, u_n)$ by

$$\Delta_{L/K}(u_1, \ldots, u_n) = \det\bigl(\mathsf{Tr}_{L/K}(u_iu_j)\bigr)_{i,\,j\in[1,n]}\,.$$

If L/K is inseparable, then $\Delta_{L/K}(u_1, \ldots, u_n) = 0$ for all $(u_1, \ldots, u_n) \in L^n$.

skriminante

Theorem 1.4.6. *Let L/K be a finite separable field extension, $[L:K] = n$, $\overline{K} \supset L$ an algebraically closed field and $\operatorname{Hom}_K(L,\overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$.*

1. *For $(u_1, \ldots, u_n) \in L^n$, we have $\Delta_{L/K}(u_1, \ldots, u_n) = \det\bigl(\sigma_\nu(u_i)\bigr)^2_{\nu,\,i\in[1,n]}$.*
2. *If $L = K(\alpha)$ and $g \in K[X]$ is the minimal polynomial of α over K, then*

$$\Delta_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = \Delta(g) = \prod_{1\le\nu<\mu\le n} \bigl(\sigma_\mu(\alpha)-\sigma_\nu(\alpha)\bigr)^2 = (-1)^{\binom{n}{2}}\mathsf{N}_{L/K}(g'(\alpha)) \ne 0\,.$$

3. *Suppose that $\boldsymbol{u} = (u_1, \ldots, u_n)$, $\boldsymbol{v} = (v_1, \ldots, v_n) \in L^n$, and let $T \in \mathsf{M}_n(K)$ be such that $\boldsymbol{u} = \boldsymbol{v}T$. Then $\Delta_{L/K}(u_1, \ldots, u_n) = \Delta_{L/K}(v_1, \ldots, v_n)\,\det(T)^2$.*
4. *An n-tuple $(u_1, \ldots, u_n) \in L^n$ is a K-basis of L if and only if $\Delta_{L/K}(u_1, \ldots, u_n) \ne 0$.*

Proof. 1. With $U = (\sigma_\nu(u_i))_{\nu,\, i \in [1,n]} \in \mathsf{M}_n(\overline{K})$, we obtain

$$U^{\mathsf{t}}U = \Bigl(\sum_{\nu=1}^{n} \sigma_\nu(u_i)\sigma_\nu(u_j)\Bigr)_{i,\, j\in[1,n]} = \Bigl(\sum_{\nu=1}^{n} \sigma_\nu(u_iu_j)\Bigr)_{i,\, j\in[1,n]} = \bigl(\mathsf{Tr}_{L/K}(u_iu_j)\bigr)_{i,\, j\in[1,n]}\,,$$

and therefore $\Delta_{L/K}(u_1,\ldots,u_n) = \det\bigl(\mathsf{Tr}_{L/K}(u_iu_j)\bigr)_{i,\, j\in[1,n]} = \det(U^{\mathsf{t}}U) = \det(U)^2$.

2. As $L = K(\alpha)$, we get $g = (X-\sigma_1(\alpha))\cdot\ldots\cdot(X-\sigma_n(\alpha))$, and 1. implies that

$$\Delta_{L/K}(1,\alpha,\ldots,\alpha^{n-1}) = \det\begin{pmatrix} 1 & \sigma_1(\alpha) & \ldots & \sigma_1(\alpha)^{n-1} \\ 1 & \sigma_2(\alpha) & \ldots & \sigma_2(\alpha)^{n-1} \\ . & . & \ldots & . \\ 1 & \sigma_n(\alpha) & \ldots & \sigma_n(\alpha)^{n-1} \end{pmatrix}^2 = \prod_{1\le\nu<\mu\le n} \bigl(\sigma_\mu(\alpha)-\sigma_\nu(\alpha)\bigr)^2$$
$$= \Delta(g) \ne 0\,,$$

with the famous Vandermonde determinant. Now we calculate

$$g' = \sum_{\nu=1}^{n}\prod_{\substack{i=1\\ i\ne\nu}}^{n}\bigl(X-\sigma_i(\alpha)\bigr)\,, \quad \text{hence} \quad g'(\sigma_\nu(\alpha)) = \prod_{\substack{i=1\\ i\ne\nu}}^{n}\bigl(\sigma_\nu(\alpha)-\sigma_i(\alpha)\bigr) \quad \text{for all} \ \ \nu\in[1,n]\,,$$

and

$$\mathsf{N}_{L/K}(g'(\alpha)) = \prod_{\nu=1}^{n}\sigma_\nu(g'(\alpha)) = \prod_{\nu=1}^{n} g'(\sigma_\nu(\alpha)) = \prod_{\nu=1}^{n}\prod_{\substack{\mu=1\\ \mu\ne\nu}}^{n}\bigl(\sigma_\mu(\alpha)-\sigma_\nu(\alpha)\bigr) = (-1)^{\binom{n}{2}}\Delta(g)\,.$$

3. For $\nu\in[1,n]$, we have $(\sigma_\nu(u_1),\ldots,\sigma_\nu(u_n)) = (\sigma_\nu(v_1),\ldots,\sigma_\nu(v_n))\,T$, and therefore

$$\Delta_{L/K}(u_1,\ldots,u_n) = \det\bigl(\sigma_\nu(u_i)\bigr)^2_{\nu,\, i\in[1,n]} = \det\bigl(\sigma_\nu(v_i)\bigr)^2_{\nu,\, i\in[1,n]}\,\det(T)^2$$
$$= \Delta_{L/K}(v_1,\ldots,v_n)\,\det(T)^2\,.$$

4. By Theorem primitiveselement 1.1.4, there exists some $\alpha\in L$ such that $L = K(\alpha)$. Then $(1,\alpha,\ldots,\alpha^{n-1})$ is a K-basis of L, and $\Delta_{L/K}(1,\alpha,\ldots,\alpha^{n-1}) \ne 0$ by 2. For any $(u_1,\ldots,u_n)\in L^n$, there is some $T\in\mathsf{M}_n(K)$ such that $(u_1,\ldots,u_n) = (1,\alpha,\ldots,\alpha^{n-1})\,T$, and then it follows by 3. that $\Delta_{L/K}(u_1,\ldots,u_n) = \Delta_{L/K}(1,\alpha,\ldots,\alpha^{n-1})\,\det(T)^2$. Hence $\Delta_{L/K}(u_1,\ldots,u_n)\ne 0$ holds if and only if $\det(T)\ne 0$, and this holds if and only if $(u_1,\ldots,u_n)$ is a K-basis of L. ☐

dualbasis

Definition and Theorem 1.4.7. *Let L/K be a finite separable field extension.*

1. *For every K-Basis $(u_1,\ldots,u_n)$ of, L, there exists a unique K-basis $(u_1^*,\ldots,u_n^*)$ of L such that $\mathsf{Tr}_{L/K}(u_iu_j^*) = \delta_{i,j}$ for all $i,\, j\in[1,n]$. $\Delta_{L/K}(u_1^*,\ldots,u_n^*) = \Delta_{L/K}(u_1,\ldots,u_n)^{-1}$.*

   $(u_1^*,\ldots,u_n^*)$ is called the *dual* basis of $(u_1,\ldots,u_n)$.
2. *Suppose that $L = K(\alpha)$, let $g\in K[X]$ be the minimal polynomial of α over K, and suppose that $g = (X-\alpha)(\beta_0+\beta_1X+\ldots+\beta_{n-1}X^{n-1}$, where $\beta_0,\ldots,\beta_{n-1}\in L$. Then*

$$\Bigl(\frac{\beta_0}{g'(\alpha)},\ldots,\frac{\beta_{n-1}}{g'(\alpha)}\Bigr) \quad \textit{is the dual basis of} \ \ (1,\alpha,\ldots,\alpha^{n-1}).$$

BEWEIS. 1. Let $(u_1,\ldots,u_n)$ be a K-basis of L. We must prove that there exists a unique matrix $T\in\mathsf{GL}_n(K)$ with the following property:

If $(u_1^*,\ldots,u_n^*)=(u_1,\ldots,u_n)T$, then $\mathsf{Tr}_{L/K}(u_iu_j^*)=\delta_{i,j}$ for all $i,\,j\in[1,n]$.

Thus let $T=(t_{i,j})_{i,\,j\in[1,n]}\in\mathsf{GL}_n(K)$ and $(u_1^*,\ldots,u_n^*)=(u_1,\ldots,u_n)\,T$. Then it follows that $\Delta_{L/K}(u_1^*,\ldots,u_n^*)=\Delta_{L/K}(u_1,\ldots,u_n)\,\det(T)^2$ and

$$\Delta_{L/K}(u_1,\ldots,u_n)=\det\bigl(\mathsf{S}_{L/K}(u_iu_j)\bigr)_{i,\,j\in[1,n]}\neq 0$$

by Theorem `diskriminante` 1.4.6. For all $i,\,j\in[1,n]$, we have

$$u_j^*=\sum_{\nu=1}^n u_\nu t_{\nu,j}\,,$$

and therefore

$$\mathsf{Tr}_{L/K}(u_iu_j^*)=\sum_{\nu=1}^n\mathsf{Tr}_{L/K}(u_iu_\nu)t_{\nu,j}=\bigl[\bigl(\mathsf{Tr}_{L/K}(u_iu_\nu)\bigr)_{i,\nu\in[1,n]}\,T\bigr]_{i,j}\,.$$

Hence $\mathsf{Tr}_{L/K}(u_iu_j^*)=\delta_{i,j}$ for all $i,\,j\in[1,n]$ if and only if $T=\bigl(\mathsf{Tr}_{L/K}(u_iu_j)\bigr)_{i,\,j\in[1,n]}^{-1}$. This implies the existence and uniqueness of T. Moreover, we obtain $\det(T)=\Delta_{L/K}(u_1,\ldots,u_n)^{-1}$, and therefore $\Delta_{L/K}(u_1',\ldots,u_n')=\Delta_{L/K}(u_1,\ldots,u_n)\det(T)^2=\Delta_{L/K}(u_1,\ldots,u_n)^{-1}$.

2. We must prove that

$$\mathsf{Tr}_{L/K}\Bigl(\alpha^i\frac{\beta_j}{g'(\alpha)}\Bigr)=\delta_{i,j}\quad\text{for all}\quad i,\,j\in[0,n-1]\,,$$

and for this we show that

$$\sum_{j=0}^{n-1}\mathsf{Tr}_{L/K}\Bigl(\alpha^i\frac{\beta_j}{g'(\alpha)}\Bigr)X^j=X^i\in K[X]\quad\text{für alle}\quad i\in[0,n-1]\,.$$

Let $\overline{K}\supset L$ be an algebraically closed extensio field and $\mathrm{Hom}_K(L,\overline{K})=\{\sigma_1,\ldots,\sigma_n\}$. Then $\sigma_1(\alpha),\ldots,\sigma_n(\alpha)$ are distinct, $g=(X-\sigma_1(\alpha))\cdot\ldots\cdot(X-\sigma_n(\alpha))$, and it suffices to prove that

$$\sum_{j=0}^{n-1}\mathsf{Tr}_{L/K}\Bigl(\alpha^i\frac{\beta_j}{g'(\alpha)}\Bigr)\sigma_l(\alpha)^j=\sigma_l(\alpha)^i\quad\text{for all } l\in[1,n]\ \text{ and }\ i\in[0,n-1].$$

We denote the trivial extensions of the homomorphisms σ_ν to the polynomial rings again by σ_ν. Then

$$\sigma_\nu\Bigl(\frac{g}{X-\alpha}\Bigr)=\frac{g}{X-\sigma_\nu(\alpha)}=\sum_{j=0}^{n-1}\sigma_\nu(\beta_j)X^j=\prod_{\substack{k=1\\k\neq\nu}}^n(X-\sigma_k(\alpha))\quad\text{for all}\quad\nu\in[1,n]\,,$$

and then we obtain, for all $i\in[0,n-1]$,

$$\sum_{j=0}^{n-1}\mathsf{Tr}_{L/K}\Bigl(\alpha^i\frac{\beta_j}{g'(\alpha)}\Bigr)\sigma_l(\alpha)^j=\sum_{j=0}^{n-1}\sum_{\nu=1}^n\sigma_\nu(\alpha)^i\,\frac{\sigma_\nu(\beta_j)}{g'(\sigma_\nu(\alpha))}\,\sigma_l(\alpha)^j=\sum_{\nu=1}^n\frac{\sigma_\nu(\alpha)^i}{g'(\sigma_\nu(\alpha))}\,\sum_{j=0}^{n-1}\sigma_\nu(\beta_j)\sigma_l(\alpha)^j$$

$$=\sum_{\nu=1}^n\frac{\sigma_\nu(\alpha)^i}{g'(\sigma_\nu(\alpha))}\,\prod_{\substack{k=1\\k\neq\nu}}^n\bigl(\sigma_l(\alpha)-\sigma_k(\alpha)\bigr)=\frac{\sigma_l(\alpha)^i}{g'(\sigma_l(\alpha))}\,g'(\sigma_l(\alpha)=\sigma_l(\alpha)^i\,.\quad\square$$

CHAPTER 2

Ideal Theory of algebraic integers

2.1. Integral elements

Definition 2.1.1. Let $R \subset S$ be commutative rings.

1. An element $x \in S$ is called *integral* over R if there exists a monoic polynomial $f \in R[X]$ such that $f(x) = 0$. In particular, every $x \in R$ is integral over R (set $f = X - x$).

   By definition, x is integral over R if and only if there exist $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in R$ such that $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$, and every such relation is called an *integral equation* for x over R.
2. $\mathrm{cl}_S(R) = \{x \in S \mid x \text{ is integral over } R\}$ is called the *integral closure* of R in S.
3. S is called *integral over* R and $R \subset S$ is called an *integral ring extension* if $\mathrm{cl}_S(R) = S$ [equivalently, every $x \in S$ is integral over R], and R is called *integrally closed in* S if $\mathrm{cl}_S(R) = R$.
4. A domain is called *integrally closed* if it is integrally closed in its quotient field.

`rialclosed`

Theorem 2.1.2. *Every factorial domain is integrally closed.*

Proof. Let R be a factorial domain, $K = \mathsf{q}(R)$, and assume that there is some $x \in K \setminus R$ which is integral over R. Then $x = a^{-1}b$, where $a,\, b \in R$, $a \neq 0$, and there is some prime element $p \in R$ such that $p \,|\, a$ and $p \nmid b$. Let $x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 = 0$, where $d \in \mathbb{N}$ and $a_0, \ldots, a_{d-1} \in R$. We multiply this equation by a^d and obtain $b^d + ay = 0$ for some $y \in R$. Now $p \,|\, a$ implies $p \,|\, b^d$ and finally $p \,|\, b$, a contradiction. $\square$

`incriterion`

Theorem 2.1.3. *Let $R \subset S$ be commutative rings, $M \subset S$ a finitely generated R-submodule of S, $x \in S$, $xM \subset M$, and suppose that, for all polynomials $g \in R[X]$, $g(x)M = \mathbf{0}$ implies $g(x) = 0$ (that is, M is $R[x]$-torsion-free). Then x is integral over R.*

Proof. Let $M = Ru_1 + \ldots + Ru_m$, where $m \in \mathbb{N}$ and $u_1, \ldots, u_m \in M$. For $j \in [1, m]$, there is a relation

$$xu_j = \sum_{\mu=1}^{m} c_{j,\mu}u_\mu \quad \text{with coefficients} \quad c_{j,\mu} \in R\,, \quad \text{and thus} \quad \sum_{\mu=1}^{m} (\delta_{j,\mu}x - c_{j,\mu})u_j = 0\,.$$

If $T = (\delta_{j,\mu}x - c_{j,\mu})_{j,\mu \in [1,m]} \in \mathsf{M}_m(R)$, $T^{\#}$ denotes its adjoint matrix and $\boldsymbol{u} = (u_1, \ldots, u_m)^{\mathsf{t}}$, then $\det(T)\boldsymbol{u} = T^{\#}T\mathsf{u} = \mathbf{0}$. Hence $\det(T)M = \mathbf{0}$, and since $\det(T) = g(x)$ for some monic polynomial $g \in R[X] \setminus R$, it follows that $g(x) = 0$, and x is integral over R. $\square$

ainintegral

Theorem 2.1.4. *Let $R \subset S$ be commutative rings.*

1. *Assume that $n \in \mathbb{N}$, $x_1, \dots, x_n \in S$, and $S = R[x_1, \dots, x_n]$. Then the following assertions are equivalent:*
   - (a) *S is integral over R.*
   - (b) *For all $i \in [1, n]$, x_i is integral over R.*
   - (c) *$S = R[x_1, \dots, x_n]$ is a finitely generated R-module.*
2. *Let $T \supset S$ be a commutative overring, let S integral over R and $x \in T$ integral over S. Then x is integral over R. In particular, T is integral over R if and only if T is integral over S and S is integral over R.*
3. $\mathrm{cl}_S(R)$ *is a ring which is integrally closed in S and integral over R.*
4. *Let $x \in S$ be integral over R and $\varphi \colon S \to S'$ a ring homomorphism. Then $\varphi(x)$ is integral over $\varphi(R)$. In particular, if $\mathfrak{A} \lhd S$, $\mathfrak{a} = \mathfrak{A} \cap R$, and if we embed $R/\mathfrak{a} \subset S/\mathfrak{A}$ by means of the identification $a + \mathfrak{a} = a + \mathfrak{A}$ for all $a \in R$, then $x + \mathfrak{A}$ is integral over $R/\mathfrak{a}$.*

Proof. 1. (a) $\Rightarrow$ (b) Obvious.

(b) $\Rightarrow$ (c) By induction on n.

$n = 1:$ Suppose that $S = R[x]$ and x is integral over R, say $x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 = 0$, where $d \in \mathbb{N}$ and $a_0, \dots, a_{d-1} \in R$. We set $M = {}_R\langle 1, x, \dots, x^{d-1}\rangle$, and we shall prove that $R[x] = M$. For this, we assert that $x^j \in M$ for all $j \in \mathbb{N}_0$, and we show this by induction on j. For $j < d$, there is nothing to do. Thus suppose that $j \ge d$ and $x^\nu \in M$ for all $\nu \in [0, j-1]$. From the integral equation we get $x^j = -a_{d-1}x^{j-1} - \ldots - a_1x^{j-d+1} - a_0x^{j-d} \in M$.

$n \ge 1$, $n \to n+1:$ By the induction hypothesis, $R[x_1, \dots, x_n]$ is a finitely generated R-module. x_{n+1} is integral over R, hence over $R[x_1, \dots, x_n]$, and therefore $R[x_1, \dots, x_{n+1}] = R[x_1, \dots, x_n][x_{n+1}]$ is a finitely generated $R[x_1, \dots, x_n]$-modulet. Hence $R[x_1, \dots, x_{n+1}]$ is a finitely generated R-module.

maincriterion

(c) $\Rightarrow$ (a) By Theorem 2.1.3, applied with $M = R[x_1, \dots, x_n]$.

2. Suppose that $x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 = 0$, where $d \in \mathbb{N}$ and $a_0, \dots, a_{d-1} \in S$. Then x is integral over $R[a_0, \dots, a_{d-1}]$, and $R[a_0, \dots, a_{d-1}, x] = R[a_0, \dots, a_{d-1}][x]$ is a finitely generated $R[a_0, \dots, a_{d-1}]$-module by 1. As $a_0, \dots, a_{d-1}$ are integral over R, it follows (again by 1.) that $R[a_0, \dots, a_{d-1}]$ is a finitely generated R-module. Hence $R[a_0, \dots, a_{d-1}, x]$ is a finitely generated R-module, and therefore x is integral over R.

3. If x, $y \in \mathrm{cl}_S(R)$, then $R[x, y]$ is a finitely generated R-module, and since $x - y$, $xy \in R[x, y]$, it follows that $\{x - y, xy\} \subset \mathrm{cl}_S(R)$. Hence $\mathrm{cl}_S(R) \subset S$ is a subring. If $x \in S$ is integral over $\mathrm{cl}_S(R)$, then x is integral over R by 2., and thus $x \in S$.

4. If $x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 = 0$ is an integral equation for x over R (where $d \in \mathbb{N}$ and $a_0, \dots, a_{d-1} \in R$), then $\varphi(x)^d + \varphi(a_{d-1})\varphi(x)^{d-1} + \ldots + \varphi(a_1)\varphi(x) + \varphi(a_0) = 0$ is an integral equation for $\varphi(x)$ over $\varphi(R)$. ☐

tegralideal

Theorem 2.1.5. *Let $R \subset S$ be commutative rings such that S is integral over R.*

1. *If $\mathfrak{a} \subsetneq R$ is an ideal of R, then $\mathfrak{a}S = {}_S\langle \mathfrak{a} \rangle \ne S$. In particular, $S^\times \cap R = R^\times$, and if S is a field, then R is a field.*
2. *Let S be a domain and $\mathbf{0} \ne \mathfrak{A} \subset S$ an ideal. Then $\mathfrak{A} \cap R \ne \mathbf{0}$, and if R is a field, then S is a field.*

Proof. 1. Let $\mathfrak{a} \subset R$ be an ideal such that $\mathfrak{a}S = S$. Then there exist some $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathfrak{a}$ and $x_1, \ldots, x_n \in S$ such that $a_1x_1 + \ldots + a_nx_n = 1$. By Theorem mainintegral 2.1.4, $R[x_1, \ldots, x_n]$ is a finitely generated R-module, say $R[x_1, \ldots, x_n] = {}_R\langle b_1, \ldots, b_m\rangle$ for some $m \in \mathbb{N}$ and $b_1, \ldots, b_m \in R[x_1, \ldots, x_n]$. Then there are relations

$$x_\nu = \sum_{j=1}^m c_{\nu,j} b_j \quad \text{and} \quad b_j b_i = \sum_{k=1}^m d_{j,i,k} b_k \quad \text{with coefficients} \quad c_{\nu,j},\ d_{j,i,k} \in R\,,$$

and therefore, for all $i \in [1, m]$,

$$b_i = \sum_{\nu=1}^m a_\nu \sum_{j=1}^m c_{\nu,j} \sum_{k=1}^m d_{j,i,k} b_k = \sum_{k=1}^m a'_{i,k} b_k\,, \quad \text{where} \quad a'_{i,k} = \sum_{\nu=1}^n \sum_{j=1}^m a_\nu c_{\nu,j} d_{j,i,l} \in \mathfrak{a}\,.$$

Thus it follows that

$$\sum_{k=1}^m (\delta_{i,k} - a'_{i,k}) b_k = 0 \quad \text{for all} \quad i \in [1, m]\,.$$

If $T = (\delta_{i,k} - a'_{i,k})_{i,k \in [1,m]} \in \mathsf{M}_n(R)$ and $\boldsymbol{b} = (b_1, \ldots b_m)^{\mathsf{t}}$, then $\det(T)\boldsymbol{b} = T^\# T \boldsymbol{b} = \mathbf{0}$. Hence it follows that $\det(T)R[x_1, \ldots, x_n] = \mathbf{0}$, and therefore $\det(T) = 0$. Expanding the determinant, we obtain $\det(T) \in 1 + \mathfrak{a}$, hence $1 \in \mathfrak{a}$ and thus $\mathfrak{a} = R$.

Clearly, $R^\times \subset S^\times \cap R$, and if $a \in S^\times \cap R$, then $aS = S$ and therefore $aR = R$. If S is a field, then $R^\bullet = R \cap S^\bullet = R \cap S^\times = R^\times$, and therefore R is a field.

2. Let $0 \neq x \in \mathfrak{A}$ and $n \in \mathbb{N}$ minimal such that $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ for some $a_0, \ldots, a_{n-1} \in R$. Then $a_0 \in xS \cap R \subset \mathfrak{A} \cap R$, and we assert that $a_0 \neq 0$. Indeed, if $a_0 = 0$, then $x \neq 0$ implies $x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1 = 0$, contradicting the minimal choice of n.

Let R be a field and $\mathfrak{A} \subset S$ a non-zero ideal. Then $\mathbf{0} \neq \mathfrak{A} \cap R \lhd R$, henc $\mathfrak{A} \cap R = R$ and thus $\mathfrak{A} = S$, since $1 \in \mathfrak{A}$. Therefore S has no non-zero proper ideals, and thus it is also a field. □

gralclosure

Theorem 2.1.6. *Let R be an integrally closed domain, $K = \mathsf{q}(R)$, L/K a finite field extension, and $S = \mathrm{cl}_L(R)$.*

1. *S is an integrally closed domain, $S \cap K = R$, and $L = \mathsf{q}(S) = \{q^{-1}x \mid x \in S,\ q \in R^\bullet\}$. In particular, S contains a K-basis of L.*
2. *Let $\alpha \in L$ and $g \in K[X]$ the minimal polynomial of α over K. Then α is integral over R if and only if $g \in R[X]$. In particular, if $\alpha \in S$, then $\mathsf{N}_{L/K}(\alpha) \in R$ and $\mathsf{Tr}_{L/K}(\alpha) \in S$, and if $(u_1, \ldots, u_n) \in S^n$ is a K-basis of L, then $\Delta(u_1, \ldots, u_n) \in R$.*
3. *Let R be noetherian and L/K separable. Then S is a finitely generated R-module and a noetherian domain. If R is even a principal ideal domain, then S is a free R-module, and every R-basis of S is a K-basis of L.*

Proof. 1. By Theorem mainintegral 2.1.4, S is integrally closed, and since R is integrally closed, it follows that $S \cap K = R$. Clearly, $\{q^{-1}x \mid x \in S,\ q \in R^\bullet\} \subset \mathsf{q}(S) \subset L$, and thus we must prove that, for every $z \in L$, there exists some $q \in R^\bullet$ such that $qx \in S$.

Let $z \in L$ and $f = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in K[X]$ the minimal polynomial of z over K. If $q \in R^\bullet$ is such that $qa_i \in R$ for all $i \in [0, d-1]$, then $(qz)^d + (qa_{d-1})(qz)^{d-1} + \ldots + (q^{d-1}a_1)(qz) + q^d a_0 = 0$ is an integral equation of qz over R, which implies $qz \in S$.

2. If $g \in R[X]$, then $g(\alpha) = 0$ is an integral equation of α over R, and thus $\alpha \in S$. Assume now that $\alpha \in S$, and let $f \in R[X]$ be a monic polynomial such that $f(\alpha) = 0$. Let $\overline{K} \supset L$ be an

algebraically closed field, and let $\alpha_2, \ldots, \alpha_n \in \overline{K}$ be such that $g = (X-\alpha)(X-\alpha_2)\cdot \ldots \cdot (X-\alpha_n)$. For $i \in [2,n]$, let $\varphi_i \colon K(\alpha) \xrightarrow{\sim} K(\alpha_i) \hookrightarrow \overline{K}$ be the unique K-homomorphism satisfying $\varphi_i(\alpha) = \alpha_i$. Then it follows that $f(\alpha_i) = \varphi_i(f(\alpha)) = 0$, hence α_i is integral over R. Therefore $R[\alpha_1, \ldots, \alpha_n]$ is integral over R, and $g \in (R[\alpha_1, \ldots, \alpha_n] \cap K)[X] = R[X]$.

3. Let $(u_1, \ldots, u_n) \in S^n$ be a K-basis of L and $(u_1', \ldots, u_n')$ its dual basis. We assert that $S \subset Ru_1' + \ldots + Ru_n'$. Indeed, if $z \in S$, then $z = a_1u_1' + \ldots + a_nu_n'$ for some $a_1, \ldots, a_n \in K$, and for all $i \in [1,n]$ we obtain

$$\mathsf{Tr}_{L/K}(u_iz) = \sum_{\nu=1}^{n} a_\nu \mathsf{Tr}_{L/K}(u_iu_\nu') = a_i \in R\,.$$

Since R is noetherian, it follows that S is a finitely generated R-module. Every ideal of S is a finitely generated R-module and thus a finitely generated ideal. Hence S is noetherian.

If R is even a principal ideal domain, then S is a free R-module, since it is a submodule of a free R-module, and by 1. it follows that every R-basis of S is a K-basis of L. $\square$

2.2. Algebraic integers

`tegralbasis`

Remarks and Definitions 2.2.1. An *algebraic number field* is a finite extension field of $\mathbb{Q}$. By a *basis* of K we mean a $\mathbb{Q}$-basis of K. Let in the sequel K be an algebraic number field of degree $n = [K:\mathbb{Q}]$.

1. $\mathcal{O}_K = \mathsf{cl}_K(\mathbb{Z})$ is called the *ring of integers* or the *maximal order* of K. By Theorem `integralclosure` 2.1.6, $\mathcal{O}_K$ is a noetherian domain and a finitely generated $\mathbb{Z}$-module. A $\mathbb{Z}$-basis $(u_1, \ldots, u_n)$ of $\mathcal{O}_K$ is called an *integral basis* of K.
2. A *complete module* or *full $\mathbb{Z}$-lattice* in K is a finitely generated $\mathbb{Z}$-module $M \subset K$ which contains a basis of K. By a *basis* of M we mean a $\mathbb{Z}$-basis of M. Note that an n-tuple $(u_1, \ldots, u_n) \in K^n$ is linearly independent over $\mathbb{Q}$ if and only if it is linearly independent over $\mathbb{Z}$.
3. Let $M \subset K$ be a complete module and $(u_1, \ldots, u_n)$ is a $\mathbb{Z}$-basis of M. Then the discriminant $\Delta(M) = \Delta_{L/K}(u_1, \ldots, u_n)$ only depends on M and not on $(u_1, \ldots, u_n)$. $\Delta(M)$ is called the *discriminant* of M.

   Indeed, let $(v_1, \ldots, v_n)$ be another basis of M. Then $(v_1, \ldots, v_n) = (u_1, \ldots, u_n)T$, where $T \in \mathsf{GL}_n(\mathbb{Z})$, and $\Delta_{L/K}(v_1, \ldots, v_n) = \Delta_{L/K}(u_1, \ldots, u_n)\det(T)^2 = \Delta_{L/K}(u_1, \ldots, u_n)$, since $|\det(T)| = 1$.
4. $\Delta_K = \Delta(\mathcal{O}_K)$ is called the *discriminant* of K. By definition, $\Delta_K \in \mathbb{Z}$.

Theorem 2.2.2. *Let K be an algebraic number field and $[K:\mathbb{Q}] = n$. For a submodule $M \subset K$, the following assertions are equivalent:*

(a) *M is a complete module in K.*

(b) *M is a free ($\mathbb{Z}$-)module of rank n.*

(c) *M is finitely generated, and $\mathbb{Q}M = K$.*

(d) *M is finitely generated, and for every $x \in K$ there exists some $q \in \mathbb{N}$ such that $qx \in M$.*

PROOF. (a) $\Rightarrow$ (b) As M is a finitely generated torsion-free $\mathbb{Z}$-module, it is free of some rank $m \in \mathbb{N}$. Since every basis of M is linearly independent over $\mathbb{Q}$, we have $m \le n$. If $(u_1, \ldots, u_n) \in M^n$ is a $\mathbb{Q}$-basis of K, then $M' = \langle u_1, \ldots, u_n \rangle \subset M$ is a free submodule of rank n, and therefore $n \le m$.

(b) $\Rightarrow$ (c) By assumption, M is finitely generated. If $(u_1, \ldots, u_n)$ is a basis of M, then $(u_1, \ldots, u_n)$ is linearly independent over $\mathbb{Q}$, and therefore $\mathbb{Q}M = \mathbb{Q}u_1 + \ldots + \mathbb{Q}u_n = K$.

(c) $\Rightarrow$ (d) If $x \in K$, then $x = \lambda_1 v_1 + \ldots + \lambda_m v_m$, where $m \in \mathbb{N}$, $\lambda_j \in \mathbb{Q}$ and $v_j \in M$ for all $j \in [1, m]$. If $q \in \mathbb{N}$ is such that $q\lambda_j \in \mathbb{Z}$ for all $j \in [1, m]$, then $qx \in M$.

(d) $\Rightarrow$ (a) Let $(u_1, \ldots, u_n)$ be a basis of K, and let $q \in \mathbb{N}$ be such that $qu_i \in M$ for all $i \in [1, n]$. Then $(qu_1, \ldots, qu_n)$ is a basis of K in M. □

Example 2.2.3. An algebraic number field K satisfying $[K:\mathbb{Q}] = 2$ is called a *quadratic number field*.

Let K be a quadratic number field. Then there exists a unique square-free integer $d \in \mathbb{Z} \setminus \{1\}$ such that $K = \mathbb{Q}(\sqrt{d})$ (we normalize $\sqrt{d} \in \mathbb{C}$ such that $\sqrt{d} > 0$ if $d > 0$, and $\Im(\sqrt{d}) > 0$ if $d < 0$). d is called the *radicand* of K. Note that $K/\mathbb{Q}$ is galois, $\mathsf{Gal}(K/\mathbb{Q}) = \{\mathrm{id}_K, \sigma\}$, and $\sigma(\mathcal{O}_K) = \mathcal{O}_K$. Every $x \in K$ has a unique representation $x = a + b\sqrt{d}$, where $a, b \in \mathbb{Q}$, and then $\sigma(x) = a - b\sqrt{d}$, $\mathsf{Tr}_{K/\mathbb{Q}}(x) = 2a$, $\mathsf{N}_{K/\mathbb{Q}}(x) = a^2 - b^2 d$, and $X^2 - 2aX + (a^2 - b^2 d) \in \mathbb{Q}[X]$ is the minimal polynomial of x over $\mathbb{Q}$.

1. If $d \equiv 1 \bmod 4$, then $\bigl(1, \frac{1+\sqrt{d}}{2}\bigr)$ is an integral basis of K, and $\Delta_K = d$.
2. If $d \equiv 2$ or $3 \bmod 4$, then $(1, \sqrt{d})$ is an integral basis of K, and $\Delta_K = 4d$.

Proof. 1. Let $d \equiv 1 \bmod 4$ and $\omega = \frac{1+\sqrt{d}}{2}$. Then $\omega^2 - \omega - \frac{d-1}{4} = 0$, hence $\omega \in \mathcal{O}_K$, and we obtain $\sigma(\omega) = \frac{1-\sqrt{d}}{2} = -\omega + 1 \in \mathcal{O}_K$. Clearly, $(1, \omega)$ is a basis of K, and we must prove: If $a, b \in \mathbb{Q}$ and $a + b\omega \in \mathcal{O}_K$, then $a, b \in \mathbb{Z}$.

Thus suppose that $a, b \in \mathbb{Q}$ and $a + b\omega \in \mathcal{O}_K$. Then $(a+b\omega) - \sigma(a+b\omega) = b\sqrt{d} \in \mathcal{O}_K$, hence $b^2 d \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, and since d is squarefree, we get $b \in \mathbb{Z}$. Hence $a = (a+b\omega) - b\omega \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, and we are done. Now we calculate

$$\Delta_K = \det \begin{pmatrix} 1 & \omega \\ 1 & \sigma(\omega) \end{pmatrix}^2 = (\sigma(\omega) - \omega)^2 = d\,.$$

2. Suppose that $d \equiv 2$ or $3 \bmod 4$. Then $\sqrt{d} \in \mathcal{O}_K$, $(1, \sqrt{d})$ is a basis of K, and we must prove: If $a, b \in \mathbb{Q}$ and $a + b\sqrt{d} \in \mathcal{O}_K$, then $a, b \in \mathbb{Z}$.

Thus suppose that $a, b \in \mathbb{Q}$ and $a + b\sqrt{d} \in \mathcal{O}_K$. Then the minimal polynomial of $a + b\sqrt{d}$ is in $\mathbb{Z}[X]$, which implies $a' = 2a \in \mathbb{Z}$, $a^2 - b^2 d \in \mathbb{Z}$ and thus $4b^2 d = a'^2 - 4(a^2 - b^2 d) \in \mathbb{Z}$. Since d is squarefree, we get $b' = 2b \in \mathbb{Z}$ and $a'^2 - b'^2 d \equiv 0 \bmod 4$. Since $d \not\equiv \ \bmod 4$, this implies $a' \equiv b' \equiv 0 \bmod 2$ and thus $a, b \in \mathbb{Z}$. Now we calculate

$$\Delta_K = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = 4d\,.$$

In both cases we obtain $K = \mathbb{Q}(\sqrt{\Delta_K}\,)$, and if

$$\omega = \frac{\sigma + \sqrt{\Delta_K}}{2}\,, \quad \text{where} \quad \sigma = \begin{cases} 1 & \text{if} \quad \Delta_K \equiv 1 \bmod 4\,, \\ 0 & \text{if} \quad \Delta_K \equiv 0 \bmod 4\,, \end{cases}$$

then $(1,\omega)$ is an integral basis of K. $\square$

Definition 2.2.4. Let K be an algebraic number field and $[K\colon\mathbb{Q}]=n$.

1. Let $M\subset K$ be a complete module. Then $\mathcal{R}(M)=\{x\in K\mid xM\subset M\}$ is called the *ring of multipliers* of M.
2. A subring $R\subset K$ is called an *order* in K if it is a complete module.

letemodules

Theorem 2.2.5 (Main Theorem on complete modules and orders)**.** *Let K be an algebraic number field, $M\subset K$ a complete module and $R\subset K$ an order in K.*

1. *Let $N\subset K$ be another complete module in K. Then there exists some $q\in\mathbb{N}$ such that $qM\subset N$, and if $M\subset N$, then $\Delta(M)=\Delta(N)\,(N\colon M)^2$.*
2. *If $\lambda\in K^\times$, then λM is a complete module,*
$$\mathcal{R}(\lambda M)=\mathcal{R}(M)\,,\quad \textit{and}\quad \Delta(\lambda M)=\mathsf{N}_{K/\mathbb{Q}}(\lambda)^2\Delta(M)\,.$$
3. *If $\lambda\in\mathcal{R}(M)^\bullet$, then $(M\colon\lambda M)=|\mathsf{N}_{K/\mathbb{Q}}(\lambda)|$.*
4. *Let $\mathbf{0}\ne C\subset K$ be a finitely generated R-module. Then C is a complete module in K, and $R\subset\mathcal{R}(C)$.*
5. *$\mathcal{R}(M)$ is an order in K, $\mathcal{R}(M)\subset\mathcal{O}_K$, and $M\cap\mathbb{N}\ne\mathbf{0}$.*
6. *R is a noetherian domain, and $R=\mathcal{R}(R)\subset\mathcal{O}_K$. If $\emptyset\ne\mathbf{0}\subset R$ is an ideal, then $(R\colon\mathfrak{a})<\infty$, and every non-zero prime ideal of R is maximal.*

Proof. Let $(u_1,\ldots,u_n)$ be a basis of M.

1. If $q\in\mathbb{N}$ is such that $qu_i\in\mathbb{N}$ for all $i\in[1,n]$, then $qM\subset N$.

Assume now that $M\subset N$. Then there exist a basis $(v_1,\ldots,v_n)$ of N and $e_1,\ldots,e_n\in\mathbb{N}$ such that $(e_1v_1,\ldots,e_nv_n)$ is a basis of M. Since $(e_1v_1,\ldots,e_nv_n)=(v_1,\ldots,v_n)D$ with the diagonal matrix $D=\operatorname{diag}(e_1,\ldots,e_n)$, it follows that

$$\Delta(M)=\Delta_{K/\mathbb{Q}}(e_1v_1,\ldots,e_nv_n)=\det(D)^2\Delta_{K/\mathbb{Q}}(v_1,\ldots,v_n)=\det(D)^2\Delta(N)\,,$$

and

$$(N\colon M)=(\mathbb{Z}v_1\oplus\ldots\oplus\mathbb{Z}v_n\colon\mathbb{Z}e_1v_1\oplus\ldots\oplus\mathbb{Z}e_nv_n)=e_1\cdot\ldots\cdot e_n=\det(D)\,.$$

2. If $\lambda\in K^\times$, then $(\lambda u_1,\ldots,\lambda u_n)$ is be a basis of λM, and therefore λM is a complete module. If $x\in\mathcal{R}(M)$, then $x\lambda M\subset\lambda M$, which implies $x\in\mathcal{R}(\lambda M)$. Hence $\mathcal{R}(M)\subset\mathcal{R}(\lambda M)$, and since $M=\lambda^{-1}(\lambda M)$, equality follows.

Let now $\operatorname{Hom}_\mathbb{Q}(K,\mathbb{C})=\{\sigma_1,\ldots,\sigma_n\}$. Then

$$\begin{aligned}\Delta(\lambda M)=\Delta_{K/\mathbb{Q}}(\lambda u_1,\ldots,\lambda u_n)=\det\bigl(\sigma_\nu(\lambda u_i)\bigr)^2_{\nu,i\in[1,n]}=\Bigl(\prod_{\nu=1}^n\sigma_\nu(\lambda)\,\det\bigl(\sigma_\nu(\lambda u_i)\bigr)_{\nu,i\in[1,n]}\Bigr)^2\\ =\mathsf{N}_{K/\mathbb{Q}}(\lambda)^2\det\bigl(\sigma_\nu(u_i)\bigr)^2_{\nu,i\in[1,n]}=\mathsf{N}_{K/\mathbb{Q}}(\lambda)^2\Delta_{K/\mathbb{Q}}(u_1,\ldots,u_n)=\mathsf{N}_{K/\mathbb{Q}}(\lambda)^2\Delta(M)\,.\end{aligned}$$

3. If $\lambda\in\mathcal{R}(M)^\bullet$, then $\lambda M\subset M$ and, by 1. and 2., $\Delta(\lambda M)=\mathsf{N}_{K/\mathbb{Q}}(\lambda)^2\Delta(M)=\Delta(M)\,(M\colon\lambda M)^2$. Hence it follows that $(M\colon\lambda M)=|\mathsf{N}_{K/\mathbb{Q}}(\lambda)|$.

4. As R is a finitely generated $\mathbb{Z}$-module and M is a finitely generated R-module, it follows that C is a finitely generated $\mathbb{Z}$-module. If $(v_1,\ldots,v_n)\in R^n$ is a basis of K and $c\in C^\bullet$, then

$(cu_1, \ldots, cu_n) \in C^n$ is a basis of K, and thus C is a complete module. Obviously, $RC = C$ implies $R \subset \mathcal{R}(C)$.

5. If $x, y \in \mathcal{R}(M)$, then $(x-y)M \subset xM + yM \subset M$ and $xyM \subset xM \subset M$. Hence it follows that $\{x-y,\, xy\} \subset \mathcal{R}(M)$, and therefore $\mathcal{R}(M) \subset K$ is a subring. If $x \in \mathcal{R}(M)$, then $xM \subset M$, and therefore $x \in \mathrm{cl}_K(\mathbb{Z}) = \mathcal{O}_K$ by Theorem `maincriterion` 2.1.3. Hence $\mathcal{R}(M) \subset \mathcal{O}_K$, and therefore $\mathcal{R}(M)$ is finitely generated.

If $x \in K^\times$, then xM is a complete module, and there exists some $q \in M$ such that $qxM \subset M$. Hence $qx \in \mathcal{R}(M)$, and therefore $\mathcal{R}(M)$ is a complete module.

It remains to prove that $M \cap \mathbb{N} \neq \mathbf{0}$. Let $x \in M^\bullet$ and $q \in \mathbb{N}$ such that $qx \in \mathcal{R}(M)$. Then $\mathbf{0} \neq qx\mathcal{R}(M) \subset \mathcal{R}(M)$ and, by Theorem `integralideal` 2.1.5, $qx\mathcal{R}(M) \cap \mathbb{Z} \neq \mathbf{0}$. Since $qx\mathcal{R}(M) \subset M$, the assertion follows.

6. Since R is a finitely generated $\mathbb{Z}$-module, every ideal of R is a finitely generated $\mathbb{Z}$-module and thus a finitely generated ideal. Hence R is noetherian. Since $RR = R$, it follows that $R \subset \mathcal{R}(R)$, and if $z \in \mathcal{R}(R)$, then $z = z1 \in R$, and therefore $\mathcal{R}(R) = R$.

If $\mathbf{0} \neq \mathfrak{a} \subset R$ is an ideal and $\lambda \in \mathfrak{a}^\bullet$, then $\lambda R \subset \mathfrak{a} \subset R$, and $(R\,{:}\,\mathfrak{a}) \le (R\,{:}\,\lambda R) = |\mathsf{N}_{K/\mathbb{Q}}(\lambda)| < \infty$. If $\mathbf{0} \neq \mathfrak{p} \subset R$ is a prime ideal, then $R/\mathfrak{p}$ is a finite domain, hence a field, and thus $\mathfrak{p}$ is a maximal ideal. □

`basissatz` **Theorem 2.2.6** (Basis Theorem for complete modules)**.** *Let K be an algebraic number field of degree $[K:\mathbb{Q}] = n$, $M \subset \mathcal{O}_K$ a complete module, $(v_1, \ldots, v_n) \in M^n$ a basis of K and $d = |\Delta_{K/\mathbb{Q}}(v_1, \ldots, v_n)|$. Then $d \in \mathbb{N}$, and we set $d = d_0^2 d_1$, where $d_0, d_1 \in \mathbb{N}$ and d_1 is squarefree. For $i \in [1, n]$, let $b_{i,i} \in \mathbb{N}$ be minimal such that*

$$u_i = \frac{1}{d_0} \sum_{j=1}^{i} b_{j,i} v_j \in M \quad \textit{for some} \quad b_{1,i}, \ldots, b_{i-1,i} \in \mathbb{Z}\,.$$

Then $(u_1, \ldots, u_n)$ is a basis of M.

In particular, M has a basis $(u_1, \ldots, u_n)$ such that $u_1 = \min(\mathfrak{a} \cap \mathbb{N})$, and every order in K has a basis $(u_1, \ldots, u_n)$ such that $u_1 = 1$.

Proof. Let $M_0 = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n \subset M \subset \mathcal{O}_K$. Then it follows that $\Delta(M) \in \mathbb{Z}$, and

$$d = |\Delta_{K/\mathbb{Q}}(v_1, \ldots, v_n)| = |\Delta(M_0)| = |\Delta(M)|\,(M\,{:}\,M_0)^2 \in \mathbb{N}\,.$$

In particular, $(M\,{:}\,M_0)^2 \,|\, d$, hence $(M\,{:}\,M_0) \,|\, d_0$, and therefore $d_0 M \subset M_0$. By assumption, we have

$$(u_1, \ldots, u_n) = (v_1, \ldots, v_n)B \quad \text{mit} \quad B = \frac{1}{d_0}\begin{pmatrix} b_{1,1} & b_{1,2} & \ldots & . & b_{n,1} \\ 0 & b_{2,2} & \ldots & . & b_{n,2} \\ 0 & 0 & \ldots & . & . \\ . & . & \ddots & . & . \\ 0 & 0 & \ldots & 0 & b_{n,n} \end{pmatrix} \in \mathsf{GL}_n(\mathbb{Q})\,.$$

Hence $(u_1, \ldots, u_n)$ is a basis of K, and $\mathbb{Z}u_1 + \ldots + \mathbb{Z}u_n \subset M$. To prove equality, we use induction on i to prove the following assertion for all $i \in [0, n]$:

A. If $c_1, \ldots, c_i \in \mathbb{Z}$ are such that $x = d_0^{-1}(c_1 v_1 + \ldots + c_i v_i) \in M$, then $x \in \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_i$.

Once **A** is proved, the assertion follows. Indeed, if $x \in M$, then $d_0x \in M_0$, and therefore there exist $c_1, \ldots, c_n \in \mathbb{Z}$ such that $x = d_0^{-1}(c_1v_1+\ldots+c_nv_n)$. By **A** we infer $x \in \mathbb{Z}u_1+\ldots\mathbb{Z}u_n$.

Proof of **A.** For $i = 0$, there is nothing to do.

$i \ge 1$, $i-1 \to i$: Let $c_1, \ldots, c_i \in \mathbb{Z}$ be such that $x = d_0^{-1}(c_1v_1+\ldots+c_iv_i) \in M$, and set $c_i = kb_{i,i}+r$, where $k \in \mathbb{Z}$ and $r \in [0, b_{i,i}-1]$. Then we obtain

$$x - ku_i = \frac{1}{d_0}\sum_{j=1}^{i}(c_j - kb_{i,j})v_j \in M \quad \text{and} \quad c_i - kb_{i,i} = r \in [0, b_{i,i}-1]\,.$$

By the minimal choice of $b_{i,i}$, it follows that $c_i - kb_{i,i} = 0$, and therefore $x - ku_i \in \mathbb{Z}u_1+\ldots+\mathbb{Z}u_{i-1}$ by the induction hypothesis. Hence $x \in \mathbb{Z}u_1+\ldots+\mathbb{Z}u_i$.

If $(v_1, \ldots, v_n)$ is chosen such that $v_1 = \min(\mathfrak{a} \cap \mathbb{N})$, then $u_1 = v_1$. $\square$

`nvorzeichen`

Theorem 2.2.7. *Let K be an algebraic number field, and suppose that $[K:\mathbb{Q}] = n = r_1+2r_2$, where $\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$ such that $\sigma_j(K) \subset \mathbb{R}$ for all $j \in [1, r_1]$, and $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ for all $j \in [1, r_2]$. Then $\operatorname{sgn}\Delta_{K/\mathbb{Q}}(u_1, \ldots, u_n) = (-1)^{r_2}$ for every basis $(u_1, \ldots, u_n)$ of K, and, in particular, $\operatorname{sgn}\Delta_K = (-1)^{r_2}$.*

Proof. Let $d = \det(\sigma_\nu(u_i))_{\nu\in[1,n]} = a+b\mathsf{i}$, where $a, b \in \mathbb{R}$. Then $\Delta_{K/\mathbb{Q}}(u_1, \ldots, u_n) = d^2$, and the matrix $\big(\overline{\sigma_\nu(u_i)}\big)_{\nu,i\in[1,n]}$ arises from $\big(\sigma_\nu(u_i)\big)_{\nu,i\in[1,n]}$ by interchanging r_2 rows. Hence it follows that $a - b\mathsf{i} = \det\big(\overline{\sigma_\nu(u_i)}\big)_{\nu,i\in[1,n]} = (-1)^{r_2}d$. If r_2 is even, then $b = 0$ and $d^2 = b^2 > 0$. If r_2 is odd, then $a = 0$ and $d^2 = (\mathsf{i}b)^2 = -b^2 < 0$. $\square$

`kriminanten`

Theorem 2.2.8. *Let K and L be galois algebraic number fields, $[K:\mathbb{Q}] = n$, $[L:\mathbb{Q}] = m$, $K \cap L = \mathbb{Q}$, $N = KL$ and $(\Delta_K, \Delta_L) = 1$. Let $(\omega_1, \ldots, \omega_n)$ be an integral basis of K and $(\eta_1, \ldots, \eta_m)$ and integral basis of L. Then $(\omega_i\eta_j)_{(i,j)\in[1,n]\times[1,m]}$ is an integral basis of N, and $\Delta_N = \Delta_K^m\Delta_L^n$.*

Proof. By Theorem `galoisshifting` 1.3.5, N/K is galois, and there are isomorphisms

$$\mathsf{Gal}(N/L) \to \mathsf{Gal}(K/\mathbb{Q})\,, \quad \text{given by} \quad \sigma \mapsto \sigma \,|\, K\,,$$

$$\mathsf{Gal}(N/K) \to \mathsf{Gal}(L/\mathbb{Q})\,, \quad \text{given by} \quad \sigma \mapsto \sigma \,|\, L$$

and

$$\mathsf{Gal}(N/K) \xrightarrow{\sim} \mathsf{Gal}(K/\mathbb{Q}) \times \mathsf{Gal}(L/\mathbb{Q}\,, \quad \text{given by} \quad \sigma \mapsto (\sigma \,|\, K, \sigma \,|\, L)\,.$$

Then $(\omega_i\eta_j)_{(i,j)\in[1,n]\times[1,m]}$ is a basis of N, since $N = {}_{\mathbb{Q}}\langle(\omega_i\eta_j)_{(i,j)\in[1,n]\times[1,m]}\rangle$ and $[N:\mathbb{Q}] = mn$. Let $\mathsf{Gal}(N/L) = \{\sigma_1, \ldots, \sigma_n\}$ and $\mathsf{Gal}(N/K) = \{\tau_1, \ldots, \tau_m\}$. Let $\alpha \in \mathcal{O}_N$, say

$$\alpha = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\omega_i\eta_j\,, \quad \text{where} \quad a_{i,j} \in \mathbb{Q} \quad \text{for all} \quad (i,j) \in [1,n]\times[1,m]\,.$$

Since $\{\omega_i\eta_j \mid (i,j) \in [1,n]\times[1,m]\} \subset \mathcal{O}_N$, it suffices to prove that $a_{i,j} \in \mathbb{Z}$ for all $(i,j) \in [1,n]\times[1,m]$. For $j \in [1,m]$, set

$$\beta_j = \sum_{i=1}^{n} a_{i,j}\omega_i \in K\,, \quad \text{which impies} \quad \alpha = \sum_{j=1}^{m}\beta_j\eta_j \quad \text{and} \quad \tau_\mu(\alpha) = \sum_{j=1}^{m}\beta_j\tau_\mu(\eta_j) \in \mathcal{O}_N\,.$$

We set $T = (\tau_\mu(\eta_j))_{j,\mu\in[1,m]}$. Then $T^\# \in \mathsf{M}_m(\mathbb{Z})$, and therefore

$$(\tau_1\alpha, \ldots, \tau_m\alpha)T^\# = (\beta_1, \ldots, \beta_m)TT^\# = (\beta_1, \ldots, \beta_m)\,\det(T) \in \mathcal{O}_N^m\,.$$

Since $\mathsf{Gal}(L/\mathbb{Q}) = \{\tau_1 \,|\, L, \ldots, \tau_m \,|\, L)$, we obtain $\det(T)^2 = \Delta_{K/\mathbb{Q}}(\eta_1, \ldots, \eta_m) = \Delta_L$ and thus it follows that $\beta_j\Delta_L \in \mathcal{O}_N \cap K = \mathcal{O}_K$ for all $j \in [1, m]$. But now

$$\beta_j\Delta_L = \sum_{i=1}^n a_{i,j}\Delta_L\omega_i \quad \text{for all} \quad j \in [1, m] \quad \text{implies} \quad a_{i,j}\Delta_L \in \mathbb{Z} \quad \text{for all} \quad (i,j) \in [1,n]\times[1,m]\,.$$

By interchanging the roles of L and K, it follows that $a_{i,j}\Delta_K \in \mathbb{Z}$ for all $(i,j) \in [1,n]\times[1,m]$, and since $(\Delta_K, \Delta_L) = 1$ this implies $a_{i,j} \in \mathbb{Z}$ for all $(i,j) \in [1,n]\times[1,m]$.

Now it follows that

$$\Delta_N = \det\bigl(\sigma_\nu\tau_\mu(\omega_i\eta_j)\bigr)^2_{(\nu,\mu),\,(i,j)\in[1,n]\times[1,m]} = \bigl[\det(\sigma_\nu\omega_i)^m_{\nu,i\in[1,n]}\,\det(\tau_\mu\eta_j)^n_{\mu,j\in[1,m]}\bigr]^2 = \Delta_K^m\Delta_L^n\,.$$

Calculation of the determinant: Let $A = (a_{i,\nu})_{i,\nu\in[1,n]} \in \mathsf{M}_n(K)$, $B = (b_{j,\mu})_{j,\mu\in[1,n]} \in \mathsf{M}_m(K)$, and define $A \otimes B = \bigl(a_{i,\nu}b_{j,\mu}\bigr)_{(i,j),(\nu,\mu)\in[1,n]\times[1,m]} \in \mathsf{M}_{mn}(K)$. Then

$$A \otimes B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \ldots & a_{1,n}B \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ a_{n,1}B & a_{n,2}B & \ldots & a_{n,n}B \end{pmatrix} = \begin{pmatrix} a_{1,1}I_m & a_{1,2}I_m & \ldots & a_{1,n}I_m \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ a_{n,1}I_m & a_{n,2}I_m & \ldots & a_{n,n}I_m \end{pmatrix} \begin{pmatrix} B & \ldots & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & B \end{pmatrix}$$

and we may apply the product formula for determinants. □

eisenstein1

Theorem 2.2.9 (Eisenstein criterion)**.** *Let K be an algebraic number field, $[K:\mathbb{Q}] = n$, $\alpha \in K$ and $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$ the minimal polynomial of α. Let $p \in \mathbb{P}$ be a prime such that $p \,|\, a_i$ for all $i \in [0, n-1]$ and $p^2 \nmid a_0$* [such a polynomial is called a *p-Eisenstein polynomial*]. *Then f is irreducible, and $\mathbb{Z}[\alpha] \subset K$ is an order satisfying $(\mathcal{O}_K : \mathbb{Z}[\alpha]) \nmid p$.*

Proof. We show first that f is irreducible. Let $\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X] = \mathbb{F}_p[X]$, $h \mapsto \overline{h}$ be the residue class map, and suppose that $f = gh$ for some polynomials $g,\, h \in \mathbb{Z}[X] \setminus \mathbb{Z}$. We may assume that both g and h are monic, and since $\overline{f} = X^n = \overline{g}\overline{h}$, it follows that $\overline{g} = X^r$ and $\overline{h} = X^s$, where $r,\, s \in \mathbb{N}$ and $r + s = n$. But this implies that $a_0 = g(0)h(0) \equiv 0 \bmod p^2$, a contradiction.

Since $\deg(f) = n$, $\mathbb{Z}[\alpha] \subset K$ is an order, and we assume that $p \,|\, (\mathcal{O}_K : \mathbb{Z}[\alpha]$. Then there exists some $\xi \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha]$ such that $p\xi \in \mathbb{Z}[\alpha]$, say $p\xi = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$, where $b_0, \ldots, b_{n-1} \in \mathbb{Z}$, and $p \nmid b_j$ for at least one $j \in [0, n-1]$. Let $j \in [0, n-1]$ be minimal such that $p \nmid b_j$. Then $p\xi = p\eta + b_j\alpha^j + \alpha^{j+1}\theta$ for some $\eta, \theta \in \mathbb{Z}[\alpha]$, and therefore $b_j\alpha^{n-1} = p(\xi - \eta)\alpha^{n-j-1} + \alpha^n\theta$. Since $\alpha^n = -a_0 - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1} \in p\mathbb{Z}[\alpha]$, it follows that $b_j\alpha^{n-1} \in p\mathcal{O}_K$, and $\mathsf{N}_{K/\mathbb{Q}}(b_j\alpha^{n-1}) \in p^n\mathbb{Z}$. Since $\mathsf{N}_{K/\mathbb{Q}}(b_j\alpha^{n-1}) = b_j^n\mathsf{N}_{K/\mathbb{Q}}(\alpha)^{n-1} = \pm b_j^n a_0^{n-1}$ and $p \nmid b_j$, we obtain $p^n \,|\, a_0^{n-1}$ and therefore $p^2 \,|\, a_0$, a contradiction. □

cyclotomic

Theorem 2.2.10. *Let* $n \in \mathbb{N}$, $n \ge 3$, $\zeta_n \in \mu_n^*(\mathbb{C})$ *and* $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta_n)$ *the n-th cyclotomic field. Then* $\mathcal{O}_{\mathbb{Q}^{(n)}} = \mathbb{Z}[\zeta_n]$, $(1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\varphi(n)})$ *is an integral basis of* $\mathbb{Q}^{(n)}$, *and*

$$\Delta_{\mathbb{Q}^{(n)}} = (-1)^{\varphi(n)/2} n^{\varphi(n)} \Big[\prod_{p\,|\,n} p^{\varphi(n)/(p-1)}\Big]^{-1}.$$

diskriminantenvorzeichen

Proof. As $n \ge 3$, there is no $\sigma \colon \mathbb{Q}^{(n)} \to \mathbb{R}$, and by Theorem 2.2.7 we obtain $r_2 = \varphi(n)/2$ and therefore $\operatorname{sgn}(\Delta_{\mathbb{Q}^{(n)}}) = (-1)^{\varphi(n)/2}$.

CASE 1: $n = p^e \ge 3$ is a prime power, $\zeta = \zeta_{p^e}$, $N = [\mathbb{Q}^{(p^e)} : \mathbb{Q}] = \varphi(p^e) = p^{e-1}(p-1)$, and $(1, \zeta, \ldots, \zeta^{N-1})$ is a basis of $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]$. The polynomial

$$\Phi = \Phi_{p^e} = \frac{X^{p^e} - 1}{X^{p^{e-1}} - 1} = \sum_{\nu=0}^{p-1} X^{p^{e-1}\nu}$$

is the minimal polynomial of ζ, $\Phi_1 = \Phi(X+1)$ is the minimal polynomial of $\zeta - 1$, and we assert that Φ_1 is a p-Eisenstein polynomial. Indeed, let $\pi \colon \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$ be the residue class homomorphism. Then

$$\pi\big((X+1)^{p^{e-1}} - 1\big)\pi(\Phi_1) = \pi\big((X+1)^{p^e} - 1\big), \quad \text{hence} \quad X^{p^{e-1}}\pi(\Phi_1) = X^{p^e} \quad \text{and} \quad \pi(\Phi_1) = X^N.$$

Since $\Phi_1(0) = \Phi(1) = p$, Φ_1 is a p-Eisenstein polynomial, and therefore $(\mathcal{O}_{\mathbb{Q}^{(p^e)}} : \mathbb{Z}[\zeta]) \nmid p$.

Next we calculate $\Delta(\mathbb{Z}[\zeta]) = (-1)^{N(N-1)/2} \mathsf{N}_{\mathbb{Q}^{(p^e)}/\mathbb{Q}}(\Phi'(\zeta))$. We have

$$\Phi'(\zeta) = \sum_{\nu=1}^{p-1} p^{e-1}\nu\zeta^{p^{e-1}\nu - 1} = p^{e-1}\zeta^{-1}\sum_{\nu=1}^{p-1}\nu\xi^\nu, \quad \text{where} \quad \xi = \zeta^{p^{e-1}} \in \mu_p^*(\mathbb{C}).$$

Hence it follows that

$$\begin{aligned}\zeta(\xi-1)\Phi'(\zeta) &= p^{e-1}(\xi - 1)\sum_{\nu=1}^{p-1}\nu\xi^\nu = p^{e-1}\Big(\sum_{\nu=1}^{p-1}\nu\xi^{\nu+1} - \sum_{\nu=0}^{p-2}(\nu+1)\xi^{\nu+1}\Big)\\ &= p^{e-1}\Big((p-1) - \xi - \sum_{\nu=1}^{p-2}\xi^{\nu+1}\Big) = p^e, \qquad \Phi'(\zeta) = \frac{p^e}{\zeta(\xi-1)},\end{aligned}$$

and

$$\mathsf{N}_{\mathbb{Q}^{(p^e)}/\mathbb{Q}}(\Phi'(\zeta)) = \frac{p^{Ne}}{\mathsf{N}_{\mathbb{Q}^{(p^e)}/\mathbb{Q}}(\zeta)\mathsf{N}_{\mathbb{Q}^{(p^e)}/\mathbb{Q}}(\xi - 1)} = \frac{p^{Ne}}{\mathsf{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi-1)^{p^{e-1}}},$$

since $\mathsf{N}_{\mathbb{Q}^{(p^e)}/\mathbb{Q}}(\zeta) = \Phi(0) = 1$ and $[\mathbb{Q}^{(p^e)} : \mathbb{Q}(\xi)] = p^{e-1}$. The polynomial

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + pX^{p-2} + \ldots + p$$

is the minimal polynomial of $\xi - 1$, and therefore $\mathsf{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi - 1) = (-1)^{p-1}p$. Putting all together, we obtain

$$\Delta(\mathbb{Z}[\zeta]) = (-1)^{N(N-1)/2}(-1)^{(p-1)p^{e-1}}p^{eN - p^{e-1}} = (-1)^{\varphi(p^e)/2}p^{p^{e-1}(ep-e-1)},$$

hence $(\mathcal{O}_{\mathbb{Q}^{(p^e)}} : \mathbb{Z}[\zeta])$ is a p-power, and therefore $\mathcal{O}_{\mathbb{Q}^{(p^e)}} = \mathbb{Z}[\zeta]$ and $\Delta_{\mathbb{Q}^{(p^e)}} = \Delta(\mathbb{Z}[\zeta])$.

CASE 2: n is arbitrary. If n is odd, then $\mathbb{Q}^{(n)} = \mathbb{Q}^{(2n)}$, and thus we assume that $n \not\equiv 2 \mod 4$. We prodeed by induction on the number of prime divisors of n, and we set $n = q^e m$, where $q \in \mathbb{P}$, $e, m \in \mathbb{N}$, $m \geq 2$ and $q \nmid m$. Since $n \not\equiv 2 \mod 4$, we get $q^e \geq 3$ and $m \geq 3$.

If $\zeta_{q^e} \in \mu_{q^e}^*(\mathbb{C})$ and $\zeta_m \in \mu_m^*(\mathbb{C})$, then $\zeta_{q^e}\zeta_m \in \mu_n^*(\mathbb{C})$. Hence $\mathbb{Q}^{(q^e)}\mathbb{Q}^{(m)} = \mathbb{Q}^{(n)}$, and we assert that $\mathbb{Q}^{(q^e)} \cap \mathbb{Q}^{(m)} = \mathbb{Q}$. Indeed, suppose that $K = \mathbb{Q}^{(q^e)} \cap \mathbb{Q}^{(m)}$ and $[K:\mathbb{Q}] = d$. By Theorem `galoisshifting` 1.3.5, we get

$$\frac{\varphi(n)}{d} = [\mathbb{Q}^{(n)}:K] = [\mathbb{Q}^{(q^e)}:K]\,[\mathbb{Q}^{(m)}:K] = \frac{\varphi(q^e)}{d}\,\frac{\varphi(m)}{d} = \frac{\varphi(n)}{d^2}\,, \quad \text{and therefore} \quad d = 1\,.$$

By the induction hypothesis, $(\Delta_{\mathbb{Q}^{(q^e)}}, \Delta_{\mathbb{Q}^{(m)}}) = 1$, and we apply Theorem `teilerfremdediskriminanten` 2.2.8 and the induction hypothesis for $\mathbb{Q}^{(q^e)}$ and $\mathbb{Q}^{(m)}$. $(1, \zeta_{q^e}, \ldots, \zeta_{q^e}^{\varphi(q^e)-1})$ is an integral basis of $\mathbb{Q}^{(q^e)}$, and $(1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1})$ is an integral basis of $\mathbb{Q}^{(m)}$. Hence the products $\zeta_{q^e}^i\zeta_m^j$ for $i \in [1, \varphi(q^e)-1]$ and $j \in [1, \varphi(m)-1]$ form an integral basis of $\mathbb{Q}^{(n)}$. Since $\mathbb{Z}[\zeta_n] \subset \mathcal{O}_{\mathbb{Q}^{(n)}} \subset \mathbb{Z}[\zeta_{q^e}\zeta_m] \subset \mathbb{Z}[\zeta_n]$, it follows that $\mathcal{O}_{\mathbb{Q}^{(n)}} = \mathbb{Z}[\zeta_n]$, and $(1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1})$ is an integral basis of $\mathbb{Q}^{(n)}$. Finally,

$$\begin{aligned}\Delta_{\mathbb{Q}^{(n)}} = \Delta_{\mathbb{Q}^{(q^e)}}^{\varphi(m)}\Delta_{\mathbb{Q}^{(m)}}^{\varphi(q^e)} &= \Big[(-1)^{\frac{\varphi(q^e)}{2}} q^{e\varphi(q^e) - \frac{\varphi(q^e)}{q-1}}\Big]^{\varphi(m)} \Big[(-1)^{\frac{\varphi(m)}{2}} m^{\varphi(m)} \prod_{p \,|\, m} p^{-\frac{\varphi(m)}{p-1}}\Big]^{\varphi(q^e)} \\ &= (-1)^{\varphi(n)} n^{\varphi(n)} \prod_{p\,|\,n} p^{-\frac{\varphi(n)}{p-1}} = n^{\varphi(n)} \prod_{p\,|\,n} p^{-\frac{\varphi(n)}{p-1}}\,,\end{aligned}$$

and the assertion follows since $\varphi(n) = \varphi(p^e)\varphi(m) \equiv 0 \mod 4$. □

2.3. Gauß sums and the quadratic reciprocity law

Definition 2.3.1. Let $p \in \mathbb{P} \setminus \{2\}$ be an odd prime. We consider the group $\mathbb{X}_p = \mathrm{Hom}(\mathbb{F}_p^\times, \mathbb{C}^\times)$ (with pointwise multiplication), and we call the elements $\chi \in \mathbb{X}_p$ *characters modulo p*. Explicitly: If $\chi_1, \chi_2 \in \mathbb{X}_p$, then $(\chi_1\chi_2)(t) = \chi_1(t)\chi_2(t)$ for all $t \in \mathbb{F}_p$, the *unit character* $\mathbf{1} \in \mathbb{X}_p$ is defined by $\mathbf{1}(t) = 1$ for all $t \in \mathbb{F}_p$, and for $\chi \in \mathbb{X}_p$, we have $\chi(t) \in \mu_{p-1}(\mathbb{C})$ and $\chi^{-1}(t) = \overline{\chi}(t) = \chi(t)^{-1} = \overline{\chi(t)}$ for all $t \in \mathbb{F}_p$. If $\mathbb{F}_p = \langle\omega\rangle$, then $\mathrm{ord}(\chi) = \mathrm{ord}(\chi(\omega))$ for all $\chi \in \mathbb{X}_p$, and therefore the map $\mathbb{X}_p \to \mu_{p-1}(\mathbb{C})$, defined by $\chi \mapsto \chi(\omega)$, is a group isomorphism. For $a \in \mathbb{Z} \setminus p\mathbb{Z}$ and $\chi \in \mathbb{X}_p$, we define $\chi(a) = \chi(a + p\mathbb{Z})$. For $\kappa = k + p\mathbb{Z} \in \mathbb{F}_p$ and $\xi \in \mu_p(\mathbb{C})$, we define $\xi^\kappa = \xi^k$. Then it follows that

$$\sum_{\kappa \in \mathbb{F}_p} \xi^\kappa = \begin{cases} p & \text{if} \quad \xi = 1\,, \\ 0 & \text{if} \quad \xi \neq 1\,. \end{cases} \quad \text{Indeed, if } \xi \neq 1, \text{ then} \quad \sum_{\kappa \in \mathbb{F}_p} \xi^\kappa = \sum_{\nu=0}^{p-1} \xi^\nu = \frac{\xi^p - 1}{\xi - 1} = 0\,.$$

Let $\zeta_p = \mathsf{e}^{2\pi\mathsf{i}/p}$ be the normalized primitive p-th root of unity. For $\chi \in \mathbb{X}_p$ and $a \in \mathbb{F}_p$, we define the *Gauß sum* by

$$\tau_p(a, \chi) = \sum_{t \in \mathbb{F}_p^\times} \chi(t)\zeta_p^{at} \in \mathbb{Z}[\zeta_{p(p-1)}\,, \quad \text{and we set} \quad \tau_p(\chi) = \tau_p(1, \chi)\,.$$

gausssum

Theorem 2.3.2. *Let $p \in \mathbb{P} \setminus \{2\}$ be an odd prime, $\chi \in \mathbb{X}_p$ and $a \in \mathbb{F}_p$. Then*

$$\tau_p(a,\chi) = \begin{cases} p-1 & \text{if} \quad a = 0 \quad \text{and} \quad \chi = \mathbf{1}\,, \\ 0 & \text{if} \quad a = 0 \quad \text{and} \quad \chi \ne \mathbf{1}\,, \\ \overline{\chi(a)}\,\tau_p(\chi) & \text{if} \quad a \ne 0\,, \end{cases} \qquad |\tau_p(\chi)| = \begin{cases} 1 & \text{if} \quad \chi = \mathbf{1}\,, \\ \sqrt{p} & \text{if} \quad \chi \ne \mathbf{1}\,, \end{cases}$$

$$\overline{\tau_p(\chi)} = \chi(-1)\tau_p(\overline{\chi}) \quad \text{and} \quad \tau_p(\chi)\tau_p(\overline{\chi}) = \chi(-1)p\,.$$

Proof. As above, we have

$$\tau_p(a,\mathbf{1}) = \sum_{t \in \mathbb{F}_p^\times} \zeta_p^{at} = \sum_{t \in \mathbb{F}_p} \zeta_p^{at} - 1 = \begin{cases} p-1 & \text{if} \quad a = 0\,, \\ -1 & \text{if} \quad a \ne 0\,, \end{cases} \qquad \text{and} \qquad |\tau_p(\mathbf{1})| = 1\,.$$

If $\chi \ne \mathbf{1}$ and $\mathbb{F}_p^\times = \langle \omega \rangle$, then

$$\tau_p(0,\chi) = \sum_{t \in \mathbb{F}_p^\times} \chi(t) = \sum_{\nu=0}^{p-2} \chi(\omega)^\nu = \frac{\chi(\omega)^{p-1} - 1}{\chi(\omega) - 1} = 0\,.$$

Thus assume that $a \in \mathbb{F}_p^\times$. Then $\mathbb{F}_p^\times = \{at \mid t \in \mathbb{F}_p^\times\}$ and therefore, putting $at = s$ and observing $\chi(a^{-1}s) = \overline{\chi(a)}\chi(s)$, we obtain

$$\tau_p(a,\chi) = \sum_{t \in \mathbb{F}_p^\times} \chi(t)\zeta_p^{at} \underset{[\,t = a^{-1}s\,]}{=} \sum_{s \in \mathbb{F}_p^\times} \chi(a^{-1}s)\zeta_p^{s} = \overline{\chi(a)} \sum_{s \in \mathbb{F}_p^\times} \chi(s)\zeta_p^{s} = \overline{\chi(a)}\tau_p(\chi)\,.$$

Hence $|\tau_p(\chi)| = |\tau_p(a,\chi)|$, and if $\chi \ne \mathbf{1}$, then $\tau_p(0,\chi) = 0$. Thus, for $\chi \ne \mathbf{1}$ we obtain

$$(p-1)|\tau_p(\chi)|^2 = \sum_{a \in \mathbb{F}_p} \tau_p(a,\chi)\overline{\tau_p(a,\chi)} = \sum_{s,\,t \in \mathbb{F}_p^\times} \chi(t)\overline{\chi(s)} \sum_{a \in \mathbb{F}_p} \zeta_p^{a(t-s)}\,.$$

Since

$$\sum_{a \in \mathbb{F}_p} \zeta_p^{a(t-s)} = 0 \quad \text{if} \quad t \ne s\,, \qquad \text{and} \qquad |\chi(t)| = 1\,,$$

it follows that $(p-1)|\tau_p(\chi)|^2 = p(p-1)$, and thus $|\tau_p(\chi)| = \sqrt{p}$. Finally, we obtain

$$\chi(-1)\tau_p(\overline{\chi}) = \tau_p(-1,\overline{\chi}) = \sum_{t \in \mathbb{F}_p^\times} \overline{\chi}(t)\zeta_p^{-t} = \overline{\sum_{t \in \mathbb{F}_p^\times} \chi(t)\zeta_p^{t}} = \overline{\tau_p(\chi)}\,,$$

and consequently $\tau_p(\chi)\tau_p(\overline{\chi}) = \chi(-1)\,|\tau_p(\chi)|^2 = \chi(-1)p$. □

Remark and Definition 2.3.3. Let $p \in \mathbb{P} \setminus \{2\}$ be an odd prime. Then there is a unique character $\varphi \in \mathbb{X}_p$ such that $\operatorname{ord}(\varphi) = 2$. If $\mathbb{F}_p = \langle \omega \rangle$, then φ is given by $\varphi(\omega^k) = (-1)^k$ for all $k \in \mathbb{Z}$. φ is called the *quadratic character modulo p*. For $a \in \mathbb{Z} \setminus p\mathbb{Z}$, we define the *Legendre symbol* by

$$\Big(\frac{a}{p}\Big) = \Big(\frac{a + p\mathbb{Z}}{p}\Big) = \varphi(a) = \begin{cases} 1 & \text{if} \quad a \in \mathbb{F}_p^{\times 2}\,, \\ -1 & \text{otherwise}\,. \end{cases}$$

By definition, $\left(\frac{a}{p}\right) = 1$ if and only if there exists some $x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod p$, and in this case a is said to be a *quadratic residue* modulo p. For all a, $b \in \mathbb{Z} \setminus p\mathbb{Z}$ we have

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \text{and} \quad \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

euler

Theorem 2.3.4 (Euler's criterion). *Let $p \in \mathbb{P} \setminus \{2\}$ be an odd prime.*

1. *If $a \in \mathbb{Z} \setminus p\mathbb{Z}$, then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p\,. \quad \textit{In particular,} \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \textit{if} \quad p \equiv 1 \mod 4\,, \\ -1 & \textit{if} \quad p \equiv 3 \mod 4\,. \end{cases}$$

2. *If $p^* = (-1)^{(p-1)/2}p$, then $\sqrt{p^*} \in \mathbb{Q}^{(p)}$.*

PROOF. Suppose that $\mathbb{F}_p^\times = \langle \omega \rangle$, and let $\varphi \in \mathbb{X}_p$ be the quadratic character modulo p.

1. Let $k \in \mathbb{N}$ be such that $\alpha = a + p\mathbb{Z} = \omega^k \in \mathbb{F}_p^\times$. Since $\omega^{(p-1)/2} \neq 1 + p\mathbb{Z}$ and $(\omega^{(p-1)/2})^2 = 1 + p\mathbb{Z}$, it follows that $\omega^{(p-1)/2} = -1 + p\mathbb{Z}$. Hence

$$\left(\frac{a}{p}\right) + p\mathbb{Z} = \varphi(\omega^k) + p\mathbb{Z} = (-1)^k + p\mathbb{Z} = (\omega^{(p-1)/2})^k = \alpha^{(p-1)/2} = a^{(p-1)/2} + p\mathbb{Z}\,,$$

and therefore

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p\,.$$

In particular,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \mod p \quad \text{implies} \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}\,.$$

2. Since $\varphi = \overline{\varphi}$, Theorem gausssum 2.3.2 implies

$$\tau_p(\varphi)^p = \varphi(-1)p = \left(\frac{-1}{p}\right)p = p^*\,,$$

and as $\tau_p(\varphi) \in \mathbb{Q}^{(p)}$, it follows that $\sqrt{p^*} \in \mathbb{Q}^{(p)}$. □

reciprocity

Theorem 2.3.5 (Quadratic Reciprocity Law).

1. *Let $p \in \mathbb{P} \setminus \{2\}$ be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \textit{if} \quad p \equiv \pm 1 \mod 8\,, \\ -1 & \textit{if} \quad p \equiv \pm 3 \mod 8\,. \end{cases}$$

2. *Let p, $q \in \mathbb{P} \setminus \{2\}$ be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \textit{if} \quad p \equiv q \equiv 3 \mod 4\,, \\ 1 & \textit{otherwise.} \end{cases}$$

Proof. 1. We calculate in $\mathbb{Z}[\mathsf{i}]/p\mathbb{Z}[\mathsf{i}]$ and observe that $-1 \not\equiv 1 \bmod p\mathbb{Z}[\mathsf{i}]$. By Theorem euler 2.3.4,

$$(1+\mathsf{i}^p)(1+\mathsf{i}) \equiv (1+\mathsf{i})^{p+1} = (2\mathsf{i})(p+1)/2 = 2^{(p-1)/2}\cdot 2\mathsf{i}^{(p+1)/2} \equiv \Big(\frac{2}{p}\Big)\, 2\mathsf{i}^{(p+1)/2} \mod p\mathbb{Z}[\mathsf{i}]\,.$$

CASE 1: $p \equiv 1 \mod 4$. Then $\mathsf{i}^p = \mathsf{i}$,

$$(1+\mathsf{i}^p)(1+\mathsf{i}) = (1+\mathsf{i})^2 = 2\mathsf{i} \equiv \Big(\frac{2}{p}\Big)(2\mathsf{i})\mathsf{i}^{(p-1)/2} \mod p\mathbb{Z}[\mathsf{i}]\,,$$

and since $(2\mathsf{i}, p) = 1$, it follows that

$$\Big(\frac{2}{p}\Big)\,(-1)^{(p-1)/4} \equiv 1 \mod p\mathbb{Z}[\mathsf{i}]\,, \quad \text{hence} \quad \Big(\frac{2}{p}\Big) = (-1)^{(p-1)/4} = (-1)^{(p^2-1)/8}\,.$$

CASE 2: $p \equiv 3 \mod 4$. Then $\mathsf{i}^p = -\mathsf{i}$,

$$(1+\mathsf{i}^p)(1+\mathsf{i}) = 2 \equiv \Big(\frac{2}{p}\Big)2\mathsf{i}^{(p+1)/2} \mod p\mathbb{Z}[\mathsf{i}]\,,$$

and since $(2, p) = 1$, it follows that

$$\Big(\frac{2}{p}\Big)\,(-1)^{(p+1)/4} \equiv 1 \mod p\mathbb{Z}[\mathsf{i}]\,, \quad \text{hence} \quad \Big(\frac{2}{p}\Big) = (-1)^{(p+1)/4} = (-1)^{(p^2-1)/8}\,.$$

2. Let $\varphi \in \mathbb{X}_p$ be the quadratic character modulo p. Then $\varphi = \overline{\varphi}$, $\tau_p(\varphi)^2 = (-1)^{(p-1)/2}p$,

$$\varphi(q+p\mathbb{Z}) = \Big(\frac{q}{p}\Big), \quad \varphi(-1+p\mathbb{Z}) = (-1)^{(p-1)/2} \quad \text{and} \quad \Big(\frac{p}{q}\Big) \equiv p^{(q-1)/2} \mod q\,.$$

We calculate the Gauss sum $\tau_p(\chi) \in \mathbb{Z}[\zeta_p]$ modulo $q\mathbb{Z}[\zeta_p]$. Since

$$\tau_p(\varphi)^q = \Big(\sum_{t\in\mathbb{F}_p^\times} \varphi(t)\zeta_p^t\Big)^q \equiv \sum_{t\in\mathbb{F}_p^\times} \varphi(t)\zeta_p^{tq} = \tau_p(q+p\mathbb{Z},\varphi) = \Big(\frac{q}{p}\Big)\,\tau_p(\varphi) \mod q\mathbb{Z}[\zeta_p]\,,$$

it follows that

$$\tau_p(\varphi)^{q+1} \equiv \Big(\frac{q}{p}\Big)\,(-1)^{(p-1)/2}p \mod q\mathbb{Z}[\zeta_p]\,.$$

On the other hand,

$$\tau_p(\varphi)^{q+1} = [\tau_p(\varphi)^2]^{(q+1)/2} = (-1)^{\frac{p-1}{2}\,\frac{q+1}{2}}\, p^{(q+1)/2} \equiv (-1)^{\frac{p-1}{2}\,\frac{q+1}{2}}\, p\,\Big(\frac{p}{q}\Big) \mod q\mathbb{Z}[\zeta_p]\,,$$

and thus we obtain

$$\Big(\frac{q}{p}\Big)\,(-1)^{(p-1)/2}p \;\equiv\; (-1)^{\frac{p-1}{2}\,\frac{q+1}{2}}\, p\,\Big(\frac{p}{q}\Big) \mod q\mathbb{Z}[\zeta_p]\,.$$

Since $((-1)^{(p-1)/2}p, q) = 1$, it follows that

$$\Big(\frac{q}{p}\Big) \equiv (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}\Big(\frac{p}{q}\Big) \mod q\mathbb{Z}[\zeta_p]\,, \quad \text{hence} \quad \Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}\,. \qquad \square$$

2.4. Dedekind domains

Definition 2.4.1. Let R be a domain and $K = \mathsf{q}(R)$.

1. For R-submodules $\mathfrak{a}, \mathfrak{b} \subset K$ we define $\mathfrak{a}^{-1} = (R : \mathfrak{a}) = \{x \in K \mid x\mathfrak{a} \subset R\}$,
$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\} \quad \text{and} \quad \mathfrak{a}\mathfrak{b} = \Big\{ \sum_{i=1}^{n} a_i b_i \;\Big|\; n \in \mathbb{N},\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \Big\}.$$
Obviously, $\mathfrak{a}^{-1}$, $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a} + \mathfrak{b}$ are R-submodules of K. The operations $+$ and $\cdot$ are associative and commutative, and $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$ for all R-submodules $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \subset K$. Moreover, $\mathfrak{a}\mathfrak{a}^{-1} \subset R$, and $\mathfrak{a} \subset \mathfrak{b}$ implies $\mathfrak{a}^{-1} \supset \mathfrak{b}^{-1}$.
2. An R-submodule $\mathfrak{a} \subset K$ is called a *fractional ideal* of R if $\mathfrak{a} \ne \mathbf{0}$ and $\mathfrak{a}^{-1} \ne \mathbf{0}$. We denote by
    - $\mathcal{F}(R)$ the set of all fractional ideals of R, and by
    - $\mathcal{I}(R) = \{\mathfrak{a} \in \mathcal{F}(R) \mid \mathfrak{a} \subset R\}$ the set of all non-zero ideals of R.
3. For $a \in K^\times$ we call $Ra \in \mathcal{F}(R)$ the *fractional principal ideal* generated by a, and we denote by $(K^\times) \subset \mathcal{F}(R)$ the set of all fractional principal ideals of R.
4. A fractional ideal $\mathfrak{a} \in \mathcal{F}(R)$ is called (R-)*invertible* if $\mathfrak{a}\mathfrak{a}^{-1} = R$.

Lemma 2.4.2. *Let R be a domain and $K = \mathsf{q}(R)$.*

1. *Let $\mathfrak{a} \subset K$ be an R-submodule.*
    - (a) *$\mathfrak{a} \in \mathcal{F}(R)$ if and only if $a\mathfrak{a} \in \mathcal{I}(R)$ for some $a \in R^\bullet$.*
    - (b) *If $\mathfrak{a}$ is a finitely generated R-module and $\mathfrak{a} \ne \mathbf{0}$, then $\mathfrak{a} \in \mathcal{F}(R)$.*
    - (c) *If R is noetherian and $\mathfrak{a} \in \mathcal{F}(R)$, then $\mathfrak{a}$ is a finitely generated R-module.*
2. *If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional R-ideals, then $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}^{-1}$ are also fractional R-ideals.*
3. *Let K be an algebraic number field.*
    - (a) *If $M \subset K$ is a complete module and $R \subset K$ an order such that $R \subset \mathcal{R}(M)$, then $M \in \mathcal{F}(R)$.*
    - (b) *If $R \subset K$ is an order and $M \in \mathcal{F}(R)$, then $M \subset K$ is a complete module.*

PROOF. 1. (a) If $\mathfrak{a} \in \mathcal{F}(R)$, then $\mathfrak{a} \ne \mathbf{0}$ and there is some $x \in K^\times$ such that $x\mathfrak{a} \subset R$. Let $c \in R^\bullet$ be such that $a = cx \in R$. Then $\mathbf{0} \ne a\mathfrak{a} = cxa \subset R$ is a non-zero ideal of R.

Conversely, if $a \in R^\bullet$ is such that $a\mathfrak{a} \in \mathcal{I}(R)$, then $\mathfrak{a} \ne \mathbf{0}$ and $a \in \mathfrak{a}^{-1}$. Hence $\mathfrak{a}^{-1} \ne \mathbf{0}$, and $\mathfrak{a} \in \mathcal{F}(R)$.

(b) Let $\mathbf{0} \ne \mathfrak{a} = {}_R\langle a_1, \ldots, a_n \rangle \subset K$. Then there is some $a \in R^\bullet$ such that $aa_i \in R$ for all $i \in [1, n]$, and it follows that $a\mathfrak{a} \subset R$, hence $a \in \mathfrak{a}^{-1}$, and thus $\mathfrak{a} \in \mathcal{F}(R)$.

(c) Let R be noetherian and $\mathfrak{a} \in \mathcal{F}(R)$. By (a), there is some $a \in R^\bullet$ such that $a\mathfrak{a} \in \mathcal{I}(R)$. Then $a\mathfrak{a} = {}_R\langle a_1, \ldots, a_n \rangle$ for some $a_1, \ldots, a_n \in R$, and therefore $\mathfrak{a} = {}_R\langle a^{-1}a_1, \ldots, a^{-1}a_n \rangle$.

2. Let $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{F}(R)$, $a \in \mathfrak{a}^\bullet$, $b \in \mathfrak{b}^\bullet$ and c, $d \in R^\bullet$ such that $c\mathfrak{a} \subset R$ and $d\mathfrak{b} \subset R$. Then $a \in \mathfrak{a} + \mathfrak{b}$ and $cd(\mathfrak{a} + \mathfrak{b}) \subset R$, hence $\mathfrak{a} + \mathfrak{b} \in \mathcal{F}(R)$. Since $(ca)(db) \in (\mathfrak{a} \cap \mathfrak{b})^\bullet$ and $\mathbf{0} \ne \mathfrak{a}^{-1} \subset (\mathfrak{a} \cap \mathfrak{b})^{-1}$, it follows that $\mathfrak{a} \cap \mathfrak{b} \in \mathcal{F}(R)$. Since $ab \in \mathfrak{a}\mathfrak{b}$ and $cd\mathfrak{a}\mathfrak{b} \subset R$, it follows that $\mathfrak{a}\mathfrak{b} \in \mathcal{F}(R)$, and finally $\mathbf{0} \ne \mathfrak{a} \subset (\mathfrak{a}^{-1})^{-1}$ implies $\mathfrak{a}^{-1} \in \mathcal{F}(R)$.

3. (a) By Theorem `completemodules` 2.2.5.6, R is noetherian, and as $M \ne \mathbf{0}$ is a finitely generated $\mathbb{Z}$-module, it is a finitely generated R-module. Hence $M \in \mathcal{F}(R)$ by 1.(b).

(b) If R is an order and $M \in \mathcal{F}(R)$, then R is noetherian, hence $M \neq \mathbf{0}$ is a finitely generated R-module, and by Theorem `completemodules` 2.2.5.4, $M \subset K$ is a complete module. ☐

`invertible` **Theorem and Definition 2.4.3.** *Let R be a domain and $K = \mathsf{q}(R)$.*

1. *Let $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{F}(R)$ and $\mathfrak{a}\mathfrak{b} = R$. Then $\mathfrak{a}$ is invertible, and $\mathfrak{b} = \mathfrak{a}^{-1}$. In particular, $(\mathcal{F}(R), \cdot)$ is a commutative monoid with unit element R, $\mathcal{F}(R)^\times = \{\mathfrak{a} \in \mathcal{F}(R) \mid \mathfrak{a}$ is invertible$\}$, and if $\mathfrak{a} \in \mathcal{F}(R)$, then $\mathfrak{a}^{-1}$ is its inverse in $\mathcal{F}(R)^\times$.*
2. *If $\mathfrak{a} \in \mathcal{F}(R)^\times$, then $\mathfrak{a}$ is finitely generated.*
3. *If $\mathfrak{a} \in \mathcal{F}(R)^\times$ and $c \in K^\times$, then $c\mathfrak{a} \in \mathcal{F}(R)^\times$, and $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$.*
4. *If $a \in K^\times$, then $aR \in \mathcal{F}(R)^\times$, and the map*

   $$\partial \colon K^\times \;\to\; \mathcal{F}(R)^\times\,, \quad \textit{defined by} \quad \partial a = aR\,,$$

   is a group homomorphism, $\operatorname{Ker}(\partial) = R^\times$, *and* $\partial(K^\times) = (K^\times) \subset \mathcal{F}(R)^\times$.

   The factor group $\mathcal{C}(R) = \mathcal{F}(R)/(K^\times)$ is called the *ideal class group* or *Picard group* of R. For $\mathfrak{a} \in \mathcal{F}(R)^\times$ we denote by $[\mathfrak{a}] \in \mathcal{C}(R)$ the ideal class containing $\mathfrak{a}$. As $[c\mathfrak{a}] = [\mathfrak{a}]$ for all $c \in K^\times$, we obtain $\mathcal{C}(R) = \{[\mathfrak{a}] \mid \mathfrak{a} \in \mathcal{I}(R)\}$.

   Two fractional ideals $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{F}(R)$ are called *equivalent*, $\mathfrak{a} \sim \mathfrak{b}$ if $[\mathfrak{a}] = [\mathfrak{b}] \in \mathcal{C}(R)$.

   There is an exact sequence $\mathbf{1} \;\to\; R^\times \;\hookrightarrow\; K^\times \;\xrightarrow{\partial} \mathcal{F}(R)^\times \;\to\; \mathcal{C}(R) \;\to\; \mathbf{1}\,.$

Proof. 1. If $\mathfrak{a}\mathfrak{b} = R$, then $\mathfrak{b} \subset \mathfrak{a}^{-1}$, and $\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$. Hence $\mathfrak{b} = \mathfrak{a}^{-1}$, and the remaining assertions are obvious.

2. If $\mathfrak{a} \in \mathcal{F}(R)^\times$, then there exist $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathfrak{a}$ and $c_1, \ldots, c_n \in \mathfrak{a}^{-1}$ such that

$$\sum_{i=1}^{n} a_i c_i = 1\,.$$

For all $c \in \mathfrak{a}$, it follows that $c_i c \in R$ for all $i \in [1, n]$, and therefore

$$c = \sum_{i=1}^{n} a_i c_i c \in {}_R\langle a_1, \ldots, a_n\rangle\,.$$

Hence $\mathfrak{a} = {}_{\,}\langle a_1, \ldots, a_n\rangle$.

3. and 4. Obvious. ☐

Definition 2.4.4. A domain R is called a *Dedekind domain* if it is noetherian, integrally closed, and every non-zero prime ideal of R is maximal. For a Dedekind domain R, we denote by $\mathcal{P}(R) = \max(R)$ the set of all non-zero prime ideals of R.

`isdedekind` **Theorem 2.4.5.** *Every principal ideal domain is a Dedekind domain.*

Proof. Let R be a principal ideal domain. Then R is noetherian and factorial. By Theorem `factorialclosed` 2.1.2 R is integrally closed. Let pR be a non-zero prime ideal of R and $pR \subset aR \subsetneq R$ for some $a \in R \setminus R^\times$. Then $p = ab$ for some $b \in R$, and as $a \notin R^\times$, we obtain $b \in R^\times$ and $pR = aR$. Thus every non-zero prime ideal of R is maximal. ☐

`dekindlemma` **Lemma 2.4.6.** *Let R be a Dedekind domain and $\mathfrak{a} \in \mathcal{I}(R)$.*

1. *There exist some* $n \in \mathbb{N}$ *and* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P}(R)$ *such that* $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset \mathfrak{a}$.
2. *If* $\mathfrak{p} \in \mathcal{P}(R)$, *then* $\mathfrak{a}\mathfrak{p}^{-1} \supsetneq \mathfrak{a}$.

Proof. 1. Assume the contrary. As R is noetherian, the set of all non-zero ideals of R which do not contain a product of principal ideals has a maximal element, say $\mathfrak{a}$. Then $\mathfrak{a} \notin \mathcal{P}(R)$, and thus there exist $b,\, c \in R \setminus \mathfrak{a}$ such $bc \in \mathfrak{a}$. Since $\mathfrak{a} \subsetneq \mathfrak{a} + bR$ and $\mathfrak{a} \subsetneq \mathfrak{a} + cR$, there exist $\mathfrak{p}_1, \ldots, \mathfrak{p}_r,\, \mathfrak{q}_1, \ldots, \mathfrak{q}_s \in \mathcal{P}(R)$ such that $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset \mathfrak{a} + bR$ and $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \subset \mathfrak{a} + cR$. Hence we obtain $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \subset (\mathfrak{a} + bR)(\mathfrak{a} + cR) \subset \mathfrak{a}$, a contradiction.

2. Since $\mathfrak{p}^{-1} \supset R$, we obtain $\mathfrak{a}\mathfrak{p}^{-1} \supset \mathfrak{a}$, and we assume to the contrary that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. For all $x \in \mathfrak{p}^{-1}$ we have $x\mathfrak{a} \subset \mathfrak{a}$, and thus x is integral over R by Theorem maincriterion 2.1.3. Hence it follows that $\mathfrak{p}^{-1} \subset R$ and thus $\mathfrak{p}^{-1} = R$. Let $a \in \mathfrak{p}^\bullet$, and let $r \in \mathbb{N}$ be minimal such that $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset aR$ for some $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ (this exists by 1.). Then it follows that $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset \mathfrak{p}$, and thus there exists some $i \in [1, r]$ such that $\mathfrak{p}_i \subset \mathfrak{p}$, say $\mathfrak{p}_1 \subset \mathfrak{p}$, and thus $\mathfrak{p}_1 = \mathfrak{p}$. By the minimal choice of r, we obtain $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \not\subset aR$. If $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \setminus aR$, then $a^{-1}b \notin R$, $b\mathfrak{p} \subset \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset aR$, hence $a^{-1}b\mathfrak{p} \subset R$ and thus $a^{-1}b \in \mathfrak{p}^{-1} \setminus R$, a contradiction. □

Theorem 2.4.7. *Let R be a domain. Then the following assertions are equivalent*:

(a) *R is a Dedekind domain.*

(b) *Every non-zero ideal $\mathfrak{a} \in \mathcal{I}(R)$ is invertible.*

(c) $\mathcal{F}(R)^\times = \mathcal{F}(R)$.

Proof. (a) ⇒ (b) Assume the contrary. Then the set of non-zero ideals which are not invertible contains a maximal element, say $\mathfrak{a}$. Let $\mathfrak{p} \in \mathcal{P}(R)$ be such that $\mathfrak{a} \subset \mathfrak{p}$. Then $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset R$ by Lemma dedekindlemma 2.4.6, and therefore $\mathfrak{a}\mathfrak{p}^{-1}$ is an invertible ideal. If $\mathfrak{b} \in \mathcal{F}(R)$ is such that $\mathfrak{a}\mathfrak{p}^{-1}\mathfrak{b} = R$, then $\mathfrak{p}^{-1}\mathfrak{b} \in \mathcal{F}(R)$, and thus $\mathfrak{a}$ is invertible, a contradiction.

(b) ⇒ (c) If $\mathfrak{a} \in \mathcal{F}(R)$, then there exists some $c \in R^\bullet$ such that $c\mathfrak{a} \in \mathcal{I}(R)$. Hence $c\mathfrak{a}$ is invertible, and thus $\mathfrak{a}$ is also invertible.

(c) ⇒ (a) Every $\mathfrak{a} \in \mathcal{I}(R) \subset \mathcal{F}(R)$ is invertible and thus finitely generated by Theorem invertible 2.4.3. Hence R is noetherian.

Let $x \in K = \mathsf{q}(R)$ be integral over R. Then $R[x]$ is a finitely generated R-module by Theorem mainintegral 2.1.4, hence $R[x] \in \mathcal{F}(R)$, and $R = R[x]^{-1}R[x] = R[x]^{-1}R[x]R[x] = R[x]$ and thus $x \in R$. Hence R is integrally closed.

Let $\mathfrak{p} \subset R$ be a non-zero prime ideal, and suppose that $\mathfrak{p}$ is not maximal. Then there exists some $\mathfrak{q} \in \mathcal{I}(R)$ such that $\mathfrak{p} \subsetneq \mathfrak{q}$, and we obtain $\mathfrak{p}\mathfrak{q}^{-1} \subset \mathfrak{q}\mathfrak{q}^{-1} = R$, since $\mathfrak{q}$ is invertible. Hence it follows that $\mathfrak{p} = (\mathfrak{p}\mathfrak{q}^{-1})\mathfrak{q}$, and as $\mathfrak{q} \not\subset \mathfrak{p}$, we get $\mathfrak{p}\mathfrak{q}^{-1} \subset \mathfrak{p}$ and therefore $\mathfrak{q}^{-1} = \mathfrak{p}^{-1}\mathfrak{p}\mathfrak{q}^{-1} \subset \mathfrak{p}^{-1}\mathfrak{p} = R$, a contradiction. □

Remarks and Definitions 2.4.8.

1. A partially ordered set $(X, \le)$ is called a *lattice* if any two elements $a,\, b \in X$ possess a supremum $\sup\{a, b\}$ and an infimum $\inf\{a, b\}$.
2. Let $(X, \le)$ and $(Y, \le)$ be lattices. A bijective map $f\colon X \to Y$ is called a *lattice isomorphism* if, for all $a,\, b \in X$, $a \le b$ holds if and only if $f(a) \le f(b)$. If f is a lattice isomorphism, then $\sup\{f(a),\, f(b)\} = f(\sup\{a, b\})$ and $\inf\{f(a),\, f(b)\} = f(\inf\{a, b\})$ for all $a,\, b \in X$.

3. A *lattice-ordered group* $(G, \cdot, \le)$ is an abelian group $(G, \cdot)$ with a partial ordering $\le$ such that $(G, \le)$ is a lattice and $a \le b$ implies $ac \le bc$ for all a, b, $c \in G$. An *isomorphism of lattice-ordered groups* is a group isomorphism which is a lattice isomorphism.
4. Let I be a set, $X = \mathbb{Z}^{(I)} = \{(x_i)_{i \in I} \in \mathbb{Z}^I \mid x_i = 0 \text{ for almost all } i \in I\}$ or $X = \mathbb{N}_0^{(I)} = \mathbb{Z}^{(I)} \cap \mathbb{N}_0^I$. For $(x_i)_{i\in I}$, $(y_i)_{i \in I} \in X$, we define $(x_i)_{i\in I} \le (y_i)_{i\in I}$ if $x_i \le y_i$ for all $i \in I$. Then $(X, \le)$ is a lattice, and for all $(x_i)_{i\in I}$, $(y_i)_{i\in I} \in X$, we have $\sup\{(x_i)_{i\in I}, (y_i)_{i\in I}\} = (\max\{x_i, y_i\})_{i\in I}$ and $\inf\{(x_i)_{i\in I}, (y_i)_{i\in I}\} = (\min\{x_i, y_i\})_{i\in I}$.
5. Let R be a domain. Then $(\mathcal{F}(R), \supset)$ is a lattice, and for all $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{F}(R)$ we have $\sup\{\mathfrak{a}, \mathfrak{b}\} = \mathfrak{a} \cap \mathfrak{b}$, and $\inf\{\mathfrak{a}, \mathfrak{b}\} = \mathfrak{a} + \mathfrak{b}$. If R is a Dedekind domain, then $(\mathcal{F}(R)^\times, \cdot, \supset)$ is a lattice-ordered group.

`edekindmain`

Theorem and Definition 2.4.9. *Let R be a Dedekind domain.*

1. *Every $\mathfrak{a} \in \mathcal{I}(R)$ is a product of prime ideals, and this product representation is unique up to the order of the factors.*
2. *Every $\mathfrak{a} \in \mathcal{F}(R)$ has a unique representation*

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathcal{P}(R)} \mathfrak{p}^{\nu_\mathfrak{p}}\,, \quad \textit{where} \quad \nu_\mathfrak{p} \in \mathbb{Z}\,, \quad \textit{and} \quad \nu_\mathfrak{p} = 0 \quad \textit{for almost all} \quad \mathfrak{p} \in \mathcal{P}(R)\,.$$

   In this representation we have $\nu_\mathfrak{p} \ge 0$ for all $\mathfrak{p} \in \mathcal{P}(R)$ if and only if $\mathfrak{a} \in \mathcal{I}(R)$.

   For $\mathfrak{a} \in \mathcal{F}(R)$ and $\mathfrak{p} \in \mathcal{P}(R)$, the integer $\mathsf{v}_\mathfrak{p}(\mathfrak{a}) = \nu_\mathfrak{p}$ is called the $\mathfrak{p}$-*adic value* of $\mathfrak{a}$.
3. *For each $\mathfrak{p} \in \mathcal{P}(R)$, the map $\mathsf{v}_\mathfrak{p} \colon \mathcal{F}(R) \to \mathbb{Z}$ is a group epimorphism, $\mathsf{v}_\mathfrak{p}(\mathfrak{p}) = 1$, $\mathcal{F}(R)$ is a free abelian group with basis $\mathcal{P}(R)$, and the map*

$$\mathsf{v} = (\mathsf{v}_\mathfrak{p})_{\mathfrak{p} \in \mathcal{P}(R)} \colon \mathcal{F}(R) \overset{\sim}{\to} \mathbb{Z}^{(\mathcal{P}(R))}\,, \quad \textit{given by} \quad \mathsf{v}(\mathfrak{a}) = (\mathsf{v}_\mathfrak{p}(\mathfrak{a}))_{\mathfrak{p} \in \mathcal{P}(R)}\,,$$

   is an isomorphism of lattice-ordered groups. In particular, if $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{F}(R)$, then
   - *$\mathfrak{a} \subset \mathfrak{b}$ if and only if $\mathsf{v}_\mathfrak{p}(\mathfrak{a}) \ge \mathsf{v}_\mathfrak{p}(\mathfrak{b})$ for all $\mathfrak{p} \in \mathcal{P}(R)$,*
   - *$\mathsf{v}_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \min\{\mathsf{v}_\mathfrak{p}(\mathfrak{a}), \mathsf{v}_\mathfrak{p}(\mathfrak{b})\}$ for all $\mathfrak{p} \in \mathcal{P}(R)$, and*
   - *$\mathsf{v}_\mathfrak{p}(\mathfrak{a} \cap \mathfrak{b}) = \max\{\mathsf{v}_\mathfrak{p}(\mathfrak{a}), \mathsf{v}_\mathfrak{p}(\mathfrak{b})\}$ for all $\mathfrak{p} \in \mathcal{P}(R)$.*
4. For $\mathfrak{p} \in \mathcal{P}(R)$, the map

$$\mathsf{v}_\mathfrak{p} \colon K \to \mathbb{Z} \cup \{\infty\}\,, \quad \text{defined by} \quad \mathsf{v}_\mathfrak{p}(x) = \begin{cases} \mathsf{v}_\mathfrak{p}(xR) & \text{if} \quad x \in K^\times\,, \\ \infty & \text{if} \quad x = 0\,, \end{cases}$$

   is called the $\mathfrak{p}$-*adic valuation* or $\mathfrak{p}$-*adic exponent* of K. *For all x, $y \in K$ and $\mathfrak{p} \in \mathcal{P}(R)$, we have*

$$\mathsf{v}_\mathfrak{p}(xy) = \mathsf{v}_\mathfrak{p}(x) + \mathsf{v}_p(y) \quad \textit{and} \quad \mathsf{v}_\mathfrak{p}(x+y) \ge \min\{\mathsf{v}_\mathfrak{p}(x), \mathsf{v}_\mathfrak{p}(y)\}\,.$$

5. *The following assertions are equivalent*:
   - (a) *R is factorial.*
   - (b) *R is a principal ideal domain.*
   - (c) *$|\mathcal{C}(R)| = 1$.*

Proof. 1. *Existence*: Assume the contrary. Then the set of all non-zero ideals of R which are not a product of prime ideals contains a maximal element, say $\mathfrak{a}$. Then $\mathfrak{a} \notin \mathcal{P}(R)$, and there exists some $\mathfrak{p} \in \mathcal{P}(R)$ such that $\mathfrak{a} \subsetneq \mathfrak{p}$. By Lemma `dedekindlemma` 2.4.6, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = R$, and therefore $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$ for some $r \in \mathbb{N}$ and $\mathfrak{p}_2, \ldots \mathfrak{p}_r \in \mathcal{P}(R)$. But then $\mathfrak{a} = \mathfrak{p}\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$, a contradiction.

Uniqueness: Let $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$, for some $r,\, s \in \mathbb{N}_0$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r,\, \mathfrak{q}_1, \ldots, \mathfrak{q}_s \in \mathcal{P}(R)$, and prove uniqueness by induction on $r+s$. If r_0 or $s = 0$, then $r = s = 0$, and there is nothing to do. Thus suppose that $r,\, s \in \mathbb{N}$. Then $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \subset \mathfrak{p}_1$, and thus there exists some $i \in [1, s]$ such that $\mathfrak{q}_i \subset \mathfrak{p}_1$. After renumbering if necessary, we may assume that $i = 1$ and obtain $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s$. By the induction hypothesis, it follows that $r = s$ and, after renumbering again if necessary, $\mathfrak{p}_i = \mathfrak{q}_i$ for all $i \in [2, r]$.

2. Let $\mathfrak{a} \in \mathcal{F}(R)$.

Existence: Let $c \in R^\bullet$ be such that $c\mathfrak{a} \in \mathcal{J}(R)$. Then $c\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ and $cR = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$ for some $r,\, s \in \mathbb{N}_0$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r,\, \mathfrak{q}_1, \ldots, \mathfrak{q}_s \in \mathcal{P}(R)$ by 1, hence $\mathfrak{a} = (cR)^{-1}(c\mathfrak{a}) = \mathfrak{q}_1^{-1} \cdot \ldots \cdot \mathfrak{q}_s^{-1}\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, and, gathering equal powers, we obtain the existence of a representation as asserted.

Uniqueness: Assume that

$$\prod_{\mathfrak{p} \in \mathcal{P}(R)} \mathfrak{p}^{\nu_\mathfrak{p}} = \prod_{\mathfrak{p} \in \mathcal{P}(R)} \mathfrak{p}^{\mu_\mathfrak{p}}\,, \quad \text{where} \quad \nu_\mathfrak{p},\, \mu_\mathfrak{p} \in \mathbb{Z}\,, \ \text{and} \ \nu_\mathfrak{p} = \mu_\mathfrak{p} = 0 \ \text{for almost all} \ \mathfrak{p} \in \mathcal{P}(R).$$

Then it follows that

$$\prod_{\substack{\mathfrak{p} \in \mathcal{P}(R) \\ \nu_\mathfrak{p} > \mu_\mathfrak{p}}} \mathfrak{p}^{\nu_\mathfrak{p} - \mu_\mathfrak{p}} = \prod_{\substack{\mathfrak{p} \in \mathcal{P}(R) \\ \nu_\mathfrak{p} < \mu_\mathfrak{p}}} \mathfrak{p}^{\mu_\mathfrak{p} - \nu_\mathfrak{p}}\,,$$

and by the uniqueness in 1. we obtain $\nu_\mathfrak{p} = \mu_\mathfrak{p}$ for all $\mathfrak{p} \in \mathcal{P}(R)$.

3. Let $\mathfrak{a},\, \mathfrak{b} \in \mathcal{F}(R)$. Then

$$\mathfrak{a}\mathfrak{b} = \prod_{\mathfrak{p} \in \mathcal{P}(R)} \mathfrak{p}^{\mathsf{v}_\mathfrak{p}(\mathfrak{a})} \prod_{\mathfrak{p} \in \mathcal{P}(R)} \mathfrak{p}^{\mathsf{v}_\mathfrak{p}(\mathfrak{b})} = \prod_{\mathfrak{p} \in \mathcal{P}(R)} \mathfrak{p}^{\mathsf{v}_\mathfrak{p}(\mathfrak{a}) + \mathsf{v}_\mathfrak{p}(\mathfrak{b})}\,,$$

and by 2. we obtain $\mathsf{v}_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = \mathsf{v}_\mathfrak{p}(\mathfrak{a}) + \mathsf{v}_\mathfrak{p}(\mathfrak{b})$ for all $\mathfrak{p} \in \mathcal{P}(R)$. Hence $\mathsf{v}_\mathfrak{p} \colon \mathcal{F}(R) \to \mathbb{Z}$ is a group homomorphism, $\mathsf{v}_\mathfrak{p}(\mathfrak{p}) = 1$ by definition, and therefore $\mathsf{v}_\mathfrak{p}$ is surjective.

By 2., $\mathcal{F}(R)$ is a free abelian group with basis $\mathcal{P}(R)$, and $\mathsf{v} \colon \mathcal{F}(R) \to \mathbb{Z}^{(\mathcal{P}(R))}$ is a group isomorphism. It remains to prove that v is a lattice isomorphism. We must prove that, for all $\mathfrak{a},\, \mathfrak{b} \in \mathcal{F}(R)$, $\mathfrak{a} \subset \mathfrak{b}$ holds if and only if $\mathsf{v}_\mathfrak{p}(\mathfrak{a}) \ge \mathsf{v}_\mathfrak{p}(\mathfrak{b})$ for all $\mathfrak{p} \in \mathsf{P}(R)$.

Let $\mathfrak{a},\, \mathfrak{b} \in \mathcal{F}(R)$ and $\mathfrak{a} \subset \mathfrak{b}$. Then $\mathfrak{a} = \mathfrak{b}(\mathfrak{b}^{-1}\mathfrak{a})$, and since $\mathfrak{b}^{-1}\mathfrak{a} \subset \mathfrak{b}^{-1}\mathfrak{b} = R$, it follows that $\mathsf{v}_\mathfrak{p}(\mathfrak{b}^{-1}\mathfrak{a}) \ge 0$ and thus $\mathsf{v}_\mathfrak{p}(\mathfrak{a}) = \mathsf{v}_\mathfrak{p}(\mathfrak{b}) + \mathsf{v}_\mathfrak{p}(\mathfrak{b}^{-1}\mathfrak{a}) \ge \mathsf{v}_\mathfrak{p}(\mathfrak{b})$ for all $\mathfrak{p} \in \mathcal{P}(R)$. As to the converse, assume that $\mathsf{v}_\mathfrak{p}(\mathfrak{a}) \ge \mathsf{v}_\mathfrak{p}(\mathfrak{b})$ for all $\mathfrak{p} \in \mathsf{P}(R)$. Then $\gamma_\mathfrak{p} = \mathsf{v}_\mathfrak{p}(\mathfrak{a}) - \mathsf{v}_\mathfrak{p}(\mathfrak{b}) \ge 0$ for all $\mathfrak{p} \in \mathcal{P}(R)$, $\gamma_\mathfrak{p} = 0$ for almost all $\mathfrak{p} \in \mathcal{P}$, hence

$$\mathfrak{c} = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\gamma_\mathfrak{p}} \in \mathcal{J}(R)\,, \quad \text{and} \quad \mathfrak{a} = \mathfrak{b}\mathfrak{c} \subset \mathfrak{b}\,.$$

4. If $x,\, y \in K^\times$, then

$$\mathsf{v}_\mathfrak{p}(xy) = \mathsf{v}_\mathfrak{p}((xR)(yR)) = \mathsf{v}_\mathfrak{p}(xR) + \mathsf{v}_\mathfrak{p}(yR) = \mathsf{v}_\mathfrak{p}(x) + \mathsf{v}_\mathfrak{p}(y)\,,$$

and if $xy = 0$, this holds trivially. If $x,\, y,\, x+y \in K^\times$, then $(x+y)R \subset xR + yR$, and therefore

$$\mathsf{v}_\mathfrak{p}(x+y) = \mathsf{v}_\mathfrak{p}((x+y)R) \ge \mathsf{v}_\mathfrak{p}(xR + yR) = \min\{\mathsf{v}_\mathfrak{p}(xR),\, \mathsf{v}_\mathfrak{p}(yR)\} = \min\{\mathsf{v}_\mathfrak{p}(x),\, \mathsf{v}_\mathfrak{p}(y)\}\,.$$

Again, if $xy(x+y)=0$, this holds trivially.

5. (a) $\Rightarrow$ (b) By 1., it suffices to prove that every $\mathfrak{p}\in\mathcal{P}(R)$ is a principal ideal. Thus let $\mathfrak{p}\in\mathcal{P}(R)$ and $a\in\mathfrak{p}^\bullet$. Then $a\notin R^\times$, and thus $a=p_1\cdot\ldots\cdot p_r$ for some $r\in\mathbb{N}$ and prime elements $p_1,\ldots,p_r\in R$. Since $a\in\mathfrak{p}$, we obtain $p_i\in\mathfrak{p}$ for some $i\in[1,r]$, hence $p_iR\subset\mathfrak{p}$, and since every non-zero prime ideal is maximal, it follows that $\mathfrak{p}=p_iR$.

(b) $\Rightarrow$ (a) This is well known.

(b) $\Leftrightarrow$ (c) By definition. □

Remarks 2.4.10 (Ideal arithmetic in Dedekind domains)**.** Let R be a Dedekind domain. Every non-zero ideal $\mathfrak{a}\in\mathcal{I}(R)$ has a unique representation

$$\mathfrak{a}=\prod_{\mathfrak{p}\in\mathcal{P}(R)}\mathfrak{p}^{\mathsf{v}_\mathfrak{p}(\mathfrak{a})}\,,\quad\text{where}\quad \mathsf{v}_\mathfrak{p}(\mathfrak{a})\in\mathbb{N}_0\,,\ \text{and}\ \ \mathsf{v}_\mathfrak{p}(\mathfrak{a})=0\ \text{ for almost all }\ \mathfrak{p}\in\mathcal{P}(R).$$

Hence $\mathcal{I}(R)$ is a factorial monoid, $\mathcal{I}(R)^\times=\{R\}$, and the map

$$\mathcal{I}(R)\ \to\ \mathbb{N}_0^{(\mathcal{P}(R))}\,,\quad\text{defined by}\quad \mathfrak{a}\ \mapsto\ (\mathsf{v}_\mathfrak{p}(a))_{\mathfrak{p}\in\mathcal{P}(R)}\,,$$

is an isomorphism. In $\mathcal{I}(R)$, divisibility is defined by

$$\mathfrak{a}\,|\,\mathfrak{b}\quad\Longleftrightarrow\quad\mathfrak{b}=\mathfrak{a}\mathfrak{c}\ \text{ for some }\ \mathfrak{c}\in\mathcal{I}(R)\quad\Longleftrightarrow\quad\mathfrak{b}\subset\mathfrak{a}\,.$$

Consequently, $(\mathcal{I}(R),|)=(\mathcal{I}(R),\supset)$ is a lattice, and the isomorphism $\mathcal{I}(R)\xrightarrow{\sim}\mathbb{N}_0^{(\mathcal{P}(R))}$ as above is a lattice isomorphism. In $(\mathcal{I}(R),|)$, we have

$$\mathfrak{a}\cap\mathfrak{b}=\sup\{\mathfrak{a},\,\mathfrak{b}\}=\operatorname{lcm}(\mathfrak{a},\mathfrak{b})=\prod_{\mathfrak{p}\in\mathcal{P}(R)}\mathfrak{p}^{\max\{\mathsf{v}_\mathfrak{p}(\mathfrak{a}),\,\mathsf{v}_\mathfrak{p}(\mathfrak{b})\}}$$

and

$$\mathfrak{a}+\mathfrak{b}=\inf\{\mathfrak{a},\,\mathfrak{b}\}=\gcd(\mathfrak{a},\mathfrak{b})=\prod_{\mathfrak{p}\in\mathcal{P}(R)}\mathfrak{p}^{\min\{\mathsf{v}_\mathfrak{p}(\mathfrak{a}),\,\mathsf{v}_\mathfrak{p}(\mathfrak{b})\}}\,.$$

In particular, $\mathfrak{a}+\mathfrak{b}=R$ if and only if $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}$, and every fractional ideal $\mathfrak{a}\in\mathcal{F}(R)$ has a unique representation $\mathfrak{a}=\mathfrak{c}^{-1}\mathfrak{b}$, where $\mathfrak{b},\,\mathfrak{c}\in\mathcal{I}(R)$ and $\mathfrak{b}+\mathfrak{c}=R$.

Theorem 2.4.11. *Let R be a Dedekind domain, $\mathfrak{a}\in\mathcal{I}(R)$ and $\mathfrak{a}=\mathfrak{p}_1^{e_1}\cdot\ldots\cdot\mathfrak{p}_r^{e_r}$, where $r\in\mathbb{N}$, $\mathfrak{p}_1,\ldots,\mathfrak{p}_r\in\mathcal{P}(R)$ are distinct and $e_1,\ldots,e_r\in\mathbb{N}$.*

1. *For $\mathfrak{p}\in\mathcal{P}(R)$, the following assertions are equivalent*:
   (a) $\mathfrak{p}\in\{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}$.
   (b) $\mathfrak{a}\subset\mathfrak{p}$.
   (c) $\mathsf{v}_\mathfrak{p}(\mathfrak{a})\ge 1$.
2. *Let $\mathfrak{a}\in\mathcal{I}(R)$, $\mathfrak{p}\in\mathcal{P}(R)$ and $e\in\mathbb{N}_0$. Then $\mathsf{v}_\mathfrak{p}(\mathfrak{a})=e$ if and only if $\mathfrak{a}=\mathfrak{p}^e\mathfrak{b}$ for some $\mathfrak{b}\in\mathcal{I}(R)$ such that $\mathfrak{p}+\mathfrak{b}=R$.*
3. (Chinese Remainder Theorem) *There is a ring isomorphism*

$$R/\mathfrak{a}\ \xrightarrow{\sim}\ R/\mathfrak{p}_1^{e_1}\times\ldots\times R/\mathfrak{p}_r^{e_r}\,,\quad\textit{given by}\quad a+\mathfrak{a}\ \mapsto\ (a+\mathfrak{p}_1^{e_1},\ldots,a+\mathfrak{p}_r^{e_r})\,.$$

Proof. 1. and 2. are obvious, and 3. is well known. □

Theorem 2.4.12 (Extension Theorem)**.** *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, $L \supset K$ a finite field extension and $S = \mathrm{cl}_L(R)$. Then S is a Dedekind domain, $L = \mathsf{q}(S)$, and the map $j\colon \mathcal{F}(R) \to \mathcal{F}(S)$, defined by $j(\mathfrak{a}) = \mathfrak{a}S = {}_S\langle \mathfrak{a}\rangle$ is a group monomorphism.*

In particular, if K is an algebraic number field, then $\mathcal{O}_K$ is a Dedekind domain.

Proof. CASE 1: L/K is separable. By Theorem 2.1.6, S is a finitely generated R-module and a noetherian domain, $L = \mathsf{q}(S)$, and by Theorem 2.1.4, S is integrally closed. Let $\mathfrak{P} \subset S$ be a non-zero prime ideal and $\mathfrak{p} = \mathfrak{P} \cap R$. By Theorem 2.1.5 it follows that $\mathfrak{p} \in \mathcal{P}(R)$, hence $R/\mathfrak{p}$ is a field, and the inclusion $R \hookrightarrow S$ induces a monomorphism $R/\mathfrak{p} \to S/\mathfrak{P}$. We identify $R/\mathfrak{p}$ with its image. Then $R/\mathfrak{p} \subset S/\mathfrak{P}$ is an integral ring extension. By Theorem 2.1.5, $S/\mathfrak{P}$ is a field and thus $\mathfrak{P} \subset S$ is a maximal ideal. Hence S is a Dedekind domain, and $L = \mathsf{q}(S)$.

CASE 2: L/K is inseparable. Let $p = \mathrm{char}(K)$, $\overline{K} \supset L$ an algebraically closed extension field and $L_0 \subset L$ the separable closure of K in L. Then there exists some p-power $q \in \mathbb{N}$ such that $L^q \subset L_0$ and thus $L \subset L_0^{1/q} \subset \overline{K}$. By CASE 1, $S_0 = \mathrm{cl}_{L_0}(R)$ is a Dedekind domain, and since the map $x \mapsto x^{1/q}$ defines an isomorphism $L \to L_0^{1/q}$, it follows that $S_0^{1/q}$ is a Dedekind domain and $L_0^{1/q} = \mathsf{q}(S^{1/q})$. Now we prove:

A. $S_0^{1/q} = \mathrm{cl}_{L_0^{1/q}}(R)$ (and consequently $S_0^{1/q} \cap L = S$.)

Proof of **A.** If $x \in S_0^{1/q}$, then $x^q \in S_0$, hence x is integral over S_0, and thus x is integral over R. As to the converse, suppose that $x \in L_0^{1/q}$ is integral over R, and let $x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 = 0$ be an integral equation of x over R, where $d \in \mathbb{N}$ and $a_0, \ldots, a_{d-1} \in R$. Then it follows that

$$0 = (x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0)^q = (x^q)^d + a_{d-1}^q (x^q)^{d-1} + \ldots + a_1^q x^q + a_0^q\,.$$

Hence x^q is integral over R, and as $x^q \in L_0$, it follows that $x^q \in S_0$ and $x \in S_0^{1/q}$. $\square$[**A.**]

Now we prove that every non-zero ideal $\mathfrak{a} \in \mathfrak{I}(S)$ is invertible. If $\mathfrak{a} \in \mathfrak{I}(S)$, then $\widetilde{\mathfrak{a}} = \mathfrak{a}S_0^{1/q} \in \mathfrak{I}(S^{1/q})$ is $S_0^{1/q}$-invertible. Hence there exist $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \widetilde{\mathfrak{a}}$ and $x_1, \ldots, x_n \in L_0^{1/q}$ such that $x_i\widetilde{\mathfrak{a}} \in S_0^{1/q}$ for all $i \in [1,n]$ and $a_1x_1 + \ldots + a_nx_n = 1$. For $i \in [1,n]$, we have

$$a_i = \sum_{j=1}^{k_i} a_{i,j} s_{i,j}^{1/q} \quad \text{for some} \quad k_i \in \mathbb{N}\,, \ \ a_{i,j} \in \mathfrak{a} \ \text{ and } \ s_{i,j} \in S_0\,,$$

and we obtain

$$1 = \Bigl(\sum_{i=1}^{n} a_i x_i\Bigr)^q = \sum_{i=1}^{n}\sum_{j=1}^{k_i} a_{i,j}^q s_{i,j} x_i^q = \sum_{i=1}^{n}\sum_{j=1}^{k_i} a_{i,j}(s_{i,j}a_{i,j}^{q-1}x_i^q)\,.$$

Thus it suffices to prove that $s_{i,j}a_{i,j}^{q-1}x_i^q \in \mathfrak{a}^{-1}$ for all $i \in [1,n]$ and $j \in [1,k_i]$. However, $s_{i,j}a_{i,j}^{q-1}x_i^q \in L$, and $s_{i,j}a_{i,j}^{q-1}x_i^q\mathfrak{a} \subset s_{i,j}(x_i\mathfrak{a})^q \subset s_{i,j}(x_i\widetilde{\mathfrak{a}})^q \subset S_0$, and thus $s_{i,j}a_{i,j}^{q-1}x_i^q \in \mathfrak{a}^{-1}$.

Obviously, if $\mathfrak{a} \in \mathcal{F}(R)$, then $\mathfrak{a}S = {}_S\langle\mathfrak{a}\rangle \in \mathcal{F}(S)$, and clearly $\mathfrak{a}\mathfrak{b}S = (\mathfrak{a}S)(\mathfrak{b}S)$ for all $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(R)$. Hence j is a group homomorphism. If $\mathfrak{a} \in \mathrm{Ker}(j)$, then $\mathfrak{a}S = S$, hence $\mathfrak{a} \subset S \cap K = R$, and thus $\mathfrak{a} = R$ by Theorem 2.1.5. $\square$

ionbehavior

Remark and Definition 2.4.13. Let R be a Dedekind domain, $K = \mathsf{q}(R)$, $L \supset K$ a finite field extension and $S = \mathrm{cl}_L(R)$. If $\mathfrak{p} \in \mathcal{P}(R)$, then $\mathfrak{p}S \in \mathfrak{I}(S)$ and $\mathfrak{p}S \ne S$ by Theorem 2.1.5. Hence Theorem 2.4.9 implies

$$\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}\,, \quad \text{where } r \in \mathbb{N},\ \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathcal{P}(S) \text{ are distinct, and } e_1, \ldots, e_r \in \mathbb{N}.$$

For $i \in [1, r]$, the number $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ is called the *ramification index* of $\mathfrak{P}_i/\mathfrak{p}$, and the number $f(\mathfrak{P}_i/\mathfrak{p}) = \dim_{R/\mathfrak{p}} S/\mathfrak{P}_i$ is called the *inertia index* or *residue class degree* of $\mathfrak{P}_i/\mathfrak{p}$. Obviously, $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\} = \{\mathfrak{P} \in \mathcal{P}(S) \mid \mathfrak{p} \subset \mathfrak{P}\} = \{\mathfrak{P} \in \mathcal{P}(S) \mid \mathfrak{P} \cap R = \mathfrak{p}\}$. We say that a prime ideal $\mathfrak{P} \in \mathcal{P}(S)$ *lies above* $\mathfrak{p}$ if $\mathfrak{P} \cap R = \mathfrak{p}$, and in this case we write $\mathfrak{P} \,|\, \mathfrak{p}$, and consequently we obtain

$$\mathfrak{p}S = \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}\,.$$

If $\mathfrak{P} \in \mathcal{P}(S)$ and $\mathfrak{p} = \mathfrak{P} \cap R$, then $\mathfrak{P}/\mathfrak{p}$ is called

- *unramified* if $e(\mathfrak{P}/\mathfrak{p}) = 1$ and $S/\mathfrak{P} \supset R/\mathfrak{p}$ is separable, and *ramified* otherwise;
- *tamely ramified* if $\mathrm{char}(R/\mathfrak{p}) \nmid e(\mathfrak{P}/\mathfrak{p})$ and $S/\mathfrak{P} \supset R/\mathfrak{p}$ is separable, and *wildely ramified* otherwise.

If $\mathfrak{p} \in \mathcal{P}(R)$, then we say that $\mathfrak{p}$

- is *ramified* or *ramifies* in L if $e(\mathfrak{P}/\mathfrak{p}) > 1$ for at least ond $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ such that $\mathfrak{P} \,|\, \mathfrak{p}$;
- is *unramified* in L if $e(\mathfrak{P}/\mathfrak{p}) = 1$ for all $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ such that $\mathfrak{P} \,|\, \mathfrak{p}$;
- is *fully ramified* in L if there is only one $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ such that $\mathfrak{P} \,|\, \mathfrak{p}$, and $e(\mathfrak{P}/\mathfrak{p}) = [L\!:\!K]$;
- is *inert* in L if $\mathfrak{p}\mathcal{O}_L \in \mathcal{P}(\mathcal{O}_L)$;
- *splits* in L if $|\{\mathfrak{P} \in \mathcal{O}_L \mid \mathfrak{P} \cap R = \mathfrak{p}\}| > 1$;
- *splits completely* in L if $e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1$ for all $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ such that $\mathfrak{P} \,|\, \mathfrak{p}$.

Let K be an algebraic number field and $p \in \mathbb{P}$ a prime. If $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, then we write $\mathfrak{p} \,|\, p$ instead of $\mathfrak{p} \,|\, p\mathbb{Z}$, and we say tha $\mathfrak{p}$ *lies above* or *divides* p. Also, we set $e(\mathfrak{p}/p) = e(\mathfrak{p}/p\mathbb{Z})$ and $f(\mathfrak{p}/p) = f(\mathfrak{p}/p\mathbb{Z})$. Note that $f(\mathfrak{p}/p) = \dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}) = p^{f(\mathfrak{p}/p)}$. Also, in the definitions above, we speak of the behavior of p in K instead of that of $p\mathbb{Z}$.

2.5. Quotient rings

Definition 2.5.1. A commutative ring R is called *local* if $|\max(R)| = 1$, and *semilocal* if $\max(R)$ is finite.

local

Theorem 2.5.2. *A commutative ring R is local if and only if $R \setminus R^\times$ is an ideal of R, and then* $\max(R) = \{R \setminus R^\times\}$.

Proof. If $R \setminus R^\times$ is an ideal of R, then obviously $\max(R) = \{R \setminus R^\times\}$, and R is local. Thus assume that R is local with unique maximal ideal $\mathfrak{m}$. If $a \in R \setminus R^\times$, then a is containes in a maximal ideal of R by Krull's Theorem, hence $a \in \mathfrak{m}$, and therefore $\mathfrak{m} = R \setminus R^\times$. ☐

caldedekind

Theorem 2.5.3. *Let R be a semilocal domain. Then every invertible fractional ideal of R is principal. In particular, every semilocal Dedekind domain is a principal ideal domain.*

Proof. We may assume that R is not a field and $\max(R) = \{\mathfrak p_1, \ldots, \mathfrak p_r\}$ for some $r \in \mathbb N$. For $j \in [1, r]$, we set

$$\mathfrak p_j^* = \bigcap_{\substack{i=1\\ i\neq j}}^{r} \mathfrak p_i \quad \text{and obtain} \quad \mathfrak p_j^* \not\subset \mathfrak p_j\,.$$

It suffices to prove that every invertible ideal is principal. Let $\mathbf 0 \ne \mathfrak a \subset R$ be an invertible ideal. For $j \in [1, r]$, we have $\mathfrak a\mathfrak p_j^* \not\subset \mathfrak a\mathfrak p_j$, we choose some $a_j \in \mathfrak a\mathfrak p_j^* \setminus \mathfrak a\mathfrak p_j$, and we set $a = a_1 + \ldots + a_r$. As $a_j\mathfrak a^{-1} \subset R$ for all $j \in [1, r]$, it follows that $a\mathfrak a^{-1} \subset R$. If $i,\, j \in [1, r]$ and $i \ne j$, then $a_i \in \mathfrak a\mathfrak p_j \setminus \mathfrak a\mathfrak p_i$, and therefore $a \equiv a_j \not\equiv 0 \mod \mathfrak a\mathfrak p_j$. Hence it follows that $a\mathfrak a^{-1} \not\subset \mathfrak p_j$ for all $j \in [1, r]$, and thus $a\mathfrak a^{-1} = R$ by Krull's Theorem. Hence $\mathfrak a = aR$ is a principal ideal. □

ientremarks

Remarks and Definitions 2.5.4 (Quotients)**.** Let R be a domain, $K = \mathsf q(R)$ and $L \supset K$ and extension field. Let $T \subset R^\bullet$ be a multiplicatively closes subset (that means, $1 \in T$ and $TT = T$). For a subset $X \subset L$, we define

$$T^{-1}X = \{t^{-1}x \mid t \in T\,,\ x \in L\}\,.$$

By definition, $X \subset T^{-1}X \subset T^{-1}L = L$.

1. Let $S \subset L$ be a subring. Then $T^{-1}S \subset L$ is a subring, $T^{-1}R \subset T^{-1}S$, and $\mathsf q(T^{-1}S) = \mathsf q(S) \subset L$. If $M \subset L$ is an S-module, then $T^{-1}M$ is a $T^{-1}S$-module, and if $E \subset M$ is such that $M = {}_S\langle E\rangle$, then $T^{-1}M = {}_{T^{-1}S}\langle E\rangle$.

   Proof. Obviously, $T^{-1}S \subset L$ is a subring, $T^{-1}R \subset T^{-1}S$, $\mathsf q(T^{-1}S) = \mathsf q(S) \subset L$, $T^{-1}M \subset L$ is a $T^{-1}S$-module, and ${}_{T^{-1}S}\langle E\rangle \subset T^{-1}M$. If $\frac{x}{t} \in T^{-1}M$, where $x \in M = {}_S\langle E\rangle$ and $t \in T$, then $x = s_1u_1 + \ldots + s_nu_n$, where $s_\nu \in S$, $u_\nu \in E$, and $\frac{x}{t} = \frac{s_1}{t}u_1 + \ldots + \frac{s_n}{t}u_n \in {}_{T^{-1}S}\langle E\rangle \subset T^{-1}M$. □

2. Let $V \subset R^\bullet$ be another multiplicatively closed subset and $M \subset L$ an R-module. Then $TV \subset R$ and $T^{-1}V \subset T^{-1}R$ are multiplicatively closed subsets, and

   $$(T^{-1}V)^{-1}(T^{-1}M) = (TV)^{-1}M\,.$$

   Proof. Obviously, $TV \subset R$ and $T^{-1}V \subset T^{-1}R$ are multiplicatively closed subsets. If $x \in M$, $t,\, t' \in T$ and $v \in V$, then the identities

   $$\frac{\frac{x}{t}}{\frac{v}{t'}} = \frac{t'x}{tv} \quad \text{and} \quad \frac{x}{tv} = \frac{\frac{x}{t}}{\frac{v}{1}}$$

   show that $(T^{-1}V)^{-1}(T^{-1}M) = (TV)^{-1}M$. □

3. If $\mathfrak a \in \mathcal F(R)$, then $T^{-1}\mathfrak a = \mathfrak a T^{-1}R \in \mathcal F(T^{-1}R)$.

   Proof. $\mathbf 0 \ne T^{-1}\mathfrak a = \mathfrak a T^{-1}R \subset K$ is a $T^{-1}R$-module. If $c \in R^\bullet$ is such that $c\mathfrak a \subset r$, then $cT^{-1}\mathfrak a \subset T^{-1}R$, and thus $T^{-1}\mathfrak a \in \mathcal F(T^{-1}R)$. □

4. If $\mathfrak a,\, \mathfrak b \in \mathcal F(R)$, then

   $$T^{-1}(\mathfrak a \cap \mathfrak b) = T^{-1}\mathfrak a \cap T^{-1}\mathfrak b\,, \quad T^{-1}(\mathfrak a + \mathfrak b) = T^{-1}\mathfrak a + T^{-1}\mathfrak b\,, \quad \text{and} \quad T^{-1}(\mathfrak a\mathfrak b) = T^{-1}\mathfrak a T^{-1}\mathfrak b\,.$$

   In particular, the map

   $$\mathcal F(R) \to \mathcal F(T^{-}R)\,, \quad \text{defined by} \quad \mathfrak a \mapsto T^{-1}\mathfrak a\,,$$

   is a monoid homomorphism. Consequently, $\mathfrak a \in \mathcal F(R)^\times$ implies $T^{-1}\mathfrak a \in \mathcal F(T^{-1}R)^\times$, and $T^{-1}\mathfrak a^{-1} = (T^{-1}\mathfrak a)^{-1}$.

Proof. Obvious. $\square$

5. If $\mathfrak{a} \triangleleft R$, then $T^{-1}\mathfrak{a} \triangleleft T^{-1}R$, $\mathfrak{a} \subset T^{-1}\mathfrak{a} \cap R$, and $T^{-1}\mathfrak{a} = T^{-1}R$ if and only if $\mathfrak{a} \cap T \neq \emptyset$.

   Proof. If $\mathfrak{a} \triangleleft R$, then obviously $T^{-1}\mathfrak{a} \triangleleft T^{-1}R$ and $\mathfrak{a} \subset T^{-1}\mathfrak{a} \cap R$. If $T^{-1}\mathfrak{a} = T^{-1}R$, then $1 = \frac{a}{t} \in T^{-1}\mathfrak{a}$ for some $a \in \mathfrak{a}$ and $t \in T$, and thus $a = t \in \mathfrak{a} \cap T$. Conversely, if $c \in \mathfrak{a} \cap T$, then $1 = \frac{c}{c} \in T^{-1}\mathfrak{a}$ and thus $T^{-1}\mathfrak{a} = T^{-1}R$. $\square$

6. If $\mathfrak{A} \triangleleft T^{-1}R$, then $\mathfrak{A} \cap R \triangleleft R$, and $\mathfrak{A} = T^{-1}(\mathfrak{A} \cap R)$. In particular, $\mathcal{I}(T^{-1}R) = \{T^{-1}\mathfrak{a} \mid \mathfrak{a} \in \mathcal{I}(R)\}$, and if R is noetherian, then $T^{-1}R$ is also noetherian.

   Proof. If $\mathfrak{A} \triangleleft T^{-1}R$, then obviously $\mathfrak{A} \cap R \triangleleft R$ and $\mathfrak{A} \supset T^{-1}(\mathfrak{A} \cap R)$. Conversely, if $\frac{a}{s} \in \mathfrak{A}$, where $a \in R$ and $s \in T$, then $a = s\frac{a}{s} \in \mathfrak{A} \cap R$ and thus $\frac{a}{s} \in T^{-1}(\mathfrak{A} \cap R)$. Together with 4., this implies $\mathcal{I}(T^{-1}R) = \{T^{-1}\mathfrak{a} \mid \mathfrak{a} \in \mathcal{I}(R)\}$. If $\mathfrak{a} \triangleleft R$ is a finitely generated ideal of R, then 1. implies that $T^{-1}\mathfrak{a}$ is a finitely generated ideal of $T^{-1}R$. Thus, if R is noetherian, then so is $T^{-1}R$. $\square$

primeideals

Theorem 2.5.5. *Let R be a domain and $T \subset R^\bullet$ a multiplicatively closed subset. Then the maps*

$$\{\mathfrak{p} \in \operatorname{spec}(R) \mid \mathfrak{p} \cap T = \emptyset\} \;\to\; \operatorname{spec}(T^{-1}R)\,, \quad \textit{defined by} \quad \mathfrak{p} \;\mapsto\; T^{-1}\mathfrak{p}$$

and

$$\operatorname{spec}(T^{-1}R) \;\to\; \{\mathfrak{p} \in \operatorname{spec}(R) \mid \mathfrak{p} \cap T = \emptyset\}\,, \quad \textit{defined by} \quad \mathfrak{P} \;\mapsto\; \mathfrak{P} \cap R\,,$$

are mutually inverse inclusion-preserving bijective maps.

quotientremarks

Proof. If $\mathfrak{P} \in \operatorname{spec}(T^{-1}R)$, then $\mathfrak{P} \cap R \in \operatorname{spec}(R)$, and $\mathfrak{P} = T^{-1}(\mathfrak{P} \cap R)$ by 2.5.4.6. Thus we must prove:

A. If $\mathfrak{p} \in \operatorname{spec}(R)$ and $\mathfrak{p} \cap T = \emptyset$, then $T^{-1}\mathfrak{p} \in \operatorname{spec}(T^{-1}R)$, and $T^{-1}\mathfrak{p} \cap R = \mathfrak{p}$.

Let $\mathfrak{p} \in \operatorname{spec}(R)$, and suppose that $\frac{a}{s}\frac{b}{t} \in T^{-1}\mathfrak{p}$ for some $a,\, b \in R$ and $s,\, t \in T$. Then $\frac{a}{s}\frac{b}{t} = \frac{c}{w}$ for some $c \in \mathfrak{p}$ and $w \in T$. Thus we obtain $abw = cst \in \mathfrak{p}$, and as $w \notin \mathfrak{p}$, it follows that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, and consequently $\frac{a}{s} \in T^{-1}\mathfrak{p}$ or $\frac{b}{t} \in T^{-1}\mathfrak{p}$. Hence $T^{-1}\mathfrak{p} \in \operatorname{spec}(T^{-1}R)$.

Obviously, $\mathfrak{p} \subset T^{-1}\mathfrak{p} \cap R$. To prove the reverse inclusion, let $a = \frac{c}{t} \in T^{-1}\mathfrak{p} \cap R$, where $c \in \mathfrak{p}$ and $t \in T$. Then it follows that $at = c \in \mathfrak{p}$, and as $t \notin \mathfrak{p}$, we get $a \in \mathfrak{p}$. $\square$

entintegral

Theorem 2.5.6. *Let $R \subset S$ be domains and $T \subset R^\bullet$ a multiplicatively closed subset. Then*

$$\operatorname{cl}_{T^{-1}S}(T^{-1}R) = T^{-1}\operatorname{cl}_S(R)\,.$$

In particular, if R is integrally closed, then $T^{-1}R$ is also integrally closed.

Proof. Suppose that $z \in \operatorname{cl}_{T^{-1}S}(T^{-1}R) \subset T^{-1}S$, say $z = \frac{x}{t}$, where $x \in S$ and $t \in T$. Let

$$\Big(\frac{x}{t}\Big)^d + \frac{a_{d-1}}{t_{d-1}}\Big(\frac{x}{t}\Big)^{d-1} + \ldots + \frac{a_1}{t_1}\Big(\frac{x}{t}\Big) + \frac{a_0}{t_0} = 0$$

be an integral equation of z over $T^{-1}R$, where $d \in \mathbb{N}$, $a_0, \ldots a_{d-1} \in R$ and $t_0, \ldots t_{d-1} \in T$. Multiplying by $t^d t_0 \cdot \ldots \cdot t_{d-1}$ yields an equation $sx^d + b_{d-1}x^{d-1} + \ldots + b_1 x + b_0 = 0$, where $s \in S$ and $b_0, \ldots, b_{d-1} \in R$. If we multiply this equation by s^{d-1}, we obtain an integral equation for sx of R, which implies $sx \in \operatorname{cl}_S(R)$ and thus $x \in T^{-1}\operatorname{cl}_S(R)$.

Assume now that $x \in \mathrm{cl}_S(R)$ and $t \in T$, and let $x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 = 0$ be an integral equation for x over R, where $d \in \mathbb{N}$ and $a_0, \ldots, a_{d-1} \in R$. Then we obtain

$$\Big(\frac{x}{t}\Big)^d + \frac{a_{d-1}}{t}\Big(\frac{x}{t}\Big)^{d-1} + \ldots + \frac{a_1}{t^{d-1}}\frac{x}{t} + \frac{a_0}{t^d} = 0\,, \quad \text{and thus} \quad \frac{x}{t} \in \mathrm{cl}_{T^{-1}S}(T^{-1}R)\,.$$

Assume now that R is integrally closed and $K = \mathsf{q}(R)$. Then $T^{-1}K = K = \mathsf{q}(T^{-1}R)$, and $\mathrm{cl}_K(T^{-1}R) = T^{-1}(\mathrm{cl}_K(R)) = T^{-1}R$. Hence $T^{-1}R$ is integrally closed. □

`entdedekind`

Theorem 2.5.7. *Let R be a Dedekind domain and $T \subset R^\bullet$ a multiplicatively closed subset.*

1. *$T^{-1}R$ is a Dedekind domain, and $\mathcal{P}(T^{-1}R) = \{T^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}(R)\,,\ \mathfrak{p} \cap T = \emptyset\}$.*
2. *Let $\mathfrak{p} \in \mathcal{P}(R)$ be such that $\mathfrak{p} \cap T = \emptyset$. Then $\mathsf{v}_{T^{-1}\mathfrak{p}}(T^{-1}\mathfrak{a}) = \mathsf{v}_\mathfrak{p}(\mathfrak{a})$ for all $\mathfrak{a} \in \mathcal{F}(R)$, and $\mathsf{v}_{T^{-1}\mathfrak{p}} = \mathsf{v}_\mathfrak{p} \colon K \to \mathbb{Z} \cup \{\infty\}$.*

Proof. 1. By `quotientremarks` 2.5.4.6, R is noetherian, by Theorem `quotientintegral` 2.5.6 R is integrally closed, and by Theorem `quotientprimeideals` 2.5.5 it follows that $\mathcal{P}(T^{-1}R) = \{T^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}(R)\,,\ \mathfrak{p} \cap T = \emptyset\}$ and every non-zero prime ideal of $T^{-1}R$ is maximal. Hence $T^{-1}R$ is a Dedekind domain.

2. If $\mathfrak{a} \in \mathcal{F}(R)$, then, by Theorem `quotientprimeideals` 2.5.5,

$$\mathfrak{a} = \mathfrak{p}^{\mathsf{v}_\mathfrak{p}(\mathfrak{a})} \prod_{\substack{\mathfrak{q} \in \mathcal{P}(R) \\ \mathfrak{q} \ne \mathfrak{p}}} \mathfrak{q}^{\mathsf{v}_\mathfrak{q}(\mathfrak{a})} \quad \text{implies} \quad T^{-1}\mathfrak{a} = (T^{-1}\mathfrak{p})^{\mathsf{v}_\mathfrak{p}(\mathfrak{a})} \prod_{\substack{\mathfrak{q} \in \mathcal{P}(R) \\ \mathfrak{q} \ne \mathfrak{p}\,,\ T \cap \mathfrak{q} = \emptyset}} (T^{-1}\mathfrak{q})^{\mathsf{v}_\mathfrak{q}(\mathfrak{a})}\,,$$

and therefore $\mathsf{v}_{T^{-1}\mathfrak{p}}(T^{-1}\mathfrak{a}) = \mathsf{v}_\mathfrak{p}(\mathfrak{a})$. If $x \in K^\times$, then $\mathsf{v}_{T^{-1}\mathfrak{p}}(x) = \mathsf{v}_{T^{-1}\mathfrak{p}}(xT^{-1}R) = \mathsf{v}_\mathfrak{p}(xR) = \mathsf{v}_\mathfrak{p}(x)$. □

2.6. Localization

Definition 2.6.1. Let R be a domain, $K = \mathsf{q}(R)$, $L \supset K$ an extension field and $\mathfrak{p} \in \mathrm{spec}(R)$. For a subset $X \subset L$, we call $X_\mathfrak{p} = (R \setminus \mathfrak{p})^{-1}X$ the *localization* of X at $\mathfrak{p}$. If $R = \mathbb{Z}$ and $\mathfrak{p} = p\mathbb{Z}$ for some prime $p \in \mathbb{P}$, we set $X_{(p)} = X_{p\mathbb{Z}}$.

`ocalization`

Theorem 2.6.2. *Let R be a domain, $K = \mathsf{q}(R)$, $L \supset K$ an extension field, $M \subset L$ an R-module, $T \subset R^\bullet$ a multiplicatively closed subset, $\mathfrak{p} \in \mathrm{spec}(R)$ and $\mathfrak{p} \cap T = \emptyset$. Then $T^{-1}M$ is a $T^{-1}R$-module, $T^{-1}\mathfrak{p} \in \mathrm{spec}(T^{-1}R)$, $T^{-1}R \setminus T^{-1}\mathfrak{p} = T^{-1}(R \setminus \mathfrak{p})$, and $(T^{-1}M)_{T^{-1}\mathfrak{p}} = M_\mathfrak{p}$.*

Proof. By `quotientremarks` 2.5.4.1, $T^{-1}M$ is a $T^{-1}R$-module, and by Theorem `quotientprimeideals` 2.5.5 we get $T^{-1}\mathfrak{p} \in \mathrm{spec}(T^{-1}R)$. If $\frac{a}{t} \in T^{-1}R$, where $a \in R$ and $t \in T$, then $\frac{a}{t} \in T^{-1}\mathfrak{p}$ if and only if $a \in \mathfrak{p}$, and consequently we obtain $T^{-1}R \setminus T^{-1}\mathfrak{p} = T^{-1}(R \setminus \mathfrak{p})$. By `quotientremarks` 2.5.4.2 we get

$$\begin{aligned}(T^{-1}M)_{T^{-1}\mathfrak{p}} &= (T^{-1}R \setminus T^{-1}\mathfrak{p})^{-1}(T^{-1}M) = T^{-1}(R \setminus \mathfrak{p})^{-1}(T^{-1}M) = (T(R \setminus \mathfrak{p}))^{-1}M \\ &= (R \setminus \mathfrak{p})^{-1}M = M_\mathfrak{p}\,. \quad \square\end{aligned}$$

`ntersection`

Theorem 2.6.3. *Let R be a domain and $K = \mathsf{q}(R)$.*

1. *Let $L \supset K$ be an extension field and $M \subset L$ and R-module. Then*

$$M = \bigcap_{\mathfrak{p} \in \max(R)} M_{\mathfrak{p}} \,.$$

2. *Suppose that $R_{\mathfrak{p}}$ is integrally closed for all $\mathfrak{p} \in \max(R)$. Then R is integrally closed.*

Proof. 1. It suffices to prove: If $x \in L$ and $x \in M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \max(R)$, then $x \in M$.

Thus let $x \in L$, $x \in M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \max(R)$, and let $J = \{c \in R \mid cx \in M\}$. Then $J \not\subset \mathfrak{p}$ for all $\mathfrak{p} \in \max(R)$. Indeed, then it follows that $J = R$, hence $1 \in J$ and $x \in M$. If $\mathfrak{p} \in \max(R)$, then $x \in M_{\mathfrak{p}}$ and therefore $sx \in M$ for some $s \in R \setminus \mathfrak{p}$. Consequently, $s \in J \setminus \mathfrak{p}$.

2. Let $x \in K$ be integal over R. Then x is integral over $R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \max(R)$. Hence $x \in R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \max(R)$, and thus $x \in R$ by 1. □

`izationisok` **Theorem 2.6.4.** *Let R be a domain and $\mathfrak{p} \in \operatorname{spec}(R)$.*

1. *$R_{\mathfrak{p}}$ is a local domain with maximal ideal $\mathfrak{p}_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$.*
2. *Let $L \subset R$ be a field and $M \subset L$ and R-module.*
   (a) *If M is R-free with basis $(u_1, \ldots, u_n)$ (for some $n \in \mathbb{N}$), then $M/\mathfrak{p}M$ is $R/\mathfrak{p}$-free with basis $(u_1 + \mathfrak{p}M, \ldots, u_n + \mathfrak{p}M)$.*
   (b) *Suppose that $\mathfrak{p} \in \max(R)$ and $n \in \mathbb{N}$. Then $\mathfrak{p}^n M_{\mathfrak{p}} \cap M = \mathfrak{p}^n M$, and there is an R-module isomorphism*

$$\iota \colon M/\mathfrak{p}^n M \;\to\; M_{\mathfrak{p}}/\mathfrak{p}^n M_{\mathfrak{p}}\,, \quad \text{given by} \quad \iota(a + \mathfrak{p}^n M) = a + \mathfrak{p}^n M_{\mathfrak{p}} \quad \text{for all } a \in M.$$

By this isomorphism, we identify $M/\mathfrak{p}^n M = M_{\mathfrak{p}}/\mathfrak{p}^n M_{\mathfrak{p}}$. In particular, we obtain $R/\mathfrak{p}^n = R_{\mathfrak{p}}/\mathfrak{p}^n R_{\mathfrak{p}}$.

Proof. 1. By Theorem `quotientprimeideals` 2.5.5.

2. (a) Obviously, $M = {}_R\langle u_1, \ldots, u_n\rangle$ implies

$$M/\mathfrak{p}M = {}_R\langle u_1 + \mathfrak{p}M, \ldots, u_n + \mathfrak{p}M\rangle = {}_{R/\mathfrak{p}}\langle u_1 + \mathfrak{p}M, \ldots, u_n + \mathfrak{p}M\rangle\,,$$

and we must prove linear independence. Thus let $a_1, \ldots, a_n \in R$ be such that

$$0 = \sum_{i=1}^n (a_i + \mathfrak{p})(u_i + \mathfrak{p}M) = \sum_{i=1}^n a_i u_i + \mathfrak{p}M \in M/\mathfrak{p}M\,, \quad \text{hence} \quad x = \sum_{i=1}^n a_i u_i \in \mathfrak{p}M\,.$$

Then

$$x = \sum_{j=1}^m c_j y_j \quad \text{for some } m \in \mathbb{N},\; c_1, \ldots, c_m \in \mathfrak{p} \text{ and } y_1, \ldots, y_m \in M,$$

and for all $j \in [1, m]$ we have

$$y_j = \sum_{i=1}^n b_{j,i} u_i \;\text{ for some }\; b_{j,1}, \ldots b_{j,n} \in R\,, \quad \text{and} \quad x = \sum_{i=1}^n \Bigl(\sum_{j=1}^m b_{j,i} c_j\Bigr) u_i\,,$$

hence

$$a_i = \sum_{j=1}^m b_{j,i} c_j \in \mathfrak{p} \quad \text{and} \quad a_i + \mathfrak{p} = 0 \in R/\mathfrak{p} \;\text{ for all }\; i \in [1, n]\,.$$

(b) Obviously, $\mathfrak{p}^n M \subset \mathfrak{p}^n M_{\mathfrak{p}} \cap M$. To prove the reverse inclusion, let $c \in \mathfrak{p}^n M_{\mathfrak{p}} \cap M$, say

$$c = \sum_{j=1}^{m} \frac{a_j u_j}{s}\,, \quad \text{where} \quad a_j \in \mathfrak{p}^n,\ u_j \in M \quad \text{and} \quad s \in R \setminus \mathfrak{p}\,.$$

Since $R = \mathfrak{p}^n + sR$, there exist some $b \in \mathfrak{p}^n$ and $t \in R$ such that $1 = b + st$, and consequently

$$c = bc + stc = bc + \sum_{j=1}^{m} a_j t u_j \ \in \mathfrak{p}^n M\,.$$

In particular, it follows that ι is injective. To prove sujectivity, let $z = \frac{u}{s} \in M_{\mathfrak{p}}$, where $u \in M$ and $s \in R \setminus \mathfrak{p}$. As above, there exist $b \in \mathfrak{p}^n$ and $t \in R$ such that $1 = b + st$. Then $z - ut = z(1 - st) = zb \in \mathfrak{p}^n M_{\mathfrak{p}}$, and therefore $z + \mathfrak{p}^n M_{\mathfrak{p}} = \iota(ut + \mathfrak{p}^n M)$. $\square$

Definition 2.6.5. A domain R is called a *discrete valuation domain* or *dv-domain* if it is a Dedekind domain, and $|\mathcal{P}(R)| = 1$.

`dv` **Theorem 2.6.6.** *Let R be a domain and $K = \mathsf{q}(R)$.*

1. *R is a dv-domain if and only if R is a local principal ideal domain and not a field.*
2. *Let R be a dv-domain, $\mathcal{P}(R) = \{\mathfrak{p}\}$ and $\pi \in K$ such that $\mathsf{v}_{\mathfrak{p}}(\pi) = 1$. Then*

   $$R = \{x \in K \mid \mathsf{v}_{\mathfrak{p}}(x) \ge 0\}\,, \quad R^\times = \{x \in K \mid \mathsf{v}_{\mathfrak{p}}(x) = 0\}\,,$$

   and $\mathfrak{p} = \{x \in K \mid \mathsf{v}_{\mathfrak{p}}(x) > 0\} = R \setminus R^\times = \pi R$. If $x \in K^\times$, then $x = \pi^{\mathsf{v}_{\mathfrak{p}}(x)} u$, where $u \in R^\times$, and if $\mathfrak{a} \in \mathcal{F}(R)$, then $\mathfrak{a} = \pi^{\mathsf{v}_{\mathfrak{p}}(\mathfrak{a})} R$.
3. *R is a Dedekind domain if and only if R is noetherian and, for all $\mathfrak{p} \in \max(R)$, $R_{\mathfrak{p}}$ is a dv-domain.*
4. *Let R be a Dedekind domain and $\mathfrak{p} \in \mathcal{P}(R)$. Then*

   $$R_{\mathfrak{p}} = \{x \in K \mid \mathsf{v}_{\mathfrak{p}}(x) \ge 0\}\,, \quad \mathsf{v}_{\mathfrak{p}R_{\mathfrak{p}}} = \mathsf{v}_{\mathfrak{p}} \colon K \to \mathbb{Z} \cup \{\infty\}\,,$$

   and if $\mathfrak{a} \in \mathcal{F}(R)$, then $\mathsf{v}_{\mathfrak{p}R_{\mathfrak{p}}}(\mathfrak{a}R_{\mathfrak{p}}) = \mathsf{v}_{\mathfrak{p}}(\mathfrak{a})$ and $\dim_{R/\mathfrak{p}}(\mathfrak{a}/\mathfrak{a}\mathfrak{p}) = 1$.

PROOF. 1. Let R be a dv-domain. As $|\mathcal{P}(R)| = 1$, it follows that R is local and not a field. By Theorem `semilocaldedekind` 2.5.3, R is a principal ideal domain. Conversely, if R is a local principal ideal domain and not a field, then R is a Dedekind domain by Theorem `principalisdedekind` 2.4.5, and $|\mathcal{P}(R)| = 1$.

2. If $\mathcal{P}(R) = \{\mathfrak{p}\}$, then $R \setminus R^\times = \mathfrak{p} = \pi R$ by Theorem `local` 2.5.2, where $\pi \in K$ is any element satisfying $\mathsf{v}_{\mathfrak{p}}(\pi) = 1$ by Theorem `dedekindmain` 2.4.9. Now all assertion follow by Theorem `dedekindmain` 2.4.9.

3. If R is a Dedekind domain and $\mathfrak{p} \in \mathcal{P}(R)$, then $R_{\mathfrak{p}}$ is a Dedekind domain by Theorem `quotientdedekind` 2.5.7. Assume now that R is noetherian and $R_{\mathfrak{p}}$ is a dv-domain for all $\mathfrak{p} \in \max(R)$. By Theorem `intersection` 2.6.3,

$$R = \bigcap_{\mathfrak{p} \in \max(R)} R_{\mathfrak{p}} \quad \text{is integrally closed}\,,$$

and it remains to prove that every non-zero prime ideal of R is maximal. Thus assume that $\mathbf{0} \ne \mathfrak{p} \subset R$ is a prime ideal, and let $\overline{\mathfrak{p}} \subset R$ be a maximal ideal such that $\mathfrak{p} \subset \overline{\mathfrak{p}}$. Then $\mathbf{0} \ne \mathfrak{p}R_{\overline{\mathfrak{p}}} \subset \overline{\mathfrak{p}}R_{\overline{\mathfrak{p}}} \subset R_{\overline{\mathfrak{p}}}$ are prime ideals, hence $\mathfrak{p}R_{\overline{\mathfrak{p}}} = \overline{\mathfrak{p}}R_{\overline{\mathfrak{p}}}$, and $\mathfrak{p} = \mathfrak{p}R_{\overline{\mathfrak{p}}} \cap R = \overline{\mathfrak{p}}R_{\overline{\mathfrak{p}}} \cap R = \overline{\mathfrak{p}}$.

4. By Theorem `quotientdedekind` 2.5.7 it follows that $\mathsf{v}_{\mathfrak{p}R_{\mathfrak{p}}} = \mathsf{v}_{\mathfrak{p}} \colon K \to \mathbb{Z} \cup \{\infty\}$ and $\mathsf{v}_{\mathfrak{p}R_{\mathfrak{p}}}(\mathfrak{a}R_{\mathfrak{p}}) = \mathsf{v}_{\mathfrak{p}}(\mathfrak{a})$ for all $\mathfrak{a} \in \mathcal{F}(R)$, and by 2. we obtain $R_{\mathfrak{p}} = \{x \in K \mid \mathsf{v}_{\mathfrak{p}}(x) \ge 0\}$.

For the proof of $\dim_{R/\mathfrak p}(\mathfrak a/\mathfrak a\mathfrak p) = 1$, observe that $R/\mathfrak p = R_\mathfrak p/\mathfrak p R_\mathfrak p$ and $\mathfrak a/\mathfrak a\mathfrak p = \mathfrak a R_\mathfrak p/\mathfrak a\mathfrak p R_\mathfrak p$ by Theorem 2.6.4.2. If $\pi \in K$ is an element such that $\mathsf v_\mathfrak p(\pi) = 1$, then $\mathfrak a R_\mathfrak p = \pi^{\mathsf v_\mathfrak p(\mathfrak a)} R_\mathfrak p$ and $\mathfrak a\mathfrak p R_\mathfrak p = \pi^{\mathsf v_\mathfrak p(\mathfrak a)+1} R_\mathfrak p$. The map $R_\mathfrak p \to \mathfrak a R_\mathfrak p/\mathfrak a\mathfrak p R_\mathfrak p$, defined by $x \mapsto \pi^{\mathsf v_\mathfrak p(\mathfrak a)} x + \mathfrak a\mathfrak p R_\mathfrak p$, is an $R_\mathfrak p$-module epimorphism with kernel $\pi R_\mathfrak p = \mathfrak p R_\mathfrak p$, and thus it defines an isomorphism $R_\mathfrak p/\mathfrak p R_\mathfrak p \overset{\sim}{\to} \mathfrak a R_\mathfrak p/\mathfrak a\mathfrak p R_\mathfrak p$, as asserted. ☐

2.7. Factorization in extension fields

Theorem 2.7.1. *Let R be a Dedekind domain, $K = \mathsf q(R)$, $L \supset K$ an extension field, $[L\colon K] = n$, $S = \mathrm{cl}_L(R)$, $\mathfrak p \in \mathcal P(R)$, and $\mathfrak p S = \mathfrak P_1^{e_1} \cdot \ldots \cdot \mathfrak P_r^{e_r}$, where $r \in \mathbb N$, $\mathfrak P_1, \ldots, \mathfrak P_r \in \mathcal P(S)$ are distinct, $e_i = \mathsf v_{\mathfrak P_i}(\mathfrak p S) \ge 1$ and $f_i = \dim_{R/\mathfrak p}(S/\mathfrak P_i)$ for all $i \in [1, r]$.*

1. *$S_\mathfrak p = \mathrm{cl}_L(R_\mathfrak p)$ is a semilocal principal ideal domain, $\mathcal P(S_\mathfrak p) = \{\mathfrak P_1 S_\mathfrak p, \ldots, \mathfrak P_r S_\mathfrak p\}$ and $\mathfrak p S_\mathfrak p = (\mathfrak P_1 S_\mathfrak p)^{e_1} \cdot \ldots \cdot (\mathfrak P_r S_\mathfrak p)^{e_r}$. $S/\mathfrak p S = S_\mathfrak p/\mathfrak p S_\mathfrak p$, $\mathfrak P_i S_\mathfrak p \cap R_\mathfrak p = \mathfrak p R_\mathfrak p$, $e_i = \mathsf v_{\mathfrak P_i S_\mathfrak p}(\mathfrak p S_\mathfrak p)$ and $f(\mathfrak P_i S_\mathfrak p/\mathfrak p R_\mathfrak p) = f_i$ for all $i \in [1, r]$.*
2. *We have*
$$\sum_{i=1}^r e_i f_i = \dim_{R/\mathfrak p}(S/\mathfrak p S) \le n\,, \quad \text{and equality holds if and only if } S_\mathfrak p \text{ is } R_\mathfrak p\text{-free.}$$
In particular, equality holds if L/K is separable.

Proof. 1. By Theorem 2.5.6, $S_\mathfrak p = \mathrm{cl}_L(R_\mathfrak p)$, and by Theorem 2.4.12 $S_\mathfrak p$ is a Dedekind domain. Clearly $\mathfrak p S_\mathfrak p = (\mathfrak p S)_\mathfrak p = (\mathfrak P_1 S_\mathfrak p)^{e_1} \cdot \ldots \cdot (\mathfrak P_r S_\mathfrak p)^{e_r}$, $e_i = \mathsf v_{\mathfrak P_i S_\mathfrak p}(\mathfrak p S_\mathfrak p)$ and $\mathfrak P_i S_\mathfrak p \cap R_\mathfrak p = \mathfrak p R_\mathfrak p$ for all $i \in [1, r]$. Since $\overline{\mathfrak P} \supset \mathfrak p$ for all $\overline{\mathfrak P} \in \mathcal P(S_\mathfrak p)$, we obtain $\mathcal P(S_\mathfrak p) = \{\mathfrak P_1 S_\mathfrak p, \ldots, \mathfrak P_r S_\mathfrak p\}$, and thus $S_\mathfrak p$ is semilocal. By the Theorems 2.6.2 and 2.6.4, we obtain $R/\mathfrak p = R_\mathfrak P/\mathfrak p R_\mathfrak p$ and $S_\mathfrak p/\mathfrak P_i S_\mathfrak p = (S_\mathfrak p)_{\mathfrak P_i S_\mathfrak p}/(\mathfrak P_i S_\mathfrak p)_{\mathfrak P_i S_\mathfrak p} = S_{\mathfrak P_i}/\mathfrak P_i S_{\mathfrak P_i}$, which implies $f_i = f(\mathfrak P_i S_\mathfrak p/\mathfrak p R_\mathfrak p)$ for all $i \in [1, r]$.

2. By 1., it suffices to consider $R_\mathfrak p$ instead of R, and thus we may assume that R is a dv-domain and $\mathcal P(R) = \{\mathfrak p\}$. Then $\mathcal P(S) = \{\mathfrak P_1, \ldots, \mathfrak P_r\}$, S is a semilocal principal ideal domain, and since $\mathfrak p S = \mathfrak P_1^{e_1} \cdot \ldots \cdot \mathfrak P_r^{e_r}$, it follows that
$$S/\mathfrak p S \cong \bigoplus_{i=1}^r S/\mathfrak P_i^{e_i}\,.$$
Now we proceed in three steps.

A. $\dim_{R/\mathfrak p}(S/\mathfrak P_i^{e_i}) = e_i f_i$ for all $i \in [1, r]$.

Proof of **A.** Let $i \in [1, r]$, $e = e_i$, $f = f_i$ and $\mathfrak P = \mathfrak P_i$. Then we have the descending sequence of $R/\mathfrak p$-vector spaces $S/\mathfrak P^e \supset \ldots \supset \mathfrak P^j/\mathfrak P^e \supset \ldots \supset \mathfrak P^{e-1}/\mathfrak P^e \supset \{\mathbf 0\}$ with quotient spaces
$$W_j = (\mathfrak P^j/\mathfrak P^e)/(\mathfrak P^{j+1}/\mathfrak P^e) \cong \mathfrak P^j/\mathfrak P^{j+1} \cong S/\mathfrak P \quad \text{for all } j \in [0, e-1] \text{ by Theorem 2.6.6}\,.$$
Consequently,
$$\dim_{R/\mathfrak p}(S/\mathfrak p S) = \sum_{j=0}^{e-1} \dim_{R/\mathfrak p}(W_j) = e \dim_{R/\mathfrak p}(S/\mathfrak P) = ef\,. \qquad \square[\mathbf{A.}]$$

B. If S is a free R-module, then $S/\mathfrak p S$ is a free $R/\mathfrak p$-module of rank n, and if L/K is separable, then S is a free R-module.

Proof of **B.** By the Theorems 2.6.4 and 2.1.6. $\square$[**B.**]

C. Let $m = \dim_{R/\mathfrak{p}}(S/\mathfrak{p}S)$ and $u_1, \ldots, u_m \in S$ such that $(u_1 + \mathfrak{p}S, \ldots, u_m + \mathfrak{p}S)$ is an $R/\mathfrak{p}$-basis of $S/\mathfrak{p}S$. Then $(u_1, \ldots, u_m)$ is linearly independent over R, $m \le n$, and $m = n$ if and only if S is R-free.

Proof of **C.** Suppose that $\mathfrak{p} = \pi R$.

Assume that $(u_1, \ldots, u_m)$ is linearly dependent over R, let $c_1, \ldots, c_m \in R$ be such that $c_1u_1 + \ldots + c_mu_m = 0$, and $k = \min\{\mathsf{v}_{\mathfrak{p}}(c_j) \mid j \in [1, m]\} = \mathsf{v}_{\mathfrak{p}}(c_1) < \infty$. Then $\pi^{-k}c_1 + \mathfrak{p} \ne 0$, and

$$\sum_{j=1}^{m}(\pi^{-k}c_j + \mathfrak{p})(u_j + \mathfrak{p}S) = \sum_{j=1}^{m}\pi^{-k}c_ju_j + \mathfrak{p}S = 0 \in S/\mathfrak{p}S\,,$$

a contradiction. If S is R-free, then it has a basis consisting of n elements, and thus $m = n$ by Theorem 2.6.4.

Assume now that $m = n$. Then $(u_1, \ldots, u_n)$ is a K-basis of L, and we shall prove that $S = {}_R\langle u_1, \ldots, u_n\rangle$. Let $x \in S$, $x = b_1u_1 + \ldots + b_nu_n$, where $b_1, \ldots, b_n \in K$, not all in R, and assume that $k = \min\{\mathsf{v}_{\mathfrak{p}}(b_j) \mid j \in [1, m]\} = \mathsf{v}_{\mathfrak{p}}(b_1) < 0$. Then $\pi^{-k}b_j \in R$ for all $j \in [1, r]$, $\pi^{-1}b_1 + \mathfrak{p} \ne 0$, and

$$0 = \pi^{-k}x + \mathfrak{p}S = \sum_{j=1}^{m}(\pi^{-k}b_j + \mathfrak{p})(u_j + S) \in S/\mathfrak{p}S\,, \quad \text{a contradiction.} \qquad \square$$

itivityofef

Theorem 2.7.2. *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite field extension and $K \subset M \subset L$ an intermediate field. Let $S = \mathrm{cl}_L(R)$ and $T = \mathrm{cl}_M(R)$ [then $S = \mathrm{cl}_L(T)$, $R = K \cap S$ and $T = M \cap S$]. Let $\mathfrak{P} \in \mathcal{P}(S)$, $\mathfrak{q} = \mathfrak{P} \cap T$ and $\mathfrak{p} = \mathfrak{P} \cap R = \mathfrak{q} \cap R$. Then $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{q})\,e(\mathfrak{q}/\mathfrak{p})$, and $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{q})\,f(\mathfrak{q}/\mathfrak{p})$.*

Proof. By definition, $\mathfrak{p}T = \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})}\mathfrak{b}$ and $\mathfrak{q}S = \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{q})}\mathfrak{B}$, where $\mathfrak{b} \in \mathcal{J}(T)$, $\mathfrak{B} \in \mathcal{J}(S)$, $\mathfrak{q} + \mathfrak{b} = T$ and $\mathfrak{P} + \mathfrak{B} = S$. Hence $\mathfrak{p}S = \mathfrak{P}^{e(\mathfrak{q}/\mathfrak{p})e(\mathfrak{P}/\mathfrak{q})}\mathfrak{b}\mathfrak{B}$, and since $1 \in \mathfrak{q} + \mathfrak{b}$ and $1 \in \mathfrak{P} + \mathfrak{B}$, it follows that $1 \in (\mathfrak{q} + \mathfrak{b})(\mathfrak{P} + \mathfrak{B}) \subset \mathfrak{P} + \mathfrak{b}\mathfrak{B}$, hence $\mathfrak{P} + \mathfrak{b}\mathfrak{B} = S$ and $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p})e(\mathfrak{P}/\mathfrak{q})$.

From the finite field extensions $R/\mathfrak{p} \subset T/\mathfrak{q} \subset S/\mathfrak{P}$ we obtain

$$f(\mathfrak{P}/\mathfrak{p}) = [S/\mathfrak{P} \colon R/\mathfrak{p}] = [S/\mathfrak{P} \colon T/\mathfrak{q}]\,[T/\mathfrak{q} \colon R/\mathfrak{p}] = f(\mathfrak{P}/\mathfrak{q})f(\mathfrak{q}/\mathfrak{p})\,. \qquad \square$$

composition

Theorem 2.7.3. *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite galois extension, $[L\colon K] = n$, $G = \mathsf{Gal}(L/K)$, $\mathfrak{P} \in \mathcal{P}(S)$, $\mathfrak{p} = \mathfrak{P} \cap R \in \mathcal{P}(R)$, $e = e(\mathfrak{P}/\mathfrak{p})$ and $f = f(\mathfrak{P}/\mathfrak{p})$. Suppose that $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$, where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathcal{P}(S)$ are distinct, $e_1, \ldots, e_r \in \mathbb{N}$, $\mathfrak{P}_1 = \mathfrak{P}$, $e_1 = e$ and $f_1 = f$. Then $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\} = \{\sigma\mathfrak{P} \mid \sigma \in G\}$, $e_i = e$ and $f_i = f$ for all $i \in [1, r]$, and $efr = n$.*

Proof. Let $\sigma \in G$. Then $\sigma(S) = S$, and $\sigma \,|\, S \colon S \to S$ is a ring isomorphism. Hence $\sigma\mathfrak{P} \in \mathcal{P}(S)$, and $\sigma\mathfrak{P} \cap R = \sigma(\mathfrak{P} \cap R) = \sigma\mathfrak{p} = \mathfrak{p}$. Since $e = e(\mathfrak{P}/\mathfrak{p})$, we obtain $\mathfrak{p}S = \mathfrak{P}^e\mathfrak{B}$, where $\mathfrak{B} \in \mathcal{J}(S)$ and $\mathfrak{P} + \mathfrak{B} = S$, $\mathfrak{p}S = \sigma(\mathfrak{P})^e\sigma\mathfrak{B}$, and $\sigma\mathfrak{P} + \sigma\mathfrak{B} = \sigma(\mathfrak{P} + \mathfrak{B}) = \sigma S = S$, which implies $e = e(\sigma\mathfrak{P}/\mathfrak{p})$. Moreover, σ induces an $R/\mathfrak{p}$-isomorphism $\sigma^* \colon S/\mathfrak{P} \to S/\sigma P$, given by $\sigma^*(a + \mathfrak{P}) = \sigma(a) + \sigma\mathfrak{P}$, and therefore $f(\sigma\mathfrak{P}/\mathfrak{p}) = \dim_{R/\mathfrak{p}} S/\sigma\mathfrak{P} = \dim_{R/\mathfrak{p}} S/\mathfrak{P} = f$.

It remains to prove that, for each $i \in [1, r]$ there exists some $\sigma \in G$ such that $\mathfrak{P}_i = \sigma\mathfrak{P}$. Assume the contrary. Then there exists some $i \in [2, r]$ such that $\mathfrak{P}_i \ne \sigma\mathfrak{P}$ for all $\sigma \in G$. By the

Chinese Remainder Theorem, there is some $x \in S$ such that $x \equiv 0 \mod \mathfrak{P}_i$ and $x \equiv 1 \mod \sigma\mathfrak{P}$ for all $\sigma \in G$. Consequently, $\sigma^{-1}(x) \equiv 1 \mod \mathfrak{P}$ for all $\sigma \in G$, and therefore

$$\mathsf{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma^{-1}(x) \in (1+\mathfrak{P}) \cap K = 1 + \mathfrak{p} \subset 1 + \mathfrak{P}_i\,.$$

On the other hand, $x \in \mathfrak{P}_i$ implies

$$\mathsf{N}_{L/K}(x) = x \prod_{\sigma \in G \setminus \{\mathrm{id}_L\}} \sigma(x) \in xS \subset \mathfrak{P}_i\,, \quad \text{a contradiction.} \qquad \square$$

ersplitting

Theorem 2.7.4 (Kummer's Weak Splitting Law)**.** *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, $\mathfrak{p} \in \mathcal{P}(R)$, and consider the residue class homomorphism*

$$R_\mathfrak{p}[X] \;\to\; R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}[X] = R/\mathfrak{p}[X]\,, \quad g \;\mapsto\; \overline{g}\,.$$

Let L/K be a finite field extension, $S = \mathrm{cl}_L(R)$ and $\alpha \in S$ such that $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$. Let $P \in R[X]$ be the minimal polynomial of α over K, and $\overline{P} = \overline{P}_1^{\,e_1} \cdot \ldots \cdot \overline{P}_r^{\,e_r}$, where $P_1, \ldots, P_r \in R[X] \setminus R$ are monic, $\overline{P}_1, \ldots, \overline{P}_r \in R/\mathfrak{p}[X]$ are irreducible and distinct, and $e_1, \ldots, e_r \in \mathbb{N}$. For $i \in [1,r]$, let $\mathfrak{P}_i = \mathfrak{p}S + P_i(\alpha)S$. Then $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathcal{P}(S)$ are distinct, $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$, and $f(\mathfrak{P}_i/\mathfrak{p}) = \deg(P_i)$ for all $i \in [1,r]$.

Proof. We set $\mathsf{k} = R/\mathfrak{p}$ and denote by $\overline{\mathsf{k}} \supset \mathsf{k}$ an algebraically closed extension field. For $i \in [1,r]$, let $\overline{\alpha}_i \in \overline{\mathsf{k}}$ be such that $\overline{P}_i(\overline{\alpha}_i) = 0$. Next we prove:

A. For every $i \in [1,r]$, there exists a unique ring homomorphism $\Phi_i \colon S \to \mathsf{k}(\overline{\alpha}_i)$ with the following propoerty: If $x \in S$ and $x = g(\alpha)$ for some polynomial $g \in R_\mathfrak{p}[X]$, then $\Phi_i(x) = \overline{g}(\overline{\alpha}_i)$.

Proof of **A.** Let $i \in [1,r]$. Uniqueness is obvious, and if Φ_i is a map with the asserted property, then it is a ring homomorphism. Thus it suffices to prove: If $x \in S$ and g, $g_1 \in R_\mathfrak{p}[X]$ are such that $x = g(\alpha) = g_1(\alpha)$, then $\overline{g}(\overline{\alpha}_i) = \overline{g}_1(\overline{\alpha}_i)$.

If g, $g_1 \in R_\mathfrak{p}[X]$ and $g(\alpha) = g_1(\alpha)$, then $(g - g_1)(\alpha) = 0$, hence $P \mid g - g_1$, $\overline{P}_i \mid \overline{P} \mid \overline{g} - \overline{g}_i$, and therefore $\overline{g}(\overline{\alpha}_i) - \overline{g}_1(\overline{\alpha}_i) = (\overline{g} - \overline{g}_i)(\overline{\alpha}_i) = 0$. $\square$[**A.**]

If $\mathfrak{P}_i = \mathrm{Ker}(\Phi_i)$, then $\mathfrak{P}_i \in \mathcal{P}(S)$, and as $\Phi \mid R \colon R \to \mathsf{k}$ is just the residue class homomorphism, we get $\mathfrak{P}_i \cap R = \mathfrak{p}$ and $f(\mathfrak{P}_i/\mathfrak{p}) = \dim_{R/\mathfrak{p}} S/\mathfrak{P}_i = [\mathsf{k}(\overline{\alpha}_i) : \mathsf{k}] = \deg(P_i)$. Therefore it remains to prove the following two assertions:

B. For all $i \in [1,r]$, we have $\mathfrak{P}_i = \mathfrak{p}S + P_i(\alpha)S\,.$

C. $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$.

Proof of **B.** Let $i \in [1,r]$. Then $\Phi_i(P_i(\alpha)) = \overline{P}_i(\overline{\alpha}_i) = 0$, and therefore it follows that $\mathfrak{p}S + P_i(\alpha)S \subset \mathrm{Ker}(\Phi_i) = \mathfrak{P}_i$. To prove the reverse inclusion, let $x \in \mathfrak{P}_i$ and $g \in R_\mathfrak{p}[X]$ be such that $x = g(\alpha)$. Then $\overline{g}(\overline{\alpha}_i) = \Phi_i(x) = 0$, hence $\overline{P}_i \mid \overline{g}$ in $\mathsf{k}[X]$, say $\overline{g} = \overline{P}_i\overline{h}$ for some $h \in R[X]$. Since $\mathsf{k}[X] = R_\mathfrak{p}[X]/\mathfrak{p}R_\mathfrak{p}[X]$, we obtain $g - P_ih \in R_\mathfrak{p}[X]$ and consequently $g(\alpha) - P_i(\alpha)h(\alpha) \in \mathfrak{p}R_\mathfrak{p}[\alpha] \cap S = \mathfrak{p}S_\mathfrak{p} \cap S = \mathfrak{p}S$ by Theorem 2.6.4. Hence it follows that $x = g(\alpha) \in \mathfrak{p}S + P_i(\alpha)S$. $\square$[**B.**]

localizationisok

Proof of **C.** We have already proved that $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\} \subset \{\mathfrak{P} \in \mathcal{P}(S) \mid \mathfrak{P} \cap R = \mathfrak{p}\}$, and we assert that equality holds. Thus let $\mathfrak{P} \in \mathcal{P}(S)$ be such that $\mathfrak{P} \cap R = \mathfrak{p}$, and consider the residue class $\overline{\alpha} = \alpha + \mathfrak{P} \in S/\mathfrak{P} = S_\mathfrak{p}/\mathfrak{P}_\mathfrak{p} \supset R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} = \mathsf{k}$. Since $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$, it follows that $S/\mathfrak{P} = \mathsf{k}[\overline{\alpha}] = \mathsf{k}(\overline{\alpha})$. Since $P(\alpha) = 0$, it follows that $\overline{P}(\overline{\alpha}) = 0$, and therefore $\overline{P}_i(\overline{\alpha}) = 0$ for some $i \in [1,r]$. Hence there exists a k-isomorphism $S/\mathfrak{P} = \mathsf{k}(\overline{\alpha}) \overset{\sim}{\to} \mathsf{k}(\overline{\alpha}_i)$ mapping $\overline{\alpha} \to \overline{\alpha}_i$. Combining it with the residue class homomorphism $S \to S/\mathfrak{P}$, we obtain a ring homomorphism $\Psi\colon S \to \mathsf{k}(\overline{\alpha}_i)$ such that $\Psi(\alpha) = \overline{\alpha}_i$, $\Psi \,|\, R\colon R \to \mathsf{k}$ is the residue class homomorphism, and consequently $\Psi(g(\alpha)) = \overline{g}(\overline{\alpha}_i)$ for every polynomial $g \in R_\mathfrak{p}[X]$. Hence it follows that $\Psi = \Phi_i$, and $\mathfrak{P} = \mathrm{Ker}(\Psi) = \mathfrak{P}_i$.

Since $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\} = \{\mathfrak{P} \in \mathcal{P}(S) \mid \mathfrak{P} \cap R = \mathfrak{p}\}$, there exist $e_1', \ldots, e_r' \in \mathbb{N}$ such that $\mathfrak{p}S = \mathfrak{P}_1^{e_1'} \cdot \ldots \cdot \mathfrak{P}_r^{e_r'}$, and we must prove $e_i' = e_i$ for all $i \in [1,r]$. Since $P_1^{e_1} \cdot \ldots \cdot P_r^{e_r} - P \in \mathfrak{p}R[X]$ and $P(\alpha) = 0$, it follows that

$$P_1(\alpha)^{e_1} \cdot \ldots \cdot P_r(\alpha)^{e_r} = (P_1^{e_1} \cdot \ldots \cdot P_r^{e_r} - P)(\alpha) \in S \cap \mathfrak{p}R[\alpha] \subset S \cap \mathfrak{p}S_\mathfrak{p} = \mathfrak{p}S = \mathfrak{P}_1^{e_1'} \cdot \ldots \cdot \mathfrak{P}_r^{e_r'}$$

and therefore

$$\prod_{i=1}^r \mathfrak{P}_i^{e_i} \;=\; \prod_{i=1}^r (\mathfrak{p}S + P_i(\alpha)S)^{e_i} \;\subset\; \mathfrak{p}S + \prod_{i=1}^r P_i(\alpha)^{e_i} S \;\subset\; \mathfrak{p}S + \prod_{i=1}^r \mathfrak{P}_i^{e_i'} \;=\; \prod_{i=1}^r \mathfrak{P}_i^{e_i'}\,.$$

Hence it follows that $e_i \ge e_i'$ for all $i \in [1,r]$, and since $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$ is $R_\mathfrak{p}$-free, we obtain

$$[L\colon K] = \sum_{i=1}^r e_i' f(\mathfrak{P}_i/\mathfrak{p}) \le \sum_{i=1}^r e_i f(\mathfrak{P}_i/\mathfrak{p}) = \deg P = [L\colon K]\,,$$

and thus it follows that $e_i = e_i'$ for all $i \in [1,r]$. □

rsplitting1

Corollary 2.7.5. *Let $p \in \mathbb{P}$ a prime. For a polynomial $h \in \mathbb{Z}[X]$, let $\overline{h} \in \mathbb{F}_p[X]$ be the residue class polynomial. Let K be an algebraic number field, $\alpha \in \mathcal{O}_K$ and $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$. Let $P \in \mathbb{Z}[X]$ be the minimal polynomial of α, and suppose that $\overline{P} = \overline{P}_1^{e_1} \cdot \ldots \cdot \overline{P}_r^{e_r} \in \mathbb{F}_p[X]$, where $r \in \mathbb{N}$, $P_1, \ldots, P_r \in \mathbb{Z}[X]$ are monic, and $\overline{P}_1, \ldots, \overline{P}_r \in \mathbb{F}_p[X]$ are distinct and irreducible.*

Then $p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$, where $\mathfrak{P}_i = p\mathcal{O}_K + P_i(\alpha)\mathcal{O}_K \in \mathcal{P}(\mathcal{O}_K)$ for all $i \in [1,r]$.

kummersplitting

Proof. By Theorem 2.7.4, it suffices to prove that $\mathcal{O}_{K,(p)} = \mathbb{Z}_{(p)}[\alpha]$. Obviously, $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ implies $\mathbb{Z}_{(p)}[\alpha] \subset \mathcal{O}_{K,(p)}$. To prove the revers inclusion, suppose that $z = \frac{c}{s} \in \mathcal{O}_{K,(p)}$, where $c \in \mathcal{O}_K$ and $s \in \mathbb{Z} \setminus p\mathbb{Z}$. Since $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$, there exists some $m \in \mathbb{N}$ such that $p \nmid m$ and $mc \in \mathbb{Z}[\alpha]$, which implies $z = \frac{mc}{ms} \in \mathbb{Z}_{(p)}[\alpha]$. □

Theorem 2.7.6 (Splitting law for quadratic number fields)**.** *Let $K = \mathbb{Q}(\sqrt{d}\,)$ be a quadratic number field, where $d \in \mathbb{Z} \setminus \{1\}$ is squarefree, and let $p \in \mathbb{P}$ be a prime.*

1. *If $p \ne 2$, $\left(\frac{d}{p}\right) = 1$ and $a \in \mathbb{Z}$ is such that $a^2 \equiv d \bmod p$, then $p\mathcal{O}_K = \mathfrak{p}_+\mathfrak{p}_-$, where $\mathfrak{p}_\pm = p\mathbb{Z} + (\sqrt{d} \pm a)\mathcal{O}_K = {}_{\mathcal{O}_K}\langle p, \sqrt{d} \pm a\rangle \in \mathcal{P}(\mathcal{O}_K)$ (p splits in K).*
2. *If $p \ne 2$ and $\left(\frac{d}{p}\right) = -1$, then $p\mathcal{O}_K \in \mathcal{P}(\mathcal{O}_K)$ (p is inert in K).*
3. *If $p \,|\, d$, then $p\mathcal{O}_K = \mathfrak{p}^2$, where $\mathfrak{p} = p\mathbb{Z} + \sqrt{d}\,\mathcal{O}_K = {}_{\mathcal{O}_K}\langle p, \sqrt{d}\rangle$ (p ramifies in K).*
4. *If $p = 2$ and $d \equiv 3 \bmod 4$, then $p\mathcal{O}_K = \mathfrak{p}^2$, where $\mathfrak{p} = 2\mathbb{Z} + (\sqrt{d} - 1)\mathcal{O}_K = {}_{\mathcal{O}_K}\langle 2, \sqrt{d} - 1\rangle$ (2 ramifies in K).*
5. *If $p = 2$ and $d \equiv 1 \bmod 8$, then $2\mathcal{O}_K = \mathfrak{p}_+\mathfrak{p}_-$, where*

$$\mathfrak{p}_\pm = 2\mathbb{Z} + \frac{1 \pm \sqrt{d}}{2}\,\mathcal{O}_K = {}_{\mathcal{O}_K}\big\langle 2, \frac{1 \pm \sqrt{d}}{2}\big\rangle \in \mathcal{P}(\mathcal{O}_K)$$

(p splits in K).

6. *If* $p=2$ *and* $d\equiv 5 \mod 8$, *then* $2\mathcal{O}_K\in\mathcal{P}(\mathcal{O}_K)$ (2 *is inert in* K).

Proof. We apply Theorem 2.7.4 and Corollary 2.7.5. Recall that

$$\mathcal{O}_K=\mathbb{Z}[\sqrt{d}\,] \text{ if } d\not\equiv 1 \mod 4\,, \quad \text{and} \quad \mathcal{O}_K=\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] \text{ if } \quad d\equiv 1 \mod 4\,.$$

CASE 1: $p\ne 2$. Then $(\mathcal{O}_K:\mathbb{Z}[\sqrt{d}])\nmid p$, $X^2-d\in\mathbb{Z}[X]$ is the minimal polynomial of $\sqrt{d}$, and we consider $X^2-\overline{d}\in\mathbb{F}_p[X]$.

- If $\big(\frac{d}{p}\big)=1$, then $\overline{d}=\overline{a}^2$ for some $a\in\mathbb{Z}\setminus p\mathbb{Z}$, and $X^2-\overline{d}=(X-\overline{a})(X+\overline{a})\in\mathbb{F}_p[X]$. Hence $p\mathcal{O}_K=\mathfrak{p}_+\mathfrak{p}_-$, where $\mathfrak{p}_\pm=p\mathbb{Z}+(\sqrt{d}\pm a)\mathcal{O}_K={}_{\mathcal{O}_K}\langle p,\sqrt{d}\pm a\rangle\in\mathcal{P}(\mathcal{O}_K)$.
- If $\big(\frac{d}{p}\big)=-1$, then $\overline{d}$ is not a square in $\mathbb{F}_p$, hence $X^2-\overline{d}\in\mathbb{F}_p[X]$ is irreducible, and therefore $p\mathcal{O}_K\in\mathcal{P}(\mathcal{O}_K)$.
- If $p\,|\,d$, then $X^2-\overline{d}=X^2\in\mathbb{F}_p[X]$. Hence $p\mathcal{O}_K=\mathfrak{p}^2$, where $\mathfrak{p}=p\mathbb{Z}+\sqrt{d}\,\mathcal{O}_K={}_{\mathcal{O}_K}\langle p,\sqrt{d}\rangle\in\mathcal{P}(\mathcal{O}_K)$.

CASE 2: $p=2$.

- If $d\equiv 2 \bmod 4$, then $\mathcal{O}_K=\mathbb{Z}[\sqrt{d}\,]$, and $X^2-\overline{d}=X^2\in\mathbb{F}_2[X]$. Hence $2\mathcal{O}_K=\mathfrak{p}^2$, where $\mathfrak{p}=2\mathbb{Z}+\sqrt{d}\,\mathcal{O}_K={}_{\mathcal{O}_K}\langle 2,\sqrt{d}\rangle$.
- If $d\equiv 3 \mod 4$, then $\mathcal{O}_K=\mathbb{Z}[\sqrt{d}\,]$, and $X^2-\overline{d}=(X-\overline{1})^2\in\mathbb{F}_2[X]$. Hence $2\mathcal{O}_K=\mathfrak{p}^2$, where $\mathfrak{p}=2\mathbb{Z}+(\sqrt{d}-1)\mathcal{O}_K={}_{\mathcal{O}_K}\langle 2,\sqrt{d}-1\rangle$.
- If $d\equiv 1 \bmod 4$, then $\mathcal{O}_K=\big[\frac{1+\sqrt{d}}{2}\big]$, and $f=X^2-X+\frac{1-d}{4}\in\mathbb{Z}[X]$ is the minimal polynomial of $\frac{1+\sqrt{d}}{2}$.

  If $d\equiv 1 \mod 8$, then $\overline{f}=X^2-X=X(X-\overline{1})\in\mathbb{F}_2[X]$, and therefore $2\mathcal{O}_K=\mathfrak{p}_+\mathfrak{p}_-$, where $\mathfrak{p}_+=2\mathbb{Z}+\frac{1+\sqrt{d}}{2}\mathcal{O}_K$ and $\mathfrak{p}_-=2\mathbb{Z}+\big(\frac{1+\sqrt{d}}{2}-1\big)\mathcal{O}_K=2\mathbb{Z}+\frac{1-\sqrt{d}}{2}\mathcal{O}_K$, hence $\mathfrak{p}_\pm={}_{\mathcal{O}_K}\big\langle 2,\frac{1\pm\sqrt{d}}{2}\big\rangle\in\mathcal{P}(\mathcal{O}_K)$.

  If $d\equiv 5 \mod 8$, then $\overline{f}=X^2+X+\overline{1}\in\mathbb{F}_2[X]$ is irreducible, and $2\mathcal{O}_K\in\mathcal{P}(\mathcal{O}_K)$. □

Theorem 2.7.7 (Splitting law for cyclotomic fields)**.** *Let* $n\in\mathbb{N}_{\ge 2}$ *and* $K=\mathbb{Q}^{(n)}=\mathbb{Q}(\zeta_n)$, *where* $\zeta_n\in\mu_n^*(\mathbb{C})$. *Let* $p\in\mathbb{P}$ *be a prime and* $n=p^em$, *where* $e\in\mathbb{N}_0$, $m\in\mathbb{N}$ *and* $p\nmid m$. *Let* $f\in\mathbb{N}$ *be minimal such that* $p^f\equiv 1 \mod m$. *Then* $f\,|\,\varphi(m)$, *and if* $\varphi(m)=fr$, *then*

$$p\mathcal{O}_K=(\mathfrak{P}_1\cdot\ldots\cdot\mathfrak{P}_r)^{\varphi(p^e)}\,,$$

where $\mathfrak{P}_1,\ldots,\mathfrak{P}_r\in\mathcal{P}(\mathcal{O}_K$ *are distinct, and* $f=f(\mathfrak{P}_i/p)$ *for all* $i\in[1,r]$.

Proof. By definition, $f=\operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(p+m\mathbb{Z})$, and therefore $f\,|\,\varphi(m)$. By Theorem 2.2.10, we obtain $\mathcal{O}_K=\mathbb{Z}[\zeta]$, and by Theorem 2.7.4 it suffices to prove that the residue class polynomial $\overline{\Phi}_n\in\mathbb{F}_p[X]$ of the cyclotomic polynomial $\Phi_n\in\mathbb{Z}[X]$ behaves as follows.

A. $\overline{\Phi}_n=\overline{\Phi}_m^{\,\varphi(p^e)}$.

B. $\overline{\Phi}_m$ is the product of r distinct irreducible monic polynomials of degree f in $\mathbb{F}_p[X]$.

Proof of **A.** By induction on m.

$m=1$: Since

$$\Phi_{p^e} = \frac{X^{p^e}-1}{X^{p^{e-1}}-1}\,, \quad \text{we get} \quad (X^{p^{e-1}}-1)\Phi_{p^e}(X^{p^e}-1)\,,$$

we obtain

$$(X-\overline{1})^{p^{e-1}}\overline{\Phi}_{p^e} = (X-\overline{1})^{p^e} \quad \text{and} \quad \overline{\Phi}_{p^e} = (X-\overline{1})^{p^e-p^{e-1}} = \overline{\Phi}_1^{\varphi(p^e)}\,.$$

$m>1$: Assume that the assertion holds for all $d<m$. Since

$$X^{p^e m}-1 = \Phi_{mp^e}(X^{p^{e-1}m}-1)\prod_{\substack{d\,|\,m\\ 1\le e<m}}\Phi_{dp^e}\,,$$

we obtain, using the induction hypothesis,

$$(X^m-\overline{1})^{p^e} = \overline{\Phi}_{mp^e}(X^m-\overline{1})^{p^{e-1}}\prod_{\substack{d\,|\,m\\ 1\le e<m}}\overline{\Phi}_d^{\varphi(p^e)}\,,$$

and therefore

$$(X^m-\overline{1})^{\varphi(p^e)} = \overline{\Phi}_{mp^e}\overline{\prod_{\substack{d\,|\,m\\ 1\le e<m}}\Phi_d}^{\varphi(p^e)} = \overline{\Phi}_n\Big(\frac{X^m-\overline{1}}{\overline{\Phi}_m}\Big)^{\varphi(p^e)} = (X^m-\overline{1})^{\varphi(p^e)}\frac{\overline{\Phi}_n}{\overline{\Phi}_m^{\varphi(p^e)}}\,,$$

which proves **A.**

Proof of **B.** Since $\overline{\Phi}_m \,|\, X^m - \overline{1}$, it follows that $\overline{\Phi}_m$ is separable, and therefore $\overline{\Phi}_m = \psi_1\cdot\ldots\cdot\psi_s$, where $s\in\mathbb{N}$ and $\psi_1,\ldots,\psi_s\in\mathbb{F}_p[X]$ are irreducible, monic and distinct. It suffices to prove that $\deg(\psi_i)=f$ for all $i\in[1,s]$, for then $\varphi(m)=\deg\overline{\Phi}_m = sf$, and thus $s=r$.

By definition, $\mathbb{F}_{p^f}=\mathbb{F}_p^{(m)}$ is a splitting field of Φ_m. We shall prove that, for all $i\in[1,s]$ and $\xi\in\mathbb{F}_{p^f}$, if $\psi_i(\xi)=0$, then $\xi\in\mu_m^*(\mathbb{F}_{p^f})$, hence $\mathbb{F}_{p^f}=\mathbb{F}_p(\xi)$ and $\deg(\psi_i)=f$. Thus let $\xi\in\mathbb{P}_{p^f}$ be such that $\psi_i(\xi)=0$ and $\operatorname{ord}(\xi)=d<m$. Since $X^m-1=(X^d-1)\Phi_m h$ for some monic polynomial $h\in\mathbb{Z}[X]$, it follows that $X^m-\overline{1}=(X^d-\overline{1})\overline{\Phi}_m\overline{h}$, and since $\Phi_m(\xi)=0$, it follows that ξ is a double root of $X^m-\overline{1}$, a contradiction. $\square$ $\square$

CHAPTER 3

Geometric methods

3.1. Geometric lattices

Recall that a finitely generated group A is called *free* if $A \cong \mathbb{Z}^n$ for some $n \in \mathbb{N}$. Then A possesses a ($\mathbb{Z}$-)basis $(u_1, \ldots, u_n)$, and the (uniquely determined) integer n is called the *rank* of A, $n = \mathrm{rk}(A)$.

`rteilersatz`

Theorem 3.1.1 (Main Theorem on finitely generated abelian groups)**.** *Let A be a finitely generated abelian group.*

1. *Let A be free of rank $n \in \mathbb{N}$ and $B \subset A$ a subgroup. Then there exist a basis $(u_1, \ldots, u_n)$ of A, some $m \in [0, n]$ and $e_1, \ldots, e_m \in \mathbb{N}$ such that $e_1 \,|\, e_2 \,|\, \ldots \,|\, e_m$, and $(e_1 u_1, \ldots, e_m u_m)$ is a basis of B.*

   In particular: B is free, $\mathrm{rk}(B) \le \mathrm{rk}(A)$, $A/B \cong \mathbb{Z}^{n-m} \oplus \mathbb{Z}/e_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/e_m\mathbb{Z}$, and $(A{:}B) < \infty$ if and only if $\mathrm{rk}(A) = \mathrm{rk}(B)$.
2. *There exist (uniquely determined) numbers $r, t \in \mathbb{N}_0$ and $e_1, \ldots, e_t \in \mathbb{N}$ such that $1 < e_1 \,|\, e_2 \,|\, \ldots \,|\, e_t$ and $A \cong \mathbb{Z}^r \oplus \mathbb{Z}/e_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/e_t\mathbb{Z}$.*
3. *Let A be free, $B \subset A$ a subgroup and $\mathrm{rk}(A) = \mathrm{rk}(B) = n \in \mathbb{N}$. Let $\boldsymbol{u} \in A^n$ be a basis of A, $\boldsymbol{v} \in B^n$ a basis of B and $T \in \mathsf{M}_n(\mathbb{Z})$ such that $\boldsymbol{v} = \boldsymbol{u}T$. Then $(A{:}B) = |\det(T)|$.*

PROOF. Elementary Algebra. $\square$

Definition 3.1.2. Let V be an $\mathbb{R}$-vector space and $\dim_{\mathbb{R}}(V) = n \in \mathbb{N}$.

1. A subset $\Gamma \subset V$ is called a (*geometric*) *lattice* if there exist some $m \in [0, n]$ and $\mathbb{R}$-linearly independent vectors $v_1 \ldots, v_m \in \Gamma$ such that $\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$ [then Γ is a free abelian group, and $(v_1, \ldots, v_m)$ is a basis of Γ]. We denote by $\mathbb{R}\Gamma$ the $\mathbb{R}$-subspace of V spanned by Γ. Then $\dim_{\mathbb{R}} \mathbb{R}\Gamma = \mathrm{rk}(\Gamma) = m$, and Γ is called *complete* (in V) if $\mathbb{R}\Gamma = V$.
2. Let $\Gamma \subset V$ be a lattice, $m \in [0, n]$ and $(v_1, \ldots, v_m)$ a basis of Γ. Then the set

   $$\mathcal{G} = \Big\{ \sum_{j=0}^{m} x_j v_j \;\Big|\; x_1, \ldots, x_m \in [0, 1) \Big\}$$

   is called a *fundamental parallelotope* of Γ. Obviously, $\mathcal{G}$ depends on $(v_1, \ldots, v_n)$, and

   $$\mathbb{R}\Gamma = \biguplus \{ \gamma + \Gamma \mid \gamma \in \mathcal{G} \} = \biguplus \{ u + \mathcal{G} \mid u \in \Gamma \} .$$

   In particular, $\mathcal{G}$ is a system of representatives of $\mathbb{R}\Gamma/\Gamma$ in $\mathbb{R}\Gamma$.

3. Let now V be an euclidean vector space, $\Gamma \subset V$ a complete lattice and $\mathcal{G}$ a fundamental parallelotope of Γ. The n-dimensional elementary volume $\operatorname{vol}(\Gamma) = \operatorname{vol}(\mathcal{G})$ is called the *volume* of Γ. If $(v_1, \ldots, v_n)$ is a basis of Γ, then $\operatorname{vol}(\Gamma) = |\det(v_1, \ldots, v_n)|$.

`gitter`

Theorem 3.1.3. *Let V be an $\mathbb{R}$-vector space, $n = \dim_{\mathbb{R}}(V) \in \mathbb{N}$ and $\Gamma \subset V$ a subgroup.*

1. *The following assertions are equivalent:*
   (a) *Γ is a lattice.*
   (b) *$0 \notin \Gamma'$ (0 is not an accumulation point of Γ).*
   (c) *$\Gamma \subset V$ is a discrete subset (that means, $\Gamma' = \emptyset$).*
2. *Let Γ be a lattice. Then Γ is complete if and only if V/Γ has a bounded system of representatives in V [that means, $V = \bigcup \{\Gamma + m \mid m \in M\}$ for some bounded subset $M \subset V$].*

Proof. By the Norm Equivalence Theorem, any two norms on V are equivalent. Hence we may investigate the topological notions with any suitable norm.

1. (a) ⇒ (b) Let $m \in [0, n]$, $(u_1, \ldots, u_m)$ a basis of Γ, $\boldsymbol{u} = (u_1, \ldots, u_m, u_{m+1}, \ldots, u_n)$ an $\mathbb{R}$-basis of V and $\|\cdot\| \colon V \to \mathbb{R}_{\geq 0}$ the norm defined by $\|\lambda_1 u_1 + \ldots + \lambda_n u_n\| = \max\{|\lambda_1|, \ldots, |\lambda_n|\}$ for all $(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$. Then it follows that $\Gamma \cap \{x \in V \mid \|x\| < 1\} = \{0\}$, and consequently $0 \notin \Gamma'$.

(b) ⇒ (c) Assume the contrary, let $c \in \Gamma'$ and $(x_n)_{n \geq 0}$ a sequence in $\Gamma \setminus \{c\}$ such that $(x_n)_{n \geq 0} \to c$. Then $(x_{n+1} - x_n)_{n \geq 0}$ is a sequence in Γ such that $(x_{n+1} - x_n)_{n \geq 0} \to 0$, and since $0 \notin \Gamma'$, there is some $m \geq 0$ such that $x_n = x_{n+1}$ for all $n \geq m$, a contradiction.

(c) ⇒ (a) Let $V_0 = \mathbb{R}\Gamma \subset V$ be the subspace of V spanned by Γ, $\dim_{\mathbb{R}} V_0 = m \in \mathbb{N}_0$ and $(u_1, \ldots, u_m) \in \Gamma^m$ an $\mathbb{R}$-basis of V_0. Then $\Gamma_0 = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_m$ is a lattice in V_0, $\mathcal{G}_0 = \{\lambda_1 u_1 + \ldots + \lambda_m u_m \mid \lambda_1, \ldots, \lambda_m \in [0, 1)\}$ is with fundamental parallelotope of Γ_0, and

$$\Gamma \subset V_0 = \bigcup \{u + \Gamma_0 \mid u \in \mathcal{G}_0\} \quad \text{implies} \quad \Gamma = \bigcup \{u + \Gamma_0 \mid u \in \Gamma \cap \mathcal{G}_0\}.$$

The set $\Gamma \cap \mathcal{G}_0 \subset V_0$ is discrete and bounded, hence finite, and therefore $d = (\Gamma : \Gamma_0) < \infty$. Thus we obtain $d\Gamma \subset \Gamma_0$, hence $\Gamma \subset d^{-1}\Gamma_0$, and since $d^{-1}\Gamma_0$ is free with basis $(d^{-1}u_1, \ldots, d^{-1}u_m)$, it follows that Γ is a free abelian group of rank $\operatorname{rk}(\Gamma) = k \leq m$. If $(v_1, \ldots, v_k)$ is a basis of Γ, then $V_0 = \mathbb{R}\Gamma = \mathbb{R}v_1 + \ldots + \mathbb{R}v_k$. Hence it follows that $k \geq \dim_{\mathbb{R}} V_0 = m$, and we finally obtain $k = m$, and that $(v_1, \ldots, v_m)$ is linearly independent over $\mathbb{R}$.

2. If Γ is complete, then every fundamental parallelotope of Γ is a bounded system of representative of V/Γ. Let now $M \subset V$ be a bounded system of representatives of V/Γ. Then $V = \Gamma + M$, we set $V_0 = \mathbb{R}\Gamma \subset V$, and we shall prove that $V_0 = V$. Thus let $v \in V$. For $k \in \mathbb{N}$, we set $kv = u_k + m_k$, where $u_k \in \Gamma$ and $m_k \in M$. Then $v = k^{-1}u_k + k^{-1}m_k$, and as M is bounded, we obtain $(k^{-1}m_k)_{k \geq 1} \to 0$. Hence it follows that $(k^{-1}u_k)_{k \geq 1} \to v$, and therefore $v \in V_0$, since $k^{-1}u_k \in \mathbb{R}\Gamma = V_0$ for all $k \in \mathbb{N}$ and $V_0 \subset V$ is closed. □

`diskret`

Corollary 3.1.4. *Let $W \subset \mathbb{R}_{>0}$ be a (multiplicative) subgroup. Then the following assertions are equivalent:*

(a) *W is discrete.* (b) *W is cylic.* (c) *$1 \notin W'$.*

If these conditions are fulfilled, then $W = \langle \rho \rangle$, where $\rho = \min\{x \in W \mid x > 1\}$ (then it follows that $W = \langle \rho^{-1} \rangle$ and $\rho^{-1} = \max\{x \in W \mid x < 1\}$).

Proof. $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$ is a topological isomorphism. Hence $W \subset \mathbb{R}_{>0}$ is discrete if and only if $\log(W) \subset \mathbb{R}$ is discrete, W is cyclic if and only if $\log(W) \subset \mathbb{R}$ is a lattice, and $1 \in W'$ if and only if $0 \in \log(W)'$. Now the assertions follow by Theorem gitter 3.1.3. □

erpunktsatz

Theorem 3.1.5 (Minkowski's Lattice Point Theorem)**.** *Let* $n \in \mathbb{N}$, $\Gamma \subset \mathbb{R}^n$ *a complete lattice and* $X \subset \mathbb{R}^n$ *a convex subset such that* $-X = X$ *and* $\lambda(X) > 2^n \operatorname{vol}(\Gamma)$ (*where* $\lambda(X)$ *denotes the Lebesgue measure of* X). *Then* $X \cap \Gamma \neq \{\mathbf{0}\}$.

Proof. We prove that there exist $v_1,\, v_2 \in \Gamma$ such that

$$v_1 \neq v_2 \quad\text{and}\quad \Bigl(\frac{1}{2}X + v_1\Bigr) \cap \Bigl(\frac{1}{2}X + v_2\Bigr) \neq \emptyset\,.$$

If this is done, then there exist $x_1,\, x_2 \in X$ such that $\frac{1}{2}x_1 + v_1 = \frac{1}{2}x_2 + v_2$, and we obtain $\mathbf{0} \neq v_1 - v_2 = \frac{1}{2}\,[x_2 + (-x_1)] \in X \cap \Gamma$.

Let $\mathcal{G}$ be a fundamental parallelotope of Γ. We assume that, contrary to our assertion, $\bigl(\frac{1}{2}X + v\bigr)_{v \in \Gamma}$ is a family of pairwise disjoint sets. Then

$$\mathbb{R}^n = \biguplus\,\{\mathcal{G} - v \mid v \in \Gamma\} \quad\text{implies}\quad \frac{1}{2}X = \biguplus \Bigl\{(\mathcal{G} - v) \cap \frac{1}{2}X \Bigm| v \in \Gamma\Bigr\}\,,$$

and since λ is σ-additive and translation-invariant, we obtain

$$\frac{1}{2^n}\lambda(X) = \lambda\Bigl(\frac{1}{2}\,X\Bigr) = \sum_{v \in \Gamma} \lambda\Bigl((\mathcal{G} - v) \cap \frac{1}{2}\,X\Bigr) = \sum_{v \in \Gamma} \lambda\Bigl(\mathcal{G} \cap \bigl(\frac{1}{2}X + v\bigr)\Bigr) \le \lambda(\mathcal{G}) = \operatorname{vol}(\Gamma)\,,$$

a contradiction. □

3.2. Minkowski theory of algebraic number fields

Definition 3.2.1. Let K be an algebraic number field and $[K:\mathbb{Q}] = n = r_1 + 2r_2$, where $r_1,\, r_2 \in \mathbb{N}_0$, and $\operatorname{Hom}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$ such that

$$\sigma_j(K) \subset \mathbb{R} \ \text{ for all } \ j \in [1, r_1]\,, \quad\text{and}\quad \sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}} \ \text{ for all } \ j \in [1, r_2]\,.$$

Then we call $\sigma_1, \ldots, \sigma_{r_1}$ the *real embeddings* and $(\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}), \ldots, (\sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}})$ the *pairs of conjugate complex embeddings* of K. The fields $\sigma_1(K), \ldots, \sigma_{r_1}(K) \subset \mathbb{R}$ are called the *real conjugates* and the field $\sigma_{r_1+1}(K), \ldots, \sigma_{r_1+r_2}(K)$ are called the *complex conjugates* of K. The algebraic number field K is called *totally real* if $r_2 = 0$, and *totally imaginary* if $r_1 = 0$.

The map $\varphi\colon K \to \mathbb{R}^n$, defined by

$$\varphi(x) = \bigl(\sigma_1(x), \ldots, \sigma_{r_1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Im\sigma_{r_1+r_2}(x),\, \Re\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x)\bigr)^{\mathsf{t}} \in \mathbb{R}^n\,,$$

is called the *geometric embedding* of K. It is a $\mathbb{Q}$-vector space monomorphism.

reinbettung

Theorem 3.2.2. *Let* K *be an algebraic number field,* $[K:\mathbb{Q}] = n = r_1 + 2r_2$*, and suppose that* $\operatorname{Hom}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$*, where* $\sigma_j(K) \subset \mathbb{R}$ *for all* $j \in [1, r_1]$ *and* $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ *for all* $j \in [1, r_2]$. *Let* $\varphi\colon K \to \mathbb{R}^n$ *be the geometric embedding and* $M \subset K$ *a complete module.*

1. $\varphi(M) \subset \mathbb{R}^n$ *is a complete lattice, and* $\operatorname{vol}(\varphi(M)) = 2^{-r_2}\sqrt{|\Delta(M)|}$.
2. *For every* $C \in \mathbb{R}_{>0}$*, there are only finitely many* $\alpha \in M$ *satisfying* $|\sigma_\nu(\alpha)| \le C$ *for all* $\nu \in [1, n]$.

3. *There exists some* $\alpha \in \mathcal{O}_K$ *such that* $K = \mathbb{Q}(\alpha)$ *and* $|\sigma_\nu(\alpha)| < 2^{n-1}|\Delta_K| + 1$ *for all* $\nu \in [1, n]$.

PROOF. 1. Let $(u_1, \ldots, u_n)$ be a basis of M. Then $\sqrt{|\Delta(M)|} = |\det\bigl(\sigma_\nu(u_j)\bigr)_{\nu,j\in[1,n]}| \neq 0$, and we shall prove that

$$|\det(\varphi(u_1), \ldots, \varphi(u_n))| = 2^{-r_2}|\det\bigl(\sigma_\nu(u_j)\bigr)_{\nu,j\in[1,n]}|\,.$$

Then $(\varphi(u_1), \ldots, \varphi(u_n))$ is linearly independent over $\mathbb{R}$, $\varphi(M) = \mathbb{Z}\varphi(u_1) + \ldots + \mathbb{Z}\varphi(u_n) \subset \mathbb{R}^n$ is a complete lattice, and $\mathrm{vol}(\varphi(M)) = |\det(\varphi(u_1), \ldots, \varphi(u_n))| = 2^{-r_2}\sqrt{|\Delta(M)|}$.

For $j \in [1, n]$, let $S_j = (\sigma_1(u_j), \ldots, \sigma_{r_1}(u_j))^{\mathsf{t}}$ and $T_j = (\sigma_{r_1+1}(u_j), \ldots, \sigma_{r_1+r_2}(u_j))^{\mathsf{t}}$. Then $(\sigma_1(u_j), \ldots, \sigma_n(u_j))^{\mathsf{t}} = (S_j, T_j, \overline{T}_j)^{\mathsf{t}} \in \mathbb{C}^n$,

$$\varphi(u_j) = \begin{pmatrix} S_j \\ \frac{1}{2\mathrm{i}}\,(T_j - \overline{T}_j) \\ \frac{1}{2}\,(T_j + \overline{T}_j) \end{pmatrix} = \begin{pmatrix} I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{2\mathrm{i}}I & -\frac{1}{2\mathrm{i}}I \\ \mathbf{0} & \frac{1}{2}I & \frac{1}{2}I \end{pmatrix} \begin{pmatrix} S_j \\ T_j \\ \overline{T}_j \end{pmatrix} \in \mathbb{C}^n\,, \quad \text{and} \quad \det \begin{pmatrix} I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{2\mathrm{i}}I & -\frac{1}{2\mathrm{i}}I \\ \mathbf{0} & \frac{1}{2}I & \frac{1}{2}I \end{pmatrix} = 2^{-r_2}\,.$$

This proves our assertion.

2. Let $\|\cdot\|$ be the maximum norm of $\mathbb{R}^n$. Then $\|\varphi(x)\| \le \max\{|\sigma_1(x)|, \ldots, |\sigma_n(x)|\}$ für all $x \in K$. If $C \in \mathbb{R}_{>0}$, then $\varphi(M_C) \subset \{\boldsymbol{z} \in \varphi(M) \mid \|\boldsymbol{z}\| \le C\}$, but this set is bounded and discrete and therefore finite.

3. Let $B = 2^{n-1}|\Delta_K| + \frac{1}{2}$ and $X = [-B, B] \times \bigl(-\frac{1}{2}, \frac{1}{2}\bigr)^{n-1} \subset \mathbb{R}^n$. Then X is convex and $-X = X$. By 1., $\varphi(\mathcal{O}_K) \subset \mathbb{R}^n$ is a complete lattice, and since

$$2^n\,\mathrm{vol}(\varphi(\mathcal{O}_K)) = 2^{n-r_2}\sqrt{|\Delta_K|} < 2^n\,|\Delta_K| + 1 = 2B = \lambda(X)\,,$$

Theorem `gitterpunktsatz` 3.1.5 implies that there is some $\alpha \in \mathcal{O}_K^\bullet$ mit $\varphi(\alpha) \in X$. We shall prove:

$K = \mathbb{Q}(\alpha)$, and $|\sigma_j(\alpha)| < 2^{n-1}|\Delta_K| + 1$ for all $j \in [1, r_1 + r_2]$.

Let $m = [K \,{:}\, \mathbb{Q}(\alpha)]$. Then there are m distinct embeddings $\tau_1, \ldots, \tau_m \in \{\sigma_1, \ldots, \sigma_n\}$ such that $\tau_j(\alpha) = \sigma_1(\alpha)$ for all $j \in [1, m]$.

CASE 1: $r_1 > 0$. Then $|\sigma_1(\alpha)| \le B < 2^{n-1}|\Delta_K| + 1$, $|\sigma_j(\alpha)| < \frac{1}{2} < 2^{n-1}|\mathsf{d}_K| + 1$ for all $j \in [2, r_1]$, and $|\sigma_{r_1+j}(\alpha)| \le |\Im\sigma_{r_1+j}(\alpha)| + |\Re\sigma_{r_1+j}(\alpha)| < 1 < 2^{n-1}|\mathsf{d}_K| + 1$ for all $j \in [1, r_2]$. Since

$$1 \le |\mathsf{N}_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)| \prod_{i=2}^{r_1} |\sigma_i(\alpha)| \prod_{i=1}^{r_2} |\sigma_{r_1+i}(\alpha)|^2 < |\sigma_1(\alpha)|$$

it follows that σ_1 is the unique complex embedding of K satisfying $|\sigma_1(\alpha)| > 1$, and therefore we obtain $m = 1$ and $K = \mathbb{Q}(\alpha)$.

CASE 2: $r_1 = 0$. Then $|\Im\sigma_1(\alpha)| \le M$, $|\Re\sigma_1(\alpha)| < \frac{1}{2}$, $|\sigma_1(\alpha)| < M + \frac{1}{2} = 2^{n-1}|\Delta_K| + 1$, and $|\sigma_j(\alpha)| \le |\Im\sigma_j(\alpha)| + |\Re\sigma_j(\alpha)| < 1 < 2^{n-1}|\Delta_K| + 1$ for all $j \in [2, r_2]$. Since

$$1 \le |\mathsf{N}_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)|^2 \prod_{i=2}^{r_2} |\sigma_i(\alpha)|^2 < |\sigma_1(\alpha)|^2 < |\Im\sigma_1(\alpha)|^2 + \frac{1}{4} \quad \text{we obtains} \quad |\Im\sigma_1(\alpha)| > \frac{1}{2}\,.$$

Hence $|\Im\sigma_\nu(\alpha)| > \frac{1}{2}$ holds only for $\nu \in \{1, r_2 + 1\}$. But since $\Im\sigma_{r_2+1}(\alpha) = -\Im\sigma_1(\alpha) \neq \Im\sigma_1(\alpha)$, we get again $m = 1$ and $K = \mathbb{Q}(\alpha)$. □

`ktanwendung`

Theorem 3.2.3. A. *Let* $r_1,\, r_2 \in \mathbb{N}_0$ *and* $n = r_1 + 2r_2 \in \mathbb{N}$. *For* $a \in \mathbb{R}_{>0}$, *we denote by* $U_{r_1,r_2}(a)$ *the set of all* $(x_1, \ldots, x_n) \in \mathbb{R}^n$ *such that*

$$\Big|\sum_{j=1}^{r_1} |x_j| + 2\sum_{j=1}^{r_2} |\,\mathsf{i}\, x_{r_1+j} + x_{r_1+r_2+j}| < a\,,$$

and for $\boldsymbol{c} = (c_1, \ldots, c_{r_1+r_2}) \in \mathbb{R}_{>0}^{r_1+r_2}$, *we denote by* $W(\boldsymbol{c})$ *the set of all* $(x_1, \ldots, x_n) \in \mathbb{R}^n$ *such that* $|x_j| < c_j$ *for all* $j \in [1, r_1]$, *and* $|\mathsf{i}x_{r_1+j} + x_{r_1+r_2+j}| < c_{r_1+j}$ *for all* $j \in [1, r_2]$.

Then $U_{r_1,r_2}(a) = -U_{r_1,r_2}(a)$, $W(\boldsymbol{c}) = -W(\boldsymbol{c})$, $U_{r_1,r_2}(a)$ *and* $W(\boldsymbol{c})$ *are convex,*

$$\lambda(U_{r_1,r_2}(a)) = 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{a^n}{n!}\,, \quad \text{and} \quad \lambda(W(\boldsymbol{c})) = 2^{r_1}\pi^{r_2}[\![\boldsymbol{c}]\!]\,, \quad \text{where} \quad [\![\boldsymbol{c}]\!] = \prod_{j=1}^{r_1} c_j \prod_{j=1}^{r_2} c_{r_1+j}^2\,.$$

B. *Let* K *be an algebraic number field,* $[K:\mathbb{Q}] = n = r_1+2r_2$, *and* $\operatorname{Hom}(K,\mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$ *such that* $\sigma_j(K) \subset \mathbb{R}$ *for all* $j \in [1, r_1]$, *and* $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ *for all* $j \in [1, r_2]$. *Let* $M \subset K$ *be a complete module.*

1. *If* $\boldsymbol{c} = (c_1, \ldots, c_{r_1+r_2}) \in \mathbb{R}_{>0}^{r_1+r_2}$ *is such that*
$$[\![\boldsymbol{c}]\!] > \Big(\frac{2}{\pi}\Big)^{r_2}\sqrt{|\Delta(M)|}\,,$$
then there exists some $\alpha \in M^\bullet$ *such that* $|\sigma_j(\alpha)| < c_j$ *for all* $j \in [1, r_1 + r_2]$
2. *If* $a \in \mathbb{R}_{>0}$ *is such that*
$$a^n > n!\Big(\frac{4}{\pi}\Big)^{r_2}\sqrt{|\Delta(M)|}\,,$$
then there exists some $\beta \in M^\bullet$ *such that*
$$\sum_{j=1}^{r_1} |\sigma_j(\beta)| + 2\sum_{j=1}^{r_2} |\sigma_{r_1+j}(\beta)| < a\,, \quad \text{and then} \quad |\mathsf{N}_{K/\mathbb{Q}}(\beta)| < \Big(\frac{a}{n}\Big)^n.$$
3. *There exists some* $\alpha \in M^\bullet$, *so dass*
$$|\mathsf{N}_{K/\mathbb{Q}}(\alpha)| \ \le\ B = \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^{r_2}\sqrt{|\Delta(M)|}\,.$$

Beweis. **A.** This is an exercise in analysis (use induction on r_1 and r_2).

B. 1. By Theorem `koerpereinbettung` 3.2.2 we obtain

$$\lambda(W(\boldsymbol{c})) = 2^{r_1}\pi^{r_2}[\![\boldsymbol{c}]\!] > 2^{r_1+r_2}\sqrt{|\Delta(M)|} = 2^n\mathrm{vol}(\varphi(M))\,,$$

and by Theorem Satz `gitterpunktsatz` 3.1.5 this implies $W(\boldsymbol{c}) \cap \varphi(M) \ne \{\mathbf{0}\}$. Hence there exists some $\alpha \in M^\bullet$ such that $\sigma_j(\alpha)| < c_j$ for all $j \in [1, r_1 + r_2]$.

2. By Theorem `koerpereinbettung` 3.2.2 we obtain

$$\lambda(U_{r_1,r_2}(a)) = 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{a^n}{n!} > 2^{r_1+r_2}\sqrt{|\Delta(M)|}\,,$$

and by Theorem Satz `gitterpunktsatz` 3.1.5 this implies $U_{r_1,r_2}(a) \cap \varphi(M) \ne \{\mathbf{0}\}$. Hence there exists some $\beta \in M^\bullet$ such that

$$\sum_{j=1}^{r_1} |\sigma_j(\beta)| + 2\sum_{j=1}^{r_2} |\sigma_{r_1+j}(\beta)| < a\,,$$

and by the mean inequality this implies

$$\sqrt[n]{|\mathsf{N}_{K/\mathbb{Q}}(\beta)|} \;=\; \sqrt[n]{\prod_{i=1}^{r_1}|\sigma_i(\beta)|\prod_{i=1}^{r_2}|\sigma_{r_1+i}(\beta)|^2} \;\le\; \frac{1}{n}\Bigl(\sum_{i=1}^{r_1}|\sigma_i(\beta)|+2\sum_{i=1}^{r_2}|\sigma_{r_1+i}(\beta)|\Bigr) \;<\; \frac{a}{n}\,.$$

3. If $q \in \mathbb{N}$ is such that $qM \subset \mathcal{O}_K$, then $\mathsf{N}_{K/\mathbb{Q}}(\mathfrak{a}) \subset \mathsf{N}_{K/\mathbb{Q}}(q^{-1}\mathcal{O}_K) \subset q^{-n}\mathbb{Z}$, and therefore there exists some $\eta \in \mathbb{R}_{>0}$ such that

$$\min\bigl\{|\mathsf{N}_{K/\mathbb{Q}}(\alpha)| \bigm| \alpha \in \mathfrak{a}\,,\ |\mathsf{N}_{K/\mathbb{Q}}(\alpha)| > B\bigr\} = B+\eta\,, \quad \text{and we set} \quad a = \sqrt[n]{n^nB+\eta}\,.$$

Since $a^n > n^nB$, 2. implies the existence of some $\alpha \in M^\bullet$ such that

$$|N_{K/\mathbb{Q}}(\alpha)| < \Bigl(\frac{a}{n}\Bigr)^n = \frac{n^nB+\eta}{n^n} \le B+\eta\,, \quad \text{and thus} \quad |\mathsf{N}_{K/\mathbb{Q}}(\alpha)| \le B\,. \qquad \square$$

`hermite` **Theorem 3.2.4** (Discriminant Theorem of Hermite and Minkowski)**.**

1. *Let K be an algebraic number field and $[K:\mathbb{Q}] = n = r_1+2r_2 \ge 2$ such that K has r_1 real embeddings and r_2 pairs of conjugate complex embeddings. Then*

$$|\Delta_K| \ge \Bigl(\frac{\pi}{4}\Bigr)^{2r_2}\Bigl(\frac{n^n}{n!}\Bigr)^2 > \ 1\,.$$

2. *For every $C \in \mathbb{R}_{>0}$ there exist only finitely many algebraic number fields K such that $|\Delta_K| \le C$.*

Proof. By Theorem `gitterpunktanwendung` 3.2.3.3, applied with $M = \mathcal{O}_K$, there exists some $\alpha \in \mathcal{O}_K^\bullet$ satisfying

$$|\mathsf{N}_{K/\mathbb{Q}}(\alpha)| \le \frac{n!}{n^n}\Bigl(\frac{4}{\pi}\Bigr)^{r_2}\sqrt{|\Delta_K|}\,,$$

and since $|\mathsf{N}_{K/\mathbb{Q}}(\alpha)| \ge 1$, this implies

$$|\Delta_K| \ge \Bigl(\frac{\pi}{4}\Bigr)^{2r_2}\Bigl(\frac{n^n}{n!}\Bigr)^2 \ge \Bigl(\frac{\pi}{4}\Bigr)^{n}\Bigl(\frac{n^n}{n!}\Bigr)^2 = \Phi(n)\,, \quad \text{and} \quad \frac{\Phi(n+1)}{\Phi(n)} = \frac{\pi}{4}\Bigl(1+\frac{1}{n}\Bigr)^{2n} > 2\,.$$

Since $\Phi(2) > 2$, it follows that $\Phi(n) > 1$ for all $n \ge 2$, and

$$\lim_{n\to\infty}\Phi(n) = \infty\,.$$

In particular, this implies 1., and for 2. we must prove:

> For every $n \in \mathbb{N}$ und $B \in \mathbb{R}_{>0}$ there exist only finitely many algebraic number fields $K \subset \mathbb{C}$ such that $[K:\mathbb{Q}] = n$ and $|\Delta_K| \le B$.

For $B \in \mathbb{R}_{>0}$ and $n \in \mathbb{N}$ we denote by $T(B,n)$ the set of all algebraic integers $\alpha \in \mathbb{C}$ of degree n with conjugates $\alpha = \alpha_1,\ldots,\alpha_n \in \mathbb{C}$ such that $|\alpha_\nu| \le B$ for all $\nu \in [1,n]$. By Theorem `koerpereinbettung` 3.2.2.3 it suffices to prove that, for all $B \in \mathbb{R}_{>0}$ and $n \in \mathbb{N}$, the set $T(B,n)$ is finite.

Thus suppose that $B \in \mathbb{R}_{>0}$, $n \in \mathbb{N}$, $\alpha \in T(B,n)$ with conjugates $\alpha_1,\ldots,\alpha_n \in \mathbb{C}$, and let $f = X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in \mathbb{Z}[X]$ be the minimal polynomial of α. For every $i \in [1,n]$, we obtain

$$|a_i| = \Bigl|\sum_{1\le\nu_1<\ldots<\nu_i\le n}\alpha_{\nu_1}\cdot\ldots\cdot\alpha_{\nu_i}\Bigr| \le \binom{n}{i}B^i\,,$$

and there exist only finitely many polynomials in $\mathbb{Z}[X]$ whose coefficients satisfy these inequalities. $\square$

Definition 3.2.5. Let K be an algebraic number field. Two complete modules $M,\ N \subset K$ are called *equivalent*, $M \sim N$ if there exists some $\lambda \in K^\times$ such that $N = \lambda M$.

In particular, two fractional ideals $\mathfrak{a},\ \mathfrak{b} \in \mathcal{F}(\mathcal{O}_K)$ are equivalent if and only if they lie in the same ideal class $C \in \mathcal{C}(\mathcal{O}_K)$.

klassenzahl

Theorem and Definition 3.2.6 (Finiteness of the class number)**.** *Let K be an algebraic number field and $R \subset K$ an order. Then the set of equivalence classes of complete modules M such that $\mathcal{R}(M) = R$ is finite.*

In particular, the group $\mathcal{C}(\mathcal{O}_K)$ is finite. The group $\mathcal{C}_K = \mathcal{C}(\mathcal{O}_K)$ is called the *class group* and $h_K = |\mathcal{C}_K|$ is called the *class number* of K.

gitterpunktanwendung

PROOF. Let $M \subset K$ be a complete module and $\mathcal{R}(\mathfrak{a}) = R$. By Theorem 3.2.3 there exists some $\alpha \in M^\bullet$ such that

$$|\mathsf{N}_{K/\mathbb{Q}}(\alpha)| \ \le\ B\frac{\sqrt{|\Delta(\mathfrak{a})|}}{\sqrt{|\Delta(R)|}} \quad \text{mit} \quad B = \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^{r_2}\sqrt{|\Delta(R)|}\,.$$

completemodules

Then $R\alpha \subset M$, hence $R \subset \alpha^{-1}M$, and by Theorem 2.2.5 we obtain

$$(\alpha^{-1}M\colon R) \ =\ \frac{\sqrt{|\Delta(R)|}}{\sqrt{|\Delta(\alpha^{-1}M)|}} \ =\ |\mathsf{N}_{K/\mathbb{Q}}(\alpha)|\frac{\sqrt{|\Delta(R)|}}{\sqrt{|\Delta(M)|}} \ \le\ B\,.$$

Hence it suffices to prove:

> For every $N \in \mathbb{N}$, there are only finitely many abelian groups A such that $R \subset A \subset K$ and $(A\colon R) \le N$.

If $N \in \mathbb{N}$ and $R \subset A \subset K$ is an abelian group such that $(A : R) \le N$, then $N!A \subset R$, hence $R \subset A \subset N!^{-1}R$, and as $N!^{-1}R/R$ is finite, there are only finitely many abelian groups A with this property.

By definition, $\mathcal{C}_K$ is the set of equivalence classes of complete modules $M \subset K$ such that $\mathcal{R}(M) = \mathcal{O}_K$. □

bsolutenorm

Theorem and Definition 3.2.7. *Let K be an algebraic number field. For a fractional ideal $\mathfrak{a} \in \mathcal{F}(\mathcal{O}_K)$ we call*

$$\mathfrak{N}(\mathfrak{a}) = \prod_{\mathfrak{p}\in\mathcal{P}(\mathcal{O}_K)} (\mathcal{O}_K\colon\mathfrak{p})^{\mathsf{v}_\mathfrak{p}(\mathfrak{a})} \in \mathbb{Q}_{>0} \quad \text{the } \textit{absolute norm} \text{ of } \mathfrak{a}.$$

1. *If $p \in \mathbb{P}$, $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{p}\,|\,p$, then $\mathfrak{N}(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}$.*
2. *$\mathfrak{N}\colon \mathcal{F}(\mathcal{O}_K) \to \mathbb{Q}_{>0}$ is a group homomorphism, $\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$ for all $\mathfrak{a} \in \mathcal{I}(\mathcal{O}_K)$, and $\mathfrak{N}(x\mathcal{O}_K) = |\mathsf{N}_{K/\mathbb{Q}}(x)|$ for all $x \in K^\times$.*
3. *For all $B \in \mathbb{R}_{>0}$, there are only finitely many $\mathfrak{a} \in \mathcal{I}(\mathcal{O}_K)$ such that $\mathfrak{N}(\mathfrak{a}) \le B$.*

PROOF. 1. If $p \in \mathbb{P}$, $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{p}\,|\,p$, then $\mathfrak{N}(\mathfrak{p}) = (\mathcal{O}_K\colon\mathfrak{p}) = p^{\dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})} = p^{f(\mathfrak{p}/p)}$.

2. By definition, $\mathfrak{N}\colon \mathcal{F}(\mathcal{O}_K) \to \mathbb{Q}_{>0}$ is a group homomorphism. To prove $\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$, we use induction on $(\mathcal{O}_K : \mathfrak{a})$. If $\mathfrak{a} = \mathcal{O}_K$ or $\mathfrak{a} \in \mathcal{P}(\mathcal{O}_K)$, there is nothing to do. Thus suppose

that $\mathfrak{a} = \mathfrak{b}\mathfrak{p}$, where $\mathfrak{b} \in \mathcal{J}(\mathcal{O}_K)$ is such that $\mathfrak{N}(\mathfrak{b}) = (\mathcal{O}_K : \mathfrak{b})$ by induction hypothesis, and $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$. Then $\mathfrak{b}/\mathfrak{a} = \mathfrak{b}/\mathfrak{b}\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$ by Theorem dv 2.6.6, and therefore

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})\mathfrak{N}(\mathfrak{p}) = (\mathcal{O}_K : \mathfrak{b})(\mathcal{O}_K : \mathfrak{p}) = (\mathcal{O}_K : \mathfrak{b})(\mathfrak{b} : \mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})\,.$$

If $x \in K^\times$, we set $x = u^{-1}z$, where $u,\ z \in \mathcal{O}_K^\bullet$, and we obtain

$$\mathfrak{N}(x\mathcal{O}_K) = \frac{\mathfrak{N}(z\mathcal{O}_K)}{\mathfrak{N}(u\mathcal{O}_K)} = \frac{(\mathcal{O}_K : z\mathcal{O}_K)}{(\mathcal{O}_K : u\mathcal{O}_K)} = \frac{|\mathsf{N}_{K/\mathbb{Q}}(z)|}{|\mathsf{N}_{K/\mathbb{Q}}(u)|} = |\mathsf{N}_{K/\mathbb{Q}}(x)|\,.$$

3. Obvious. □

Theorem 3.2.8. *Let K be an algebraic number field. In every ideal class $C \in \mathcal{C}_K$ there exists some ideal $\mathfrak{a} \in \mathcal{J}(\mathcal{O}_K)$ such that*

$$\mathfrak{N}(\mathfrak{a}) \le \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^{r_2}\sqrt{|\Delta_K|}\,.$$

Proof. Let $C \in \mathcal{C}_K$ and $\mathfrak{b} \in \mathcal{J}(\mathcal{O}_K)$ such that $\mathfrak{b} \in C^{-1}$. By Theorem gitterpunktanwendung 3.2.3, there exists some $\alpha \in \mathfrak{b}^\bullet$ such that

$$|\mathsf{N}_{K/\mathbb{Q}}(\alpha)| \le \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^{r_2}\sqrt{|\Delta(\mathfrak{b})|}\,.$$

Since $|\Delta(\mathfrak{b})| = |\Delta(\mathcal{O}_K)|\mathfrak{N}(\mathfrak{b})^2$, we obtain $\sqrt{|\Delta(\mathfrak{b})|} = \sqrt{|\Delta_K|}\mathfrak{N}(\mathfrak{b})$, and if $\mathfrak{a} = \alpha\mathfrak{b}^{-1}$, then $\mathfrak{a} \in \mathcal{J}(\mathcal{O}_K)$, $\mathfrak{a} \in C$, and

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})^{-1}|\mathsf{N}_{K/\mathbb{Q}}(\alpha)| \le \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^{r_2}\sqrt{|\Delta_K|}\,.$$ □

heitensatz

Theorem 3.2.9 (Dirichlet's Unit Theorem)**.** *Let K be an algebraic number field, $R \subset K$ an order and $[K:\mathbb{Q}] = n = r_1 + 2r_2$, where r_1 denotes the number of real embeddings and r_2 denotes the number of pairs of conjugate complex embeddings of K.*

1. *$R^\times$ consists of all $\alpha \in R$ such that $|\mathsf{N}_{K/\mathbb{Q}}(\alpha)| = 1$.*
2. *$\mu(R)$ is a finite cyclic group, and $R^\times \cong \mu(R) \times \mathbb{Z}^{r_1+r_2-1}$. Explicitly: There exist some $\zeta \in \mu(R)$ and $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in R^\times$ such that every $\varepsilon \in R^\times$ has a unique representation*

$$\Box\varepsilon = \zeta^d \prod_{i=1}^{r_1+r_2-1} \varepsilon_i^{k_i} \quad \textit{where} \quad d \in [0, \mathrm{ord}(\zeta) - 1] \quad \textit{and} \quad k_1, \ldots, k_{r_1+r_2-1} \in \mathbb{Z}\,.$$

Every such $(r_1 + r_2 - 1)$-tuple $(\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1})$ is called a *system of fundamental units* of R [or of K if $R = \mathcal{O}_K$].

Proof. 1. If $\alpha \in$, then $\alpha \in R^\times$ if and only if $1 = (R : \alpha R) = |\mathsf{N}_{K/\mathbb{Q}}(\alpha)|$.

2. Let $\mathrm{Hom}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$, where $\sigma_j(K) \subset \mathbb{R}$ for all $j \in [1, r_1]$ and $\sigma_{r_1+r_1+j} = \overline{\sigma_{r_1+j}}$ for all $j \in [1, r_2]$. We wet $r = r_1 + r_2$ define the *logarithmic embedding* $\lambda \colon K \to \mathbb{R}^r$ by

$$\lambda(x) = (\lambda_1(x), \ldots, \lambda_r(x))\,, \quad \text{where} \quad \lambda_j(x) = l_j \log|\sigma_j(x)| \quad \text{and} \quad l_j = \begin{cases} 1 & \text{if } j \in [1, r_1]\,, \\ 2 & \text{if } j \in [r_1 + 1, r]\,, \end{cases}$$

and we consider the hyperplane $H = \{(x_1, \ldots, x_r) \in \mathbb{R}^r \mid x_1 + \ldots + x_r = 0\} \subset \mathbb{R}^r$. Then $\dim_{\mathbb{R}} H = r - 1$, and $\lambda(R^\times) \subset H$. By Theorem koerpereinbettung 3.2.2, the sets

$$\{\alpha \in R \mid |\sigma_j(\alpha)| \le C \ \text{ for all } j \in [1, r]\} \quad \text{and} \quad \{\alpha \in R \mid |\lambda_j(\alpha)| \le C \ \text{ for all } j \in [1, r]\}$$

are finite for every $C \in \mathbb{R}_{>0}$. Hence $\lambda(R^\times) \subset H$ is a discrete subgroup, and thus a lattice, say $\lambda(R^\times) \cong \mathbb{Z}^s$ for some $s \in [0, r-1]$. The map $\lambda \,|\, R^\times \colon R^\times \to \lambda(R^\times)$ is an epimorphism, and since $\lambda(R^\times)$ is free, there exists a homomorphism $j \colon \lambda(R^\times) \to R^\times$ such that $\lambda \circ j = \mathrm{id}_{\lambda(R^\times)}$. In particular, $R^\times = \mathrm{Ker}(\lambda \,|\, R^\times) \times j(\lambda(R^\times)) \cong \mathrm{Ker}(\lambda \,|\, R^\times) \times \lambda(R^\times)$.

Since $\mathrm{Ker}(\lambda \,|\, R^\times) = \{\alpha \in R^\times \mid \lambda(\alpha) = \mathbf{0}\} \subset K^\times$ is a finite subgroup, it follows that $\mathrm{Ker}(\lambda \,|\, R^\times) = \mu(R)$ is cyclic. Thus it remains to prove that $s = r-1$, that is, $\lambda(R^\times) \subset H$ is a complete lattice. By Theorem `gitter` 3.1.3 we must prove that $H/\lambda(R^\times)$ has a bounded system of representatives in H.

For $\boldsymbol{x} = (x_1, \ldots, x_r) \in \mathbb{R}^r_{>0}$ and $\alpha \in K^\times$ we define

$$\mathcal{L}(\boldsymbol{x}) = (l_1 \log x_1, \ldots, l_r \log x_r)\,, \quad \llbracket \boldsymbol{x} \rrbracket = \prod_{i=1}^r x_i^{l_i}\,, \quad \alpha\boldsymbol{x} = \bigl(|\sigma_1(\alpha)|x_1, \ldots, |\sigma_r(\alpha)|x_r\bigr)\,,$$

and we obtain $\llbracket \alpha\boldsymbol{x} \rrbracket = |\mathsf{N}_{K/\mathbb{Q}}(\alpha)|\, \llbracket \boldsymbol{x} \rrbracket$ and $\mathcal{L}(\alpha\boldsymbol{x}) = \lambda(\alpha) + \mathcal{L}(\boldsymbol{x})$.

Now we consider the set $S = \{\boldsymbol{x} \in \mathbb{R}^r_{>0} \mid \llbracket \boldsymbol{x} \rrbracket = 1\}$. By definition $\mathcal{L}(S) = H$, and $\varepsilon S = S$ for all $\varepsilon \in R^\times$ ist. We shall prove:

A. There exists a bounded set $T \subset S$ such that

$$S = \bigcup_{\varepsilon \in R^\times} \varepsilon T\,.$$

Proof of **A.** Let $\boldsymbol{c} = (c_1, \ldots, c_r) \in \mathbb{R}^r_{>0}$ and $\alpha_1, \ldots, \alpha_N \in R^\bullet$ such that

$$\llbracket \boldsymbol{c} \rrbracket > \Bigl(\frac{2}{\pi}\Bigr)^{r_2} \sqrt{|\Delta(R)|}\,,$$

and $\{\alpha_1 R, \ldots, \alpha_N R\}$ is the set of all principal ideals $\mathfrak{a} \subset R$ satisfying $(R \colon \mathfrak{a}) \le \llbracket \boldsymbol{c} \rrbracket$. Now we set

$$X = \prod_{i=1}^r (0, c_i) \subset \mathbb{R}^r_{>0} \quad \text{and} \quad T = S \cap \bigcup_{\nu=1}^N \alpha_\nu^{-1} X \subset S\,.$$

Then T is bounded, $\varepsilon T \subset S$ for all $\varepsilon \in R^\times$, and it suffices to prove that

$$S \subset \bigcup_{\varepsilon \in R^\times} \varepsilon T\,.$$

Thus suppose that $\boldsymbol{y} = (y_1, \ldots, y_r) \in S$. Then

$$\prod_{i=1}^r (y_i^{-1} c_i)^{l_i} = \llbracket \boldsymbol{c} \rrbracket > \Bigl(\frac{2}{\pi}\Bigr)^{r_2} \sqrt{|\Delta(R)|}\,,$$

and by Theorem `gitterpunktanwendung` 3.2.3 there exists some $\alpha \in R^\bullet$ such that $|\sigma_i(\alpha)| < y_i^{-1} c_i$ for all $i \in [1, r]$. But then it follows that $\alpha\boldsymbol{y} \in X$, and

$$(R \colon \alpha R) = |\mathsf{N}_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^r |\sigma_i(\alpha)|^{l_i} < \prod_{i=1}^r (y_i^{-1} c_i)^{l_i} = \llbracket \boldsymbol{c} \rrbracket\,.$$

Hence there exists some $\nu \in [1, N]$ such that $\alpha R = \alpha_\nu R$, which implies $\varepsilon = \alpha^{-1}\alpha_\nu \in R^\times$, and since $\varepsilon^{-1}\alpha_\nu \boldsymbol{y} = \alpha\boldsymbol{y} \in X$ it follows that $\boldsymbol{y} \in \varepsilon\alpha_\nu^{-1} X \cap S \subset \varepsilon T$. $\square$[**A.**]

Now it is easy to finish the proof. Since $T \subset S$ is bounded, there exists some $B \in \mathbb{R}_{>0}$ such that $T \subset [B^{-1}, B]^r$. Then $\mathcal{L}(T) \subset \mathbb{R}^r$ is also bounded, and as

$$H = \mathcal{L}(S) = \bigcup_{\varepsilon \in R^\times} \mathcal{L}(\varepsilon T) = \bigcup_{\varepsilon \in R^\times} \bigcup_{t \in T} \{\lambda(\varepsilon) + \mathcal{L}(t)\} = \lambda(R^\times) + \mathcal{L}(T)\,,$$

we see that $\mathcal{L}(T) \subset H$ is a bounded system of representatives of $H/\lambda(R^\times)$. $\square$

dreinheiten

Theorem 3.2.10 (Quadratic orders)**.** *Let* $\Delta \in \mathbb{Z}$ *be not a square,* $\Delta \equiv 0$ *or* $1 \bmod 4$ *and* $K = \mathbb{Q}(\sqrt{\Delta}\,)$*. Then*

$$\mathcal{O}_\Delta = \Big\{ \frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u,\, v \in \mathbb{Z}\,,\ u \equiv v\Delta \bmod 2 \Big\}$$

is the unique order in K *with discriminant* Δ*. If* $(\mathcal{O}_K : \mathcal{O}_\Delta) = f$*, then* $\Delta = \Delta_K f^2$*, and*

$$\mathcal{O}_\Delta^\times = \Big\{ \frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u,\, v \in \mathbb{Z}\,,\ |u^2 - \Delta v^2| = 4 \Big\}\,.$$

1. *If* $\Delta < 0$*, then* $\mathcal{O}_\Delta^\times = \mu(\mathcal{O}_\Delta)$*, and*

$$|\mathcal{O}_\Delta^\times| = \begin{cases} 6 & \textit{if} \quad \Delta = -3\,, \\ 4 & \textit{if} \quad \Delta = -4\,, \\ 2 & \textit{if} \quad \Delta < -4\,. \end{cases}$$

2. *If* $\Delta > 0$ *and* $\varepsilon_\Delta = \min\{\varepsilon \in \mathcal{O}_\Delta^\times \mid \varepsilon > 1\}$*, then* $\mathcal{O}_\Delta^\times = \langle -1, \varepsilon_\Delta\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$*.*

Proof. Let $d \in \mathbb{Z}$ be the squarefree kernel of Δ and $\Delta = dq^2$, where $q \in \mathbb{N}$. Then $\Delta_K = s^2 d$ and $\Delta = \Delta_K f^2$, where

$$s = \begin{cases} 1 & \text{if} \quad d \equiv 1 \bmod 4\,, \\ 2 & \text{if} \quad d \not\equiv 1 \bmod 4\,, \end{cases} \qquad \text{and} \quad \Delta = \Delta_K f^2\,, \quad \text{where} \quad f = \frac{q}{s} \in \mathbb{N}\,.$$

Let now $\sigma \in \{0,1\}$ be such that $\Delta_K \equiv \sigma \bmod 2$, and set

$$\omega = \frac{\sigma + \sqrt{\Delta_K}}{2}\,.$$

Then $\mathcal{O}_K = \mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega$, and we assert that $\mathcal{O}_{K,f} = \mathbb{Z} + \mathbb{Z}f\omega$ is the unique order with discriminant Δ in K. Indeed, $\mathcal{O}_{K,f} \subset \mathcal{O}_K$ is an order, and since $(\mathcal{O}_K : \mathcal{O}_{K,f}) = f$, it follows that $\Delta(\mathcal{O}_{K,f}) = \Delta_K f^2 = \Delta$. Conversely, if $R \subset \mathcal{O}_K$ is an order of discriminant $\Delta = \Delta_K f^2$, then $(\mathcal{O}_K : R) = f$, hence $f\omega \in R$, $\mathcal{O}_{K,f} \subset R$, and as $(\mathcal{O}_K : R) = (\mathcal{O}_K : \mathcal{O}_{K,f}) = f$, it follows that $R = \mathcal{O}_{K,f}$. Hence we must prove that

$$\mathcal{O}_{K,f} = \Big\{ \frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u,\, v \in \mathbb{Z}\,,\ u \equiv v\Delta \bmod 2 \Big\}\,.$$

Note that $\Delta = \Delta_K f^2 \equiv f\sigma \bmod 2$. If $x \in \mathcal{O}_{K,f}$, then $x = a + bf\omega$ for some $a,\, b \in \mathbb{Z}$, hence

$$x = a + b\,\frac{f\sigma + f\sqrt{\Delta_K}}{2} = \frac{2a + bf\sigma + b\sqrt{\Delta}}{2}\,, \quad \text{and} \quad 2a + bf\sigma \equiv b\Delta \bmod 2\,.$$

Conversely, if $u,\, v \in \mathbb{Z}$ and $u \equiv v\Delta \equiv vf\sigma \bmod 2$, then

$$\frac{u + v\sqrt{\Delta}}{2} = \frac{u - vf\sigma}{2} + vf\,\frac{\sigma + \sqrt{\Delta_K}}{2} \in \mathbb{Z} + \mathbb{Z}f\omega = \mathcal{O}_{K,f}\,.$$

Now it follows that

$$\mathcal{O}_\Delta^\times = \bigl\{\alpha \in \mathcal{O}_\Delta \bigm| |\mathsf{N}_{K/\mathbb{Q}}(\alpha)| = 1\,\bigr\} = \Bigl\{\frac{u+v\sqrt{\Delta}}{2} \Bigm| u,\, v \in \mathbb{Z}\,,\ |u^2-\Delta v^2| = 4\Bigr\}$$

(observe that $|u^2-\Delta v^2| = 4$ implies $u \equiv v\Delta \mod 2\,$).

If $\Delta < 0$, then it is easily checked that, for all $(u,v) \in \mathbb{Z}^2$, we have $|u^2-v^2\Delta| = u^2+v^2|\Delta| = 4$ if and only if we are in one of the following cases:

- $\Delta = -3$, $(u,v) \in \{(\pm 2, 0),\, (\pm 1 \pm 1),\, (\pm 1, \mp 1)\,\}$;
- $\Delta = -4$, $(u,v) \in \{(\pm 2, 0),\, (0, \pm 1)\,\}$;
- $\Delta < -4$, $(u,v) \in \{(\pm 2, 0)\,\}$.

If $\Delta > 0$, then $\mathcal{O}_\Delta \subset \mathbb{R}$, hence $\mu(\mathcal{O}_\Delta) = \{\pm 1\}$, and by Theorem einheitensatz 3.2.9 (whith $r_1 = 2$ and $r_2 = 0$) we get $\mathcal{O}_\Delta^\times = \langle -1, \varepsilon_0\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ for some $\varepsilon_0 \in \mathcal{O}_\Delta^\times \setminus \{\pm 1\}$.

As $\{\varepsilon_1 \in \mathcal{O}_\Delta^\times \mid O_\Delta^\times = \langle -1, \varepsilon_1\rangle\,\} = \{\pm\varepsilon_0, \pm\varepsilon_0^{-1}\}$, there exists a unique $\varepsilon_\Delta \in \mathbb{R}_{>1}$ such that $\mathcal{O}_\Delta^\times = \langle -1, \varepsilon_\Delta\rangle$. Then $\mathcal{O}_\Delta \cap \mathbb{R}_{>1} = \{\varepsilon_\Delta^n \mid n \in \mathbb{N}\}$, and therefore $\varepsilon_\Delta = \min\{\varepsilon \in \mathcal{O}_\Delta^\times \mid \varepsilon > 1\,\}$. $\square$

CHAPTER 4

Valuations and local methods

4.1. Absolute values and valuations

Definition 4.1.1. Let K be a field.

1. A (discrete rank one) *valuation* of K is a surjective map $v\colon K \to \mathbb{Z} \cup \{\infty\}$ such that the following properties hold for all $x,\, y \in K$:
   - **(V1)** $v(x) = \infty$ if and only if $x = 0$.
   - **(V2)** $v(xy) = v(x) + v(y)$.
   - **(V3)** $v(x+y) \geq \min\{v(x), v(y)\}$.
2. An *absolute value* of K is a map $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ such that the following properties hold for all $x,\, y \in K$:
   - **(A1)** $|x| = 0$ if and only if $x = 0$, and there exists some $x \in K^\times$ such that $|x| \neq 1$.
   - **(A2)** $|xy| = |x|\,|y|$.
   - **(A3)** $|x+y| \leq |x| + |y|$.
3. An absolute value $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ is called *non-archimedean* or *ultrametric* if
   $$|x+y| \leq \max\{|x|,\, |y|\} \quad \text{for all} \quad x,\, y \in K\,.$$
   Otherwise $|\cdot|$ is called *archimedean.*
4. An absolute value $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ is called *discrete* if it is non-archimedean and $|K^\times|$ is a discrete subset of $\mathbb{R}_{>0}$. By Corollary diskret 3.1.4 this holds if and only if $|K^\times| = \langle \rho \rangle$ for some $\rho \in (0,1)$.
5. If $|\cdot|$ is a [(non-)archimedean, discrete] absolute value, then we call $(K, |\cdot|)$ a [(non-) archimedean, discrete] *valued field.*
6. Let $(K, |\cdot|)$ and $(K', |\cdot|')$ be valued fields. A *value homomorphism* $\varphi\colon (K, |\cdot|) \to (K', |\cdot|')$ is a field homomorphism $\varphi\colon K \to K'$ satisfying $|\varphi(x)|' = |x|$ for all $x \in K$.

ionexamples

Remarks and Examples 4.1.2.

1. Let R be a Dedekind domain, $K = \mathsf{q}(R)$ and $\mathfrak{p} \in \mathcal{P}(R)$. Then $\mathsf{v}_\mathfrak{p}\colon K \to \mathbb{Z} \cup \{\infty\}$ is a valuation, called the $\mathfrak{p}$*-adic valuation* of K (see Theorem and Definition dedekindmain 2.4.9). For a prime $p \in \mathbb{P}$, the valuation $\mathsf{v}_p = \mathsf{v}_{p\mathbb{Z}}\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is called the p*-adic valuation* of $\mathbb{Q}$.
2. Let $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ be an absolute value. If $x \in K^\times$, then $|x| > 1$ if and only if $|x^{-1}| < 1$, and thus there exist $x,\, y \in K$ such that $0 < |x| < 1 < |y|$. If $\varphi\colon K_0 \to K$ is a field homomorphism, then $|\cdot|_\varphi = |\cdot| \circ \varphi\colon K_0 \to \mathbb{R}_{\geq 0}$ is an absolute value of K_0 if and only if there is some $x \in K_0^\times$ such that $|\varphi(x)| \neq 1$. In particular, if $K_0 \subset K$ is a subfield, then

$|\cdot|\restriction K_0$ is an absolute value of K_0 if and only if there exists some $x \in K_0^\times$ such that $|x| \ne 1$.

3. The ordinary absolute value of complex numbers will be denoted by $|\cdot|_\infty$. For every subfield $K \subset \mathbb{C}$, $|\cdot|_\infty \colon K \to \mathbb{R}_{\ge 0}$ is an archimedean absolute value (we write again $|\cdot|_\infty$ instead of $|\cdot|_\infty \restriction K$).
4. Let K be an algebraic number field, $[K:\mathbb{Q}] = n = r_1 + 2r_2$, and suppose that $\mathrm{Hom}(K,\mathbb{C}) = \{\sigma_1,\ldots,\sigma_n\}$ such that $\sigma_j(K) \subset \mathbb{R}$ for all $j \in [1,r_1]$ and $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ for all $j \in [1,r_2]$. For $j \in [1,r_1+r_2]$, define
$$|\cdot|_{\infty,j} = |\cdot|_\infty \circ \sigma_j \colon K \to \mathbb{R}_{\ge 0} \quad \text{by} \quad |a|_{\infty,j} = |\sigma_j(a)|_\infty\,.$$
Then $|\cdot|_{\infty,1},\ldots,|\cdot|_{\infty,r_1+r_2}$ are distinct archimedean absolute values of K [indeed, if $i,\, j \in [1, r_1+r_2]$ and $i \ne j$, then there is some $a \in K$ such that $\sigma_i(a) \ne \sigma_j(a)$ and $\sigma_i(a) \ne \overline{\sigma_j(a)}$. Hence there exists some $g \in \mathbb{N}$ such that $|g+\sigma_i(a)|_\infty \ne |g+\sigma_j(a)|_\infty$, and consequently $|g+a|_{\infty,i} \ne |g+a|_{\infty,j}$].
5. Let K be a field, $v \colon K \to \mathbb{Z} \cup \{\infty\}$ be a valuation and $\rho \in (0,1)$. Then
$$|\cdot|_{v,\rho} \colon K \to \mathbb{R}_{\ge 0}\,, \quad \text{defined by} \quad |a|_{v,\rho} = \rho^{v(a)} \quad (\text{with } \rho^\infty = 0\,)$$
is a absolute value. We call $|\cdot|_{v,\rho}$ an *absolute value associated with* v.
If R is a Dedekind domain, $K = \mathsf{q}(R)$ and $\mathfrak{p} \in \mathcal{P}(R)$, then we set $|\cdot|_{\mathfrak{p},\rho} = |\cdot|_{\mathsf{v}_\mathfrak{p},\rho}$ and call $|\cdot|_{\mathfrak{p},\rho}$ a $\mathfrak{p}$*-adic absolute value.*
If $p \in \mathbb{P}$ is a prime, then the absolute value $|\cdot|_p = |\cdot|_{p\mathbb{Z},p^{-1}} \colon \mathbb{Q} \to \mathbb{R}_{\ge 0}$ is called the p*-adic absolute value.* For $a \in \mathbb{Q}^\times$, we have $|a|_p = p^{-\mathsf{v}_p(a)}$. In particular, we have the *product formula*
$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |a|_p = 1\,.$$
Let K be an algebraic number field. For $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, we define the *normalized* $\mathfrak{p}$*-adic absolute value* $|\cdot|_\mathfrak{p} \colon K \to \mathbb{R}_{\ge 0}$ by
$$|a|_\mathfrak{p} = \mathfrak{N}(\mathfrak{p})^{-\mathsf{v}_\mathfrak{p}(a)} \quad \text{for all} \quad a \in K\,.$$
6. Let $(K, |\cdot|)$ be a discrete valued field and $\rho \in (0,1)$ such that $|K^\times| = \langle \rho \rangle$. We define
$$v \colon K \to \mathbb{Z} \cup \{\infty\} \quad \text{by} \quad v(a) = \frac{\log|a|}{\log \rho} \quad (= \infty \text{ for } a = 0\,) \quad \text{for all} \quad a \in K\,.$$
Then v is a valuation and $|\cdot| = |\cdot|_{v,\rho}$ is an absolute value associated with v. We call v the *valuation associated with* $|\cdot|$.

Theorem 4.1.3 (Elementary properties of absolute values and valuations)**.** *Let K be a field.*

1. *Let $|\cdot| \colon K \to \mathbb{R}_{\ge 0}$ be an absolute value.*
   (a) *$|\cdot| \restriction K^\times \colon K^\times \to \mathbb{R}_{>0}$ is a group epimorphism, $|z| = 1$ for all $z \in \mu(K)$, and $|-a| = |a|$ for all $a \in K$.*
   (b) *For all $x,\, y \in K$, we have $\big||x| - |y|\big| \le |x-y| \le |x| + |y|$.*
   (c) *If $|\cdot|$ is non-archimedean, $x,\, y \in K$ and $|x| \ne |y|$, then $|x+y| = \max\{|x|, |y|\}$.*
   (d) *If $|\cdot|$ is non-archimedean, $n \in \mathbb{N}_{\ge 2}$, $x_1,\ldots,x_n \in K$ and $x_1 + \ldots + x_n = 0$, then there exist $i,\, j \in [1,n]$ such that $i \ne j$, and $|x_i| = |x_j| = \max\{|x_1|,\ldots,|x_n|\}$.*

2. *Let* $v\colon K \to \mathbb{Z} \cup \{\infty\}$ *be a valuation.*
    - (a) $v \restriction K^\times \colon K^\times \to \mathbb{Z}$ *is a group epimorphism, and* $v(z) = 0$ *for all* $z \in \mu(K)$*. In particular,* $v(1) = 0$ *and* $v(-a) = v(a)$ *for all* $a \in K$*.*
    - (b) *If* $x, y \in K$ *and* $v(x) \ne v(y)$*, then* $v(x+y) = v(x-y) = \min\{v(x), v(y)\}$*.*
    - (c) *If* $n \in \mathbb{N}_{\ge 2}$*,* $x_1, \ldots, x_n \in K$ *and* $x_1 + \ldots + x_n = 0$*, then there exist* $i, j \in [1,n]$ *such that* $i \ne j$*, and* $v(x_i) = v(x_j) = \min\{v(x_1), \ldots, v(x_n)\}$*.*

Proof. 1. (a) By definition, $|\cdot| \restriction K^\times$ is a homomorphism. If $z \in \mu(K)$ and $n \in \mathbb{N}$ is such that $z^n = 1$, then $1 = |z^n| = |z|^n$, and thus $|z| = 1$. If $a \in K$, then $|-a| = |-1|\,|a| = |a|$.

(b) Let $x, y \in K$. Then $|x-y| = |x+(-y)| \le |x| + |-y| = |x| + |y|$. On the other hand, $|x| = |(x-y)+y| \le |x-y| + |y|$ implies $|x| - |y| \le |x-y|$, and if we interchange x and y, we get $|y| - |x| \le |y-x| = |x-y|$. Hence $\big||x| - |y|\big| \le |x-y|$.

(c) Assume that $x, y \in K$ and $|x| < |y|$. Then

$$|y| = |(x+y) + (-x)| \le \max\{|x+y|, |x|\} \le \max\{|x|, |y|\} = |y|\,,$$

and thus equality holds.

(d) Assume the contrary. Then there exist $x_1, \ldots, x_n \in K$ such that $x_1 + \ldots + x_n = 0$, and there is some $i \in [1,n]$ such that $|x_i| < |x_j|$ for all $j \in [1,n] \setminus \{i\}$. We may assume that $i = 1$. Then $|x_2 + \ldots + x_n| \le \max\{|x_2|, \ldots, |x_n|\} < |x_1|$, and therefore $0 = |x_1 + (x_2 + \ldots + x_n)| = |x_1|$, a contradiction.

2. Consider an associated absolute value and apply 1. $\square$

`nichtarch`

Theorem 4.1.4. *Let* K *be a field and* $F \subset K$ *its prime ring.*

1. *A map* $|\cdot|\colon K \to \mathbb{R}_{\ge 0}$ *is a non-archimedean absolute value of* K *if and only if it satisfies* **(A1)***,* **(A2)** *and*

    (A3′) *For all* $x \in K$*, if* $|x| \le 1$*, then* $|1+x| \le 1$*.*

2. *Let* $|\cdot|\colon K \to \mathbb{R}_{\ge 0}$ *be an absolute value. Then the following assertions are equivalent:*
    - (a) $(K, |\cdot|)$ *is non-archimedean.*
    - (b) $|x| \le 1$ *for all* $x \in F$*.*
    - (c) $|F|$ *is bounded.*

    In particular, if $\operatorname{char}(K) = 0$*, then every absolute value of* K *is non-archimedean.*

Proof. 1. If $|\cdot|$ is a non-archimedean absolute value, $x \in K$ and $|x| \le 1$, then it follows that $|1+x| \le \max\{|1|, |x|\} \le 1$. Conversely, suppose that $|\cdot|\colon K \to \mathbb{R}_{\ge 0}$ satisfies **(A1)**, **(A2)** and **(A3′)**. We must prove that $|x+y| \le \max\{|x|, |y|\} \le |x| + |y|$ for all $x, y \in K$. We may assume that $x, y \in K^\times$ and $|x| \le |y|$. Then $|xy^{-1}| = |x|\,|y|^{-1} \le 1$ and therefore $|x+y| = |y|(1 + |xy^{-1}|) \le |y| \le |x| + |y|$.

2. (a) $\Rightarrow$ (b) If $x \in F$, then there exists some $n \in \mathbb{N}_0$ such that $x = \pm n\,1_F$, and thus it suffices to prove that $|n\,1_F| \le 1$ for all $n \in \mathbb{N}$. We use induction on n. For $n = 0$, there is nothing to do. If $n \ge 0$ and $|n\,1_F| \le 1$, then $|(n+1)1_F| = |n1_F + 1_F| \le 1$ by 1.

(b) $\Rightarrow$ (c) Obvious.

(c) $\Rightarrow$ (a) Let $B \in \mathbb{R}$ be such that $|z| \le B$ for all $z \in F$, $x, y \in K$ and $n \in \mathbb{N}$. Then

$$|x+y|^n = |(x+y)^n| = \Bigl|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\Bigr| \le \sum_{i=0}^{n} \Bigl|\binom{n}{i} 1_K\Bigr|\, |x|^i |y|^{n-i} \le (n+1)B \max\{|x|, |y|\}^n\,,$$

and therefore $|x+y| \le \sqrt[n]{(n+1)B}\ \max\ |x|, |y|\}$. For $n \to \infty$ we get $|x+y| \le \max\{|x|, |y|\}$. $\square$

Remarks and Definitions 4.1.5. Let $(K, |\cdot|)$ be a valued field. We define

$$\mathsf{d} = \mathsf{d}_{|\cdot|} \colon K \times K \to \mathbb{R}_{\ge 0} \quad \text{by} \quad \mathsf{d}(x, y) = |x - y| \quad \text{for all} \quad x, y \in K\,.$$

Then d is a metric on K. The topology, defined by d, is called the $|\cdot|$*-topology.* For $a \in K$ and $\varepsilon \in \mathbb{R}_{>0}$ we consider the open ε-ball $B_\varepsilon(a) = B_\varepsilon^{|\cdot|}(a) = \{x \in K \mid |x - a| < \varepsilon\} = a + B_\varepsilon(0)$. Then $\{B_\varepsilon(a) \mid \varepsilon \in \mathbb{R}_{>0}\}$ is a fundamental system of open neighborhoods of a in the $|\cdot|$-topology.

If $(x_n)_{n\ge0}$ is a sequence in K and $x \in K$, then $(x_n)_{n\ge0}$ *converges* to x in the $|\cdot|$-topology if $(|x_n - x|)_{n\ge0} \to 0$, and in this case we write

$$(x_n)_{n\ge0} \xrightarrow{|\cdot|} x \quad \text{or} \quad |\cdot|\text{-}\lim_{n\to\infty} x_n = x\,.$$

Endowed with the $|\cdot|$-topology, K is a topological field, and $|\cdot| \colon K \to \mathbb{R}_{\ge0}$ is continuous. In particular, for all sequences $(x_n)_{n\ge0}$, $(y_n)_{n\ge0}$ in K and $x, y \in K$ the following assertions hold:

- If $(x_n)_{n\ge0} \xrightarrow{|\cdot|} x$ and $(y_n)_{n\ge0} \xrightarrow{|\cdot|} y$, then $(x_n \pm y_n)_{n\ge0} \xrightarrow{|\cdot|} x \pm y$ and $(x_ny_n)_{n\ge0} \xrightarrow{|\cdot|} xy$.
- If $(x_n)_{n\ge0} \xrightarrow{|\cdot|} x$ and $x \ne 0$, then there exists some $m \ge 0$ such that $x_n \ne 0$ for all $n \ge m$, and $(x_n^{-1})_{n\ge m} \xrightarrow{|\cdot|} x^{-1}$.
- If $(x_n)_{n\ge0} \xrightarrow{|\cdot|} x$, then $(|x_n|)_{n\ge0} \to |x|$.

Proofs are as in elementary analysis.

If $\varphi\colon (K, |\cdot|) \to (K', |\cdot|')$ is a value homomorphism of valued fields, then $\varphi\colon K \to \varphi(K)$ is a topological map.

Two absolute values $|\cdot|_1$ and $|\cdot|_2$ of a field K are called *equivalent*, $|\cdot_1 \sim |\cdot|_2$ if they induce the same topology.

`equivalent`

Theorem 4.1.6. *Let K be a field.*

1. *Let $|\cdot|_1, |\cdot|_2\colon K \to \mathbb{R}_{\ge0}$ be absolute values. Then the following assertions are equivalent:*
   (a) $|\cdot|_1 \sim |\cdot|_2$.
   (b) *For all $x \in K$, $|x|_1 < 1$ if and only if $|x|_2 < 1$.*
   (c) *There exists some $s \in \mathbb{R}_{>0}$ such that $|\cdot|_2 = |\cdot|_1^s$.*
2. *Let $|\cdot|\colon K \to \mathbb{R}_{\ge0}$ be an absolute value and $s \in (0, 1)$. Then $|\cdot|^s$ is also an absolute value.*
3. *Let $v\colon K \to \mathbb{Z} \cup \{\infty\}$ be a valuation. For $i \in \{1, 2\}$, let $\rho_i \in (0, 1)$ and $|\cdot|_i = |\cdot|_{v,\rho_i}$. Then*

$$|\cdot|_2 = |\cdot|_1^s\,, \quad \textit{where} \quad s = \frac{\log\rho_2}{\log\rho_1}\,.$$

In particular, any two absolute values associated with a valuation are equivalent. Conversely, equivalent discrete absolute values have the same associated valuation.

4. *Let $K_0 \subset K$ be a subfield and $|\cdot|_1, |\cdot|_2 \colon K \to \mathbb{R}_{\ge 0}$ absolute values of K such that $|\cdot|_1 \restriction K_0 = |\cdot|_2 \restriction K_0$ is an absolute value of K_0. Then $|\cdot|_1 \sim |\cdot|_2$ implies $|\cdot|_1 = |\cdot|_2$.*

Proof. (a) $\Rightarrow$ (b) If $x \in K$ and $i \in \{1,2\}$, then $|x|_i < 1$ if and only if $(|x^n|_i)_{n\ge 0} \to 0$, and this holds if and only if $(x^n)_{n\ge 0} \overset{|\cdot|_i}{\to} 0$. However, if $|\cdot|_1 \sim |\cdot|_2$, then $(x^n)_{n\ge 0} \overset{|\cdot|_1}{\to} 0$ if and only if $(x^n)_{n\ge 0} \overset{|\cdot|_2}{\to} 0$.

(b) $\Rightarrow$ (c) If $x \in K^\times$ and $|x|_1 = 1$, then also $|x|_2 = 1$. Indeed, otherwise it follows that either $|x|_2 > 1$ or $|x^{-1}|_2 > 1$, hence $|x|_1 > 1$ or $|x^{-1}|_1 > 1$, but never $|x|_1 = 1$.

We set $S = \{x \in K^\times \mid |x|_1 > 1\}$. It suffices to prove that there exists some $s \in \mathbb{R}_{>0}$ such that $|x|_2 = |x|_1^s$ for all $x \in S$. Indeed, if $x \in K^\times$ and $|x|_1 < 1$, then $x^{-1} \in S$, and therefore $|x|_2 = |x^{-1}|_2^{-1} = (|x^{-1}|_1^s)^{-1} = |x|_1^s$, and if $|x|_1 = 1$, then $|x|_2 = 1$ and thus also $|x|_2 = |x|_1^s$. Hence it follows that $|x|_2 = |x|_1^s$ for all $x \in K$.

We shall prove: For all $x, y \in S$ and $r \in \mathbb{Q}$, we have

$$\frac{\log|x|_1}{\log|y|_1} < r \quad \text{if and only if} \quad \frac{\log|x|_2}{\log|y|_2} < r\,. \tag{\textbf{A}}$$

Suppose that (**A**) holds. Then we obtain, for all $x, y \in S$:

$$\frac{\log|x|_1}{\log|y|_1} = \frac{\log|x|_2}{\log|y|_2}\,, \quad \text{hence} \quad \frac{\log|x|_2}{\log|x|_1} = \frac{\log|y|_2}{\log|y|_1} = s \in \mathbb{R}_{>0}\,.$$

Consequently, it follows that $\log|x|_2 = s\log|x|_1$ and thus $|x|_2 = |x|_1^s$ for all $x \in S$.

For the proof of (**A**) suppose that $x, y \in S$ and $r = \frac{m}{n} \in \mathbb{Q}$, where $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then we obtain, for $i \in \{1,2\}$,

$$\frac{\log|x|_i}{\log|y|_i} < r = \frac{m}{n} \iff \log|x^n|_i < \log|y^m|_i \iff \log\Bigl|\frac{x^n}{y^m}\Bigr|_i < 0 \iff \Bigl|\frac{x^n}{y^m}\Bigr|_i < 1\,.$$

By (b), we have

$$\Bigl|\frac{x^n}{y^m}\Bigr|_1 < 1 \quad \text{if and only if} \quad \Bigl|\frac{x^n}{y^m}\Bigr|_2 < 1\,,$$

hence (**A**) holds, and we are done.

(c) $\Rightarrow$ (a) Obvious.

2. Obviously, $|\cdot|^s$ satisfies (**A1**) and (**A2**). Thus it remains to prove (**A3**) and it suffices to do this for $x, y \in K^\times$. Thus let $x, y \in K^\times$ and set $\alpha = (|a|^s + |b|^s)^{1/s} \in \mathbb{R}_{>0}$. Then

$$\frac{|a|}{\alpha} \le 1\,, \ \frac{|b|}{\alpha} \le 1\,, \quad \text{and therefore} \quad 1 = \Bigl(\frac{|a|}{\alpha}\Bigr)^s + \Bigl(\frac{|b|}{\alpha}\Bigr)^s \ge \frac{|a|}{\alpha} + \frac{|b|}{\alpha}\,.$$

Hence it follows that $|a| + |b| \le \alpha$, and consequently $|a+b|^s \le (|a|+|b|)^s \le \alpha^s = |a|^s + |b|^s$.

3. For all $x \in K$, we have $|x|_2 = \rho_2^{\log v(x)} = \rho_1^{s\log v(x)} = |x|_1^s$. Assume now that $|\cdot|_1$ and $|\cdot|_2$ are equivalent absolute values of K, let $s \in \mathbb{R}_{>0}$ be such that $|\cdot|_2 = |\cdot|_1^s$, and $|K^\times|_1 = \langle\rho\rangle$. Then $|K^\times|_2 = \langle\rho^s\rangle$, and for all $x \in K$ we obtain

$$v(x) = \frac{\log|x|_2}{\log\rho^s} = \frac{s\log|x|_1}{s\log\rho} = \frac{\log|x|_1}{\log\rho}\,,$$

and therefore v is a valuation associated with both $|\cdot|_1$ and $|\cdot|_2$.

4. By assumption, there exists some $x \in K_0$ such that $|x|_1 = |x|_2 > 1$. If $|\cdot|_1 \sim |\cdot|_2$, then $|\cdot|_2 = |\cdot|_1^s$ for some $s \in \mathbb{R}_{>0}$, and $|x|_1^s = |x|_2 = |x|_1$ implies $s = 1$. □

`wat` **Theorem 4.1.7** (Weak Approximation Theorem)**.** *Let K be a field, $r \in \mathbb{N}$, and suppose that $|\cdot|_1, \ldots, |\cdot|_r$ are pairwise not equivalent absolute values of K.*

1. *There exists some $z \in K$ such that $|z|_1 > 1$ and $|z|_i < 1$ for all $i \in [2, r]$.*
2. *Let $(x_1, \ldots, x_r) \in K^r$.*
   - (a) *For every $\varepsilon \in \mathbb{R}_{>0}$, there exists some $x \in K$ such that $|x - x_i|_i < \varepsilon$ for all $i \in [1, r]$.*
   - (b) *There exists a sequence $(x_n)_{n\ge0}$ in K such that $(x_n)_{n\ge0} \xrightarrow{|\cdot|_i} x_i$ for all $i \in [1, r]$.*

PROOF. 1. By induction on r. For $r = 1$, there is nothing to do.

$r = 2$: By Theorem `equivalent` 4.1.6, there exist α, $\beta \in K$ such that $|\alpha|_1 < 1$, $|\alpha|_2 \ge 1$, $|\beta|_2 < 1$ and $|\beta_1| \ge 1$. Then it follows that $z = \alpha^{-1}\beta \in K$, $|z|_1 > 1$ and $|z|_2 < 1$.

$r \ge 3$, $r - 1 \to r$: By the induction hypothesis, there exist x, $y \in K$ satisfying $|x|_1 > 1$, $|x|_i < 1$ for all $i \in [2, r-1]$, $|y|_1 > 1$ and $|y|_r < 1$.

CASE 1: $|x|_r \le 1$. For $n \ge 1$, we set $z_n = x^n y \in K$. Then $(|z_n|_1)_{n\ge1} = (|x|_1^n\,|y|_1)_{n\ge1} \to \infty$, $(|z_n|_i)_{n\ge1} = (|x|_i^n\,|y|_i)_{n\ge1} \to 0$ for all $i \in [2, r-1]$, and $|z_n|_r = |x|_r^n\,|y|_r < 1$ for all $n \ge 1$. Therefore, for $n \gg 1$, $z = z_n$ has the desired properties.

CASE 2: $|x|_r > 1$. For $n \ge 1$, we set

$$z_n = \frac{x^n y}{1 + x^n} \quad \text{and obtain} \quad |z_n|_1 = \Big|\frac{x^n y}{1 + x^n}\Big|_1 = \frac{|y|_1}{|1 + x^{-n}|_1} \ge \frac{|y|_1}{1 + |x|_1^{-n}}\,.$$

Hence $(|z_n|_1)_{n\ge1} \to |y|_1 > 1$, and therefore $|z_n|_1 > 1$ for $n \gg 1$. Since

$$|z_n|_r = \Big|\frac{x^n y}{1 + x^n}\Big|_r = \frac{|y|_r}{|1 + x^{-n}|_r} \le \frac{|y|_r}{1 - |x|_r^{-n}} \quad \text{and} \quad \Big(\frac{|y|_r}{1 + |x|_r^{-n}}\Big)_{n\ge1} \to |y|_r < 1\,,$$

it follows that $|z_n|_r < 1$ for $n \gg 1$. For $i \in [2, r-1]$, we get

$$|z_n|_i = \Big|\frac{x^n y}{1 + x^n}\Big|_i \le \frac{|x|_i^n\,|y|_i}{1 - |x|_i^n} \qquad \text{and} \qquad \Big(\frac{|x|_i^n\,|y|_i}{1 - |x|_i^n}\Big)_{n\ge1} \to 0\,,$$

and therefore $|z_n|_r < 1$ for $n \gg 1$. Hence again, for $n \gg 1$, $z = z_n$ has the desired properties.

2. For every $i \in [1, r]$, 1. implies the existence of some $z_i \in K$ such that $|z_i|_i > 1$ and $|z_i|_j < 1$ for all $j \in [1, r] \setminus \{i\}$. For $n \ge 1$, let

$$y_i^{(n)} = \frac{z_i^n}{1 + z_i^n}\,, \quad \text{hence} \quad \big(y_i^{(n)}\big)_{n\ge0} \xrightarrow{|\cdot|_i} 1 \quad \text{and} \quad \big(y_i^{(n)}\big)_{n\ge0} \xrightarrow{|\cdot|_j} 0 \quad \text{for all } j \in [1, r] \setminus \{i\}\,.$$

Then we set

$$x^{(n)} = \sum_{j=1}^{r} y_j^{(n)} x_j \quad \text{and obtain} \quad (x^{(n)})_{n\ge1} \xrightarrow{|\cdot|_i} x_i \quad \text{for all } i \in [1, r].$$

In particular, it follows that $|x^{(n)} - x_i|_i < \varepsilon$ for all sufficiently large $n \in \mathbb{N}$ and all $i \in [1, r]$. □

`nichtarch1` **Theorem 4.1.8.** *Let $(K, |\cdot|)$ be a non-archimedean valued field.*

1. *If R is a Dedekind domain, $K = \mathsf{q}(R)$ and $|x| \le 1$ for all $x \in R$, then $|\cdot| = |\cdot|_{\mathfrak{p},\rho}$ for some $\mathfrak{p} \in \mathcal{P}(R)$ and $\rho \in (0, 1)$.*
2. *If K is an algebraic number field, then $|\cdot| \sim |\cdot|_{\mathfrak{p}}$ for some $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$.*

PROOF. 1. We set $\mathfrak{p} = \{x \in R \mid |x| < 1\}$, and we assert that $\mathfrak{p} \in \mathcal{P}(R)$. Obviously, $R \setminus \mathfrak{p} = \{x \in R^\bullet \mid |x| = 1\}$ is multiplicatively closed, hence $\mathfrak{p}$ is a prime ideal, and since $|z| \neq 1$ for some $z \in K^\times$, there exists some $x \in R^\bullet$ such that $|x| < 1$. Hence $\mathfrak{p} \neq \{0\}$, $\mathfrak{p} \in \mathcal{P}(R)$, and if $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, then $\rho = |\pi| \in (0,1)$ and $\mathsf{v}_\mathfrak{p}(\pi) = 1$. If $x \in K^\times$, then $x = \pi^{\mathsf{v}_\mathfrak{p}(x)} u$, where $u \in R_\mathfrak{p}^\times$ and thus $u = rs^{-1}$ for some r, $s \in R \setminus \mathfrak{p}$. Hence it follows that $|x| = |\pi|^{\mathsf{v}_\mathfrak{p}(x)} = |x|_{\mathfrak{p},\rho}$, and thus $|\cdot| = |\cdot|_{\mathfrak{p},\rho}$ as asserted.

2. By 1., it suffices to prove that $|x| \le 1$ for all $x \in \mathcal{O}_K$. Assume to the contrary that $|x| > 1$ for some $x \in \mathcal{O}_K$, and let $x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 = 0$ be an integral equation for x, where $d \in \mathbb{N}$ and $a_0, \ldots, a_{d-1} \in \mathbb{Z}$. By Theorem nichtarch 4.1.4, we obtain $|a_i| \le 1$ for all $i \in [0, d-1]$, and therefore $|x|^d = |a_{d-1}x^{d-1} + \ldots + a_1x + a_0| \le \max\{|x|^i \mid i \in [0, d-1]\} < |x|^d$, a contradiction. $\square$

valueq

Theorem 4.1.9. *Let* $\|\cdot\| \colon \mathbb{Q} \to \mathbb{R}_{\ge 0}$ *be an absolute value.*

1. *If* $\|\cdot\|$ *is non-archimedean, then* $\|\cdot\| \sim |\cdot|_p$ *for some prime* $p \in \mathbb{P}$.
2. *If* $\|\cdot\|$ *is archimedean, then there exists some* $s \in (0,1]$ *such that* $\|\cdot\| = |\cdot|_\infty^s$.

PROOF. 1. By Theorem nichtarch1 4.1.8.2.

2. By Theorem nichtarch 4.1.4 there exists some $m \in \mathbb{N}$ such that $\|m\| > 1$. Let now k, $n \in \mathbb{N}$ be arbitrary, $n \ge 2$, and let the n-adic digit expansion of m^k be given by

$$m^k = a_0 + a_1n + \ldots + a_sn^s\,, \quad \text{where} \quad s \in \mathbb{N}_0\,,\ a_0, \ldots, a_s \in [0, n-1] \ \text{ and } \ a_s \neq 0\,.$$

Then $n^s \le m^k$, hence $s \log n \le k \log m$, and since $\|a_i\| = \|1 + \ldots + 1\| \le a_i < n$ for all $i \in [0, s]$, we obtain

$$\|m\|^k = \|m^k\| \le \sum_{i=0}^{s} \|a_i\|\,\|n\|^i < (s+1)n\,\max\{1, \|n\|^s\}$$
$$\le \Big(\frac{k \log m}{\log n} + 1\Big) n\,\max\big\{1,\ \|n\|^{(k \log m)/\log n}\big\}\,.$$

Hence

$$\|m\| \le \sqrt[k]{kn\Big(\frac{\log m}{\log n} + \frac{1}{k}\Big)}\,\max\big\{1,\ \|n\|^{\log m/\log n}\big\}\,, \quad \text{and, as } k \to \infty,\ \ \|m\| \le \|n\|^{\log m/\log n}\,,$$

and therefore

$$\|n\| > 1 \quad \text{and} \quad \frac{\log \|m\|}{\log m} \le \frac{\log \|n\|}{\log n}\,.$$

In particular, we may interchange m and n. Hence we obtain

$$\frac{\log \|m\|}{\log m} = \frac{\log \|n\|}{\log n} \quad \text{for all} \quad m,\, n \in \mathbb{N}_{\ge 2}\,. \quad \text{and we set} \quad s = \frac{\log \|m\|}{\log m} \in \mathbb{R}_{>0}\,.$$

Then it follows that $\|n\| = n^s = |n|_\infty^s$ for all $n \in \mathbb{N}$, and thus also $\|x\| = |x|_\infty^s$ for all $x \in \mathbb{Q}$. Since $2^s = |2|_\infty^s = \|2\| \le \|1\| + \|1\| = 2$, we finally get $s \le 1$. $\square$

4.2. Completions

Definition 4.2.1. Let $(K, |\cdot|)$ be a valued field.

1. A sequence $(x_n)_{n\ge 0}$ in K is called a $(|\cdot|)$-*Cauchy sequence* if, for all $\varepsilon \in \mathbb{R}_{>0}$, there exists some $n_0 \ge 0$ such that $|x_m - x_n| < \varepsilon$ for all $m,\, n \ge n_0$.
2. $(K, |\cdot|)$ is called *complete* if every Cauchy sequence in K is convergent.
3. A *completion* of $(K, |\cdot|)$ is a valued field $(K', |\cdot|')$ such that
   - $K \subset K'$ is a subfield, and $|\cdot|' \restriction K = |\cdot|$.
   - K is dense in K' (every element of K' is the $|\cdot|'$-limit of a sequence in K).

Remarks 4.2.2. Let $(K, |\cdot|)$ be a valued field.

1. Every convergent sequence is a Cauchy sequence. [Proof: As in elementary analysis].
2. If $(x_n)_{n\ge 0}$ is a Cauchy sequence in K, then $(|x_n|)_{n\ge 0}$ is a convergent sequence in $\mathbb{R}$. [Proof: By Cauchy's convergence criterion, since $\big||x_n| - |x_m|\big| \le |x_n - x_m|$ for all $m,\, n \ge 0$].
3. Let $|\cdot|'$ be an absolute value of K which is equivalent to $|\cdot|$. Then a sequence in K is a $|\cdot|'$-Cauchy sequence if and only if it is a $|\cdot|$-Cauchy sequence, and $(K, |\cdot|)$ is complete if and only if $(K, |\cdot|')$ is complete. [Proof: Obvious].

$(\mathbb{R}, |\cdot|_\infty)$ and $(\mathbb{C}, |\cdot|_\infty)$ are complete archimedean valued fields.

`completion`

Theorem 4.2.3 (Completion Theorem)**.** *Let* $(K, |\cdot|)$ *be a valued field.*

1. $(K, |\cdot|)$ *has a completion.*
2. *Let* $(K^*, |\cdot|^*)$ *be a complete valued field,* $f\colon (K, |\cdot|) \to (K^*, |\cdot|^*)$ *a value homomorphism and* $(K', |\cdot|')$ *a completion of* $(K, |\cdot|)$*. Then there exists a unique value homomorphism* $f'\colon (K', |\cdot|') \to (K^*, |\cdot|^*)$ *such that* $f' \,|\, K = f$.
3. *Let* $(K_1, |\cdot|_1)$ *be another valued field and* $\varphi\colon (K, |\cdot|) \to (K_1, |\cdot|_1)$ *a value isomorphism. Let* $(K', |\cdot|')$ *be a completion of* $(K, |\cdot|)$ *and* $(K_1', |\cdot|_1')$ *a completion of* $(K_1, |\cdot|_1)$*. Then there exists a unique value isomorphism* $\varphi'\colon (K', |\cdot|') \to (K_1', |\cdot|_1')$ *such that* $\varphi' \,|\, K = \varphi$.

   In particular, if $(K', |\cdot|')$ *and* $(K'', |\cdot|'')$ *are completions of* K*, then there exists a unique value isomorphism* $\phi\colon (K', |\cdot|') \to (K'', |\cdot|'')$ *such that* $\phi \,|\, K = \mathrm{id}_K$.
4. *Let* $(K^*, |\cdot|^*)$ *be a complete valued field such that* $K \subset K^*$ *is a subfield and* $|\cdot|^* \restriction K = |\cdot|$*. Let* $\overline{K} \subset K^*$ *be the closure of* K *in* K^**. Then* $(\overline{K}, |\cdot|^* \restriction \overline{K})$ *is a completion of* $(K, |\cdot|)$*. In particular,* $K \subset K^*$ *is closed if and only if* $(K, |\cdot|)$ *is complete.*
5. *Let* $(K', |\cdot|')$ *be a completion of* $(K, |\cdot|)$ *and* $s \in (0,1)$*. Then* $(K', |\cdot|'^s)$ *is a completion of* $(K, |\cdot|^s)$*.*

PROOF. 1. Let CS be the set of all Cauchy sequences and ZS the set of all sequences converging to 0 in K. For two sequences $\boldsymbol{x} = (x_n)_{n\ge 0}$, $\boldsymbol{y} = (y_n)_{n\ge 0}$ and $\diamond \in \{+, -, \cdot\}$, we define $\boldsymbol{x} \diamond \boldsymbol{y} = (x_n \diamond y_n)_{n\ge 0}$. For $a \in K$, we denote by $\mathsf{c}(a) = (a)_{n\ge 0}$ the constant sequence with value a.

I. $(\mathsf{CS}, +, \cdot)$ is a local ring with maximal ideal ZS, and $\mathsf{c}\colon K \to \mathsf{CS}$ is a ring monomorphisms.

Proof of **I.** It is easily checked that CS is a commutative ring, $\mathsf{c}\colon K \to \mathsf{CS}$ is a ring homomorphism and $\mathsf{ZS} \subset \mathsf{CS}$ is an ideal. In order to show that $\mathsf{ZS} \subset \mathsf{CS}$ is a maximal ideal, we prove that, for all $\boldsymbol{x} \in \mathsf{CS} \setminus \mathsf{ZS}$, there exists some $\boldsymbol{y} \in \mathsf{CS}$ such that $\boldsymbol{xy} \in \mathsf{c}(1) + \mathsf{ZS}$.

Thus let $\boldsymbol{x} = (x_n)_{n\ge0} \in \mathsf{CS} \setminus \mathsf{ZS}$. Then there exists some $\eta \in \mathbb{R}_{>0}$ such that, for all $k \ge 0$ there is some $n \ge k$ such that $|x_n| \ge \eta$. We define $\boldsymbol{y} = (y_n)_{n\ge0}$, where $y_n = x_n^{-1}$ if $x_n \ne 0$, and $y_n = 0$ if $x_n = 0$. We must prove that $\boldsymbol{y} \in \mathsf{CS}$ and $x_n \ne 0$ for all $n \gg 1$. Let $\varepsilon \in \mathbb{R}_{>0}$, and choose some $\varepsilon^* \in (0,\eta)$ such that $\varepsilon^*(\eta - \varepsilon^*)^{-2} < \varepsilon$. As $\boldsymbol{x} \in \mathsf{CS}$, there exists some $n_1 \ge 0$ such that $|x_m - x_n| < \varepsilon^*$ for all $n \ge m \ge n_1$. Let $n_0 \ge n_1$ be such that $|x_{n_0}| \ge \eta$. For all $n \ge m \ge n_0$ we obtain $|x_n| \ge |x_{n_0}| - |x_{n_0} - x_n| > \eta - \varepsilon^* > 0$ and

$$|y_n - y_m| = \Bigl|\frac{1}{x_n} - \frac{1}{x_m}\Bigr| = \frac{|x_n - x_m|}{|x_n x_m|} < \frac{\varepsilon^*}{(\eta - \varepsilon^*)^2} < \varepsilon\,. \qquad \square[\mathbf{I}.]$$

Now we define $K^* = \mathsf{CS}/\mathsf{ZS}$, $j\colon K \to K^*$ by $j(x) = \mathsf{c}(x) + \mathsf{ZS}$, and $|\cdot|^*\colon K^* \to \mathbb{R}_{\ge0}$ by

$$|(x_n)_{n\ge0} + \mathsf{ZS}|^* = \lim_{n\to\infty} |x_n| \quad \text{for all} \quad (x_n)_{n\ge0} \in \mathsf{CS}\,.$$

It is easily checked that this definition does not depend on the representing Cauchy sequence $(x_n)_{n\ge0}$, $|\cdot|^*$ is an absolute value and $j\colon (K, |\cdot|) \to (K^*, |\cdot|^*)$ is a value homomorphism.

II. If $(x_n)_{n\ge0}$ is a Cauchy sequence in K, then $(j(x_n))_{n\ge0} \xrightarrow{|\cdot|^*} (x_k)_{k\ge0} + \mathsf{ZS}$. In particular, $j(K)$ is dense in K^*.

Proof of **II.** Let $(x_n)_{n\ge0}$ be a Cauchy sequence in K and $\varepsilon \in \mathbb{R}_{>0}$. Then there exists some $n_0 \ge 0$ such that $|x_n - x_k| \le \varepsilon$ for all n, $k \ge n_0$. Now we obtain, for all $n \ge n_0$,

$$\bigl|j(x_n) - \bigl((x_k)_{k\ge0} + \mathsf{ZS}\bigr)\bigr|^* = |(x_n - x_k)_{k\ge0} + \mathsf{ZS}|^* = \lim_{k\to\infty} |x_n - x_k| \le \varepsilon, ,$$

and therefore $(j(x_n))_{n\ge0} \xrightarrow{|\cdot|^*} (x_k)_{k\ge0} + \mathsf{ZS}$. $\square$[**II.**]

III. $(K^*, |\cdot|^*)$ is complete.

Proof of **III.** Let $(\boldsymbol{x}^{(n)})_{n\ge0}$ be a $|\cdot|^*$-Cauchy sequence in K^*. For $n \in \mathbb{N}$, let $y_n \in K$ be such that $|\boldsymbol{x}^{(n)} - j(y_n)|^* < \frac{1}{n}$ (by **II.**). For all $m \ge n \ge 0$, we obtain

$$\begin{aligned} |y_n - y_m| &= |j(y_n - y_m)|^* = |j(y_n) - j(y_m)|^* \\ &\le |\boldsymbol{x}^{(n)} - \boldsymbol{x}^{(m)}|^* + |\boldsymbol{x}^{(n)} - j(y_n)|^* + |\boldsymbol{x}^{(m)} - j(y_m)|^* < |\boldsymbol{x}^{(n)} - \boldsymbol{x}^{(m)}|^* + \frac{1}{n} + \frac{1}{n}\,, \end{aligned}$$

and since Let $(\boldsymbol{x}^{(n)})_{n\ge0}$ is a Cauchy sequence, it follows that $(y_n)_{n\ge0} \in \mathsf{CF}$, and therefore

$$\boldsymbol{y} = (y_n)_{n\ge0} + \mathsf{ZS} = |\cdot|^*\text{-}\lim_{n\to\infty} j(y_n) \in K^*\,.$$

Since $|\boldsymbol{x}^{(n)} - \boldsymbol{y}|^* \le |\boldsymbol{x}^{(n)} - j(y_n)|^* + |j(y_n) - \boldsymbol{y}|^*$, it follows that $(\boldsymbol{x}^{(n)} \xrightarrow{|\cdot|^*} \boldsymbol{y}$. $\square$[**III.**]

By the Exchange Lemma, there exists a valued field $(K', |\cdot|')$ and a value isomorphism $j'\colon (K', |\cdot|') \to (K^*, |\cdot|^*)$ such that $K \subset K'$ and $j' \,|\, K = j$. By **II.** and **III.** $(K^*, |\cdot|^*)$ is a completion of $(j(K), |\cdot|^* \restriction j(K))$, and therefore $(K', |\cdot|')$ is a completion of $(K, |\cdot|)$.

2. *Uniqueness*: Let $f'\colon (K', |\cdot|') \to (K^*, |\cdot|^*)$ be a value homomorphism such that $f' \,|\, K = f$. Let $x' \in K'$ and $(x_n)_{n\ge0}$ a sequence in K such that $(x_n)_{n\ge0} \xrightarrow{|\cdot|'} x'$. Then

$$f'(x') = |\cdot|^*\text{-}\lim_{n\to\infty} f'(x_n) = |\cdot|^*\text{-}\lim_{n\to\infty} f(x_n)\,,$$

and thus f' is uniquely determined by f.

Existence: For $x' \in K'$, let $(x_n)_{n\ge 0}$ be a sequence in K such that $(x_n)_{n\ge0} \overset{|\cdot|'}{\to} x'$. We assert that the sequence $(f(x_n))_{n\ge0}$ converges in K^*, and that the limit only depends on x'. Indeed, for $m \ge n \ge 0$, we obtain $|f(x_n) - f(x_m)|^* = |f(x_n - x_m)|^* = |x_n - x_m| = |x_n - x_m|'$, and as $(x_n)_{n\ge0}$ is a Cauchy sequence in K', it follows that $(f(x_n)_{n\ge0}$ is a Cauchy sequence in K^* and thus convergent. If $(x'_n)_{n\ge0}$ is another sequence in K such that $(x'_n)_{n\ge0} \overset{|\cdot|'}{\to} x'$, then $(x_n - x'_n)_{n\ge0} \overset{|\cdot|'}{\to} 0$, and therefore $(f(x_n) - f(x'_n))_{n\ge0} = (f(x_n - x'_n))_{n\ge0} \overset{|\cdot|^*}{\to} 0$.

For $x' \in K'$ as above, we define

$$f'(x') = |\cdot|^*\text{-}\lim_{n\to\infty} f(x_n) \in K^*\,.$$

If $x \in K$, we use the constant sequence $(x)_{n\ge0}$ to define $f'(x)$, and we obtain $f'(x) = f(x)$. Hence $f' \,|\, K = f$. If $x', y' \in K'$, we consider sequences $(x_n)_{n\ge0}\,, (y_n)_{n\ge0}$ in K such that $(x_n)_{n\ge0} \overset{|\cdot|'}{\to} x'$ and $(y_n)_{n\ge0} \overset{|\cdot|'}{\to} y'$. Then $(f(x_n))_{n\ge0} \overset{|\cdot|^*}{\to} f'(x')$, $(f(y_n))_{n\ge0} \overset{|\cdot|^*}{\to} f'(y')$, and if $\diamond \in \{+,\cdot\}$, then $(x_n \diamond y_n)_{n\ge0} \overset{|\cdot|'}{\to} x' \diamond y'$, and therefore

$$\begin{aligned} f'(x' \diamond y') = |\cdot|^*\text{-}\lim_{n\to\infty} f(x_n \diamond y_n) &= |\cdot|^*\text{-}\lim_{n\to\infty} \big(f(x_n) \diamond f(y_n)\big) \\ &= |\cdot|^*\text{-}\lim_{n\to\infty} f(x_n) \diamond |\cdot|^*\text{-}\lim_{n\to\infty} f(y_n) = f'(x') \diamond f'(y')\,. \end{aligned}$$

Hence f' is a field homomorphism, and since

$$|f'(x')|^* = \lim_{n\to\infty} |f(x_n)|^* = \lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |x_n|' = |x'|'\,,$$

it follows that f' is a value homomorphism.

3. By 2., there exist unique value homomorphisms $\varphi' \colon (K', |\cdot|') \to (K'_1, |\cdot|'_1)$ such that $\varphi' \,|\, K = \varphi$, and $\varphi'_1 \colon (K'_1, |\cdot|'_1) \to (K', |\cdot|')$ such that $\varphi'_1 \,|\, K_1 = \varphi^{-1}$, and we must prove that φ' is an isomorphism. But $\varphi'_1 \circ \varphi' \colon (K', |\cdot|') \to (K', |\cdot|')$ and $\varphi' \circ \varphi'_1 \colon (K'_1, |\cdot|'_1) \to (K'_1, |\cdot|'_1)$ are value homomorphisms such that $\varphi'_1 \circ \varphi' \,|\, K = \mathrm{id}_K = \mathrm{id}_{K'} \,|\, K$ and ,$\varphi' \circ \varphi'_1 \,|\, K_1 = \mathrm{id}_{K_1} = \mathrm{id}_{K'_1} \,|\, K_1$. By the uniqueness in 2. it follows that $\varphi'_1 \circ \varphi' = \mathrm{id}_{K'}$ and $\varphi' \circ \varphi'_1 = \mathrm{id}_{K'_1}$. In particular, φ' is an isomorphism.

4. It suffices to prove that every $|\cdot|^*$-Cauchy sequence in $\overline{K}$ converges in $\overline{K}$. Thus let $(x_n)_{n\ge0}$ be a $|\cdot|^*$-Cauchy sequence in $\overline{K}$. Since $(K^*, |\cdot|^*)$ is complete, there exists some $x \in K^*$ such that $(x_n)_{n\ge0} \overset{|\cdot|^*}{\to} x$, and thus $x \in \overline{K}$.

5. By Theorem equivalent 4.1.6, $|\cdot|^s$ and $|\cdot|'^s$ are absolute values, $|\cdot| \sim |\cdot|^s$ and $|\cdot|' \sim |\cdot|'^s$. Hence the assertion follows.

Remarks and Definitions 4.2.4. Let $(K, |\cdot|)$ be a valued field and V a K-vector space.

1. A ($|\cdot|$-compatible) *norm* on V is a map $\|\cdot\| \colon V \to \mathbb{R}_{\ge0}$ such that the following properties hold for all $u, v \in V$ and $\lambda \in K$,:
   (N1) $\|u\| = 0$ if and only if $u = 0$.
   (N2) $\|u + v\| \le \|u\| + \|v\|$.
   (N3) $\|\lambda u\| = |\lambda|\,\|u\|$.

2. Let $\|\cdot\|\colon V \to \mathbb{R}_{\ge 0}$ be a norm. The map $V \times V \to \mathbb{R}_{\ge 0}$, defined by $(u,v) \mapsto \|u-v\|$, is a metric and defines a topology on V, called the $\|\cdot\|$-*topology.* For $a \in V$ and $\varepsilon \in \mathbb{R}_{>0}$, we define the open ε-ball of a with respect to $\|\cdot\|$ by
$$B_\varepsilon^{\|\cdot\|}(a) = \{u \in V \mid \|u-a\| < \varepsilon\} = a + B_\varepsilon^{\|\cdot\|}(0)\,.$$
Then $\{B_\varepsilon^{\|\cdot\|}(a) \mid \varepsilon \in \mathbb{R}_{>0}\}$ is a fundamental system of open neighborhoods of a. A sequence $(u_n)_{n\ge 0}$ in V converges to $u \in V$ in the $\|\cdot\|$-topology if $(\|u_n-u\|)_{n\ge 0} \to 0$, and in this case we write
$$(u_n)_{n\ge 0} \overset{\|\cdot\|}{\to} u \quad \text{or} \quad \|\cdot\|\text{-}\lim_{n\to\infty} u_n = u\,.$$
A sequence $(u_n)_{n\ge 0}$ in V is called a $\|\cdot\|$-*Cauchy sequence* if for every $\varepsilon \in \mathbb{R}_{>0}$ there exists some $n_0 \ge 0$ such that $\|x_n - x_m\| < \varepsilon$ for all $m \ge n \ge n_0$.
Every convergent sequence in V is a $\|\cdot\|$-Cauchy sequence, and V is called $\|\cdot\|$-*complete*, if every $\|\cdot\|$-Cauchy sequence converges.
3. Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on V are called *equivalent* if they induce the same topology. Obviously, $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent if and only if there exist $C_1,\, C_2 \in \mathbb{R}_{>0}$ such that $\|u\|_2 \le C_1\|u\|_1$ and $\|u\|_1 \le C_2\|u\|_2$ for all $u \in V$.
If $\|\cdot\|_1$ and $\|\cdot\|_2$ on V are equivalent norms, then a sequence in V is a $\|\cdot\|_1$-Cauchy sequence if and only if it is a $\|\cdot\|_2$-Cauchy sequence, and V is $\|\cdot\|_1$-complete if and only if it is $\|\cdot\|_2$-complete.

`equivalence`

Theorem 4.2.5 (Norm Equivalence Theorem)**.** *Let $(K,\cdot)$ be a complete valued field and V a finite-dimensional K-vector space. Then any two $|\cdot|$-compatible norms on V are equivalent, and V is complete with respect to each of them.*

Proof. We consider first the case $V = K^p$ for some $p \in \mathbb{N}$, and define the maximum norm $\|\cdot\|_0 = \|\cdot\|_0^{(p)}\colon K^p \to \mathbb{R}_{\ge 0}$ by $\|((x_1,\ldots,x_p)\|_0 = \max\{|x_1|,\ldots,|x_p|\}$. Then $\|\cdot\|_0$ is a $|\cdot|$-compatible norm on K^p, and
$$B_\varepsilon^{\|\cdot\|_0}(\boldsymbol{a}) = \prod_{i=1}^p B_\varepsilon^{\|\cdot\|}(a_i) \quad \text{for each } \boldsymbol{a} = (a_1,\ldots,a_p) \in K^p \text{ and } \varepsilon \in \mathbb{R}_{>0}\ .$$
Hence the $\|\cdot\|_0$-topology on K^p is the product topology of $(K,|\cdot|)$. In particular, a sequence $(\boldsymbol{x}^{(n)})_{n\ge 0} = ((x_1^{(n)},\ldots,x_p^{(n)})_{n\ge 0}$ converges to $\boldsymbol{x} = (x_1,\ldots,x_p)$ in the $\|\cdot\|_0$-topology if and only if $(x_i^{(n)})_{n\ge 0} \overset{|\cdot|}{\to} x^{(i)}$ for all $i \in [1,p]$, and $(\boldsymbol{x}^{(n)})_{n\ge 0}$ is a $\|\cdot\|_0$-Cauchy sequence if and only if $(x_i^{(n)})_{n\ge 0}$ is a Cauchy sequence in $(K,|\cdot|)$ for all $i \in [1,p]$. Hence K^p is $\|\cdot\|_0$-complete. We prove:

A. Every $|\cdot|$-compatible norm on K^p is equivalent to $\|\cdot\|_0$.

Proof of **A.** By induction on p. Let $\|\cdot\|$ be a $|\cdot|$-compatible norm on K^p.

$p=1$: Then $|\cdot\|_0 = |\cdot|\colon K \to \mathbb{R}_{\ge 0}$, and for all $a \in K$ we obtain $\|a\| = |a|\,\|1\| = \|1\|\,\|a\|_0$.

$p \ge 2$, $p-1 \to p$: Let $(\boldsymbol{e}_1,\ldots,\boldsymbol{e}_p)$ be the canonical basis of K^p. If $\boldsymbol{a} = (a_1,\ldots,a_p) \in K^p$, then
$$\|\boldsymbol{a}\| = \Big\|\sum_{i=1}^p a_i\boldsymbol{e}_i\Big\| \le \sum_{i=1}^p |a_i|\,\|\boldsymbol{e}_i\| \le \|\boldsymbol{a}\|_0 \sum_{i=1}^p \|\boldsymbol{e}_i\|\,,$$

and it remains to prove that there exists some $C \in \mathbb{R}_{>0}$ such that $\|\boldsymbol{a}\|_0 \le C\,\|\boldsymbol{a}\|$ for all $\boldsymbol{a} \in K^p$. We assume the contrary. Then it follows that, for every $n \in \mathbb{N}$, there exists some $\boldsymbol{a}^{(n)} = (a_1^{(n)}, \ldots, a_p^{(n)}) \in K^p$ such that $\|\boldsymbol{a}^{(n)}\|_0 > n\|\boldsymbol{a}^{(n)}\|$. For $n \in \mathbb{N}$, let $j(n) \in [1,p]$ be such that $\|\boldsymbol{a}^{(n)}\|_0 = |a_{j(n)}^{(n)}|$. Then there exists some $j \in [1,p]$ and an infinite set $T \subset \mathbb{N}_0$ such that $j(n) = j$ for all $n \in T$. We may assume that $j = p$ and $(\boldsymbol{a}^{(n)})_{n\in T} = (\boldsymbol{a}^{(n)})_{n\ge 1}$. Then it follows that $\|\boldsymbol{a}^{(n)}\|_0 = |a_p^{(n)}| > n\|\boldsymbol{a}^{(n)}\|$ for all $n \ge 1$, we set

$$\boldsymbol{b}^{(n)} = \frac{1}{a_p^{(n)}}\,\boldsymbol{a}^{(n)} \quad \text{and obtain} \quad \|\boldsymbol{b}^{(n)}\|_0 = \frac{1}{|a_p^{(n)}|}\|\boldsymbol{a}^{(n)}\|_0 = 1 > n\|\boldsymbol{b}^{(n)}\|\,, \quad \text{hence} \quad \|\boldsymbol{b}^{(n)}\| < \frac{1}{n}\,,$$

and thus $(\boldsymbol{b}^{(n)})_{n\ge1} \xrightarrow{\|\cdot\|} \boldsymbol{0} \in K^p$. Note that $\boldsymbol{b}^{(n)} = (b_1^{(n)}, \ldots, b_{p-1}^{(n)}, 1)$ for all $n \ge 1$.

Now we define $\pi\colon K^p \to K^{p-1}$ by $\pi(x_1, \ldots, x_p) = (x_1, \ldots, x_{p-1})$, $\nu\colon K^{p-1} \to K^p$ by $\nu(x_1, \ldots, x_{p-1}) = (x_1, \ldots, x_{p-1}, 0)$, and $\|\cdot\|^* = \|\cdot\| \circ \nu\colon K^{p-1} \to \mathbb{R}_{\ge 0}$. Then $\|\boldsymbol{x}\|^* = \|\nu(\boldsymbol{x})\|$ for all $\boldsymbol{x} \in K^{p-1}$, and $\|\cdot\|^*$ is a $|\cdot|$-compatible norm on K^{p-1}. By the induction hypothesis, $\|\cdot\|^*$ is equivalent to then maximum norm $\|\cdot\|_0^{(p-1)}$ of K^{p-1}, and thus K^{p-1} is $\|\cdot\|^*$-complete.

For all $m \ge n \ge 1$, we obtain (observing that $b_p^{(n)} = b_p^{(m)} = 1$)

$$\begin{aligned}\|\pi(\boldsymbol{b}^{(n)}) - \pi(\boldsymbol{b}^{(m)}\|^* = \|\pi(\boldsymbol{b}^{(n)} - \boldsymbol{b}^{(m)})\|^* &= \|\nu\circ\pi(\boldsymbol{b}^{(n)} - \boldsymbol{b}^{(m)})\| \\ &= \|\boldsymbol{b}^{(n)} - \boldsymbol{b}^{(m)}\| \le \|\boldsymbol{b}^{(n)}\| + \|\boldsymbol{b}^{(m)}\| < \frac{1}{n} + \frac{1}{m}\,.\end{aligned}$$

It follows that $(\pi(\boldsymbol{b}^{(n)})_{n\ge1}$ is a $\|\cdot\|^*$-Cauchy sequence in K^{p-1}, and thus it is convergent, say $(\pi(\boldsymbol{b}^{(n)})_{n\ge1} \xrightarrow{\|\cdot\|^*} \boldsymbol{b}^* \in K^{p-1}$. Since $\|\nu\circ\pi(\boldsymbol{b}^{(n)}) - \nu(\boldsymbol{b}^*\| = \|\nu(\pi(\boldsymbol{b}^{(n)}) - \boldsymbol{b}^*)\| = \|\pi(\boldsymbol{b}^{(n)}) - \boldsymbol{b}^*\|^*$, it follows that $(\nu\circ\pi(\boldsymbol{b}^{(n)})_{n\ge1} \xrightarrow{\|\cdot\|} \nu(\boldsymbol{b}^*)$, and therefore

$$(\boldsymbol{b}^{(n)})_{n\ge1} = \big((\nu\circ\pi)(\boldsymbol{b}^{(n)}) + \boldsymbol{e}_p\big)_{n\ge1} \xrightarrow{\|\cdot\|} \nu(\boldsymbol{b}^*) + \boldsymbol{e}_p \ne \boldsymbol{0}\,, \quad \text{a contradiction.} \qquad \square[\mathbf{A}.]$$

Now we derive the general case. For $i \in \{1, 2\}$, let $\|\cdot\|_i$ be $|\cdot|$-compatible norms on a K-vector space V such that $\dim_K(V) = p \in \mathbb{N}$, let $\Phi\colon K^p \to V$ be a K-isomorphism and $\|\cdot\|_i' = \|\cdot\|_i\circ\Phi\colon K^p \to \mathbb{R}_{\ge0}$. Then $\|\cdot\|_1'$, $\|\cdot\|_2'$ are $|\cdot|$-compatible norms on K^p, hence they are equivalent to the maximum norm, and K^p is $\|\cdot\|_i'$-complete. Applying Φ, it follows that $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent, and V is $\|\cdot\|_i$-complete. $\square$

`ngeindeutig` **Theorem 4.2.6.** *Let $(K, |\cdot|_0)$ be a complete valued field and $\overline{K}/K$ an algebraic extension.*

1. *There exists at most one absolute value $|\cdot|\colon \overline{K} \to \mathbb{R}_{\ge0}$ such that $|\cdot| \restriction K = |\cdot|_0$.*
2. *Let $\overline{K}$ be an algebraic closure of K and $|\cdot|\colon \overline{K} \to \mathbb{R}_{\ge0}$ an absolute value such that $|\cdot| \restriction K = |\cdot|_0$.*
   (a) *If $K \subset L \subset \overline{K}$ be an intermediate field and $\sigma \in \mathrm{Hom}_K(L, \overline{K})$. Then $|\sigma(\alpha)| = |\alpha|$ for all $\alpha \in L$. In particular, if α and β are conjugate over K, then $|\alpha| = |\beta|$.*
   (b) *If $\alpha \in \overline{K}$ and $X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in K[X]$ is the minimal polynomial of α over K, then $|\alpha| = |a_0|_0^{1/d}$.*

(c) *Let $K \subset L \subset \overline{K}$ be an intermediate field and $[L\!:\!K] = n \in \mathbb{N}$. Then $|\cdot|_L = |\cdot| \upharpoonright L$ is a absolute value of L, $(K, |\cdot|_L)$ is complete, and*

$$|\alpha| = \sqrt[n]{|\mathsf{N}_{L/K}(\alpha)|_0} \quad \textit{for all} \quad \alpha \in L\,.$$

Moreover, $\mathsf{N}_{L/K}\colon L \to K$ and $\mathsf{Tr}_{L/K}\colon L \to K$ are continuous.

(d) (Krasner's Lemma) *Let $|\cdot|$ be non-archimedean, $\alpha, \beta \in \overline{K}$ such that α is separable over K, and let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over K. If $|\beta - \alpha| < |\alpha_i - \alpha|$ for all $i \in [2, n]$, then $\alpha \in K(\beta)$.*

PROOF. 1. Let $|\cdot|, |\cdot|'\colon \overline{K} \to \mathbb{R}_{\ge 0}$ be absolute values such that $|\cdot| \upharpoonright K = |\cdot|' \upharpoonright K = |\cdot|_0$. If $\alpha \in \overline{K}$, then $|\cdot| \upharpoonright K(\alpha)$ and $|\cdot|' \upharpoonright K(\alpha)$ are $|\cdot|_0$-compatible norms on the K-vector space $K(\alpha)$ and absolute values on field $K(\alpha)$. By Theorem `normequivalence` 4.2.5, they are equivalent, and thus $|\cdot| = |\cdot|'$ by Theorem `equivalent` 4.1.6.

2. (a) Let $\overline{\sigma} \in \mathsf{Gal}(\overline{K}/K)$ be such that $\overline{\sigma} \,|\, L = \sigma$. Then $|\cdot| \circ \overline{\sigma}\colon \overline{K} \to \mathbb{R}_{\ge 0}$ is an absolute value of $\overline{K}$ such that $|\cdot| \circ \overline{\sigma} \,|\, K = |\cdot|_0$. By 1., it follows that $|\cdot| \circ \overline{\sigma} = |\cdot|$, and thus $|\sigma(\alpha)| = |\overline{\sigma}(\alpha)| = |\alpha|$ for all $\alpha \in L$.

(b) Let

$$X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 = \prod_{\nu=1}^{d} (X - \alpha_\nu)\,, \quad \text{where} \quad \alpha = \alpha_1, \ldots, \alpha_d \in \overline{K}\,.$$

For all $\nu \in [1, d]$, α_ν and α are conjugate over K, hence $|\alpha_\nu| = |\alpha|$, and therefore

$$|a_0|_0 = |a_0| = \prod_{\nu=1}^{d} |\alpha_\nu| = |\alpha|^d\,.$$

(c) Obviously, $|\cdot|_L$ is an absolute value of K and a $|\cdot|_0$-compatible norm on L, and Theorem `normequivalence` 4.2.5 implies that $(L, |\cdot|_L)$ is complete. If $\alpha \in L$, $X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in K[X]$ is the minimal polynomial of α over K and $m = [L\!:\!K(\alpha)]$, then $n = md$ and

$$|\mathsf{N}_{L/K}(\alpha)|_0 = |a_0^m|_0 = |\alpha^m|^d = |\alpha|^n\,.$$

Let $\mathcal{H} = \mathrm{Hom}_K(L, \overline{K}$ and q the degree of inseparability of L/K. Then

$$\mathsf{N}_{L/K} = \Big(\prod_{\sigma \in \mathcal{H}} \sigma\Big)^q \quad \text{and} \quad \mathsf{Tr}_{L/K} = q \sum_{\sigma \in \mathcal{H}} \sigma\,.$$

For all $\sigma \in \mathcal{H}$, the map $\sigma\colon (L, |\cdot|_L) \to (\overline{K}, |\cdot|)$ is a valuation homomorphism and thus continuous. Therefore $\mathsf{N}_{L/K}$ and $\mathsf{Tr}_{L/K}$ are also continuous.

(d) Assume that $|\beta - \alpha| < |\alpha_i - \alpha|$ for all $i \in [2, n]$, but $\alpha \notin K(\beta)$. Then $K(\beta) \subsetneq K(\alpha, \beta)$, and thus there exists some $i \in [2, n]$ such that α and α_i are conjugate over $K(\beta)$. Then $\beta - \alpha$ and $\beta - \alpha_i$ are also conjugate over $K(\beta)$, and therefore $|\beta - \alpha| = |\beta - \alpha_i|$. Hence it follows that $|\alpha_i - \alpha| = |(\beta - \alpha) - (\beta - \alpha_i)| \le |\beta - \alpha| < |\alpha_i - \alpha|$, a contradiction. ☐

`ostrowski` **Theorem 4.2.7.** *Let $(K, \|\cdot\|)$ be a complete archimedean valued field. Then there exists a value isomorphism $\Phi\colon (K, \|\cdot\|) \to (\mathbb{K}, |\cdot|_\infty^s)$ for some $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ and $s \in (0, 1]$.*

PROOF. As $\|\cdot\|$ is archimedean, it follows by the Theorems `nichtarch` 4.1.4 and `valueq` 4.1.9, that K has characteristic 0, hence we may assume that $\mathbb{Q} \subset K$, and $\|\cdot\| \restriction \mathbb{Q} = |\cdot|_\infty^s$ for some $s \in (0,1]$. By Theorem `completion` 4.2.3, $(\mathbb{R}, |\cdot|_\infty^s)$ is a completion of $(\mathbb{Q}, |\cdot|_\infty^s)$, and thus there exists a value homomorphism $\Phi\colon (\mathbb{R}, |\cdot|_\infty^s) \to (K, \|\cdot\|)$. By the Exchange Lemma, we may assume that $\mathbb{R} \subset K$ and $\|\cdot\| \restriction \mathbb{R} = |\cdot|_\infty^s$. If $\mathbb{R} = K$, we are done. Thus suppose that $\mathbb{R} \subsetneq K$. Then it suffices to prove the following assertion.

A. For every $\xi \in K$, there exists a polynomial $g \in \mathbb{R}[X]$ such that $\deg(g) = 2$ and $g(\xi) = 0$.

Suppose that **A.** holds. Then there exists a field isomorphism $\Phi\colon K \to \mathbb{C}$, and, again by the Exchange Lemma, we may assume that $K = \mathbb{C}$. Then $|\cdot|_\infty^s$ and $\|\cdot\|$ are absolute values on K such that $|\cdot|_\infty^s \restriction \mathbb{R} = \|\cdot\| \restriction \mathbb{R}$, hence $|\cdot|_\infty^s = \|\cdot\|$ by Theorem `fortsetzungeindeutig` 4.2.6. Hence it really suffices to prove **A.**

Proof of **A.** Let $\xi \in K$. Throughout this proof, we write $|\cdot|$ instead of $|\cdot|_\infty$. We shall prove that there exists some $z \in \mathbb{C}$ such that ξ is a zero of the polynomial $g = X^2 - (z+\overline{z})X + z\overline{z} \in \mathbb{R}[X]$. Assume the contrary, and define

$$f\colon \mathbb{C} \to \mathbb{R}_{\ge 0} \quad \text{by} \quad f(z) = \|\xi^2 - (z+\overline{z})\xi + z\overline{z}\,\|\,.$$

Then f is continuous, $f(z) > 0$ and

$$f(z) \ge \|z\overline{z}\| \Big[1 - \frac{\|\xi\|^2}{\|z\overline{z}\|} - \|\xi\| \Big\|\frac{z+\overline{z}}{z\overline{z}}\Big\|\Big] = |z|^{2s}\Big[1 - \frac{\|\xi\|^2}{|z|^{2s}} - \|\xi\| \Big|\frac{1}{z} + \frac{1}{\overline{z}}\Big|^s\Big] \quad \text{for all } z \in \mathbb{C}\,.$$

Hence it follows that

$$\lim_{z\to\infty} f(z) = \infty\,, \quad \text{and therefore there exists} \quad m = \min f(\mathbb{C}) \in \mathbb{R}_{>0}\,.$$

The set $S = \{z \in \mathbb{C} \mid f(z) = m\}$ is bounded and closed, hence compact, and thus there exists some $z_0 \in S$ such that $|z_0| \ge |z|$ for all $z \in S$. We fix some $\varepsilon \in (0,m)$ and consider the polynomial

$$g_\varepsilon = X^2 - (z_0 + \overline{z}_0)X + z_0\overline{z}_0 + \varepsilon = (X - z_1)(X - z_2) \in \mathbb{R}[X]\,,$$

where z_1, $z_2 \in \mathbb{C}$ and $|z_1| \ge |z_2|$. Hence $|z_1|^2 \ge |z_1 z_2| = z_0\overline{z}_0 + \varepsilon > |z_0|^2$, which implies $z_1 \notin S$ and therefore $f(z_1) > m$.

For $n \in \mathbb{N}$, let $G_n = (g_\varepsilon - \varepsilon)^n - (-\varepsilon)^n \in \mathbb{R}[X]$. Then $\deg(G_n) = 2n$, $G(z_1) = 0$, and therefore

$$G_n = \prod_{i=1}^{2n}(X - \alpha_i)\,, \text{ here } z_1 = \alpha_1, \ldots, \alpha_{2n} \in \mathbb{C}, \text{ and } G_n \in \mathbb{R}[X] \text{ implies } \quad G_n = \prod_{i=1}^{2n}(X - \overline{\alpha}_i)\,.$$

Hence we obtain

$$\|G_n(\xi)\|^2 = \prod_{i=1}^{2n}\|(\xi - \alpha_i)(\xi - \overline{\alpha}_i)\| = \prod_{i=1}^{2n}\|\xi^2 - (\alpha_i + \overline{\alpha}_i)\xi + \alpha_i\overline{\alpha}_i\| = \prod_{i=1}^{2n} f(\alpha_i) \ge f(z_1)m^{2n-1}\,,$$

and, on the other hand,

$$\|G_n(\xi)\| \le \|g_\varepsilon(\xi) - \varepsilon\|^n + \varepsilon^n = \|\xi^2 - (z_0 + \overline{z}_0)\xi + z_0\overline{z}_0\|^n + \varepsilon^n = f(z_0)^n + \varepsilon^n = m^n + \varepsilon^n\,.$$

Therefore it follows that

$$\frac{f(z_1)}{m} \le \frac{\|G_n(\xi)\|^2}{m^{2n}} \le \frac{(m^n + \varepsilon^n)^2}{m^{2n}} = \Big[1 + \Big(\frac{\varepsilon}{m}\Big)^n\Big]^2, \quad \text{and since} \quad \lim_{n\to\infty}\Big[1 + \Big(\frac{\varepsilon}{m}\Big)^n\Big]^2 = 1\,,$$

we conclude $f(z_1) \le m$, a contradiction. $\square$

Corollary 4.2.8. *Let* K *be an algebraic number field,* $[K:\mathbb{Q}] = n = r_1 + 2r_2$ *and* $\mathrm{Hom}(K,\mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$ *such that* $\sigma_j(K) \subset \mathbb{R}$ *for all* $j \in [1, r_1]$*, and* $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ *for all* $j \in [1, r_2]$*. For* $j \in [1, r_1+r_2]$*, let* $|\cdot|_{\infty,j} = |\cdot|_\infty \circ \sigma_j$ *(see* Example 4.1.2.4*). If* $\|\cdot\|$ *is an archimedean absolute value of* K*, then there is a unique* $j \in [1, r_1+r_2]$ *such that* $\|\cdot\| \sim |\cdot|_{\infty,j}$*.*

Proof. Uniqueness follows by Example 4.1.2.4. Thus let $\|\cdot\|$ be an archimedean absolute value of K and $(\widehat{K}, \|\cdot\|)$ a completion of $(K, \|\cdot\|)$. By Theorem 4.2.7 there exists some $s \in (0,1]$ and either a valuation isomorphism $\Phi\colon (\widehat{K}, \|\cdot\|) \to (\mathbb{R}, |\cdot|_\infty^s)$ or a valuation isomorphism $\Phi\colon (\widehat{K}, \|\cdot\|) \to (\mathbb{C}, |\cdot|_\infty^s)$. In both cases, it follows that $\varphi = \Phi \,|\, K \in \mathrm{Hom}(K, \mathbb{C})$, and thus there exists some $j \in [1, r_1+r_2]$ such that $\varphi \in \{\sigma_j, \overline{\sigma}_j\}$. Hence $\|\cdot\| = |\cdot|_\infty^s \circ \sigma_j = |\cdot|_{\infty,j}^s \sim |\cdot|_{\infty,j}$. $\square$

4.3. Arithmetic of discrete valued fields

discrete1

Theorem and Definition 4.3.1. *Let* $(K, |\cdot|)$ *be a discrete valued field and* $\rho \in (0,1)$ *such that* $|K^\times| = \langle \rho \rangle$*. Let* $v\colon K \to \mathbb{Z} \cup \{\infty\}$ *be the associated valuation, given by*

$$v(a) = \frac{\log|a|}{\log \rho} \quad \text{and} \quad |a| = \rho^{v(a)} \quad \text{for all } a \in K\,.$$

We define

$$\mathcal{O}_v = \{x \in K \mid v(x) \ge 0\} = \{x \in K \mid |x| \le 1\} = \{x \in K \mid |x| < \rho^{-1}\}\,, \quad \text{and}$$
$$\mathfrak{p}_v = \{x \in K \mid v(x) > 0\} = \{x \in K \mid v(x) \ge 1\} = \{x \in K \mid |x| < 1\} = \{x \in K \mid |x| \le \rho\}.$$

Then $\mathcal{O}_v$ *is a dv-domain,* $\mathcal{P}(\mathcal{O}_v) = \{\mathfrak{p}_v\}$*,* $\mathcal{O}_v^\times = \{x \in K \mid v(x) = 0\} = \{x \in K \mid |x| = 1\}$*, and* $v = \mathsf{v}_{\mathfrak{p}_v}\colon K \to \mathbb{Z} \cup \{\infty\}$*. If* $\{0\} \ne \mathfrak{a} \in \mathcal{F}(\mathcal{O}_v)$*, then there exists some* $a \in \mathfrak{a}$ *such that* $v(a) = \min v(\mathfrak{a}) \in \mathbb{Z}$*, and for each such* a *we have* $\mathfrak{a} = a\mathcal{O}_v$*.*

$\mathcal{O}_v$ is called the *valuation domain*, $\mathfrak{p}_v$ is called the *valuation ideal* and $\mathsf{k}_v = \mathcal{O}_v/\mathfrak{p}_v$ is called the *residue class field* of $(K, |\cdot|)$ or of (K, v). Every $\pi \in K$ satisfying $v(\pi) = 1$ [or, equivalently, $|\pi| = \rho$] is called a *prime element* or a *uniformizing parameter.*

Let $\pi \in K$ *be a uniformizing parameter. Then* $\mathfrak{p}_v^k = \pi^k \mathcal{O}_v = \{x \in K \mid v(x) \ge k\}$ *for all* $k \in \mathbb{Z}$*, and for all* $k \in \mathbb{N}$*, there is a* k_v*-vector space isomorphism*

$$\phi\colon \mathcal{O}_v/\mathfrak{p}_v^k \overset{\sim}{\to} \mathfrak{p}_v^k/\mathfrak{p}_v^{k+1}\,, \quad \text{given by} \quad \phi(x + \mathfrak{p}_v) = \pi^k x + \mathfrak{p}_v^{k+1} \quad \text{for all } x \in \mathcal{O}_v\,.$$

Proof. If $x, y \in \mathcal{O}_v$, then $|x| \le 1$, $|y| \le 1$, $|x-y| \le \max\{|x|, |y|\} \le 1$ and therefore $|xy| = |x|\,|y| \le 1$. Hence it follows that $\{x-y, xy\} \subset \mathcal{O}_v$, and therefore $\mathcal{O}_v \subset K$ is a subring. By definition, $\mathcal{O}_v^\times = \{x \in \mathcal{O}_v^\bullet \mid x^{-1} \in \mathcal{O}_v\} = \{x \in K^\times \mid |x| \le 1,\ |x|^{-1} \le 1\} = \{x \in K \mid |x| = 1\}$. Since there is an element $x \in K$ such that $|x| \ne 1$, there is some $x \in K$ such that $|x| > 1$, and thus $\mathcal{O}_v \ne K$.

If $x, y \in \mathfrak{p}_v$ and $c \in \mathcal{O}_v$, then $|x| < 1$, $|y| < 1$, $|c| \le 1$, $|x-y| \le \max\{|x|, |y|\} < 1$ and $|cx| = |c|\,|x| < 1$. Hence it follows that $\{x-y, cx\} \subset \mathfrak{p}_v$, $\mathfrak{p}_v \subset \mathcal{O}_v$ is an ideal, and $\mathcal{O}_v^\times = \mathcal{O}_v \setminus \mathfrak{p}_v$. Therefore $\mathcal{O}_v$ is a local domain with maximal ideal $\mathfrak{p}_v$.

Let $\{0\} \ne \mathfrak{a} \in \mathcal{F}(\mathcal{O}_v)$. Then there is some $c \in \mathcal{O}_v^\bullet$ such that $c\mathfrak{a} \subset \mathcal{O}_v$, hence $\mathfrak{a} \subset c^{-1}\mathcal{O}_v$, and $v(\mathfrak{a}) \subset -v(\mathfrak{a}) + \mathbb{N}_0 \subset \mathbb{Z}$. Hence there exists some $a \in \mathfrak{a}$ such that $v(a) = \min v(\mathfrak{a})$, and clearly $a\mathcal{O}_v \subset \mathfrak{a}$. Conversely, if $x \in \mathfrak{a}$, then $v(x) \ge v(a)$, hence $v(a^{-1}x) = -v(a) + v(x) \ge 0$, $a^{-1}x \in \mathcal{O}_v$ and $x \in \mathcal{O}_v$. Hence $\mathfrak{a} = a\mathcal{O}_v$. In particular, $\mathcal{O}_v$ is a principal ideal domain and thus a dv-domain with $\mathcal{P}(\mathcal{O}_v) = \{\mathfrak{p}_v\}$.

Let $\pi \in K$ be a uniformizing parameter. Then $1 = v(\pi) = \min v(\mathfrak{p}_v)$, hence $\mathfrak{p}_v = \pi\mathcal{O}_v$, and $\mathfrak{p}_v^k = \pi^k\mathcal{O}_v = \{x \in K \mid v(x) \ge k\}$ for all $k \in \mathbb{Z}$. If $x \in K^\times$, then $x = \pi^{v(x)}u$ for some $u \in \mathcal{O}_v^\times$, and $x\mathcal{O}_v = \pi^{v(x)}\mathcal{O}_v = \mathfrak{p}_v^{v(x)}$. By definition, this implies $\mathsf{v}_{\mathfrak{p}_v}(x) = v(x)$, and thus $\mathsf{v}_{\mathfrak{p}_v} = v\colon K \to \mathbb{Z} \cup \{\infty\}$.

For $k \in \mathbb{N}$, the map

$$\phi_0\colon \mathcal{O}_v \;\to\; \mathfrak{p}_v^k/\mathfrak{p}_v^{k+1} = \pi^k\mathcal{O}_v/\pi^{k+1}\mathcal{O}_v\,, \quad \text{defined by} \quad \phi_0(x) = \pi^k x + \pi^{k+1}\mathcal{O}_v$$

is an epimorphism, and $\operatorname{Ker}(\phi_0) = \{x \in \mathcal{O}_v \mid v(\pi^k x) \ge k+1\} = \{x \in \mathcal{O}_v \mid v(x) \ge 1\} = \mathfrak{p}_v$. Hence ϕ_0 induces an isomorphism ϕ as asserted, and obviously ϕ is an isomorphism of k_v-vector spaces. □

discrete2

Theorem 4.3.2. *Let $(K, |\cdot|)$ be a discrete valued field, $\rho \in (0,1)$ such that $|K^\times| = \langle\rho\rangle$, and $v\colon K \to \mathbb{Z} \cup \{\infty\}$ the associated valuation. In the following, convergence always means convergence with respect to $|\cdot|$.*

1. *Let $(x_n)_{n\ge0}$ be a sequence in K and $x \in K$.*
   - (a) *$(x_n)_{n\ge0} \to x$ if and only if $(v(x_n - x))_{n\ge0} \to \infty$.*
   - (b) *If $(x_n)_{n\ge0} \to x$ and $x \ne 0$, then $v(x_n) = v(x)$ for all $n \gg 1$.*
   - (c) *$(x_n)_{n\ge0}$ is a Cauchy sequence if and only if $(x_{n+1} - x_n)_{n\ge0} \to 0$.*
   - (d) *Let $(K, |\cdot|)$ be complete. Then the infinite series*

     $$\sum_{n\ge0} x_n \quad \text{converges in } K \text{ if and only if } \quad (x_n)_{n\ge0} \to 0\,.$$

     Moreover,

     $$(x_n)_{n\ge0} \to x \quad \text{if and only if} \quad x = x_0 + \sum_{n=0}^{\infty}(x_{n+1} - x_n)\,, \quad \text{and then}$$

     $$x - x_k = \sum_{n=k}^{\infty}(x_{n+1} - x_n) \quad \text{and} \quad v(x - x_k) \ge \inf\{v(x_{n+1} - x_n) \mid n \ge k\} \quad \text{for all } k \ge 0.$$
2. *For all $n \in \mathbb{Z}$, $\mathfrak{p}_v^n \subset K$ is open and closed. In particular, $\mathcal{O}_v \subset K$ and $\mathcal{O}_v^\times \subset K$ are both open and closed, and, for every $a \in K$, $\{a + \mathfrak{p}_v^n \mid n \in \mathbb{N}\}$ is a fundamental system of neighborhoods of a.*

PROOF. 1. (a) By definition, $(x_n)_{n\ge0} \to x$ if and only if $(|x_n - x|)_{n\ge0} = (\rho^{v(x_n - x)})_{n\ge0} \to 0$, and this holds if and only if $(v(x_n - x))_{n\ge0} \to \infty$.

(b) If $(x_n)_{n\ge0} \to x \ne 0$, then $v(x_n - x) > v(x)$ for all $n \gg 1$ by (a), and therefore $v(x_n) = v((x_n - x) + x) = v(x)$ for all $n \gg 1$.

(c) If $(x_n)_{n\ge0}$ is a Cauchy sequence and $\varepsilon \in \mathbb{R}_{>0}$, then there exists some $n_0 \ge 0$ such that $|x_m - x_n| < \varepsilon$ for all $m \ge n \ge n_0$, and in particular $|x_{n+1} - x_n| < \varepsilon$ for all $n \ge n_0$. Hence $(x_{n+1} - x_n)_{n\ge0} \to 0$.

Conversely, assume that $(x_{n+1} - x_n)_{n\ge0} \to 0$, and let $\varepsilon \in \mathbb{R}_{>0}$. Then there is some $n_0 \ge 0$ such that $|x_{n+1} - x_n| < \varepsilon$ for all $n \ge n_0$. If $m \ge n \ge n_0$, then

$$|x_m - x_n| = \Big|\sum_{i=n}^{m-1}(x_{i+1} - x_i)\Big| \le \max\{|x_{i+1} - x_i| \mid i \in [n, m-1]\} < \varepsilon\,,$$

and thus $(x_n)_{n\ge 0}$ is a Cauchy sequence.

(d) For $n \ge 0$, we set

$$s_n = \sum_{k=0}^{n-1} x_k \,. \quad \text{By definition,} \quad \sum_{n\ge 0} x_n \quad \text{converges if and only if} \quad (s_n)_{n\ge 0} \quad \text{converges.}$$

Since $(K, |\cdot|)$ is complete, the sequence $(s_n)_{n\ge 0}$ converges if and only if it is a Cauchy sequence, and this holds if and only if $(x_n) - n \ge 0 = (s_{n+1} - s_n)_{n\ge 0} \to 0$.

By definition, $(x_n)_{n\ge 0} \to x$ if and only if

$$x = \lim_{m\to\infty} x_m = \lim_{m\to\infty} \Big(x_0 + \sum_{n=0}^{m-1} (x_{n+1} - x_n) \Big) = x_0 + \sum_{n=0}^{\infty} (x_{n+1} - x_n) \,.$$

Assume that his holds. If $k \ge 0$, then

$$x - x_k = \lim_{m\to\infty} (x_m - x_k) = \lim_{m\to\infty} \sum_{n=k}^{m-1} (x_{n+1} - x_n) = \sum_{n=l}^{\infty} (x_{n+1} - x_n) \,,$$

and, for each $m \ge k$,

$$|x_m - x_k| = \Big| \sum_{n=k}^{m-1} (x_{n+1} - x_n) \Big| \ge \min\{ |x_{n+1} - x_n| \mid n \in [k, m-1] \} \ge \inf\{ |x_{n+1} - x_n| \mid n \ge k \} \,,$$

which implies

$$|x - x_k| = \lim_{m\to\infty} |x_m - x_k| \ge \inf\{ |x_{n+1} - x_n| \mid n \ge k \} \,.$$

2. Since $|\cdot| \colon K \to \mathbb{R}_{\ge 0}$ is continuous, it follows that $\mathcal{O}_v = \{x \in K \mid |x| \le 1\}$ is closed, and that $\mathcal{O}_v = \{x \in K \mid |x| < \rho^{-1}\}$ is open. Let $\pi \in K$ be a uniformizing parameter and $n \in \mathbb{Z}$. Then the map $K \to K$, $x \mapsto \pi^n x$, is topological. Hence $\mathfrak{p}_v^n = \pi^n \mathcal{O}_v$ is also open and closed.

If $a \in K$ and $n \in \mathbb{N}$, then $a + \mathfrak{p}_v^n = \{x \in K \mid |x - a| \le \rho^n\}$, and since $(\rho^n)_{n\ge 1} \to 0$, these sets are a fundamental system of neighborhoods of a. □

`discrete3` **Theorem 4.3.3.** *Let $(K, |\cdot|)$ be a complete discrete valued field, $\rho \in (0,1)$, $|K^\times| = \langle \rho \rangle$, and $v \colon K \to \mathbb{Z} \cup \{\infty\}$ the associated valuation. Let $\pi \in K$ be a uniformizing parameter and $\mathcal{R} \subset \mathcal{O}_v$ a set of representatives for k_v.*

1. *Every $a \in \mathcal{O}_v$ has a unique representation*

$$a = \sum_{n=0}^{\infty} a_n \pi^n \,, \quad \text{where} \quad a_n \in \mathcal{R} \ \text{ for all } \ n \ge 0 \,.$$

2. *Every $a \in K^\times$ has a unique representation*

$$a = \sum_{n=d}^{\infty} a_n \pi^n \,, \quad \text{where} \quad d \in \mathbb{Z} \,, \quad a_n \in \mathcal{R} \ \text{ for all } \ n \ge d, \ \text{and} \ a_d \notin \mathfrak{p}_v \,.$$

In this representation, $d = v(a)$.

3. *If $\mathcal{R}$ is endowed with the discrete topology, then the map*

$$\Phi\colon \mathcal{R}^{\mathbb{N}_0} \;\to\; \mathcal{O}_v\,, \quad \text{defined by} \quad \Phi((a_n)_{n\ge0}) = \sum_{n=0}^{\infty} a_n\pi^n\,,$$

is topological. In particular, if k_v is finite, then $\mathcal{O}_v$ is compact.

Proof. 1. Since $v(a_n\pi^n) = v(a_n) + n \ge n$, we obtain $(v(a_n\pi^n))_{n\ge0} \to \infty$, $(a_n\pi^n)_{n\ge0} \to 0$, and thus the series converges.

Uniqueness: Suppose that

$$a = \sum_{n=0}^{\infty} a_n\pi^n = \sum_{n=0}^{\infty} a_n'\pi^n\,, \quad \text{where } a_n,\ a_n' \in \mathcal{R},\ \ a_n \ne a_n' \ \text{ for some } n \ge 0.$$

If $k = \min\{n \in \mathbb{N}_0 \mid a_n \ne a_n'\}$, then

$$0 = \sum_{n=0}^{\infty}(a_n - a_n')\pi^n = (a_k - a_k')\pi^k + \pi^{k+1}c \quad \text{for some } c \in \mathcal{O}_v\,,$$

and since $a_k - a_k' \notin \mathfrak{p}_v$, it follows that $v((a_k - a_k')\pi^k) = k < k+1 \le v(\pi^{k+1}c)$, a contradiction.

Existence: It suffices to prove:

A. For every $n \in \mathbb{N}_0$, there exists a unique $(n+1)$-tuple $(a_0, \ldots a_n) \in \mathcal{R}^{n+1}$ such that

$$a - \sum_{\nu=0}^{n} a_\nu\pi^\nu \in \pi^{n+1}\mathcal{O}_v\,.$$

Indeed, if **A.** holds, then there exists a sequence $(a_n)_{n\ge0}$ in $\mathcal{R}$ such that

$$a - \sum_{\nu=0}^{n} a_\nu\pi^\nu \in \pi^{n+1}\mathcal{O}_v \quad \text{for all } n \ge 0 \text{ and therefore} \quad a = \lim_{n\to\infty}\sum_{\nu=0}^{n} a_\nu\pi^\nu = \sum_{n=0}^{\infty} a_n\pi^n\,.$$

Proof of **A.** By induction on n. Suppose that $n \ge 0$, and let $a_0, \ldots, a_{n-1} \in \mathcal{R}$ be such that

$$a - \sum_{\nu=0}^{n-1} a_\nu\pi^\nu = \pi^n c \quad \text{for some} \quad c \in \mathcal{O}_v\,.$$

Then there exists a unique $a_n \in \mathcal{R}$ such tha $c \in a_n + \pi\mathcal{O}_v$, and we obtain

$$a - \sum_{\nu=0}^{n} a_\nu\pi^\nu = \pi^n(c - a_n) \in \pi^{n+1}\mathcal{O}_v\,.$$

2. *Uniqueness.* If

$$a = \sum_{n=d}^{\infty} a_n\pi^n\,, \quad \text{where} \quad d \in \mathbb{Z}\,, \quad a_n \in \mathcal{R} \ \text{ for all } n \ge d, \text{ and } \ a_d \notin \mathfrak{p}_v\,,$$

then $a = \pi^d a_d + \pi^{d+1}c$, where $c \in \mathcal{O}_v$, and therefore $v(a) = d$. Hence d is uniquely determined by a, and since

$$\pi^{-d}a = \sum_{n=0}^{\infty} a_{n+d}\pi^n \in \mathcal{O}_v\,,$$

the uniqueness of the sequence $(a_n)_{n\ge d}$ follows by 1.

Existence. If $v(a) = d \in \mathbb{Z}$, then $\pi^{-d}a \in \mathcal{O}_v^\times$, and by 1. it follows that

$$\pi^{-d}a = \sum_{n=d}^{\infty} a_n \pi^{n-d}\,, \quad \text{where} \quad a_n \in \mathcal{R} \quad \text{for all} \quad n \ge d,$$

hence $\pi^{-d}a = a_d + \pi c$ for some $c \in \mathcal{O}_v$, and since $v)(\pi^{-d}a) = 0$, it follows that $a_d \notin \mathfrak{p}_v$.

3. Φ is bijective by 1. Let $(a_n)_{n\ge0}$ is a sequence in $\mathcal{R}$,

$$a = \Phi((a_n)_{n\ge0} = \sum_{n=0}^{\infty} a_n\pi^n\,, \quad \text{and} \quad U_m = \prod_{j=0}^{m-1}\{a_j\} \times \prod_{j\ge m} \mathcal{R} \subset \mathcal{R}^{\mathbb{N}_0} \quad \text{for all} \quad m \in \mathbb{N}\,.$$

Then $\{U_m \mid m \in \mathbb{N}\}$ is a fundamental system of neighborhoods of $(a_n)_{n\ge0}$ in $\mathcal{R}^{\mathbb{N}_0}$, and $\Phi(U_m) = a + \mathfrak{p}_v^m$ for all $m \in \mathbb{N}$. By Theorem discrete2 4.3.2.2, Φ is topological. If k_v is finite, then $\mathcal{R}$ is finite, and $\mathcal{R}^{N_0}$ is compact by Tychonoff's Theorem. Hence $\mathcal{O}_v$ is compact. □

discrete4

Theorem 4.3.4. *Let $(K, |\cdot|)$ be a discrete valued field, $\rho \in (0,1)$ such that $|K^\times| = \langle\rho\rangle$, $v\colon K \to \mathbb{Z}\cup\{\infty\}$ the associated valuation, and $(K', |\cdot|')$ a completion of $(K, |\cdot|)$.*

Then $|\cdot|'$ is discrete, $|K'^\times|' = \langle\rho\rangle$, and if $v'\colon K' \to \mathbb{Z}\cup\{\infty\}$ denotes the valuation associated with $|\cdot|'$, then $v' \,|\, K = v$, $\mathcal{O}_{v'} = \overline{\mathcal{O}_v} \subset K'$, $\mathfrak{p}_{v'}^k = \overline{\mathfrak{p}_v^k} = \mathfrak{p}_v^k\mathcal{O}_{v'}$ and $\mathfrak{p}_{v'}^k \cap K = \mathfrak{p}_v^k$ for all $k \in \mathbb{Z}$. Moreover, for every $k \in \mathbb{N}$, there is an isomorphism

$$j\colon \mathcal{O}_v/\mathfrak{p}_v^k \xrightarrow{\sim} \mathcal{O}_{v'}/\mathfrak{p}_{v'}^k\,, \quad \textit{given by} \quad j(a + \mathfrak{p}_v^k) = a + \mathfrak{p}_{v'}^k \quad \textit{for all } a \in \mathcal{O}_v\,,$$

by means of which we will identify these groups in the sequel. In particular, $\mathsf{k}_v = \mathsf{k}_{v'}$.

PROOF. By Theorem nichtarch 4.1.4, $|\cdot|'$ is non-archimedean. Since $K \subset K'$ is dense and $|\cdot|'\colon K \to \mathbb{R}_{\ge0}$ is continuous, it follows that $\langle\rho\rangle \cup \{0\} = |K| \subset |K'|' \subset \overline{|K|} = \overline{\langle\rho\rangle \cup \{0\}} = \langle\rho\rangle \cup \{0\}$. Hence $|\cdot|'$ is discrete, $|K'^\times|' = \langle\rho\rangle$, and $v' \,|\, K = v$.

For $k \in \mathbb{Z}$, we obtain $\mathfrak{p}_{v'}^k \cap K = \{x \in K \mid v'(x) \ge k\} = \{x \in K \mid v(x) \ge k\} = \mathfrak{p}_v^k$ by Theorem discrete1 4.3.1, and since $\mathfrak{p}_{v'}^k \subset K'$ is closed, it follows that $\overline{\mathfrak{p}_v^k} \subset \mathfrak{p}_{v'}^k$. To prove the reverse inclusion, let $x \in \mathfrak{p}_{v'}^k$ and $(x_n)_{n\ge0}$ a sequence in K such that $(x_n)_{n\ge0} \xrightarrow{|\cdot|'} x$. Since $\mathfrak{p}_{v'}^k \subset K'$ is open, it follows that $x_n \in \mathfrak{p}_{v'}^k \cap K = \mathfrak{p}_v^k$ for all $n \gg 1$, and therefore $x \in \overline{\mathfrak{p}_v^k}$. Hence $\mathfrak{p}_{v'}^k = \overline{\mathfrak{p}_v^k}$, and, in particular, $\mathcal{O}_{v'} = \overline{\mathcal{O}_v}$.

If $k \in \mathbb{N}$, then $\mathfrak{p}_v^k = \mathcal{O}_v \cap \mathfrak{p}_{v'}^k$, and thus there exists a monomorphism $j\colon \mathcal{O}_v/\mathfrak{p}_v^k \to \mathcal{O}_{v'}/\mathfrak{p}_{v'}^k$ such that $j(a + \mathfrak{p}_v^k) = a + \mathfrak{p}_{v'}^k$ for all $a \in \mathcal{O}_v$, and we must prove that j is surjective. Thus let $x \in \mathcal{O}_{v'} = \overline{\mathcal{O}_v}$, and let $(x_n)_{n\ge0}$ be a sequence in $\mathcal{O}_v$ such that $(x_n)_{n\ge0} \xrightarrow{|\cdot|'} x$. Then it follows that $v'(x_n - x) \ge k$ for all $n \gg 1$, and thus $x_n - x \in \mathfrak{p}_{v'}^k$ and $x + \mathfrak{p}_{v'}^k = j(x_n + \mathfrak{p}_v^k)$. □

dekindvalue

Theorem and Definition 4.3.5. *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, $\mathfrak{p} \in \mathcal{P}(R)$ and $\mathsf{v}_\mathfrak{p}\colon K \to \mathbb{Z}\cup\{\infty\}$ the $\mathfrak{p}$-adic valuation. Then $\mathsf{v}_\mathfrak{p} = \mathsf{v}_{\mathfrak{p}R_\mathfrak{p}}$, $\mathcal{O}_{\mathsf{v}_\mathfrak{p}} = \{x \in K \mid \mathsf{v}_\mathfrak{p}(x) \ge 0\} = R_\mathfrak{p}$ and $\mathfrak{p}_{\mathsf{v}_\mathfrak{p}} = \{x \in K \mid \mathsf{v}_\mathfrak{p}(x) > 0\} = \mathfrak{p}R_\mathfrak{p}$.*

Let $\rho \in (0,1)$, $|\cdot|_{\mathfrak{p},\rho}$ an absolute associated with $\mathsf{v}_\mathfrak{p}$, and $(K_\mathfrak{p}, |\cdot|')$ a completion of $(K, |\cdot|_{\mathfrak{p},\rho})$. Then $(K_\mathfrak{p}, |\cdot|')$ is a complete discrete valued field, and if $\widehat{\mathsf{v}}_\mathfrak{p}\colon K_\mathfrak{p} \to \mathbb{Z}\cup\{\infty\}$ denotes the associated discrete valuation, then $K_\mathfrak{p}$ and $\widehat{\mathsf{v}}_\mathfrak{p}$ do not depend on ρ.

The field $K_\mathfrak{p}$ is called the $\mathfrak{p}$-*adic completion* of K. We denote its valuation domain and valuation ideal by

$$\widehat{R}_\mathfrak{p} = \mathcal{O}_{\widehat{\mathsf{v}}_\mathfrak{p}} = \{x \in K_\mathfrak{p} \mid \widehat{\mathsf{v}}_\mathfrak{p}(x) \ge 0\} \quad \text{and} \quad \widehat{\mathfrak{p}} = \mathfrak{p}_{\widehat{\mathsf{v}}_\mathfrak{p}} = \{x \in K_\mathfrak{p} \mid \widehat{\mathsf{v}}_\mathfrak{p}(x) > 0\}\,.$$

Then $\widehat{\mathsf{v}}_\mathfrak{p} = \mathsf{v}_{\widehat{\mathfrak{p}}}$, *and* $\mathsf{v}_{\widehat{\mathfrak{p}}} \,|\, K = \mathsf{v}_\mathfrak{p}$.

For all $k \in \mathbb{Z}$, *we have* $\mathfrak{p}^k \subset \mathfrak{p}^k R_\mathfrak{p} = \widehat{\mathfrak{p}}^k \cap K \subset \widehat{\mathfrak{p}}^k = \mathfrak{p}^k \widehat{R}_\mathfrak{p} = \overline{\mathfrak{p}^k} \subset \widehat{R}_\mathfrak{p}$, *and* $\overline{R} = \widehat{R}_\mathfrak{p}$. *If* $k \in \mathbb{N}$, *then* $\mathfrak{p}^k = \mathfrak{p}^k R_\mathfrak{p} \cap R = \widehat{\mathfrak{p}}^k \cap R$, *and the inclusion maps* $R \hookrightarrow R_\mathfrak{p} \hookrightarrow \widehat{R}_\mathfrak{p}$ *induce isomorphisms* $R/\mathfrak{p} \xrightarrow{\sim} R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \xrightarrow{\sim} \widehat{R}_\mathfrak{p}/\widehat{\mathfrak{p}}$.

By means of the above isomorphisms, we shall identify the residue class fields and obtain $R/\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \mathsf{k}_{\mathsf{v}_\mathfrak{p}} = \mathsf{k}_{\widehat{\mathsf{v}}_\mathfrak{p}} = \widehat{R}_\mathfrak{p}/\widehat{\mathfrak{p}}$. We also write $\mathsf{v}_\mathfrak{p}$ instead of $\widehat{\mathsf{v}}_\mathfrak{p}$.

Proof. By Theorem `dv` 2.6.6 we have $\mathsf{v}_\mathfrak{p} = \mathsf{v}_{\mathfrak{p}R_\mathfrak{p}}$, $\mathcal{O}_{\mathsf{v}_\mathfrak{p}} = \{x \in K \mid \mathsf{v}_\mathfrak{p}(x) \ge 0\} = R_\mathfrak{p}$, and thus also $\mathfrak{p}_{\mathsf{v}_\mathfrak{p}} = \{x \in K \mid \mathsf{v}_\mathfrak{p}(x) > 0\} = \mathfrak{p}R_\mathfrak{p}$.

Next we prove that $K_\mathfrak{p}$ and $\widehat{\mathsf{v}}_\mathfrak{p}$ do not depend on ρ. Indeed, suppose that $0 < \rho_1 < \rho_2 < 1$. By Theorem `equivalent` 4.1.6 it follows that

$$|\cdot|_{\mathfrak{p},\rho_2} = |\cdot|_{\mathfrak{p},\rho_1}^s\,, \quad \text{where} \quad s = \frac{\log\rho_2}{\log\rho_1} \in (0,1)\,.$$

If $(K_\mathfrak{p}, |\cdot|'_{\mathfrak{p},\rho_1})$ is a completion of $(K, |\cdot|_{\mathfrak{p},\rho_1})$, then Theorem `completion` 4.2.3.5 implies that $(K_\mathfrak{p}, |\cdot|'^s_{\mathfrak{p},\rho_1})$ is a completion of $(K, |\cdot|_{\mathfrak{p},\rho_2})$. Since $|\cdot|'_{\mathfrak{p},\rho_1} \sim |\cdot|'^s_{\mathfrak{p},\rho_1}$, these two absolute values induce the same valuation. Hence $K_\mathfrak{p}$ and $\widehat{\mathsf{v}}_\mathfrak{p}$ do not depend on ρ, $\widehat{\mathsf{v}}_\mathfrak{p} = \mathsf{v}_{\widehat{\mathfrak{p}}}$ by Theorem `discrete1` 4.3.1, and $\widehat{\mathsf{v}}_\mathfrak{p} \,|\, K = \mathsf{v}_\mathfrak{p}$ by Theorem `discrete4` 4.3.4.

If $k \in \mathbb{Z}$, then Theorem `discrete4` 4.3.4 implies $\mathfrak{p}^k R_\mathfrak{p} = \widehat{\mathfrak{p}}^k \cap K$ and $\widehat{\mathfrak{p}}^k = \mathfrak{p}^k_{\widehat{\mathsf{v}}_\mathfrak{p}} = \overline{\mathfrak{p}^k_{\widehat{\mathsf{v}}_\mathfrak{p}}} = \overline{\mathfrak{p}^k R_\mathfrak{p}} \supset \overline{\mathfrak{p}^k}$. It remains to prove that $\mathfrak{p}^k R_\mathfrak{p} \subset \overline{\mathfrak{p}^k} \subset K_\mathfrak{p}$. Thus let $z = s^{-1}x \in \mathfrak{p}^k R_\mathfrak{p}$, where $x \in \mathfrak{p}^k$ and $s \in R \setminus \mathfrak{p}$. If $n \in \mathbb{N}$, then $\mathfrak{p}^n + sR = R$, and thus there exist $u_n \in \mathfrak{p}^n$ and $t_n \in R$ such that $1 = u_n + st_n$. Since $\widehat{\mathsf{v}}_\mathfrak{p}(z - xt_n) = \widehat{\mathsf{v}}_\mathfrak{p}(z(1 - st_n)) = \widehat{\mathsf{v}}_\mathfrak{p}(z) + \widehat{\mathsf{v}}_\mathfrak{p}(u_n) \ge k + n$, it follows that $(xt_n)_{n\ge1} \to z$ in $K_\mathfrak{p}$, and since $xt_n \in \mathfrak{p}^k$ for all $n \ge 1$, we obtain $z \in \overline{\mathfrak{p}^k}$. For $k = 0$, we obtain $\overline{R} = \widehat{R}_\mathfrak{p}$.

If $k \in \mathbb{N}$, then $\widehat{\mathfrak{p}}^k \cap R_\mathfrak{p} = \mathfrak{p}^k R_\mathfrak{p}$ by Theorem `discrete4` 4.3.4, and thus $\widehat{\mathfrak{p}}^k \cap R = \mathfrak{p}^k R_\mathfrak{p} \cap R = \mathfrak{p}^k$ by Theorem `localizationisok` 2.6.4. By the same Theorems, the inclusion maps $R \hookrightarrow R_\mathfrak{p} \hookrightarrow \widehat{R}_\mathfrak{p}$ induce isomorphisms $R/\mathfrak{p} \xrightarrow{\sim} R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \xrightarrow{\sim} \widehat{R}_\mathfrak{p}/\mathfrak{p}$. □

Definition and Remarks 4.3.6. Let $p \in \mathbb{P}$ be a prime. The completion $(\mathbb{Q}_p, |\cdot|_p)$ of $(\mathbb{Q}, |\cdot|_p)$ is called the *p-adic number field*. Its valuation domain $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \mathsf{v}_p(x) \ge 0\}$ is called the *domain of p-adic integers*.

$\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Z}_p$ are dense subrings, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = Z_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{Z}_p/p\mathbb{Z}_p$ according to Theorem and Definition `dedekindvalue` 4.3.5. Hence $[0, p-1]$ is a system of representatives of $\mathbb{F}_p = \mathsf{k}_{v_p}$ in $\mathbb{Z}_p$. In particular, $\mathbb{Z}_p$ is compact, and every $x \in \mathbb{Z}_p$ has a unique representation

$$x = \sum_{n=0}^{\infty} a_n p^n\,, \quad \text{where} \quad a_n \in [0, p-1] \ \text{ for all } \ n \ge 0\,.$$

`hensel` **Theorem 4.3.7** (Hensel's Lemma). *Let* $(K, |\cdot|)$ *be a complete discrete valued field. Let* $v\colon K \to \mathbb{Z} \cup \{\infty\}$ *the associated valuation,*

$$\mathcal{O}_v[X] \to \mathsf{k}_v[X]\,, \quad h \mapsto \overline{h} = h + \mathfrak{p}_v[X]$$

the natural residue class map and $f \in \mathcal{O}_v[X]$.

1. *Assume that* $\overline{f} = \varphi\psi \neq 0$, *where* $\varphi,\, \psi \in \mathsf{k}_v[X]$ *and* $(\varphi, \psi) = 1$. *Then there exist* $g,\, h \in \mathcal{O}_v[X]$ *such that* $f = gh$, $\overline{g} = \varphi$, $\overline{h} = \psi$, $\deg(g) = \deg(\varphi)$, *and if* φ *is monic, then* g *is also monic.*
2. *Let* $\alpha \in \mathsf{k}_v$ *be such that* $\overline{f}(\alpha) = 0$ *and* $\overline{f}'(\alpha) \neq 0$. *Then there exists some* $a \in \mathcal{O}_v$ *such that* $f(a) = 0$ *and* $\overline{a} = \alpha$.
3. *Let* f *be monic and* $\overline{f} = \varphi_1 \cdot \ldots \cdot \varphi_r$, *where* $r \in \mathbb{N}$, $\varphi_1, \ldots, \varphi_r \in \mathsf{k}_v[X]$ *are monic, and* $(\varphi_i,\, \varphi_j) = 1$ *for all* $i,\, j \in [1, r]$ *such that* $i \neq j$. *Then there exist monic polynomials* $g_1, \ldots, g_r \in \mathcal{O}_v[X]$ *such that* $f = g_1 \cdot \ldots \cdot g_r$, *and* $\overline{g}_i = \varphi_i$ *for all* $i \in [1, r]$.

PROOF. 1. Let $\pi \in K$ be a uniformizing parameter, $m = \deg(\varphi)$, $n = \deg(\psi)$ and $d = \deg(f)$. Then $m,\, n \in \mathbb{N}_0$, and $d \geq m + n$. We construct recursively sequences $(g_k)_{k \geq 0}$ and $(h_k)_{k \geq 0}$ in $\mathcal{O}_v[X]$ having the following properties for all $k \geq 0$:

1) $\deg(g_k) = m$, $\deg(h_k) \leq d - m$, $\overline{g}_k = \varphi$, $\overline{h}_k = \psi$, and if φ is monic, then g_k is monic.

2) $f - g_k h_k \in \pi^{k+1}\mathcal{O}_v[X]$.

3) If $k \geq 1$, then $\{g_k - g_{k-1},\, h_k - h_{k-1}\} \subset \pi^k \mathcal{O}_v[X]$.

Let $g_0,\, h_0 \in \mathcal{O}_v[X]$ be such that $\deg(g_0) = m$, $\deg(h_0) = n$, $\overline{g}_0 = \varphi$, $\overline{h}_0 = \psi$, and g_0 is monic if φ is monic. Then $\overline{f - g_0 h_0} = \overline{f} - \varphi\psi = 0$, and thus $f - g_0 h_0 \in \pi\mathcal{O}_v[X]$.

Suppose now that $k \geq 0$, and there exist $g_0,\, h_0, \ldots, g_k,\, h_k \in \mathcal{O}_v[X]$ such that **1)**, **2)** and **3)** hold, and set $P = \pi^{-k-1}(f - g_k h_k) \in \mathcal{O}_v[X]$. We shall prove:

$(*)$ There exist $\alpha,\, \beta \in \mathsf{k}_v[X]$ such that $\alpha\varphi + \beta\psi = \overline{P}$, $\deg(\alpha) \leq d - m$ and $\deg(\beta) < m$.

Proof of $(*)$. Since $(\varphi, \psi) = 1$, there exist $\alpha',\, \beta' \in \mathsf{k}_v[X]$ such that $\alpha'\varphi + \beta'\psi = \overline{P}$. By division with remainder, we find some $\rho \in \mathsf{k}_v[X]$ such that $\deg(\beta' - \rho\varphi) < m = \deg(\varphi)$, and if $\alpha = \alpha' + \rho\psi$ and $\beta = \beta' - \rho\varphi$, then $\alpha\varphi + \beta\psi = \overline{P}$, $\deg(\beta) < m$,

$$\begin{aligned} \deg(\alpha) + m = \deg(\alpha\varphi) &= \deg(\overline{P} - \beta\psi) \leq \max\{\deg(\overline{P}),\, \deg(\beta) + \deg(\psi)\} \\ &\leq \max\{\deg(f),\, \deg(g_k) + \deg(h_k),\, \deg(\beta) + \deg(\psi)\} \\ &\leq \max\{d,\, m + (d - m),\, m - 1 + n\} = d\,, \quad \text{and therefore} \quad \deg(\alpha) \leq d - m\,. \quad \square(*) \end{aligned}$$

Let $A,\, B \in \mathcal{O}_v[X]$ be such that $\overline{A} = \alpha$, $\overline{B} = \beta$, $\deg(A) = \deg(\alpha)$ and $\deg(B) = \deg(\beta)$, and define

$$g_{k+1} = g_k + \pi^{k+1}B\,, \quad h_{k+1} = h_k + \pi^{k+1}A \in \mathcal{O}_v[X]\,.$$

Then $\overline{g}_{k+1} = \overline{g}_k = \varphi$, $\overline{h}_{k+1} = \overline{h}_k = \psi$, $\deg(h_{k+1}) \leq \max\{\deg(h_k),\, \deg(A)\} \leq d - m$, and since $\deg(B) < m = \deg(g_k)$, it follows that $\deg(g_{k+1}) = m$, and if φ is monic, then g_k and thus also g_{k+1} is monic. By definition, $g_{k+1} - g_k \in \pi^{k+1}\mathcal{O}_v$, $h_{k+1} - h_k \in \pi^{k+1}\mathcal{O}_v$, and

$$f - g_{k+1}h_{k+1} = f - g_k h_k - \pi^{k+1}(Ag_k + Bh_k + \pi^{k+1}AB) = \pi^{k+1}(P - Ag_k - Bh_k - \pi^{k+1}AB)\,.$$

Since $\overline{P - Ag_k - Bh_k - \pi^{k+1}AB} = \overline{P} - \alpha\varphi - \beta\psi = 0$, it follows that $f - g_{k+1}h_{k+1} \in \pi^{k+2}\mathcal{O}_v[X]$. Hence the sequences $(g_k)_{k \geq 0}$ and $(h_k)_{k \geq 0}$ are constructed.

For $k \geq 0$, we set

$$g_k = \sum_{i=0}^{m} a_{k,i}X^i \quad \text{and} \quad h_k = \sum_{i=0}^{d-m} b_{k,i}X^i\,.$$

By construction, we obtain $a_{k,i}-a_{k-1,i}\in\pi^k\mathcal{O}_v$ and thus $v(a_{k,i}-a_{k-1,i})\geq k$ for all $k\geq 1$ and $i\in[0,m]$; and $b_{k,i}-b_{k-1,i}\in\pi^k\mathcal{O}_v$ and thus $v(b_{k,i}-b_{k-1,i})\geq k$ for all $k\geq 1$ and $i\in[0,d-m]$. Hence the sequences $(a_{k,i})_{k\geq 0}$ and $(b_{k,i})_{k\geq 0}$ are Cauchy sequences in $\mathcal{O}_v$ and thus convergent in $\mathcal{O}_v$, since $(K,|\cdot|)$ is complete and $\mathcal{O}_v\subset K$ is closed. We set

$$a_i=\lim_{k\to\infty}a_{k,i}\quad\text{for all}\quad i\in[0,m],\quad\text{and}\quad b_i=\lim_{k\to\infty}b_{k,i}\quad\text{for all}\quad i\in[0,d-m],$$

$$g=\sum_{i=0}^{m}a_iX^i\quad\text{and}\quad h=\sum_{i=0}^{d-m}b_iX^i\in\mathcal{O}_v[X]\,.$$

By Theorem discrete2 4.3.2, we obtain $v(a_i-a_{k,i})\geq\inf\{v(a_{j+1,i}-a_{j,i}\mid j\geq k\}\geq k+1$ for all $k\geq 0$ and $i\in[0,m]$; and $v(b_i-b_{k,i})\geq\inf\{v(b_{j+1,i}-b_{j,i}\mid j\geq k\}\geq k+1$ for all $k\geq 0$ and $i\in[0,d-m]$. Therefore it follows that $g-g_k\in\pi^{k+1}\mathcal{O}_v[X]$ and $h-h_k\in\pi^{k+1}\mathcal{O}_v[X]$.

For all $k\geq 0$, $\overline{a}_{k,m}$ is the leading coefficient of $\overline{g}_k=\varphi$, hence $\overline{a}_{k,m}\neq 0$, $a_{k,m}\in\mathcal{O}_v^\times$, and since $\mathcal{O}_v^\times\subset K$ is closed, we obtain $a_m\in\mathcal{O}_v^\times$, and thus $\deg(g)=m=\deg(\varphi)$. If φ is monic, then $a_{k,m}=1$ for all $k\geq 0$, hence $a_m=1$ and g is monic. Finally, we obtain

$$f-gh=(f-g_kh_k)-g_k(h-h_k)-h(g-g_k)\in\pi^{k+1}\mathcal{O}_v[X]\quad\text{for all}\quad k\geq 0\,,$$

and therefore $f=gh$.

2. By assumption, α is a simple zero of $\overline{f}$. Hence $\overline{f}=(X-\alpha)\psi$, where $\psi\in\mathsf{k}_v[X]$ and $\psi(\alpha)\neq 0$. Hence $(X-\alpha,\psi)=1$, and by 1., applied with $\varphi=X-\alpha$, there exist some $a\in\mathcal{O}_v$ and $h\in\mathcal{O}_v[X]$ such that $\overline{a}=\alpha$, $\overline{h}=\psi$ and $f=(X-a)h$. In particular, $f(a)=0$.

3. By induction on r. For $r=1$, there is nothing to do.

$r\geq 2$, $r-1\to r$: Since $(\varphi_1\cdot\ldots\cdot\varphi_{r-1},\varphi_r)=1$, by 1., there exist $g,\,g_r\in\mathcal{O}_v[X]$ such that $f=gg_r$, $\overline{g}=\varphi_1\cdot\ldots\cdot\varphi_{r-1}$, $\overline{g}_r=\varphi_r$, and g_r is monic. Hence g is monic, and by the induction hypothesis, there exist monic polynomials $g_1,\ldots,g_{r-1}\in\mathcal{O}_v[X]$ such that $g=g_1\cdot\ldots\cdot g_{r-1}$ and $\overline{g}_i=\varphi_i$ for all $i\in[1,r-1]$. □

Theorem 4.3.8. *Let $(K,|\cdot|)$ be a complete discrete valued field, $v\colon K\to\mathbb{Z}\cup\{\infty\}$ the associated valuation and $|\mathsf{k}_v|=q<\infty$. Then $|\mu_{q-1}(\mathcal{O}_v)|=q-1$.*

Proof. Let $\mathcal{O}_v[X]\to\mathsf{k}_v[X]$, $h\mapsto\overline{h}$ be the residue class map. Then

$$\overline{X^{q-1}-1}=\prod_{\alpha\in\mathsf{k}_v^\times}(X-\alpha)\in\mathsf{k}_v[X]\,,$$

and by Theorem hensel 4.3.7.3, the polynomial $X^{q-1}-1$ splits into distinct linear factors in $\mathcal{O}_v[X]$. Hence $|\mu_{q-1}(\mathcal{O}_v)|=q-1$. □

educibility **Theorem 4.3.9.** *Let $(K,|\cdot|)$ be a complete discrete valued field and $f\in K[X]$ irreducible. If $n\in\mathbb{N}$ and $f=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0$, then $\max\{|a_i|\mid i\in[0,n]\}=\max\{|a_0|,\,|a_n|\}$. In particular, if f is monic and $\mathcal{O}$ is the valuation domain of $(K,|\cdot|)$, then $a_0\in\mathcal{O}$ implies $f\in\mathcal{O}[X]$.*

Proof. Let $r\in[0,n]$ be minimal such that $|a_r|=\min\{|a_0|,\ldots,|a_n|\}$, and assume that, contrary to our assertion, $\max\{|a_0|,\,|a_n|\}<|a_r|$. Then $a_r^{-1}f=b_nX^n+\ldots+b_1X+b_0\in\mathcal{O}_v[X]$ is irreducible, $|b_j|<1$ for all $j\in[0,r-1]$, $|b_r|=1$, $0<r<n$, and the residue class

polynomial $\overline{a_r^{-1}f} \in \mathsf{k}_v[X]$ splits in the form $\overline{a_r^{-1}f} = X^r\psi$, where $\psi \in \mathsf{k}_v[X]$, $\deg(\psi) = n-r$ and $\psi(0) = \overline{b}_r \neq 0$. By Theorem $\overset{\texttt{hensel}}{\overline{4.3.7}}$, applied with $\varphi = X^r$, it follows that $a_r^{-1}f$ is reducible. □

Without proof, we state the following refinement of Hensel's Lemma.

`henselore` **Theorem 4.3.10** (Lemma of Hensel-Ore)**.** *Let* $(K, |\cdot|)$ *be a complete discrete valued field,* $v\colon K \to \mathbb{Z} \cup \{\infty\}$ *the associated valuation and* $\pi \in K$ *a uniformizing parameter.*

Let $f,\, G,\, H \in \mathcal{O}_v[X]$ *be monic and* $f - GH \in \pi^{v(\Delta(f))+1}\mathcal{O}_v[X]$. *Then there exist monic polynomials* $g,\, h \in \mathcal{O}_v[X]$ *such that* $f = gh$, $g - G \in \pi^\theta \mathcal{O}_v[X]$ *and* $h - H \in \pi^\theta\mathcal{O}_v[X]$, *where* $\theta = \max\{v(\Delta(g)),\, v(\Delta(h))\} + 1$.

Theorem 4.3.11 (Squares in $\mathbb{Q}_p$)**.**

1. *Let* $p \in \mathbb{P} \setminus \{2\}$ *be an odd prime, and* $a = p^k u \in \mathbb{Q}_p^\times$, *where* $k = \mathsf{v}_p(a) \in \mathbb{Z}$ *and* $u \in \mathbb{Z}_p^\times$. *Then* $a \in \mathbb{Q}_p^{\times 2}$ *if and only if* $k \equiv 0 \bmod 2$ *and* $\overline{u} = u + p\mathbb{Z} \in \mathbb{F}_p^{\times 2}$. *In particular:*
   - *There is an isomorphism* $\vartheta\colon \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \overset{\sim}{\to} \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \cong \mathsf{C}_2^2$ *such that, for* $a \in \mathbb{Q}_p^\times$ *as above,* $\vartheta(a\mathbb{Q}_p^{\times 2}) = (a + 2\mathbb{Z},\, \overline{u}\mathbb{F}_p^{\times 2})$.
   - *If* $a \in \mathbb{Z} \setminus p\mathbb{Z}$, *then* $a \in \mathbb{Q}_p^{\times 2}$ *if and only if* a *is a quadratic residue modulo* p.
2. *Let* $a = 2^k u \in \mathbb{Q}_2^\times$, *where* $k = \mathsf{v}_2(a) \in \mathbb{Z}$ *and* $u \in \mathbb{Z}_2^\times$. *Then* $a \in \mathbb{Q}_2^{\times 2}$ *if and only if* $k \equiv 0 \bmod 2$ *and* $u \equiv 1 \bmod 8\mathbb{Z}_2$. *In particular:*
   - *There is an isomorphism* $\vartheta\colon \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \overset{\sim}{\to} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathsf{C}_2^3$ *such that, for* $a \in \mathbb{Q}_p^\times$ *as above,* $\vartheta(a\mathbb{Q}_p^{\times 2}) = (a + 2\mathbb{Z},\, u + 8\mathbb{Z}_2)$.
   - *If* $a \in \mathbb{Z} \setminus 2\mathbb{Z}$, *then* $a \in \mathbb{Q}_2^{\times 2}$ *if and only if* $a \equiv 1 \bmod 8$.

Proof. 1. If $a = p^k u \in \mathbb{Q}_p^{\times 2}$, then obviously $k \equiv 0 \bmod 2$ and $\overline{u} \in \mathbb{F}_p^{\times 2}$. For the converse, it suffices to prove that $\overline{u} \in \mathbb{F}_p^{\times 2}$ implies $u \in \mathbb{Z}_p^2$. Thus assume that $\overline{u} = \xi^2$ for some $\xi \in \mathbb{F}_p$. Then ξ is a simple zero of the residue class polynomial $\overline{X^2 - u}$, and by Theorem $\overset{\texttt{hensel}}{\overline{4.3.7}}$, there exists some $x \in \mathbb{Z}_2$ such that $x^2 = u$ and $\overline{x} = \xi$. Note that this argument fails for $p = 2$, since $\overline{X^2 - u} \in \mathbb{F}_2[X]$ is not separable.

Let $\vartheta_0\colon \mathbb{Q}_p^\times \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ be defined by $\vartheta_0(p^k u) = (k + 2\mathbb{Z},\, \overline{u}F_p^{\times 2})$ for $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Then ϑ_0 is an epimorphism, and, as we have just proved, $\operatorname{Ker}(\vartheta_0) = \mathbb{Q}_p^{\times 2}$, and therefore ϑ_0 induces an isomorphism $\vartheta\colon \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \overset{\sim}{\to} \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ as asserted. Since $\mathbb{F}_p^\times$ is cyclic of order $p-1$, it follows that $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \cong \mathsf{C}_2$.

If $a \in \mathbb{Z} \setminus p\mathbb{Z} \subset \mathbb{Z}_p^\times$, then $a + p\mathbb{Z} \in \mathbb{F}_p^{\times 2}$ if and only if a is a quadratic residue modulo p.

2. We might use the Lemma of Hensel-Ore. but we give a direct proof. If $a = 2^k u \in \mathbb{Q}_2^{\times 2}$, then obviously $k \equiv 0 \bmod 2$ and $u \equiv 1 \bmod 8\mathbb{Z}_2$, since $(\mathbb{Z}_2/8\mathbb{Z}_2)^\times = (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathsf{C}_2^2$. For the converse, it suffices to prove that $u \equiv 1 \bmod 8\mathbb{Z}_2$ implies $u \in \mathbb{Z}_2^2$.

Thus let $u \in 1 + 8\mathbb{Z}_2$, and construct recursively a sequence $(x_n)_{n\geq 0}$ in $\mathbb{Z}_2$, such that

$$x_{n+1} - x_n \in 2^{n+2}\mathbb{Z}_2 \quad \text{and} \quad x_n^2 - u \in 2^{n+3}\mathbb{Z}_2 \quad \text{for all } n \geq 0.$$

We set $x_0 = 1$. Suppose that $n \geq 0$ and let $x_n \in \mathbb{Z}_2$ be such that $x_n^2 = u + 2^{n+3}z$ for some $z \in \mathbb{Z}_2$. We set $x_{n+1} = x_n + 2^{n+2}z$ and obtain $x_{n+1}^2 = u + 2^{n+3}(1 + x_n)z + 2^{2n+4}z^2 \in u + 2^{n+4}\mathbb{Z}_2$, since $1 + x_n \in 2\mathbb{Z}_2$. The sequence $(x_n)_{n\geq 0}$ is a Cauchy sequence in $\mathbb{Z}_2$, and if $(x_n)_{n\geq 2} \to x \in \mathbb{Z}_2$, then $x^2 = u$.

Let $\vartheta_0\colon \mathbb{Q}_2^\times \to \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}_2/8\mathbb{Z}_2)^\times$ be defined by $\vartheta_0(2^k u) = (k + 2\mathbb{Z},\, u + 8\mathbb{Z}_2)$ for $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Then ϑ_0 is an epimorphism, and, as we have just proved, $\operatorname{Ker}(\vartheta_0) = \mathbb{Q}_2^{\times 2}$, and therefore ϑ_0 induces an isomorphism $\vartheta\colon \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}\times(\mathbb{Z}/8\mathbb{Z})^\times$ as asserted (note that $(\mathbb{Z}_2/8\mathbb{Z}_2)^\times = (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathsf{C}_2^2$). $\square$

4.4. Extension of absolute values (complete case)

`eextension`

Theorem 4.4.1. *Let $(K, |\cdot|)$ be a complete valued field.*

1. *Let L/K be a finite extension and $n = [L:K]$. Then there is a unique absolute value $|\cdot|_L$ of L such that $|\cdot|_L \restriction K = |\cdot|$.*
   - (a) *$(L, |\cdot|_L)$ is complete, and $|x| = \sqrt[n]{|\mathsf{N}_{L/K}(x)|}$ for all $x \in L$.*
   - (b) *Let $(K, |\cdot|)$ be discrete. Then $(L, |\cdot|_L)$ is also discrete. If $\mathcal{O}$ is the valuation domain of K, then $\mathrm{cl}_L(\mathcal{O}_K)$ is the valuation domain of L, and every finitely generated $\mathcal{O}_K$-submodule $M \subset L$ is closed.*
2. *Let $\overline{K}$ be an algebraic closure of K. Then $|\cdot|$ has a unique extension to an absolute value of $\overline{K}$.*

PROOF. CASE 1: $(K, |\cdot|)$ is archimedean.

By Theorem `ostrowski` 4.2.7 we may assume that $(K, |\cdot|) = (\mathbb{R}, |\cdot|_\infty^s)$ or $(K, |\cdot|) = (\mathbb{C}, |\cdot|_\infty^s)$ for some $s \in (0, 1]$. If $K = \mathbb{C}$, there is nothing to do. If $K = \mathbb{R}$, then $\overline{K} = \mathbb{C}$, and if $z \in \mathbb{C}$, then $|z| = |z|_\infty^s = \sqrt{|z\overline{z}|_\infty^s} = \sqrt{|\mathsf{N}_{\mathbb{C}/\mathbb{R}}(z)|_\infty^s}$.

CASE 2: $(K, |\cdot|)$ is non-archimedean. We prove the Theorem only if $(K, |\cdot|)$ is discrete.

1. Let $\mathcal{O}$ be the valuation domain of $(K, |\cdot|)$, L/K a finite extension and $[L:K] = n$. We define $|\cdot|_L\colon L \to \mathbb{R}_{\ge 0}$ by

$$|x|_L = \sqrt[n]{|\mathsf{N}_{L/K}(x)|} \quad \text{for all} \quad x \in L\,.$$

Then $|\cdot|_L \restriction K = |\cdot|$, $|x|_L = 0$ if and only if $x = 0$, $|xy|_L = |x|_L|y|_L$ for all $x, y \in L$, and $|L^\times|_L \subset \sqrt[n]{|K^\times|} \subset \mathbb{R}$ is discrete.

Next we prove that $|x|_L \le 1$ implies $|1 + x|_L \le 1$ and $x \in \mathrm{cl}(\mathcal{O})$ for all $x \in L$. Thus let $x \in L$, $f = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in K[X]$ the minimal polynomial of x over K and $d = [L:K(x)]$. Then $|x|_L = \sqrt[n]{|\mathsf{N}_{L/K}(x)|} = \sqrt[n]{|a_0|^d}$, and if $|x|_L \le 1$, then $|a_0| \le 1$, and as f is irreducible, it follows that $f \in \mathcal{O}[X]$ by Theorem `henselirreducibility` 4.3.9. Hence $x \in \mathrm{cl}_L(\mathcal{O})$, and since $f(X-1) \in \mathcal{O}[X]$ is the minimal polynomial of $x+1$ over K, we obtain

$$|x+1|_L = \sqrt[n]{|\mathsf{N}_{L/K}(x+1)|} = \sqrt[n]{|f(-1)|^d} \le 1\,.$$

Hence $|\cdot|_L$ is a discrete absolute value of L by Theorem `nichtarch` 4.1.4, and if $\mathcal{O}'$ denotes the valuation domain of L, then $\mathcal{O}' \subset \mathrm{cl}(\mathcal{O})$. Since $\mathcal{O}'$ is integrally closed, it follows that $\mathcal{O}' = \mathrm{cl}(\mathcal{O})$. By Theorem `fortsetzungeindeutig` 4.2.6, $||_L$ is the unique extension of $|\cdot|$ to L, and $(L, |\cdot|_L)$ is complete.

Let now $M \subset L$ be a finitely generated $\mathcal{O}$-submodule. Since $\mathcal{O}$ is a principal ideal domain and M is torsion-free, it follows that M is free. Let $(u_1, \ldots, u_m)$ be an $\mathcal{O}$-basis of M, and

$V = KM \subset L$. Then $|\cdot|_L \restriction V \colon V \to \mathbb{R}_{\ge 0}$ is a $|\cdot|$-compatible norm on V. If V carries the $|\cdot|_L$-topology and K^m carries the product topology, then the map

$$\Phi\colon K^m \to V\,, \quad \text{defined by} \quad \Phi(a_1,\ldots,a_m) = \sum_{j=1}^{m} a_j u_j\,,$$

is a topological isomorphism, and as $\mathcal{O} \subset K$ is closed, it follows that $M = \Phi(\mathcal{O}^m) \subset L$ is closed.

2. Let $K \subset L \subset L' \subset \overline{K}$ be intermediate fields such that $[L'\colon K] < \infty$. By Theorem `fortsetzungeindeutig` 4.2.6 it follows that $|\cdot|_{L'} \restriction L = |\cdot|_L$, and therefore there exists a unique function $|\cdot|'\colon \overline{K} \to \mathbb{R}_{\ge 0}$ such that $|\cdot|' \restriction L = |\cdot|_L$ for all intermediate fields L such that $[L:K] < \infty$. If $x,\,y \in \overline{K}$ and $L = K(x,y)$, then $[L:K] < \infty$. Hence we obtain $|x|' = |x|_L = 0$ if and only if $x = 0$, $|xy|' = |xy|_L = |x|_L|y|_L = |x|'|y|'$ and $|x+y| = |x+y|_L \le \max\{|x|_L, |y|_L\} = \max\{|x|', |y|'\}$. Therefore $|\cdot|'$ is an absolute value of $\overline{K}$ such that $|\cdot|' \restriction K = |\cdot|$, and uniqueness follows by Theorem `fortsetzungeindeutig` 4.2.6. □

`localfield` **Definition 4.4.2.** For a discrete valued complete field $K = (K, |\cdot|)$ we denote by

- $v_K\colon K \to \mathbb{Z} \cup \infty$ the associated valuation;
- $\mathcal{O}_K = \mathcal{O}_{v_K}$ the valuation domain;
- $\mathfrak{p}_K = \mathfrak{p}_{v_K}$ the valuation ideal;
- $\mathsf{k}_K = \mathsf{k}_{v_K} = \mathcal{O}_K/\mathfrak{p}_K$ the residue class field.

For a finite extension L/K we denote by $|\cdot|\colon L \to \mathbb{R}_{\ge 0}$ the extension of $|\cdot|$ to L, we refer to L/K as a *finite extension of complete discrete valued fields* with absolute value $|\cdot|$ and we denote by

$$\mathcal{O}_L[X] \;\to\; \mathsf{k}_L\,,\; h \to \overline{h}$$

the residue class map.

`extensions` **Theorem and Definition 4.4.3.** *Let L/K a finite extension of discrete valued fields with absolute value $|\cdot|$ and $[L\colon K] = n$.*

1. $\mathcal{O}_L = \mathrm{cl}_L(\mathcal{O}_K)$ *and* $\mathfrak{p}_L \cap K = \mathfrak{p}_L \cap \mathcal{O}_K = \mathfrak{p}_K$*,*

   We call $e(L/K) = e(\mathfrak{p}_L/\mathfrak{p}_K)$ the *ramification index* and $f(L/K) = f(\mathfrak{p}_L/\mathfrak{p}_K)$ the *residue class degree* of L/K. By definition,

   $$\mathfrak{p}_K\mathcal{O}_L = \mathfrak{p}_L^{e(L/K)} \quad \text{and} \quad f(L/K) = [\mathsf{k}_L \colon \mathsf{k}_K]\,.$$

   The extension L/K is called

   - *unramified* if $e(L/K) = 1$ and $\mathsf{k}_L/\mathsf{k}_K$ is separable, and *ramified* otherwise;
   - *tamely ramified* if $\mathrm{char}(\mathsf{k}_K) \nmid e(L/K)$ and $\mathsf{k}_L/\mathsf{k}_K$ is separable, and *wildly ramified* otherwise;
   - *fully ramified* if $e(L/K) = n$.

   By definition, L/K is unramified [ramified, tamely ramified, wildly ramified] if and only if $\mathfrak{p}_L/\mathfrak{p}_K$ has this property (see Definition `decompositionbehavior` 2.4.13).

2. *Let $e = e(L/K)$ and $f = f(L/K)$.*

   (a) *$ef \le n$, and equality holds if and only if $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module. In particular, if L/K is separable, then $ef = n$.*

(b) $(|L^\times|:|K^\times|) = e$, $v_L\,|\,K = ev_K$, $e\,|\,n$, *and* $v_K\circ\mathsf{N}_{L/K} = \frac{n}{e}v_L$. *In particular, we have the commutative diagrams*

$$\begin{tikzcd} L^\times \arrow[r, "v_L"] & \mathbb{Z} \\ K^\times \arrow[u, "\mathrm{incl}"] \arrow[r, "v_K"] & \mathbb{Z} \arrow[u, "\cdot e"'] \end{tikzcd} \quad \textit{and} \quad \begin{tikzcd} L^\times \arrow[r, "v_L"] \arrow[d, "\mathsf{N}_{L/K}"'] & \mathbb{Z} \arrow[d, "\cdot\frac{n}{e}"] \\ K^\times \arrow[r, "v_K"] & \mathbb{Z} \end{tikzcd} .$$

Proof. 1. By Theorem $\overset{\texttt{completeextension}}{4.4.1}$, $\mathcal{O}_L = \mathrm{cl}_L(\mathcal{O}_K)$, and since $\mathcal{P}(\mathcal{O}_L) = \{\mathfrak{p}_L\}$ and $\mathcal{P}(\mathcal{O}_K) = \{\mathfrak{p}_K\}$, it follows tha $\mathfrak{p}_L\cap K = \mathfrak{p}_L\cap\mathcal{O}_L\cap K = \mathfrak{p}_L\cap\mathcal{O}_K = \mathfrak{p}_K$.

2. (a) By Theorem $\overset{\texttt{dedekindextension1}}{2.7.1}$ it follows that $ef\le n$, and equality holds if and only if $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module.

(b) Let π_K be a uniformizing parameter of K and π_L a uniformizing parameter of L. Then $\mathfrak{p}_K = \pi_K\mathcal{O}_K$, $\mathfrak{p}_L = \pi_L\mathcal{O}_L$, and since $\pi_K\mathcal{O}_L = \pi_L^e\mathcal{O}_L$, it follows that $\pi_K = \pi_L^e u$ for some $u\in\mathcal{O}_L^\times$, and $|\pi_K| = |\pi_L|^e$. Hence $(|L^\times|:|K^\times|) = (\langle|\pi_L|\rangle:\langle|\pi_L|^e\rangle) = e$, and $v_L(\pi_K) = e$.

If $a\in K^\times$, then $a = \pi_K^{v_K(a)}\varepsilon$, where $\varepsilon\in\mathcal{O}_K^\times\subset\mathcal{O}_L^\times$, and thus $v_L(a) = v_K(a)v_L(\pi_K) = ev_K(a)$. Hence $v_L\,|\,K = e\,v_K$. Since $\pi_K^n = \mathsf{N}_{L/K}(\pi_K) = \mathsf{N}_{L/K}(\pi_L)^e\mathsf{N}_{L/K}(u)$ and $\mathsf{N}_{L/K}(u)\in\mathcal{O}_K^\times$, it follows that $n = v_K(\pi_K^n) = e\,v_K(\mathsf{N}_{L/K}(\pi_L))$, and therefore $e\,|\,n$. If $x\in L^\times$, then $x = \pi_L^{v_L(x)}w$ for some $w\in\mathcal{O}_L^\times$, hence $\mathsf{N}_{L/K}(x) = \mathsf{N}_{L/K}(\pi_L)^{v_L(x)}\mathsf{N}_{L/K}(w)$, and since $\mathsf{N}_{L/K}(w)\in\mathcal{O}_K^\times$, we obtain

$$v_K(\mathsf{N}_{L/K}(x)) = v_L(x)v_K(\mathsf{N}_{L/K}(\pi_L)) = \frac{n}{e}v_L(x)\,, \quad \text{and therefore} \quad v_K\circ\mathsf{N}_{L/K} = \frac{n}{e}\,v_L\,. \qquad \square$$

extensions1

Theorem 4.4.4. *Let L/K a finite extension of discrete valued fields.*

1. *Let $b,\,\pi\in\mathcal{O}_L$ be such that $\mathsf{k}_L = \mathsf{k}_K(\overline{b}\,)$ and $v_L(\pi) = 1$. Then $\mathcal{O}_L = \mathcal{O}_K[b,\pi]$.*
2. *If $\mathsf{k}_L/\mathsf{k}_K$ is separable, then there exists some $x\in\mathcal{O}_L$ such then $\mathcal{O}_L = \mathcal{O}_K[x]$.*

Proof. 1. Let $f = [\mathsf{k}_L:\mathsf{k}_K]$. Then

$$\mathsf{k}_L = \sum_{i=0}^{f-1}\mathsf{k}_K\overline{b}^{\,i}\,, \quad \text{and we set} \quad M = \sum_{i=0}^{f-1}\mathcal{O}_K b^i\,.$$

Then M contains a set of representatives of k_L in $\mathcal{O}_L$, and therefore every $x\in\mathcal{O}_L$ has a representation

$$x = \sum_{n=0}^{\infty}\Bigl(\sum_{i=0}^{f-1}c_{n,i}b^i\Bigr)\pi^n\,, \quad \text{where} \quad c_{n,i}\in\mathcal{O}_K \ \text{ for all } n\ge 0 \text{ and } i\in[0,f-1].$$

In particular, it follows that $\mathcal{O}_K[b,\pi]\subset\mathcal{O}_L$ is dense. Since b and π are integral over $\mathcal{O}_K$, $\mathcal{O}_K[b,\pi]$ is a finitely generated $\mathcal{O}_K$-module, hence closed in L, and therefore $\mathcal{O}_K[b,\pi] = \mathcal{O}_L$.

2. Let $b\in\mathcal{O}_L$ be such that $\mathsf{k}_L = \mathsf{k}_K(\overline{b}\,)$, and let $g\in\mathcal{O}_K[X]$ be monic such that $\overline{g}\in\mathsf{k}_K[X]$ is the minimal polynomial of $\overline{b}$ over k_K. Then $\overline{g}$ is separable, and therefore $\overline{g'(b)} = \overline{g}'(\overline{b}\,)\ne 0$. Let $p\in L$ be a uniformizing parameter of L. Then $g(b+p)\equiv g(b)+pg'(b)\bmod\mathfrak{p}_L^2$, and $\overline{g(b)} = \overline{g(b+p)} = \overline{g}(\overline{b}\,) = 0\in\mathsf{k}_K$. Hence $g(b)\notin\mathfrak{p}_L^2$ or $g(b+p)\notin\mathfrak{p}_L^2$, and we set

$$x = \begin{cases} b & \text{if } \ g(b)\notin\mathfrak{p}_L^2\,, \\ b+p & \text{if } \ g(b)\in\mathfrak{p}_L^2\,. \end{cases}$$

Then $v_L(g(x))=1$, and by 1. we obtain $\mathcal{O}_L=\mathcal{O}_K[x,g(x)]=\mathcal{O}_K[x]$. □

Definition 4.4.5. Let K be a discrete valued field and $d\in\mathbb{N}$. A polynomial

$$g=X^d+a_{d-1}X^{d-1}+\ldots+a_1X+a_0\in K[X]$$

is called an *Eisenstein polynomial* if $v(a_0)=1$ and $v(a_i)\ge 1$ for all $i\in[1,d-1]$.

`eisenstein`

Theorem 4.4.6. *Let L/K be a finite extension of complete discrete valued fields, and let $n=[L\!:\!K]$.*

1. *Let $L=K(\alpha)$, and let $g\in\mathcal{O}_K[X]$ be an Eisenstein polynomial such that $g(\alpha)=0$. Then g is irreducible, L/K is fully ramified, and $v_L(\alpha)=1$.*
2. *Let L/K be fully ramified and $\pi\in L$ a uniformizing parameter. Then $\mathcal{O}_L=\mathcal{O}_K[\pi]$, and the minimal polynomial of π over K is an Eisenstein polynomial.*
3. *Let L/K be fully and tamely ramified and $n=[L\!:\!K]$. Then there exists a uniformizing parameter $\pi\in L$ such that $\pi^n\in K$. In particular, $L=K(\sqrt[n]{t}\,)$ for some uniformizing parameter $t\in K$.*

PROOF. 1. If $g=X^d+a_{d-1}X^{d-1}+\ldots+a_1X+a_0\in K[X]$, then $d\ge n\ge e=e(L/K)$, $v_L(a_i)\ge e$ for all $i\in[0,d-1]$, and $dv_L(\alpha)=v_L(\alpha^d)\ge\min\{v_L(a_i\alpha^i)\mid i\in[0,d-1]\,\}\ge e$. Hence $v_L(\alpha)\ge 1$, $v_L(a_i\alpha^i)\ge e+1>e=v_L(a_0)$ for all $i\in[1,d-1]$, and therefore $d\le dv_L(\alpha)=e$. Hence $d=e=n$, g is irreducible, L/K is fully ramified and $v_L(\alpha)=1$.

2. Let $|\cdot|\colon K\to\mathbb{R}_{\ge 0}$ be an absolute value of K, $d=[K(\pi):K]$, $m=[L:K(\pi)]$ and $g=X^d+a_{d-1}X^{d-1}+\ldots+a_1X+a_0\in K[X]$ the minimal polynomial of π over K. Then $dm=n=e(L/K)$, and Theorem 4.4.3 implies $1=v_L(\pi)=v_K(\mathsf{N}_{L/K}(\pi))=v_K(a_0^m)=m$. Hence $L=K(\pi)$, $v_K(a_0)=1$, and by Theorem 4.3.9 we obtain $|a_i|\le|a_0|<1$ and thus $v_K(a_i)\ge 1$ for all $i\in[1,d]$. Hence g is an Eisenstein polynomial, and since $f(L/K)=1$, we obtain $\mathcal{O}_L=\mathcal{O}_K[\pi]$ by Theorem 4.4.4 (applied with $b=1$).

3. By assumption, $e(L/K)=n$, $f(L/K)=1$, and $\mathrm{char}(\mathsf{k}_K)\nmid n$, which implies that $1_Kn\in\mathcal{O}_K^\times$. Let $|\cdot|\colon K\to\mathbb{R}_{\ge 0}$ be an absolute value of K, $\overline{K}\supset K$ an algebraic closure of K and $|\cdot|\overline{K}\to\mathbb{R}_{\ge 0}$ the extension of $|\cdot|$. Let π_K be a uniformizing parameter of K, π_L a uniformizing parameter of L, and $\pi_L^n=\pi_Ku$, where $u\in\mathcal{O}_L^\times$. Since $\mathsf{k}_L=\mathsf{k}_K$, there is some $u_0\in\mathcal{O}_K^\times$ such that $\gamma=u-u_0\in\mathfrak{p}_L$, hence $\pi_L^n-\pi_Ku_0=\pi_K\gamma\in\mathfrak{p}_L^2$ and $|\pi_K\gamma|<|\pi_L|$.

The polynomial $g=X^n-\pi_Ku_0\in K[X]$ is a separable Eisenstein polynomial, hence irreducible, and we set

$$g=\prod_{i=1}^n(X-\alpha_i)\in\overline{K}[X]\,.$$

Then $\alpha_i^n=\pi_Ku_0$, and therefore $|\alpha_i|=|\pi_K|^{1/n}=|\pi_L|$ for all $i\in[1,n]$. Since

$$|g(\pi_L)|=|\pi_K\gamma|=\prod_{i=1}^n|\pi_L-\alpha_i|<|\pi_L|\,,$$

There exists some $i\in[1,n]$ such that $|\pi_L-\alpha_i|<|\pi_L|$, say $|\pi_L-\alpha_1|<|\pi_L|$. Then we obtain, observing that $|nx|=|x|$ for all $x\in\overline{K}$,

$$|g'(\alpha_1)|=|n\alpha_1^{n-1}|=|\alpha_1|^{n-1}=\prod_{i=2}^n|\alpha_1-\alpha_i|\le\prod_{i=2}^n\max\{|\alpha_1|,\,|\alpha_i|\}=|\alpha_1|^{n-1}\,.$$

Hence $|\alpha_1 - \alpha_i| = |\alpha_1|$ for all $i \in [2,n]$, and therefore $|\pi_L - \alpha_1| < |\pi_L| = |\alpha_1| = |\alpha_i - \alpha_1|$. Since $\alpha_1, \ldots, \alpha_n$ are the conjugates of α over K, Krasner's Lemma (Theorem fortsetzungeindeutig 4.2.6) implies $\alpha_1 \in K(\pi_L) = L \ \ \alpha_1^n = \pi_K u_0 \in K$, and $v_L(\alpha_1) = v_L(\pi_L) = 1$. Hence the assertion follows with $\pi = \alpha_1$. $\square$

unramified1

Theorem 4.4.7. *Let K be a complete discrete valued field.*

1. *Let L/K be a finite separable unramified extension, $[L:K] = n$, $x \in \mathcal{O}_L$ such that $\mathsf{k}_L = \mathsf{k}_K(\overline{x})$ and $g \in \mathcal{O}_K[X]$ the minimal polynomial of x over K. Then $\mathcal{O}_L = \mathcal{O}_K[x]$, and $\overline{g} \in \mathsf{k}_K[X]$ is the minimal polynomial of $\overline{x}$ over k_K. In particular, $\overline{g}$ is separable.*
2. *Let $g \in \mathcal{O}_K[X]$ be monic such that $\overline{g} \in \mathsf{k}_K[X]$ is irreducible and separable, and suppose that $L = K(x)$, where $g(x) = 0$. Then L/K is unramified, and $\mathsf{k}_L = \mathsf{k}_K(\overline{x})$.*
3. *Let $\mathsf{k}' \supset \mathsf{k}_K$ be a finite separable extension. Then there exists an up to K-isomorphisms unique finite unramified extension M/K such that there is a k_K-isomorphism $\mathsf{k}_M \xrightarrow{\sim} \mathsf{k}'$.*

Proof. 1. Let $\psi \in \mathsf{k}_K[X]$ be the minimal polynomial of $\overline{x}$ over k_K. Then $\psi \,|\, \overline{g}$, and $n \ge \deg(g) \ge \deg(\psi) = [\mathsf{k}_L : \mathsf{k}_K] = f(L/K) = n$. Hence $\deg(g) = \deg(\psi)$, and therefore $\overline{g} = \psi$. By Theorem localextensions1 4.4.4.1 (with $\pi_L = \pi_K \in \mathcal{O}_K$) it follows that $\mathcal{O}_L = \mathcal{O}_K[x]$.

2. Let $n = \deg(g) = [L:K]$. Then $n = \deg(\overline{g}) = [\mathsf{k}_K(\overline{x}) : \mathsf{k}_K] \le [\mathsf{k}_L : \mathsf{k}_K] \le n$. Hence $\mathsf{k}_L = \mathsf{k}_K(\overline{x})$ and $\overline{g}$ is the minimal polynomial of $\overline{x}$ over k_K. Hence $\mathsf{k}_L/\mathsf{k}_K$ is separable, and L/K is unramified.

3. Let $\mathsf{k}' = \mathsf{k}_K(\alpha)$ and $g \in \mathcal{O}_K[X]$ a monic polynomial such that $\overline{g} \in \mathsf{k}_K[X]$ is the minimal polynomial of α over k_K. Then g is irreducible, and $\overline{g}$ is separable. Let $M = K(x)$, where $g(x) = 0$. By 2., M/K is unramified, and $\mathsf{k}_M = \mathsf{k}_K(\overline{x})$. Since $\overline{g}(\overline{x}) = 0$, there exists a k_K-isomorphism $\omega\colon \mathsf{k}_M \to \mathsf{k}'$ such that $\omega(\overline{x}) = \alpha$.

It remains to prove the uniqueness. Thus let M'/K be an unramified finite extension, $\omega'\colon \mathsf{k}_{M'} \to \mathsf{k}'$ a k_K-isomorphism and $\alpha' \in \mathsf{k}_{M'}$ such that $\omega'(\alpha') = \alpha$. Then $\overline{g}(\alpha') = 0$, and by Hensel's Lemma there exists some $x' \in M'$ such that $g(x') = 0$ and $\overline{x'} = \alpha'$. Hence there exists a K-isomorphism $\varphi\colon M \to M'$ such that $\varphi(x) = x'$. $\square$

unramified2

Theorem 4.4.8. *Let L/K be a finite extension of complete discrete valued fields, and let $\mathsf{k}_K \subset \mathsf{k}' \subset \mathsf{k}_L$ be an intermediate field such that k'/k_K is separable. Then there exists a unique intermediate field $K \subset M \subset L$ such that M/K is unramified and $\mathsf{k}_M = \mathsf{k}'$.*

In particular: The assignment $M \mapsto \mathsf{k}_M$ defines a bijective map from the set of all intermediate fields $K \subset M \subset L$ such that M/K is unramified onto the set of all intermediate field $\mathsf{k}_K \subset \mathsf{k}' \subset \mathsf{k}_L$ such that k'/k_K is separable.

Proof. Let $\mathsf{k}' = \mathsf{k}_K(\alpha) \subset \mathsf{k}_L$ and $g \in \mathcal{O}_K[X]$ a monic polynomial such that $\overline{g} \in \mathsf{k}_K[X]$ is the minimal polynomial of α over k_K. Then g is irreducible and $\overline{g}$ is separable. By Hensel's Lemma, there exists some $x \in \mathcal{O}_L$ such that $g(x) = 0$ and $\overline{x} = \alpha$. If $M = K(x) \subset L$, then M/K is unramified, and $\mathsf{k}_M = \mathsf{k}_K(\alpha) = \mathsf{k}'$.

It remains to prove the uniqueness. Thus let $K \subset M' \subset L$ be an intermediate field such that M'/K is unramified and $\mathsf{k}_{M'} = \mathsf{k}'$. Again by Hensel's Lemma, there exists some $x' \in \mathcal{O}_{M'}$ such that $g(x') = 0$ and $\overline{x'} = \alpha$. Then $M' = K(x')$, and we assert that $x = x'$. Assume the contrary. Then $x \ne x'$, hence $(X-x)(X-x') \,|\, g$, and $(X-\alpha)^2 \,|\, \overline{g}$, contradicting the separability of $\overline{g}$. $\square$

nertiafield

Theorem and Definition 4.4.9. *Let L/K be a finite extension of complete discrete valued fields.*

1. *Let $K \subset M \subset L$ be an intermediate field. Then L/K is unramified if and only if L/M and M/K are both unramified.*
2. *There exists a unique intermediate field T of L/K with the following property:*

   If $K \subset M \subset L$ is any intermediate field, then M/K is unramified if and only if $M \subset T$.

   T is called the *inertia field* of L/K.

   If L/K and $\mathsf{k}_L/\mathsf{k}_K$ are both separable, then $[T{:}K] = f(L/K)$, L/T is fully ramified, and $[L{:}T] = e(L/K)$.

Proof. 1. $e(L/K) = e(L/M)e(M/K) = 1$ if and only if $e(L/M) = e(M/K) = 1$, and $\mathsf{k}_L/\mathsf{k}_K$ is separable if and only if $\mathsf{k}_L/\mathsf{k}_M$ and $\mathsf{k}_M/\mathsf{k}_K$ are both separable.

2. The uniqueness of T is obvious. Thus let k' be the separable closure of k_K in k_L. By Theorem unramified2 4.4.8 there exists a unique intermediate field $K \subset T \subset L$ such that T/K is unramified and $\mathsf{k}_T = \mathsf{k}'$. If $\mathsf{k}_L/\mathsf{k}_K$ is separable, then $\mathsf{k}_T = \mathsf{k}_L$, and $[T{:}K] = [\mathsf{k}_L{:}\mathsf{k}_K] = f(L/K)$.

Let $K \subset M \subset L$ be any intermediate field. If $M \subset T$, then M/K is unramified by 1. If M/K is unramified, then $\mathsf{k}_M \subset \mathsf{k}' = \mathsf{k}_T$, and by Theorem unramified2 4.4.8 there exists a unique intermediate field $K \subset M' \subset T$ such that $\mathsf{k}_{M'} = \mathsf{k}_M$. But then M and M' are intermediate fields of L/K such that M/K and M'/K are unramified and $\mathsf{k}_M = \mathsf{k}_{M'}$. Hence $M = M' \subset T$.

If L/K and $\mathsf{k}_L/\mathsf{k}_K$ are both separable, then $[L:K] = e(L/K)f(L/K)$, and thus $[L:T] = e(L/K) = e(L/T)$. □

4.5. Extension of absolute values (general case)

alextension

Remarks and Definitions 4.5.1. Let $(K, |\cdot|)$ be a discrete or archimedean valued field, L/K a finite separable extension and $L = K(\alpha)$. Let $(\widehat{K}, |\cdot|)$ be a completion of $(K, |\cdot|)$, $\widehat{K}^{\mathsf{a}}$ an algebraic closure of $\widehat{K}$, and $|\cdot|\colon \widehat{K}^{\mathsf{a}} \to \mathbb{R}_{\ge 0}$ the extension of $|\cdot|$ to $\widehat{K}^{\mathsf{a}}$.

1. For $\varphi \in \mathrm{Hom}_K(L, \widehat{K}^{\mathsf{a}})$, we define $|\cdot|_\varphi = |\cdot| \circ \varphi\colon L \to \mathbb{R}_{\ge 0}$. Then $|\cdot|_\varphi$ is an absolute value of L, $|x|_\varphi = |\varphi(x)|$ for all $x \in L$, and $|\cdot|_\varphi \restriction K = |\cdot|$. By definition, $\varphi\colon (L, |\cdot|_\varphi) \to (\varphi(L), |\cdot|)$ is a value isomorphism.

   $\varphi(L) = K(\varphi(\alpha)) \subset \widehat{K}(\varphi(\alpha)) \subset \widehat{K}^{\mathsf{a}}$, $(\widehat{K}(\varphi(\alpha)){:}\widehat{K}) < \infty$, and therefore $(\widehat{K}(\varphi(\alpha), |\cdot|)$ is complete. We assert that $\varphi(L) = K(\varphi(\alpha)) \subset \widehat{K}(\varphi(\alpha))$ is dense.

   [*Proof.* If $z \in \widehat{K}(\varphi(\alpha))$, then $z = c_0 + c_1\varphi(\alpha) + \ldots + c_m\varphi(\alpha)^m$, where $m \in \mathbb{N}_0$ and $c_j \in \widehat{K}$ for all $j \in [0, m]$. Let $(c_{j,n})_{n \ge 0}$ be a sequence in K such that $(c_{j,n})_{n\ge 0} \overset{|\cdot|}{\to} c_j$ and $z_n = c_{0,n} + c_{1,n}\varphi(\alpha) + \ldots + c_{m,n}\varphi(\alpha)^m \in K(\varphi(\alpha))$. Then $(z_n)_{n \ge 0} \overset{|\cdot|}{\to} z$.]

   Hence $(\widehat{K}(\varphi(\alpha)), |\cdot|)$ is a completion of $(K(\varphi(\alpha)), |\cdot|) = (\varphi(L), |\cdot|)$, and we denote by $(L_\varphi, |\cdot|_\varphi)$ be a completion of $(L, |\cdot|_\varphi)$. Then there exists a unique value isomorphism $\widehat{\varphi}\colon (L_\varphi, |\cdot|_\varphi) \overset{\sim}{\to} (\widehat{K}(\varphi(\alpha)), |\cdot|)$ such that $\widehat{\varphi} \,|\, L = \varphi$, and, in particular, $\widehat{\varphi} \,|\, K = \mathrm{id}_K$. If K_φ is the topological closure of K in L_φ, then $(K_\varphi, |\cdot|_\varphi)$ is a completion of $(K, |\cdot|)$, hence $\widehat{\varphi}(K_\varphi) = \widehat{K}$, and we identify these two completions of $(K, \cdot)$. Then $\widehat{\varphi}\colon L_\varphi \overset{\sim}{\to} \widehat{K}(\varphi(\alpha))$ is a $\widehat{K}$-isomorphism. We call the extension $L_\varphi/\widehat{K}$ a (*complete*) *localization of* L/K.

2. Let $\varphi_1,\, \varphi_2 \in \mathrm{Hom}_K(L, \widehat{K}^{\mathsf{a}})$. Then $|\cdot|_{\varphi_1} = |\cdot|_{\varphi_2}$ if and only if $\varphi_1(\alpha)$ and $\varphi_2(\alpha)$ are conjugate over $\widehat{K}$ (then φ_1 and φ_2 are called *equivalent embeddings* of L into $\widehat{K}^{\mathsf{a}}$).

   [*Proof.* Assume first that $|\cdot|_{\varphi_1} = |\cdot|_{\varphi_2}$. Then we may assume that $L_{\varphi_1} = L_{\varphi_2}$, and for $i \in \{1,2\}$ there exist value isomorphisms $\widehat{\varphi}_i \colon (L_{\varphi_i}, |\cdot|_{\varphi_i}) \xrightarrow{\sim} (\widehat{K}(\varphi_i(\alpha)), |\cdot|)$ which are $\widehat{K}$-isomorphisms satisfying $\widehat{\varphi}_i(\alpha) = \alpha_i$. Then $\widehat{\varphi}_2 \circ \widehat{\varphi}_1{}^{-1} \colon \widehat{K}(\varphi_1(\alpha)) \xrightarrow{\sim} \widehat{K}(\varphi_2(\alpha))$ is a $\widehat{K}$-isomorphism satisfying $\widehat{\varphi}_2 \circ \widehat{\varphi}_1{}^{-1}(\varphi_1(\alpha)) = \varphi_2(\alpha)$. Hence $\varphi_1(\alpha)$ and $\varphi_2(\alpha)$ are conjugate over $\widehat{K}$.

   Let now $\varphi_1(\alpha)$ and $\varphi_2(\alpha)$ be conjugate over $\widehat{K}$, and let $\Phi \colon \widehat{K}(\varphi_1(\alpha)) \xrightarrow{\sim} \widehat{K}(\varphi_2(\alpha))$ be a $\widehat{K}$-isomorphism such that $\Phi(\varphi_1(\alpha)) = \varphi_2(\alpha)$. Then $|\cdot|_\Phi = |\cdot| \circ \Phi \colon \widehat{K}(\varphi_1(\alpha)) \to \mathbb{R}_{\ge 0}$ is an absolute value of $\widehat{K}(\varphi_1(\alpha))$ satisfying $|\cdot|_\Phi \restriction \widehat{K} = |\cdot|$, and therefore $|\cdot|_\Phi = |\cdot|$ by Theorem `fortsetzungeindeutig` 4.2.6. Since $\Phi \circ \varphi_1 \in \mathrm{Hom}_K(L, \widehat{K}^{\mathsf{a}})$, $\Phi \circ \varphi_1 \,|\, L = \mathrm{id}_K$ and $\Phi \circ \varphi_1(\alpha) = \varphi_2(\alpha)$, it follows that $\Phi \circ \varphi_1 = \varphi_2$, and $|\cdot|_{\varphi_2} = |\cdot| \circ \varphi_2 = |\cdot| \circ \Phi \circ \varphi_1 = |\cdot|_\Phi \circ \varphi_1 = |\cdot| \circ \varphi_1 = |\cdot|_{\varphi_1}$.]

3. Let finally $\|\cdot\| \colon L \to \mathbb{R}_{\ge 0}$ be an absolute value satisfying $\|\cdot\| \restriction K = |\cdot|$. Then there exists some $\varphi \in \mathrm{Hom}_K(L, \widehat{K}^{\mathsf{a}})$ such that $\|\cdot\| = |\cdot|_\varphi$.

   [*Proof.* Let $(L', \|\cdot\|')$ be a completion of $(L, \|\cdot\|)$ and $\overline{K} \subset L'$ the (topological) closure of K. Then $(\overline{K}, \|\cdot\|' \restriction \overline{K})$ is a completion of $(K, |\cdot|)$, and $L = K(\alpha) \subset \overline{K}(\alpha) \subset \widehat{L}$ is dense. By Theorem `fortsetzungeindeutig` 4.2.6, $(\overline{K}(\alpha), \|\cdot\|' \restriction \overline{K}(\alpha))$ is complete, hence $\overline{K}(\alpha) \subset \widehat{L}$ is closed, and thus $\overline{K}(\alpha) = \widehat{L}$. Let $\iota \colon (\overline{K}, \|\cdot\|' \restriction \overline{K}) \xrightarrow{\sim} (\widehat{K}, |\cdot|)$ be the unique value isomorphism satisfying $\iota \,|\, K = \mathrm{id}_K$, and let $\Phi \colon \widehat{L} = \overline{K}(\alpha) \to \widehat{K}^{\mathsf{a}}$ be a homomorphism such that $\Phi \,|\, \overline{K} = \iota$. Then $|\cdot|_\Phi = |\cdot| \circ \Phi \colon \widehat{L} \to \mathbb{R}_{\ge 0}$ is an absolute value of $\widehat{L}$, and since $|\cdot|_\Phi \restriction \overline{K} = \|\cdot\|' \restriction \overline{K}$, it follows that $|\cdot|_\Phi = \|\cdot\|'$. If $\varphi = \Phi \,|\, L \colon L \to \widehat{K}^{\mathsf{a}}$, then $\varphi \in \mathrm{Hom}_K(L, \widehat{K}^{\mathsf{a}})$ and $\|\cdot\| = \|\cdot\|' \restriction L = |\cdot|_\Phi \restriction L = |\cdot|_\varphi$.]

`lextension1` **Theorem 4.5.2.** *Let $(K, |\cdot|)$ be a discrete or archimedean valued field and L/K a finite separable extension. Let $(\widehat{K}, |\cdot|)$ be a completion of $(K, |\cdot|)$, $\widehat{K}^{\mathsf{a}}$ an algebraic closure of $\widehat{K}$, and $|\cdot| \colon \widehat{K}^{\mathsf{a}} \to \mathbb{R}_{\ge 0}$ the extension of $|\cdot|$ to $\widehat{K}^{\mathsf{a}}$. For $\varphi \in \mathrm{Hom}_K(L, \widehat{K}^{\mathsf{a}})$, set $|\cdot|_\varphi = |\cdot| \circ \varphi \colon L \to \mathbb{R}_{\ge 0}$, and let $[\varphi]$ be the equivalence class of embeddings of L into $\widehat{K}^{\mathsf{a}}$.*

1. *The assignment $[\varphi] \mapsto |\cdot|_\varphi$ defines a bijective map from the set of all equivalence classes of embeddings of L into $\widehat{K}^{\mathsf{a}}$ onto the set of all absolute values of L extending $|\cdot|$.*
2. *Let $L = K(\alpha)$, $g \in K[X]$ the minimal polynomial of α over K and $g = g_1 \cdot \ldots \cdot g_r$, where $r \in \mathbb{N}$ and $g_1, \ldots, g_r \in \widehat{K}[x]$ are monic and irreducible. For $i \in [1,r]$, let $\alpha_i \in \widehat{K}^{\mathsf{a}}$ be such that $g_i(\alpha_i) = 0$ and $\varphi_i \colon L \to \widehat{K}^{\mathsf{a}}$ the unique K-homomorphism satisfying $\varphi_i(\alpha) = \alpha_i$. Then $\{\varphi_1, \ldots, \varphi_r\}$ is a complete system of pairwise not equivalent embeddings of L into $\widehat{K}^{\mathsf{a}}$, and $|\cdot|_{\varphi_1}, \ldots, |\cdot|_{\varphi_r}$ are the distinct absolute values of L extending $|\cdot|$.*

   If $i \in [1,r]$ and $(\widehat{L}_i, |\cdot|_{\varphi_i})$ denotes a completion of $(L, |\cdot|_{\varphi_i})$ such that $\widehat{K} \subset \widehat{L}_i$, then there exists a unique value isomorphism $\widehat{\varphi}_i \colon (\widehat{L}_i, |\cdot|_{\varphi_i}) \xrightarrow{\sim} (\widehat{K}(\alpha_i), |\cdot|)$ such that $\widehat{\varphi}_i \,|\, \widehat{K} = \mathrm{id}_{\widehat{K}}$ and $\widehat{\varphi}_i(\alpha) = \alpha_i$. It satisfies $\widehat{\varphi}_i \,|\, L = \varphi_i$. In particular, $\widehat{L}_i/\widehat{K}$ is a finite separable extension.
3. *Let $|\cdot|_1, \ldots, |\cdot|_r \colon L \to \mathbb{R}_{\ge 0}$ be the distinct absolute valued of L extending $|\cdot|$. For $i \in [1,r]$, let $(\widehat{L}_i, |\cdot|_i)$ be a completion of $(L, |\cdot|_i)$, and suppose that $\widehat{K} \subset \widehat{L}_i$. Then*

$|\cdot|_1, \ldots, |\cdot|_r$ *are pairwise not equivalent,*

$$[L\!:\!K] = \sum_{i=1}^r [\widehat{L}_i\!:\!\widehat{K}]\,, \quad \textit{and if} \;\; \delta\colon L \;\to\; \prod_{i=1}^r \widehat{L}_i \quad \textit{is defined by} \quad \delta(x) = (x, \ldots, x)\,,$$

then $\delta(L)$ is dense in the product space. Moreover, we have

$$\mathsf{N}_{L/K}(x) = \prod_{i=1}^r \mathsf{N}_{\widehat{L}_i/\widehat{K}}(x) \quad \textit{and} \quad \mathsf{Tr}_{L/K}(x) = \sum_{i=1}^r \mathsf{Tr}_{\widehat{L}_i/\widehat{K}}(x) \quad \textit{for all} \;\; x \in L\,.$$

Proof. 1. By the construction made in 4.5.1.

2. By 1. and the construction made in 4.5.1, it suffices to prove $\varphi_1, \ldots, \varphi_r$ are pairwise not equivalent, and that every embedding of L into $\widehat{K}^{\mathsf{a}}$ is equivalent to some φ_i. Since g is separable, the polynomials $g_1, \ldots, g_r$ are distinct, and therefore $\alpha_1, \ldots, \alpha_r$ are pairwise not conjugate over $\widehat{K}$. Hence $\varphi_1, \ldots, \varphi_r$ are pairwise not equivalent.

If $\varphi \in \mathrm{Hom}_K(L, \widehat{K}^{\mathsf{a}})$, then $g(\varphi(\alpha)) = 0$, hence $g_i(\varphi(\alpha)) = 0$ for some $i \in [1, r]$, and then $\alpha_i = \varphi_i(\alpha)$ and $\varphi(\alpha)$ are conjugate over $\widehat{K}$. Hence φ is equivalent to φ_i.

3. We maintain the notions of 2. (in particular, $|\cdot|_i = |\cdot|_{\varphi_i}$). By Theorem 4.1.6, the absolute values $|\cdot|_1, \ldots, |\cdot|_r$ ar pairwise not equivalent, and

$$[L\!:\!K] = \deg(g) = \sum_{i=1}^r \deg(g_i) = \sum_{i=1}^r [\widehat{K}(\alpha_i)\!:\!\widehat{K}] = \sum_{i=1}^r [\widehat{L}_i\!:\!\widehat{K}]\,.$$

Let

$$\|\cdot\|\colon \prod_{i=1}^r \widehat{L}_i \;\to\; \mathbb{R}_{\ge 0} \quad \text{be defined by} \quad \|(x_1, \ldots, x_r)\| = \max\{|x_1|_1, \ldots, |x_r|_r\}\,.$$

Then $\|\cdot\|$ is a $|\cdot|$-compatible norm and induces the product topology. For the proof that $\delta(L)$ is dense, let $\boldsymbol{x} = (x_1, \ldots, x_r) \in \widehat{L}_1 \times \ldots \times \widehat{L}_r$ and $\varepsilon \in \mathbb{R}_{>0}$. For every $i \in [1, r]$, there is some $y_i \in L$ such that $|y_i - x_i|_i < \frac{\varepsilon}{2}$, and by Theorem 4.1.7, there exists some $x \in L$ such that $|x - y_i|_i < \frac{\varepsilon}{2}$ for all $i \in [1, r]$, and therefore $|x - x_i|_i \le |x - y_i|_i + |y_i - x_i|_i < \varepsilon$, which implies $\|\delta(x) - \boldsymbol{x}\| < \varepsilon$.

For $i \in [1, r]$, let $n_i = [\widehat{K}(\alpha_i)\!:\!\widehat{K}] = [\widehat{L}_i\!:\!\widehat{K}]$ and $\mathrm{Hom}_{\widehat{K}}(\widehat{K}(\alpha_i), \widehat{K}^{\mathsf{a}}) = \{\varphi_{i,1}, \ldots, \varphi_{i,n_i}\}$. Then $\mathrm{Hom}_{\widehat{K}}(\widehat{L}_i, \widehat{K}^{\mathsf{a}}) = \{\varphi_{i,1} \circ \widehat{\varphi}_i, \ldots, \varphi_{i,n_i} \circ \widehat{\varphi}_i\}$, and $\mathrm{Hom}_K(L, \widehat{K}^{\mathsf{a}}) = \{\varphi_{i,\nu} \circ \varphi_i \mid i \in [1, r],\; \nu \in [1, n_i]\,\}$. For $x \in L$, this implies

$$\mathsf{N}_{L/K}(x) = \prod_{i=1}^r \prod_{\nu=1}^{n_i} \varphi_{i,\nu} \circ \varphi_i(x) = \prod_{i=1}^r \prod_{\nu=1}^{n_i} \varphi_{i,\nu} \circ \widehat{\varphi}_i(x) = \prod_{i=1}^r \mathsf{N}_{\widehat{L}_i/\widehat{K}}(x)\,,$$

and similar for the trace. □

Theorem and Definition 4.5.3. *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite separable extension, $S = \mathrm{cl}_L(R)$, $\mathfrak{p} \in \mathcal{P}(R)$, $\rho \in (0, 1)$ and $|\cdot|_{\mathfrak{p}} = |\cdot|_{\mathfrak{p},\rho}\colon K \to \mathbb{R}_{\ge 0}$ be a $\mathfrak{p}$-adic absolute value. Then $|x|_{\mathfrak{p}} = \rho^{\mathsf{v}_{\mathfrak{p}}}(x)$ for all $x \in K$, where $\mathsf{v}_{\mathfrak{p}}\colon K \to \mathbb{Z} \cup \{\infty\}$ denotes the $\mathfrak{p}$-adic valuation.*

1. *Let $\mathfrak{P} \in \mathcal{P}(S)$, $\mathfrak{P} \cap R = \mathfrak{p}$, $e = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p})$ and $|\cdot|_{\mathfrak{P}} = |\cdot|_{\mathfrak{P},\rho^{1/e}}$.*
   (a) *$\mathsf{v}_{\mathfrak{P}} \,|\, K = e\, v_{\mathfrak{p}}\colon K \to \mathbb{Z} \cup \{\infty\}$, and $|\cdot|_{\mathfrak{P}} \!\restriction\! K = |\cdot|_{\mathfrak{p}}$.*

(b) *Let* $(K_\mathfrak{p}, |\cdot|_\mathfrak{p})$ *be a completion of* $(K, |\cdot|_\mathfrak{p})$, *let* $\widehat{R}_\mathfrak{p}$ *be its valuation domain,* $\widehat{\mathfrak{p}}$ *its valuation ideal and* $\mathsf{v}_\mathfrak{p}\colon K_\mathfrak{p} \to \mathbb{Z} \cup \{\infty\}$ *its valuation. Let* $(L_\mathfrak{P}, |\cdot|_\mathfrak{P})$ *be a completion of* $(L, |\cdot|_\mathfrak{P})$ *such that* $K_\mathfrak{p} \subset L_\mathfrak{P}$, *let* $\widehat{S}_\mathfrak{P}$ *be its valuation domain,* $\widehat{\mathfrak{P}}$ *its valuation ideal and* $\mathsf{v}_\mathfrak{P}\colon L_\mathfrak{P} \to \mathbb{Z} \cup \{\infty\}$ *its valuation* (see Theorem `dedekindvalue` 4.3.5). *Then* $L_\mathfrak{P}/K_\mathfrak{p}$ *is a finite separable extension of discrete valued fields with residue class fields* $\mathsf{k}_{K_\mathfrak{p}} = R/\mathfrak{p}$, $\mathsf{k}_{L_\mathfrak{P}} = S/\mathfrak{P}$, $e(L_\mathfrak{P}/K_\mathfrak{p}) = e$ *and* $f(L_\mathfrak{P}/K_\mathfrak{p}) = f$. *Moreover,* $\widehat{S}_\mathfrak{P} = S\widehat{R}_\mathfrak{p}$ *and* $L_\mathfrak{P} = LK_\mathfrak{p}$.

The extension $L_\mathfrak{P}/K_\mathfrak{p}$ is called the *completion of* L/K *at* $\mathfrak{P}/\mathfrak{p}$.

2. *Let* $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$, *where* $r \in \mathbb{N}$, $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathcal{P}(S)$ *are distinct, and, for all* $i \in [1, r]$, $e_i = e(\mathfrak{P}_i/\mathfrak{p})$, $f_i = f(\mathfrak{P}_i/\mathfrak{p})$, *and* $|\cdot|_{\mathfrak{P}_i} = |\cdot|_{\mathfrak{P}_i, \rho^{1/e_i}}$. *Then* $|\cdot|_{\mathfrak{P}_1}, \ldots, |\cdot|_{\mathfrak{P}_r}$ *are precisely the distinct extensions of* $|\cdot|_\mathfrak{p}$ *to* L. *For all* $x \in L$, *we have*

$$\mathsf{N}_{L/K}(x) = \prod_{i=1}^{r} \mathsf{N}_{L_{\mathfrak{P}_i}/K_\mathfrak{p}}(x) \quad \textit{and} \quad \mathsf{Tr}_{L/K}(x) = \sum_{i=1}^{r} \mathsf{Tr}_{L_{\mathfrak{P}_i}/K_\mathfrak{p}}(x)$$

3. *Let* $L = K(\alpha)$, $g \in K[X]$ *the minimal polynomial of* α *over* K, *and* $g = g_1 \cdot \ldots \cdot g_r$, *where* $r \in \mathbb{N}$ *and* $g_1, \ldots, g_r \in K_\mathfrak{p}[X]$ *are monic and irreducible. For* $i \in [1, r]$, *let* $\widehat{L}_i = \widehat{K}(\alpha_i)$, *where* $g_i(\alpha_i) = 0$. *Then* $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$, *where* $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathcal{P}(S)$ *are distinct,* $e_i = e(\widehat{L}_i/\widehat{K})$ *and* $f(\mathfrak{P}_i/\mathfrak{p}) = f(\widehat{L}_i/\widehat{K})$ *for all* $i \in [1, r]$.

Proof. 1. (a) Let $\pi \in R \setminus \mathfrak{p}$ and $\Pi \in S \setminus \mathfrak{P}$. Then $\mathsf{v}_\mathfrak{p}(\pi) = \mathsf{v}_\mathfrak{P}(\Pi) = 1$, and we obtain $\Pi^e S_\mathfrak{P} = \mathfrak{P}^e S_\mathfrak{P} = \mathfrak{p} S_\mathfrak{P} = \mathfrak{p} R_\mathfrak{p} S_\mathfrak{P} = \pi S_\mathfrak{P}$. Hence it follows that $\pi = \Pi^e u$ for some $u \in S_\mathfrak{P}^\times$, and $\mathsf{v}_\mathfrak{P}(\pi) = e\mathsf{v}_\mathfrak{P}(\Pi) = e$. If $x \in K^\times$, then $x = \pi^{\mathsf{v}_\mathfrak{p}(x)} v$ for some $v \in R_\mathfrak{p}^\times \subset S_\mathfrak{P}^\times$, and $\mathsf{v}_\mathfrak{P}(x) = \mathsf{v}_\mathfrak{p}(x)\mathsf{v}_\mathfrak{P}(\pi) + \mathsf{v}_\mathfrak{P}(v) = e\mathsf{v}_\mathfrak{p}(x)$. Hence $\mathsf{v}_\mathfrak{P} \,|\, K = e\,\mathsf{v}_\mathfrak{p}$. Moreover, $|x|_\mathfrak{P} = (\rho^{1/e})^{\mathsf{v}_\mathfrak{P}(x)} = \rho^{\mathsf{v}_\mathfrak{p}(x)} = |x|_\mathfrak{p}$, and therefore $|\cdot|_\mathfrak{P} \restriction K = |\cdot|_\mathfrak{p}$.

(b) By Theorem `generalextension1` 4.5.2, $L_\mathfrak{P}/K_\mathfrak{p}$ is a finite separable extension of discrete valued fields. By Theorem `dedekindvalue` 4.3.5, $\mathsf{k}_{K_\mathfrak{p}} = \widehat{R}_\mathfrak{p}/\widehat{p} = R/\mathfrak{p}$ and $\mathsf{k}_{L_\mathfrak{P}} = \widehat{S}_\mathfrak{P}/\widehat{P} = S/\mathfrak{P}$. Hence it follows that $f(L_\mathfrak{P}/K_\mathfrak{p}) = [\mathsf{k}_{L_\mathfrak{P}} \colon \mathsf{k}_{K_\mathfrak{p}}] = [S/\mathfrak{P} \colon R/\mathfrak{p}] = f$. Moreover, $\widehat{\mathfrak{p}}\widehat{S}_\mathfrak{P} = \mathfrak{p}\widehat{R}_\mathfrak{p} S\widehat{S}_\mathfrak{P} = \mathfrak{p}S\widehat{S}_\mathfrak{P} = \mathfrak{P}^e\widehat{S}_\mathfrak{P} = \widehat{\mathfrak{P}}^e$, and therefore $e(L_\mathfrak{P}/K_\mathfrak{p}) = e$.

As $\overline{S} = \widehat{S}_\mathfrak{P}$, it follows that $S\widehat{R}_\mathfrak{p} \subset \widehat{S}_\mathfrak{P}$ is dense. S is a finitely generated R-module, hence $S\widehat{R}_\mathfrak{p}$ is a finitely generated $\widehat{R}_\mathfrak{p}$-module, and by Theorem `completeextension` 4.4.1, $S\widehat{R}_\mathfrak{p} \subset L_\mathfrak{P}$ is closed. Hence $S\widehat{R}_\mathfrak{p} = S_\mathfrak{P}$, and since $L_\mathfrak{P} \supset LK_\mathfrak{p} \supset L\widehat{R}_\mathfrak{p} = \mathsf{q}(SR_\mathfrak{p}) = \mathsf{q}(\widehat{S}_\mathfrak{P}) = L_\mathfrak{P}$, we obtain $LK_\mathfrak{p} = L_\mathfrak{P}$.

2. If $i, j \in [1, r]$, $i \ne j$ and $a \in \mathfrak{P}_i \setminus \mathfrak{P}_j$, then $|a|_{\mathfrak{P}_i} < 1$ and $|a|_{\mathfrak{P}_j} = 1$, hence $|\cdot|_{\mathfrak{P}_i} \ne |\cdot|_{\mathfrak{P}_j}$. Let now $\|\cdot\|\colon L \to \mathbb{R}_{\ge 0}$ be an absolute value such that $\|\cdot\| \restriction K = |\cdot|_\mathfrak{p}$. Then $\|\cdot\|$ is a discrete absolute value, and we assert that $\|x\| \le 1$ for all $x \in S$.

Indeed, if $x \in S$ and $x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 = 0$ is an integral equation for x over R, then $\|x\|^d = \|a_{d-1}x^{d-1} + \ldots + a_1 x + a_0\| \le \max\{|a_i|_\mathfrak{p}\,\|x\|^i \mid i \in [0, d-1]\} \le \max\{1, \|x\|^{d-1}\}$ and thus $\|x\| \le 1$. By Theorem `nichtarch1` 4.1.8, there is some $\mathfrak{P} \in \mathcal{P}(S)$ such that $\|\cdot\| = |\cdot|_{\mathfrak{P},\theta}$ for some $\theta \in (0, 1)$. Since $\mathfrak{P} \cap R = \{c \in R \mid |c|_\mathfrak{p} < 1\} = \mathfrak{p}$, it follows that $\mathfrak{P} = \mathfrak{P}_i$ for some $i \in [1, r]$, hence $\|\cdot\| \sim |\cdot|_{\mathfrak{P}_i}$ and thus $\|\cdot\| = |\cdot|_{\mathfrak{P}_i}$ for some $i \in [1, r]$.

The formulas for the norm and the trace follow by Theorem `generalextension1` 4.5.2.

3. Obvious by 2. and Theorem `generalextension1` 4.5.2. □

4.6. Different and discriminant

different1 **Theorem and Definition 4.6.1.** *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite separable extension, and $S = \mathrm{cl}_L(R)$.*

1. $\mathfrak{C}_{S/R} = \{x \in L \mid \mathsf{Tr}_{L/K}(xS) \subset R\}$ *is a fractional ideal of S, and $S \subset \mathfrak{C}_{S/R}$.*

   $\mathfrak{C}_{S/R}$ is called *Dedekind' complementary module* and $\mathfrak{D}_{S/R} = \mathfrak{C}_{S/R}^{-1} \in \mathfrak{I}(S)$ is called the *different* of S/R.
2. *Let S be R-free, $(u_1, \ldots, u_n)$ an R-basis of S and $(u_1^*, \ldots, u_n^*)$ the dual basis of L/K. Then $\mathfrak{C}_{S/R} = Ru_1^* + \ldots + Ru_n^*$.*
3. *Let $\alpha \in S$ be such that $S = R[\alpha]$, and let $g \in R[X]$ be the minimal polynomial of α over K. Then $\mathfrak{D}_{S/R} = g'(\alpha)S$.*

Proof. 1. and 2. If $x, y \in \mathfrak{C}_{S/R}$ and $c \in S$. Then $\mathsf{Tr}_{L/K}(cxs) \in \mathsf{Tr}_{L/K}(xS) \subset R$ and $\mathsf{Tr}_{L/K}((x+y)s) = \mathsf{Tr}_{L/K}(xs) + \mathsf{Tr}_{L/K}(ys) \in R$ for all $s \in S$. Hence $cx \in S$ and $x + y \in S$, and thus $\mathfrak{C}_{S/R}$ is an S-module. Since $\mathsf{Tr}_{L/K}(S) \subset R$, it follows that $S \subset \mathfrak{C}_{S/R}$.

Let $(u_1, \ldots, u_n) \in S^n$ be a K-basis of L and $(u_1^*, \ldots, u_n^*)$ the dual basis of L. We assert that $\mathfrak{C}_{S/R} \subset Ru_1^* + \ldots + Ru_n^*$. Indeed, if $c \in \mathfrak{C}_{S/R}$, then $c = a_1u_1^* + \ldots + a_nu_n^*$ for some $a_1, \ldots, a_n \in K$. For all $i \in [1, n]$, we get

$$a_i = \sum_{\nu=1}^{n} a_\nu \mathsf{Tr}_{L/K}(u_\nu^* u_i) = \mathsf{Tr}_{L/K}(cu_i) \in R\,, \quad \text{and therefore} \quad c \in Ru_1^* + \ldots + Ru_n^*\,.$$

If $(u_1, \ldots, u_n)$ be an R-basis of S and $c \in S$, then $c = a_1u_1 + \ldots + a_nu_n$, where $a_1, \ldots, a_n \in R$, and $\mathsf{Tr}_{L/K}(cu_i^*) = a_i \in R$ for all $i \in [1, r]$. Hence $\{u_1^*, \ldots, u_n^*\} \subset \mathfrak{C}_{S/R}$, and therefore $\mathfrak{C}_{S/R} = Ru_1^* + \ldots + Ru_n^*$.

3. Let

$$g = \sum_{\nu=0}^{n} a_\nu X^\nu\,, \quad \text{where} \quad a_n = 1\,, \quad \text{and} \quad \frac{g}{X - \alpha} = \sum_{\nu=0}^{n-1} \beta_\nu X^\nu\,, \quad \text{where} \quad \beta_1, \ldots, \beta_{n-1} \in S\,.$$

Then $(1, \alpha, \ldots, \alpha^{n-1})$ is an R-basis of S,

$$\Bigl(\frac{\beta_0}{g'(\alpha)}, \ldots, \frac{\beta_{n-1}}{g'(\alpha)}\Bigr) \quad \text{is the dual basis of } L/K \text{, and} \qquad \mathfrak{C}_{S/R} = \frac{1}{g'(\alpha)} \sum_{\nu=0}^{n-1} \beta_\nu R\,.$$

We shall prove that $(\beta_0, \ldots, \beta_{n-1})$ is an R-basis of S. Once this is done, it follows that $g'(\alpha)\mathfrak{C}_{S/R} = S$, and $\mathfrak{D}_{S/R} = g'(\alpha)S$. Since $g(\alpha) = 0$, we obtain

$$g = \sum_{\nu=0}^{n} a_\nu (X^\nu - \alpha^\nu) = (X - \alpha) \sum_{\nu=1}^{n} a_\nu \sum_{j=0}^{\nu-1} \alpha^{\nu-1-j} X^j = (X - \alpha) \sum_{j=0}^{n-1} \Bigl(\sum_{\nu=j+1}^{n} a_\nu \alpha^{\nu-1-j} \Bigr) X^j\,,$$

and consequently $\beta_j = a_{j+1} + a_{j+2}\alpha + \ldots + a_n\alpha^{n-1-j}$ for all $j \in [0, n-1]$. Observing $a_n = 1$, this yields to the matrix equation

$$\begin{pmatrix} \beta_{n-1} \\ \beta_{n-2} \\ \vdots \\ \beta_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ a_{n-1} & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix} = A \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}, \quad \text{where} \quad A \in \mathsf{GL}_n(R)\,.$$

Hence $(\beta_0, \ldots, \beta_{n-1})$ is an R-basis of S. $\square$

Definition 4.6.2. Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite separable extension, and $S = \mathrm{cl}_L(R)$.

1. The *ideal norm* $\mathcal{N}_{S/R} \colon \mathcal{F}(S) \to \mathcal{F}(R)$ is the unique group homomorphism satisfying $\mathcal{N}_{S/R}(\mathfrak{P}) = \mathfrak{p}^f$ if $\mathfrak{P} \in \mathcal{P}(S)$, $\mathfrak{p} = \mathfrak{P} \cap R$ and $f = f(\mathfrak{P}/\mathfrak{p})$ [note that $\mathcal{F}(S)$ is the free abelian group with basis $\mathcal{P}(S)$].

   If $R = \mathbb{Z}$, $K = \mathbb{Q}$ and L is an algebraic number field, then $\mathcal{N}_{\mathcal{O}_L/\mathbb{Z}}(\mathfrak{P}) = \mathfrak{N}(\mathfrak{P})\mathbb{Z}$ for all $\mathfrak{P} \in \mathcal{P}(S)$, and therefore $\mathcal{N}_{\mathcal{O}_L/\mathbb{Z}}(\mathfrak{A}) = \mathfrak{N}(\mathfrak{A})\mathbb{Z}$ for all $\mathfrak{A} \in \mathcal{F}(S)$ (see Theorem 3.2.7).
2. The *relative discriminant* $\mathfrak{d}_{S/R} \in \mathcal{I}(R)$ is defined by $\mathfrak{d}_{S/R} = \mathcal{N}_{S/R}(\mathfrak{D}_{S/R})$.

different2 **Theorem 4.6.3.** *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite separable extension, $[L\!:\!L] = n$, and $S = \mathrm{cl}_L(R)$.*

1. *If $\mathfrak{a} \in \mathcal{F}(R)$, then $\mathcal{N}_{S/R}(\mathfrak{a}S) = \mathfrak{a}^n$.*
2. *If $z \in L^\times$, then $\mathcal{N}_{S/R}(zS) = \mathsf{N}_{L/K}(z)R$.*
3. *Let $\mathfrak{p} \in \mathcal{P}(R)$.*
   (a) *$\mathcal{N}_{S_\mathfrak{p}/R_\mathfrak{p}}(\mathfrak{A}S_\mathfrak{p}) = \mathcal{N}_{S/R}(\mathfrak{A})R_\mathfrak{p}$ for all $\mathfrak{A} \in \mathcal{F}(S)$.*
   (b) *$\mathfrak{D}_{S_\mathfrak{p}/R_\mathfrak{p}} = \mathfrak{D}_{S/R}S_\mathfrak{p}$, $\mathfrak{d}_{S_\mathfrak{p}/R_\mathfrak{p}} = \mathfrak{d}_{S/R}R_\mathfrak{p}$, and*
   $$\mathsf{v}_\mathfrak{p}(\mathfrak{d}_{S/R}) = \sum_{\mathfrak{P} \,|\, \mathfrak{p}} f(\mathfrak{P}/\mathfrak{p})\mathsf{v}_\mathfrak{P}(\mathfrak{D}_{S/R}),$$
   where the sum runs over all $\mathfrak{P} \in \mathcal{P}(S)$ such that $\mathfrak{P} \cap R = \mathfrak{p}$.
4. *If S is R-free with basis $(u_1, \ldots, u_n)$, then $\mathfrak{d}_{S/R} = \Delta_{L/K}(u_1, \ldots, u_n)R$.*
5. *If $\alpha \in S$ is such that $S = R[\alpha]$ and $g \in R[X]$ is the minimal polynomial of α over R, then $\mathfrak{d}_{S/R} = \Delta(g)R$.*

Proof. 1. Since the assignments $\mathfrak{a} \mapsto \mathcal{N}_{S/R}(\mathfrak{a}S)$ and $\mathfrak{a} \mapsto \mathfrak{a}^n$ define homomorphisms $\mathcal{F}(R) \to \mathcal{F}(R)$, it suffices to prove that $\mathcal{N}_{S/R}(\mathfrak{p}S) = \mathfrak{p}^n$ for all $\mathfrak{p} \in \mathcal{P}(R)$. Thus let $\mathfrak{p} \in \mathcal{P}(R)$ and $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$, where $r \in \mathbb{N}$, $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathcal{P}(S)$ are distinct and $e_1, \ldots, e_r \in \mathbb{N}$. Then

$$\mathcal{N}_{S/R}(\mathfrak{p}S) = \prod_{i=1}^r \mathcal{N}_{S/R}(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^r \mathfrak{p}^{e_i f(\mathfrak{P}_i/\mathfrak{p})} = \mathfrak{p}^n, \quad \text{since} \quad \sum_{i=1}^r e_i f(\mathfrak{P}_i/\mathfrak{p}) = n.$$

2. Let $z \in L^\times$. We note that

$$zS = \prod_{\mathfrak{P} \in \mathcal{P}(S)} \mathfrak{P}^{\mathsf{v}_\mathfrak{P}(z)} = \prod_{\mathfrak{p} \in \mathcal{P}(R)} \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathfrak{P}^{\mathsf{v}_\mathfrak{P}(z)} \quad \text{and} \quad \mathcal{N}_{S/R}(zS) = \prod_{\mathfrak{p} \in \mathcal{P}(R)} \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})\mathsf{v}_\mathfrak{P}(z)}.$$

For $\mathfrak{p} \in \mathcal{P}(R)$ and $\mathfrak{P} \,|\, \mathfrak{p}$ we consider the completion $L_\mathfrak{P}/K_\mathfrak{p}$ at $\mathfrak{P}/\mathfrak{p}$ (see Theorem 4.5.3). Then $f(\mathfrak{P}/\mathfrak{p}) = f(L_\mathfrak{P}/K_\mathfrak{p})$, and Theorem 4.4.3 implies $\mathsf{v}_\mathfrak{p} \circ \mathsf{N}_{L_\mathfrak{P}/K_\mathfrak{p}} = f(\mathfrak{P}/\mathfrak{p})\mathsf{v}_\mathfrak{P}$. Hence

$$\sum_{\mathfrak{P} \,|\, \mathfrak{p}} f(\mathfrak{P}/\mathfrak{p})\mathsf{v}_\mathfrak{P}(z) = \sum_{\mathfrak{P} \,|\, \mathfrak{p}} \mathsf{v}_\mathfrak{p}(\mathsf{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(z)) = \mathsf{v}_\mathfrak{p}\Big(\prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathsf{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(z)\Big) = \mathsf{v}_\mathfrak{p}(\mathsf{N}_{L/K}(z)),$$

and we obtain

$$\mathcal{N}_{S/R}(zS) = \prod_{\mathfrak{p}\in\mathcal{P}(R)} \mathfrak{p}^{\sum_{\mathfrak{P}\,|\,\mathfrak{p}} f(\mathfrak{P}/\mathfrak{p})\mathsf{v}_{\mathfrak{P}}(z)} = \prod_{\mathfrak{p}\in\mathcal{P}(R)} \mathfrak{p}^{\mathsf{v}_{\mathfrak{p}}(\mathsf{N}_{L/K}(z))} = \mathsf{N}_{L/K}(z)R\,.$$

3. (a) As the assignments $\mathfrak{A} \mapsto \mathcal{N}_{S_\mathfrak{p}/R_\mathfrak{p}}(\mathfrak{A}S_\mathfrak{p})$ and $\mathfrak{A} \mapsto \mathcal{N}_{S/R}(\mathfrak{A})R_\mathfrak{p}$ define homomorphisms $\mathcal{F}(S) \to \mathcal{F}(R_\mathfrak{p})$, it suffices to prove that $\mathcal{N}_{S_\mathfrak{p}/R_\mathfrak{p}}(\mathfrak{Q}S_\mathfrak{p}) = \mathcal{N}_{S/R}(\mathfrak{Q})R_\mathfrak{p}$ for all $\mathfrak{Q} \in \mathcal{P}(S)$. Thus let $\mathfrak{Q} \in \mathcal{P}(S)$, $\mathfrak{Q} \cap R = \mathfrak{q}$ and $f = f(\mathfrak{Q}/\mathfrak{q})$.

If $\mathfrak{q} \ne \mathfrak{p}$, then $\mathfrak{Q}S_\mathfrak{p} = S_\mathfrak{p}$, hence $\mathcal{N}_{S_\mathfrak{p}/R_\mathfrak{p}}(\mathfrak{Q}S_\mathfrak{p}) = R_\mathfrak{p}$, and $\mathcal{N}_{S/R}(\mathfrak{Q})R_\mathfrak{p} = \mathfrak{q}^f R_\mathfrak{p} = R_\mathfrak{p}$.

If $\mathfrak{q} = \mathfrak{p}$, then $\mathfrak{P}S_\mathfrak{p} \cap R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$ and $f = f(\mathfrak{P}S_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p})$ by Theorem 2.7.1. Hence we obtain $\mathcal{N}_{S_\mathfrak{p}/R_\mathfrak{p}}(\mathfrak{P}S_\mathfrak{p}) = (\mathfrak{p}R_\mathfrak{p})^f = \mathfrak{p}^f R_\mathfrak{p} = \mathcal{N}_{S/R}(\mathfrak{P})R_\mathfrak{p}$.

(b) We first deal with the different. Since the assignment $\mathfrak{A} \mapsto \mathfrak{A}R_\mathfrak{p} = \mathfrak{A}S_\mathfrak{p}$ defines a group homomorphism $\mathcal{F}(S) \to \mathcal{F}(S_\mathfrak{p})$, it suffices to prove that $\mathfrak{C}_{S_\mathfrak{p}/R_\mathfrak{p}} = \mathfrak{C}_{S/R}S_\mathfrak{p}$, for then $\mathfrak{D}_{S_\mathfrak{p}/R_\mathfrak{p}} = \mathfrak{C}_{S_\mathfrak{p}/R_\mathfrak{p}}^{-1} = \mathfrak{C}_{S/R}^{-1}S_\mathfrak{p} = \mathfrak{D}_{S/R}S_\mathfrak{p}$.

$\mathfrak{C}_{S_\mathfrak{p}/R_\mathfrak{p}} \subset \mathfrak{C}_{S/R}S_\mathfrak{p}$: Let $z \in \mathfrak{C}_{S_\mathfrak{p}/R_\mathfrak{p}}$. Since S is a finitely generated R-module, there exist some $m \in \mathbb{N}$ and $u_1, \ldots, u_m \in S$ such that $S = {}_R\langle u_1, \ldots, u_m\rangle$. Then $S_\mathfrak{p} = {}_{R_\mathfrak{p}}\langle u_1, \ldots, u_m\rangle$, and therefore $\mathsf{Tr}_{L/K}(zu_j) \in R_\mathfrak{p}$, say $\mathsf{Tr}_{L/K}(zu_j) = s^{-1}c_j$ for all $j \in [1,m]$, where $c_j \in R$ and $s \in R \setminus \mathfrak{p}$. Thus we obtain $\mathsf{Tr}_{L/K}(szu_j) = c_j \in R$ for all $j \in [1,m]$, hence $\mathsf{Tr}_{L/K}(szS) \subset R$, $sz \in \mathfrak{C}_{S/R}$ and $z \in (\mathfrak{C}_{S/R})_\mathfrak{p} = \mathfrak{C}_{S/R}S_\mathfrak{p}$.

$\mathfrak{C}_{S/R}S_\mathfrak{p} \subset \mathfrak{C}_{S_\mathfrak{p}/R_\mathfrak{p}}$: Let $s^{-1}z \in \mathfrak{C}_{S/R}S_\mathfrak{p} = (\mathfrak{C}_{S/R})_\mathfrak{p}$, where $z \in \mathfrak{C}_{S/R}$ and $s \in R \setminus \mathfrak{p}$. If $x = t^{-1}c \in S_\mathfrak{p}$, where $c \in S$ and $t \in R \setminus \mathfrak{p}$, then $\mathsf{Tr}_{L/K}(s^{-1}zt^{-1}c) = (st)^{-1}\mathsf{Tr}_{L/K}(zc) \in R_\mathfrak{p}$. Hence $\mathsf{Tr}_{L/K}(s^{-1}zS_\mathfrak{p}) \subset R_\mathfrak{p}$, and therefore $s^{-1}z \in \mathfrak{C}_{S_\mathfrak{p}/R_\mathfrak{p}}$.

Now we consider the discriminant. Obviously,

$$\mathfrak{d}_{S_\mathfrak{p}/R_\mathfrak{p}} = \mathcal{N}_{S_\mathfrak{p}/R_\mathfrak{p}}(\mathfrak{D}_{S_\mathfrak{p}/R_\mathfrak{p}}) = \mathcal{N}_{S_\mathfrak{p}/R_\mathfrak{p}}(\mathfrak{D}_{S/R}S_\mathfrak{p}) = \mathcal{N}_{S/R}(\mathfrak{D}_{S/R})R_\mathfrak{p} = \mathfrak{d}_{S/R}R_\mathfrak{p}\,.$$

For the evaluation of $\mathsf{v}_\mathfrak{p}(\mathfrak{d}_{S/R})$, we set

$$\mathfrak{D}_{S/R} = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} \mathfrak{P}^{\mathsf{v}_\mathfrak{P}(\mathfrak{D}_{S/R})}\mathfrak{A}\,, \quad \text{where} \quad \mathfrak{A} \in \mathcal{J}(S) \ \text{ and } \ \mathsf{v}_\mathfrak{P}(\mathfrak{A}) = 0 \ \text{ for all } \mathfrak{P}\,|\,\mathfrak{p}\,.$$

Then

$$\mathfrak{d}_{S/R} = \mathcal{N}_{S/R}(\mathfrak{D}_{S/R}) = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})\mathsf{v}_\mathfrak{P}(\mathfrak{D}_{S/R})}\mathcal{N}_{S/R}(\mathfrak{A})\,,$$

and the assertion follows since $\mathsf{v}_\mathfrak{p}(\mathcal{N}_{S/R}(\mathfrak{A})) = 0$.

4. Let $(u_1, \ldots, u_n)$ be an R-basis of S and $(u_1^*, \ldots, u_n^*)$ the dual basis of L/K. It suffices to prove that $\mathfrak{d}_{S/R}R_\mathfrak{p} = \Delta_{L/K}(u_1, \ldots, u_n)R_\mathfrak{p}$ for all $\mathfrak{p} \in \mathcal{P}(R)$.

Thus let $\mathfrak{p} \in \mathcal{P}(R)$. Then $S_\mathfrak{p}$ is a semilocal Dedekind domain, hence a principal ideal domain, and $(u_1, \ldots, u_n)$ is an $R_\mathfrak{p}$-basis of $S_\mathfrak{p}$. Hence $\mathfrak{C}_{S_\mathfrak{p}/R_\mathfrak{p}} = {}_{R_\mathfrak{p}}\langle u_1^*, \ldots, u_n^*\rangle$, and there exists some $\beta \in L^\times$ such that $\mathfrak{C}_{S_\mathfrak{p}/R_\mathfrak{p}} = \beta S_\mathfrak{p} = {}_{R_\mathfrak{p}}\langle \beta u_1, \ldots \beta u_n\rangle$. Let $T \in \mathsf{GL}_n(R_\mathfrak{p})$ be such that $(\beta u_1, \ldots, \beta u_n) = (u_1^*, \ldots, u_n^*)T$. Then

$$\begin{aligned}\Delta_{L/K}(\beta u_1, \ldots, \beta u_n) &= \mathsf{N}_{L/K}(\beta)^2\Delta_{L/K}(u_1, \ldots, u_n)\\ &= \Delta_{L/K}(u_1^*, \ldots, u_n^*)\det(T) = \Delta_{L/K}(u_1, \ldots, u_n)^{-1}\det(T)\,,\end{aligned}$$

hence $\Delta_{L/K}(u_1,\ldots,u_n)^2 = \mathsf{N}_{L/K}(\beta)^{-2}\det(T)$, and therefore

$$\begin{aligned}\Delta_{L/K}(u_1,\ldots,u_n)R_{\mathfrak p} &= \mathsf{N}_{L/K}(\beta)^{-1}R_{\mathfrak p} = \mathcal{N}_{S_{\mathfrak p}/R_{\mathfrak p}}(\beta^{-1}S_{\mathfrak p}) = \mathcal{N}_{S_{\mathfrak p}/R_{\mathfrak p}}(\mathfrak{D}_{S_{\mathfrak p}/R_{\mathfrak p}}) = \mathfrak{d}_{S_{\mathfrak p}/R_{\mathfrak p}}\\ &= \mathfrak{d}_{S/R/}R_{\mathfrak p}\,.\end{aligned}$$

5. If $S = R[\alpha]$ and $g \in R[X]$ is the minimal polynomial of α over K, then $\mathfrak{D}_{S/R} = g'(\alpha)S$, and therefore $\mathfrak{d}_{S/R} = \mathcal{N}_{S/R}(g'(\alpha)S) = \mathsf{N}_{L/K}(g'(\alpha))R = \Delta(g)R$. □

`different3`

Theorem 4.6.4. *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, $K \subset M \subset L$ finite separable extension fields, $S = \mathrm{cl}_L(R)$ and $T = \mathrm{cl}_M(R)$ [then $T = S \cap M$ and $S = \mathrm{cl}_L(T)$]. Then*

$$\mathfrak{D}_{S/R} = (\mathfrak{D}_{T/R}S)\mathfrak{D}_{S/T}\,, \quad \mathcal{N}_{S/R} = \mathcal{N}_{T/R}\circ\mathcal{N}_{S/T} \quad \textit{and} \quad \mathfrak{d}_{S/R} = \mathcal{N}_{T/R}(\mathfrak{d}_{S/T})\mathfrak{d}_{T/R}^{[L:M]}\,.$$

Proof. 1. We prove first that $\mathfrak{C}_{S/R} = (\mathfrak{C}_{T/R}S)\mathfrak{C}_{S/T}$. Since the assignment $\mathfrak{B} \mapsto \mathfrak{B}S$ defines a group homomorphism $\mathcal{F}(T) \to \mathcal{F}(S)$, this implies

$$\mathfrak{D}_{S/R} = \mathfrak{C}_{S/R}^{-1} = (\mathfrak{C}_{T/R}S)^{-1}\mathfrak{C}_{S/T}^{-1} = (\mathfrak{C}_{T/R}^{-1}S)\mathfrak{C}_{S/T}^{-1} = (\mathfrak{D}_{T/R}S)\mathfrak{D}_{S/T}\,.$$

$\mathfrak{C}_{S/R} \subset (\mathfrak{C}_{T/R}S)\mathfrak{C}_{S/T}$: Let $x \in \mathfrak{C}_{S/R}$. Then

$$R \supset \mathsf{Tr}_{L/K}(xS) = \mathsf{Tr}_{L/K}(xST) = \mathsf{Tr}_{M/K}(\mathsf{Tr}_{L/M}(xS)T) \quad \text{implies} \quad \mathsf{Tr}_{L/M}(xS) \subset \mathfrak{C}_{T/R}\,,$$

$T = \mathfrak{C}_{T/R}^{-1}\mathfrak{C}_{T/R} \supset \mathfrak{C}_{T/R}^{-1}\mathsf{Tr}_{L/M}(xS) = \mathsf{Tr}_{L/M}(x\mathfrak{C}_{T/R}^{-1}S)$ implies $x\mathfrak{C}_{T/R}^{-1} \subset \mathfrak{C}_{S/T}$, and therefore $x \in \mathfrak{C}_{T/R}\mathfrak{C}_{S/T} = (\mathfrak{C}_{T/R}S)\mathfrak{C}_{S/T}$.

$(\mathfrak{C}_{T/R}S)\mathfrak{C}_{S/T} \subset \mathfrak{C}_{S/R}$: Let $x \in \mathfrak{C}_{T/R}$ and $z \in \mathfrak{C}_{S/T}$. Then

$$\mathsf{Tr}_{L/K}(xzS) = \mathsf{Tr}_{M/K}(x\mathsf{Tr}_{L/M}(zS)) \subset \mathsf{Tr}_{M/K}(xT) \subset R \quad \text{implies} \quad xz \in \mathfrak{C}_{S/R}\,,$$

and therefore $(\mathfrak{C}_{T/R}S)\mathfrak{C}_{S/T} = {}_{\mathbb{Z}}\langle\{xz \mid x \in \mathfrak{C}_{T/R},\ z \in \mathfrak{C}_{S/T}\}\rangle \subset \mathfrak{C}_{S/R}$.

2. Since $\mathcal{N}_{S/R}$ and $\mathcal{N}_{T/R}\circ\mathcal{N}_{S/T}$ are homomorphisms $\mathcal{F}(S) \to \mathcal{F}(R)$, it suffices to prove that $\mathcal{N}_{S/R}(\mathfrak{P}) = \mathcal{N}_{T/R}\circ\mathcal{N}_{S/T}(\mathfrak{P})$ for all $\mathfrak{P} \in \mathcal{P}(S)$. Thus let $\mathfrak{P} \in \mathcal{P}(S)$, $\mathfrak{q} = \mathfrak{P} \cap T$ and $\mathfrak{p} = \mathfrak{P} \cap R$. Then $\mathfrak{p} = \mathfrak{q} \cap R$, and $\mathcal{N}_{T/R}\circ\mathcal{N}_{S/T}(\mathfrak{P}) = \mathcal{N}_{T/R}(\mathfrak{q}^{f(\mathfrak{P}/\mathfrak{q})}) = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{q})} = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})} = \mathcal{N}_{S/R}(\mathfrak{P})$.

3. By 1. and 2, we obtain

$$\begin{aligned}\mathfrak{d}_{S/R} &= \mathcal{N}_{S/R}(\mathfrak{D}_{S/R}) = \mathcal{N}_{S/R}(\mathfrak{D}_{T/R}S)\mathcal{N}_{S/R}(\mathfrak{D}_{S/T})\\ &= \mathcal{N}_{T/R}(\mathcal{N}_{S/T}(\mathfrak{D}_{T/R}S))\mathcal{N}_{T/R}(\mathcal{N}_{S/T}(\mathfrak{D}_{S/T}) = \mathcal{N}_{T/R}(\mathfrak{D}_{T/R}^{[L:M]})\mathcal{N}_{T/R}(\mathfrak{d}_{S/T})\\ &= \mathfrak{d}_{T/R}^{[L:M]}\mathcal{N}_{T/R}(\mathfrak{d}_{S/T})\,. \quad \square\end{aligned}$$

`different4`

Theorem 4.6.5. *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite separable extension and $S = \mathrm{cl}_L(R)$.*

1. *If $\mathfrak{P} \in \mathcal{P}(S)$ and $\mathfrak{P} \cap R = \mathfrak{p}$, then $\mathfrak{D}_{S/R}\widehat{S}_{\mathfrak P} = \mathfrak{D}_{\widehat{S}_{\mathfrak P}/\widehat{R}_{\mathfrak p}}$.*
2. *If $\mathfrak{p} \in \mathcal{P}(R)$, then*

$$\mathcal{N}_{S/R}(\mathfrak{A})\widehat{R}_{\mathfrak p} = \prod_{\mathfrak{P}\,|\,\mathfrak{p}}\mathcal{N}_{\widehat{S}_{\mathfrak P}/\widehat{R}_{\mathfrak p}}(\mathfrak{A}\widehat{S}_{\mathfrak P}) \quad \textit{for all } \mathfrak{A} \in \mathcal{F}(S), \textit{ and} \quad \mathfrak{d}_{S/R}\widehat{R}_{\mathfrak p} = \prod_{\mathfrak{P}\,|\,\mathfrak{p}}\mathfrak{d}_{\widehat{S}_{\mathfrak P}/\widehat{R}_{\mathfrak p}}\,,$$

where the products run over all $\mathfrak{P} \in \mathcal{P}(S)$ such that $\mathfrak{P}\,|\,\mathfrak{p}$.

Proof. 1. Let $\mathfrak{P} \in \mathcal{P}(S)$ and $\mathfrak{p} = \mathfrak{P} \cap R$. Then $\mathfrak{D}_{S/R}S_{\mathfrak{p}} = \mathfrak{D}_{S_{\mathfrak{p}}/R_{\mathfrak{p}}}$, and $\widehat{S}_{\mathfrak{P}} = (\widehat{S_{\mathfrak{p}}})_{\mathfrak{P}S_{\mathfrak{p}}}$. Hence it suffices to prove the formula for $R_{\mathfrak{p}}$ instead of R, and we may assume that $R = R_{\mathfrak{p}}$ is a dv-domain.

Suppose that $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}$, where $r \in \mathbb{N}$, $\mathfrak{P} = \mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathfrak{P}(S)$ are distinct and $e_1, \ldots, e_r \in \mathbb{N}$. Then $\mathcal{P}(S) = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$. Let $|\cdot|_{\mathfrak{p}} \colon K \to \mathbb{R}_{\geq 0}$ be a $\mathfrak{p}$-adic absolute value of K, and for $i \in [1, r]$ let $|\cdot|_{\mathfrak{P}_i} \colon L \to \mathbb{R}_{\geq 0}$ be the $\mathfrak{P}_i$-adic absolute value of L such that $|\cdot|_{\mathfrak{P}_i} \restriction K = |\cdot|_{\mathfrak{p}}$ (see Theorem dedekindext 4.5.3). Let $(K_{\mathfrak{p}}, |\cdot|_{\mathfrak{p}})$ be a completion of $(K, |\cdot|)$ and $(L_{\mathfrak{P}_i}, |\cdot|_{\mathfrak{P}_i})$ a completion of $(L, |\cdot|_{\mathfrak{P}_i})$ such that $K_{\mathfrak{p}} \subset L_{\mathfrak{P}_i}$. Then the map $\mathsf{Tr}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}} \colon L_{\mathfrak{P}_i} \to K_{\mathfrak{p}}$ is continuous,

$$\mathsf{Tr}_{L/K}(x) = \sum_{i=1}^{r} \mathsf{Tr}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(x) \quad \text{for all} \quad x \in L\,,$$

and the image of the diagonal embedding $\delta \colon L \to L_{\mathfrak{P}_1} \times \ldots \times L_{\mathfrak{P}_r}$ is dense. In particular, for every $(y_1, \ldots, y_r) \in L_{\mathfrak{P}_1} \times \ldots \times L_{\mathfrak{P}_r}$ there is a sequence $(x_n)_{n \geq 0}$ in L such that $(x_n)_{n\geq 0} \overset{|\cdot|_{\mathfrak{P}_i}}{\to} y_i$ for all $i \in [1, r]$.

After these preparations we come to the actual proof. It suffices to show that $\mathfrak{C}_{S/R}$ is a dense subset of $\mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}$. Indeed, since $\mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}} \in \mathcal{F}(\widehat{S}_{\mathfrak{P}})$, it follows that $\mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}} \subset L_{\mathfrak{P}}$ is closed, and we obtain $\mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}} \subset \overline{\mathfrak{C}_{S/R}} = \mathfrak{C}_{S/R}\widehat{S}_{\mathfrak{P}} \subset \mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}$, hence $\mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}} = \mathfrak{C}_{S/R}\widehat{S}_{\mathfrak{P}}$, and $\mathfrak{D}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}} = \mathfrak{C}^{-1}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}} = (\mathfrak{C}_{S/R}\widehat{S}_{\mathfrak{P}})^{-1} = \mathfrak{C}^{-1}_{S/R}\widehat{S}_{\mathfrak{P}} = \mathfrak{D}_{S/R}\widehat{S}_{\mathfrak{P}}$.

$\mathfrak{C}_{S/R} \subset \mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}$: Let $x \in \mathcal{C}_{S/R}$. We must prove that $\mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy) \in \widehat{R}_{\mathfrak{p}}$ for all $y \in \widehat{S}_{\mathfrak{P}}$. Thus suppose that $y \in \widehat{S}_{\mathfrak{P}}$, and let $(y_n)_{n\geq 0}$ be a sequence in L such that $(y_n)_{n\geq 0} \overset{|\cdot|_{\mathfrak{P}}}{\to} y$ and $(y_n)_{n\geq 0} \overset{|\cdot|_{\mathfrak{P}_j}}{\to} 0$ for all $j \in [2, r]$. For all $i \in [1, r]$, $\widehat{S}_{\mathfrak{P}_i} \subset L_{\mathfrak{P}_i}$ is open, and thus we obtain $y_n \in \widehat{S}_{\mathfrak{P}_i} \cap L = S_{\mathfrak{P}_i}$ for all $n \gg 1$. Hence it follows that $y_n \in S_{\mathfrak{P}_1} \cap \ldots \cap S_{\mathfrak{P}_r} = S$ for all $n \gg 1$. Now

$$\mathsf{Tr}_{L/K}(xy_n) = \mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy_n) + \sum_{j=2}^{r} \mathsf{Tr}_{L_{\mathfrak{P}_j}/K_{\mathfrak{p}}}(xy_n) \in R = R_{\mathfrak{p}} \quad \text{for all } n \gg 1,$$

$(\mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy_n))_{n\geq 0} \overset{|\cdot|_{\mathfrak{p}}}{\to} \mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy)$ and $(\mathsf{Tr}_{L_{\mathfrak{P}_j}/K_{\mathfrak{p}}}(xy_n))_{n\geq 0} \overset{|\cdot|_{\mathfrak{p}}}{\to} 0$ for all $j \in [2, r]$, and therefore

$$\mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy) = |\cdot|_{\mathfrak{p}}\text{-}\lim_{n\to\infty} \mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy_n) \in \overline{R} = \widehat{R}_{\mathfrak{p}}\,.$$

$\mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}} \subset \overline{\mathfrak{C}_{S/R}}$: Let $x \in \mathfrak{C}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}$ and $(x_n)_{n\geq 0}$ a sequence in L such that $(x_n)_{n\geq 0} \overset{|\cdot|_{\mathfrak{P}}}{\to} x$ and $(x_n)_{n\geq 0} \overset{|\cdot|_{\mathfrak{P}_j}}{\to} 0$ for all $j \in [2, r]$. Let $u_1, \ldots, u_m \in S$ be such that $S = {}_R\langle u_1, \ldots, u_m\rangle$. Then it follows that $\widehat{S}_{\mathfrak{P}} = S\widehat{R}_{\mathfrak{p}} = {}_{\widehat{R}_{\mathfrak{p}}}\langle u_1, \ldots, u_m\rangle$ (inside $L_{\mathfrak{P}}$), and therefore

$$\mathsf{Tr}_{L/K}(x_n u_\mu) = \mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x_n u_\mu) + \sum_{j=2}^{r} \mathsf{Tr}_{L_{\mathfrak{P}_j}/K_{\mathfrak{p}}}(x_n u_\mu) \quad \text{for all } n \geq 0 \text{ and } \mu \in [1, m].$$

Since $(\mathsf{Tr}_{L_{\mathfrak{P}_j}/K_{\mathfrak{p}}}(x_n u_\mu))_{n\geq 0} \overset{|\cdot|_{\mathfrak{p}}}{\to} 0$ for all $j \in [2, r]$ and $(\mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x_n u_\mu))_{n\geq 0} \overset{|\cdot|_{\mathfrak{p}}}{\to} \mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xu_\mu)$, it follows that $((\mathsf{Tr}_{L/K}(x_n u_\mu))_{n\geq 0} \overset{|\cdot|_{\mathfrak{p}}}{\to} \mathsf{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xu_\mu) \in \widehat{R}_{\mathfrak{p}}$ for all $\mu \in [1, m]$. Since $\widehat{R}_{\mathfrak{p}} \subset K_{\mathfrak{p}}$

is open, it follows that $\mathsf{Tr}_{L/K}(x_n u_\mu) \in \widehat{R}_{\mathfrak{p}} \cap K = R_{\mathfrak{p}} = R$ for all $n \gg 1$ and all $\mu \in [1, m]$, which implies that $\mathsf{Tr}_{L/K}(x_n S) \subset R$ and thus $x_n \in \mathfrak{C}_{S/R}$ for all $n \gg 1$. Consequently, we obtain $x \in \overline{\mathfrak{C}_{S/R}}$.

2. Let $\mathfrak{p} \in \mathcal{P}(R)$ and $\mathfrak{A} \in \mathcal{F}(S)$. Since $S_{\mathfrak{p}}$ is a principal ideal domain, we obtain $\mathfrak{A}S_{\mathfrak{p}} = xS_{\mathfrak{p}}$ for some $x \in L$ and, by Theorem 4.6.3,

$$\begin{aligned}\mathcal{N}_{S/R}(\mathfrak{A})\widehat{R}_{\mathfrak{p}} = \mathcal{N}_{S/R}(\mathfrak{A})R_{\mathfrak{p}}\widehat{R}_{\mathfrak{p}} = \mathcal{N}_{S_{\mathfrak{p}}/R_{\mathfrak{p}}}(xS_{\mathfrak{p}})\widehat{R}_{\mathfrak{p}} = \mathsf{N}_{L/K}(x)\widehat{R}_{\mathfrak{p}} \\ = \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathsf{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x)\widehat{R}_{\mathfrak{p}} = \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathcal{N}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}(x\widehat{S}_{\mathfrak{P}}) = \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathcal{N}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}(\mathfrak{A}\widehat{S}_{\mathfrak{P}})\,.\end{aligned}$$

Hence we obtain

$$\mathfrak{d}_{S/R}\widehat{R}_{\mathfrak{p}} = \mathcal{N}_{S/R}(\mathfrak{D}_{S/R})\widehat{R}_{\mathfrak{p}} = \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathcal{N}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}(\mathfrak{D}_{S/R}\widehat{S}_{\mathfrak{P}}) = \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathcal{N}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}(\mathfrak{D}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}) = \prod_{\mathfrak{P} \,|\, \mathfrak{p}} \mathfrak{d}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}}\,. \qquad \square$$

Theorem 4.6.6. *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite separable extension, $S = \mathrm{cl}_L(R)$, $\mathfrak{P} \in \mathcal{P}(S)$, $\mathfrak{p} = \mathfrak{P} \cap R$, and $e = e(\mathfrak{P}/\mathfrak{p})$. Assume that the residue class extension $R/\mathfrak{p} \subset S/\mathfrak{P}$ is separable. Then $\mathsf{v}_{\mathfrak{P}}(\mathfrak{D}_{S/R}) \ge e-1$, and equality holds if and only if $\mathrm{char}(R/\mathfrak{p}) \nmid e$.*

In particular, $\mathfrak{P}/\mathfrak{p}$ is ramified if and only if $\mathsf{v}_{\mathfrak{P}}(\mathfrak{D}_{S/R}) > 0$, and $\mathfrak{p}$ is ramified in L if and only if $\mathsf{v}_{\mathfrak{p}}(\mathfrak{d}_{S/R}) > 0$.

Proof. We consider the local completion $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ (see Theorem 4.5.3). Since $\mathsf{k}_{K_{\mathfrak{p}}} = R/\mathfrak{p}$, $\mathsf{k}_{L_{\mathfrak{P}}} = S/\mathfrak{P}$, $\mathsf{v}_{\mathfrak{P}}(\mathfrak{D}_{S/R}) = \mathsf{v}_{\mathfrak{P}}(\mathfrak{D}_{S/R}\widehat{S}_{\mathfrak{P}}) = \mathsf{v}_{\mathfrak{P}}(\mathfrak{D}_{\widehat{S}_{\mathfrak{P}}/\widehat{R}_{\mathfrak{p}}})$ and $e = e(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, the subsequent local result Theorem 4.6.7 implies $\mathsf{v}_{\mathfrak{P}}(\mathfrak{D}_{S/R}) \ge e-1$, and equality holds if and only if $\mathrm{char}(R/\mathfrak{p}) \nmid e$.

$\mathfrak{P}/\mathfrak{p}$ is ramified if and only if $e = 1$, and this holds if and only if $\mathsf{v}_{\mathfrak{P}}(\mathfrak{D}_{S/R}) = 0$. Hence $\mathfrak{p}$ is ramified in L if and only if $\mathsf{v}_{\mathfrak{P}'}(\mathfrak{D}_{S/R}) > 0$ for some $\mathfrak{P}' \in \mathcal{P}(S)$ such that $\mathfrak{P}' \,|\, \mathfrak{p}$, and by Theorem 4.6.3 this hold if and only if $\mathsf{v}_{\mathfrak{p}}(\mathfrak{d}_{S/R}) > 0$. $\square$

Theorem 4.6.7. *Let L/K be a finite separable extension of discrete valued complete fields with valuation domains $\mathcal{O}_K$ and $\mathcal{O}_L = \mathrm{cl}_L(\mathcal{O}_K)$. Keep all notations of* Definition 4.4.2 and Theorem 4.4.3.*, and assume that $e = e(L/K)$ and $\mathsf{k}_L/\mathsf{k}_K$ is separable.*

Then $\mathsf{v}_L(\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}) \ge e-1$, and equality holds if and only if $\mathrm{char}(R/\mathfrak{p}) \nmid e$.

Proof. CASE 1: L/K is unramified. By Theorem 4.4.7, there exists some $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, and if $g \in \mathcal{O}_K[X]$ denotes the minimal polynomial of α over K, then the residue class polynomial $\overline{g} \in \mathsf{k}_K[X]$ is separable. In particular, $\overline{g'(\alpha)} = \overline{g}\,'(\alpha) \ne 0$, hence $g'(\alpha) \in \mathcal{O}_L^\times$, and $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K} = g'(\alpha)\mathcal{O}_L = \mathcal{O}_L$.

CASE 2: L/K is fully ramified. By Theorem 4.4.6, $[L:K] = e$, s$\mathcal{O}_L = \mathcal{O}_K[\pi]$, where $\pi \in K$, $v_L(\pi) = 1$, and the minimal polynomial $g \in \mathcal{O}_K[X]$ of π over K is an Eisenstein polynomial. Suppose that $g = X^e + a_{e-1}X^{e-1} + \ldots + a_1X + a_0$, where $v_K(a_0) = 1$ and $v_K(a_i) \ge 1$ for all $i \in [1, e-1]$. Then

$$g'(\pi) = e\pi^{e-1} + \sum_{i=1}^{e} ia_i\pi^{i-1}\,, \quad \text{and} \quad \mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K} = g'(\pi)\mathcal{O}_L\,.$$

For all $i \in [1, e-1]$ we have $v_L(ia_i\pi^{i-1}) = ev_K(ia_i) + i - 1 \geq e$, and since

$$v_L(e\pi^{e-1}) = v_L(e1_K) + e - 1 = \begin{cases} e-1 & \text{if} \quad \mathrm{char}(\mathsf{k}_K) \nmid e\,, \\ \quad \geq e & \text{if} \quad \mathrm{char}(\mathsf{k}_K) \mid e\,, \end{cases}$$

we obtain $v_L(g'(\pi)) = e-1$ if $\mathrm{char}(\mathsf{k}_K) \nmid e$, and $v_L(g'(\pi)) \geq e$ if $\mathrm{char}(\mathsf{k}_K) \mid e$.

GENERAL CASE: By Theorem `inertiafield` 4.4.9, there exists an intermediate field $K \subset T \subset L$ such that T/K is unramified, L/T is fully ramified and $[L:T] = e$. By Theorem `different3` 4.6.4 we obtain $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K} = \mathfrak{D}_{\mathcal{O}_T/\mathcal{O}_K}\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_T} = \mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_T}$, and the assertion follows by CASE 2. □

Corollary 4.6.8. *Let R be a Dedekind domain, $K = \mathsf{q}(R)$, L/K a finite separable extension, $S = \mathrm{cl}_L(R)$, and suppose that all residue class fields $R/\mathfrak{p}$ for $\mathfrak{p} \in \mathcal{P}(R)$ are perfect. Then $\mathfrak{p} \in \mathcal{P}(R)$ ramifies in L if and only if $\mathsf{v}_\mathfrak{p}(\mathfrak{d}_{S/R}) > 0$. In particular, only finitely many $\mathfrak{p} \in \mathcal{P}(R)$ ramify in L.*

Proof. Obvious by Theorem `differentvalue` 4.6.6. □

Definition 4.6.9. Let L/K be a finite extension of algebraic number fields of of discrete valued complete fields. Then we call

$\mathfrak{D}_{L/K} = \mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$ the *different of* L/K and $\mathfrak{d}_{L/K} = \mathfrak{d}_{\mathcal{O}_L/\mathcal{O}_K}$ the *discriminant of* L/K.

Theorem 4.6.10. *Let K be an algebraic number field.*

1. $\mathfrak{d}_{K/\mathbb{Q}} = \Delta_K\mathbb{Z}$.
2. *Let $p \in \mathbb{P}$ be a prime. Then p ramifies in K if and only if $p \mid \Delta_K$.*
3. *At least one and at most finitely many primes ramify in K.*

Proof. 1. By Theorem `different2` 4.6.3.4, observing Definition `integralbasis` 2.2.1.

2. By Theorem `differentvalue` 4.6.6.

3. By 2. and Theorem `hermite` 3.2.4. □

CHAPTER 5

Exercises

1. Let $K \subset L$, $M \subset \overline{K}$ be fields, and suppose that $\overline{K}/K$ is algebraic.

a) If L/K is normal, then LM/M is normal.

b) If L/K and M/K are normal, then LM/K and $L \cap M/K$ are normal.

c) Assume that $K \subset L \subset M$. If M/K is normal, then M/L is normal. If M/L and L/K are both normal, then M/K need not be normal (give an example where $[M:K] = 4$).

2. The sequences $(u_n)_{n\geq 1}$ and $(v_n)_{n\geq 1}$ in $\mathbb{R}$ are recursively defined by

$$u_1 = -2\,, \quad v_1 = 0\,, \quad u_{n+1} = \sqrt{2+u_n}\,, \quad v_{n+1} = \sqrt{2-u_n}\,.$$

For all $n \in \mathbb{N}$, the number $\zeta = \frac{1}{2}(u_n + \mathrm{i}v_n)$ is a primitive 2^n-th root of unity.

3. Show that $\mathbb{Q}^{(5)} = \mathbb{Q}(\sqrt{-10-2\sqrt{5}}\,)$, $\mathbb{Q}^{(6)} = \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}^{(8)} = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$. Determine the splitting field L and its degree $[L:\mathbb{Q}]$ for the following polynomials:

a) $X^4 - 2$; **b)** $X^4 + 4$; **c)** $X^5 - 5$ **d)** $X^{10} - 5$; **e)** $X^8 - 3$; **f)** $X^8 - 2$.

4. Let K be a field and $n \in \mathbb{N}$.

a) $\mu_n^*(K) \neq \emptyset \iff |\mu_n(K)| = n \iff |\mu_n^*(K)| = \varphi(n)$.

b) If $\mu_n^*(K) \neq \emptyset$, then $X^n - 1 \in K[X]$ is separable and $\operatorname{char}(K) \nmid n$.

c) If $\operatorname{char}(K) = p > 0$ and $n = p^d m$, where $d \in \mathbb{N}_0$, $m \in \mathbb{N}$ and $p \nmid m$, then $\mu_n(K) = \mu_m(K)$.

d) Let p be a prime, and let $f \in \mathbb{N}$ be minimal such that $p^f \equiv 1 \mod n$. Then $f \mid \varphi(n)$, and $\mathbb{F}_{p^f}$ is the splitting field of $X^n - 1$ over $\mathbb{F}_p$.

5. The Möbius function $\mu \colon \mathbb{N} \to \mathbb{C}$ is defined by

$$\mu(n) = \begin{cases} (-1)^r & \text{if} \quad n = p_1 \cdot \ldots \cdot p_r\,, \text{ where } r \in \mathbb{N}_0 \text{ and } p_1, \dots p_r \text{ are distinct primes,} \\ 0 & \text{if} \quad \text{there exists a prime } p \text{ such that } p^2 \mid n. \end{cases}$$

a) If $n \in \mathbb{N}$, then

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if} \quad n = 1\,, \\ 0 & \text{if} \quad n > 1\,. \end{cases} \quad \text{[Hint: First do the case where } n \text{ is a prime power]}$$

b) Let F, $f \colon \mathbb{N} \to \mathbb{C}$ be functions. Then:

$$F(n) = \sum_{d|n} f(d) \ \text{ for all } n \in \mathbb{N} \iff f(n) = \sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) \ \text{ for all } n \in \mathbb{N}.$$

c) For all $n \in \mathbb{N}$,

$$n = \sum_{d|n} \varphi(d)\,, \quad \frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d} \quad \text{and} \quad \Phi_n = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}\,.$$

5. Let q be a prime power. For $n \in \mathbb{N}$, let $\mathcal{F}_q(n)$ be the set of all monic irreducible polynomials $f \in \mathbb{F}_q[X]$ such that $\deg(f) = n$, and $\psi_q(n) = |\mathcal{F}_q(n)|$.

a) If $f \in \mathbb{F}_q[X]$, then $f \mid X^{q^n} - X$ if and only if $\deg(f) \mid n$, and

$$X^{q^n} - X = \prod_{d \mid n} \prod_{f \in \mathcal{F}_q(n)} f\,.$$

b) Let μ denote the Möbius function. Then, for all $n \in \mathbb{N}$,

$$q^n = \sum_{d \mid n} d\psi_q(d) \quad \text{and} \quad \psi_q(n) = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}\,.$$

6. Let K be a field and Λ the set of all irreducible monic irreducible polynomials $f \in K[X] \setminus K$. Let $\boldsymbol{X} = (X_f)_{f \in \Lambda}$ be a family of indeterminates indexed by Λ, $K[\boldsymbol{X}]$ the polynomial ring and $\mathfrak{a} = {}_{K[\boldsymbol{X}]}\langle \{ f(X_f) \mid f \in \Lambda \} \rangle \lhd K[\boldsymbol{X}]$. Then $\mathfrak{a} \neq K[\boldsymbol{X}]$, and if $\mathfrak{m} \lhd K[\boldsymbol{X}]$ is a maximal ideal such that $\mathfrak{a} \subset \mathfrak{m}$, then $\overline{K} = K[\boldsymbol{X}]/\mathfrak{m}$ is a field, and there is a (natural) monomorphism $K \to \overline{K}$. If we identify K with its image in $\overline{K}$, then $\overline{K} \supset K$ is an extension field, and every $f \in K[X] \setminus K$ has a zero in $\overline{K}$.

7. Let $\overline{K}/K$ be an algebraic field extension such that every polynomial $f \in K[X] \setminus K$ has a zero in $\overline{K}$. Then $\overline{K}$ is an algebraic closure of K (first do the separable case and use the Primitive Element Theorem). Together with **6.** this gives a new proof for the existence of an algebraic closure (did you use Zorn's Lemma?).

8. a) A finite separable field extension has only finitely many intermediate fields. This is not true for inseparable extensions.

b) Let $L \subset \mathbb{C}$ be a subfield. If $L/\mathbb{Q}$ is normal, then either $L \subset \mathbb{R}$ or $L_0 = L \cap \mathbb{R}$ is a subfield such that $[L : L_0] = 2$.

9. Let $m,\, n \in \mathbb{N}$, $d = \gcd(m,n)$ and $e = \operatorname{lcm}(m,n)$. Then $\mathbb{Q}^{(e)} = \mathbb{Q}^{(m)}\mathbb{Q}^{(n)}$ and $\mathbb{Q}^{(d)} = \mathbb{Q}^{(m)} \cap \mathbb{Q}^{(n)}$. Hint: Use Galois theory and the formula

$$\varphi(n) = n \prod_{p \mid n} \Bigl(1 - \frac{1}{p}\Bigr)\,.$$

10. Let K be a field and $n \in \mathbb{N}$ such that $\operatorname{char}(K) \nmid n$ and $\mu_n^*(K) \neq \emptyset$. If $a,\, b \in K^\times$, then $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$ if and only if $b = a^j c^n$ for some $c \in K^\times$ and $j \in [0, n-1]$ such that $(j,n) = 1$. Hint: Use the canonical monomorphisms $\mathsf{Gal}(K(\sqrt[n]{a})/K) \to \mu_n(K)$ and $\mathsf{Gal}(K(\sqrt[n]{b})/K) \to \mu_n(K)$.

11. Let $K = \mathbb{Q}^{(3)} = \mathbb{Q}(\sqrt{-3})$, $\theta \in \mathbb{C}$, $\theta^3 = z \in K^\times \setminus K^{\times 3}$ and $N = K(\theta)$ $[\,N = K(\sqrt[3]{z})$ for short$\,]$. Then N/K is cyclic, $[N : K] = 3$ and $[N : \mathbb{Q}] = 6$.

a) $N/\mathbb{Q}$ is galois if and only if $\overline{z} = z^j b^3$ for some $j \in \{1, 2\}$ and $b \in K^\times$ (use Exercise **10**). In fact, $N/\mathbb{Q}$ is cyclic if $j = 2$, and $\mathsf{Gal}(N/\mathbb{Q}) \cong \mathfrak{S}_3$ if $j = 1$. Then either $N \cap \mathbb{R} = \mathbb{Q}(\theta + \overline{\theta})$, or $j = 1$ and $N \cap \mathbb{R} = \mathbb{Q}(\theta^2)$.

b) Let $L/\mathbb{Q}$ be a cyclic extension and $[L : \mathbb{Q}] = 3$. Then there exists some $\alpha \in \mathbb{Z}[\sqrt{-3}\,]$ such that $L = \mathbb{Q}(\sqrt[3]{\alpha^2\overline{\alpha}} + \sqrt[3]{\alpha\overline{\alpha}^2}\,)$. Conclude that $L/\mathbb{Q}$ is a cyclic extension of degree 3 if and only if there exist $a,\, b,\, m \in \mathbb{Z}$ such that $m = a^2 + 3b^2$, $mab \neq 0$, and L is the splitting field of $X^3 - 3mX + 2ma$. Hint: If L is the splitting field of a polynomial $X^3 + pX + q$, then $[L : \mathbb{Q}] = 3$ if and only if $-4p^3 - 27q^2 \in \mathbb{Q}^{\times 2}$.

12. Let p be a prime and L the splitting field of $X^4 - p$ (over $\mathbb{Q}$). Determine $\mathsf{Gal}(L/\mathbb{Q})$ and all intermediate fields of $L/\mathbb{Q}$.

13. Let K be an algebraic number field, $[K:\mathbb{Q}] = n$, and for $f \in \mathbb{N}$, set $\mathcal{O}_{K,f} = \mathbb{Z} + f\mathcal{O}_K$. Then $\mathcal{O}_{K,f}$ is an order in K, and $(\mathcal{O}_K:\mathcal{O}_{K,f}) = f^{n-1}$.

Assume now that $n = 2$ and $\omega = \frac{\Delta_K + \sqrt{\Delta_K}}{2}$.

a) $(1, f\omega)$ is a basis of $\mathcal{O}_{K,f}$, and $\Delta(\mathcal{O}_{K,f}) = Df^2$.

b) If $R \subset K$ is any order and $(\mathcal{O}_K:R) = f$, then $R = \mathcal{O}_{K,f}$.

14. Let $K = \mathbb{Q}(\alpha)$, where α is a zero of the (irreducible!) polynomial $X^3 - X - 4$. Then $(1, \alpha, \frac{\alpha+\alpha^2}{2})$ is an integral basis of K. Hint: It suffices to prove that $\frac{\alpha+\alpha^2}{2} \in \mathcal{O}_K$ (why?)

15. Let K be an algebraic number field, $M \subset \mathcal{O}_K$ a complete module and $D = \Delta(M)$. Then $D \in \mathbb{Z}$, and $D \equiv 0$ or $1 \bmod 4$ (in particular, this holds for $D = \Delta_K$). Hint: The defining determinant is of the form $(P - N)^2$.

16. a) Let $F \subset K \subset L$ be fields such that $\operatorname{char}(K) \ne 2$, $[L:K] = [K:F] = 2$, and $L = K(\sqrt{\alpha}\,)$ for some $\alpha \in K^\times$. Then L/F is galois if and only if $\mathsf{N}_{K/F}(\alpha) \in K^{\times 2}$, and L/F is cyclic if and only if $\mathsf{N}_{K/F}(\alpha) \in K^{\times 2} \setminus F^{\times 2}$.

b) Let $F \subset K$ be fields such that $\operatorname{char}(K) \ne 2$ and $K = F(\sqrt{D}\,)$ for some $D \in F \setminus F^\times$. Then K can be embedded into a field L such that L/F is cyclic of degree 4 if and only if D is the sum of two squares in F. Discuss the consequences for quadratic number fields.

17. Let K be a field, $n \in \mathbb{N}$ and $a \in K^\times$. Then the polynomial $X^n - a$ is irreducible over K if and only if the following conditions are fulfilled:

- $a \notin K^p$ for all primes p dividing n;
- $a \notin -4K^4$ if $4 \,|\, n$

(Theorem of Capelli).

18. Let p be an odd prime. Determine an integral basis of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

19. An algebraic number field K is called a *pure cubic field* if $K = \mathbb{Q}(\sqrt[3]{m})$ for some $m \in \mathbb{Q} \setminus \mathbb{Q}^3$. If K is a pure cubic field, then there exist unique integers a, $b \in \mathbb{N}$ such that ab is squarefree, $m = ab^2$ and $K = \mathbb{Q}(\sqrt[3]{m})$. If it is in this form and $\theta = \sqrt[3]{m}$, then:

- If $m \not\equiv \pm 1 \bmod 9$, then $\bigl(1, \theta, \frac{\theta^2}{b}\bigr)$ is an integral basis of K, and $\Delta_K = -27(ab)^2$.
- If $m \equiv e \bmod 9$, where $e \in \{\pm 1\}$, then $\bigl(1, \frac{\theta^2}{b}, \frac{1+e\theta+\theta^2}{3}\bigr)$ is an integral basis of K, and $\Delta_K = -3(ab)^2$.

19. Let $p \in \mathbb{P} \setminus 2$ be an odd prime.

a) If $p \ne 3$, then 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \bmod 12$, and -3 is a quadratic residue modulo p if and only if $p \equiv 1 \bmod 3$.

b) Do the same for 5 instead of 3.

20. Let $m \in \mathbb{N}$, $m = 2^e p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \ge 2$, where r, $e \in \mathbb{N}_0$, $p_1, \ldots, p_r \in \mathbb{P} \setminus \{2\}$ are distinct odd primes, and $e_1, \ldots, e_r \in \mathbb{N}$. If $a \in \mathbb{Z}$ and $(a, m) = 1$, then a is a quadratic residue modulo m (that is, the congruence $x^2 \equiv a \bmod m$ is solvable) if and only if the following conditions hold:

- $\bigl(\frac{a}{p_i}\bigr) = 1$ for all $i \in [1, r]$.
- $a \equiv 1 \bmod 4$ if $e = 2$.
- $a \equiv 1 \bmod 8$ if $e \ge 3$.

21. Let $m \in \mathbb{N}$, $m \geq 3$ and $K = \mathbb{Q}(\zeta_m)$. Then $1 - \zeta_m \in \mathcal{O}_K^\times$ if and only if m is not a prime power.

22. Let R be a domain. An element $u \in R^\bullet \setminus R^\times$ is called an *atom* if, for all $a, b \in R$, $u = ab$ implies $a \in R^\times$ or $b \in R^\times$. R is called *atomic* if every $a \in R^\bullet \setminus R^\times$ is a product of atoms.

a) $u \in R^\bullet \setminus R^\times$ is an atom if and only if the principal ideal uR is maximal among principal ideals.

b) Suppose that R satisfies the ascending chain condition for principal ideals (ACCP). Then R is atomic. In particular, every noetherian domain is atomic.

c) The domain $\overline{\mathbb{Z}} = \mathrm{cl}_{\mathbb{C}}(\mathbb{Z})$ is not atomic (hence not noetherian), but every finitely generated ideal of $\overline{\mathbb{Z}}$ is invertible (a domain with this property is called a *Prüfer domain*).

d) Let R be a Dedekind domain, write its class group $\mathcal{C}(R)$ additively, and let $\mathfrak{a} \in \mathcal{I}(R)$, say $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, where $r \in \mathbb{N}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P}(R)$. Then $\mathfrak{a}$ is a principal ideal if and only if $[\mathfrak{p}_1] + [\mathfrak{p}_2] + \ldots + [\mathfrak{p}_r] = \mathbf{0}$ (in this case, $[\mathfrak{p}_1][\mathfrak{p}_2] \cdot \ldots \cdot [\mathfrak{p}_r]$ is called a *zero sum sequence*). Moreover, $\mathfrak{a}$ is the principal ideal generated by an atom if and only if $[\mathfrak{p}_1][\mathfrak{p}_2] \cdot \ldots \cdot [\mathfrak{p}_r]$ is a minimal zero-sum sequence (that means, no proper subsum equals zero).

23. Let R be a Dedekind domain.

a) Let $r \in \mathbb{N}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P}(R)$ distinct and $e_1, \ldots, e_r \in \mathbb{N}_0$. Then there exists some $a \in R$ such that $\mathsf{v}_{\mathfrak{p}_i}(a) = e_i$ for all $i \in [1, r]$. Hint: If $\mathfrak{p} \in \mathcal{P}(R)$, $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, $e \in \mathbb{N}_0$, $a \in R$ and $a \equiv \pi^e \mod \mathfrak{p}^{e+1}$, then $a \in \mathfrak{p}^e \setminus \mathfrak{p}^{e+1}$.

b) Let $\mathfrak{a} \in \mathcal{I}(R)$. In every ideal class of R there exists an ideal $\mathfrak{c}$ such that $\mathfrak{a} + \mathfrak{c} = R$.

c) If $\mathfrak{a} \in \mathcal{I}(R)$, then $R/\mathfrak{a}$ is a principal ideal ring, and $\mathfrak{a} = {}_R\langle a, b\rangle$ for some $a, b \in \mathfrak{a}$.

24. Let $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$, where $d \in \{-1, -2, -3, -7, -11\}$. Then $\mathcal{O}_K$ is factorial. Prove that for every $x \in K^\times$, there exists some $q \in \mathcal{O}_K$ such that $|x - q| < 1$, and thus $\mathcal{O}_K$ is euclidean.

25. **a)** Let R be an atomic domain (see **22.**), and suppose that every $a \in R^\bullet \setminus R^\times$ is a product of atoms in an essentially unique way (what means this precisely?) Then R is factorial.

b) Let $d \in \mathbb{Z}$, $d < 0$, and suppose that $\mathbb{Z}[\sqrt{d}]$ is factorial. Then $d = -1$, $d = -2$ or $d = -p$ for some prime $p \equiv 3 \mod 4$.

26. Let R be a Dedekind domain, $\mathfrak{p} \in \mathcal{P}(R)$, $K = \mathsf{q}(R)$ and L/K a finite separable field extension.

a) Let $K \subset L_1, L_2 \subset L$ be intermediate fields such that $L = L_1L_2$. If $\mathfrak{p}$ splits completely in L_1 and in L_2 then it also splits completely in L.

b) Let $K \subset L_1 \subset L$ be an intermediate field such that L/K is the normal closure of L_1/K. If $\mathfrak{p}$ splits completely in L_1, then it splits completely in L.

27. The Fibonacci sequence $(F_n)_{n \geq 0}$ is recursively defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$. Then

$$F_n = \frac{1}{\sqrt{5}}\Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big] \quad \text{for all} \quad n \geq 0\,, \quad \text{and} \quad F_p \equiv \Big(\frac{p}{5}\Big) \mod p$$

for all primes $p \in \mathbb{P} \setminus \{2, 5\}$. Calculate in the field $\mathbb{F}_{25}$.

28. Sums of two squares. Use that $\mathcal{O}_{\mathbb{Q}(\mathsf{i})} = \mathbb{Z}[\mathsf{i}]$ is factorial.

a) Let $n \in \mathbb{N}$. Then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $2 \,|\, \mathsf{v}_p(n)$ for all primes $p \equiv 3 \mod 4$. Moreover, $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ such that $(a, b) = 1$ if and only if $4 \nmid n$ and no prime $p \equiv 3 \mod 4$ divides n.

b) If $r = \frac{m}{n} \in \mathbb{Q}$, where $m,\, n \in \mathbb{N}$ and $(m,n) = 1$, then r is the sum of two rational squares if and only if both m and n are the sums of two integral squares. In particular, a positive integer is the sum of two rational squares if and only if it is the sum of two integral squares.

c) If $r \in \mathbb{Q}$ is the sum of two rational squares, then there are infinitely many $(x,y) \in \mathbb{Q}^2$ such that $r = x^2 + y^2$.

d) Let $n \in \mathbb{N}$, $\mathsf{r}(n) = |\{(a,b) \in \mathbb{Z}^2 \mid n = a^2 + b^2\}|$, and define $\chi(n) = (-1)^{(n-1)/2}$ if $2 \nmid n$, and $\chi(n) = 0$ if $2 \,|\, n$. Then

$$\mathsf{r}(n) = |\{(a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 = n\} = 4 \sum_{\substack{1 \le d | n \\ d \text{ odd}}} \chi(d) = 4(A - B)\,,$$

where $A = |\{d \in \mathbb{N} \mid d \,|\, n,\; d \equiv 1 \bmod 4\}|$ and $B = |\{d \in \mathbb{N} \mid d \,|\, n,\; d \equiv 3 \bmod 4\}|$. In particular, if $p \equiv 1 \bmod 4$ is a prime, then p has a "unique" representation as sum of two squares. Hints: Set $n = 2^k m,\;\; m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $k,\, r \in \mathbb{N}_0,\;\; p_1, \ldots, p_r$ are distinct odd primes, and $e_1, \ldots, e_r \in \mathbb{N}_0$. Then

$$\mathsf{r}(n) = 4\,|\{\mathfrak{a} \lhd \mathbb{Z}[\mathsf{i}] \mid (\mathbb{Z}[\mathsf{i}] : \mathfrak{a}) = n\}| = 4 \prod_{i=1}^{r} |\{\mathfrak{a} \lhd \mathbb{Z}[\mathsf{i}] \mid (\mathbb{Z}[\mathsf{i}] : \mathfrak{a}) = p_i^{e_i}\}|\,,$$

for an odd prime power p^e we have $|\{\mathfrak{a} \lhd \mathbb{Z}[\mathsf{i}] \mid (\mathbb{Z}[\mathsf{i}] : \mathfrak{a}) = p^e\}| = \sum_{\nu=0}^{e} \chi(p^\nu)$.

29. For $i \in \{1,2,3\}$, let $K_i = \mathbb{Q}(\theta_i)$, where $\theta_1^3 - 18\theta_1 - 6 = 0,\;\; \theta_2^3 - 36\theta_2 - 78 = 0$, and $\theta_3^3 - 54\theta_3 - 150 = 0$. In all cases, $(1, \theta_i, \theta_i^2)$ is an integral basis, and $\Delta_{K_i} = 22356$ (use the Eisenstein criterion). However, the fields are distinct (indeed, 5 splits only in K_3, and 11 splits in K_1, but not in K_2).

30. The Dirichlet field. Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, where $d_1,\, d_2 \in \mathbb{Z} \setminus \{1\}$ are squarefree and distinct. Then $K/\mathbb{Q}$ is a galois algebraic number field of degree 4 with three quadratic subfields $K_1,\, K_2, K_3$. A rational prime p splits in K in one of the following 4 ways.

I. $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, where $f(\mathfrak{p}_i/p) = 1$ (p splits completely).
II. $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $f(\mathfrak{p}_i/p) = 2$ (p has inert divisors).
III. $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2$, where $f(\mathfrak{p}_i/p) = 1$ (p splits ramified).
IV. $p\mathcal{O}_K = \mathfrak{p}^4$, where $f(\mathfrak{p}/p) = 1$ (p ramifies completely)

If p splits in K_1 and K_2, then p also splits in K_3, and p splits completely in K. If p splits in K_1 and is inert in K_2, then p is also inert in K_3 and has inert divisors in K. If p splits in K_1 and ramifies in K_2, then p also ramifies in K_3 and splits ramified in K. If p ramifies in $K_1,\; K_2$ and K_3, then $p = 2$ and p ramifies completely in K.

31. The domains $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{-2})} = \mathbb{Z}[\sqrt{-2}]$ are factorial [for $\mathbb{Z}[\sqrt{-2}]$ see Exercise 24, for $\mathbb{Z}[\sqrt{2}]$ use that for every $x \in \mathbb{Q}(\sqrt{2})$ there exists some $q \in \mathbb{Z}[\sqrt{2}]$ such that $|\mathsf{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(x - q)| < 1$].

A prime p splits in $\mathbb{Q}(\sqrt{2})$ if and only if $p = x^2 - 2y^2$ for some $x,\, y \in \mathbb{Z}$, and then it follows that $p \equiv \pm 1 \bmod 8$. A prime p splits in $\mathbb{Q}(\sqrt{-2})$ if and only if $p = x^2 + 2y^2$ for some $x,\, y \in \mathbb{Z}$, and then it follows that $p \equiv 1$ or $3 \bmod 8$. Now apply Exercise 30 to the field $\mathbb{Q}^{(8)} = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$, and deduce that

$$\Big(\frac{2}{p}\Big) = (-1)^{(p^2-1)/8}\,.$$

Observe that p splits in $\mathbb{Q}(\sqrt{-1})$ if and only if $p \equiv 1 \bmod 4$, and that p splits completely in $\mathbb{Q}^{(8)}$ if and only if $p \equiv 1 \bmod 8$.

32. Let K be a galois algebraic number field and $G = \mathsf{Gal}(K/\mathbb{Q})$. For $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_K)$ set $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$. Then $G_{\mathfrak{P}} \subset G$ is a subgroup, called the *decomposition group* of $\mathfrak{P}$, and its fixed field $K_{\mathfrak{P}} = K^{G_{\mathfrak{P}}}$ is called the *decomposition field* of $\mathfrak{P}$.

a) Let $p \in \mathbb{P}$, $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, and $G = \biguplus_{i=1}^{r} \sigma_i G_{\mathfrak{P}}$. Then $\{\sigma_i\mathfrak{P} \mid i \in [1, r]\}$ is the set of all prime ideals of $\mathcal{O}_K$ lying above p, and $G_{\sigma_i\mathfrak{P}} = \sigma_i G_{\mathfrak{P}} \sigma_i^{-1}$ for all $i \in [1, r]$. (Hint: G operates transitively on the set of all $\mathfrak{P} \,|\, p$). In particular, $|G_{\mathfrak{P}}| = e(\mathfrak{P}/p) f(\mathfrak{P}/p)$, and if $\mathfrak{q} = \mathfrak{P} \cap K_{\mathfrak{P}}$, then $\mathfrak{P}$ is the only prime ideal lying above $\mathfrak{q}$, and $e(\mathfrak{q}/p) = f(\mathfrak{q}/p) = 1$.

b) Let $K/\mathbb{Q}$ be cyclic of even degree $[K:\mathbb{Q}] = 2d$ and K_0 the only quadratic subfield of K. Let $p \in \mathbb{P}$ and $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_K)$ such that $\mathfrak{P} \,|\, p$. Then the following assertions are equivalent: (i) $2 \,|\, (G:G_{\mathfrak{P}})$; (ii) $K_0 \subset K_{\mathfrak{P}}$; (iii) p splits in K_0; (iv) $p\mathcal{O}_K$ is the product of an even number of prime ideals.

c) A structural proof of the Quadratic Reciprocity Law. Let p and q be distinct odd primes, $q^* = (-1)^{(q-1)/2} q$, $K = \mathbb{Q}^{(q)}$ the q-th cyclotomic field, $K_0 = \mathbb{Q}(\sqrt{q^*}) \subset K$, and $\mathfrak{P} \in \mathcal{O}_K$ such that $\mathfrak{P} \,|\, p$. Apply **b)** and the decomposition law for cyclotomic fields to show that

$$\Big(\frac{p}{q}\Big) = 1 \ \Big[\iff p^{(q-1)/2} \equiv 1 \bmod q \Big] \iff \Big(\frac{q^*}{p}\Big) = 1\,.$$

33. Let $\Delta \in \mathbb{N}$ be not a square and $\Delta \equiv 0$ or $1 \bmod 4$.

a) Let v_0 be the smallest $v \in \mathbb{N}$ such that $\Delta v^2 + 4e$ is a square for some $e \in \{\pm 1\}$. If $\Delta > 5$, $u_0 \in \mathbb{N}$, $e_0 \in \{\pm 1\}$ and $\Delta v_0^2 + 4e_0 = u_0^2$, then $\varepsilon_\Delta = \frac{u_0 + v_0\sqrt{\Delta}}{2}$ is the fundamental unit of $\mathcal{O}_\Delta$, and $\mathsf{N}_{\mathbb{Q}(\sqrt{\Delta}/\mathbb{Q}}(\varepsilon_\Delta) = e_0$. What is special for $\Delta = 5$?

b) Let $n \in \mathbb{N}$, $s \in \{\pm 1\}$, $D = n^2 + s$, $\Delta = D$ if $D \equiv 1 \bmod 4$, and $\Delta = 4D$ if $D \not\equiv 1 \bmod 4$. Then $\varepsilon_\Delta = n + \sqrt{D}$.

c) Let $\Delta \equiv 1 \bmod 4$ and $\varepsilon_\Delta = \frac{u + v\sqrt{\Delta}}{2}$, where $u, v \in \mathbb{Z}$ and $u \equiv v \bmod 2$ [in fact, **a)** implies that $u, v \in \mathbb{N}$; also note that $\mathcal{O}_{4\Delta} = \mathbb{Z}[\sqrt{\Delta}] \subset \mathbb{Z}\big[\frac{1+\sqrt{\Delta}}{2}\big] = \mathcal{O}_\Delta$]. Then $\varepsilon_{4\Delta} = \varepsilon_\Delta$ if $u \equiv v \equiv 0 \bmod 2$, and $\varepsilon_{4\Delta} = \varepsilon_\Delta^3$ if $u \equiv v \equiv 1 \bmod 2$. If $\Delta \equiv 5 \bmod 8$, then $\varepsilon_{4\Delta} = \varepsilon_\Delta$.

d) If $\mathsf{N}_{\mathbb{Q}(\sqrt{\Delta})/Q}(\varepsilon_\Delta) = -1$, then no prime $p \equiv 3 \bmod 4$ divides Δ.

34. Determine all integral solutions of the diophantine equation $3x^2 - 4y^2 = 11$. Hint: Determine the fundamental unit of $\mathcal{O}_{48} = \mathbb{Z}[\sqrt{12}]$ and all solutions $(u, y) \in \mathbb{Z}^2$ of the norm equation $\mathsf{N}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(u + y\sqrt{12}) = 33$.

35. Let K be a quadratic number field and $\mathsf{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$.

a) $\tau(R) = R$ for every order $R \subset K$. In particular, $\tau(\mathcal{O}_K) = \mathcal{O}_K$, and if $\mathfrak{a} \in \mathcal{J}(\mathcal{O}_K)$, then $\tau(\mathfrak{a}) \in \mathcal{J}(\mathcal{O}_K)$, and $\mathfrak{a}\,\tau(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})\mathcal{O}_K$.

b) An ideal $\mathfrak{a} \in \mathcal{J}(\mathcal{O}_K)$ is called *ambiguous* if $\tau(\mathfrak{a}) = \mathfrak{a}$ [equivalently, $\mathfrak{a}^2 = \mathfrak{N}(\mathfrak{a})\mathcal{O}_K$]. Let $p_1, \ldots, p_t$ be the prime divisors of Δ_K and $p_i\mathcal{O}_K = \mathfrak{p}_i^2$ for all $i \in [1, t]$. Then an ideal $\mathfrak{a} \in \mathcal{J}(\mathcal{O}_K)$ is ambiguous if and only if $\mathfrak{a} = a\mathfrak{p}_{i_1} \cdot \ldots \cdot \mathfrak{p}_{i_r}$ for some $a \in \mathbb{N}$, $r \in \mathbb{N}_0$ and $1 \le i_1 < \ldots < i_r \le t$.

c) Let $\varepsilon \in \mathcal{O}_K^\times$, $\mathsf{N}_{K/\mathbb{Q}}(\varepsilon) = 1$ and $\alpha = 1 + \varepsilon$. Then $\alpha^2 = \mathsf{N}_{K/\mathbb{Q}}(\alpha)\varepsilon$, and $\alpha\mathcal{O}_\Delta$ is an ambiguous ideal. Deduce that $\mathsf{N}_{K/\mathbb{Q}}(\varepsilon_\Delta) = -1$ if Δ_K is a prime.

36. a) If $K = \mathbb{Q}(\sqrt{6})$, then $h_K = 1$, and if If $K = \mathbb{Q}(\sqrt{-6})$, then $h_K = 2$. Determine (in both cases) the prime ideal factorization of $6\mathcal{O}_K$.

b) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Then $\Delta_K = 24^2$ (it is a compositum of fields with coprime discriminants), $h_K = 1$ (though $\mathbb{Q}(\sqrt{-6}) \subset K$), and $\mathcal{O}_K^\times = \langle 1+\sqrt{2}, \frac{1+\sqrt{-3}}{2}\rangle$.

c) $h_{\mathbb{Q}(\sqrt{-23})} = 3$, $h_{\mathbb{Q}(\sqrt{-14})} = h_{\mathbb{Q}(\sqrt{-21})} = 4$, $\mathcal{C}_{\mathbb{Q}(\sqrt{-14})}$ cylic, and $\mathcal{C}_{\mathbb{Q}(\sqrt{-21})}$ is not cyclic.

37. Let R be a Dedekind domain. $K = \mathsf{q}(R)$, $S \subset \mathcal{P}(R)$ a finite subset, $S' = \mathcal{P}(R) \setminus S$, and $R^S = \{x \in K \mid \mathsf{v}_\mathfrak{p}(x) \ge 0 \text{ for all } \mathfrak{p} \in S'\}$. Then R^S is a Dedekind domain,

$$R^S = \bigcap_{\mathfrak{p} \in S'} R_\mathfrak{p} = \Big(R \setminus \bigcup_{\mathfrak{p}\in S} \mathfrak{p}\Big)^{-1} R, \quad \text{and there is a (natural) exact sequence}$$

$$1 \to R^\times \to (R^S)^\times \to \prod_{\mathfrak{p}\in S} K^\times/R_\mathfrak{p}^\times \to \mathcal{C}(R) \to \mathcal{C}(R^S) \to 1\,.$$

In particular, let K be an algebraic number field with r_1 real and r_2 pairs of complex embeddings, and $R = \mathcal{O}_K$. In this case, $(\mathcal{O}_K^S)^\times$ is called the *S-unit group* and $\mathcal{C}(R^S)$ is called the *S-class group* of K. By the exact sequence it follows that $\mathcal{C}(\mathcal{O}_K^S)$ is finite and $(\mathcal{O}_K^S)^\times \cong \mu(K) \times \mathbb{Z}^{|S|+r_1+r_2-1}$.

38. Let (K, v) be a discrete valued field, $U_v = \mathcal{O}_v^\times$, and for $n \in \mathbb{N}$ set $U_v^n = 1 + \mathfrak{p}_v^n$.

a) There exist (natural) isomorphisms $U_v/U_v^1 \xrightarrow{\sim} \mathsf{k}_v^\times$ and $U_v^n/U_v^{n+1} \xrightarrow{\sim} \mathsf{k}_v$ for all $n \in \mathbb{N}$.

b) If $K \subset \mathbb{Q}$, $p \in \mathbb{P}$ is a prime and $v(p) = e \in \mathbb{N}$, then $v \,|\, \mathbb{Q} = e\mathsf{v}_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ (where v_p denotes the p-adic valuation). The infinite series

$$\mathsf{e}(x) = \sum_{n=0}^\infty \frac{x^n}{n!} \quad \text{converges for all } x \in K \text{ satisfying} \quad v(x) > \frac{e}{p-1}\,,$$

and for those x we have $v(\mathsf{e}(x) - 1) = v(x)$.

Prove first: If $n \in \mathbb{N}$ and $n = a_0 + a_1 p + \ldots + a_r p^r$, where $r \in \mathbb{N}_0$ and $a_0, \ldots, a_r \in [0, p-1]$, then

$$\mathsf{v}_p(n!) = \frac{n - (a_0 + \ldots + a_r)}{p-1} \quad \text{and} \quad v\Big(\frac{x^n}{n!}\Big) \ge n\Big(v(x) - \frac{e}{p-1}\Big)\,.$$

39. (Power series rings) Let R be a commutative ring and R^* the set of all sequences $f = (f_n)_{n\ge0}$ in R, endowed with an addition and multiplication defined by

$$(f_n)_{n\ge0} + (g_n)_{n\ge0} = (f_n + g_n)_{n\ge0} \quad \text{and} \quad (f_n)_{n\ge0} \cdot (g_n)_{n\ge0} = \Big(\sum_{j=0}^n f_j g_{n-j}\Big)_{n\ge0}\,.$$

Then R^* is a commutative ring, and the map $\iota\colon R \to R^*$, defined by $\iota(c) = (c, 0, 0, \ldots)$ for $c \in R$, is a ring monomorphism.

We identify R with $\iota(R) \subset R^*$, set $t = (0, 1, 0, 0, \ldots) \in R^*$, and write the elements $f = (f_n)_{n\ge0}$ in the form

$$f = \sum_{n=0}^\infty f_n t^n\,.$$

Then we call $R^* = R[\![t]\!]$ the *power series ring* in t over R. It contains the polynomial ring $R[t]$ as a subring.

a) $R[\![t]\!]^\times = \{f \in R[\![t]\!] \mid f_0 \in R^\times\}$.

b) For $f \in R[\![t]\!]$, we call $\operatorname{ord}(f) = \inf\{n \in \mathbb{N}_0 \mid f_n \ne 0\} \in \mathbb{N}_0 \cup \{\infty\}$ the order of f. Then $\operatorname{ord}(f+g) \ge \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$, with equality if $\operatorname{ord}(f) \ne \operatorname{ord}(g)$, and $\operatorname{ord}(fg) \ge$

$\mathrm{ord}(f) + \mathrm{ord}(g)$, with equality if R is a domain. In particular, if R is a domain, then $R[\![t]\!]$ is a domain.

c) Let $\rho \in (0,1)$ be a real number. For $f,\, g \in R[\![t]\!]$, we set $\mathsf{d}(f,g) = \rho^{\mathrm{ord}(f-g)}$. Then d is a metric on $R[\![t]\!]$. For $f \in R[\![t]\!]$ and $n \in \mathbb{N}$, we set $B_n(f) = f + t^n R[\![t]\!]$. Then $\{B_n(f) \mid n \in \mathbb{N}\}$ is a fundamental system of neighborhoods of f (in particular, the topology does not depend on ρ). Addition and multiplication on R are continuous, and $R[\![t]\!] = \overline{R[t]}$. If $(g_n)_{n\ge 0}$ is any sequence in $R[\![t]\!]$ such that $(\mathrm{ord}(g_n))_{n\ge 0} \to \infty$ and $f \in R[\![t]\!]$, then the series $\sum_{n=0}^{\infty} f_n g_n$ converges. In particular, if $g \in R[\![t]\!]$, and $\mathrm{ord}(g) \ge 1$, then $f(g) \in R[\![t]\!]$.

d) If $\mathrm{char}(R) = p$ is a prime, then

$$f^p = \sum_{n=0}^{\infty} f_n^p t^{np} \quad \text{for all } f \in R[\![t]\!].$$

e) Let R be a field. Then $R(\!(t)\!) = \mathsf{q}(R[\![t]\!])$ is called the *field of formal Laurent series* over R. Its elements have a unique representation

$$h = \sum_{n=-\infty}^{\infty} h_n t^n\,, \quad \text{where} \quad h_n \in K \quad \text{and} \quad h_n = 0 \quad \text{for almost all} \quad n < 0\,.$$

The function ord has a unique extension to a valuation $\mathrm{ord}\colon F(\!(t)\!) \to \mathbb{Z} \cup \{\infty\}$, and $(F(\!(t)\!), \mathrm{ord})$ is a complete discrete valued field with valuation domain $R[\![t]\!]$.

40. Let K be a field of characteristic 0. For formal Laurent series $f \in K(\!(t)\!)$ define its derivative $f' \in K(\!(t)\!)$ as usual and give algebraic proofs of all differentiation rules including the chain rule (you may assume the corresponding rules for polynomials). Define the formal exponential and the formal logarithm by

$$\mathsf{E}(t) = \sum_{n=0}^{\infty} \frac{1}{n!} t^n \quad \text{and} \quad \mathsf{L}(t) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} t^n$$

and prove $E'(t) = E(t)$, $L'(t) = (1+t)^{-1}$, $E(L(t)) = 1 + t$ and $L(E(t) - 1) = t$.

41. Let F be a field and $K = F(t)$ a rational function field. Then there is a unique valuation $\mathsf{v}_\infty\colon K \to \mathbb{Z} \cup \{\infty\}$ such that $\mathsf{v}_\infty(f) = -\deg(f)$ for all $f \in F[t]$. For every monic irreducible polynomial $p \in F[t]$, let v_p be the $pK[t]$-adic valuation of K. Then $\{\mathsf{v}_p \mid p \in F[t] \text{ monic and irreducible}\} \cup \{\mathsf{v}_\infty\}$ is the set of all valuations $v\colon K \to \mathbb{Z} \cup \infty\}$ such that $v \,|\, F^\times = 0$. If $p \in F[t]$ is a monic irreducible polynomial and k_p denotes the residue class field of (K, v_p), then $\dim_F(\mathsf{k}_p) = \deg(p)$.

If $u = t^{-1}$, then $\mathsf{v}_\infty = \mathsf{v}_{uF[u]}$, $(F(\!(t)\!), \mathrm{ord})$ is the completion of (K, v_t), and $(F(\!(u)\!), \mathrm{ord})$ is the completion of (K, v_∞).

42. Let K be a field. Then $K(t) \subset K(\!(t)\!)$. The following *Theorem of Hankel* characterizes $K(t) \cap K[\![t]\!]$. For $f \in K[\![t]\!]$ and $n,\, s \in \mathbb{N}_0$, set $D_n^s = \det(f_{n+i+j})_{i,\,j\in[0,s]} \in \mathsf{M}_{s+1}(K)$. Then $f \in K(t)$ if and only if there exists some $s \in \mathbb{N}_0$ such that $D_n^s = 0$ for all $n \gg 1$.

Hint: One direction is easy. For the other one, use a determinant relation due to Sylvester: For $A = (a_{i,j})_{i,j\in[1,n]}$, set $A^\circ = (a_{i,j})_{i,j\in[2,n-1]}$, and let $\alpha_{i,j} = (-1)^{i+j} \det(a_{\nu,\mu})_{(\nu,\mu)\ne(i,j)}$ be the coefficient of $a_{i,j}$ in the determinant expansion of A. Then

$$\det(A)\det(A^\circ) = (\alpha_{1,1}\alpha_{n,n} - \alpha_{n,1}\alpha_{1,n})\,.$$

Deduce $D^s_n D^{s-2}_{n+2} = D^{s-1}_{n+2} D^{s-1}_n - (D^{s-1}_{n+1})^2$. Now prove that there exists a smallest s such that, for some $n_0 \geq 0$, $D^s_n = 0$ for all $n \geq n_0$ and $D^{s-1}_n \neq 0$ for all $n \geq n_0 + 1$. Finally determinate the coefficients of a polynomial of degree s in the denominator of f from a system of linear equations.

43. Let $p \in \mathbb{P}$ be a prime and $z \in \mathbb{Q}_p^\times$. Then z has a unique p-adic expansion

$$z = \sum_{n=d}^{\infty} a_n p^n\,, \quad \text{where} \ \ a_n \in [0, p-1] \ \ \text{for all} \ \ n \geq d \ \ \text{and} \ \ a_d \neq 0\,.$$

In this expansion, $d = \mathsf{v}_p(z)$. The sequence $(a_n)_{n \geq 0}$ is ultimately periodic if and only if $z \in \mathbb{Q}$. Calculate the p-adic expansion of 2 and of -2, and the 5-adic expansion of $\frac{2}{3}$.

44. Let $\mathbb{Z}[\![t]\!]$ be the power series ring and $p \in \mathbb{P}$ a prime. Then there is a natural isomorphism $\mathbb{Z}[\![t]\!]/(t-p)\mathbb{Z}[\![t]\!] \xrightarrow{\sim} \mathbb{Z}_p$.

45. Let $p,\, q \in \mathbb{P}$ be primes and $\Phi \colon \mathbb{Q}_p \to \mathbb{Q}_q$ and isomorphism. Then $p = q$ and $\Phi = \mathrm{id}_{\mathbb{Q}_p}$.

46. Let (K, v) be a complete discrete valued field, $f \in \mathcal{O}_v[X]$, $r \in \mathbb{N}$ and $a \in \mathcal{O}_v$ such that $v(f(a)) \geq 2r - 1$ and $v(f'(a)) = r - 1$. Then there exists some $b \in \mathcal{O}_v$ such that $f(b) = 0$ and $v(b - a) \geq r$. Hint: Construct a sequence $(b_\nu)_{\nu \geq 0}$ recursively by $b_0 = a$, $v(b_\nu - b_{\nu+1}) \geq r + \nu$ and $v(f(b_\nu)) \geq 2r + \nu - 1$. Observe that $f(u + v) \equiv f(u) + vf'(u) \mod v^2\mathcal{O}_v$.

Use the above result to prove:

a) If $a \in \mathbb{Z}_2^\times$, then $a \in \mathbb{Z}_2^{\times 2}$ if and only if $a \equiv 1 \mod 8$.

b) If $a \in \mathbb{Z}_3^\times$, then $a \in \mathbb{Z}_3^{\times 3}$ if and only if $a \equiv \pm 1 \mod 9$.

c) Let (K, v) be a above and $m \in \mathbb{N}$ such that $\mathrm{char}(K) \nmid m$. Then there exists some $r \in \mathbb{N}$ such that $\{a \in \mathcal{O}_v \mid a \equiv 1 \mod \mathfrak{p}_v^r\} \subset \mathcal{O}_v^{\times m}$.

47. Let $p \in \mathbb{P}$ be a prime, $\overline{\mathbb{Q}}_p$ an algebraic closure of $\mathbb{Q}_p$ and $|\cdot|_p \colon \overline{\mathbb{Q}}_p \to \mathbb{R}_{\geq 0}$ the extension of the p-adic valuation. Then $|\cdot|_p \colon \overline{\mathbb{Q}}_p \to \mathbb{R}_{\geq 0}$ is a non-archimedean non-discrete absolute value,and $(\overline{\mathbb{Q}}_p, |\cdot|_p)$ is not complete.

Hints: Assume the contrary. For $n \in \mathbb{N}$, let $\zeta_n \in \overline{\mathbb{Q}}_p$ be a primitive n-th root of unity. Then

$$\alpha = \sum_{\substack{n=1 \\ p \nmid n}}^{\infty} \zeta_n p^n \in \overline{\mathbb{Q}}_p\,, \quad \text{and for } m \in \mathbb{N} \text{ such that } p \nmid m, \text{ set } \ \alpha_m = p^{-m}\Big(\alpha - \sum_{\substack{n=0 \\ p \nmid n}}^{m-1} \zeta_n p^n\Big)\,.$$

Then $\alpha_m \in K = \mathbb{Q}_p(\alpha)$, and the residue class field of K contains infinitely many roots of unity. [The completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}}_p$ is algebraically closed, but this is more involved].

48. Every complete discrete valued field is uncountable.

49. Let $(K, |\cdot|)$ be a discrete valued complete field, $\overline{K} \supset K$ and algebraic closure, $\alpha \in \overline{K}$ separable over K, $n \in \mathbb{N}$ and $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in K[X]$ the minimal polynomial of α over K. Then there exists some $\varepsilon \in \mathbb{R}_{>0}$ with the following property:

If $Q = X^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0 \in K[X]$ and $|a_\nu - b_\nu| < \varepsilon$ for all $\nu \in [0, n-1]$, then there exists some $\beta \in \overline{K}$ such that $Q(\beta) = 0$ and $K(\alpha) = K(\beta)$. Hint: Krasner's Lemma.

50. Let p be a prime number. For $n \in \mathbb{N}$, let $\mathbb{Q}_p^{(n)} = \mathbb{Q}_p(\zeta_n)$, where ζ_n is a primitive n-th root of unity. Suppose that $n = p^k m$, where $k \in \mathbb{N}_0$, $m \in \mathbb{N}$ and $p \nmid m$. Let $f \in \mathbb{N}$ be minimal such that $p^f \equiv 1 \mod m$.

a) $(\mathbb{Q}_p^{(m)}:\mathbb{Q}_p) = f = f(\mathbb{Q}_p^{(m)}/\mathbb{Q}_p)$, $e(\mathbb{Q}_p^{(m)}/\mathbb{Q}_p) = 1$, and $\mathcal{O}_{\mathbb{Q}_p^{(m)}} = \mathbb{Z}_p[\zeta_m]$ (use Hensel's Lemma).

b) $(\mathbb{Q}_p^{(p^k)}:\mathbb{Q}_p) = p^{k-1}(p-1) = e(\mathbb{Q}_p^{(p^k)}/\mathbb{Q}_p)$, $f(\mathbb{Q}_p^{(p^k)}/\mathbb{Q}_p) = 1$, and $\mathcal{O}_{\mathbb{Q}_p^{(p^k)}} = \mathbb{Z}_p[\zeta_{p^k}]$ (use an Eisenstein polynomial).

c) $\mathbb{Q}_p^{(n)} = \mathbb{Q}_p^{(m)}\mathbb{Q}_p^{(p^k)}$, $\mathbb{Q}_p^{(m)} \cap \mathbb{Q}_p^{(p^k)} = \mathbb{Q}_p$, $(\mathbb{Q}_p^{(n)}:\mathbb{Q}_p) = p^{k-1}(p-1)f$, and $\mathcal{O}_{\mathbb{Q}_p^{(n)}} = \mathbb{Z}_p[\zeta_n]$.

51. Let (K, v) be a complete discrete valued field, $|\mathsf{k}_K| = q < \infty$, $\overline{K} \supset K$ an algebraic closure and $n \in \mathbb{N}$. Then there exists a unique field L such that $K \subset L \subset \overline{K}$, $[L:K] = n$ and L/K is unramified. Explicitly, $L = K^{(q^n-1)}$ is the field of (q^n-1)-th roots of unity over K, and L/K is cyclic.

52. Recall Exercise 39e).

a) Let R be an algebraically closed field, $K = R(\!(t)\!)$ the Laurent series field and L/K a finite extension of degree n. Then $L = R(\!(t^{1/n})\!)$.

b) Let (K, v) be a discrete valued complete field with residue class field k_K. Assume that k_K has a separating transcendence basis over its prime field, and $\mathrm{char}(K) = \mathrm{char}(\mathsf{k}_K)$. Then $K \cong \mathsf{k}_K(\!(t^{1/n})\!)$. Hint: Let F be a common prime field of K and k_K, $(\tau_i)_{i\in I}$ a separating transcendence basis of k_K/F, and $(t_i)_{i\in I}$ a system of representatives in $\mathcal{O}_K$. Let R be a maximal field such that $F(\{t_i \mid i \in I\}) \subset R \subset \mathcal{O}_K$ (Zorn's Lemma). Then $\mathcal{O}_K = R[\![t]\!]$ for some $t \in \mathcal{O}_K$.

53. Let K be a discrete valued complete field and $K \subset L,\ M \subset \overline{K}$ finite extensions.

a) If L/K is unramified, then LM/M is unramified.

b) If L/K and M/K are unramified, then LM/K is unramified.

c) If L/K is separable and T is the inertia field of L/K, then L/T is fully ramified. If L/K is galois, then T/K and $\mathsf{k}_L/\mathsf{k}_K$ are also galois, and there is a natural isomorphism $\mathsf{Gal}(T/K) \overset{\sim}{\to} \mathsf{Gal}(\mathsf{k}_L/\mathsf{k}_K)$.

d) If L/K separable, then $e(LM/M) \le e(L/K)$.

54. Let K be an algebraic number field, $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, and let $K \subset L,\ M \subset \overline{\mathbb{Q}}$ be algebraic number fields.

a) Let $\mathfrak{q} \in \mathcal{P}(\mathcal{O}_M)$ be such that $\mathfrak{q} \mid \mathfrak{p}$. If $\mathfrak{p}$ splits completely in L, then $\mathfrak{q}$ splits completely in LM.

b) If $\mathfrak{p}$ splits completely in L and in M, then $\mathfrak{p}$ splits completely in LM,

c) If M/K is the normal closure of L/K and $\mathfrak{p}$ splits completely in L, then $\mathfrak{p}$ splits completely in M,

Hint: Consider the complete localizations at $\mathfrak{p}$.

55. Let $(K, |\cdot|_0)$ be a discrete valued field, L/K a finite galois extension, $G = \mathsf{Gal}(L/K)$, $|\cdot|$ an absolute value of L and $|\cdot| \restriction K = |\cdot|_0$. Let $(\widehat{K}, |\cdot|_0)$ be a completion of $(K, |\cdot|_0)$ and $(\widehat{L}, |\cdot|)$ a completion of $(L, |\cdot|)$ such that $\widehat{K} \subset \widehat{L}$. For $\sigma \in G$, set $|\cdot|_\sigma = |\cdot|\circ\sigma\colon L \to \mathbb{R}_{\ge 0}$. Then $\{|\cdot|_\sigma \mid \sigma \in G\}$ is the set of all absolute values of L extending $|\cdot|_0$, $\widehat{L}/\widehat{K}$ is galois, and if $G_0 = \{\sigma \in G \mid |\cdot|_\sigma = |\cdot|\}$, then there is an isomorphism $\mathsf{Gal}(\widehat{L}/\widehat{K}) \overset{\sim}{\to} G_0$, given by $\tau \mapsto \tau \mid L$.

56. Let $l,\ p \in \mathbb{P}$ be primes, $l \ne p$, $c \in \mathbb{Q} \setminus \mathbb{Q}^l$ and $K = \mathbb{Q}(\sqrt[l]{c}\,) \subset \mathbb{C}$. Then there exists some $a \in \mathbb{Z} \setminus Z^l$ such that $\mathsf{v}_p(a) \in [0, l-1]$ and $K = \mathbb{Q}(\sqrt[l]{a}\,)$. We set $\overline{a} = a + p\mathbb{Z} \in \mathbb{F}_p$.

a) If $p \mid a$, then $p\mathcal{O}_K = \mathfrak{p}^l$ for some $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$.

b) Suppose that $p \nmid a$ and $p \equiv 1 \mod l$. If $\overline{a} \notin \mathbb{F}_p^l$, then $p\mathcal{O}_K \in \mathcal{P}(\mathcal{O}_K)$, and if $\overline{a} \in \mathbb{F}_p^l$, then $p\mathcal{O}_K = \mathfrak{p}_1 . \therefore \cdot \mathfrak{p}_l$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_l \in \mathcal{O}_K$ are distinct, and $f(\mathfrak{p}_i/p) = 1$ for all $i \in [1, l]$.

c) Suppose that $p \nmid a$, $p \not\equiv 1 \mod l$, and let $f \in \mathbb{N}$ be minimal such that $p^f \equiv 1 \mod l$. Then $p\mathcal{O}_K = \mathfrak{p}_0\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, where $r \in \mathbb{N}$, $l = 1 + fr$, $\mathfrak{p}_0, \ldots \mathfrak{p}_r \in \mathcal{P}(\mathcal{O}_K)$ are distinct, $f(\mathfrak{p}_0/p) = 1$, and $f(\mathfrak{p}_i/p) = f$ for all $i \in [1, r]$.

sni Hint: Factorize the polynomial $X^l - \overline{a}$ over $\mathbb{F}_p$ and then (by means of Hensel's Lemma) $X^l - a$ over $\mathbb{Q}_p$.