Lemma 3.52. (i) $\mathfrak{a} \subset \mathfrak{b} \Longrightarrow \mathfrak{b}^* \subset \mathfrak{a}^*$.

(ii) $\mathfrak{a} \subset A \Longleftrightarrow \mathfrak{a}^* \supset A$

(iii) *Für ein Primideal* $\mathfrak{p}$ *gilt* $\mathfrak{p}^* \supsetneq A$.

Beweis. (i) ist folgt durch Auswertung der Definitionen.
(ii) $\mathfrak{a} \subset A \Rightarrow 1 \in \mathfrak{a}^* \Rightarrow A \subset \mathfrak{a}^*$. Gilt $\mathfrak{a}^* \supset A$ folgt $1 \in \mathfrak{a}^*$, also $\mathfrak{a} = 1\mathfrak{a} \subset A$.
(iii) Sei $a \in \mathfrak{p}$, $a \neq 0$. Nach 3.44 existieren Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset (a) \subset \mathfrak{p}$. OE sei n minimal gewählt. Nach 3.45 gilt $\mathfrak{p}_i \subset \mathfrak{p}$ für ein i, etwa $\mathfrak{p}_1 \subset \mathfrak{p}$. Wegen $\dim A \leq 1$ folgt $\mathfrak{p}_1 = \mathfrak{p}$. Wegen $\mathfrak{p}_2 \cdots \mathfrak{p}_n \not\subset (a)$ (Im Fall $n = 1$ ist das leere Produkt gleich A) existiert ein $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$ mit $b \notin aA$ also $a^{-1}b \notin A$. Aber $b\mathfrak{p} \in \mathfrak{p}_2 \cdots \mathfrak{p}_n \cdot \mathfrak{p}_1 \subset (a)$, also $a^{-1}b \in \mathfrak{p}^*$. □

Lemma 3.53. *Sei* $\mathfrak{a} \subset A$ *und* $\mathfrak{a}^* = A$. *Dann gilt* $\mathfrak{a} = A$.

Beweis. Wäre $\mathfrak{a} \neq A$, so existierte ein Primideal $\mathfrak{p} \subset A$ mit $\mathfrak{a} \subset \mathfrak{p}$. Wir erhalten $\mathfrak{a}^* \supset \mathfrak{p}^* \supsetneq A$. Widerspruch □

Lemma 3.54. *Für* $\mathfrak{a} \subset A$ *gilt* $\mathfrak{a}\mathfrak{a}^* = A$.

Beweis. Sei $\mathfrak{b} = \mathfrak{a}\mathfrak{a}^* \subset A$. Z.z.: $\mathfrak{b} = A$. Es gilt

$$\mathfrak{a}(\mathfrak{a}^*\mathfrak{b}^*) = \mathfrak{b}\mathfrak{b}^* \subset A.$$

Daher gilt $\mathfrak{a}^*\mathfrak{b}^* \subset \mathfrak{a}^*$. Sei nun $\beta \in \mathfrak{b}^*$ beliebig. Wegen $1 \in \mathfrak{a}^*$ und $\beta \cdot \mathfrak{a}^* \subset \mathfrak{a}^*$ ist nach 3.4 (iii) (mit $M = \mathfrak{a}^*$) β ganz über A, also in A. Daher gilt $\mathfrak{b}^* \subset A$. Wegen $\mathfrak{b} \subset A$ folgt $\mathfrak{b}^* \supset A$, also $\mathfrak{b}^* = A$. Nach 3.53 folgt $\mathfrak{b} = A$. □

Theorem 3.55. *Die Menge der von* 0 *verschiedenen gebrochenen Ideale eines Dedekindrings bildet bzgl. Multiplikation eine abelsche Gruppe. Das Inverse zu* $\mathfrak{a}$ *ist durch*

$$\mathfrak{a}^{-1} = \{a \in K \mid a\mathfrak{a} \subset A\} \qquad [= a^*]$$

gegeben.

Bezeichnung dieser Gruppe: $J(A)$.

Beweis. Die gebrochenen Ideale bilden ein abelsches Monoid. Z.z. ist die Existenz Inverser. Sei $\mathfrak{a} \neq 0$ beliebig. Für $0 \neq x \in K$ gilt $\mathfrak{a}^* = (xA)(x\mathfrak{a})^*$.
Wählen wir x so, dass $x\mathfrak{a} \subset A$ gilt, so folgt nach 3.54

$$\mathfrak{a}^*\mathfrak{a} = (xA)(x\mathfrak{a})^*\mathfrak{a} = (x\mathfrak{a})^*(x\mathfrak{a}) = A.$$ □

Definition 3.56. Seien $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale. Wir sagen $\mathfrak{a}$ teilt $\mathfrak{b}$ ($\mathfrak{a} \mid \mathfrak{b}$), wenn ein ganzes Ideal $\mathfrak{c} \subset A$ mit $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ existiert.

Satz 3.57. *Es gilt*

$$\mathfrak{a} \mid \mathfrak{b} \Longleftrightarrow \mathfrak{b} \subset \mathfrak{a}.$$

Beweis. $\Rightarrow$: Aus $\mathfrak{ac} = \mathfrak{b}$ und $\mathfrak{c} \subset A$ folgt $\mathfrak{b} = \mathfrak{ac} \subset \mathfrak{a}A = \mathfrak{a}$.
$\Leftarrow$ $\mathfrak{a} = (0)$ teilt nur sich selbst, also sei $\mathfrak{a} \neq 0$. Sei $\mathfrak{b} \subset \mathfrak{a}$. Dann ist

$$\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{a} = A$$

ein ganzes Ideal und es gilt $\mathfrak{ac} = \mathfrak{b}$. □

Korollar 3.58. *Für ein ganzes Ideal $0 \neq \mathfrak{a} \subsetneqq A$ gilt $\mathfrak{a}^{n+1} \subsetneqq \mathfrak{a}^n$ für alle $n \in \mathbb{N}$. D.h. wir erhalten eine strikt fallende Folge von Idealen*

$$A \supsetneqq \mathfrak{a} \supsetneqq \mathfrak{a}^2 \supsetneqq \mathfrak{a}^3 \supsetneqq \cdots$$

Beweis. Es gilt $\mathfrak{a}^{n+1} = \mathfrak{a}^n\mathfrak{a} \subset \mathfrak{a}^n A = \mathfrak{a}^n$. Aus $\mathfrak{a}^n = \mathfrak{a}^{n+1}$ würde durch Multiplikation mit $\mathfrak{a}^{-n}$ die Gleichheit $A = \mathfrak{a}$ folgen. □

Beweis von Theorem 3.43. Sei $\mathfrak{a} \subset A$, $\mathfrak{a} \neq 0$, ein ganzes Ideal. Der Fall $\mathfrak{a} = A$ ist formal (A =leeres Produkt von Primidealen). Sei $\mathfrak{a} \subsetneqq A$. Da jedes echte Ideal in einem Primideal liegt und wegen 3.44 finden wir Primideale $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ mit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{a} \subset \mathfrak{p}.$$

Nach 3.45 ist (OE) $\mathfrak{p}_1 \subset \mathfrak{p}$ und daher $\mathfrak{p}_1 = \mathfrak{p}$. Dann gilt

$$\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}_1^{-1}\mathfrak{a} \subset A.$$

Gilt $\mathfrak{p}_1^{-1}\mathfrak{a} = A$, so folgt $\mathfrak{a} = \mathfrak{p}_1$. Ansonsten ist $\mathfrak{p}_1^{-1}A$ in einem Primideal enthalten und wir erhalten induktiv nach $r \leq n$ Schritten

$$\mathfrak{p}_r^{-1}\mathfrak{p}_{r-1}^{-1} \ldots \mathfrak{p}_1^{-1}\mathfrak{a} = A,$$

also $\mathfrak{a} = \mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Es verbleibt die Eindeutigkeit zu zeigen. Sei

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m.$$

Es gilt $\mathfrak{a} \subset \mathfrak{p}_1$ und nach 3.45 gilt (OE) $\mathfrak{q}_1 \subset \mathfrak{p}_1$, also $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplikation mit $\mathfrak{p}_1^{-1}$ gibt

$$\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_m.$$

Dieser Prozess bricht ab und wir erhalten $n = m$ und nach Umnummerierung $\mathfrak{p}_i = \mathfrak{q}_i$. □

Korollar 3.59. *Jedes gebrochene Ideal $\mathfrak{a} \neq 0$ hat eine eindeutige Darstellung der Form*

$$\mathfrak{a} = \prod_{\mathfrak{p}\, PI} \mathfrak{p}^{v_\mathfrak{p}}, \quad v_\mathfrak{p} \in \mathbb{Z},\ v_\mathfrak{p} = 0 \ \textit{ f.f.a. } \mathfrak{p}.$$

Mit anderen Worten: $J(A)$ ist die freie abelsche Gruppe über der Menge der Primideale von A.

Beweis. Schreibe $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}^{-1}$ mit $\mathfrak{b}, \mathfrak{c} \subset A$ und wende 3.43 an. □

Beispiel 3.60. Wir betrachten die Zerlegung

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$.

Sei

$$\mathfrak{p} = (2, 1 + \sqrt{-5}) = 2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$$

und

$$\begin{aligned} \mathfrak{q}_1 &= (3, 1 + \sqrt{-5}), \\ \mathfrak{q}_2 &= (3, 1 - \sqrt{-5}). \end{aligned}$$

Dann gilt mit $A = \mathbb{Z}[\sqrt{-5}]$:

$$\begin{aligned} \mathfrak{p}^2 &= (4, 2(1 + \sqrt{-5}), (1 + \sqrt{-5})^2) \\ &= (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) \\ &\subset (2). \end{aligned}$$

Wegen $2 = (2 + 2\sqrt{-5}) - 4 - (-4 + 2\sqrt{-5}) \in \mathfrak{p}^2$, folgt $\mathfrak{p}^2 = (2)$.

Analog

$$\begin{aligned} \mathfrak{q}_1\mathfrak{q}_2 &= (9, 3(1 + \sqrt{-5}), 3(1 - \sqrt{-5}), 6) \\ &\subset (3) \end{aligned}$$

und $3 = 9 - 6 \in \mathfrak{q}_1\mathfrak{q}_2$, also $\mathfrak{q}_1\mathfrak{q}_2 = (3)$.

Außerdem berechnet man leicht:

$$\begin{aligned} \mathbb{Z}[\sqrt{-5}]/\mathfrak{p} &\cong \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}[\sqrt{-5}]/\mathfrak{q}_i &\cong \mathbb{Z}/3\mathbb{Z} \quad \text{für} \quad i = 1, 2, \end{aligned}$$

also sind $\mathfrak{p}, \mathfrak{q}_1, \mathfrak{q}_2$ Primideale.

Wegen $2 \notin \mathfrak{q}_1$ (sonst $1 = 3 - 2 \in \mathfrak{q}_1$) gilt $1 - \sqrt{-5} = 2 - (1 + \sqrt{-5}) \notin \mathfrak{q}_1$ also $\mathfrak{q}_2 \neq \mathfrak{q}_1$. Folglich ist

$$(6) = \mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2$$

die eindeutige Primidealzerlegung von (6). Schon berechnet: $(2) = \mathfrak{p}^2$, $(3) = \mathfrak{q}_1\mathfrak{q}_2$. Zudem gilt

$$\begin{aligned} (1 + \sqrt{-5}) &= \mathfrak{p}\mathfrak{q}_1, \\ (1 - \sqrt{-5}) &= \mathfrak{p}\mathfrak{q}_2. \end{aligned}$$

Z.B.

$$\mathfrak{p}\mathfrak{q}_1 = (6, 2(1 + \sqrt{-5}), 3(1 + \sqrt{-5}), (1 + \sqrt{-5})^2),$$

also $\mathfrak{p}\mathfrak{q}_1 \subset (1 + \sqrt{-5})$. Andererseits gilt

$$(1 + \sqrt{-5}) = 3(1 + \sqrt{-5}) - 2(1 + \sqrt{-5}) \in \mathfrak{p}\mathfrak{q}_1.$$

Für ganze Ideale $0 \neq \mathfrak{a}, \mathfrak{b} \subset A$ kann man nun mit Hilfe von 3.43 in natürlicher Weise den ggT definieren. Ist $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, $\mathfrak{b} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n}$ (Exponent $= 0$ erlaubt), so setzt man

$$\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{\min(e_1, f_1)} \cdots \mathfrak{p}_n^{\min(e_n, f_n)}.$$

Satz 3.61. *Für $0 \neq \mathfrak{a}, \mathfrak{b} \subset A$ gilt* $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$.

Beweis. Nach 3.57 ist der ggT das kleinste Ideal, das sowohl $\mathfrak{a}$ also auch $\mathfrak{b}$ umfasst, also $\mathfrak{a} + \mathfrak{b}$. □

Satz 3.62. *Für ein ganzes Ideal $\mathfrak{a} \subsetneq A$ gilt*

$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n = (0).$$

Beweis. $\mathfrak{b} := \bigcap_{n=1}^{\infty} \mathfrak{a}^n$ ist ein Ideal, das durch beliebige Potenzen von $\mathfrak{a}$ teilbar ist. Für $\mathfrak{b} \neq (0)$ würde dies der eindeutigen Primzerlegung widersprechen. □

Bemerkung 3.63. Die Eigenschaft aus 3.62 heißt: „A ist $\mathfrak{a}$-adisch separiert“. Sie gilt allgemeiner für nullteilerfreie noethersche Ringe (siehe Algebra 2, 24.17).

Um nun doch effektiv mit Elementen von A rechnen zu können muss man die folgenden Effekte untersuchen:

1) Wie weit weichen Ideale davon ab Hauptideal zu sein?
2) Wie weit bestimmt ein Hauptideal seinen Erzeuger?

Zu 2) Wegen $(x) = (y) \Longleftrightarrow x = uy$, $u \in A^\times$ müssen wir die Einheitengruppe von A bestimmen.

Zu 1)

Definition 3.64. Sei $P(A) \subset J(A)$ die Untergruppe der gebrochenen Hauptideale $\neq 0$. Die Faktorgruppe

$$Cl(A) := J(A)/P(A)$$

heißt die **Idealklassengruppe** von A.

Wir werden $A^\times$ und $Cl(A)$ im Fall $A = \mathcal{O}_K$, K Zahlkörper genauer untersuchen.

3.5 Idealnorm

Im ganzen Abschnitt sei $K|\mathbb{Q}$ eine endliche Erweiterung. Dann ist $\mathcal{O}_K$ ein Dedekindring. Als abelsche Gruppe gilt (nach 3.22) $\mathcal{O}_K \cong \mathbb{Z}^n$, $n = [K : \mathbb{Q}]$. Ist $\mathfrak{a} \subset \mathcal{O}_K$, $\mathfrak{a} \neq (0)$ ein Ideal und $0 \neq \alpha \in \mathfrak{a}$, so gilt

$$\alpha\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$$

und deshalb auch $\mathfrak{a} \cong \mathbb{Z}^n$. Folglich ist $\mathrm{Rg}_{\mathbb{Z}}(\mathcal{O}_K/\mathfrak{a}) = n - n = 0$ und deshalb ist $\mathcal{O}_K/\mathfrak{a}$ als endlich erzeugte abelsche Gruppe vom Rang Null endlich.

Definition 3.65. Die **Norm** eines Ideals $\mathfrak{a} \subset \mathcal{O}_K$ ist definiert durch

$$\mathfrak{N}(\mathfrak{a}) = \begin{cases} 0, & \mathfrak{a} = 0, \\ \#\mathcal{O}_K/\mathfrak{a}, & \mathfrak{a} \neq 0. \end{cases}$$

Satz 3.66. *Für $a \in \mathcal{O}_K$ gilt*

$$\mathfrak{N}(a\mathcal{O}_K) = |N_{K|\mathbb{Q}}(a)|.$$

Beweis. Es gilt $\mathfrak{N}(a\mathcal{O}_K) = \#\mathrm{coker}\,(\varphi_a)$,

$$\varphi_a : \mathcal{O}_K \hookrightarrow \mathcal{O}_K,\ x \longmapsto ax.$$

Wir stellen φ_a bzgl. einer $\mathbb{Z}$-Basis von $\mathcal{O}_K$ als Matrix dar. Basiswechsel in Quelle und Ziel mit Matrizen aus $Gl_n(\mathbb{Z})$ lassen $\mathrm{coker}\,\varphi_a$ invariant und ändern $\det\varphi_a$ höchstens um ein Vorzeichen. Nach dem Elementarteilersatz für den Hauptidealring $\mathbb{Z}$ hat φ_a nach geeignetem Basiswechsel die Matrixform

$$\begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_n \end{pmatrix}, \quad e_1 \mid e_2 \mid \cdots \mid e_n.$$

Es gilt $N_{K|\mathbb{Q}}(a) = \det\varphi_a = \pm e_1 \cdots e_n$ und

$$\mathrm{coker}\,\varphi_a = \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_n\mathbb{Z},$$

also $\#\mathrm{coker}\,\varphi_a = |e_1 \cdots e_n| = |N_{K|\mathbb{Q}}(a)|$. □

Lemma 3.67. *Für $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ teilerfremd gilt $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.*

Beweis. Nach dem Chinesischen Restsatz gilt

$$\mathcal{O}_K/\mathfrak{ab} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}.$$ □

Jetzt eliminieren wir die Voraussetzung der Teilerfremdheit.

Lemma 3.68. *Sei A ein Dedekindring und $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale $\neq 0$. Dann existiert ein zu $\mathfrak{a}$ teilerfremdes Ideal $\mathfrak{c} \subset A$, $\mathfrak{c} \neq 0$, so dass $\mathfrak{bc}$ ein Hauptideal ist.*

Beweis. Sei $\mathfrak{a} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_n^{a_n}$, $\mathfrak{b} = \mathfrak{p}_1^{b_1} \dots \mathfrak{p}_n^{b_n}$ (Exponent 0 zugelassen). Nach 3.62 existiert für jedes i ein $\alpha_i \in \mathfrak{p}_i^{b_i} \smallsetminus \mathfrak{p}_i^{b_i+1}$. Nach dem Chinesischen Restsatz finden wir $\alpha \in A$ mit $\alpha \equiv \alpha_i \bmod \mathfrak{p}_i^{b_i+1}$, $i = 1, \dots, n$. Die Primidealzerlegung von (α) sieht so aus:

$$(\alpha) = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n} \cdot (\text{Produkt von Primidealen die nicht in } \mathfrak{a} \text{ und } \mathfrak{b} \text{ vorkommen})$$

Wir benennen das letzte Produkt mit $\mathfrak{c}$, also $(\alpha) = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n} \cdot \mathfrak{c}$.

Dann gilt $\mathfrak{a} + \mathfrak{c} = A$ und $\mathfrak{bc} = (\alpha)$. □

Lemma 3.69. *Seien $\mathfrak{a}$, $\mathfrak{b} \subset A$ Ideale $\neq 0$. Dann gibt es einen Isomorphismus von A-Moduln $A/\mathfrak{a} \xrightarrow{\sim} \mathfrak{b}/\mathfrak{ab}$.*

Beweis. Wir wählen $\mathfrak{c}$ wie in 3.68: $\mathfrak{a} + \mathfrak{c} = A$, $\mathfrak{bc} = (\alpha)$, $\alpha \in A$. Wir betrachten die Abbildung

$$\varphi : A \longrightarrow \mathfrak{b}/\mathfrak{ab}, \quad x \longmapsto \alpha x \bmod \mathfrak{ab}.$$

Wegen $\alpha \in \mathfrak{bc} \subset \mathfrak{b}$ ist die Abbildung definiert. Nun gilt

$$\begin{aligned} \ker(\varphi) &= \{x \in A \mid \alpha x \in \mathfrak{ab}\} \\ &= \mathfrak{ab} \cdot (\alpha)^{-1} \cap A \\ &= \mathfrak{ac}^{-1} \cap A \\ &= \mathfrak{c}^{-1}(\mathfrak{a} \cap \mathfrak{c}) \\ (\mathfrak{a} + \mathfrak{c} = (1)): \quad &= \mathfrak{c}^{-1}(\mathfrak{ac}) = \mathfrak{a}. \end{aligned}$$

Bleibt die Surjektivität von φ zu zeigen: Es gilt $\mathfrak{a} + \mathfrak{c} = A \Rightarrow \mathfrak{ab} + \mathfrak{bc} = \mathfrak{b} \Rightarrow \mathfrak{ab} + (\alpha) = \mathfrak{b}$. □

Satz 3.70. *Für Ideale $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ gilt $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.*

Beweis. Ist $\mathfrak{a} = 0$ oder $\mathfrak{b} = 0$, so ist die Aussage trivial. Sei $\mathfrak{a} \neq 0 \neq \mathfrak{b}$. Dann gilt:

$$\begin{aligned} \mathfrak{N}(\mathfrak{ab}) = \#\mathcal{O}_K/\mathfrak{ab} &= (\#\mathcal{O}_K/\mathfrak{b})\#(\mathfrak{b}/\mathfrak{ab}) \\ 3.69: &= \mathfrak{N}(\mathfrak{b}) \cdot \#(\mathcal{O}_K/\mathfrak{a}) \\ &= \mathfrak{N}(\mathfrak{a}) \cdot \mathfrak{N}(\mathfrak{b}). \end{aligned}$$

□

Satz 3.71. *Sei $K|\mathbb{Q}$ galoissch. Dann gilt*

$$\prod_{\sigma \in \mathrm{Gal}(K|\mathbb{Q})} \sigma(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a}) \cdot \mathcal{O}_K.$$

Erläuterung: Für $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ und $\alpha \in \mathcal{O}_K$ gilt $\sigma(\alpha) \in \mathcal{O}_K$. Daher ist mit $\mathfrak{a}$ auch $\sigma(\mathfrak{a}) \subset \mathcal{O}_K$ ein Ideal: $\alpha \in \mathcal{O}_K$, $a \in \sigma(\mathfrak{a}) \Rightarrow \alpha a = \sigma(\sigma^{-1}(\alpha)a) \in \sigma(\mathfrak{a})$.

Wir beweisen den Satz später.

Jetzt verallgemeinern wir den Begriff der Diskriminante. Wie oben sehen wir: Jedes gebrochene Ideal $0 \neq \mathfrak{a} \subset K$ ist als abelsche Gruppe $\cong \mathbb{Z}^n$ und für $\mathfrak{a} \subset \mathfrak{a}'$ gilt: $(\mathfrak{a}' : \mathfrak{a}) < \infty$

Definition 3.72. Sei $0 \neq \mathfrak{a} \subset K$ ein gebrochenes Ideal und

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

Wir setzen

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Sp}_{K|\mathbb{Q}}(\alpha_i\alpha_j)).$$

Diese Definition hängt nicht von der Wahl der Basis $\alpha_1, \ldots, \alpha_n$ ab. Nach 3.20 gilt $d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i\alpha_j)^2$ wobei $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$.

Satz 3.73. *Sind $0 \neq \mathfrak{a} \subset \mathfrak{a}' \subset K$ gebrochene Ideale, so gilt*

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}').$$

Insbesondere gilt für ein ganzes Ideal $\mathfrak{a} \subset \mathcal{O}_K$

$$d(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})^2 \cdot d_K.$$

Beweis. Sei $M \in Gl_n(\mathbb{Q})$ die Basiswechselmatrix von einer Basis von $\mathfrak{a}'$ zu einer von $\mathfrak{a}$. Wegen $\mathfrak{a} \subset \mathfrak{a}'$ gilt $M \in M_{n,n}(\mathbb{Z})$. Wir erhalten $d(\mathfrak{a}) = \det(M)^2 \cdot d(\mathfrak{a}')$. Durch Ändern der Basen bekommen wir M auf Diagonalform (Elementarteilersatz) und sehen

$$|\det(M)| = (\mathfrak{a}' : \mathfrak{a}).$$

Dies zeigt die erste Behauptung. Die zweite folgt, da per definitionem $d_K = d(\mathcal{O}_K)$, $\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$. □

4 Endlichkeitssätze für Zahlkörper

4.1 Gitter

Definition 4.1. Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum. Ein **Gitter** in V ist eine Untergruppe der Form

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

mit linear unabhängigen Vektoren $v_1, \ldots, v_m$ in V. Das m-Tupel $(v_1, \ldots, v_m)$ heißt **Basis** von Γ und die Menge

$$\Phi = \Phi(v_1, \ldots, v_m) = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R} \quad 0 \leq x_i \leq 1\}$$

heißt **Grundmasche**. Das Gitter heißt **vollständig**, wenn $m = n$.

Bemerkungen 4.2. 1) Begriffe wie beschränkt in V, abgeschlossen in V usw. hängen nicht von der Identifikation $V \cong \mathbb{R}^n$ ab!
2) Γ ist genau dann vollständig, wenn die Translate $\Phi + \gamma$, $\gamma \in \Gamma$, ganz V überdecken.
3) nicht jede e.e. Untergruppe von V ist ein Gitter, z.B. $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subset \mathbb{R}$ ist kein Gitter.
4) Ein Gitter ist eine *diskrete Teilmenge*, d.h. zu $\gamma \in \Gamma$ existiert eine offene Umgebung U von γ in V mit $U \cap \Gamma = \{\gamma\}$.

Grund: Ergänze $v_1, \ldots, v_m$ durch Vektoren $v_{m+1}, \ldots, v_n$ zu einer Basis von V. Für $\gamma = a_1 v_1 + \cdots + a_m v_m \in \Gamma$ setze

$$U = \{x_1 v_1 + \cdots + x_n v_n \mid |a_i - x_i| < 1, \quad i = 1, \ldots, m\}.$$

Satz 4.3. *Eine Untergruppe $\Gamma \subset V$ ist genau dann ein Gitter, wenn sie diskret ist.*

Beweis. Gitter sind diskret. Sei $\Gamma \subset V$ eine diskrete Untergruppe.
Behauptung: Γ hat keine Häufungspunkte in V.
Grund: Da

$$V \times V \longrightarrow V, \ (v, w) \longmapsto v - w,$$

stetig ist, gibt es zu jeder offenen Umgebung U der 0 eine offene Umgebung U' der 0 mit $v, w \in U' \Rightarrow v - w \in U$. Wäre nun $x \in V$ ein Häufungspunkt von Γ, so ist nach der Definition der Durchschnitt $(x + U') \cap \Gamma$ unendlich. Insbesondere existieren $\gamma_1, \gamma_2 \in (x + U') \cap \Gamma$, $\gamma_1 \neq \gamma_2$, also $0 \neq \gamma_1 - \gamma_2 \in U' - U' \subset U$. Wählen wir nun U so klein, dass $U \cap \Gamma = \{0\}$ ist, erhalten wir ein Widerspruch.

Sei nun V_0 der von Γ in V erzeugte $\mathbb{R}$-Untervektorraum und $m = \dim_{\mathbb{R}} V_0$. Sei $u_1, \ldots, u_m$ eine in Γ gelegene Basis von V_0. Setze

$$\Gamma_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subset \Gamma.$$

Dann ist Γ_0 ein vollständiges Gitter in V_0.

Behauptung: $(\Gamma : \Gamma_0) < \infty$.

Beweis der Behauptung: Sei $\Phi_0 \subset V_0$ die Grundmasche zur Basis $u_1, \ldots, u_m$ von Γ_0. Da Γ_0 vollständiges Gitter in V_0 ist, gilt

$$V_0 = \bigcup_{\gamma \in \Gamma_0} \gamma + \Phi_0.$$

Möge $\gamma_i \in \Gamma$ über ein Repräsentantensystem von Γ/Γ_0 laufen. Dann schreiben wir $\gamma_i = \mu_i + \gamma_{0i}$ mit $\mu_i \in \Phi_0$, $\gamma_{0i} \in \Gamma_0$. Die $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$ liegen in der beschränkten Menge Φ_0 und haben keine Häufungspunkt in $V \Rightarrow$ es sind nur endlich viele.

Sei nun $q = (\Gamma : \Gamma_0)$. Dann gilt $q\Gamma \subset \Gamma_0$, also $\Gamma \subset \frac{1}{q}\Gamma_0$. Daher ist Γ als Untergruppe einer freien abelschen Gruppe von endlichem Rang selbst frei, d.h. es existiert eine $\mathbb{Z}$-Basis $v_1, \ldots, v_r$ von Γ, $r \leq m$. Nun erzeugt Γ den Vektorraum V_0, also erzeugen $v_1, \ldots, v_r$ ganz $V_0 \Rightarrow r = m$ und $v_1, \ldots, v_m$ sind linear unabhängig. □

Lemma 4.4. *Ein Gitter $\Gamma \subset V$ ist genau dann vollständig wenn eine beschränkte Teilmenge $M \subset V$ existiert, so dass*

$$V = \bigcup_{\gamma \in \Gamma} \gamma + M.$$

Beweis. Ist Γ vollständig, so wähle für M eine Grundmasche. Umgekehrt sei M wie oben. Sei V_0 der durch Γ aufgespannte Unterraum. Gilt $V_0 = V$, sind wir fertig. Ansonsten wählen wir eine beliebige Metrik auf V, d.h. wir machen V zu einem euklidischen Vektorraum. Da M beschränkt ist liegt jeder Punkt $x \in V$ mit $d(x, V_0)$ hinreichend groß nicht in $V_0 + M \supset \Gamma + M$. Widerspruch. □