

Algebraische Zahlentheorie

Goethe–Universität Frankfurt — Wintersemester 2015/2016
für Bachelor und Master

JAKOB STIX

ZUSAMMENFASSUNG. — Die Vorlesung Algebraische Zahlentheorie behandelt Dedekindringe, speziell Ringe von ganzalgebraischen Zahlen, die Geometrie der Zahlen nach Minkowski und damit die Endlichkeit der Klassengruppe und den Dirichletschen Einheitensatz, Ringerweiterungen von Dedekindringen, Verzweigungstheorie, und wofür die Zeit noch bleibt.

Dieses Skript wird fortlaufend aktualisiert. Es muß davon ausgegangen werden, daß es noch einige Zeit dauern wird, bis eine stabile Version entstanden ist und die größten Fehler korrigiert sind. Sie lesen das Skript **auf eigene Gefahr!**

Bitte teilen Sie mir Korrekturvorschläge per Email oder persönlich nach der Vorlesung mit.

INHALTSVERZEICHNIS

1. Einführung	3
Literatur	3
Teil 1. Dedekindringe	4
2. Ganzalgebraische Zahlen	4
2.1. Ganz Elemente und Ringerweiterungen	4
2.2. Der ganze Abschluß	6
2.3. Ganzzahlringe	7
2.4. Die Diskriminante und Spurform	8
2.5. Die additive Struktur	9
2.6. Ganzzahlbasen, Ordnungen und Diskriminante	9
2.7. Algebraische Struktur von Ordnungen	14
3. Dedekindringe	15
3.1. Ganzzahlringe sind Dedekindringe	15
3.2. Diskrete Bewertungsringe	17
3.3. Lokalisieren von Ringen, Moduln, Idealen und Algebren	22
3.4. Lokalisieren und Ganzheit	28
3.5. Lokale Eigenschaften	30
4. Die Klassengruppe	31
4.1. Gebrochene und invertierbare Ideale	32
4.2. Divisoren und Klassengruppe	35
4.3. Schwache Approximation	38
Teil 2. Geometrie der Zahlen	41
5. Gitter	41
5.1. Algebraische und topologische Eigenschaften von Gittern	41
5.2. Metrische Eigenschaften von Gittern	43
6. Der Minkowski–Raum	45
6.1. Unendliche Stellen eines Zahlkörpers	45
6.2. Die lokale Beschreibung eines Zahlkörpers bei unendlichen Stellen	46
6.3. Die natürliche hermitesche Metrik	47
6.4. Diskriminante und Volumen im Minkowski–Raum	47

6.5. Kanonisches Maß versus Lebesgue-Maß	49
7. Endlichkeitssätze — additive Theorie	49
7.1. Die Norm eines gebrochenen Ideals	49
7.2. Anwendung des Minkowskischen Gitterpunktsatzes	51

1. EINFÜHRUNG

Die Zahlentheorie beschäftigt sich unter anderem mit den (rationalen) Lösungen von Polynomgleichungen mit rationalen Koeffizienten. Dies führt zwangsläufig auf Zahlkörpererweiterungen F/\mathbb{Q} , das sind algebraische Erweiterungen von \mathbb{Q} mit endlichem Grad $[F : \mathbb{Q}]$. Denn zu einem irreduziblen Polynom $f(X) \in \mathbb{Q}[X]$ liefert der Zahlkörper $F = \mathbb{Q}[X]/(f)$ die universelle Lösung $(X \bmod f) \in F$.

Algebraische Zahlentheorie verleiht algebraischen Zahlkörpern arithmetische Feinstruktur. Dazu betrachtet man den Ring der ganzen Zahlen $\mathfrak{o}_F \subseteq F$ mit seinen Primidealen. Dieser verhält sich in mancherlei Hinsicht wie eine glatte Kurve. Zum Beispiel gibt es lokale Parameter. Wenn in \mathfrak{o}_F eindeutige Primfaktorzerlegung gilt, sind dies genau die Primelemente in \mathfrak{o}_F . Zumindest lokal gibt es immer eindeutige Primfaktorzerlegung, also auch lokale Parameter. Erweiterungen der Ganzzahlringen entsprechen verzweigte Überlagerungen von glatten Kurven: zumindest im zahmen Fall wird lokal aus einem Parameter eine Wurzel gezogen und geometrisch entsteht ein Verhalten wie bei der Funktion

$$z \mapsto z^e$$

im Komplexen. Es gibt aber auch wilde Verzweigung, und dies macht algebraische Zahlentheorie komplizierter als das geometrische Analogon der glatten Kurve.

In manch anderer Hinsicht benimmt sich \mathfrak{o}_F wie ein offener Teil eines 3-dimensionalen Gebildes, in dem die Primzahlen wie eindimensionale Knoten immersiirt sind. Diese Sichtweise trifft bei kohomologischen Fragen auf, zu denen diese Vorlesung hinführen möchte (das Ziel aber nicht erreichen wird).

LITERATUR

- [Mi] James S. Milne, [Algebraic number theory](#), online lecture notes.
- [Neu06] Jürgen Neukirch, [Algebraische Zahlentheorie](#), Nachdruck, Springer, 2006.
- [Sch07] Alexander Schmidt, [Einführung in die algebraische Zahlentheorie](#), Springer, 2007, xi+215 Seiten.
- [Ser79] Jean-Pierre Serre, [Local fields](#), Springer, Graduate Texts in Mathematics 67, 1979.

Teil 1. Dedekindringe

2. GANZALGEBRAISCHE ZAHLEN

2.1. Ganz Elemente und Ringerweiterungen. Wir wollen die ganzen Zahlen \mathbb{Z} verallgemeinern. Dazu brauchen wir den Begriff einer ganzen Ringerweiterung.

Definition 2.1. (1) In einem Ringhomomorphismus $A \rightarrow B$ heißt ein Element $b \in B$ ganz über A , wenn es ein normiertes Polynom

$$f(X) = X^d + a_1 X^{d-1} + \dots + a_d \in A[X]$$

gibt mit $f(b) = 0$ in B . Ein solches Polynom nennen wir **Ganzheitspolynom** für b .

(2) Ein Ringhomomorphismus $A \rightarrow B$ heißt **ganz**, wenn alle $b \in B$ ganz über A sind.

Beispiel 2.2. (1) Jedes $b \in \text{im}(A \rightarrow B)$ ist ganz über A . Das lineare Polynom $X - a$ ist ein Ganzheitspolynom für $f(a)$.

(2) Ein surjektiver Ringhomomorphismus $A \rightarrow B$ ist ganz.

(3) In einer Körpererweiterung $K \hookrightarrow L$ ist ein $y \in L$ ganz über K genau dann, wenn y algebraisch über K ist. Eine ganze Körpererweiterung ist dasselbe wie eine algebraische Körpererweiterung.

(4) Sei $B \subseteq C$ ein Teilring und $A \rightarrow B$ ein Ringhomomorphismus, damit auch die Ersetzung $A \rightarrow C$. Ein Element $b \in B$ ist auch ein Element von C . Dann ist b ganz über A als Element von B genau dann, wenn b ganz ist über A als Element von C .

Ein ganzes Element zu sein hängt also nur von der von b erzeugten Unteralgebra $A[b] \subseteq B$ ab, also dem Bild von $A[X] \rightarrow B$ mit $X \mapsto b$.

(5) Sei $A_0 \subseteq B$ das Bild von $A \rightarrow B$. Dann ist ein $b \in B$ ganz über A genau dann, wenn es ganz über A_0 ist.

Wie beim Begriff des algebraischen Elements bei Körpererweiterungen brauchen wir ein besseres Kriterium für *ganz*, um zu zeigen, daß Summen und Produkte von ganzen Elementen wieder ganz sind.

Satz 2.3. Sei $A \rightarrow B$ ein Ringhomomorphismus und $b \in B$. Dann

$$b \text{ ist ganz über } A \iff A[b] \text{ ist endlich erzeugter } A\text{-Modul.}$$

Genauer:

(1) Sind $b_1, \dots, b_n \in B$ ganz über A , dann ist die davon erzeugte A -Unteralgebra

$$A[b_1, \dots, b_n] \subseteq B$$

als A -Modul endlich erzeugt.

(2) Wenn $b \in B$ in einer A -Unteralgebra $B_0 \subseteq B$ liegt, die als A -Modul endlich erzeugt ist, dann ist b ganz über A .

Beweis. (1) Die A -Algebra $A[b_1, \dots, b_n]$ ist das Bild des Polynomrings $A[X_1, \dots, X_n]$ unter Auswertung in $X_i \mapsto b_i$. Daher wird $A[b_1, \dots, b_n]$ von den Bildern der Monome $b_1^{e_1} \dots b_n^{e_n}$ als A -Modul erzeugt.

Wir nehmen nun an, daß die b_i ganz über A sind mit Ganzheitsrelationen vom Grad d_i . Dann erzeugen schon die Monome $b_1^{e_1} \dots b_n^{e_n}$ mit $e_i < d_i$. Dies zeigt man per Induktion nach dem Grad, in dem man die Ganzheitsrelation nutzt, um einen Faktor $b_i^{d_i}$ in einem Monom durch eine Linearkombination von b_i -Potenzen mit kleinerem Exponenten zu ersetzen.

Von diesen Monomen mit $e_i < d_i$ für alle i gibt es nur endlich viele.

(2) Sei $x_1, \dots, x_r \in B_0$ ein Erzeugendensystem als A -Modul. Dann gibt es $c_{ij} \in A$ mit

$$bx_i = \sum_{j=1}^r c_{ij} x_j$$

Mit der Matrix $C = (c_{ij}) \in M_r(A)$, die auf B_0^r wirkt erhalten wir

$$\begin{pmatrix} bx_1 \\ \vdots \\ bx_r \end{pmatrix} = C \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}$$

oder $M = b \cdot \mathbf{1} - C$ annulliert den Vektor mit Einträgen x_i . Sei $M^\#$ die adjunkte Matrix mit $M^\#M = \det(M) \cdot \mathbf{1}$. Dann gilt

$$0 = M^\#M \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \det(M) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}.$$

Also annulliert $\det(M)$ jeden der x_i und damit $\det(M) \cdot B_0 = 0$. Wegen $1 \in B_0$ folgt $\det(M) = 0 \in B$.

Wenn wir $\det(M)$ nach der Leibniz-Formel ausrechnen, dann erhalten wir mit dem charakteristischen Polynom

$$\chi_C(X) = X^r + \dots \in A[X]$$

den Satz von Cayley–Hamilton:

$$\chi_C(b) = \det(M) = 0$$

und das ist die gesuchte Ganzheitsrelation für b . \square

Korollar 2.4. Sei $A \rightarrow B$ ein Ringhomomorphismus. Die Menge der über A ganzen Elemente von B bilden eine A -Unteralgebra von B .

Beweis. Wir müssen sehen, daß mit $b_1, b_2 \in B$ ganz über A auch $b_1 + b_2$ und b_1b_2 ganz über A sind. Wegen Satz 2.3 ist $A[b_1, b_2] \subseteq B$ ein endlich erzeugter A -Modul. Diese Unteralgebra enthält Summe und Produkt, und so sind diese ebenfalls ganz über A wieder mit Satz 2.3. \square

Korollar 2.5. Seine $A \rightarrow B \rightarrow C$ Ringhomomorphismen. Dann gilt:

- (1) B ganz über A und C ganz über $B \implies C$ ganz über A .
- (2) C ganz über $A \implies C$ ganz über B .
- (3) Wenn $B \subseteq C$ injektiv ist, dann gilt auch:

$$C \text{ ganz über } A \implies B \text{ ganz über } A.$$

Beweis. (2) Eine Ganzheitsrelation für $c \in C$ mit Koeffizienten in A führt via $A \rightarrow B$ zu einer mit Koeffizienten in B .

(3) haben wir bereits behandelt.

(1) Sei $c \in C$ und $f(X) = X^n + b_1X^{n-1} + \dots + b_n \in B[X]$ mit $f(c) = 0$. Sei c_i das Bild von b_i in C . Wir setzen abkürzend

$$A_0 = A[c_1, \dots, c_n] \subseteq C.$$

Dann ist c auch ganz über A_0 , denn alle nötigen Koeffizienten einer Ganzheitsrelation sind vorhanden. Genauer ist

$$A_0[c] = A_0 + A_0c + \dots + A_0c^{n-1}$$

als A -Modul. Weil A_0 als A -Modul nach Satz 2.3 endlich erzeugt ist, denn die b_i sind ganz über A , folgt auch, daß $A_0[c]$ als A -Modul endlich erzeugt ist. Wieder nach Satz 2.3 folgt, daß c ganz über A ist. \square

2.2. Der ganze Abschluß.

Definition 2.6. (1) Ein Ring A heißt **ganz abgeschlossen** in einer Ringerweiterung $A \subseteq B$, wenn jedes $b \in B$, das ganz über A ist, bereits in A liegt.

(2) Der **ganze Abschluß** eines Rings A in einer Ringerweiterung $A \subseteq B$ ist die A -Unteralgebra $\tilde{A} \subseteq B$, die aus allen über A ganzen Elementen von B besteht.

Beispiel 2.7. In einer Körpererweiterung L/K ist der ganze Abschluß von K in L der Zwischenkörper aller über K algebraischen Elemente.

Definition 2.8. Ein **normaler** (oder **ganz abgeschlossener**) Integritätsring ist ein Integritätsring A mit Quotientenkörper K , so daß für alle $x \in K$, die über A ganz sind, gilt $x \in A$.

Beispiel 2.9. (1) Körper sind normale Integritätsringe.

(2) Faktorielle Ringe, also insbesondere Hauptidealringe wie \mathbb{Z} oder Polynomringe $k[X]$ über einem Körper k sind normale Integritätsringe.

Sei A faktoriell und $x = p/q \in K$ ein über A ganzes Element des Quotientenkörpers K von A als gekürzter Bruch mit teilerfremden $p, q \in A$. Sei $f(X) = X^d + a_1X^{d-1} + \dots \in A[X]$ eine Ganzheitsrelation für x . Dann gilt

$$0 = q^d f(x) = p^d + q \cdot (a_1 p^{d-1} + a_2 p^{d-2} q + \dots + a_d q^{d-1}),$$

und q ist ein Teiler von p^d . Dies geht aber bei teilerfremden p, q nur, wenn q eine Einheit ist. Aber dann ist $x = q^{-1}p \in A$.

Proposition 2.10. Sei A ein normaler Integritätsring mit Quotientenkörper K und L/K eine algebraische Körpererweiterung. Sei B der ganze Abschluß von A in L .

(1) B ist ein normaler Integritätsring mit Quotientenkörper L .

(2) Ein $b \in L$ ist ganz über A \iff das Minimalpolynom $P_{b/K}(X)$ von b über K hat Koeffizienten in A .

Beweis. (1) Zu $y \in L$ gibt es $a_i, s \in A$ mit

$$y^n + \frac{a_1}{s} y^{n-1} + \dots + \frac{a_n}{s} = 0.$$

Skalieren mit s liefert

$$(sy)^n + a_1 (sy)^{n-1} + sa_2 (sy)^{n-2} + \dots + s^{n-1} a_n = 0.$$

Daher ist $b = sy$ ganz über A , und $y = \frac{b}{s} \in \text{Quot}(B)$ zeigt $L = \text{Quot}(B)$ (sogar mit Nennern aus A !).

(2) Wenn $P_{b/K}(X)$ Koeffizienten aus A hat, dann ist b ganz über A . Für die Umkehrung erweitern wir L so daß $P_{b/K}(X)$ in L in Linearfaktoren zerfällt. Das ändert nichts an der Frage, ob b ganz über A ist.

Sei $f(X) \in A[X]$ eine Ganzheitspolynom für b . Dann gilt $P_{b/K}(X) \mid f(X)$ in $K[X]$. Insbesondere sind alle Nullstellen von $P_{b/K}(X)$ auch Nullstellen von $f(X)$ und damit auch ganz über A . Die Koeffizienten von $P_{b/K}(X)$ sind Polynomial in den Nullstellen mit Koeffizienten aus \mathbb{Z} , nämlich \pm die elementarsymmetrischen Polynome. Daher sind die Koeffizienten von $P_{b/K}(X)$ aus K und ganz über A . Weil A normal ist, folgt $P_{b/K}(X) \in A[X]$. \square

Korollar 2.11. Mit der Notation wie in Proposition 2.10 gilt: B enthält eine K -Basis von L . Die natürliche Abbildung

$$B \otimes_A K \rightarrow L$$

ist ein Isomorphismus.

Beweis. Das Tensorprodukt ist eine Lokalisierung, also wird das injektive $B \hookrightarrow L$ zum immer noch injektiven $B \otimes_A K \rightarrow L \otimes_A K$. Da aber die Elemente von $A \setminus \{0\}$ in L bereits invertierbar sind, ist $L \otimes_A K = L$. Dies zeigt „Isomorphismus“.

Das Bild der natürlichen Abbildung ist nichts anderes als der K -Spann von B . \square

Norm und Spur berechnen sich als Koeffizienten des Minimalpolynoms. Daher haben wir sofort das folgende Korollar.

Korollar 2.12. *Sei A ein normaler Integritätsring mit Quotientenkörper K und L/K eine endliche algebraische Körpererweiterung. Sei B der ganze Abschluß von A in L . Norm und Spur schränken ein zu*

(1) *einem A -Modulhomomorphismus*

$$\mathrm{tr}_{L/K} : B \rightarrow A,$$

(2) *einer multiplikativen Abbildung*

$$N_{L/K} : B \rightarrow A.$$

2.3. Ganzzahlringe.

Definition 2.13. Ein **Zahlkörper** ist eine endliche Körpererweiterung von \mathbb{Q} .

Nach dem Satz vom primitiven Element kann ein Zahlkörper F von einem geeigneten Element $\alpha \in F$ erzeugt werden. Da F/\mathbb{Q} nur endlich viele Zwischenweiterungen $\mathbb{Q} \subseteq M \subseteq F$ besitzt und jede davon in F ein echter \mathbb{Q} -Untervektorraum ist, tut es jedes

$$\alpha \in F \setminus \bigcup_{M \subsetneq F} M.$$

Damit hat F die Form

$$F = \mathbb{Q}[X]/(f(X))$$

mit dem irreduziblen Minimalpolynom $f(X) = P_{\alpha/\mathbb{Q}}(X) \in \mathbb{Q}[X]$ des Elements α .

Definition 2.14. Der Ring der ganzen algebraischen (oder ganzalgebraischen) Zahlen \mathfrak{o}_F in F ist der ganze Abschluß von \mathbb{Z} in F .

Korollar 2.15. $\mathbb{Z} = \mathfrak{o}_{\mathbb{Q}}$.

Beweis. \mathbb{Z} ist ein Hauptidealring. □

Beispiel 2.16. Die Gaußschen ganzen Zahlen $\mathbb{Z}[i]$ sind der Ring der ganzen Zahlen in $\mathbb{Q}(i)$. Zum einen ist $i^2 = -1$ eine Ganzheitsrelation für i , somit $\mathbb{Z}[i] \subseteq \mathfrak{o}_{\mathbb{Q}(i)}$. Zum andern ist $\mathbb{Z}[i]$ bezüglich der Norm ein euklidischer Ring und damit ein Hauptidealring. Nach Beispiel 2.9 ist damit $\mathbb{Z}[i]$ normal. Jedes über \mathbb{Z} ganze Element von $\mathbb{Q}(i)$ ist erst recht ganz über $\mathbb{Z}[i]$, also bereits in $\mathbb{Z}[i]$. Das zeigt $\mathbb{Z}[i] = \mathfrak{o}_{\mathbb{Q}(i)}$.

Bemerkung 2.17. Aus Beispiel 2.2 (4) schließen wir, daß für ein Element eines Zahlkörpers die Eigenschaft ganzalgebraisch zu sein, nicht vom Zahlkörper abhängt, in dem man es betrachtet. Sei $F \subseteq E$ eine Erweiterung von Zahlkörpern und $x \in F$. Dann ist x ganz als Element von F genau dann, wenn es ganz als Element von E ist. Das führt zu

$$\mathfrak{o}_E \cap F = \mathfrak{o}_F$$

und im Spezialfall zu $\mathfrak{o}_F \cap \mathbb{Q} = \mathbb{Z}$.

Beispiel 2.18. Ein **quadratischer Zahlkörper** ist ein F/\mathbb{Q} vom Grad 2. Diese sind von der Form $F = \mathbb{Q}(\sqrt{d})$ für ein eindeutiges quadratfreies $d \in \mathbb{Z}$. Wir bestimmen mittels Proposition 2.10 den Ganzzahlring \mathfrak{o}_F . Sicher gilt

$$\mathbb{Z}[\sqrt{d}] \subseteq \mathfrak{o}_F,$$

aber nicht immer herrscht hier Gleichheit. Ein $y = a + b\sqrt{d} \in F$ mit $a, b \in \mathbb{Q}$ ist ganz genau dann, wenn

$$\mathrm{tr}(y) = 2a \quad \text{und} \quad N(y) = a^2 - db^2$$

ganze Zahlen sind. Damit hat a höchstens Nenner 2. Weil d quadratfrei ist, gilt dasselbe für b :

$$\mathbb{Z}[\sqrt{d}] \subseteq \mathfrak{o}_F \subseteq \frac{1}{2} \cdot \mathbb{Z}[\sqrt{d}].$$

Aus $N(y) \in \mathbb{Z}$ folgt, daß entweder beide $a, b \in \mathbb{Z}$ oder beide halbzahlig: $a, b \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$, also $a = \alpha/2, b = \beta/2$ mit ungeraden α, β . Letzteres geht nur, wenn $4 \mid \alpha^2 - d\beta^2 \equiv 1 - d \pmod{4}$. Wenn $d \equiv 1 \pmod{4}$, dann ist $\omega = \frac{1+\sqrt{d}}{2}$ ganz als Lösung von

$$X^2 - X + \frac{1-d}{4} = 0.$$

Insgesamt ergibt sich nun für quadratfreies $d \in \mathbb{Z}$:

$$\mathfrak{o}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \pmod{4} \\ \mathbb{Z}[\omega] & d \equiv 1 \pmod{4} \end{cases}$$

Bemerkung 2.19. Aus dem Gauß-Lemma folgt, daß für eine ganzalgebraische Zahl die Ganzheitspolynome in $\mathbb{Z}[X]$ genau die Vielfache in $\mathbb{Z}[X]$ des Minimalpolynoms sind.

2.4. Die Diskriminante und Spurform. Sei $M \simeq A^n$ ein freier A Modul vom Rang n und

$$t : M \times M \rightarrow A$$

eine symmetrische A -Bilinearform auf M . Diese wird nach Wahl einer A -Basis $x_1, \dots, x_n \in M$ durch die Gramsche Matrix

$$G = (t(x_i, x_j)) \in M_n(A)$$

beschrieben. Die Diskriminante der Bilinearform bezüglich der Basis $\underline{x} = (x_1, \dots, x_n)$ ist

$$\Delta = \Delta(x_1, \dots, x_n) = \det(G) \in A.$$

Basiswechsel mit $S \in \mathrm{GL}_n(A)$ transformiert die Gramsche Matrix zu $G' = S^t G S$ und ändert damit die Diskriminante zu

$$\Delta' = \det(S)^2 \cdot \Delta.$$

Wir definieren die **Diskriminante** der A -Bilinearform durch

$$\Delta_M = \Delta(x_1, \dots, x_n) \cdot (A^\times)^2$$

als Element von A bis auf multiplikative Quadrate von Einheiten. Als solche hängt Δ_M nicht von der Wahl der Basis ab.

Bemerkung 2.20. Wenn $A = \mathbb{Z}$, dann liefert die Diskriminante einen Wert in \mathbb{Z} , denn $\mathbb{Z}^\times = \{\pm 1\}$ und Quadrate von Einheiten sind immer 1.

Proposition 2.21. *Eine symmetrische Bilinearform auf einem freien A -Modul M ist perfekt, d.h. die adjungierte Abbildung induziert einen Isomorphismus*

$$M \simeq \mathrm{Hom}_A(M, A)$$

genau dann, wenn $\Delta_M \in A^\times$.

Beweis. Die Gramsche Matrix ist die Matrix der adjungierten Abbildung bezüglich Basis und dualer Basis. \square

Zu einer endlichen Körpererweiterung L/K haben wir die **Spurform**, eine symmetrische K -Bilinearform

$$\begin{aligned} \mathrm{tr}_{L/K} : L \times L &\rightarrow K \\ (x, y) &\mapsto \mathrm{tr}_{L/K}(xy). \end{aligned}$$

Aus der Algebra ist bekannt:

Satz 2.22. L/K ist separabel \iff die Spurform ist nichtausgeartet.

Sei A ein normaler Integritätsring mit Quotientenkörper K . Sei L/K endlich separabel und sei B der ganze Abschluß von A in L . Weil die Spur ganze Elemente auf ganze Elemente abbildet, schränkt die Spurform zu einer A -Bilinearform

$$\mathrm{tr}_{L/K} : B \times B \rightarrow A$$

ein. Diese Spurform sagt sehr viel über die Erweiterung $A \subseteq B$ aus.

2.5. Die additive Struktur. Die Existenz einer Basis wie in der folgenden Proposition wird durch Korollar 2.11 gewährleistet.

Proposition 2.23. *Sei A ein normaler Integritätsring mit Quotientenkörper K . Sei L/K endlich separabel und sei B der ganze Abschluß von A in L . Sei β_1, \dots, β_n eine K -Basis von L mit $\beta_i \in B$. Sei Δ_M die Diskriminante der Spurform eingeschränkt auf $M = \langle \beta_i ; i = 1, \dots, n \rangle_A$. Dann gilt*

$$M \subseteq B \subseteq \frac{1}{\Delta_M} M.$$

Beweis. Sei $x = \sum_i a_i \beta_i \in L$ mit $a_i \in K$ ganz über A . Dann gilt für alle $i = 1, \dots, n$

$$\mathrm{tr}_{L/K}(x\beta_i) \in A$$

weil A normal ist.

Sei G die Gramsche Matrix der Spurform bezüglich der Basis β_1, \dots, β_n . Dann

$$G \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \vdots \\ \sum_j \mathrm{tr}_{L/K}(\beta_i \beta_j) a_j \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ \sum_j \mathrm{tr}_{L/K}(\beta_i x) \\ \vdots \end{pmatrix} \in A^n$$

und aus dem Determinantentrick folgt

$$\Delta_M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = G^\# G \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in G^\# A^n \subseteq A^n. \quad \square$$

Korollar 2.24. *Mit der Notation wie in Proposition 2.23 folgt, daß B ein A -Untermodul eines freien A -Moduls vom Rang $n = [L : K]$ ist.*

Beweis. Der Modul $\frac{1}{\Delta_M} M$ ist freier A -Modul vom Rang n . □

Korollar 2.25. *Sei A ein Hauptidealring mit Quotientenkörper K . Sei L/K endlich separabel und sei B der ganze Abschluß von A in L . Dann ist B ein freier A -Modul vom Rang $[L : K]$.*

Beweis. Hauptidealringe sind normale Integritätsringe. Daher ist B ein Untermodul eines freien Moduls nach Korollar 2.24. Nach dem Elementarteilersatz ist damit B selbst ein freier A -Modul. Den Rang berechnet man aus

$$\mathrm{rg}_A(B) = \dim_K(B \otimes_A K) = \dim_K(L). \quad \square$$

Korollar 2.26. *Sei F ein Zahlkörper. Dann ist \mathfrak{o}_F als abelsche Gruppe frei von Rang $[F : \mathbb{Q}]$.*

Beweis. \mathbb{Z} ist ein Hauptidealring. □

2.6. Ganzzahlbasen, Ordnungen und Diskriminante. Der Ring der ganzen Zahlen \mathfrak{o}_F in einem Zahlkörper ist eine Ordnung in F :

Definition 2.27. Sei F ein Zahlkörper. Eine **Ordnung** in F ist ein Teilring

$$\mathfrak{o} \subseteq F,$$

der

- (i) eine \mathbb{Q} -Basis von F enthält, und

(ii) als abelsche Gruppe endlich erzeugt ist.

Der Ring der ganzen Zahlen \mathfrak{o}_F wird **Maximalordnung** (oder **Hauptordnung**) genannt.

Aus Satz 2.3 folgt, daß eine Ordnung \mathfrak{o} in F in \mathfrak{o}_F enthalten sein muß. Der Name Maximalordnung ist also gerechtfertigt. Weiter ist

$$\mathbb{Q} \otimes \mathfrak{o} = \mathbb{Q}\mathfrak{o} = F$$

und daher \mathfrak{o} als abelsche Gruppe frei vom Rang $[F : \mathbb{Q}]$.

Definition 2.28. Die (**absolute**) **Diskriminante** einer Ordnung $\mathfrak{o} \subseteq F$ ist die Diskriminante der Spurform

$$\mathrm{tr}_{F/\mathbb{Q}} : \mathfrak{o} \times \mathfrak{o} \rightarrow \mathbb{Z}$$

und damit ein Element $\Delta_{\mathfrak{o}} \in \mathbb{Z}$.

Die Diskriminante der Maximalordnung \mathfrak{o}_F bezeichnen wir mit

$$\Delta_F$$

und nennen sie die (**absolute**) **Diskriminante** des Zahlkörpers F .

Bemerkung 2.29. Wir betonen nochmals, daß man die Diskriminante durch Wahl einer \mathbb{Z} -Basis $\alpha_1, \dots, \alpha_n$ von \mathfrak{o}_F durch

$$\Delta_F = \det(\mathrm{tr}_{F/\mathbb{Q}}(\alpha_i \alpha_j)) \in \mathbb{Z}$$

berechnet. Die Diskriminante ist eine wichtige Invariante von F , die wir später als Wurzel eines Volumens wiederfinden.

Proposition 2.30. Sei $\alpha_1, \dots, \alpha_n \in F$ eine \mathbb{Q} -Basis eines Zahlkörpers aus ganzen Elementen und $M = \langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{Z}}$ die von diesen Elementen erzeugte abelsche Gruppe. Dann gilt

$$\Delta_M = (\mathfrak{o}_F : M)^2 \cdot \Delta_F.$$

Insbesondere, wenn Δ_M quadratfrei ist, dann ist bereits $\mathfrak{o}_F = M$.

Beweis. Wir berechnen Δ_M bezüglich einer geeigneten \mathbb{Z} -Basis. Nach dem Elementarteilersatz gibt es $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$ und eine \mathbb{Z} -Basis $\alpha_1, \dots, \alpha_n$ von \mathfrak{o}_F mit

$$M = \langle \lambda_1 \alpha_1, \dots, \lambda_n \alpha_n \rangle_{\mathbb{Z}}.$$

Die Basiswechselmatrix von der Basis für \mathfrak{o}_F zur Basis für M ist diagonal mit Einträgen λ_i . Es gilt

$$(\mathfrak{o}_F : M) = \# \prod_{i=1}^n (\mathbb{Z}/\lambda_i \mathbb{Z}) = \prod_{i=1}^n |\lambda_i|.$$

Für die Determinanten der entsprechenden Gramschen Matrizen ergibt sich

$$\Delta_M = (\mathrm{tr}_{F/\mathbb{Q}}(\lambda_i \alpha_i \lambda_j \alpha_j)) = \left(\prod_i \lambda_i \right)^2 \cdot \Delta_F = (\mathfrak{o}_F : M)^2 \cdot \Delta_F.$$

Das insbesondere ist dann klar. □

Korollar 2.31. Sei $\mathfrak{o} \subseteq F$ eine Ordnung. Dann ist $(\mathfrak{o}_F : \mathfrak{o}) < \infty$ und

$$\Delta_{\mathfrak{o}} = (\mathfrak{o}_F : \mathfrak{o})^2 \cdot \Delta_F.$$

Beispiel 2.32. Sei $D = e^2 \cdot d$ mit $e, d \in \mathbb{Z}$ und $d \neq 1$ quadratfrei. Dann ist $F = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper und

$$\mathfrak{o} = \mathbb{Z}[\sqrt{D}] \subseteq \mathfrak{o}_F$$

eine Ordnung der Diskriminante (bezüglich \mathbb{Z} -Basis $1, \sqrt{D}$ berechnet)

$$\Delta_{\mathfrak{o}} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D.$$

Beispiel 2.33. Sei $d \neq 1$ quadratfrei und $F = \mathbb{Q}(\sqrt{d})$ der zugehörige quadratische Zahlkörper. Für $d \not\equiv 1 \pmod{4}$ ist

$$\mathfrak{o}_F = \mathbb{Z}[\sqrt{d}]$$

und

$$\Delta_F = 4d$$

haben wir bereits ausgerechnet. Sei deshalb nun $d \equiv 1 \pmod{4}$ und $\omega = \frac{1+\sqrt{d}}{2}$. Dann ist

$$\mathfrak{o}_F = \mathbb{Z}[\omega]$$

und (bezüglich der Basis $1, \omega$)

$$\Delta_F = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

Satz 2.34 (Stickelbergerscher Diskriminantensatz). *Sei F ein Zahlkörper. Dann ist die Diskriminante Δ_F entweder kongruent 0 oder 1 modulo 4.*

Beweis. Sei $\alpha_1, \dots, \alpha_n$ eine \mathbb{Z} -Basis von \mathfrak{o}_F und $\sigma_1, \dots, \sigma_n$ seien die Einbettungen $F \hookrightarrow \bar{\mathbb{Q}}$. In der Leibniz-Formel für die Determinante der Matrix $C = (\sigma_i(\alpha_j))$ schreiben wir P für die Summe der Beiträge zu geraden Permutationen, und N für die Summe der Beiträge zu ungeraden Permutationen:

$$\det(C) = P - N.$$

Sei \tilde{F} eine Galoissche Hülle von F/\mathbb{Q} . Die Wirkung von $G = \text{Gal}(\tilde{F}/\mathbb{Q})$ auf C ist durch Permutation der Zeilen. Daher gilt für alle $g \in G$:

$$g(\{P, N\}) = \{P, N\}.$$

Demnach sind Summe $P + N$ und Produkt PN Galoisinvariant, also in \mathbb{Q} . Da dies polynomiale Ausdrücke in den Einträgen von C und damit ganze algebraische Zahlen sind, gilt $P + N, PN \in \mathbb{Z}$. Demnach

$$\Delta_F = \det(C)^2 = (P - N)^2 = (P + N)^2 - 4PN \equiv (P + N)^2 \pmod{4}.$$

Quadrate sind aber 0 oder 1 (mod 4). □

Satz 2.35. *Seien F_1, F_2 Zahlkörper mit zueinander teilerfremder Diskriminante Δ_{F_1} und Δ_{F_2} , und sei $F = F_1 F_2$ das Kompositum.*

(1) *Sind $\alpha_1, \dots, \alpha_n$ eine \mathbb{Z} -Basis von \mathfrak{o}_{F_1} und β_1, \dots, β_m eine \mathbb{Z} -Basis von \mathfrak{o}_{F_2} , dann liefert*

$$\{\alpha_i \beta_j ; 1 \leq i \leq n, 1 \leq j \leq m\}$$

eine \mathbb{Z} -Basis von \mathfrak{o}_F .

(2) $\mathfrak{o}_F = \mathfrak{o}_{F_1} \otimes_{\mathbb{Z}} \mathfrak{o}_{F_2}$.

(3) *Die Diskriminante von F berechnet sich als*

$$\Delta_F = \Delta_{F_1}^{[F_2:\mathbb{Q}]} \cdot \Delta_{F_2}^{[F_1:\mathbb{Q}]}.$$

Beweis. □

Sei L/K eine endliche separable Erweiterung und \bar{K} ein algebraischer Abschluß von K . Dann gilt

$$\text{tr}_{L/K}(y) = \sum_{\sigma \in \text{Hom}_K(L, \bar{K})} \sigma(y).$$

Damit bekommt die Gramsche Matrix zur Spurform eine besondere Gestalt. Wir nummerieren

$$\text{Hom}_K(L, \bar{K}) = \{\sigma_1, \dots, \sigma_n\}$$

mit $n = [L : K]$ und betrachten für eine K -Basis $\alpha_1, \dots, \alpha_n$ von L die Matrix

$$C = (\sigma_i(\alpha_j)) \in M_n(\bar{K}).$$

Dann ist

$$(C^t C)_{ij} = \sum_k \sigma_k(\alpha_i) \sigma_k(\alpha_j) = \text{tr}_{L/K}(\alpha_i \alpha_j)$$

somit $C^t C$ die Gramsche Matrix der Spurform. Folglich gilt in der üblichen Notation für $M = \langle \alpha_1, \dots, \alpha_n \rangle_A$

$$\Delta_M = \det(C)^2.$$

Dies nutzen wir nun für spezielle Ordnungen aus.

Beispiel 2.36. Seien F ein Zahlkörper und $\alpha \in \mathfrak{o}_F$ ein ganzes primitives Element, also $F = \mathbb{Q}(\alpha)$. Dann ist $\mathbb{Z}[\alpha] \subseteq \mathfrak{o}_F$ eine Ordnung mit \mathbb{Z} -Basis $1, \alpha, \dots, \alpha^{n-1}$, wobei $n = [F : \mathbb{Q}]$. Wir schreiben $f(X)$ für das Minimalpolynom von α und faktorisieren (über einer Galoisschen Hülle):

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

wobei $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ die verschiedenen konjugierten von α sind. Aus der Produktregel folgt

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Seien $\sigma_1, \dots, \sigma_n$ die verschiedenen Einbettungen von F nach $\bar{\mathbb{Q}}$. Dann gilt (berechnet bezüglich der \mathbb{Z} -Basis $1, \alpha, \dots, \alpha^{n-1}$) mit der Formel für die Vandermonde-Determinante

$$\begin{aligned} \Delta_{\mathbb{Z}[\alpha]} &= \det((\sigma_i(\alpha^j))^2) = \det((\alpha_i^j))^2 \\ &= \left(\prod_{i < j} (\alpha_i - \alpha_j) \right)^2 = (-1)^{d(d-1)/2} \prod_i f'(\alpha_i) = (-1)^{d(d-1)/2} N_{F/\mathbb{Q}}(f'(\alpha)). \end{aligned} \quad (2.1)$$

Beispiel 2.37. Sei $F = \mathbb{Q}(\alpha)$ mit Minimalpolynom von α von der Form

$$f(X) = X^n + aX + b.$$

Dann ist

$$\Delta_{\mathbb{Z}[\alpha]} = (-1)^{n(n-1)/2} \cdot (n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n).$$

Wir müssen wegen (2.1) nur die Norm der Ableitung ausgewertet in α ausrechnen. Dazu setzen wir

$$\beta = f'(\alpha) = n\alpha^{n-1} + a$$

und

$$-\alpha\beta = -n\alpha^n - a\alpha = n(a\alpha + b) - a\alpha = (n-1)a(\alpha + \varepsilon)$$

wobei

$$\varepsilon = \frac{nb}{(n-1)a}.$$

Uns interessiert $N_{F/\mathbb{Q}}(\beta)$, wir kennen $N_{F/\mathbb{Q}}(-\alpha) = b$ aus dem konstanten Term des Minimalpolynoms und wir berechnen mittels Taylorentwicklung

$$N_{F/\mathbb{Q}}(\alpha + \varepsilon) = (-1)^n \cdot \text{konst. Koeff. von } f(X - \varepsilon) = (-1)^n f(-\varepsilon) = \varepsilon^n + (-1)^{n-1} a\varepsilon + (-1)^n b.$$

Daher gilt

$$\begin{aligned} b \cdot N_{F/\mathbb{Q}}(f'(\alpha)) &= N_{F/\mathbb{Q}}(-\alpha\beta) = N_{F/\mathbb{Q}}((n-1)a(\alpha + \varepsilon)) \\ &= (n-1)^n a^n N_{F/\mathbb{Q}}(\alpha + \varepsilon) \\ &= (n-1)^n a^n \cdot (\varepsilon^n + (-1)^{n-1} a\varepsilon + (-1)^n b) \\ &= (n-1)^n a^n \left(\left(\frac{nb}{(n-1)a} \right)^n + (-1)^{n-1} a \frac{nb}{(n-1)a} + (-1)^n b \right) \\ &= (nb)^n + (-1)^{n-1} (n-1)^{n-1} nba^n + (-1)^n (n-1)^n a^n b \\ &= (nb)^n + (-1)^{n-1} (n-1)^{n-1} ba^n \end{aligned}$$

und daraus folgt mit (2.1) die Behauptung.

Speziell für ein Minimalpolynom

$$f(X) = X^3 + aX + b$$

eines primitiven Elements eines kubischen Zahlkörpers folgt

$$\Delta_{\mathbb{Z}[\alpha]} = -(27b^2 + 4a^3).$$

Der folgende Satz gibt Hilfestellung beim Auffinden einer \mathbb{Z} -Basis von \mathfrak{o}_F .

Satz 2.38 (Struktursatz). *Sei α ein primitives, ganz algebraisches Element des Zahlkörpers F , und $[F : \mathbb{Q}] = n$. Dann gibt es $f_0 = 1, f_1(X), \dots, f_n(X) \in \mathbb{Q}[X]$ und natürliche Zahlen*

$$d_1 \mid d_2 \mid \dots \mid d_{n-1}$$

mit

$$d_i f_i(X) \in \mathbb{Z}[X]$$

und

$$1, f_1(\alpha), \dots, f_{n-1}(\alpha)$$

ist eine \mathbb{Z} -Basis von \mathfrak{o}_F . Weiter gilt

$$\Delta_{\mathbb{Z}[\alpha]} = \left(\prod_{i=1}^{n-1} d_i \right)^2 \Delta_F.$$

Beweis. Wir setzen für $i = 0, \dots, n-1$

$$M_i = \mathfrak{o}_F \cap \bigoplus_{e \leq i} \mathbb{Q} \cdot \alpha^e,$$

das sind also die Elemente aus \mathfrak{o}_F , die als \mathbb{Q} -Polynom in α den Grad $\leq i$ haben. Dann ist

$$\mathbb{Z} = M_0 \subseteq M_1 \subseteq \dots \subseteq M_{n-1} = \mathfrak{o}_F$$

eine aufsteigende ausschöpfende Filtrierung von \mathfrak{o}_F durch abelsche Untergruppen.

Wir konstruieren nun induktiv d_i und $f_i(X)$ mit

$$M_i = \langle f_0(\alpha), \dots, f_i(\alpha) \rangle_{\mathbb{Z}}.$$

Der Anfang ist klar: $M_0 = \mathbb{Z} = \langle 1 \rangle_{\mathbb{Z}}$. Weiter betrachten wir die Projektion pr_i auf den Koeffizienten von α^i in der exakten Sequenz

$$0 \rightarrow M_{i-1} \rightarrow M_i \xrightarrow{\text{pr}_i} \mathbb{Q}.$$

Da $\text{pr}_i(\alpha^i) = 1 \in \text{im}(\text{pr}_i)$ eine endlich erzeugte Untergruppe von \mathbb{Q} ist, folgt leicht, daß es eine natürliche Zahl $d_i > 0$ mit

$$\text{pr}_i(M_i) = \frac{1}{d_i} \mathbb{Z} \subseteq \mathbb{Q}$$

gibt. Wir wählen

$$f_i(X) = \frac{1}{d_i} X^i + \text{kleinere Grade}$$

so daß $f_i(\alpha) \in M_i$ ein Urbild von $1/d_i$ ist. Dann ist nach Konstruktion

$$\text{pr}_i(\alpha f_{i-1}(\alpha)) = \frac{1}{d_{i-1}} \in \frac{1}{d_i} \mathbb{Z}$$

also $d_{i-1} \mid d_i$ wie behauptet. Ebenso folgt aus der exakten Sequenz sofort

$$M_i = \langle M_{i-1}, f_i(\alpha) \rangle_{\mathbb{Z}} = \langle f_0(\alpha), \dots, f_i(\alpha) \rangle_{\mathbb{Z}}.$$

Es bleibt zu zeigen, daß $d_i f_i(X) \in \mathbb{Z}[X]$. Dazu betrachten wir

$$\frac{d_i}{d_{i-1}} f_i(\alpha) - f_{i-1}(\alpha) \alpha \in M_{i-1}$$

was per Induktion nur noch Teiler von d_{i-1} als Nenner hat. Damit ist per Induktion

$$d_i f_i(X) = d_{i-1} \left(\frac{d_i}{d_{i-1}} f_i(X) - f_{i-1}(X)X \right) + d_i f_{i-1}(X)X \in \mathbb{Z}[X],$$

was zu zeigen war.

Die Aussage über die Diskriminanten folgt aus Proposition 2.30 und der Determinante des Basiswechsels von $1, \alpha, \dots, \alpha^{n-1}$ zu $1, f_1(\alpha), \dots, f_{n-1}(\alpha)$, welche als Diagonalterme genau die d_i hat. \square

2.7. Algebraische Struktur von Ordnungen. Für manche algebraische Fragen ist es nötig, eine \mathbb{Z} -Algebra durch Erzeuger und Relationen darstellen zu können. Unsere Definition des Ganzzahrrings liefert dies nicht.

Proposition 2.39. *Sei F ein Zahlkörper und $\alpha \in f_F$ ein ganzes Element. Sei $f(X) = P_{\alpha/\mathbb{Q}}(X) \in \mathbb{Z}[X]$ das Minimalpolynom von α . Dann induziert die Auswertung in $X = \alpha$ einen Ringisomorphismus*

$$\mathbb{Z}[X]/(f(X)) \xrightarrow{\sim} \mathbb{Z}[\alpha].$$

Beweis. Wir dürfen ohne Einschränkung annehmen, daß $F = \mathbb{Q}(\alpha)$. Dann ist $\mathbb{Z}[\alpha] \subseteq F$ eine Ordnung und als abelsche Gruppe frei vom Rang $n = [F : \mathbb{Q}] = \deg(f)$.

Weil $f(X)$ normiert ist, wird $\mathbb{Z}[X]/(f(X))$ von den Monomen X^i mit $0 \leq i \leq n-1$ als abelsche Gruppe erzeugt. Genauer ist

$$\bigoplus_{i=0}^{n-1} \mathbb{Z} \cdot X^i \simeq \mathbb{Z}[X]/(f(X))$$

als abelsche Gruppe, weil kein Polynom vom Grad $< \deg(f)$ in $\mathbb{Z}[X]$ ein Vielfaches von $f(X)$ sein kann. Daher ist $\mathbb{Z}[X]/(f(X))$ auch eine freie abelsche Gruppe vom Rang $n = [F : \mathbb{Q}]$.

Die Auswertung ist per Definition surjektiv. Es bleibt die Frage, warum die Auswertung injektiv ist. Dies kann man nach $-\otimes_{\mathbb{Z}} \mathbb{Q}$ für die entsprechende \mathbb{Q} -lineare Abbildung von Vektorräumen der Dimension n beantworten. Aber bei Vektorräumen der gleichen Dimension ist surjektiv \iff injektiv. Damit ist alles bewiesen. \square

Wir konstruieren nun ein Beispiel für eine Maximalordnung \mathfrak{o}_F , die nicht von der Form $\mathbb{Z}[\alpha]$ ist.

Beispiel 2.40. Sei p eine Primzahl $\equiv 1 \pmod{8}$. Dann erzeugt

$$\omega = \frac{1 + \sqrt{p}}{2}$$

den Ganzzahrring in $F = \mathbb{Q}(\sqrt{p})$. Die Diskriminante ist $\delta_F = p$. Das Minimalpolynom von ω ist

$$X^2 - X + \frac{1-d}{4}.$$

Es gilt

$$\mathfrak{o}_F/2\mathfrak{o}_F \simeq \mathbb{Z}[X]/(X^2 - X + \frac{1-d}{4}) \otimes_{\mathbb{Z}} \mathbb{F}_2 = \mathbb{F}_2[X]/(X^2 - X + \frac{1-d}{4}) = \mathbb{F}_2[X]/(X(X-1)) = \mathbb{F}_2 \times \mathbb{F}_2.$$

Der letzte Isomorphismus kommt von der Auswertung in 0 für den einen und in $1 \in \mathbb{F}_2$ für den anderen Faktor.

Sei nun $q \neq p$ eine weitere Primzahl $\equiv 1 \pmod{8}$. Dann haben die beiden quadratischen Zahlkörper $\mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{q})$ zueinander teilerfremde Diskriminante. Sei $F = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ das

Kompositum. Den Ganzzahlring \mathfrak{o}_F berechnet man nun mittels Satz 2.35. Insbesondere interessiert uns

$$\begin{aligned} \mathfrak{o}_F/2\mathfrak{o}_F &= \mathfrak{o}_F \otimes \mathbb{F}_2 = (\mathfrak{o}_{\mathbb{Q}(\sqrt{p})} \otimes \mathfrak{o}_{\mathbb{Q}(\sqrt{q})}) \otimes \mathbb{F}_2 \\ &= (\mathfrak{o}_{\mathbb{Q}(\sqrt{p})} \otimes \mathbb{F}_2) \otimes_{\mathbb{F}_2} (\mathfrak{o}_{\mathbb{Q}(\sqrt{q})} \otimes \mathbb{F}_2) \\ &= (\mathbb{F}_2 \times \mathbb{F}_2) \otimes_{\mathbb{F}_2} (\mathbb{F}_2 \times \mathbb{F}_2) \\ &= \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2. \end{aligned}$$

Jetzt nehmen wir an, daß mit einem geeigneten $\alpha \in \mathfrak{o}_F$ gilt: $\mathfrak{o}_F = \mathbb{Z}[\alpha]$. Sei $f(X)$ das Minimalpolynom von α . Dann ist

$$\mathfrak{o}_F/2\mathfrak{o}_F \simeq \mathbb{Z}[X]/(f(X)) \otimes \mathbb{F}_2 = \mathbb{F}_2[X]/(f(X))$$

ein Quotient von $\mathbb{F}_2[X]$. Dieser besteht aus 4 Faktoren \mathbb{F}_2 . Die mutmaßliche Surjektion

$$\mathbb{F}_2[X] \twoheadrightarrow \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$$

entspricht Koordinatenweise der Auswertung von X in einem Element $a_i \in \mathbb{F}_2$. Sind zwei der a_i gleich, kann der Ringhomomorphismus nicht surjektiv sein, denn die Werte in den entsprechenden Faktoren sind stets gleich. Nun hat \mathbb{F}_2 nur 2 Elemente. Wir sind mit 4 verschiedenen Faktoren somit überfordert. Folglich kann \mathfrak{o}_F nicht von der Form $\mathbb{Z}[\alpha]$ sein.

3. DEDEKINDRINGE

3.1. Ganzzahlringe sind Dedekindringe. Dedekindringe sind nach Hauptidealringen die nächst komplizierten kommutativen Ringe. Lokal sind sie nichts anderes als Hauptidealringe.

Definition 3.1. Ein **Dedekindring** ist ein noetherscher Integritätsring der Dimension 1, der in seinem Quotientenkörper ganz abgeschlossen ist.

Wir erinnern an die Definition der (Krull-)Dimension eines Rings.

Definition 3.2. Die **(Krull-)Dimension** eines Rings R ist

$$\dim(R) = \sup\{n \mid \text{es gibt eine Kette } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n \text{ von Primidealen in } R\}.$$

Beispiel 3.3. Ein Hauptidealring, der kein Körper ist, ist ein Dedekindring, zum Beispiel \mathbb{Z} oder der Polynomring $k[X]$ über einem Körper k sind Dedekindringe. In der Tat sind Hauptidealringe

- noethersch: jedes Ideal ist von einem Element erzeugt.
- ganz abgeschlossen im Quotientenkörper: Hauptidealringe sind faktoriell und damit normal, Beispiel 2.9.
- Und Hauptidealringe haben Dimension 1, sofern sie kein Körper sind. Primideale sind (0) oder von einem Primelement π erzeugt. Eine maximale Primidealkette sieht daher so aus: $(0) \subsetneq \mathfrak{p} = (\pi)$. Damit ist die Dimension 1.

Satz 3.4. Sei F ein Zahlkörper. Dann ist \mathfrak{o}_F ein Dedekindring.

Beweis. Da \mathbb{Z} als Hauptidealring ein Dedekindring ist, folgt dies sofort aus dem allgemeineren folgenden Satz. □

Satz 3.5. Sei A ein Dedekindring mit Quotientenkörper K und L/K eine endliche separable Erweiterung. Sei B der ganze Abschluß von A in L .

Dann ist B ein Dedekindring mit Quotientenkörper L .

Beweis. Korollar 2.11 zeigt, daß B eine K -Basis von L enthält und daher ist L der Quotientenkörper von B . Als Unterring eines Körpers ist B ein Integritätsring. Per Definition als ganzer Abschluß in L und, weil ganz zu sein transitiv ist, ist B ganz abgeschlossen in L .

Weil L/K endlich separabel ist, zeigt Korollar 2.24, daß B als A -Modul ein Untermodul eines freien A -Moduls vom Rang $[L : K]$ ist. Weil A noethersch ist, ist damit B als A -Modul

noethersch. Jedes Ideal $\mathfrak{b} \subseteq B$ ist insbesondere ein A -Untermodule und als solcher endlich erzeugt (mit Koeffizienten aus A). Damit ist \mathfrak{b} aber auch als B -Modul endlich erzeugt, also ein endlich erzeugtes Ideal. Somit ist B noethersch.

Jetzt zeigen wir, daß $\dim(B) = 1$. Wenn $\dim(B) = 0$, dann ist B selbst ein Körper und somit gleich L , siehe Proposition 2.10. Damit ist aber auch $K \subseteq L$ ganz über A . Weil A ganzabgeschlossen in K ist, folgt $A = K$ und $\dim(A) = 0$, ein Widerspruch.

Jetzt müssen wir nur noch $\dim(B) \leq 1$ zeigen. Als Integritätsring hat B das Primideal (0) . Dies ist das einzige minimale Primideal in B . Wir müssen zeigen, daß jedes Primideal $(0) \neq \mathfrak{q} \subseteq B$ schon ein maximales Ideal ist. Sei nun $\mathfrak{p} = \mathfrak{q} \cap A$. Dann ist die induzierte Abbildung

$$A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$$

injektiv, also A/\mathfrak{p} ein Integritätsring und \mathfrak{p} ein Primideal von A .

Sei $0 \neq y \in \mathfrak{q}$ und sei $f(X) = X^d + a_1X^{d-1} + \dots + a_d \in A[X]$ ein Ganzheitspolynom für y . Weil B ein Integritätsring ist, dürfen wir annehmen, daß $a_d \neq 0$. Dann ist

$$a_d = -y \cdot (y^{d-1} + a_1y^{d-2} + \dots + a_{d-1}) \in \mathfrak{q} \cap A = \mathfrak{p}$$

somit $\mathfrak{p} \neq (0)$.

Weil $\dim(A) = 1$ gilt, muß \mathfrak{p} ein maximales Ideal sein, und $k = A/\mathfrak{p}$ ist ein Körper. Weil B ein endlicher A -Modul ist, wird auch B/\mathfrak{q} als A/\mathfrak{p} -Modul endlich erzeugt. Damit ist B/\mathfrak{q} ein Integritätsring und eine k -Algebra, die ein endlich dimensionaler k -Vektorraum ist. Nach dem folgenden Lemma ist B/\mathfrak{q} ein Körper und \mathfrak{q} deshalb ein maximales Ideal. \square

Lemma 3.6. *Sei k ein Körper, R eine k -Algebra, die ein Integritätsring ist und als k -Vektorraum endlich dimensional ist. Dann ist R ein Körper.*

Beweis. Wir müssen zeigen, daß alle $0 \neq x \in R$ ein Inverses haben. Die Multiplikation

$$x \cdot : R \rightarrow R$$

ist injektiv, weil R ein Integritätsring ist und außerdem in $\text{End}_k(R)$. Für endlich dimensionale k -Vektorräume sind injektive Endomorphismen automatisch bijektiv, also surjektiv. Also gibt es ein $y \in R$ mit $xy = 1$. \square

Bemerkung 3.7. Der Satz von Krull–Akizuki besagt, daß Satz 3.5 auch für beliebige endliche Erweiterungen L/K gilt, die nicht notwendig separabel sind. Die Schwierigkeit hierbei liegt in dem Nachweis, daß der ganze Abschluß B von A wieder noethersch ist. Im Gegensatz zum separablen Fall muß nämlich B im Allgemeinen kein endlich erzeugter A -Modul sein.

Bemerkung 3.8. Sei F ein Zahlkörper und $\mathfrak{o} \subseteq F$ eine Ordnung. Dann ist \mathfrak{o} ein Dedekindring genau dann, wenn $\mathfrak{o} = \mathfrak{o}_F$ die Maximalordnung ist. Klar, nur \mathfrak{o}_F ist in F ganzabgeschlossen.

Mit \mathfrak{o}_F teilt \mathfrak{o} die Eigenschaften

- Integritätsring: als Unterring eines Körpers,
- noethersch: als Untergruppe von \mathfrak{o}_F ist \mathfrak{o} eine endlich erzeugte \mathbb{Z} -Algebra, also noethersch,
- $\dim(\mathfrak{o}) = 1$: selber Beweis wie für \mathfrak{o}_F .

Die Primideale von \mathbb{Z} sind gerade (0) und alle (p) mit p eine Primzahl.

Korollar 3.9. *Sei F ein Zahlkörper. Ein von 0 verschiedenes Primideal \mathfrak{p} von \mathfrak{o}_F enthält genau eine Primzahl $p \in \mathbb{Z}$, welche durch*

$$(p) = \mathfrak{p} \cap \mathbb{Z}$$

charakterisiert ist. Der Restklassenring $\kappa(\mathfrak{p}) = \mathfrak{o}_F/\mathfrak{p}$ ist eine endliche Körpererweiterung von $\mathbb{F}_p = \mathbb{Z}/(p)$, und damit ein endlicher Körper mit

$$N(\mathfrak{p}) := \#\kappa(\mathfrak{p}) = (\mathfrak{o}_F : \mathfrak{p}) = p^{\dim_{\mathbb{F}_p}(\kappa(\mathfrak{p}))}$$

Elementen.

Beweis. Das ergibt sich sofort aus dem Beweis von Satz 3.5 im Spezialfall von \mathfrak{o}_F als Erweiterung von \mathbb{Z} . \square

3.2. Diskrete Bewertungsringe. Das Konzept der Nullstellen- und Polordnung wird durch den Begriff der diskreten Bewertung abstrahiert.

Definition 3.10. Eine **diskrete Bewertung** eines Körpers K ist ein surjektiver Gruppenhomomorphismus

$$v : K^\times \rightarrow \mathbb{Z},$$

so daß für alle $x, y \in K^\times$ mit $x + y \neq 0$ gilt

$$v(x + y) \geq \min\{v(x), v(y)\}.$$

Elemente $\pi \in K^\times$ mit $v(\pi) = 1$ heißen **uniformisierende Elemente** von v .

Die folgenden Beispiele sind für uns die wichtigsten.

Beispiel 3.11. (1) Sei p eine Primzahl \mathbb{Z} . Wir definieren die p -adische Bewertung auf \mathbb{Q} durch

$$v_p : \mathbb{Q}^\times \rightarrow \mathbb{Z}$$

$$v_p\left(p^n \frac{a}{b}\right) = n \text{ wenn } p \nmid ab.$$

Diese p -adische Bewertung zählt die Faktoren p in einer rationalen Zahl. Sie ist wohldefiniert und ein Homomorphismus aufgrund der eindeutigen Primfaktorzerlegung in \mathbb{Z} . Die nötige Abschätzung gilt, weil die Summe mindestens durch die Primpotenz teilbar ist, durch die beide Summanden teilbar sind.

(2) Hier ist die abstrakte Variante. Sei R ein Ring mit eindeutiger Primfaktorzerlegung, also etwa ein Hauptidealring wie \mathbb{Z} oder $k[T]$ für einen Körper k . Sei $\pi \in R$ ein Primelement und $K = \text{Quot}(R)$. Dann gibt es für jedes $x \in K^\times$ eindeutig

$$x = \pi^n \frac{y}{z}$$

mit $n \in \mathbb{Z}$ und $y, z \in R$, wobei π kein Teiler von y und z ist. Die π -(adische) Bewertung auf K ist gegeben durch

$$v_\pi : K^\times \rightarrow \mathbb{Z}$$

$$v_\pi\left(\pi^n \frac{y}{z}\right) = n \text{ wenn } \pi \nmid yz.$$

Wie im Spezialfall $R = \mathbb{Z}$ und $\pi = p$ folgt alles sofort: wohldefiniert, Gruppenhomomorphismus, Abschätzung der Teilbarkeitsordnung.

(3) Das abstrakte Beispiel liefert konkret für $R = k[T]$ und $\pi = T$ die Bewertung

$$\text{ord}_0 : k(T)^\times \rightarrow \mathbb{Z}$$

welches jeder rationalen Funktion die Nullstellenordnung in $T = 0$ zuordnet.

Lemma 3.12. Sei v eine diskrete Bewertung auf dem Körper K . Dann gilt für alle $x \in K^\times$:

- (1) $v(-x) = v(x)$, insbesondere $v(-1) = 0$.
- (2) $v(1/x) = -v(x)$.

Beweis. Es gilt $2v(-1) = v((-1)^2) = v(1) = 0$ in \mathbb{Z} , also $v(-1) = 0$. Der Rest ist noch trivialer. \square

Proposition 3.13 (Nicht-archimedische Dreiecksungleichung). Sei v eine diskrete Bewertung auf dem Körper K . Dann gilt für $x, y, x + y \in K^\times$, wenn

$$v(x) \neq v(y),$$

genauer

$$v(x + y) = \min\{v(x), v(y)\}.$$

Beweis. Wir zeigen, daß für $a, b, c \in K^\times$ mit $a + b + c = 0$ das Minimum von

$$\{v(a), v(b), v(c)\}$$

mindestens doppelt angenommen wird. Daraus folgt mit $a = x$, $b = y$ und $c = -(x + y)$ die Behauptung.

Angenommen, das Minimum wird nur einmal angenommen. Dann gilt oBdA

$$v(a) < v(b), v(c)$$

und dann ist

$$v(a) = v(-a) = v(b + c) \geq \min\{v(b), v(c)\} > v(a)$$

ein Widerspruch. □

Proposition 3.14. *Sei v eine diskrete Bewertung auf dem Körper K . Dann gilt:*

(1) *Die Menge*

$$R = \{x \in K^\times ; v(x) \geq 0\} \cup \{0\}$$

*ist ein Unterring von K mit $K = \text{Quot}(R)$, genannt der **Bewertungsring** von v .*

(2) *Die Einheitengruppe von R ist*

$$R^\times = \{x \in K^\times ; v(x) = 0\}.$$

(3) *Der Ring R ist ein Hauptidealring mit einem bis auf Einheiten eindeutigen Primelement. Die Primelemente sind genau die Uniformisierenden der Bewertung v .*

(4) *Der Ring R hat ein eindeutiges maximales Ideal*

$$\mathfrak{m} = \{x \in K^\times ; v(x) > 0\} \cup \{0\},$$

und dieses wird von π erzeugt, wenn π uniformisierendes Element ist.

(5) *Der Faktorring $k = R/\mathfrak{m}$ ist ein Körper, genannt der **Restklassenkörper** von v .*

Beweis. (1) Nach der Dreiecksungleichung gilt mit $x, y \in R$ auch $v(x+y) \geq \min\{v(x), v(y)\} \geq 0$, also $x + y \in R$ (wenn $x + y = 0$, so ist das trivial). Da $x, y \in R$ auch $xy \in R$ impliziert, und wegen $1^2 = 1$ notwendig $v(1) = 0$, ist R in der Tat ein Unterring.

Ein $x \in R$ ist eine Einheit, genau dann, wenn es ein $y \in R$ gibt mit $xy = 1$. Da

$$v(y) = v(1) - v(x) = -v(x)$$

geht das genau dann, wenn $v(x) = 0$ ist. Dann hat $y = 1/x \in K$ auch Bewertung 0 und ist in R . Dies zeigt (2).

Sei π eine Uniformisierende, also $v(\pi) = 1$. Dann setzen wir für $x \in K^\times$

$$y = x/\pi^{v(x)}$$

finden $v(y) = v(x) - v(x) \cdot v(\pi) = 0$. Demnach ist $y \in R^\times$ und

$$x = \pi^{v(x)}y.$$

Es folgt, daß K der Quotientenkörper von R ist. Damit ist nun (1) gezeigt.

(3) Sei $I \subseteq R$ ein Ideal. Wir setzen

$$n = v(I) = \min\{m ; \text{ es gibt } x \in I \text{ mit } v(x) = m\}.$$

Das Minimum existiert, denn es handelt sich um das Minimum einer Teilmenge von \mathbb{N}_0 . Außerdem wird das Minimum angenommen. Sei $x \in I$ ein solches Element mit $v(x) = n$. Dann ist für jedes $y \in I$ mit $z = y/x$

$$v(z) = v(y) - v(x) \geq 0,$$

also $z \in R$ und

$$y = xz \in (x).$$

Wir schließen $I = (x)$ und R ist Hauptidealring.

Sei π eine Uniformisierende von v . Jede Nichteinheit $x \in R$ hat $v(x) > 0$ und wird daher durch π geteilt. Damit ist π das einzige mögliche Primelement (bis auf Einheit). In der Tat ist π irreduzibel, da $x, y \in R$ mit $xy = \pi$ erzwingt

$$1 = v(\pi) = v(x) + v(y),$$

und $v(x), v(y)$ sind 0 und 1 in einer Reihenfolge. Nach (2) ist somit ein Faktor eine Einheit.

(4) Man sieht sofort wie in (3), daß

$$\mathfrak{m} = (\pi).$$

Da $R \setminus \mathfrak{m} = R^\times$ nur aus Einheiten besteht und ein echtes Ideal keine Einheiten enthalten darf, ist jedes Ideal in \mathfrak{m} enthalten. Damit ist \mathfrak{m} das eindeutige maximale Ideal von R .

(5) Der Faktorring $k = R/\mathfrak{m}$ ist ein Körper, weil \mathfrak{m} maximal ist. □

Beispiel 3.15. Der Potenzreihenring $K[[T]]$ über einem Körper K ist ein Hauptidealring mit genau einem Primelement T (bis auf Multiplikation mit einer Einheit). Die T -Bewertung auf $K((T)) := \text{Quot}(K[[T]])$ wird gegeben durch

$$v : K((T))^\times \rightarrow \mathbb{Z}$$

$$v\left(\sum_{i \geq 0} a_i T^i\right) \mapsto \min\{i ; a_i \neq 0\}$$

Der zugehörige Bewertungsring ist $K[[T]]$, das maximale Ideal besteht aus den Potenzreihen mit konstantem Element 0 und der Restklassen Körper ist als Quotient

$$K[[T]] \rightarrow K$$

$$f \mapsto f(0),$$

die einzige Auswertung von T in K , die sinnvoll ist.

Insbesondere folgt aus diesen Überlegungen, daß

$$K((T)) = \left\{ f = \sum_{i \geq n} a_i T^i ; n \in \mathbb{Z}, a_i \in K \right\} = \bigcup_{n \geq 0} T^{-n} K[[T]]$$

gilt. Der Quotientenkörper des formalen Potenzreihenrings ist somit der formale Laurentreihenring (mit endlicher Polordnung).

Satz 3.16. *Sei R ein Ring. Dann sind äquivalent:*

- (a) R ist ein diskreter Bewertungsring.
- (b) R ist ein Hauptidealring mit nur einem nichttrivialen Primideal.
- (c) R ist lokaler noetherscher Integritätsring mit maximalem Ideal $\mathfrak{m} = (\pi)$ erzeugt von einem nicht-nilpotenten Element.

Bemerkung 3.17. Die Eigenschaften von Satz 3.16 sind auch äquivalent zur folgenden Abschwächung von (c):

- (c') R ist lokaler noetherscher Ring mit maximalem Ideal $\mathfrak{m} = (\pi)$ erzeugt von einem nicht-nilpotenten Element.

Das kann (und soll man) in [Ser79] nachlesen.

Beweis von Satz 3.16. (a) \implies (b) haben wir in Proposition 3.14 gesehen. (b) \implies (c) ist trivial.

(c) \implies (a): Es ist $\mathfrak{m}^n = (\pi^n)$. Wir zeigen zuerst elementar den Krull'sche Durchschnittssatz im Spezialfall von R :

$$\bigcap_{n \geq 0} \mathfrak{m}^n = (0).$$

Sei $f \neq 0$ im Schnitt. Dann gibt es $0 \neq x_n \in R$ für alle $n \in \mathbb{N}$ mit

$$f = x_n \cdot \pi^n.$$

Dann ist

$$\pi^n(x_n - \pi x_{n+1}) = \pi^n x_n - \pi^{n+1} x_{n+1} = f - f = 0$$

somit $x_n = \pi \cdot x_{n+1}$. Damit haben wir eine aufsteigende Kette von Idealen

$$(x_1) \subseteq \dots \subseteq (x_n) \subseteq (x_{n+1}) \subseteq \dots$$

Diese wird wegen noethersch stationär. Für $n \gg 0$ gilt also $x_{n+1} \in (x_n)$, d.h., es gibt $a_n \in R$ mit

$$x_{n+1} = a_n x_n = a_n (\pi x_{n+1}) = (a_n \pi) x_{n+1},$$

also $a_n \pi = 1$ und π ist Einheit. Damit gilt $R = (\pi) = \mathfrak{m}$, Widerspruch.

Nun können wir schließen, daß

$$R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \dots \supseteq \bigcap_{n \geq 0} \mathfrak{m}^n = (0),$$

d.h. für jedes $0 \neq x \in R$ existiert ein eindeutiges $n \in \mathbb{N}_0$ mit

$$x \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}.$$

Weil $\mathfrak{m} = (\pi)$ Hauptideal ist, gibt es somit $u \in R$ mit

$$x = u \cdot \pi^n$$

aber weil $x \notin \mathfrak{m}^{n+1}$ muß $u \in R \setminus \mathfrak{m} = R^\times$ eine Einheit sein.

Die Zuordnung $x \mapsto n$ mit $x = u \cdot \pi^n$ und $u \in R^\times$ ist die gesuchte diskrete Bewertung (wenn man sie auf den Quotientenkörper in der offensichtlichen Weise als Differenz von Zähler und Nenner fortsetzt). \square

Theorem 3.18. *Sei R ein Ring. Dann sind äquivalent:*

- (a) R ist diskreter Bewertungsring.
- (b) R ist Hauptidealring mit nur einem nichttrivialen Primideal.
- (c) R ist lokaler Dedekindring.
- (d) R ist normaler, noetherscher Integritätsring mit genau einem von (0) verschiedenen Primideal.

Beweis. (a) \implies (b) haben wir in Proposition 3.14 gesehen.

(b) \implies (c): Ein Hauptidealring, der kein Körper ist, ist ein Dedekindring. Ein Hauptidealring mit genau einem nichttrivialen Primideal ist ein lokaler Ring.

(c) \implies (d): In einem lokalen Dedekindring (R, \mathfrak{m}) gibt es die Primideale $(0) \subsetneq \mathfrak{m}$. Alle anderen Primideale wären echt dazwischen und führten zu $\dim(R) > 1$. Also gibt es nur (0) und \mathfrak{m} . Der Rest ist offensichtlich für einen Dedekindring.

(d) \implies (a): Jedes maximale Ideal ist Primideal. Wenn es nur (0) und ein weiteres Primideal \mathfrak{m} gibt, dann kann es neben \mathfrak{m} keine weiteren maximalen Ideale geben. Somit ist (R, \mathfrak{m}) ein lokaler Ring. Nach Satz 3.16 reicht es nun zu zeigen, daß \mathfrak{m} ein Hauptideal ist.

Sei K der Quotientenkörper von R und

$$\mathfrak{m}' = \{x \in K ; x\mathfrak{m} \subseteq R\}.$$

Dann gilt $1 \in \mathfrak{m}'$ und

$$\mathfrak{m} \subseteq \mathfrak{m}' \cdot \mathfrak{m} := \left\{ \sum_{i=1}^n x_i y_i ; x_i \in \mathfrak{m}', y_i \in \mathfrak{m} \right\} \subseteq R.$$

Das Ideal $I = \mathfrak{m}' \cdot \mathfrak{m}$ ist also entweder \mathfrak{m} oder R .

Fall 1: $I = \mathfrak{m}$. Dieser Fall führt nach einigen Schritten zu einem Widerspruch.

Schritt 1: Wenn $I = \mathfrak{m}$, dann definiert

$$\begin{aligned} \mathfrak{m}' &\rightarrow \text{End}_R(\mathfrak{m}) \\ x &\mapsto (y \mapsto xy) \end{aligned}$$

eine treue Operation auf einem endlich erzeugten R -Modul. Nach dem Determinantentrick sind die Elemente aus \mathfrak{m}' ganz über R . Weil R normal ist, folgt $\mathfrak{m}' \subseteq R$ und daher $\mathfrak{m}' = R$.

Schritt 2: Für jedes $0 \neq y \in \mathfrak{m}$ ist der Ring (Lokalisierung an Potenzen von y)

$$R_y = \left\{ z \in K ; \exists n \in \mathbb{N}, x \in R : z = \frac{x}{y^n} \right\} \subseteq K$$

bereits gleich K . Dafür reicht es, zu zeigen, daß R_y ein Körper ist. Angenommen, R_y ist kein Körper. Dann gibt es ein Primideal $(0) \neq \mathfrak{q} \subseteq R_y$. In R_y ist y invertierbar, also $y \notin \mathfrak{q}$. Sei $0 \neq z \in \mathfrak{q}$. Dann wählen wir $x \in R$ und $n \in \mathbb{N}_0$ mit $z = \frac{x}{y^n}$. Insbesondere ist $x = y^n z \in \mathfrak{q}$.

Der Schnitt $\mathfrak{p} = \mathfrak{q} \cap R$ ist ein Primideal mit $y \notin \mathfrak{p}$ und $x \in \mathfrak{p}$. Von den zwei Primidealen (0) und \mathfrak{m} von R kommt damit für \mathfrak{p} keines in Frage! Dies ist ein Widerspruch, und dies zeigt $R_y = K$.

Schritt 3: Wir wählen nun $0 \neq z \in \mathfrak{m}$ beliebig. Sei $\mathfrak{m} = (y_1, \dots, y_r)$. Dann gibt es nach Schritt 1 Elemente $x_i \in R$ und $n \in \mathbb{N}$ (unabhängig von i) mit

$$\frac{1}{z} = \frac{x_i}{y_i^n},$$

also $y_i^n = x_i z \in (z)$ für alle $i = 1, \dots, r$. Daher gilt für $N \gg 0$

$$\mathfrak{m}^N \subseteq (z).$$

Schritt 4: Sei nun N minimal mit $\mathfrak{m}^N \subseteq (z)$. Weil $z \in \mathfrak{m}$ gilt $N \geq 1$. Insbesondere gibt es

$$y \in \mathfrak{m}^{N-1} \setminus (z).$$

Dann folgt

$$y \cdot \mathfrak{m} \subseteq \mathfrak{m}^N \subseteq (z),$$

also $\frac{y}{z} \in \mathfrak{m}' = R$ im Widerspruch zu $y \notin (z)$. Fall I tritt also nicht auf.

Fall 2: $I = R$. Dann ist $1 \in R = \mathfrak{m}' \cdot \mathfrak{m}$ und es gibt $x_1, \dots, x_r \in \mathfrak{m}'$ und $y_1, \dots, y_r \in \mathfrak{m}$ mit

$$1 = \sum_{i=1}^r x_i y_i.$$

Jeder der Summanden $x_i y_i \in R$ und nicht alle sind in \mathfrak{m} , denn sonst könnte ihre Summe nicht 1 sein. Es gibt also ein i mit $u_i = x_i y_i \in R^\times$. Wir setzen $x = u_i^{-1} x_i \in \mathfrak{m}'$ und $y = y_i \in \mathfrak{m}$, so daß

$$xy = 1.$$

Für ein beliebiges $z \in \mathfrak{m}$ gilt dann

$$z = z(xy) = (zx)y \in (y),$$

weil $zx \in \mathfrak{m} \cdot \mathfrak{m}' = R$. Damit ist $\mathfrak{m} = (y)$ ein Hauptideal. □

3.3. Lokalisieren von Ringen, Moduln, Idealen und Algebren. Lokalisieren ist eine Standardtechnik der kommutativen Algebra.

Definition 3.19. Eine **multiplikative** (oder genauer eine **multiplikativ abgeschlossene** Teilmenge eines Rings R ist eine Teilmenge $S \subseteq R$ mit

- (i) $1 \in S$,
- (ii) für alle $s, t \in S$ ist $st \in S$.

Synonym verwenden wir auch die Bezeichnung **multiplikatives System** für eine multiplikative Teilmenge.

Satz 3.20 (Existenz und Eindeutigkeit der Lokalisierung). *Sei R ein Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Dann gibt es eine R -Algebra*

$$\iota_S : R \rightarrow S^{-1}R$$

mit den folgenden Eigenschaften.

- (i) $\iota_S(S) \subseteq (S^{-1}R)^\times$,
- (ii) für jede R -Algebra $f : R \rightarrow A$ mit $f(S) \subseteq A^\times$ gibt es genau eine Faktorisierung $S^{-1}f$ wie im kommutativen Diagramm

$$\begin{array}{ccc} R & \xrightarrow{f} & A \\ & \searrow \iota_S & \nearrow S^{-1}f \\ & & S^{-1}R \end{array}$$

Die R -Algebra $S^{-1}R$ ist eindeutig bis auf eindeutigen Isomorphismus.

Beweis. Die Eindeutigkeitsaussage beweist sich rein formal aus den geforderten Eigenschaften von selbst. Der Gehalt des Satzes steckt in der Konstruktion eines solchen $\iota_S : R \rightarrow S^{-1}R$. Die Idee zur Konstruktion ist das formale *Bruchrechnen*. Wir definieren

$$S^{-1}R := R \times S / \sim$$

nach der Äquivalenzrelation

$$(a, s) \sim (b, t) \iff \text{es gibt } u \in S \text{ mit } u(at - bs) = 0.$$

Dies ist trivialerweise symmetrisch und reflexiv ist auch klar (mit $u = 1$). Transitiv sieht man wie folgt. Sei $(a, s) \sim (b, t)$, bezeugt durch $u \in S$ und $u(at - bs) = 0$, und sei $(b, t) \sim (c, r)$, bezeugt durch $v \in S$ und $v(br - ct) = 0$, dann ist $(a, s) \sim (c, r)$, weil $uvt \in S$ und

$$uvt(ar - cs) = vr(uat) - us(vct) = vr(ubs) - us(vbr) = 0.$$

Wir schreiben suggestiv

$$\frac{a}{s}$$

für die Äquivalenzklasse mit Vertreter (a, s) . Die Definition der Relation liest sich dann

$$\frac{a}{s} = \frac{uat}{ust} = \frac{ubs}{ust} = \frac{b}{t}$$

als bekannte Gleichung durch Erweitern und Kürzen von Brüchen.

Addition und Multiplikation auf $S^{-1}R$ definiert man wie für Brüche:

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &:= \frac{at + bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &:= \frac{ab}{st}. \end{aligned}$$

Es ist eine Übungsaufgabe zu zeigen, daß dies aus $S^{-1}R$ einen Ring mit $1 = \frac{1}{1}$ und $0 = \frac{0}{1}$ macht. Die Abbildung $\iota_S : R \rightarrow S^{-1}R$

$$\iota_S(a) = \frac{a}{1}$$

ist offensichtlich ein Ringhomomorphismus. Sei $s \in S$. Wegen

$$\iota_S(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1} = 1$$

schickt ι_S die Elemente von S auf Einheiten von $S^{-1}R$.

Sei $f : R \rightarrow A$ ein Ringhomomorphismus wie in (ii). Da S in $S^{-1}R$ auf Einheiten geht, kann $F = S^{-1}f$ höchstens dann existieren, wenn auch $f(S) \subseteq A^\times$ gilt. Dann definieren wir $F : S^{-1}R \rightarrow A$ durch

$$F\left(\frac{a}{s}\right) := f(a)f(s)^{-1}.$$

Dies ist eine wohldefinierte Abbildung, denn aus $a/s = b/t$ folgt mit $u \in S$ und $u(at - bs)$

$$f(a)f(s)^{-1} = f(uat)f(ust)^{-1} = f(ubs)f(ust)^{-1} = f(b)f(t)^{-1}.$$

Außerdem ist F ein Ringhomomorphismus: die Eins wird bewahrt

$$F(1) = F(1/1) = f(1)f(1)^{-1} = 1,$$

F ist additiv

$$\begin{aligned} F(a/s + b/t) &= F((at + bs)/st) = f(at + bs)f(st)^{-1} \\ &= f(at)f(st)^{-1} + f(bs)f(st)^{-1} = F(a/s) + F(b/t), \end{aligned}$$

und multiplikativ

$$\begin{aligned} F(a/s \cdot b/t) &= F(ab/st) = f(ab)f(st)^{-1} \\ &= f(a)f(s)^{-1} \cdot f(b)f(t)^{-1} = F(a/s) \cdot F(b/t), \end{aligned}$$

Die in (ii) geforderte Faktorisierungseigenschaft gilt, da für alle $a \in R$

$$F(a/1) = f(a)f(1)^{-1} = f(a).$$

Die Definition von F ist zudem die einzig mögliche, da

$$F\left(\frac{a}{s}\right) = F\left(\frac{a}{1} \cdot \frac{1}{s}\right) = F(\iota_S(a)\iota_S(s)^{-1}) = F(\iota_S(a)) \cdot F(\iota_S(s))^{-1} = f(a)f(s)^{-1}.$$

Die verbleibenden Details der Beweise, insbesondere das Assoziativgesetz und das Distributivgesetz in $S^{-1}R$, bleiben der geneigten Leserschaft zur Übung überlassen. \square

Bemerkung 3.21. Die Bedingung (i) in Satz 3.20 zu fordern ist notwendig, weil sonst $\text{id} : R \rightarrow R$ selbst auch (ii) löst und $S^{-1}R$ nicht mehr eindeutig ist.

Beispiel 3.22. (1) Sei R ein Integritätsring. Dann ist $S = R \setminus \{0\}$ multiplikativ und

$$\text{Quot}(R) = (R \setminus \{0\})^{-1}R$$

der Quotientenkörper. Aus der universellen Eigenschaft von Satz 3.20 folgt, daß insbesondere $R \rightarrow \text{Quot}(R)$ den universellen injektiven Homomorphismus in einen Körper darstellt. Jede Einbettung $R \hookrightarrow K$ in einen Körper K faktorisiert eindeutig zu $\text{Quot}(R) \hookrightarrow K$. Der Quotientenkörper ist der kleinste Körper, der R enthält.

(2) Seien S und T multiplikative Teilmengen des Rings R . Dann ist auch

$$ST = \{st \mid s \in S, t \in T\}$$

multiplikativ, und es gilt

$$(ST)^{-1}R = (\iota_S(T))^{-1}S^{-1}R$$

als R -Algebren. Das folgt sofort aus der universellen Eigenschaft: ST ist in $(\iota_S(T))^{-1}S^{-1}R$ invertierbar, da st invertierbar ist, wenn nur s und t invertierbar sind. Also gibt es

$$(ST)^{-1}R \rightarrow (\iota_S(T))^{-1}S^{-1}R$$

$$\frac{a}{st} \mapsto \frac{a}{t}.$$

Umgekehrt sind S und $\iota_S(T)$ in $(ST)^{-1}R$ invertierbar, somit existieren eindeutig die punktierten Pfeile im Diagramm

$$\begin{array}{ccccc} R & \longrightarrow & S^{-1}R & \longrightarrow & (\iota_S(T))^{-1}(S^{-1}R) \\ & \searrow & \dashrightarrow & & \downarrow \\ & & & & (ST)^{-1}R \end{array}$$

Die nun konstruierte Abbildung ist die inverse Abbildung zur ersten.

- (3) Sei $f \in R$ ein beliebiges Element. Dann ist

$$S_f := \{1, f, f^2, \dots, f^n, \dots\}$$

multiplikativ. Die Lokalisierung bezeichnen wir mit

$$R_f := R\left[\frac{1}{f}\right] := S_f^{-1}R.$$

In diesem Ring werden als Nenner nur Potenzen von f zugelassen. Aus der universellen Eigenschaft bekommt man einen Isomorphismus

$$R_f = R[X]/(1 - Xf).$$

Proposition 3.23. Sei S eine multiplikative Teilmenge im Ring R . Dann ist

$$\ker(R \rightarrow S^{-1}R) = \{a \in R; \text{ es gibt } s \in S \text{ mit } sa = 0\}.$$

Beweis. $\iota_S(a) = 0$ bedeutet $\frac{a}{1} = \frac{0}{1}$, und das sagt, es gibt $s \in S$ mit $s(a \cdot 1 - 0 \cdot 1) = 0$. \square

Korollar 3.24. Sei R ein Integritätsring und $S \subseteq R$ multiplikativ mit $0 \notin S$. Dann ist

$$R \hookrightarrow S^{-1}R \hookrightarrow \text{Quot}(R)$$

injektiv.

Beweis. Sofort aus Proposition 3.23, da in einem Integritätsring keine Nullteiler existieren. \square

Satz 3.25 (Lokalisierung von Moduln). Sei R ein Ring und $S \subseteq R$ ein multiplikatives System. Zu einem R -Modul M gibt es einen R -Modulhomomorphismus $R \rightarrow S^{-1}R$ mit der Eigenschaft:

- (i) für alle $t \in S$ ist die Multiplikation mit t auf $S^{-1}M$ bijektiv,
- (ii) für alle R -Modulhomomorphismen $\varphi : M \rightarrow N$, so daß alle $t \in S$ auf N durch Multiplikation bijektiv operieren, gibt es eine eindeutige Fortsetzung $S^{-1}\varphi : S^{-1}M \rightarrow N$, also ein kommutatives Diagramm

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ & \searrow & \nearrow \\ & & S^{-1}M \end{array}$$

Der Modulhomomorphismus $M \rightarrow S^{-1}M$ ist mit den angegebenen Eigenschaften eindeutig bis auf eindeutigen Isomorphismus.

Beweis. Die Eindeutigkeit ist formal. Die Existenz wird durch die folgende Konstruktion gewährleistet. Es ist

$$S^{-1}M = M \times S / \sim$$

bezüglich der Äquivalenzrelation

$$(x, s) \sim (y, t) \iff \text{es gibt } u \in S : u(tx - sy) = 0.$$

Der Rest des Beweises verläuft parallel zum Beweis von Satz 3.20 und bringt keine neuen Erkenntnisse. \square

Bemerkung 3.26. (1) Auf dem Modul $S^{-1}M$ operieren alle $t \in S$ bijektiv durch Multiplikation. Daher ist $S^{-1}M$ auf eindeutige Weise durch

$$\frac{a}{s} \cdot \frac{x}{t} = \frac{ax}{st}$$

mit $a \in R, s, t \in S$ und $x \in M$ ein $S^{-1}R$ -Modul.

(2) Die Lokalisierung an S ist sogar ein Funktor. Auf Objekten haben wir $M \rightsquigarrow S^{-1}M$ konstruiert. Zu einem R -Modulhomomorphismus $\varphi : M \rightarrow N$ gehört wegen der universellen Eigenschaft von $S^{-1}M$ im Diagramm

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \downarrow & & \downarrow \\ S^{-1}M & \xrightarrow{S^{-1}\varphi} & S^{-1}N \end{array}$$

der Pfeil $S^{-1}\varphi$ der Form

$$S^{-1}\varphi\left(\frac{x}{s}\right) = \frac{\varphi(x)}{s}.$$

Dieser ist eindeutig, sogar ein $S^{-1}R$ -Modulhomomorphismus und offensichtlich funktoriell. Wir erhalten den Lokalisierungsfunktor auf Moduln

$$\begin{aligned} S^{-1} : \text{Mod}(R) &\rightarrow \text{Mod}(S^{-1}R) \\ M &\mapsto S^{-1}M. \end{aligned}$$

(3) Auch für Moduln ist das Lokalisieren transitiv. Seien $S, T \subseteq R$ multiplikativ. Dann ist natürlich

$$(ST)^{-1}M = T^{-1}(S^{-1}M).$$

Satz 3.27. *Sei S ein multiplikatives System in einem Ring R . Dann gibt es für alle $M \in \text{Mod}(R)$ einen natürlichen Isomorphismus*

$$S^{-1}M = M \otimes_R S^{-1}R.$$

Beweis. Da S in $S^{-1}R$ auf Einheiten abgebildet wird, ist $M = M \otimes_R R \rightarrow M \otimes_R S^{-1}R$ ein R -Modulhomomorphismus in einen R -Modul, auf dem die Multiplikation mit allen $s \in S$ bijektiv ist. Aus der universellen Eigenschaft ergibt sich ein eindeutiger R - sogar $S^{-1}R$ -Modulhomomorphismus

$$\begin{aligned} S^{-1}M &\rightarrow M \otimes_R S^{-1}R \\ \frac{x}{s} &\mapsto x \otimes \frac{1}{s}. \end{aligned}$$

In die umgekehrte Richtung betrachten wir die R -bilineare Abbildung

$$\begin{aligned} M \times S^{-1}R &\rightarrow S^{-1}M \\ \left(x, \frac{a}{s}\right) &\mapsto \frac{ax}{s}. \end{aligned}$$

Diese induziert nach der universellen Eigenschaft einen R -sogar $S^{-1}R$ -Modulhomomorphismus

$$M \otimes_R S^{-1}R \rightarrow S^{-1}M$$

$$x \otimes \frac{a}{s} \mapsto \frac{ax}{s}.$$

Diese beiden Homomorphismen sind offensichtlich natürlich und invers zueinander. \square

Satz 3.28. *Lokalisieren von Moduln ist ein exakter Funktor.*

Beweis. Sei S ein multiplikatives System in einem Ring R und sei $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ eine kurze exakte Sequenz von R -Moduln. Wir müssen zeigen, daß auch die induzierte Sequenz

$$0 \rightarrow S^{-1}M' \rightarrow S^{-1}M \rightarrow S^{-1}M'' \rightarrow 0$$

exakt ist. Da Lokalisieren ein Tensorprodukt $- \otimes_R S^{-1}R$ ist, folgt aus allgemeinen Gründen, daß Lokalisieren rechtsexakt ist. Wir müssen also nur zeigen, daß ein injektiver R -Modulhomomorphismus $i : M' \hookrightarrow M$ nach Lokalisieren immer noch injektiv ist.

Sei $y \in S^{-1}M'$ und $S^{-1}i(y) = 0 \in S^{-1}M$. Dann gibt es $x \in M'$ und $s \in S$ mit $y = \frac{x}{s}$, und

$$0 = S^{-1}i(y) = \frac{i(x)}{s}.$$

Weiter gibt es dann $u \in S$ mit $u(1 \cdot i(x) - s \cdot 0) = 0$, also $0 = ui(x) = i(ux)$. Da i injektiv ist, folgt $0 = ux = u(1 \cdot x - s \cdot 0)$. Das bedeutet rückwärts, daß $y = \frac{x}{s} = 0 \in S^{-1}M'$. Damit ist $S^{-1}i$ injektiv. \square

Definition 3.29. Ein **endlich präsentierter R -Modul** ist ein R -Modul M , für den es $n_1, n_0 \in \mathbb{N}_0$ und eine exakte R -Modulsequenz

$$R^{n_1} \xrightarrow{A} R^{n_0} \xrightarrow{p} M \rightarrow 0$$

gibt. Eine solche Sequenz nennt man eine **endliche Präsentation** von M .

Bemerkung 3.30. Eine endliche Präsentation wie in der Definition besagt, daß M von n_0 -vielen Elementen, den Bildern $x_i = p(e_i)$ für $i = 1, \dots, n_0$ mit der Standardbasis e_i von R^{n_0} erzeugt werden kann. Weiter besagt die Präsentation, daß die R -linearen Relationen, die zwischen den x_i in M gelten, durch die n_1 -vielen Relationen $A(e_j)$ mit $j = 1, \dots, n_1$ erzeugt werden können. Wenn man A durch eine Matrix beschreibt, dann sind die Koeffizienten der erzeugenden Relationen in den Spalten der Matrix abzulesen.

Satz 3.31. *Sei M ein endlich präsentierter R -Modul und $S \subseteq R$ multiplikativ. Dann ist für alle R -Moduln N die natürliche Abbildung*

$$S^{-1} \operatorname{Hom}_R(M, N) \rightarrow \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

ein Isomorphismus von $S^{-1}R$ -Moduln.

Beweis. Schritt 1: Die Aussage ist trivialerweise wahr für $M = R$. Dann ist nämlich

$$\operatorname{Hom}_R(R, N) = N \quad \text{und} \quad \operatorname{Hom}_{S^{-1}R}(S^{-1}R, S^{-1}N) = S^{-1}N$$

durch Auswertung bei 1 und die behauptete Abbildung nach dieser Identifizierung gleich der Identität.

Schritt 2: Wenn die Aussage für R -Moduln M_1 und M_2 anstelle von M gilt, dann auch für $M = M_1 \oplus M_2$. In der Tat ist

$$S^{-1} \operatorname{Hom}_R(M_1 \oplus M_2, N) = (S^{-1} \operatorname{Hom}_R(M_1, N)) \oplus (S^{-1} \operatorname{Hom}_R(M_2, N))$$

und

$$\operatorname{Hom}_{S^{-1}R}(S^{-1}(M_1 \oplus M_2), S^{-1}N) = \operatorname{Hom}_{S^{-1}R}(S^{-1}M_1, S^{-1}N) \oplus \operatorname{Hom}_{S^{-1}R}(S^{-1}M_2, S^{-1}N)$$

und die Abbildung ist aufgrund ihrer Natürlichkeit mit der Aufspaltung als direkte Summe verträglich. Damit ist sie ein Isomorphismus genau dann, wenn sie komponentenweise ein Isomorphismus ist.

Schritt 3: Aus Schritt 1 und 2 folgt per Induktion die Aussage für $M = R^n$ und beliebige $n \in \mathbb{N}_0$.

Schritt 4: Wir wählen nun eine endliche Präsentation $R^{n_1} \rightarrow R^{n_0} \rightarrow M \rightarrow 0$. Auf diese Sequenz wenden wir zum einen die Funktoren $S^{-1} \text{Hom}_R(-, N)$ und zum andern die Funktoren $S^{-1}(-)$ und $\text{Hom}_{S^{-1}R}(-, S^{-1}N)$ an. Aus den jeweiligen Exaktheitseigenschaften folgt das kommutative Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & S^{-1} \text{Hom}_R(M, N) & \longrightarrow & S^{-1} \text{Hom}_R(R^{n_0}, N) & \longrightarrow & S^{-1} \text{Hom}_R(R^{n_1}, N) \\ & & \downarrow \beta_M & & \downarrow \beta_{R^{n_0}} & & \downarrow \beta_{R^{n_1}} \\ 0 & \rightarrow & \text{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) & \rightarrow & \text{Hom}_{S^{-1}R}(S^{-1}R^{n_0}, S^{-1}N) & \rightarrow & \text{Hom}_{S^{-1}R}(S^{-1}R^{n_1}, S^{-1}N) \end{array}$$

mit exakten Zeilen. Die beiden rechten vertikalen Abbildungen sind nach Schritt 3 Isomorphismen. Damit ist es auch β_M nach dem 5-er Lemma (man denke sich das Diagramm nach links durch Nullen fortgesetzt, um auf die 5 Spalten zu kommen). \square

Lemma 3.32. *Sei R ein Ring, $S \subseteq R$ ein multiplikatives System und $\iota : R \rightarrow A$ eine R -Algebra. Dann ist auch $\iota(S) \subseteq A$ ein multiplikatives System und*

$$S^{-1}A = \iota(S)^{-1}A.$$

Das heißt, die Lokalisierung als R -Modul an S und als Ring an $\iota(S)$ stimmen als $S^{-1}R$ -Moduln überein. Insbesondere ist $S^{-1}A$ durch $S^{-1}\iota : S^{-1}R \rightarrow S^{-1}A$ eine $S^{-1}R$ -Algebra.

Beweis. Trivial durch Ausnutzen der jeweiligen universellen Eigenschaften, oder durch Vergleich der Konstruktion. \square

Proposition 3.33. *Sei R ein Ring und S eine multiplikative Teilmenge.*

- (1) *Sei $\mathfrak{a} \subseteq R$ ein Ideal. Dann ist $S^{-1}\mathfrak{a} \subseteq S^{-1}R$ ein Ideal.*
- (2) *Sei $\mathfrak{a} \subseteq R$ ein Ideal. Dann haben wir einen Isomorphismus von $S^{-1}R$ -Algebren*

$$S^{-1}R/S^{-1}\mathfrak{a} = S^{-1}(R/\mathfrak{a}).$$

- (3) *Jedes Ideal $\mathfrak{b} \subseteq S^{-1}R$ ist von der Form $S^{-1}\mathfrak{a}$ für ein Ideal $\mathfrak{a} \subseteq R$.*
- (4) *Seien $\mathfrak{a}_1, \mathfrak{a}_2$ Ideale von R . Dann gilt*

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \implies S^{-1}\mathfrak{a}_1 \subseteq S^{-1}\mathfrak{a}_2.$$

Beweis. (1) Da Lokalisieren exakt ist, bleibt $S^{-1}\mathfrak{a} \hookrightarrow S^{-1}R$ injektiv. Außerdem sind Untermoduln von $S^{-1}R$ dasselbe wie Ideale.

Die Aussage (2) folgt aus der Exaktheit des Lokalisierens und Lemma 3.32 für die Interpretation als $S^{-1}R$ -Algebren.

(3) Zum Ideal $\mathfrak{b} \subseteq S^{-1}R$ betrachten wir

$$\mathfrak{a} = \{x \in R ; \frac{x}{1} \in \mathfrak{b}\} = \iota_S^{-1}(\mathfrak{b}).$$

Als Urbild eines Ideals ist $\mathfrak{a} \subseteq R$ ein Ideal. Außerdem gilt offensichtlich

$$S^{-1}\mathfrak{a} \subseteq \mathfrak{b}.$$

Wenn $\frac{x}{s} \in \mathfrak{b}$, dann ist $\frac{x}{1} = s \cdot \frac{x}{s} \in \mathfrak{b}$ und damit $x \in \mathfrak{a}$, oder $\frac{x}{s} \in S^{-1}\mathfrak{a}$. Es folgt $S^{-1}\mathfrak{a} = \mathfrak{b}$.

(4) ist klar. \square

Satz 3.34. *Sei R ein Ring und S eine multiplikative Teilmenge. Die Lokalisierung an S ist eine bijektive, inklusionserhaltende Abbildung*

$$S^{-1} : \{\mathfrak{p} \in \text{Spec}(R) ; \mathfrak{p} \cap S = \emptyset\} \xrightarrow{\sim} \text{Spec}(S^{-1}R)$$

$$\mathfrak{p} \mapsto S^{-1}\mathfrak{p}.$$

Die Umkehrabbildung wird durch $\mathfrak{q} \mapsto \iota_S^{-1}(\mathfrak{q})$ beschrieben.

Beweis. Wenn $\mathfrak{p} \subseteq R$ ein Primideal ist, dann ist der Faktorring zum Ideal $S^{-1}\mathfrak{p}$

$$S^{-1}R/S^{-1}\mathfrak{p} = S^{-1}(R/\mathfrak{p})$$

die Lokalisierung am Bild \bar{S} von S in R/\mathfrak{p} . Da R/\mathfrak{p} ein Integritätsring ist, gilt dasselbe für die Lokalisierung, sofern $0 \notin \bar{S} \subseteq R/\mathfrak{p}$. Äquivalent dazu ist $S \cap \mathfrak{p} = \emptyset$. In diesem Fall ist $S^{-1}\mathfrak{p}$ ein Primideal und die Abbildung wohldefiniert.

Die Umkehrabbildung führt zu einem Ideal $\mathfrak{p} = \iota_S^{-1}(\mathfrak{q})$, so daß per Definition die induzierte Abbildung

$$R/\mathfrak{p} \hookrightarrow S^{-1}R/\mathfrak{q}$$

injektiv ist. Daher ist auch R/\mathfrak{p} ein Integritätsring, und \mathfrak{p} ist ein Primideal. Wenn $S \cap \mathfrak{p} \neq \emptyset$, dann wäre auch $S \cap \mathfrak{q} \neq \emptyset$ und $\mathfrak{q} = S^{-1}R$, Widerspruch. Die Umkehrabbildung ist also auch wohldefiniert.

Offensichtlich gilt $\mathfrak{p} \subseteq \iota_S^{-1}(S^{-1}\mathfrak{p})$. Wenn $x \in \iota_S^{-1}(S^{-1}\mathfrak{p})$, dann gibt es $y \in \mathfrak{p}$ und $s \in S$ mit $\frac{x}{1} = \iota_S(x) = \frac{y}{s}$. Dann gibt es $u \in S$ mit $u(xs - y) = 0$, also

$$x(us) = uy \in \mathfrak{p}.$$

Da $us \in S \subseteq R \setminus \mathfrak{p}$, muß der andere Faktor $x \in \mathfrak{p}$ sein, denn \mathfrak{p} ist ein Primideal. Daher gilt

$$\mathfrak{p} = \iota_S^{-1}(S^{-1}\mathfrak{p}).$$

Betrachten wir nun ein Primideal $\mathfrak{q} \subseteq S^{-1}R$ und setzen $\mathfrak{p} = \iota_S^{-1}(\mathfrak{q})$. Dann gilt nach dem Beweis von Proposition 3.33

$$S^{-1}\mathfrak{p} = \mathfrak{q},$$

und die Bijektion ist bewiesen. Die Behauptung über die Inklusionsrelation folgt aus Proposition 3.33 (4). \square

3.4. Lokalisieren und Ganzheit.

Proposition 3.35. *Sei $A \rightarrow B$ eine Ringhomomorphismus, so daß B ganz über A ist. Sei $S \subseteq A$ eine multiplikative Teilmenge.*

Dann ist $S^{-1}A \rightarrow S^{-1}B$ ein Ringhomomorphismus, für den $S^{-1}B$ ganz über $S^{-1}A$ ist.

Beweis. Sei $y \in S^{-1}B$ beliebig. Dann gibt es $s \in S$ und $b \in B$ mit $y = b/s$. Nach Voraussetzung ist b ganz über A . Es gibt also ein normiertes Polynom $f \in A[X]$ mit $f(b) = 0$. Sei $d = \deg(f)$ der Grad von f . Das Polynom

$$g(X) = s^{-d}f(sX) \in S^{-1}A[X]$$

ist normiert und hat $g(y) = s^{-d}f(b) = 0$. \square

Proposition 3.36. *Sei $A \subseteq B$ eine ganz abgeschlossene Ringerweiterung. Sei $S \subseteq A$ eine multiplikative Teilmenge.*

Dann ist $S^{-1}A \rightarrow S^{-1}B$ eine ganz abgeschlossene Ringerweiterung.

Beweis. Lokalisieren ist exakt, daher ist $S^{-1}A \rightarrow S^{-1}B$ auch injektiv. Wir nehmen nun ein $y = b/s$ mit $b \in B$, $s \in S$ und y ist ganz über $S^{-1}A$. Es gibt dann ein normiertes Polynom

$$f(X) = X^d + \frac{a_1}{s_1}X^{d-1} + \dots + \frac{a_{d-1}}{s_{d-1}}X + \frac{a_d}{s_d} \in S^{-1}A[X]$$

mit $f(y) = 0$. Durch Erweitern können wir annehmen, daß $s = s_1 = \dots = s_d$. Das Polynom

$$g(X) = s^d f(X/s) = X^d + a_1 X^{d-1} + a_2 s X^{d-2} + \dots + a_{d-1} s^{d-2} X + a_d s^{d-1} \in A[X]$$

ist normiert und

$$g(b) = s^d f(b/s) = s^d f(y) = 0 \in S^{-1}B.$$

Also $g(b) \in \ker(B \rightarrow S^{-1}B)$, d.h., es gibt ein $t \in S$ mit $tg(b) = 0 \in B$. Sei

$$h(X) = X^d + a_1 t X^{d-1} + a_2 s t^2 X^{d-2} + \dots + a_{d-1} s^{d-2} t^{d-1} X + a_d s^{d-1} t^d \in A[X].$$

Dann ist

$$h(tb) = t^d g(b) = t^{d-1}(tg(b)) = 0.$$

Folglich ist tb ganz über A , somit nach Voraussetzung $tb \in A$. Damit ist

$$y = \frac{b}{s} = \frac{tb}{ts} \in S^{-1}A. \quad \square$$

Satz 3.37. Sei A ein Dedekindring und $S \subseteq R$ eine multiplikative Teilmenge, so daß es ein Primideal $\mathfrak{p} \neq 0$ von A gibt mit $S \cap \mathfrak{p} = \emptyset$.

Dann ist auch $S^{-1}A$ ein Dedekindring, und zwar mit dem gleichen Quotientenkörper wie A .

Beweis. Als Lokalisierung eines Integritätsrings ist $S^{-1}A$ ein Integritätsring mit dem gleichen Quotientenkörper K wie A . Proposition 3.36 zeigt, daß $S^{-1}A \subseteq S^{-1}K = K$ ganz abgeschlossen ist, denn A ist als Dedekindring in K ganz abgeschlossen.

Jedes Ideal \mathfrak{b} von $S^{-1}A$ ist von der Form $S^{-1}\mathfrak{a}$ für das Ideal

$$\mathfrak{a} = \{x \in A ; x/1 \in \mathfrak{b}\} \subseteq A.$$

Eine aufsteigende Idealkett in $S^{-1}A$ ist daher die Lokalisierung einer aufsteigenden Idealkette von A . Weil A noethersch ist, wird diese stationär. Folglich ist auch $S^{-1}A$ noethersch.

Die Menge der Primideale von $S^{-1}A$ ist nach Satz 3.34 als bezüglich Inklusion partiell geordnete Menge mit einer Teilmenge von $\text{Spec}(A)$ zu identifizieren. Die Dimension ist also

$$\dim S^{-1}A \leq \dim(A) = 1.$$

Nach Voraussetzung enthält $\text{Spec}(S^{-1}A)$ zumindest $(0) \subsetneq \mathfrak{p}$ aus $\text{Spec}(A)$. Damit ist

$$\dim S^{-1}A = 1. \quad \square$$

Notation 3.38. Für jeden Ring R und ein Primideal $\mathfrak{p} \in \text{Spec}(R)$ ist die Lokalisierung an $R \setminus \mathfrak{p}$ besonders interessant. Wir bezeichnen den **lokalen Ring bei \mathfrak{p}** wie üblich mit

$$R_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}R$$

und für einen R -Modul M mit

$$M_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}M.$$

Korollar 3.39. Sei A ein Dedekindring und $0 \neq \mathfrak{p} \in \text{Spec}(A)$. Dann ist $A_{\mathfrak{p}}$ ein diskreter Bewertungsring.

Beweis. Nach Satz 3.37 ist $A_{\mathfrak{p}}$ wieder ein Dedekindring. Per Konstruktion und Satz 3.34 hat $A_{\mathfrak{p}}$ nur die Primideale

$$\text{Spec}(A_{\mathfrak{p}}) = \{(0), \mathfrak{p}\}.$$

Daher hat $A_{\mathfrak{p}}$ nur ein maximales Ideal, ist somit ein lokaler Dedekindring. Nun folgt das Korollar aus Theorem 3.18. \square

Notation 3.40. Wir bezeichnen die diskrete Bewertung, die zu $A_{\mathfrak{p}}$ für einen Dedekindring A und ein Primideal $\mathfrak{p} \neq (0)$ gehört, mit

$$v_{\mathfrak{p}} : K^{\times} \rightarrow \mathbb{Z}.$$

Dabei ist wie üblich K der Quotientenkörper von A und ebenso $A_{\mathfrak{p}}$.

Beispiel 3.41. Für den Dedekindring \mathbb{Z} und das Primideal $\mathfrak{p} = (p)$ kommt bei $v_{\mathfrak{p}} = v_p$ gerade die p -adische Bewertung auf \mathbb{Q} heraus.

3.5. Lokale Eigenschaften. Viele Eigenschaften erhalten sich beim Lokalisieren. Die besseren unter diesen lassen sich sogar dadurch nachweisen, dass man die Eigenschaft nach Lokalisieren an allen Primidealen verifiziert.

Proposition 3.42. *Sei R ein Ring und M ein R -Modul. Dann sind äquivalent:*

- (a) $M = 0$.
- (b) $M_{\mathfrak{p}} = 0$ für alle Primideale \mathfrak{p} von R .
- (c) $M_{\mathfrak{m}} = 0$ für alle maximalen Ideale \mathfrak{m} von R .

Beweis. (a) \implies (b) \implies (c) ist trivial. Sei also (c) erfüllt und sei $x \in M$ beliebig. Dann ist

$$\text{Ann}_R(x) = \{a \in R ; ax = 0\}$$

das Annulatorideal von $x \in M$. Angenommen, $\text{Ann}_R(x)$ ist ein echtes Ideal. Dann gibt es ein maximales Ideal \mathfrak{m} von R mit $\text{Ann}_R(x) \subseteq \mathfrak{m}$. Dies führt zu den folgenden Abbildungen:

$$M \supseteq \langle x \rangle_R \simeq R / \text{Ann}_R(x) \twoheadrightarrow R / \mathfrak{m}.$$

Wir lokalisieren an \mathfrak{m} , was exakt ist und $(R/\mathfrak{m})_{\mathfrak{m}} = R/\mathfrak{m}$ hat. Somit erhalten wir mit

$$0 = M_{\mathfrak{m}} \supseteq (\langle x \rangle_R)_{\mathfrak{m}} \simeq (R / \text{Ann}_R(x))_{\mathfrak{m}} \twoheadrightarrow (R/\mathfrak{m})_{\mathfrak{m}} = R/\mathfrak{m} \neq 0$$

einen Widerspruch. □

Korollar 3.43. *Sei $f : M \rightarrow N$ ein R -Modulhomomorphismus. Die Eigenschaften*

$$\mathcal{P} = \text{injektiv, surjektiv, bijektiv, Nullabbildung}$$

sind lokal, d.h. es sind äquivalent:

- (a) f hat \mathcal{P} .
- (b) $f_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ hat \mathcal{P} für alle Primideale \mathfrak{p} von R .
- (c) $f_{\mathfrak{m}} : M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$ hat \mathcal{P} für alle maximalen Ideale \mathfrak{m} von R .

Beweis. Da Lokalisieren exakt ist, gilt

$$\begin{aligned} \ker(f_{\mathfrak{p}}) &= \ker(f)_{\mathfrak{p}}, \\ \text{coker}(f_{\mathfrak{p}}) &= \text{coker}(f)_{\mathfrak{p}}, \\ \text{im}(f_{\mathfrak{p}}) &= \text{im}(f)_{\mathfrak{p}}. \end{aligned}$$

Das Korollar folgt nun aus Proposition 3.42 angewandt auf $\ker(f)$, $\text{coker}(f)$, $\ker(f)$ und $\text{coker}(f)$, oder $\text{im}(f)$. □

Korollar 3.44. *Seien N_1, N_2 Untermoduln des R -Moduls M .*

- (1) *Es sind äquivalent:*
 - (a) $N_1 = N_2$.
 - (b) $N_{1,\mathfrak{p}} = N_{2,\mathfrak{p}}$ für alle Primideale \mathfrak{p} von R .
 - (c) $N_{1,\mathfrak{m}} = N_{2,\mathfrak{m}}$ für alle maximalen Ideale \mathfrak{m} von R .
- (2) *Es sind äquivalent:*
 - (a) $N_1 \subseteq N_2$.
 - (b) $N_{1,\mathfrak{p}} \subseteq N_{2,\mathfrak{p}}$ für alle Primideale \mathfrak{p} von R .
 - (c) $N_{1,\mathfrak{m}} \subseteq N_{2,\mathfrak{m}}$ für alle maximalen Ideale \mathfrak{m} von R .

Beweis. (1) folgt aus (2) angewandt auf $N_1 \subseteq N_2$ und $N_2 \subseteq N_1$.

Aussage (2) folgt aus Korollar 3.43 angewandt auf das Nullsein der Komposition der Modulhomomorphismen

$$N_1 \hookrightarrow M \twoheadrightarrow M/N_2. \quad \square$$

Bemerkung 3.45. Korollar 3.43 illustriert die folgende Methode. Man codiert eine Eigenschaft durch exakte Sequenzen, zeigt, daß die Sequenz nach Lokalisieren die entsprechende lokale Eigenschaft codiert, und schließt daraus, daß die Eigenschaft eine lokale Eigenschaft ist.

Satz 3.46. *Sei A ein Dedekindring mit Quotientenkörper $K = \text{Quot}(A)$. Dann gilt für den Schnitt in K*

$$A = \bigcap_{\mathfrak{p} \in \max(A)} A_{\mathfrak{p}} = \{x \in K^{\times} ; v_{\mathfrak{p}}(x) \geq 0 \quad \forall \mathfrak{p} \in \max(A)\} \cup \{0\}$$

Beweis. Die Lokalisierung $A_{\mathfrak{p}}$ ist natürlich ein Unterring von K . Der Satz ist also wohlformuliert. Es gilt offensichtlich

$$A \subseteq \bigcap_{\mathfrak{p} \in \max(A)} A_{\mathfrak{p}}.$$

Wir nehmen daher ein $f = x/y \in K^{\times}$, das im Schnitt liegt, also für alle \mathfrak{p} gibt es $w_{\mathfrak{p}} \in A_{\mathfrak{p}}$ mit $x = yw_{\mathfrak{p}}$. Wir betrachten weiter das Ideal in A

$$(y : x) = ((y) : (x)) = \ker(A \xrightarrow{x \cdot} A/yA) = \{z \in A ; zx \in (y)\}.$$

Dies lokalisiert gut wie man aus der Beschreibung als Kern sieht, also

$$(y : x)_{\mathfrak{p}} = ((y)_{\mathfrak{p}} : (x)_{\mathfrak{p}}) = (y : x) \text{ in } A_{\mathfrak{p}}.$$

Aber lokal ist $x = yw_{\mathfrak{p}}$, daher $xA_{\mathfrak{p}} \subseteq yA_{\mathfrak{p}}$ und Multiplikation mit $x \cdot : A_{\mathfrak{p}} \rightarrow A_{\mathfrak{p}}/yA_{\mathfrak{p}}$ ist die Nullabbildung. Wenn aber bei Lokalisieren an allen maximalen Idealen die Nullabbildung rauskommt, dann war $x \cdot : A \rightarrow A/yA$ bereits die Nullabbildung. Ergo $x \in (y)$ und somit $f = x/y \in A$. \square

Bemerkung 3.47. Wenn man auf die Beschreibung mit den Bewertungen $v_{\mathfrak{p}}(-)$ verzichtet, dann gilt der Satz allgemeiner für Integritätsringe. Man kann zeigen, daß man im allgemeinen bei ganzabgeschlossenen noetherschen Ringen A nur über die Primideale \mathfrak{p} der Höhe 1 zu schneiden braucht. Das sind im Fall von Dedekindringen gerade die maximalen Primideale. Die dazugehörigen lokalen Ringe sind im ganzabgeschlossenen Fall auch allgemeiner diskrete Bewertungsringe.

Definition 3.48. Eine **endliche Stelle** eines Zahlkörpers F ist eine diskrete Bewertung von \mathfrak{o}_F , die zu einem Primideal von \mathfrak{o}_F gehört¹. Wir bezeichnen die Menge aller endlichen Stellen von F mit

$$M_{F,f}$$

und die Lokalisierung in $v \in M_{F,f}$ mit

$$\mathfrak{o}_{F,v} = \{x \in F^{\times} ; v(x) \geq 0\} \cup \{0\}.$$

Korollar 3.49. *Sei F ein Zahlkörper. Dann gilt:*

$$\mathfrak{o}_F = \bigcap_{v \in M_{F,f}^f} \mathfrak{o}_{F,v}.$$

Bemerkung 3.50. Seien F ein Zahlkörper und $v \in M_{F,f}$ eine endliche Stelle. Ein $x \in K$ bezeichnet man als v -ganz (oder als lokal ganz bei v), wenn $x = 0$ oder $v(x) \geq 0$ (äquivalent $x \in \mathfrak{o}_{F,v}$) gilt. Korollar 3.49 besagt, dann, daß die ganzen Elemente von K , also \mathfrak{o}_F , gerade die Elemente sind, die überall an allen endlichen Stellen von F lokal ganz sind.

4. DIE KLASSENGRUPPE

Die Klassengruppe ist eine wichtige arithmetische Invariante eines Dedekindrings. Sie mißt das Ausmaß des Versagens des Fundamentalsatzes der Arithmetik.

¹Als Korollar zum Satz von Ostrowski: das sind alle diskreten Bewertungen von F .

4.1. **Gebrochene und invertierbare Ideale.** Ideale sind „ideale Zahlen“, gebrochene Ideale sind dann „ideale Brüche“ mit beschränktem Nenner.

Definition 4.1. Sei R ein Integritätsring mit Quotientenkörper K .

(1) Ein **gebrochenes Ideal** von R ist ein R -Untermodul

$$I \subseteq K,$$

für das es ein $s \in R$ gibt, so daß

$$sI \subseteq R$$

ein Ideal ist.

(2) Das Produkt $IJ = I \cdot J$ zweier gebrochener Ideale ist der von den Produkten xy mit $x \in I$ und $y \in J$ erzeugte R -Untermodul von K .

Lemma 4.2. *Das Produkt zweier gebrochener Ideale ist ein gebrochenes Ideal.*

Beweis. Seien I, J zwei gebrochene Ideale und $s, t \in R$ mit sI, tJ sind Ideale von R . Dann ist

$$st(I \cdot J) = (sI) \cdot (tJ)$$

auch ein Ideal von R , somit IJ auch ein gebrochenes Ideal. \square

Lemma 4.3. *Ist R noethersch, so sind gebrochene Ideale von R endlich erzeugte R -Moduln.*

Beweis. I und sI haben bis auf Skalieren mit s die gleichen Erzeuger. \square

Definition 4.4. Ein **invertierbares Ideal** von R ist ein gebrochenes Ideal $I \subseteq R$, so daß es ein anderes gebrochenes Ideal $J \subseteq K$ gibt mit

$$I \cdot J = R.$$

Beispiel 4.5. Sei R ein diskreter Bewertungsring mit Quotientenkörper K , diskreter Bewertung v und Uniformisierende $\pi \in R$. Sei $I \subseteq K$ ein gebrochenes Ideal. Dann ist $I = (0)$ oder von der Form

$$I = \pi^n R = (\pi^n)$$

für das eindeutige $n \in \mathbb{Z}$ mit

$$n = \min\{v(x) ; x \in I\}.$$

Alle gebrochene Ideale $\neq (0)$ sind invertierbare Ideale:

$$(\pi^n)(\pi^{-n}) = R.$$

Beispiel 4.6. Sei R ein Integritätsring mit Quotientenkörper K . Zu einem $x \in K^\times$ ist

$$(x) = Rx \subseteq K$$

ein gebrochenes Ideal. Gebrochene Ideale dieser Form nennt man **(gebrochene) Hauptideale**.

Gebrochene Hauptideale sind invertierbare Ideale, weil für alle $x, y \in K^\times$

$$(x)(y) = (xy)$$

und daher ist (x^{-1}) das Inverse zu (x) .

Proposition 4.7. *Sei R ein Integritätsring. Die Menge*

$$I_R = \{I ; \text{invertierbares Ideal von } R\}$$

ist eine abelsche Gruppe bezüglich Multiplikation, die Idealgruppe von R .

Beweis. Das ist offensichtlich, denn R ist eine Eins für Multiplikation von gebrochenen Idealen, Assoziativität ist sowieso klar, und die Existenz eines Inversen wird ja gerade per Definition gefordert. Man muß nur kurz überlegen, daß R ein invertierbares Ideal ist, und daß das Inverse zu einem invertierbaren Ideal selbst auch invertierbar ist. Aber das ist beides klar. \square

Proposition 4.8. *Sei R ein Integritätsring und $S \subseteq R$ ein multiplikatives System. Lokalisieren liefert einen Gruppenhomomorphismus*

$$\begin{aligned} I_R &\rightarrow I_{S^{-1}R} \\ I &\mapsto S^{-1}I \end{aligned}$$

Beweis. Ist K der Quotientenkörper von R und $t \in R$ mit $tI \subseteq R$. Dann ist $S^{-1}I \subseteq S^{-1}K = K$ und $tS^{-1}I = S^{-1}(tI) \subseteq S^{-1}R$. Damit ist die Abbildung wohldefiniert.

Die Verträglichkeit von Lokalisieren mit Produkten von gebrochenen Idealen ist klar. \square

Beispiel 4.9. Sei R ein diskreter Bewertungsring mit Bewertung v und Uniformisierende $\pi \in R$. Die Zuordnung

$$\begin{aligned} I_R &\rightarrow \mathbb{Z} \\ I &\mapsto v(I) := \min\{v(x) ; x \in I\} \end{aligned}$$

ist ein Gruppenisomorphismus. Das folgt sofort, weil wir die Situation bei einem diskreten Bewertungsring so vollkommen explizit in der Hand haben.

Satz 4.10. *In einem Dedekindring A sind alle gebrochenen Ideale $I \neq (0)$ invertierbar.*

Beweis. Wir raten das Inverse als die maximale Menge von Elementen von K , die in einem Inversen liegen können:

$$I' = \{x \in K ; xI \subseteq A\}.$$

Dies kann man anders schreiben als

$$I' = \ker(K \rightarrow \text{Hom}_A(I, K/A))$$

wobei die Abbildung $x \in K$ auf die Linksmultiplikation $a \mapsto xa + A$ eingeschränkt auf I ist:

$$x \cdot : I \rightarrow K/A.$$

Die Menge $I' \subseteq K$ ist offensichtlich ein A -Modul und für jedes $t \in I$ gilt per Definition $tI' \subseteq A$. Damit ist I' ein gebrochenes Ideal.

Für jedes maximale Primideal \mathfrak{p} von A gilt (Lokalisieren ist exakt und verträglich mit Hom nach Satz 3.31)

$$\begin{aligned} (I')_{\mathfrak{p}} &= \ker(K \rightarrow \text{Hom}_A(I, K/A))_{\mathfrak{p}} \\ &= \ker(K_{\mathfrak{p}} \rightarrow \text{Hom}_A(I, K/A)_{\mathfrak{p}}) \\ &= \ker(K \rightarrow \text{Hom}_{A_{\mathfrak{p}}}(I_{\mathfrak{p}}, K_{\mathfrak{p}}/A_{\mathfrak{p}})) = (I_{\mathfrak{p}})'. \end{aligned}$$

Hier bezeichnen wir mit $(I_{\mathfrak{p}})'$ die entsprechende Konstruktion analog zu I' angewandt auf die Lokalisierung $I_{\mathfrak{p}}$.

Wir müssen nur noch zeigen, daß die offensichtliche Inklusion

$$I \cdot I' \subseteq A$$

eine Gleichheit ist. Das dürfen wir nach Lokalisieren an maximalen Primidealen \mathfrak{p} von A testen. Dies führt zu

$$(I \cdot I')_{\mathfrak{p}} = I_{\mathfrak{p}}(I')_{\mathfrak{p}} = I_{\mathfrak{p}} \cdot (I_{\mathfrak{p}})' = A_{\mathfrak{p}}.$$

Und das gilt, weil $A_{\mathfrak{p}}$ ein diskreter Bewertungsring ist: Wenn $I_{\mathfrak{p}} = (\pi^n)$ für eine Uniformisierende $\pi \in A_{\mathfrak{p}}$, dann ist $(I_{\mathfrak{p}})' = (\pi^{-n})$. \square

Theorem 4.11. *Sei A ein noetherscher Integritätsring mit Quotientenkörpern K . Es sind äquivalent:*

- (a) *Jedes gebrochene Ideal $I \neq (0)$ von A ist invertierbar.*
- (b) *A ist ein Dedekindring.*

Beweis. Die eine Richtung haben wir eben in Satz 4.10 bewiesen. Wir nehmen also nun an, daß alle gebrochenen Ideale $I \neq (0)$ von A invertierbar sind und müssen zeigen, daß A ein Dedekindring ist.

Sei $\mathfrak{p} \neq (0)$ ein Primideal von A . Dann ist \mathfrak{p} ein gebrochenes Ideal und nach Voraussetzung invertierbar. Es gibt also $I \subseteq K$ mit $\mathfrak{p} \cdot I = A$. Das gilt dann insbesondere mit

$$I = \mathfrak{p}' = \{x \text{ in } K ; x\mathfrak{p} \in A\},$$

weil in jedem Fall $I \subseteq \mathfrak{p}'$ und dann $A \subseteq \mathfrak{p} \cdot I \subseteq \mathfrak{p} \cdot \mathfrak{p}' \subseteq A$.

Wir lokalisieren nun an \mathfrak{p} . Dann ist $\mathfrak{p}_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ das maximale Ideal von $A_{\mathfrak{p}}$. Nach Lokalisieren in \mathfrak{p} finden wir, daß

$$\mathfrak{p}_{\mathfrak{p}} \cdot (\mathfrak{p}')_{\mathfrak{p}} = A_{\mathfrak{p}}.$$

Wie im Beweis von Theorem 3.18 folgt daraus, daß \mathfrak{p} lokal in $A_{\mathfrak{p}}$ von einem Element erzeugt wird. Die lokale Charakterisierung von Dedekindringen also von diskreten Bewertungsringen aus Satz 3.16, zeigt, daß

$$A_{\mathfrak{p}}$$

ein diskreter Bewertungsring ist. Insbesondere ist $\dim(A_{\mathfrak{p}}) = 1$. Da nach Satz 3.34 Primidealketten unterhalb von \mathfrak{p} in der Lokalisierung als Primidealketten derselben Länge überleben, und weil \mathfrak{p} beliebig $\neq (0)$ gewählt war, folgt

$$\dim(A) = 1.$$

Es bleibt zu zeigen, daß A ganz abgeschlossen in K ist. Sei $\tilde{A} \subseteq K$ der ganze Abschluß von A in K . Wir wollen zeigen, daß die Inklusion

$$A \subseteq \tilde{A}$$

eine Gleichheit ist. Das können wir lokal durch Lokalisieren in beliebigen maximalen Primidealen \mathfrak{p} von A testen. Nach Proposition 3.35 ist

$$A_{\mathfrak{p}} \subseteq (\tilde{A})_{\mathfrak{p}}$$

eine ganze Erweiterung. Weil $(\tilde{A})_{\mathfrak{p}} \subseteq K_{\mathfrak{p}} = K$ und $A_{\mathfrak{p}}$ als diskreter Bewertungsring selbst ganz abgeschlossen ist, folgt

$$A_{\mathfrak{p}} = (\tilde{A})_{\mathfrak{p}},$$

und das war zu zeigen. \square

Definition 4.12. Sei A ein Dedekindring und \mathfrak{p} ein maximales Primideal. Wir definieren die Abbildung

$$\begin{aligned} v_{\mathfrak{p}} : I_A &\rightarrow \mathbb{Z} \\ I &\mapsto v_{\mathfrak{p}}(I) = \min\{v_{\mathfrak{p}}(x) ; x \in I\}. \end{aligned}$$

Bemerkung 4.13. Die Abbildung $v_{\mathfrak{p}}$ auf gebrochenen Idealen ist die Komposition

$$I_A \xrightarrow{(-)_{\mathfrak{p}}} I_{A_{\mathfrak{p}}} \xrightarrow{v_{\mathfrak{p}}} \mathbb{Z},$$

wobei die zweite Abbildung diejenige aus Beispiel 4.9 ist. Insbesondere ist $v_{\mathfrak{p}}$ ein Gruppenhomomorphismus und

$$I_{\mathfrak{p}} = (\pi^{v_{\mathfrak{p}}(I)}).$$

Hier ist $\pi \in A_{\mathfrak{p}}$ eine Uniformisierende der diskreten Bewertung $v_{\mathfrak{p}}$.

Definition 4.14. Zu gebrochenen Idealen $I, J \subseteq K$ definieren wir das gebrochene Ideal

$$(I : J) = \{x \in K ; xJ \subseteq I\} = \ker(K \rightarrow \text{Hom}_A(J, K/I)).$$

Proposition 4.15. Seien A ein Dedekindring und \mathfrak{p} ein maximales Primideal.

Die Bewertung von gebrochenen Idealen hat die folgenden Eigenschaften: für alle gebrochenen Ideale I, J und alle $x \in K^{\times}$ gilt:

- (i) $v_p(IJ) = v_p(I) + v_p(J)$,
- (ii) $v_p(I + J) = \min\{v_p(I), v_p(J)\}$,
- (iii) $v_p(I \cap J) = \max\{v_p(I), v_p(J)\}$,
- (iv) $v_p((I : J)) = v_p(I) - v_p(J)$,
- (v) $v_p((x)) = v_p(x)$.

Beweis. Nachrechnen im Fall eines diskreten Bewertungsringes. Der allgemeine Fall folgt nach Lokalisieren. □

Proposition 4.16. *Sei $I \subseteq K$ ein gebrochenes Ideal. Dann ist*

$$I = \{x \in K ; v_p(x) \geq v_p(I) \text{ für alle maximalen Primideale } \mathfrak{p}\}.$$

Beweis. Es gilt $x \in I \iff (x) \subseteq I \iff$ für alle maximalen Primideale \mathfrak{p} von A ist $(x)_{\mathfrak{p}} \subseteq I_{\mathfrak{p}}$, und das bedeutet gerade $v_p(x) \geq v_p(I)$. □

4.2. Divisoren und Klassengruppe. Wir wenden uns nun dem idealen Fall des Fundamentalsatzes der Arithmetik zu: der eindeutigen Primidealzerlegung.

Proposition 4.17. *Sei A ein Dedekindring mit Quotientenkörper K . Für alle*

- (1) $x \in K^\times$ ist $v_p(x) \neq 0$
- (2) gebrochenen Ideale $I \subseteq K$ von A ist $v_p(I) \neq 0$
- (3) Ideale $(0) \neq \mathfrak{a} \subseteq A$ ist $v_p(\mathfrak{a}) \neq 0$

nur für endlich viele maximale Primideale \mathfrak{p} von A .

Beweis. Weil $v_p(x) = v_p((x))$ folgt (a) aus (b). Weil ein gebrochenes Ideal I von der Form $s^{-1}\mathfrak{a}$ mit $s \in A$ und $\mathfrak{a} \subseteq A$ ist, und weil

$$v_p(I) = v_p(\mathfrak{a}) - v_p(s),$$

folgt (b) aus (c) angewandt auf \mathfrak{a} und (s) .

Wir müssen also (c) zeigen. Es gilt sowieso $v_p(\mathfrak{a}) \geq 0$ und $v_p(\mathfrak{a}) > 0 \iff \mathfrak{a} \subseteq \mathfrak{p}$. (Nachweis durch Lokalisieren an allen maximalen Primidealen \mathfrak{q} von A .) Damit folgt die Behauptung aus dem folgenden allgemeineren Satz. □

Satz 4.18. *In einem noetherschem Ring R ist für jedes Ideal $\mathfrak{a} \subseteq R$ die Menge*

$$V(\mathfrak{a})^0 := \{\mathfrak{p} \in \text{Spec}(R) ; \mathfrak{a} \subseteq \mathfrak{p}, \text{ und kein Primideal } \mathfrak{a} \subseteq \mathfrak{q} \subsetneq \mathfrak{p}\}$$

der minimalen Primoberideale endlich.

Beweis. Der Beweis verwendet die wichtige Technik der **noetherschen Induktion**. Wir betrachten die Menge der Gegenbeispiele

$$\mathcal{B} = \{\mathfrak{a} ; \text{ Ideal von } R \text{ mit unendlich vielen minimalen Primoberidealen}\}.$$

Angenommen \mathcal{B} ist nicht leer. Weil R noethersch ist, gibt es dann ein maximales Gegenbeispiel $\mathfrak{a} \subseteq R$. Dann ist \mathfrak{a} nicht Primideal, sonst wäre \mathfrak{a} selbst das einzige minimale Primoberideal von \mathfrak{a} . Deshalb gibt es Zeugen $x, y \in R$ mit $x, y \notin \mathfrak{a}$ aber $xy \in \mathfrak{a}$. Betrachten wir $\mathfrak{b} = \mathfrak{a} + Rx$ und $\mathfrak{c} = \mathfrak{a} + Ry$. Dann ist für jedes Primideal \mathfrak{p} mit $\mathfrak{a} \subseteq \mathfrak{p}$ auch $xy \in \mathfrak{p}$, also $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. Daraus folgt $\mathfrak{b} \subseteq \mathfrak{p}$ oder $\mathfrak{c} \subseteq \mathfrak{p}$, kurz

$$V(\mathfrak{a})^0 \subseteq V(\mathfrak{b})^0 \cup V(\mathfrak{c})^0.$$

Weil \mathfrak{b} und \mathfrak{c} echt größer sind als \mathfrak{a} , haben \mathfrak{b} und \mathfrak{c} jeweils nur endlich viele minimale Primoberideale, und damit dann auch \mathfrak{a} , Widerspruch. □

Lemma 4.19. *Sei A ein Dedekindring und $\mathfrak{p}, \mathfrak{q}$ seien maximale Primideale. Dann gilt*

$$\mathfrak{q}_{\mathfrak{p}} = \mathfrak{q}A_{\mathfrak{p}} = \begin{cases} \mathfrak{p}_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}} & \text{für } \mathfrak{p} = \mathfrak{q}, \\ A_{\mathfrak{p}} & \text{für } \mathfrak{p} \neq \mathfrak{q}. \end{cases}$$

Beweis. Wenn $\mathfrak{p} = \mathfrak{q}$, dann ist die Behauptung trivial. Wenn $\mathfrak{p} \neq \mathfrak{q}$, dann gibt es $s \in (A \setminus \mathfrak{p}) \cap \mathfrak{q} \neq \emptyset$, denn beide Primideale sind maximal. Also liegt $1 = s/s \in \mathfrak{q}_{\mathfrak{p}}$, und damit gilt $\mathfrak{q}_{\mathfrak{p}} = (1) = A_{\mathfrak{p}}$. \square

Satz 4.20 (Eindeutige Primidealzerlegung). *In einem Dedekindring A haben gebrochene Ideale eindeutige Primidealzerlegung. Für jedes gebrochene Ideal $I \neq (0)$ gilt:*

- (1) $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$, wobei wir nur über die maximalen Primideale \mathfrak{p} von A mit $v_{\mathfrak{p}}(I) \neq 0$ multiplizieren und \mathfrak{p}^n für $n \in \mathbb{Z}$ im Sinne von invertierbaren Idealen gedacht ist.
- (2) Wenn $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ paarweise verschieden sind und $n_i \in \mathbb{Z}$ mit

$$I = \prod_{i=1}^r \mathfrak{p}_i^{n_i},$$

dann ist $n_i = v_{\mathfrak{p}_i}(I)$ und $v_{\mathfrak{p}}(I) = 0$ für alle $\mathfrak{p} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_r$.

Beweis. (1) Das wichtigste ist, daß es sich nach Proposition 4.17 um ein endliches Produkt handelt. Das Produkt ist also wohldefiniert. Anschließend kann man die Behauptete Gleichheit von gebrochenen Idealen nach Lokalisieren für alle maximalen Primideale \mathfrak{p} beweisen. Aber lokalisiert steht da nur

$$I_{\mathfrak{p}} = \left(\prod_{\mathfrak{q}} \mathfrak{p}^{v_{\mathfrak{q}}(I)} \right)_{\mathfrak{p}} = (\mathfrak{p}^{v_{\mathfrak{p}}(I)})_{\mathfrak{p}} \cdot \prod_{\mathfrak{q} \neq \mathfrak{p}} (\mathfrak{q}^{v_{\mathfrak{q}}(I)})_{\mathfrak{p}} = (\mathfrak{p}_{\mathfrak{p}})^{v_{\mathfrak{p}}(I)} \cdot \prod_{\mathfrak{q} \neq \mathfrak{p}} A_{\mathfrak{p}} = (\mathfrak{p}_{\mathfrak{p}})^{v_{\mathfrak{p}}(I)},$$

und das ist gerade die Definition von $v_{\mathfrak{p}}(I)$.

- (2) Wenn $I = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$, dann kann man für jedes \mathfrak{p} lokalisieren und erhält

$$\mathfrak{p}_{\mathfrak{p}}^{v_{\mathfrak{p}}(I)} = I_{\mathfrak{p}} = \left(\prod_{i=1}^r \mathfrak{p}_i^{n_i} \right)_{\mathfrak{p}} = \prod_{i=1}^r (\mathfrak{p}_i)_{\mathfrak{p}}^{n_i} = \begin{cases} (\mathfrak{p}_{\mathfrak{p}})_{\mathfrak{p}}^{n_i} & \text{falls } \mathfrak{p} = \mathfrak{p}_i \text{ für ein } i. \\ A_{\mathfrak{p}} = (\mathfrak{p}_{\mathfrak{p}})^0 & \text{sonst.} \end{cases}$$

Daraus folgt sofort die Behauptung. \square

Es gilt auch die Umkehrung: Primidealzerlegung charakterisiert Dedekindringe.

Theorem 4.21 (Noether 1927). *Ein noetherscher Integritätsring mit eindeutiger Primidealzerlegung ist ein Dedekindring.*

Definition 4.22. Sei A ein Dedekindring.

- (1) Ein **(Weil-)Divisor** von A ist eine formale \mathbb{Z} -Linearkombination von maximalen Primidealen.
- (2) Die **Divisorgruppe** ist die freie abelsche Gruppe auf der Menge der maximalen Primideale

$$\text{Div}(A) = \bigoplus_{\mathfrak{p} \neq (0)} \mathbb{Z} \cdot \mathfrak{p}.$$

Das ist gerade die Gruppe der Divisoren von A .

Korollar 4.23. *Sei A ein Dedekindring. Die Bewertungen der gebrochenen Ideale $v_{\mathfrak{p}}$ bilden zusammen einen Gruppenisomorphismus*

$$v : I_A \xrightarrow{\sim} \text{Div}(A)$$

$$I \mapsto \sum_{\mathfrak{p}} v_{\mathfrak{p}}(I) \cdot \mathfrak{p}.$$

Beweis. Das folgt sofort aus der eindeutigen Primidealzerlegung in A aus Satz 4.20. \square

Sei A ein Dedekindring mit Quotientenkörper K . Zu $x \in K^{\times}$ haben wir das **gebrochene Hauptideal** $(x) \in I_A$. Unter dem Isomorphismus mit der Divisorgruppe erhalten wir den **Hauptdivisor** zu x

$$\text{div}(x) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(x) \cdot \mathfrak{p}.$$

Die Zuordnung $\text{div}(-)$ ist ein Gruppenhomomorphismus.

Definition 4.24. Sei A ein Dedekindring mit Quotientenkörper K . Der Quotient

$$\text{Cl}(A) = \text{Div}(A) / \text{div}(K^\times)$$

wird **Klassengruppe** (genauer **Divisorklassengruppe**) von A .

Unter der Picardgruppe verstehen wir hier² die Gruppe

$$\text{Pic}(A) = I_A / \{(x) ; x \in K^\times\}.$$

der gebrochenen Ideale modulo der gebrochenen Hauptideale.

Bemerkung 4.25. Es folgt sofort aus Korollar 4.23, daß

$$\text{Pic}(A) \simeq \text{Cl}(A).$$

Die Picardgruppe spricht über Ideale, also A -Moduln, während die Klassengruppe über Primideale modulo einer Relation spricht. Letzteres sind im allgemeineren Kontext Zykel bis auf rationale Äquivalenz. Diese beiden Standpunkte fallen für Dedekindringe zusammen, finden aber im Allgemeinen verschiedene Verallgemeinerungen.

Proposition 4.26. Sei A ein Dedekindring. Dann gibt es eine exakte Sequenz

$$0 \rightarrow A^\times \rightarrow K^\times \xrightarrow{\text{div}} \text{Div}(A) \rightarrow \text{Cl}(A) \rightarrow 0.$$

Beweis. Wir müssen nur zeigen, daß

$$A^\times = \{x \in K^\times ; \text{div}(x) = 0\}$$

Trivialer Divisor $\text{div}(x) = 0$ ist äquivalent zu $v_{\mathfrak{p}}(x) \geq 0$ und $v_{\mathfrak{p}}(x^{-1}) \geq 0$ für alle maximalen Primideale \mathfrak{p} . Nach Satz 3.46 bedeutet das gerade $x \in A$ und $x^{-1} \in A$, also $x \in A^\times$. \square

Korollar 4.27. Sei A ein Dedekindring. Dann sind äquivalent:

- (a) $\text{Cl}(A) = 0$.
- (b) A ist Hauptidealring.
- (c) A ist faktoriell, d.h. noetherscher Integritätsring mit eindeutiger Primfaktorzerlegung.
- (d) In A sind alle irreduziblen Elemente Primelemente.

Beweis. (a) \implies (b): Wenn $\text{Cl}(A) = 0$, dann ist $\text{Pic}(A) = 0$ und somit jedes Ideal $\mathfrak{a} \in I_A$ von der Form (x) für ein $x \in K^\times$. Weil \mathfrak{a} ein Ideal ist, gilt dann

$$v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}((x)) = v_{\mathfrak{p}}(\mathfrak{a}) \geq 0$$

und nach Satz 3.46 bedeutet das gerade $x \in A$. Damit ist $\mathfrak{a} = (x)$ ein Hauptideal.

(b) \implies (c): Hauptidealringe sind faktoriell, siehe *Grundlagen der Algebra*.

(c) \implies (d): In faktoriellen Ringen sind irreduzible Elemente prim, weil sie ja eine Faktorisierung in Primelemente haben müssen.

(d) \implies (a): Wegen $\text{Cl}(A) = \text{Pic}(A)$, müssen wir zu jedem gebrochenen Ideal zeigen, daß es ein Hauptideal ist. Es reicht dies für Erzeuger, also für die maximalen Primideale nach Satz 4.20. Sei also \mathfrak{p} ein maximales Primideal von A . Dann gibt es $0 \neq x \in \mathfrak{p}$. Das Element x zerlegt sich als Produkt von irreduziblen Elementen, von denen ein Faktor bereits in \mathfrak{p} liegen muß. Ohne Einschränkung ist x bereits irreduzibel. Nun sagt (d), daß x Primelement ist. Wir haben damit eine Primidealkette

$$(0) \subsetneq (x) \subseteq \mathfrak{p}.$$

Da $\dim(A) = 1$ folgt $\mathfrak{p} = (x)$. \square

Für einen Zahlkörper gibt es eine spezielle Notation und Terminologie.

²Das stimmt mit der üblichen Definition als Isomorphieklassen von projektiven Moduln, die lokal vom Rang 1 sind, zusammen mit dem Tensorprodukt als Verknüpfung überein.

Definition 4.28. Die Klassenzahl des Zahlkörpers F ist

$$\text{Cl}_F := \text{Cl}(\mathfrak{o}_F)$$

und die Klassenzahl von F ist die Ordnung der Klassengruppe

$$h_F = |\text{Cl}_F|.$$

4.3. Schwache Approximation. Der folgende Satz hat Ähnlichkeit mit dem Mittag-Lefflerschen Satz aus der Funktionentheorie, wenn man bei den Bewertungen $v_{\mathfrak{p}}$ an Nullstellenordnungen im Punkte \mathfrak{p} denkt.

Satz 4.29 (Schwache Approximation). *Sei A ein Dedekindring mit Quotientenkörper K . Seien $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ paarweise verschiedene maximale Primideale von A , und seien $x_i \in K$, $n_i \in \mathbb{Z}$ für $i = 1, \dots, r$.*

Dann gibt es ein $x \in K$ mit

- (i) $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ für alle $i = 1, \dots, r$, und
- (ii) $v_{\mathfrak{p}}(x) \geq 0$ für alle $\mathfrak{p} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_r$.

Beweis. Sei $s \in A$ mit $sx_i = a_i \in A$. Angenommen wir können den Satz beweisen für a_i anstelle von x_i mit $a \in A$ anstelle von $x \in K$ und den Approximationsbedingungen

- (i) $v_{\mathfrak{p}_i}(a - a_i) \geq n_i + v_{\mathfrak{p}_i}(s)$ für alle $i = 1, \dots, r$, und
- (ii) $v_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}(s)$ für alle \mathfrak{p} mit $v_{\mathfrak{p}}(s) > 0$.

in diesem Fall ist $x = a/s$ eine Lösung des ursprünglichen Approximationsproblems.

Wir dürfen also ohne Einschränkung verlangen, daß $x_i \in A$, alle $n_i \geq 0$ (das Problem ist nur schwerer mit größeren n_i) und wir suchen ein $x \in A$ mit

$$v_{\mathfrak{p}_i}(x - x_i) \geq n_i$$

für alle $i = 1, \dots, r$. Die zweite Bedingung ist dann automatisch.

Nun ist das Approximationsproblem linear. Wenn für alle $i = 1, \dots, r$ ein $a_i \in A$ existiert, mit

$$v_{\mathfrak{p}_i}(a_i - x_i) \geq n_i$$

und für alle $j = 1, \dots, r$, $j \neq i$

$$v_{\mathfrak{p}_j}(a_i) \geq n_j,$$

dann löst

$$x = a_1 + \dots + a_r$$

aufgrund der Dreiecksungleichung für Bewertungen das ursprüngliche Approximationsproblem.

Sei also ohne Einschränkung $x_1 \in A$ beliebig und $x_2 = \dots = x_r = 0$. Wenn $r = 1$, dann ist nichts zu tun, denn $x = x_1$ löst das Problem. Ansonsten betrachten wir das Ideal

$$\mathfrak{a} := \mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2} \cdot \dots \cdot \mathfrak{p}_r^{n_r} \subseteq A.$$

Nach Lokalisieren an einem beliebigen maximalen Primideal \mathfrak{q} ist $\mathfrak{a}_{\mathfrak{q}} = A_{\mathfrak{q}}$, denn ein Summand wird mindestens zu $A_{\mathfrak{q}}$. Folglich ist $\mathfrak{a} = A$. Wir können daher schreiben

$$x_1 = (x_1 - x) + x$$

mit $x \in \mathfrak{p}_2^{n_2} \cdot \dots \cdot \mathfrak{p}_r^{n_r}$ und $x - x_1 \in \mathfrak{p}_1^{n_1}$. Dieses x ist das gesuchte Element. \square

Korollar 4.30 (Chinesischer Restsatz I). *Sei A ein Dedekindring, Seien $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ paarweise verschiedene maximale Primideale von A , und seien $n_i \in \mathbb{N}_0$ für $i = 1, \dots, r$. Dann gilt*

- (1) $\prod_{i=1}^r \mathfrak{p}_i^{n_i} = \bigcap_{i=1}^r \mathfrak{p}_i^{n_i}$.
- (2) Die natürliche Abbildung

$$A / \prod_{i=1}^r \mathfrak{p}_i^{n_i} \rightarrow \prod_{i=1}^r A / \mathfrak{p}_i^{n_i}$$

ist ein Ringisomorphismus.

Beweis. (2) Die Surjektivität der natürlichen Abbildung $\pi : A \rightarrow \prod_{i=1}^r A/\mathfrak{p}_i^{n_i}$ ist im Prinzip eine äquivalente Umformulierung des schwachen Approximationssatzes (in der Form aus dem Beweis ohne Nenner). Der Kern besteht aus dem Schnitt

$$\ker(\pi) = \bigcap_{i=1}^r \mathfrak{p}_i^{n_i}$$

und so bleibt für (2) nur noch (1) zu zeigen.

(1) folgt nach lokalisieren an einem beliebigen maximalen Primideal \mathfrak{q} . Wenn $\mathfrak{q} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_r$, dann steht auf beiden Seiten $A_{\mathfrak{q}}$. Ansonsten überlebt genau der Faktor mit $\mathfrak{p}_i = \mathfrak{q}$, die anderen Faktoren des Produkts bzw. des Schnitts sind $A_{\mathfrak{q}}$ und tragen nichts bei. Dies reduziert auf den Fall $r = 1$ von nur einer Primidealpotez, und die ist trivial. \square

Definition 4.31. Zwei Ideale \mathfrak{a} und \mathfrak{b} eines Rings R heißen **teilerfremd**, wenn $\mathfrak{a} + \mathfrak{b} = (1)$ ist.

Bemerkung 4.32. Für einen Dedekindring A sind Ideale \mathfrak{a} und \mathfrak{b} genau dann teilerfremd, wenn es kein maximales Primideal \mathfrak{p} von A gibt mit $v_{\mathfrak{p}}(\mathfrak{a}) > 0$ und $v_{\mathfrak{p}}(\mathfrak{b}) > 0$.

Korollar 4.33 (Chinesischer Restsatz II). *Sei A ein Dedekindring und seien \mathfrak{a} und \mathfrak{b} teilerfremde Ideale von A . Dann gilt*

- (1) $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.
- (2) Die natürliche Abbildung

$$A/\mathfrak{a}\mathfrak{b} \rightarrow A/\mathfrak{a} \times A/\mathfrak{b}$$

ist ein Ringisomorphismus.

Beweis. Die Primidealfaktorisierungen von \mathfrak{a} und \mathfrak{b} haben kein gemeinsames Primideal als Faktor. Dann folgt das Korollar sofort aus Korollar 4.30 angewandt auf die Primidealfaktorisierungen von \mathfrak{a} , von \mathfrak{b} und von $\mathfrak{a}\mathfrak{b}$. \square

In einem Dedekindring findet man Elemente des Quotientenkörpers mit vorgegebenen Bewertung an endlich vielen Stellen:

Korollar 4.34. *Sei A ein Dedekindring mit Quotientenkörper K . Seien $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ paarweise verschiedene maximale Primideale von A , und seien $n_i \in \mathbb{Z}$ für $i = 1, \dots, r$. Dann gibt es ein $x \in K$ mit*

- (i) $v_{\mathfrak{p}_i}(x) = n_i$ für alle $i = 1, \dots, r$, und
- (ii) $v_{\mathfrak{p}}(x) \geq 0$ für alle $\mathfrak{p} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_r$.

Wenn alle $n_i \geq 0$ sind, dann findet man sogar $x \in A$.

Beweis. Das ist eine Übungsaufgabe, die sofort aus dem schwachen Approximationssatz folgt. \square

Korollar 4.35. *Ein Dedekindring mit nur endlich vielen Primidealen ist ein Hauptidealring.*

Beweis. Seien $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ eine vollständige Liste der maximalen Primideale von A . Die Behauptung folgt sofort aus Korollar 4.34, weil damit für A die Divisorabbildung

$$K^\times \twoheadrightarrow \text{Div}(A) = \bigoplus_{i=1}^r \mathbb{Z} \cdot \mathfrak{p}_i$$

surjektiv ist. \square

Korollar 4.36. *Jedes gebrochene Ideal I eines Dedekindrings A kann von höchstens 2 Elementen erzeugt werden.*

Beweis. Sei $s \in K$ mit $\mathfrak{a} = sI$ ist eine Ideal. Es reicht offensichtlich die Behauptung für \mathfrak{a} zu zeigen.

Wenn $\mathfrak{a} = (0)$, dann ist nichts zu zeigen. Wir nehmen daher an, daß es $0 \neq x \in \mathfrak{a}$ gibt. Die Inklusion

$$(x) \subseteq \mathfrak{a}$$

ist nach Lokalisieren an \mathfrak{p} ein Isomorphismus, wenn $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(\mathfrak{a})$. Dies gilt an allen bis auf endlich vielen Stellen \mathfrak{p} . Wir nehmen die Liste der Ausnahmen \mathfrak{p} und alle \mathfrak{p} mit $v_{\mathfrak{p}}(\mathfrak{a}) > 0$:

$$\{\mathfrak{p}_1, \dots, \mathfrak{p}_s\} = \{\mathfrak{p} ; v_{\mathfrak{p}}(x) \neq v_{\mathfrak{p}}(\mathfrak{a}) \text{ oder } v_{\mathfrak{p}}(\mathfrak{a}) > 0\}.$$

Nach Korollar 4.34 können wir ein $y \in A$ finden mit

$$v_{\mathfrak{p}_i}(y) = v_{\mathfrak{p}_i}(\mathfrak{a}) \quad \text{für alle } i = 1, \dots, s.$$

Dann ist $y \in \mathfrak{a}$ nach Proposition 4.16, und

$$(x, y) = \mathfrak{a},$$

dies gilt lokal an jedem maximalen Primideal \mathfrak{p} :

- Wenn $\mathfrak{p} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_s$, dann ist $\mathfrak{a}_{\mathfrak{p}} = (x)_{\mathfrak{p}} \subseteq (x, y)_{\mathfrak{p}} \subseteq \mathfrak{a}_{\mathfrak{p}}$.
- Wenn $\mathfrak{p} = \mathfrak{p}_i$ für ein $i = 1, \dots, s$, dann ist $\mathfrak{a}_{\mathfrak{p}} = (y)_{\mathfrak{p}} \subseteq (x, y)_{\mathfrak{p}} \subseteq \mathfrak{a}_{\mathfrak{p}}$. □

Teil 2. Geometrie der Zahlen

5. GITTER

5.1. Algebraische und topologische Eigenschaften von Gittern. Ein endlich dimensionaler \mathbb{R} -Vektorraum V trägt eine natürliche Topologie durch Strukturtransport via eines Isomorphismus

$$V \simeq \mathbb{R}^n.$$

Je zwei dieser Isomorphismen unterscheiden sich um eine Automorphismus von \mathbb{R} , der die Topologie nicht verändert.

Eine Teilmenge $A \subseteq X$ eines topologischen Raumes heißt diskret, wenn die von X auf A induzierte Topologie die diskrete Topologie ist, d.h. für alle $a \in A$ gibt es eine offene Umgebung $U \subseteq X$ mit

$$U \cap A = \{a\}.$$

Definition 5.1. Ein **Gitter** in einem endlich dimensionalen \mathbb{R} -Vektorraum V ist eine diskrete Untergruppe $\Gamma \subseteq V$.

Bemerkung 5.2. Eine Untergruppe $\Gamma \subseteq V$ ist diskret genau dann, wenn $0 \in \Gamma$ diskret ist, d.h. wenn es eine offene Teilmenge $U \subseteq V$ gibt mit

$$U \cap \Gamma = \{0\}.$$

Translation ist ein Homöomorphismus und daher ist dann für alle $\gamma \in \Gamma$ die Menge $\gamma + U$ eine offenen Umgebung von γ , die als einzigen Gitterpunkt Γ enthält.

Beispiel 5.3. (1) $\mathbb{Z}[i] \subseteq \mathbb{C}$.

(2) $\mathbb{Z}^n \subseteq \mathbb{R}^n$.

(3) Kein Gitter ist $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$, obwohl auch $\mathbb{Z}[\sqrt{2}] \simeq \mathbb{Z}^2$ eine endlich erzeugte freie abelsche Gruppe ist.

Lemma 5.4. Eine diskrete Untergruppe $\Gamma \subseteq \mathbb{R}$ ist entweder $\Gamma = \{0\}$ oder es gibt ein $0 \neq x \in \mathbb{R}$ und

$$\Gamma = \{nx ; n \in \mathbb{Z}\} \simeq \mathbb{Z}.$$

Beweis. Die Menge

$$\{z \in \Gamma ; z > 0\}$$

ist entweder leer, dann haben wir $\Gamma = \{0\}$, oder aber sie besitzt als nach unten durch 0 beschränkte Menge ein Infimum x . Weil Γ diskret ist und das Infimum ein Häufungspunkt von Γ , also ein Grenzwert einer Folge aus Γ ist, muß besagte Folge letztendlich konstant werden: das Infimum ist ein Minimum (wird angenommen). Damit ist auch $x > 0$, denn jedes Element in der betrachteten Menge ist ja > 0 .

Angenommen es gibt ein Element $z \in \Gamma \setminus \mathbb{Z} \cdot x$. Wir betrachten $\vartheta = z/x$ und setzen $n = \lfloor \vartheta \rfloor \in \mathbb{Z}$. Dann ist auch

$$z' = z - nx \in \Gamma \setminus \mathbb{Z} \cdot x,$$

aber nach Konstruktion

$$0 < z' < x.$$

Das ist ein Widerspruch zur Konstruktion von x . Folglich gilt schon $\Gamma = \mathbb{Z} \cdot x$ wie behauptet. \square

Satz 5.5. Sei V ein endlich dimensionaler \mathbb{R} -Vektorraum und $\Gamma \subseteq V$ eine Untergruppe. Dann sind äquivalent:

(a) Γ ist eine Gitter.

(b) Γ ist als abelsche Gruppe von über \mathbb{R} linear unabhängigen Vektoren erzeugt.

(c) Die natürliche Abbildung

$$\mathbb{R} \otimes_{\mathbb{Z}} \Gamma \rightarrow V$$

ist injektiv und Γ ist eine endliche erzeugte abelsche Gruppe.

Beweis. (b) \implies (c): Sei $\gamma_1, \dots, \gamma_r$ ein Erzeugendensystem von Γ bestehend aus \mathbb{R} -linear unabhängigen Vektoren. Jedes Element in $\mathbb{R} \otimes_{\mathbb{Z}} \Gamma$ hat dann die Form

$$\sum_{i=1}^r x_i \otimes \gamma_i$$

für gewisse $x_i \in \mathbb{R}$. Unter der natürlichen Abbildung nach V wird dies auf die Linearkombination

$$x_1 \gamma_1 + \dots + x_r \gamma_r \in V$$

abgebildet. (c) folgt sofort.

(c) \implies (a): Als Untergruppe eines \mathbb{R} -Vektorraums ist Γ ohne Torsion. Daher gilt als abelsche Gruppe $\Gamma \simeq \mathbb{Z}^r$ nach dem Struktursatz für endlich erzeugte abelsche Gruppen. Die Abbildung $\Gamma \subseteq V$ faktorisiert dann als

$$\Gamma \simeq \mathbb{Z}^r \hookrightarrow \mathbb{R}^r = \mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}^r \simeq \mathbb{R} \otimes_{\mathbb{Z}} \Gamma \hookrightarrow V$$

letzteres wegen (c). Die auf Γ induzierte Topologie ist daher dieselbe, wie die auf $\mathbb{Z}^r \subseteq \mathbb{R}^r$, dem Standardgitter der ganzzahligen Vektoren im \mathbb{R}^r . Also ist Γ diskret, somit ein Gitter.

(a) \implies (b): Dies beweisen wir per Induktion über

$$r = \dim \langle \Gamma \rangle_{\mathbb{R}}.$$

Für $r = 0$ ist nichts zu tun. Für $r = 1$ ist Γ diskret in $\langle \Gamma \rangle_{\mathbb{R}} \simeq \mathbb{R}$. Diesen Fall behandelt Lemma 5.4.

Wir nehmen nun an, daß der Satz bewiesen ist für $< r$. Seien $v_1, \dots, v_r \in \Gamma$ linear unabhängige Vektoren. Seien

$$W_0 = \langle v_1, \dots, v_{r-1} \rangle_{\mathbb{R}} \subset W = \langle v_1, \dots, v_r \rangle_{\mathbb{R}} = \langle \Gamma \rangle_{\mathbb{R}}$$

und

$$\Gamma_0 = \Gamma \cap W_0.$$

Dann ist Γ_0 ein Gitter in W_0 und zwangsläufig

$$\dim \langle \Gamma_0 \rangle_{\mathbb{R}} \leq \dim W_0 = r - 1.$$

Der Satz gilt somit für Γ_0 . Seien $\gamma_1, \dots, \gamma_{r-1}$ eine \mathbb{Z} -Basis von Γ_0 aus \mathbb{R} -linear unabhängigen Vektoren. Dann kann man die v_1, \dots, v_{r-1} durch die $\gamma_1, \dots, \gamma_{r-1}$ ersetzen. Wir betrachten nun

$$\text{pr} : \Gamma \subseteq W \rightarrow W/W_0 = \mathbb{R} \cdot v_r.$$

Das Bild $\bar{\Gamma} = \text{pr}(\Gamma) \subseteq \mathbb{R}$ ist ein Gitter, weil für alle $0 < c \in \mathbb{R}$

$$\begin{aligned} \bar{\Gamma} \cap \{av_r ; |a| < c\} &= \text{pr} \left((\Gamma \cap (W_0 \times (-c, c) \cdot v_r)) \right) \\ &= \text{pr} \left(\Gamma \cap \left\{ x = av_r + \sum_{i=1}^{r-1} a_i \gamma_i ; |a_i| \leq 1, |a| \leq c \right\} \right) \end{aligned}$$

Weil Γ diskret und $\{x = av_r + \sum_{i=1}^{r-1} a_i \gamma_i ; |a_i| \leq 1, |a| \leq c\}$ beschränkt ist, handelt es sich um eine endliche Menge. Somit ist $\bar{\Gamma}$ diskret in $\mathbb{R} \cdot v_r \simeq \mathbb{R}$. Erneut Lemma 5.4 zeigt $\bar{\Gamma} \simeq \mathbb{Z} \cdot \bar{\gamma}$.

Nun betrachten wir die kurze exakte Sequenz

$$0 \rightarrow \Gamma_0 \rightarrow \Gamma \xrightarrow{\text{pr}} \bar{\Gamma} \rightarrow 0.$$

Wählen wir ein Urbild $\gamma_r \in \Gamma$ mit $\text{pr}(\gamma_r) = \bar{\gamma}$, so folgt wie üblich

$$\Gamma = \langle \gamma_1, \dots, \gamma_r \rangle_{\mathbb{Z}}$$

und dies zeigt (b). □

Korollar 5.6. Jede \mathbb{Z} -Basis eines Gitters $\Gamma \subseteq \mathbb{R}$ ist auch \mathbb{R} -linear unabhängig.

Beweis. Sofort aus dem Beweis von Satz 5.5 □

Definition 5.7. Ein Gitter Γ in einem endlichdimensionalen \mathbb{R} -Vektorraum V heißt **vollständig**, falls Γ eine \mathbb{R} -Basis von V enthält, also $\mathbb{R} \otimes_{\mathbb{Z}} \Gamma \simeq V$ gilt.

Sei $\Gamma \subseteq V$ ein vollständiges Gitter und $\underline{v} = (v_1, \dots, v_n)$ eine \mathbb{Z} -Basis, dann bezeichnen wir eine **Grundmasche** von Γ (bezüglich \underline{v}) mit

$$\Phi = \Phi(\underline{v}) := \left\{ x = \sum_{i=1}^n t_i v_i ; 0 \leq t_i \leq 1 \text{ für alle } i = 1, \dots, n \right\}.$$

Satz 5.8. Sei $\Gamma \subseteq V$ ein Gitter. Dann sind äquivalent:

- (a) Γ ist vollständig.
- (b) V/Γ ist mit der Quotiententopologie kompakt.
- (c) Es gibt eine beschränkte Menge $M \subseteq V$ mit

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

Beweis. (a) \implies (b): Wenn Γ vollständig ist, dann ist Φ kompakt und $\Phi \rightarrow V/\Gamma$ surjektiv. Als Bild einer kompakten Menge ist dann auch V/Γ kompakt.

(b) \implies (c): Sei $\|\cdot\|$ eine Norm auf V . Wir betrachten die Bilder der Mengen

$$U_r = \{x \in V ; \|x\| < r\}$$

unter $\pi : V \rightarrow V/\Gamma$. Die Bilder $\pi(U_r)$ in V/Γ sind offen und wegen $\bigcup_{r>0} U_r = V$ ist

$$\bigcup_{r>0} \pi(U_r) = V/\Gamma.$$

Weil V/Γ kompakt ist, reichen endlich viele dieser Bilder. Weil die Bilder aufsteigend ineinander enthalten sind, reicht schon eins, sagen wir U_R . Sei $M = \text{Abschluß von } U_R$. Dann ist M beschränkt und $\bigcup_{\gamma \in \Gamma} \gamma + M = V$.

(c) \implies (a): Angenommen Γ ist nicht vollständig. Dann ist algebraisch $\Gamma \subseteq V$ isomorph zu $\mathbb{Z}^r \subseteq \mathbb{R}^n$ als Untergruppe mit ganzzahligen Koordinaten und Einträgen 0 für die Koordinaten x_{r+1}, \dots, x_n . Dabei ist $r < n$, weil Γ als nicht vollständig angenommen wird. Die Koordinate x_n definiert dann eine Linearform

$$x_n : V \rightarrow \mathbb{R}$$

die auf Γ identisch 0 ist und auf M beschränkt. Daher ist x_n auf $V = \bigcup_{\gamma \in \Gamma} \gamma + M$ beschränkt: Widerspruch. □

5.2. Metrische Eigenschaften von Gittern. Nun betrachten wir ein vollständiges Gitter in einem euklidischen Vektorraum. Die zusätzliche metrische Eigenschaft macht die algebraisch ununterscheidbaren Gitter, alle sind isomorph zu $\mathbb{Z}^n \subseteq \mathbb{R}^n$, verschieden durch die relative Position von Orthonormalbasen zu Gitterbasen.

Sei $(V, \langle -, - \rangle)$ ein euklidischer Vektorraum der Dimension n . Dazu gehört ein translationsinvariantes Maß, eine Volumenform, die für eine ONB e_1, \dots, e_n von V dem Würfel

$$\Phi(\underline{e}) = \left\{ x = \sum_{i=1}^n t_i e_i ; 0 \leq t_i \leq 1 \text{ für alle } i = 1, \dots, n \right\}$$

das Volumen

$$\text{vol}(\Phi(\underline{e})) = 1$$

zuordnet. Nach der linearen Transformationsformel für das Volumen gilt dann für einen Endomorphismus A mit $Ae_i = v_i$

$$\text{vol}(\Phi(v_1, \dots, v_n)) = |\det(A)|.$$

Proposition 5.9. Sei $\Gamma \subseteq V$ ein vollständiges Gitter im euklidischen Vektorraum $(V, \langle -, - \rangle)$. Sei Δ_Γ die Diskriminante von Γ bezüglich der Bilinearform $\langle -, - \rangle$. Es gilt

$$\text{vol}(V/\Gamma) = \text{vol}(\Phi) = \sqrt{|\Delta_\Gamma|}.$$

Beweis. Wir führen Koordinaten bezüglich einer ONB e_1, \dots, e_n ein. Sei v_1, \dots, v_n eine \mathbb{Z} -Basis von Γ und $A = (a_{ij}) = [v_1, \dots, v_n]$ die Matrix mit den Spalten v_i , also $Ae_i = v_i$. Dann ist

$$A^t A = \left(\sum_{\nu=1}^n a_{\nu i} a_{\nu j} \right) = (\langle v_i, v_j \rangle)$$

die Gram'sche Matrix von $\langle -, - \rangle$ bezüglich der v_1, \dots, v_n . Damit ist

$$\Delta_\Gamma = \det(\langle v_i, v_j \rangle) = \det(A^t) \det(A) = \det(A)^2 = \text{vol}(\Phi(v))^2. \quad \square$$

Definition 5.10. Man versteht (mißbräuchlich) unter dem **Volumen** von Γ die Zahl

$$\text{vol}(\Gamma) = \text{vol}(V/\Gamma) = \sqrt{|\Delta_\Gamma|}.$$

Eine bessere Terminologie ist **Ko-Volumen**.

Definition 5.11. Sei V ein \mathbb{R} -Vektorraum und $A \subseteq V$ eine Teilmenge.

- (1) A ist **zentralsymmetrisch**, wenn $-A = A$.
- (2) A ist **konvex**, wenn für alle $x, y \in A$ die Strecke zwischen x und y in A liegt, d.h. für alle $0 \leq t \leq 1$ gilt

$$tx + (1-t)y \in A.$$

Satz 5.12 (Minkowskischer Gitterpunktsatz). Sei $\Gamma \subseteq V$ ein vollständiges Gitter in einem euklidischen Vektorraum V der Dimension $n = \dim(V)$. Sei $M \subseteq V$ eine Teilmenge, die zentralsymmetrisch, konvex und meßbar ist. Wenn

$$\text{vol}(M) > 2^n \cdot \text{vol}(\Gamma),$$

dann enthält M einen von 0 verschiedenen Gitterpunkt von Γ .

Beweis. Angenommen alle Translate $\gamma + \frac{1}{2}M$ für $\gamma \in \Gamma$ sind disjunkt. Dann gilt

$$\begin{aligned} \text{vol}(\Gamma) = \text{vol}(\Phi) &\geq \sum_{\gamma \in \Gamma} \text{vol}\left(\left(\gamma + \frac{1}{2}M\right) \cap \Phi\right) = \sum_{\gamma \in \Gamma} \text{vol}\left(\frac{1}{2}M \cap (\Phi - \gamma)\right) \\ &= \text{vol}\left(\frac{1}{2}M \cap \bigcup_{\gamma \in \Gamma} \Phi - \gamma\right) = \text{vol}\left(\frac{1}{2}M\right) = 2^{-n} \text{vol}(M) \end{aligned}$$

im Widerspruch zur Voraussetzung.

Seien $\gamma_1 \neq \gamma_2$ Gitterelemente mit

$$x \in \gamma_1 + \frac{1}{2}M \cap \gamma_2 + \frac{1}{2}M.$$

Dann gibt es $m_1, m_2 \in M$ mit

$$x = \gamma_1 + \frac{1}{2}m_1 = \gamma_2 + \frac{1}{2}m_2.$$

Folglich ist

$$0 \neq \gamma_1 - \gamma_2 = \left(x - \frac{1}{2}m_1\right) - \left(x - \frac{1}{2}m_2\right) = \frac{1}{2}m_2 + \frac{1}{2}(-m_1).$$

Weil M zentralsymmetrisch ist, haben wir $-m_1 \in M$, und weil M konvex ist auch $\frac{1}{2}m_2 + \frac{1}{2}(-m_1) \in M$. Somit ist

$$\gamma_1 - \gamma_2 \in \Gamma \cap M$$

der gesuchte Gitterpunkt. □

Beispiel 5.13. Sei $\Gamma \subseteq V$ ein vollständiges Gitter in einem euklidischen Vektorraum V , und sei v_1, \dots, v_n eine \mathbb{Z} -Basis von Γ . Wir setzen für $r > 0$

$$B_r = \left\{ x = \sum_{i=1}^n t_i v_i ; -r < t_i < r \right\},$$

das ist der r -Ball in der sup-Norm bezüglich der Basis v_1, \dots, v_n . Dann ist für alle $0 < r < 1$

$$B_r \cap \Gamma = \{0\}$$

und

$$\lim_{r \rightarrow 1} \text{vol}(B_r) = 2^n \text{vol}(\Gamma).$$

Da B_r konvex und zentralsymmetrisch ist, zeigt dies, daß die Voraussetzung im Minkowskischen Gitterpunktsatz in Bezug auf die Abschätzung scharf ist.

6. DER MINKOWSKI-Raum

Auf Minkowski gehen Ergebnisse zurück, die darauf beruhen, die ganzen Zahlen \mathfrak{o}_F eines Zahlkörpers vom Grad $n = [F : \mathbb{Q}]$ als Gitterpunkte in einem n -Dimensionalen reellen euklidischen Raum aufzufassen.

6.1. Unendliche Stellen eines Zahlkörpers. Sei F ein Zahlkörper vom Grad $n = [F : \mathbb{Q}]$. Die Menge der komplexen Einbettungen

$$\text{Hom}_{\mathbb{Q}}(F, \mathbb{C})$$

hat n Elemente. Die Galoisgruppe $\text{Gal}(\mathbb{C}/\mathbb{R})$ wirkt durch Komposition auf den $\tau : F \rightarrow \mathbb{C}$, und zwar die komplexe Konjugation durch

$$\tau \mapsto \bar{\tau} = (a \mapsto \overline{\tau(a)}).$$

Definition 6.1. Die **unendlichen Stellen** des Zahlkörpers F sind die $\text{Gal}(\mathbb{C}/\mathbb{R})$ -orbits auf $\text{Hom}_{\mathbb{Q}}(F, \mathbb{C})$. Wir bezeichnen diese als

$$M_{F, \infty} = M_{F, \mathbb{R}} \amalg M_{F, \mathbb{C}}$$

wobei die **reellen Stellen** $M_{F, \mathbb{R}} = \text{Hom}_{\mathbb{Q}}(F, \mathbb{R})$ die Einbettungen $\rho : F \rightarrow \mathbb{R}$ sind, und die **komplexen Stellen** $M_{F, \mathbb{C}}$ aus Paaren von komplex konjugierten Einbettungen $\sigma, \bar{\sigma} : F \rightarrow \mathbb{C}$ bestehen, die nicht über \mathbb{R} faktorisieren.

Die Anzahl der reellen Stellen bezeichnen wir mit $r = r_F$ und die der komplexen Stellen mit $s = s_F$.

Proposition 6.2. *Es gilt*

$$r + 2s = [F : \mathbb{Q}]$$

Beweis. Offensichtlich. □

Satz 6.3. *Sei F ein Zahlkörper mit s komplexen Stellen. Dann ist*

$$\text{sign}(\Delta_F) = (-1)^s.$$

Beweis. Wir nehmen die Notation aus dem Stickelbergerschen Determinantensatz, Satz 2.34, wieder auf. Damit ist

$$\Delta_F = \det(\sigma_i(\alpha_j))^2 = (P - N)^2 \in \mathbb{Z}.$$

Die komplexe Konjugation auf \mathbb{C} vertauscht konjugierte komplexe Einbettungen $\sigma, \bar{\sigma} : F \hookrightarrow \mathbb{C}$ und fixiert die reellen Einbettungen $\rho : F \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$. Die entsprechende Permutation ist ein Produkt aus s Transpositionen und hat Signum $(-1)^s$. Daher gilt

$$\overline{P - N} = (-1)^s (P - N)$$

und

$$\Delta_F = (P - N)^2 = (-1)^s \overline{P - N} \cdot (P - N) = (-1)^s |P - N|^2$$

mit demselben Vorzeichen wie $(-1)^s$. □

6.2. Die lokale Beschreibung eines Zahlkörpers bei unendlichen Stellen. Die Abbildung

$$j_{\mathbb{C}} : F_{\mathbb{C}} := F \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} \prod_{\tau: F \rightarrow \mathbb{C}} \mathbb{C} \quad (6.1)$$

$$a \otimes z \mapsto j_{\mathbb{C}}(a \otimes z) = (\tau(a)z)_{\tau}$$

ist ein \mathbb{C} -Algebrenisomorphismus³. In der Tat haben beide Seiten $\dim_{\mathbb{C}} = n$ und die lineare Unabhängigkeit der Charaktere zeigt die Injektivität.

Etwas weit hergeholt aber dennoch wahr stellt (6.1) einen Vergleichsisomorphismus zwischen der 0-ten de Rham Kohomologie von $\text{Spec}(F)$ mit der 0-ten (Betti)-Singulären-Kohomologie von $\text{Spec}(F)$ dar.

Zwar ist (6.1) \mathbb{C} -linear, dennoch sind die komplexen Konjugationen (also die reellen Strukturen) verschieden:

$$a \otimes z \mapsto a \otimes \bar{z}$$

$$(x_{\tau})_{\tau} \mapsto (\bar{x}_{\bar{\tau}})_{\tau}.$$

Definition 6.4. Wir bezeichnen mit **Frobenius bei ∞** und der Notation Φ_{∞} die \mathbb{R} -lineare Abbildung, welche das folgende Diagramm kommutativ macht:

$$\begin{array}{ccc} F_{\mathbb{C}} & \xrightarrow{\text{id} \otimes \bar{}} & F_{\mathbb{C}} \\ \downarrow j_{\mathbb{C}} & & \downarrow j_{\mathbb{C}} \\ \prod_{\tau} \mathbb{C} & \xrightarrow{\Phi_{\infty}} & \prod_{\tau} \mathbb{C}, \end{array}$$

die also die komplexe Konjugation von $F_{\mathbb{C}}$ auf $\prod_{\tau} \mathbb{C}$ transportiert.

Lemma 6.5. Konkret ist

$$\Phi_{\infty}((x_{\tau})_{\tau}) = (\bar{x}_{\bar{\tau}})_{\tau}$$

die gleichzeitige komplexe Konjugation der Komponenten von $x = (x_{\tau})_{\tau}$ und die Permutation der Einbettungen $\tau : F \rightarrow \mathbb{C}$ mittels Komposition mit der komplexen Konjugation.

Beweis.

$$\Phi_{\infty}(j_{\mathbb{C}}(a \otimes z)) = \Phi_{\infty}((\tau(a)z)_{\tau}) = (\overline{(\tau(a)z)})_{\tau} = (\tau(a)\bar{z})_{\tau}. \quad \square$$

Bemerkung 6.6. Wir betrachten die semi-lineare Involution Φ_{∞} als Wirkung der Galoisgruppe $\text{Gal}(\mathbb{C}/\mathbb{R})$ auf $\prod_{\tau} \mathbb{C}$.

³Alternative: Sei $F = \mathbb{Q}(\alpha)$ mit $f(X) \in \mathbb{Q}[X]$ normiertem Minimalpolynom von α . Dann ist

$$f(X) = \prod_{\tau: F \rightarrow \mathbb{C}} (X - \tau(\alpha))$$

Wir finden $F = \mathbb{Q}[X]/(f)$ und berechnen nach dem Chinesischen Restsatz für Polynome

$$F_{\mathbb{C}} = \mathbb{Q}[X]/(f) \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}[X]/(f) \simeq \prod_{\tau} \mathbb{C}[X]/(X - \tau(\alpha)) = \prod_{\tau} \mathbb{C}$$

wobei der Isomorphismus gerade $a \otimes z$ auf $\tau(a)z$ in der τ -Komponente abbildet.

6.3. Die natürliche hermitesche Metrik. Wir haben auf F die Spurform und ebenso durch Erweiterung der Skalare die Spurform auf $F_{\mathbb{C}}$ als komplexe bilineare Form. Wir machen daraus eine hermitesche Form, indem wir das zweite Argument zuerst konjugieren:

$$\begin{aligned} \langle -, - \rangle : \mathbb{F}_{\mathbb{C}} \times \mathbb{F}_{\mathbb{C}} &\rightarrow \mathbb{C} \\ \langle a \otimes z, b \otimes w \rangle &= \operatorname{tr}_F(ab)z\bar{w}. \end{aligned}$$

Auf $\prod_{\tau} \mathbb{C}$ haben wir die hermitesche Standardform: für alle $x = (x_{\tau})_{\tau}$ und $y = (y_{\tau})_{\tau}$

$$\langle x, y \rangle = \sum_{\tau} x_{\tau} \bar{y}_{\tau}.$$

Lemma 6.7. *Die hermitesche Metrik auf $\prod_{\tau} \mathbb{C}$ ist $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ -äquivariant: für alle $x, y \in \prod_{\tau} \mathbb{C}$ gilt*

$$\langle \Phi_{\infty}(x), \Phi_{\infty}(y) \rangle = \overline{\langle x, y \rangle}.$$

Beweis. Sei $x = (x_{\tau})$ und $y = (y_{\tau})$. Dann rechnen wir

$$\langle \Phi_{\infty}(x), \Phi_{\infty}(y) \rangle = \sum_{\tau} \Phi(x)_{\tau} \overline{\Phi(y)_{\tau}} = \sum_{\tau} \bar{x}_{\tau} y_{\tau} = \sum_{\tau} \bar{x}_{\tau} y_{\tau} = \overline{\sum_{\tau} x_{\tau} \bar{y}_{\tau}} = \overline{\langle x, y \rangle}. \quad \square$$

Wir identifizieren F mittels $F \rightarrow F \otimes_{\mathbb{Q}} \mathbb{C}$ und $j_{\mathbb{C}}$ mit seinem Bild.

Bemerkung 6.8. Seien $a, b \in F$. Dann ist

$$\langle a, b \rangle = \sum_{\tau} \tau(a) \overline{\tau(b)} = \sum_{\tau} \tau(a) \bar{\tau}(b).$$

Das ist verwandt mit der Spurform

$$\operatorname{tr}_{F|\mathbb{Q}}(ab) = \sum_{\tau} \tau(ab) = \sum_{\tau} \tau(a)\tau(b),$$

aber eben nicht exakt die Spurform.

6.4. Diskriminante und Volumen im Minkowski–Raum. Wir gehen nun zur \mathbb{R} -Algebra

$$F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R}$$

über. Dies sind die Invarianten von $\mathbb{F}_{\mathbb{C}}$ unter der komplexen Konjugation. Entsprechend interessieren wir uns nun für den Minkowski–Raum.

Definition 6.9. Der **Minkowski–Raum** des Zahlkörpers F ist

$$\left(\prod_{\tau} \mathbb{C} \right)^{+} := \{x \in \prod_{\tau} \mathbb{C} ; \Phi_{\infty}(x) = x\}$$

als euklidischer Vektorraum bezüglich der Einschränkung von $\langle -, - \rangle$.

Bemerkung 6.10. Für $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ -Moduln M bezeichnet man oft die Invarianten mit

$$M^{+} = M^{\operatorname{Gal}(\mathbb{C}/\mathbb{R})} = \{x \in M ; \sigma(x) = x \text{ für alle } \sigma \in \operatorname{Gal}(\mathbb{C}/\mathbb{R})\} = H^0(\operatorname{Gal}(\mathbb{C}/\mathbb{R}), M).$$

Lemma 6.11. *Die Einschränkung von $\langle -, - \rangle$ auf $\left(\prod_{\tau} \mathbb{C} \right)^{+}$ ist ein Skalarprodukt.*

Beweis. Für alle $x, y \in \left(\prod_{\tau} \mathbb{C} \right)^{+}$ gilt

$$\langle x, y \rangle = \langle \Phi_{\infty}(x), \Phi_{\infty}(y) \rangle = \overline{\langle x, y \rangle}.$$

Also nimmt $\langle x, y \rangle$ Werte in \mathbb{R} an. Weiter gilt $\langle x, x \rangle > 0$ für $x \neq 0$, weil $\langle -, - \rangle$ hermitesches Skalarprodukt ist. \square

Die Abbildung $j_{\mathbb{C}}$ induziert einen Isomorphismus auf $\text{Gal}(\mathbb{C}/\mathbb{R})$ -Invarianten:

$$j_{\mathbb{R}} : F \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \left(\prod_{\tau} \mathbb{C} \right)^+.$$

Satz 6.12. *Sei F ein Zahlkörper. Dann bildet*

$$j : F \rightarrow F \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \left(\prod_{\tau} \mathbb{C} \right)^+$$

jede Ordnung und jedes gebrochene Ideal von F auf ein vollständiges Gitter des Minkowski-Raumes ab.

Beweis. Für ein gebrochenes Ideal $I \subseteq F$ mit $s \in F^{\times}$ so daß $sI = \mathfrak{a} \subseteq \mathfrak{o}_F$, folgt

$$I \otimes_{\mathbb{Z}} \mathbb{Q} = \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathfrak{o}_F \otimes_{\mathbb{Z}} \mathbb{Q} = F,$$

denn \mathfrak{a} hat endlichen Index in \mathfrak{o}_F . Allgemeiner gilt für jede Ordnung \mathfrak{o} von F

$$\mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Q} = F.$$

Sei Γ eine Ordnung \mathfrak{o} oder ein gebrochenes Ideal $I \subseteq F$. Dann ist auch

$$\Gamma \otimes_{\mathbb{Z}} \mathbb{R} = (\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} = F \otimes_{\mathbb{Q}} \mathbb{R}.$$

Wir haben somit ein Gitter nach Satz 5.5 und ein vollständiges Gitter per Definition von vollständig. \square

Satz 6.13. *Sei F ein Zahlkörper. Dann gilt*

$$\text{vol}(\mathfrak{o}_F) = \sqrt{|\Delta_F|}$$

und analog für jede Ordnung in F .

Beweis. Sei $n = [F : \mathbb{Q}]$ und sei $\alpha_1, \dots, \alpha_n$ eine \mathbb{Z} -Basis von \mathfrak{o}_F . Nummerieren wir mit τ_1, \dots, τ_n alle Einbettungen $F \hookrightarrow \mathbb{C}$. Dann betrachten wir die Matrix

$$A = (\tau_i(\alpha_j)) \in M_n(\mathbb{C})$$

und finden die Gramsche Matrix zu $\langle -, - \rangle$ bezüglich $\alpha_1, \dots, \alpha_n$ als

$$A^t \bar{A} = \left(\sum_{k=1}^n \tau_k(\alpha_i) \overline{\tau_k(\alpha_j)} \right)_{1 \leq i, j \leq n} = \left(\sum_{\tau} \tau(\alpha_i) \overline{\tau(\alpha_j)} \right) = (\langle \alpha_i, \alpha_j \rangle).$$

Damit gilt

$$\text{vol}(\mathfrak{o}_F) = \sqrt{|\det(\langle \alpha_i, \alpha_j \rangle)|} = \sqrt{|\det(A^t \bar{A})|} = |\det(A)|.$$

Die Diskriminante von \mathfrak{o}_F haben wir bezüglich der Spurform definiert. Die zugehörige Gramsche Matrix ist

$$A^t A = \left(\sum_{\tau} \tau(\alpha_i) \tau(\alpha_j) \right) = (\text{tr}_{F|\mathbb{Q}}(\alpha_i \alpha_j)),$$

somit

$$|\Delta_F| = \sqrt{|\det(\text{tr}_{F|\mathbb{Q}}(\alpha_i \alpha_j))|} = \sqrt{|\det(A^t A)|} = |\det(A)|. \quad \square$$

Korollar 6.14. *Sei F ein Zahlkörper und $\mathfrak{a} \subseteq \mathfrak{o}_F$ ein Ideal. Dann hat $j(\mathfrak{a})$ als vollständiges Gitter in $(\prod_{\tau} \mathbb{C})^+$ das Kovolumen*

$$\text{vol}(j(\mathfrak{a})) = \sqrt{|\Delta_F|} \cdot (\mathfrak{o}_F : \mathfrak{a}).$$

Beweis. Satz 6.13 und sinngemäß Korollar 2.31. \square

6.5. Kanonisches Maß versus Lebesgue-Maß. Mit dem Raum der Invarianten zu operieren ist für konkrete Rechnungen unpraktisch. Die Galoisoperation vertauscht Koordinaten gemäß der Galoisoperation auf Einbettungen $\tau : F \rightarrow \mathbb{C}$. Demnach ist

$$x = (x_\tau)_\tau \in \left(\prod_\tau \mathbb{C} \right)^+ \iff \begin{cases} x_\rho \in \mathbb{R} & \tau = \rho \text{ reelle,} \\ x_{\bar{\sigma}} = \bar{x}_\sigma & \tau = \sigma \text{ komplex.} \end{cases}$$

Von den komplexen Einbettungen brauchen wir also nur die Hälfte.

Wir vereinbaren, daß von nun an $\rho \in M_{F,\mathbb{R}}$ und σ über ein Vertretersystem von $M_{F,\mathbb{C}}$ laufen. Dann ist

$$j_{\mathbb{R}} : F \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{\rho} \mathbb{R} \times \prod_{\sigma} \mathbb{C}.$$

Betrachten wir auf den komplexen Koordinaten z Realteil $\Re(z)$ und Imaginärteil $\Im(z)$ als reelle Koordinaten, so erhalten wir

$$j_{\mathbb{R}} : F \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{\rho} \mathbb{R} \times \prod_{\sigma} \mathbb{C} \simeq \mathbb{R}^{r+2s} = \mathbb{R}^n$$

verbunden mit einem weiteren Standardskalarprodukt, das wir mit

$$\langle -, - \rangle_L$$

bezeichnen. Ebensowenig bekommt die zugehörige Volumenform einen Index L . Wir folgen Neukirch und nennen das von $\prod_{\tau} \mathbb{C}$ induzierte Skalarprodukt das **kanonische Skalarprodukt**.

Leider sind die beiden Skalarprodukte nicht gleich, so daß es zu Skalierungen in den zugehörigen Volumenformen kommt.

Proposition 6.15. *Seien $x = (x_\tau)_\tau, y = (y_\tau) \in \left(\prod_{\tau} \mathbb{C} \right)^+$. Dann gilt:*

(1) $\langle x, y \rangle_L = \sum_{\tau} \lambda_{\tau}^{-1} \cdot x_{\tau} \bar{y}_{\tau}$ mit

$$\lambda_{\tau} = \begin{cases} 1 & \tau \text{ reell,} \\ 2 & \tau \text{ komplex.} \end{cases}$$

(2) $\langle x, y \rangle = \sum_{\rho} x_{\rho} y_{\rho} + 2 \sum_{\sigma} (\Re(x_{\sigma}) \Re(y_{\sigma}) + \Im(x_{\sigma}) \Im(y_{\sigma}))$.

(3) Für ein vollständiges Gitter im Minkowski-Raum von F gilt

$$\text{vol}(\Gamma) = 2^s \text{vol}_L(\Gamma).$$

Beweis. (1) und (2) sind nur Ausdruck der folgenden Rechnung auf den komplexen Faktoren. Wir betrachten $z = a + ib, w = u + iv \in \mathbb{C}$. Dann gilt

$$\langle z, w \rangle = z\bar{w} + \bar{z}w = 2\Re(z\bar{w}) = 2(au + bv) = 2\langle z, w \rangle_L.$$

Das Skalieren des Volumens in (3) folgt sofort. Die Gramsche Matrix bezüglich Standardskalarprodukt muß in $2s$ Spalten mit 2 skaliert werden, und zwar denen zu den reellen Koordinaten der komplexen Stellen, um die Gramsche Matrix bezüglich des kanonischen Skalarproduktes zu erhalten. Da das Volumen mit der Wurzel der Determinante dieser Matrix geht, folgt (3). \square

7. ENDLICHKEITSSÄTZE — ADDITIVE THEORIE

7.1. Die Norm eines gebrochenen Ideals. Sei F ein Zahlkörper. Die Norm eines Ideals $\mathfrak{a} \subseteq \mathfrak{o}_F$ ist definiert als

$$N(\mathfrak{a}) = (\mathfrak{o}_F : \mathfrak{a}) = \#\mathfrak{o}_F/\mathfrak{a}.$$

Aufgrund des Chinesischen Restsatzes gilt für teilerfremde Ideale $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{o}_F$

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Sei $\mathfrak{p} \subseteq \mathfrak{o}_F$ ein maximales Primideal und $n \in \mathbb{N}_0$. Wir betrachten die Filtrierung durch Primidealepotenzen

$$\mathfrak{o}_F \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \dots \supseteq \mathfrak{p}^n.$$

Nach Lokalisieren bei \mathfrak{p} gilt mit einer Uniformisierenden $\pi \in \mathfrak{o}_{F,\mathfrak{p}}$

$$\mathfrak{p}^r/\mathfrak{p}^{r+1} \simeq (\mathfrak{p}^r/\mathfrak{p}^{r+1})_{\mathfrak{p}} = (\pi^r)/(\pi^{r+1}) \simeq \mathfrak{o}_{F,\mathfrak{p}}/(\pi) \simeq \mathfrak{o}_F/\mathfrak{p}.$$

Also gilt für alle r :

$$(\mathfrak{p}^r : \mathfrak{p}^{r+1}) = \#\mathfrak{p}^r/\mathfrak{p}^{r+1} = \#\mathfrak{o}_F/\mathfrak{p} = N(\mathfrak{p})$$

und somit

$$N(\mathfrak{p}^n) = (\mathfrak{o}_F : \mathfrak{p}^n) = \prod_{r=0}^{n-1} (\mathfrak{p}^r : \mathfrak{p}^{r+1}) = N(\mathfrak{p})^n.$$

Insbesondere gilt daher für $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$

$$N(\mathfrak{a}) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{n_{\mathfrak{p}}}.$$

Die Norm setzt sich aufgrund der eindeutigen Primidealzerlegung eindeutig zu einem Gruppenhomomorphismus fort.

Definition 7.1. Sei F ein Zahlkörper. Wir setzen

$$I_F = I_{\mathfrak{o}_F}.$$

Die Norm eines gebrochenen Ideals ist der Wert des Normhomomorphismus

$$N : I_F \rightarrow \mathbb{Q}^{\times},$$

der durch $N(\mathfrak{p}) = \#\mathfrak{o}_F/\mathfrak{p}$ auf Primidealen gegeben ist.

Proposition 7.2. *Es gilt für $x \in F^{\times}$*

$$N((x)) = |N_{F/\mathbb{Q}}(x)|.$$

Beweis. Beide Seiten sind multiplikativ, also nehmen wir ohne Einschränkung $x \in \mathfrak{o}_F$ an. Aus dem Elementarteilersatz folgt

$$(\mathfrak{o}_F : x\mathfrak{o}_F) = |\det(x \cdot : F \rightarrow F)|$$

mit der Determinante von $x \cdot$ als Endomorphismus des \mathbb{Q} -Vektorraums F . Die Determinante ändert sich nicht bei Skalarerweiterung:

$$\det(x \cdot : F \rightarrow F) = \det(x \cdot : F_{\mathbb{C}} \rightarrow F_{\mathbb{C}}).$$

Über \mathbb{C} kann $x \cdot$ mittels $j_{\mathbb{C}}$ in Diagonalform gebracht werden als:

$$j(x) \cdot = (\tau(x))_{\tau} \cdot : \prod_{\tau} \mathbb{C} \rightarrow \prod_{\tau} \mathbb{C},$$

und somit ist die Determinante gerade

$$\det(x \cdot : F_{\mathbb{C}} \rightarrow F_{\mathbb{C}}) = \prod_{\tau} \tau(x) = N_{F/\mathbb{Q}}(x). \quad \square$$

Lemma 7.3. *Es gilt für ein gebrochenes Ideal I von F :*

$$\text{vol}(I) = N(I) \text{vol}(\mathfrak{o}_F) = N(I) \sqrt{|\Delta_F|}.$$

Beweis. Die Formel gilt für Ideale. Ferner, wenn $I \subseteq J$ eine Inklusion gebrochener Ideale ist, dann gibt es ein Ideal $\mathfrak{a} \subseteq \mathfrak{o}_F$ mit

$$I = \mathfrak{a}J$$

und damit (teste nach Lokalisieren)

$$J/I \simeq \mathfrak{o}_F/\mathfrak{a}.$$

Somit gilt

$$\frac{N(I)}{N(J)} = N(\mathfrak{a}) = (\mathfrak{o}_F : \mathfrak{a}) = (J : I) = \frac{\text{vol}(I)}{\text{vol}(J)},$$

weil eine Grundmasche zu J genau $(J : I)$ -mal in der Grundmasche zu I aufgeht, eben durch Translation mit einem geeigneten Vertretersystem von $(J : I)$.

Damit gilt das Lemma für I genau dann, wenn es für J gilt. □

Satz 7.4. *Sei F ein Zahlkörper und $c > 0$ eine reelle Zahl. Dann gibt es nur endlich viele Ideale $\mathfrak{a} \subseteq \mathfrak{o}_F$ mit*

$$N(\mathfrak{a}) \leq c.$$

Beweis. Für jedes maximale Primideal \mathfrak{p} gibt es eine Primzahl $p \in \mathbb{Z}$ mit $(p) = \mathfrak{p} \cap \mathbb{Z}$. Dann ist $\kappa(\mathfrak{p}) = \mathfrak{o}_F/\mathfrak{p}$ ein \mathbb{F}_p -Vektorraum und

$$N(\mathfrak{p}) = p^{[\kappa(\mathfrak{p}):\mathbb{F}_p]} \geq p.$$

Aufgrund der eindeutigen Primidealzerlegung reicht daher die Endlichkeit von

$$\{\mathfrak{p} \in \text{Spec}(\mathfrak{o}_F) ; \mathfrak{p} \cap \mathbb{Z} = (p)\}$$

für jede Primzahl p . Aber das ist gerade die Menge der Primidealteiler von $p\mathfrak{o}_F$, also endlich. □

7.2. Anwendung des Minkowskischen Gitterpunktsatzes.

Satz 7.5. *Seien F ein Zahlkörper und $I \in I_F$ ein gebrochenes Ideal. Seien $c_\tau \in \mathbb{R}_{>0}$ gegeben mit $c_\tau = c_{\bar{\tau}}$ für alle $\tau : F \rightarrow \mathbb{C}$ und*

$$\prod_{\tau} c_{\tau} > \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|\Delta_F|} \cdot N(I).$$

Dann gibt es $0 \neq x \in I$ mit für alle τ gilt:

$$|\tau(x)| < c_{\tau}.$$

Beweis. Wir betrachten die Menge

$$X_c = \{x = (x_{\tau})_{\tau} \in \left(\prod_{\tau} \mathbb{C}\right)^+ ; |x_{\tau}| < c_{\tau}\}.$$

Diese Menge ist offensichtlich zentralsymmetrisch, konvex und meßbar.

Comment: Bild der Menge X_c ; nicht Ball in sup-norm, obwohl das erstmal so aussieht.

Das Volumen ist

$$\begin{aligned} \text{vol}(X_c) &= 2^s \text{vol}_L(X_c) = 2^s \prod_{\rho} 2c_{\rho} \cdot \prod_{\sigma} \pi c_{\sigma}^2 = 2^r (2\pi)^s \prod_{\tau} c_{\tau} \\ &> 2^r (2\pi)^s \cdot \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|\Delta_F|} \cdot N(I) = 2^n \text{vol}(I). \end{aligned}$$

Die Existenz von $0 \neq x \in I \cap X_c$ folgt nun aus dem Minkowskischen Gitterpunktsatz, Satz 5.12. □

Theorem 7.6 (Endlichkeit der Klassenzahl). *Die Klassengruppe $\text{Cl}(F)$ eines Zahlkörpers F ist eine endliche abelsche Gruppe.*

Beweis. Nach Satz 7.4 reicht es zu zeigen, daß es eine uniforme obere Schranke C gibt, so daß jedes gebrochene Ideal $I \in I_F$ ein Ideal \mathfrak{a} als Vertreter seiner Klasse in $\text{Cl}(F)$ mit

$$N(\mathfrak{a}) \leq C.$$

Wir fixieren $\varepsilon > 0$. Sei $I \in I_F$ beliebig. Wir wenden Satz 7.5 auf I^{-1} und beliebige c_{τ} mit

$$\prod_{\tau} c_{\tau} = (1 + \varepsilon) \cdot \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|\Delta_F|} \cdot N(I^{-1}) =: C \cdot N(I^{-1})$$

an. Wir finden $x \in I^{-1}$ mit

$$|N_{F|\mathbb{Q}}(x)| = \left| \prod_{\tau} \tau(x) \right| < \prod_{\tau} c_{\tau}.$$

Es ist $\mathfrak{a} = xI \subseteq I^{-1}I = \mathfrak{o}_F$ ein Ideal und

$$N(\mathfrak{a}) = \frac{N((x))}{N(I^{-1})} = \frac{|N_{F/\mathbb{Q}}(x)|}{N(I^{-1})} < \frac{\prod_{\tau} c_{\tau}}{N(I^{-1})} = (1 + \varepsilon) \cdot \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|\Delta_F|} = C. \quad \square$$

JAKOB STIX, INSTITUT FÜR MATHEMATIK, GOETHE-UNIVERSITÄT FRANKFURT, ROBERT-MAYER-STR. 6-8,
60325 FRANKFURT AM MAIN, GERMANY

E-mail address: `stix@math.uni-frankfurt.de`