Algebraische Zahlentheorie

Anton Deitmar

Inhaltsverzeichnis

1 Erinnerungen an die Algebra

1.1 Ringe

Definition 1.1.1. Ein **Ring** ist eine abelsche Gruppe $(R, +)$ zusammen mit einer bilinearen assoiativen Abbildung $R \times R \to R$, $(a, b) \mapsto ab$.

Definition 1.1.2. Ein **Ring mit Eins** ist ein Paar $(R, \mathbf{1})$ bestehend aus einem Ring R und einem Element $\mathbf{1} \in \mathbb{R}$ mit der Eigenschaft $a\mathbf{1} = \mathbf{1}a = a$ fuer jedes $a \in R$. Die Eins $\mathbf{1}$ wird in der Regel als 1 geschrieben.

Definition 1.1.3. Eine **Einheit** in einem Ring R mit Eins ist ein Element a, fuer das es ein $b \in R$ gibt, so dass $ab = \mathbf{1}$. Die Einheiten bilden eine multiplikative Gruppe, die als $R^\times$ geschrieben wird.

Definition 1.1.4. Ein **kommutativer Ring** ist ein Ring R, in dem $ab = ba$ gilt fuer alle $a, b \in R$.

> **Vereinbarung:** In diesem Skript soll das Wort "Ring" ab jetzt fuer "kommutativer Ring mit Eins" stehen.

Definition 1.1.5. Seien R, S Ringe. Ein **Ringhomomorphismus** ist eine Abbildung $\phi : R \to S$ so dass

- ϕ ist ein Gruppenhomomorphismus $(R, +) \to (S, +)$,
- $\phi(1) = 1$,
- $\phi(ab) = \phi(a)\phi(b)$.

Lemma 1.1.6 (Polynomdivision ueber beliebigen Ringen)**.** *Sei R ein Ring und sei $f \in R[x]$ ein normiertes Polynom. Ist dann g ein weiteres Polynom, dann existieren eindeutig bestimmte Polynome q, r mit* $\operatorname{grad}(r) < \operatorname{grad}(f)$*, so dass*

$$g = fq + r.$$

Definition 1.1.7. Ein Integritätsring R heißt **faktoriell**, falls jede Nichteinheit in $R \setminus \{0\}$ als Produkt von Primelementen darstellen lässt, das heißt wenn wir eine

sogenannte **Primfaktorzerlegung** haben. Die Faktoren sind dann bis auf Reihenfolge und Assoziiertheit eindeutig bestimmt. In einem faktoriellen Ring gilt

$$p \text{ irreduzibel} \quad \Leftrightarrow \quad p \text{ Primelement.}$$

Jeder Hauptidealring ist faktoriell. Insbesondere ist $\mathbb{Z}$ faktoriell und für jeden Körper K ist der Polynomring $K[x]$ faktoriell.

Proposition 1.1.8.

(a) *Sei R ein faktorieller Ring und K sein Quotientenkoerper. Seien f, g normierte Polynome in $K[x]$ so dass fg in $R[x]$ liegt. Dann liegen f und g beide in $R[x]$.*

(b) *(Gauß) Ist R ein faktorieller Ring, dann ist auch der Polynomring $R[x]$ faktoriell.*

* * *

1.2 Ideale

Definition 1.2.1. Ein **Ideal** in einem Ring R ist eine additive Untergruppe $\mathfrak{a}$ mit $ax \in \mathfrak{a}$, fuer jedes $a \in R$ und jedes $x \in \mathfrak{a}$. Die Quotientengruppe $R/\mathfrak{a}$ erbt dann eine Ringstruktur, so dass die Projektion $R \to R/\mathfrak{a}$ ein Ringhomomorphismus ist.

Ist $\alpha \in R$, dann ist $\alpha R = \{\alpha r : r \in R\}$ ein Ideal, ein sogenanntes **Hauptideal**.

Definition 1.2.2. Ein **Nullteiler** ist ein Element $a \in R \setminus \{0\}$, so dass es ein $b \neq 0$ in R gibt, so dass $ab = 0$. Der Ring R heisst **nullteilerfrei** oder **integer** oder auch **Integritaetsring**, falls es keinen Nullteiler in R gibt.

Definition 1.2.3. Ein **Hauptidealring** ist ein integrer Ring R, in dem jedes Ideal ein Hauptideal ist.

Definition 1.2.4. Ein Integritätsring R heißt **euklidischer Ring**, falls es eine Abbildung $\delta : R \setminus 0 \to \mathbb{N}_0$ gibt, so dass zu je zwei $a, b \in R \setminus \{0\}$ zwei Elemente $q, r \in R$ existieren mit

$$a = bq + r$$

und $r = 0$ oder $\delta(r) < \delta(b)$. Man nennt δ die **Gradabbildung** des euklidischen Rings.

Jeder euklidische Ring ist ein Hauptidealring.

Es gilt

$$R \text{ euklidisch } \Rightarrow R \text{ Hauptidealring } \Rightarrow R \text{ faktoriell.}$$

Definition 1.2.5. Sei R ein Hauptidealring und seien $a, b \in R$. Ein **größter gemeinsamer Teiler** $\mathrm{ggT}(a,b)$ ist ein Erzeuger des Ideals $aR + bR$. Ein ggT ist bis auf Multiplikation mit einer Einheit eindeutig festgelegt.

Definition 1.2.6. Ein Ideal $\mathfrak{p} \neq R$ eines Rings R heisst **Primideal**, wenn für $x, y \in R$ gilt

$$xy \in \mathfrak{p} \quad \Rightarrow \quad x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}.$$

Ein Ideal $\mathfrak{a} \subset R$ ist genau dann ein Primideal, wenn $R/\mathfrak{a}$ integer ist. Ein Ideal $\mathfrak{a}$ heisst **maximales Ideal**, wenn es maximal in der Menge aller Ideale $\neq R$ ist. Jedes Ideal ist in einem maximalen Ideal enthalten und ein Ideal $\mathfrak{a}$ ist genau dann maximal, wenn $R/\mathfrak{a}$ ein Koerper ist. Daher ist jedes maximale Ideal prim.

Beispiel 1.2.7. Ein Beispiel fuer ein Primideal, das nicht maximal ist, ist $\mathfrak{p} = xK[x,y]$ im Ring $R = K[x,y]$, wobei K ein Koerper ist.

Definition 1.2.8. Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ in einem Ring heißen **teilerfremd**, falls $\mathfrak{a} + \mathfrak{b} = R$ gilt.

Definition 1.2.9. Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale, so definieren wir das Ideal $\mathfrak{a}\mathfrak{b}$ als

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{j=1}^{n} a_j b_j : a_j \in \mathfrak{a},\ b_j \in \mathfrak{b} \right\}.$$

Sind etwa beides Hauptideale, $\mathfrak{a} = aR$ und $\mathfrak{b} = bR$, dann ist auch $\mathfrak{a}\mathfrak{b}$ ein Hauptideal, nämlich $\mathfrak{a}\mathfrak{b} = abR$.

Definition 1.2.10. Ein Ring R heisst **noethersch**, falls jedes Ideal endlich-erzeugt ist. Das bedeutet, dass es zu jedem Ideal $\mathfrak{a}$ Elemente $a_1, \ldots, a_n \in R$ gibt, so dass

$$\mathfrak{a} = Ra_1 + \cdots + Ra_n.$$

* * *

1.3 Teilbarkeit

Definition 1.3.1. Seien a, b Elemente eines Integritätsrings R.

(a) Man sagt a **teilt** b oder ist ein **Teiler** von b, falls es ein $c \in R$ gibt so dass $ac = b$. In diesem Fall schreibt man $a \mid b$. Ist a kein Teiler von b, so schreibt man $a \nmid b$.

(b) a und b heißen **assoziiert**, wenn es eine Einheit $u \in R^\times$ gibt mit $a = bu$.

Definition 1.3.2. Sei R ein Integritätsring und p ein Element, das weder Null noch eine Einheit ist.

(a) Das Element p heißt **irreduzibel**, falls aus der Gleichung $p = ab$ in R stets folgt, dass a oder b eine Einheit ist.

(b) Das Element p heißt **Primelement**, falls aus $p \mid ab$ stets folgt $p \mid a$ oder $p \mid b$.

* * *

1.4 Moduln

Definition 1.4.1. Ein **Modul** über dem Ring R ist eine abelsche Gruppe $(M, +)$, deren neutrales Element als 0 geschrieben wird, zusammen mit einer Abbildung

$$\begin{aligned} R \times M &\to M \\ (a, m) &\mapsto am, \end{aligned}$$

dergestalt, dass folgende Axiome erfüllt sind:

$$1m = m \qquad\qquad (ab)m = a(bm)$$
$$a(m+n) = am + an \qquad\qquad (a+b)m = am + bm.$$

Definition 1.4.2. Ein **Untermodul** ist eine additive Untergruppe $N \subset M$, so dass $aN \subset N$ für jedes $a \in R$ gilt.

Definition 1.4.3. Ein **Modulhomomorphismus** ist eine Abbildung $\phi : M \to M$ zwischen R-Modulen, so dass

$$\phi(m+n) = \phi(m) + \phi(n), \qquad\qquad \phi(am) = a\phi(m).$$

Statt Modulhomomorphismus sagt man auch R**-lineare Abbildung**.

Satz 1.4.4 (Elementarteilersatz für Moduln)**.** *Sei R ein Hauptidealring und F ein endlich-freier Modul, sowie $M \subset F$ ein Untermodul. Dann existieren Elemente $x_1, \ldots, x_k$ von F, die Teil einer Basis sind, sowie Koeffizienten $a_1, \ldots, a_k \in R$ mit*

- $a_i \mid a_{i+1}$ *falls* $1 \leq i \leq k-1$ *und*
- $a_1 x_1, \ldots, a_k x_k$ *ist eine Basis von M.*

Die a_j sind bis auf Assoziiertheit durch M eindeutig bestimmt, sie werden die **Elementarteiler** *von M genannt.*

Insbesondere folgt: Ein Untermodul M eines endlich-freien Moduls F ist endlich-frei und es gilt $\mathrm{Rang}(M) \leq \mathrm{Rang}(F)$.

* * *

2 Ganzzahlringe

2.1 Ganzheit

Ringe sind hier immer kommutativ mit Eins.

Erinnerung: Ein Polynom $f(x) = a_0 + a_1x + \cdots + a_nx^n$ heisst **normiert**, wenn der Leitkoeffizient gleich Eins ist, wenn also $a_n = 1$ gilt.

Definition 2.1.1. Sei $A \subset B$ eine Ringerweiterung. Ein Element $b \in B$ heisst **ganz ueber** A, wenn es ein normiertes Polynom $f(x) \in A[x]$ gibt, so dass $f(b) = 0$ gilt. Die Ringerweiterung B/A heisst **ganz**, falls jedes $b \in B$ ganz ueber A ist.

Beispiele 2.1.2.

(a) Die Erweiterung $\mathbb{Z}[i]/\mathbb{Z}$ ist ganz, denn ein gegebenes $\alpha = a + bi \in \mathbb{Z}[i]$ ist Nullstelle des Polynoms

$$f(x) = x^2 - 2ax + (a^2 + b^2).$$

(b) Die Erweiterung $\mathbb{Q}/\mathbb{Z}$ ist nicht ganz, denn waere etwa $\alpha = \frac{1}{2}$ ganz ueber $\mathbb{Z}$, also etwa Nullstelle des Polynoms

$$p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$$

mit $a_j \in \mathbb{Z}$, dann liefert Multiplikation mit 2^n, dass

$$0 = 2^n a_0 + 2^{n-1}a_1 + \cdots + 1a_{n-1} + 1,$$

woraus folgen wuerde, dass 1 eine gerade Zahl ist.

Satz 2.1.3. *Sei B/A eine Ringerweiterung. Fuer $b_1, \ldots, b_n \in B$ sind aequivalent:*

(a) *$b_1, \ldots, b_n$ sind alle ganz ueber A,*

(b) *der Ring $A[b_1, \ldots, b_n]$ ist als A-Modul endlich erzeugt.*

Beweis. (a)⇒(b): mit Induktion nach n. Fuer $n = 1$ sei $b \in B$ ganz ueber A. Wir zeigen, dass $A[b]$ als A-Modul endlich erzeugt ist. Sei hierzu f ein normiertes Polynom in

$A[x]$ mit $f(b) = 0$. Sei d der Grad von f und sei $g \in A[x]$ ein weiteres Polynom. Da f normiert ist, existieren Polynome q, r mit $\operatorname{grad}(r) < \operatorname{grad} f$ und $g = fq + r$. Schreibe $r(x) = a_0 + \cdots + a_{d-1}x^{d-1}$. Es folgt $g(b) = r(b) = a_0 + a_1 b + \cdots + a_{d-1}b^{d-1}$ und daher wird $A[b]$ als A-Modul von $1, b, \ldots, b^{n-1}$ erzeugt.

Nun der Induktionsschritt $n \to n+1$: Sind $b_1, \ldots, b_{n+1}$ ganz ueber A, dann ist nach Induktionsschritt $R = A[b_1, \ldots, b_n]$ als A-Modul endlich erzeugt. Ferner ist $A[b_1, \ldots, b_{n+1}] = R[b_{n+1}]$ als R-Modul endlich erzeugt. Zusammen folgt, dass $A[b_1, \ldots, b_{n+1}]$ als A-Modul endlich erzeugt ist.

(a)⇐(b): Sei $R = A[b_1, \ldots, b_n]$ als A-Modul erzeugt von $w_1, \ldots, w_r$. Fuer $b \in A[b_1, \ldots, b_n]$ ist dann

$$bw_i = \sum_{j=1}^{r} a_{i,j} w_j$$

fuer geeignete $a_{i,j} \in A$. Die Matrix $M = bI - (a_{i,j}) \in \mathrm{M}_r(R)$ annulliert also den Vektor $(w_1, \ldots, w_r)^t$. Nach dem Laplace-Entwicklungssatz gibt es eine Matrix $M^{\#}$ so dass $M^{\#}M = \det(bI - (a_{i,j}))\boldsymbol{a}$. Das bedeutet, dass $\det(bI - (a_{i,j}))w_j = 0$ fuer alle $w_1, \ldots, w_r$. Es gibt aber Koeffizienten $\lambda_1, \ldots, \lambda_r \in A$ mit $1 = \lambda_1 w_1 + \cdots + \lambda_r w_r$, so dass $\det(bI - (a_{i,j})) = 0$ folgt. Das normierte Polynom $\det(xI - (a_{i,j}))$ annulliert also b, welches demnach ganz ueber A ist. □

Korollar 2.1.4. *Sind $b_1, \ldots, b_n$ ganz ueber A, dann ist jedes Element von $A[b_1, \ldots, b_n]$ ganz ueber A. Die ganzen Elemente bilden also einen Ring.*

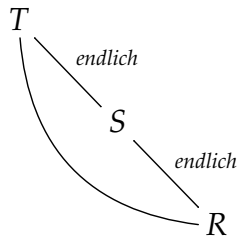
Beweis. Sei $b \in A[b_1, \ldots, b_n]$, dann ist $A[b_1, \ldots, b_n, b] = A[b_1, \ldots, b_n]$ endlich erzeugt ueber A und damit ist b ganz ueber A. □

Definition 2.1.5. Eine Ringerweiterung S/R heisst **endliche Ringerweiterung**, falls B als A-Modul endlich-erzeugt ist, wenn es also $b_1, \ldots, b_n \in B$ gibt, so dass

$$B = Ab_1 + \cdots + Ab_n.$$

Satz 2.1.6.

(a) *Sind $T/S/R$ endliche Ringerweiterungen, dann ist T/R ebenfalls endlich.*



(b) *Sind $C/B/A$ ganze Ringerweiterungen, dann ist auch C/A ganz.*

Beweis. (a) Nach Voraussetzung gibt es $v_1, \dots, v_n \in T$ und $w_1, \dots, w_m \in S$, so dass

$$T = Sv_1 + \cdots + Sv_n,$$
$$S = Rw_1 + \cdots + Rw_m.$$

Einsetzen liefert

$$\begin{aligned} T &= \big(Rw_1 + \cdots + Rw_m\big)v_1 + \cdots + \big(Rw_1 + \cdots + Rw_m\big)v_n \\ &= R(w_1v_2) + R(w_2v_1) + \cdots + R(w_mv_n). \end{aligned}$$

Also ist T als R-Modul endlich-erzeugt.

(b) Sei $c \in C$. Dann gibt es $b_0, \dots, b_{n-1} \in B$ mit $0 = b_0 + b_1c + \cdots + b_{n-1}c^{n-1} + c^n$. Sei dann $R = A[b_0, \dots, b_{n-1}]$. Dann ist $R[c]$ ein endlich-erzeugter R-Modul. Ferner ist R ein endlich-erzeugter A-Modul, nach Teil (a) ist $R[c]$ ein endlich-erzeugter A-Modul, damit ist c ganz ueber A. □

Beispiel 2.1.7. Sei $A = \mathbb{Z}$ und $B = \mathbb{Q}$. Sei $b = \frac{p}{q} \in \mathbb{Q}$ ganz ueber $\mathbb{Z}$, dann ist $\mathbb{Z}[b]$ endlich erzeugter $\mathbb{Z}$-Modul, dann folgt $q = 1$ also sind die $\mathbb{Z}$-ganzen Elemente in $\mathbb{Q}$ genau die Elemente von $\mathbb{Z}$ selbst.

Definition 2.1.8. Sei B/A eine Ringerweiterung. Die Menge

$$\overline{A} = \{b \in B : b \text{ ganz ueber } A\}$$

ist ein Ring mit $A \subset \overline{A} \subset B$, genannt der **ganze Abschluss** von A in B. Es gilt $\overline{\overline{A}} = \overline{A}$ und A heisst **ganzabgeschlossen** in B, wenn $\overline{A} = A$.

Proposition 2.1.9. *Sei A integer und K der Quotientenkoeper. Sei L/K eine algebraische Koerpererweiterung und sei $B \subset L$ der ganze Abschluss von A in L.*

(a) *Zu jedem $\alpha \in L$ gibt es ein $c \in A$, so dass $c\alpha \in B$. Insbesondere also $L = KB$.*

(b) *Ist $V \neq 0$ ein B-Untermodul von L, dann gilt auch $KV = L$.*

Beweis. (a) Sei $\alpha \in L$ und sei

$$m(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

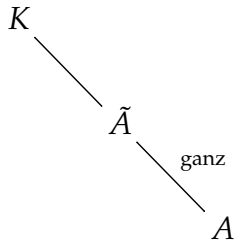
das Minimalpolynom. Fuer gegebenes $c \in K$ betrachte das Polynom

$$\begin{aligned} f(x) &= c^n m\left(\frac{x}{c}\right) \\ &= c^n \left(a_0 + \frac{a_1}{c}x + \cdots + \frac{a_{n-1}}{c^{n-1}}x^{n-1} + \frac{x^n}{c^n}\right) \\ &= c^n a_0 + c^{n-1}a_1\, x + \cdots + c a_{n-1}\, x^{n-1} + x^n. \end{aligned}$$

Dann folgt $f(c\alpha) = c^n m(\alpha) = 0$. Indem man c als das Produkt der Nenner der a_j waehlt, kann man $f \in A[x]$ erreichen, sowie $c \in A$ und $c\alpha \in B$.

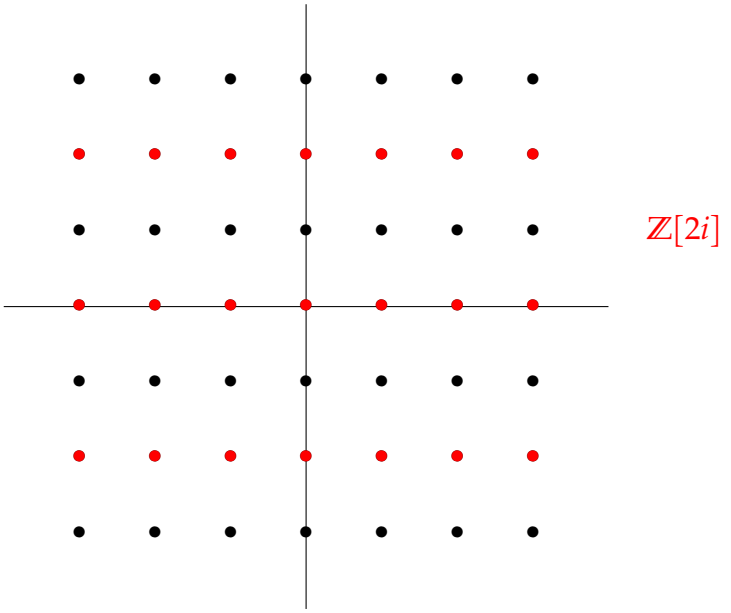
(b) Sei $0 \neq v \in V$, dann gilt $KV \supset KBv = Lv = L$. □

Definition 2.1.10. Ist A integer und $K = \mathrm{Quot}(A)$ der Quotientenkoerper und sei $\tilde{A}$ der ganze Abschluss von A in K. Gilt $A = \tilde{A}$, so heisst A **ganzabgeschlossen** (ohne einen Oberring anzugeben).



Beispiel 2.1.11. (a) Der Ring $\mathbb{Z}[2i]$ ist ein Unterring von $\mathbb{Z}[i]$, der denselben Quotientenkoerper $\mathbb{Q}(i)$ hat.

(b) $\mathbb{Z}[i]$ ist ganzabgeschlossen, $\mathbb{Z}[2i]$ aber nicht, der Ganzabschluss von $\mathbb{Z}[2i]$ ist gleich $\mathbb{Z}[i]$.



Beweis. (a) Der Quotientenkoerper K von $\mathbb{Z}[2i]$ enthaelt $2i$ und damit i. Er wird von $2i$ erzeugt, hat also Grad 2 ueber $\mathbb{Q}$, damit muss er $\mathbb{Q}(i)$ sein.

(b) Der Ring $\mathbb{Z}[i]$ ist eulidisch, also ein Hauptidealring, also faktoriell. In der naechsten Proposition zeigen wir, dass faktorielle Ringe ganzabgeschlossen sind.

Fuer die zweite Aussge muessen wir zeigen, dass jedes $\alpha \in \mathbb{Z}[i]$ eine normierte Gleichung ueber $\mathbb{Z}[2i]$ erfuellt. Ist α nicht in $\mathbb{Z}[2i]$, also etwa $\alpha = a + bi$ mit $a, b \in \mathbb{Z}$ und b ungerade, dann liegt $r = a + (b-1)i$ in $\mathbb{Z}[2i]$ und es gilt $\alpha - r = i$, also

$$-1 = (\alpha - r)^2 = \alpha^2 - 2\alpha r + r^2.$$

Damit wird α von dem Polynom $f(x) = x^2 - 2rx + r^2 + 1 \in \mathbb{Z}[2i]$ annulliert. □

Erinnerung. Ist R integer, dann ist jedes Primelement auch irreduzibel. In einem faktoriellen Ring gilt auch die Umkehrung.

Proposition 2.1.12. *Ist der Ring A faktoriell, dann ist A ganzabgeschlossen. Also sind insbesondere Hauptidealringe ganzabgeschlossen.*

Beweis. Sei $\frac{a}{b}$ im Quotientenkoerper ganz ueber A, also etwa

$$a_0 + a_1\frac{a}{b} + \cdots + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \frac{a^n}{b^n} = 0.$$

Wir koennen a und b als teilerfremd annehmen, es gibt also kein Primelement p, das

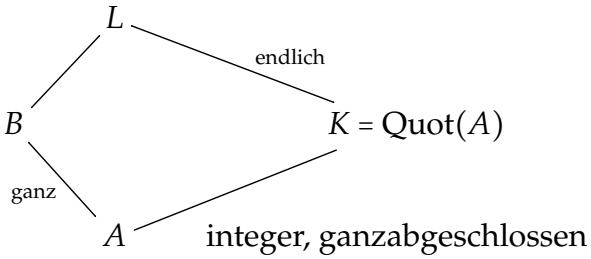
beide teilt. Wir haben

$$a_0 b^n + a_1 b^{n-1} a + \cdots + a^n = 0.$$

Sei p ein Primelement, das b teilt. Dann folgt hieraus, dass p auch a^n teilt, also auch a, was nicht sein kann, also gibt es solch ein Primelement nicht, damit ist b eine Einheit, also $\frac{a}{b}$ in A □

Ab jetzt sei

- A integer, ganzabgeschlossen,
- $K = \mathrm{Quot}(A)$,
- L/K eine endliche Koerpererweiterung,
- B der ganze Abschluss von A in L.



Es folgt dann, dass auch B ganzabgeschlossen ist. Da L/K endlich ist, ist L auch der Quotientenkoerper von B, ja es gilt sogar $L = S^{-1}B$, wobei $S = A \setminus \{0\}$. Das bedeutet, jedes $\beta \in L$ ist von der Form $\beta = \frac{b}{a}$, mit $0 \neq a \in A$ und $b \in B$. DENN: gilt

$$a_n \beta^n + \cdots + a_0 = 0,$$

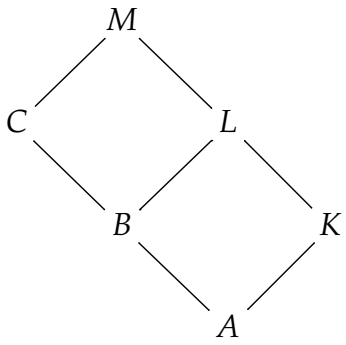
dann multipliziere diese Gleichung mit a_n^{n-1} um zu sehen, dass $b = a_n \beta$ ganz ueber A ist, also in B liegt.

Lemma 2.1.13. *$\beta \in L$ ist genau dann ganz ueber A, wenn sein Minimalpolynom m_β in $A[x]$ liegt.*

Beweis. Ist m_β in $A[x]$, dann ist β ganz. Sei also umgekehrt β ganz und $f \in A[x]$ normiert mit $f(\beta) = 0$. Das Mipo m_β teilt f in $K[x]$, also sind alle Nullstellen $\beta_1, \ldots, \beta_r$ von m_β ganz, also sind alle Koeffizienten von $m_\beta(x) = \prod_{j=1}^{r}(x - \beta_j)$ in K und ganz ueber A, liegen also in A. □

Lemma 2.1.14. *Sei A ein ganzabgeschlossener Integritaetsring mit Quotientenkoerper K. Seien $M/L/K$ endliche Koerpererweiterungen und $C \subset M$, $B \subset L$ die ganzen Abschluesse von A. Dann ist C auch der Ganzabschluss von B in M.*

Insbesondere, im Fall $B = C$ folgt, dass B ganzabgeschlossen ist.



Proof. Sei C' der Ganzabschluss von B in M. Nach Satz 2.1.6 ist die Erweiterung C'/A ganz, also folgt $C' \subset C$. Fuer die Rueckrichtung sei $\alpha \in C$, dann ist $A[\alpha]$ als A-Modul endlich-erzeugt. Dann ist aber auch $B[\alpha] = B(A[\alpha])$ als B-Modul endlich-erzeugt, also ist α ganz ueber B. □

* * *

2.2 Norm und Spur

Sei $\alpha \in L$ und sei $M_\alpha : L \to L$ die Multiplikation mit α, also $M_\alpha(x) = \alpha x$. Dann ist M_α eine lineare Abbildung auf dem K-Vektorraum L. Sei

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}(M_\alpha)$$

die **Spur** von α und sei

$$\mathrm{N}_{L/K}(\alpha) = \det(M_\alpha)$$

die **Norm** von α. Dann folgt

$$\mathrm{Tr}_{L/K}(x + y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$$

und

$$\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\,\mathrm{N}_{L/K}(y).$$

Satz 2.2.1. *Ist L/K separabel und E die Menge aller K-Einbettungen von L in einen algebraischen Abschluss $\overline{K}$ von K, so gilt*

(a) *das charakteristische Polynom $\chi_\alpha(x) = \det(x - M_\alpha)$ ist gleich*

$$\chi_\alpha(x) = \prod_{\sigma \in E} (x - \sigma(\alpha)),$$

(b)

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in E} \sigma(\alpha),$$

(c)

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in E} \sigma(\alpha).$$

(d) *Ist α bereits in K, dann folgt*

$$\mathrm{Tr}_{L/K}(\alpha) = [L : K]\, \alpha, \qquad \mathrm{N}_{L/K}(\alpha) = \alpha^{[L:K]}.$$

Beweis. Teil (d) folgt sofort aus (b) und (c), da in dem Fall $\sigma(\alpha) = \alpha$ gilt.

Sei zunaechst $L = K(\alpha)$, dann hat m_α den Grad $d = [L : K] = |E|$. Das Polynom

$$\prod_{\sigma \in E} (x - \sigma(\alpha))$$

hat dieselben Nullstellen wie m_α und denselben Grad, ist also gleich m_α, also in $K[x]$. Das charakteristische Polynom χ_α erfuellt $\chi_\alpha(M_\alpha) = 0$, also gilt fuer $x \in L$,

$$0 = \chi_\alpha(M_\alpha)(x) = \chi_\alpha(\alpha)x,$$

so dass $\chi_\alpha(\alpha) = 0$ folgt. Da der Grad von χ_α ebenfalls gleich d ist, folgt $\chi_\alpha = m_\alpha$ und damit (a). Daraus folgen dann (b) und (c) durch Koeffizientenvergleich.

Fuer den allgemeinen Fall betrachte den Koerperturm $L/K(\alpha)/K$ Es gilt $\det_{L/K}(xI - M_\alpha) = \det_{K(\alpha)/K}(xI - M_\alpha)^{[L:K(\alpha)]}$, wie man sieht, indem man eine Basis $v_1, \ldots, v_r$ von $L/K(\alpha)$ waehlt, sowie eine Basis $w_1, \ldots, w_s$ von $K(\alpha)/K$ und benutzt, dass

$(v_i w_j)$ eine Basis von L/K ist. Auf

$$E = \mathrm{Hom}_K(L, \overline{K})$$

haben wir die Aequivalenzrelation

$$\sigma \sim \gamma \quad \Leftrightarrow \quad \sigma\alpha = \gamma\alpha.$$

Sei $\sigma_1, \ldots, \sigma_m$ ein Vertretersystem, (dann ist $m = s$, was aber hier nicht gebraucht wird). Es folgt

$$m_\alpha(x) = \prod_{j=1}^{m} (x - \sigma_j(\alpha))$$

und also

$$\prod_{\sigma \in E} (x - \sigma(\alpha)) = \Big(\prod_{j=1}^{m} \big(x - \sigma_j(\alpha)\big) \Big)^{[L:K(\alpha)]}. \qquad \square$$

Korollar 2.2.2. *Fuer endliche separable Koerpererweiterungen $M/L/K$ gilt*

$$\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K},$$
$$\mathrm{N}_{L/K} \circ \mathrm{N}_{M/L} = \mathrm{N}_{M/K}.$$

Beweis. Das Korollar gilt zwar allgemein, wird in dieser Vorlesung aber nur im separablen Fall gebraucht, wir nehmen also an, dass M/K separabel ist und fixieren einen algebraischen Abschluss $\overline{K}$ von K. Auf $\mathrm{Hom}(M, \overline{K})$ haben wir die Aequivalenzrelation

$$\sigma \sim \tau \quad \Leftrightarrow \quad \sigma|_L = \tau|_L.$$

Die Anzahl der Aequivalenzklassen ist $|\mathrm{Hom}(L, \overline{K})| = [L : K] = m$. Ist $\sigma_1, \ldots, \sigma_m$ ein Vertretersystem, dann besteht $\mathrm{Hom}(L, \overline{K})$ genau aus den Einschraenkungen der σ_j, also folgt

$$\begin{aligned} \mathrm{Tr}_{M/K}(\alpha) &= \sum_{j=1}^{m} \sum_{\sigma \sim \sigma_j} \sigma(\alpha) \\ &= \sum_{j=1}^{m} \mathrm{Tr}_{\sigma_j(M)/\sigma_j(L)}(\sigma_j(\alpha)) \\ &= \sum_{j=1}^{m} \sigma_j\big(\mathrm{Tr}_{M/L}(\alpha)\big). \end{aligned}$$

Fuer die Norm rechne ebenso. □

* * *

2.3 Die Diskriminante

Definition 2.3.1. Sei $v_1, \dots, v_n$ eine Basis der separablen Erweiterung L/K. Die **Diskriminante** dieser Basis sei

$$D(v_1, \dots, v_n) = \det\left((\sigma_i v_j)\right)^2,$$

wobei $E = \mathrm{Hom}(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$. Die Diskriminante haengt nicht von der Reihenfolge der σ_j ab, wohl aber von der Basis (v_j).

Beispiele 2.3.2. (a) Fuer $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$ und die Basis $1, i$ ist die Matrix $(\sigma_i v_j)$ gleich $\left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right)$, so dass

$$D(1, i) = -4.$$

(b) Seien $L = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$. Fuer die Basis $1, \sqrt{2}$ ist $(\sigma_i v_j)$ gleich $\left(\begin{smallmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{smallmatrix}\right)$ und daher

$$D(1, \sqrt{2}) = 8.$$

(c) Sei $L = \mathbb{Q}(\sqrt{5})$ und betrachte die Basis $1, \alpha = \frac{1+\sqrt{5}}{2}$. Die Matrix ist $\left(\begin{smallmatrix} 1 & \alpha \\ 1 & \alpha^c \end{smallmatrix}\right)$ mit $\alpha^c = \frac{1-\sqrt{5}}{2}$. Dann ist $\alpha - \alpha^c = -\sqrt{5}$ und daher

$$D(1, \alpha) = 5.$$

Satz 2.3.3. *Sei L/K separabel.*

(a) *Ist die Basis von der Gestalt $(1, \theta, \theta^2, \dots, \theta^{n-1})$ fuer ein $\theta \in L$, so gilt*

$$D(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2,$$

wobei $\theta_j = \sigma_j(\theta)$. Es gilt auch

$$D(1, \theta, \dots, \theta^{n-1}) = (-1)^{n(n-1)/2} N_{K(\theta)/K}(f'(\theta)),$$

wobei $f(x)$ das Minimalpolynom von θ ist und $f'(x)$ dessen Ableitung.

(b) *Es gilt*

$$D(v_1, \ldots, v_n) = \det\left(\mathrm{Tr}_{L/K}(v_i v_j)\right)$$

und damit liegt die Diskriminante in K.

(c) *Die Diskriminante $D(v_1, \ldots, v_n)$ ist stets $\neq 0$.*

(d) *$(x, y) = \mathrm{Tr}_{L/K}(xy)$ ist eine nicht ausgeartete Bilinearform auf dem K-Vektorraum L, genannt die* **Spurform**.

Beweis. (a) Erste Behauptung:

$$\det\begin{pmatrix} 1 & \theta_1 & \ldots & \theta_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \theta_n & \ldots & \theta_n^{n-1} \end{pmatrix} = \prod_{i<j} (\theta_j - \theta_i).$$

Wir beweisen die erste Behauptung duch Induktion nach n: Fuer $n = 1$ ist $D(1) = 1$ und das Produkt ist das leere Produkt, also 1.

$n \to n + 1$: Wir ersetzen θ_{n+1} durch eine Unbestimmte x und betrachten das Polynom

$$P(x) = \det\begin{pmatrix} 1 & \theta_1 & \ldots & \theta_1^{n} \\ \vdots & \vdots & & \vdots \\ 1 & \theta_n & \ldots & \theta_n^{n} \\ 1 & x & \ldots & x^n \end{pmatrix}$$

Es Grad n und $\theta_1, \theta_2, \ldots \theta_n$ als Nullstellen. Der Leitkoeffizient c ist nach Induktionsvoraussetzung gleich

$$c = \det\begin{pmatrix} 1 & \theta_1 & \ldots & \theta_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \theta_n & \ldots & \theta_n^{n-1} \end{pmatrix} = \prod_{i<j<n+1} (\theta_j - \theta_i).$$

Es folgt

$$P(x) = c\prod_{i=1}^{n}(x-\theta_i) = \left(\prod_{i<j<n+1}(\theta_j-\theta_i)\right)\left(\prod_{i=1}^{n}(x-\theta_i)\right)$$

Setzt man $x = \theta_{n+1}$, so folgt die erste Behauptung.

Fuer die zweite Aussage schreibe $\theta = \theta_1$ und $f(x) = \prod_j(x-\theta_j)$. Man bildet die Ableitung f' nach der Leibniz-Regel

$$f'(x) = \sum_j \prod_{i\neq j}(x-\theta_i).$$

Setzt man $\theta = \theta_1$ ein, verschwinden alle Summanden bis auf den ersten

$$f'(\theta)) = \prod_{j\neq 1}(\theta_1-\theta_j)$$

und also

$$N_{K(x)/K}(f'(\theta)) = \prod_\sigma\prod_{j\neq 1}(\sigma(\theta_1)-\sigma(\theta_j)) = \prod_{i\neq j}(\theta_i-\theta_j).$$

Jeder Faktor tritt zweimal auf mit verschiedenen Vorzeichen. Sammelt man diese ein, erhaelt man die Behauptung.

(b) Es gilt

$$\mathrm{Tr}_{L/K}(v_{i_0}v_{j_0}) = \sum_k \sigma_k(v_{i_0})\sigma_k(v_{j_0}) = \left[(\sigma_i v_j)^t(\sigma_i v_j)\right]_{i_0,j_0},$$

also

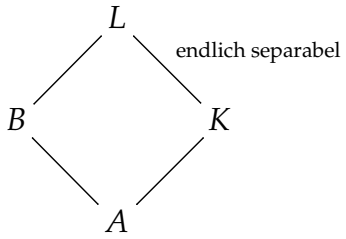
$$\det \mathrm{Tr}_{L/K}(v_iv_j) = \det(\sigma_i v_j)^2.$$

(d) Da L/K separabel ist, existiert ein primitives Element $\theta \in L$, also $L = K(\theta)$. Dann ist die Form (x,y) durch die Matrix $S = \mathrm{Tr}_{L/K}(\theta^{i-1}\theta^{j-1})$ gegeben. Diese ist nicht ausgeartet, denn

$$\det(S) = D(1,\theta,\ldots,\theta^{n-1}) = \prod_{i<j}(\theta_i-\theta_j)^2 \neq 0.$$

(c) folgt aus (d), da $D(v_1,\ldots,v_n)$ die Determinante der Matrix der Form $(.,.)$ ist. □

Wir betrachten jetzt wieder die Situation



wobei A ein ganzabgeschlossener Integritaetsring mit Quotientenkoerper K ist und B der ganze Abschluss von A in L.

Lemma 2.3.4. (a) *Ist $\beta \in B$, dann gilt* $\mathrm{Tr}_{L/K}(\beta), \mathrm{N}_{L/K}(\beta) \in A$.

(b) *Fuer $\beta \in B$ gilt*

$$\beta \in B^\times \quad \Leftrightarrow \quad \mathrm{N}_{L/K}(\beta) \in A^\times.$$

Beweis. (a) Sei $b \in B$. Dann ist auch jedes $\sigma(b)$ ganz ueber A, wenn $\sigma \in E = \mathrm{Hom}_K(L, \overline{K})$. Damit sind $X = \mathrm{Tr}_{L/K}(b) = \sum_\sigma \sigma(b)$ und $N(b) = \prod_\sigma \sigma(b)$ ganz ueber A, aber gleichzeitig liegen sie in K und da A ganzabgeschlossen ist, liegen sie in A.

(b) "$\Rightarrow$" Ist $\alpha\beta = 1$ dann folgt $\mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta) = \mathrm{N}_{L/K}(\alpha\beta) = 1$.
"$\Leftarrow$" Wir koennen annehmen, dass $L \subset \overline{K}$. Sei zunaechst L/K normal, also galoisch. Sei $\mathrm{N}_{L/K}(\beta)a = 1$ mit $a \in A$, dann folgt $\beta\ [(\prod_{\sigma \neq I} \sigma(\beta))\, a] = 1$ und da alle $\sigma(b)$ in B liegen, ist $\beta \in B^\times$.

Als naechstes sei N die normale Huelle von L, also $N/L/K$ so dass N/K galoisch. Ferner seien C der ganze Abschluss von B in N und $n = [N/L]$. Nach Satz 2.2.1 (d) und Korollar 2.2.2 gilt

$$\mathrm{N}_{N/K}(\beta) = \mathrm{N}_{L/K}\left(\mathrm{N}_{N/L}(\beta)\right) = \mathrm{N}_{L/K}\left(\beta^n\right) = \mathrm{N}_{L/K}(\beta)^n \in A^\times.$$

Damit folgt $\beta \in C^\times$ und damit $\beta^n = \mathrm{N}_{N/L}(\beta) \in B^\times$, also $\beta \in B^\times$. □

Lemma 2.3.5. *Sei $v_1, \ldots, v_n$ eine Basis von L/K und nimm an, dass $v_j \in B$ fuer jedes j, dann gilt fuer die Diskriminante $d = D(v_1, \ldots v_n)$, dass*

$$dB \subset Av_1 \oplus \cdots \oplus Av_n.$$

Insbesondere folgt: liegen $v_1, \ldots, v_n$ alle in B, dann ist $d \in A$.

Beweis. Durch Multiplikation aller v_j mit einem $\lambda \in K$ kann man $v_j \in B$ erreichen (Proposition 2.1.9). Nehmen wir das also an. Sei $\alpha = a_1 v_1 + \cdots + a_n v_n \in B$, $a_j \in K$. Dann sind die a_j Loesungen des Gleichungssystems

$$\mathrm{Tr}_{L/K}(v_i \alpha) = \sum_j \mathrm{Tr}_{L/K}(v_i v_j) a_j = \left(S \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \right)_i .$$

Nun liegt $\mathrm{Tr}_{L/K}(v_i \alpha)$ in A und die Eintraege der Matrix S ebenfalls. Nach der Cramerschen Regel folgt $a_i \in \frac{1}{d} A$, wobei $d = \det(S) = D(v_1, \ldots, v_n)$. Also $d a_i \in A$, so dass

$$d\alpha \in A v_1 \oplus \ldots A v_n. \qquad \square$$

Definition 2.3.6. Eine **Ganzheitsbasis** ist eine Basis $v_1, \ldots, v_n$ von L/K so dass gilt

$$B = A v_1 \oplus \cdots \oplus A v_n.$$

Beispiele 2.3.7.

(a) $\mathbb{Z}[i]$ hat $1, i$ als Ganzheitsbasis.

(b) $\mathbb{Z}[\sqrt{5}]$ hat $1, \frac{1+\sqrt{5}}{2}$ als Ganzheitsbasis.

Satz 2.3.8. *Ist L/K endlich separabel und ist A ein Hauptidealring, so ist jeder endlich erzeugte B-Untermodul $0 \neq V \subset L$ ein freier A-Modul vom Rang $[L : K]$. Insbesondere hat B eine Ganzheitsbasis ueber A.*

Beweis. Sei $V \neq 0$ ein endlich erzeugter B-Untermodul von L. Sei $w_1, \ldots, w_n$ eine Basis von L/K. Nach Proposition 2.1.9 koennen wir annehmen, dass $w_j \in B$ fuer jedes j. Mit $d = D(v_1, \ldots, v_n)$ gilt nach Lemma 2.3.5

$$dB \subset A w_1 \oplus \cdots \oplus A w_n.$$

Sei $v_1, \ldots, v_r$ ein Erzeugendensystem des B-Moduls V. Es existiert nun ein $a \in A$ so dass $a v_i \in B$ fuer jedes i, also $aV \subset B$, so dass

$$adV \subset dB \subset \underbrace{A w_1 \oplus \cdots \oplus A w_n}_{V_0}.$$

Nach dem Elementarteilersatz ist adV als Untermodul des Freien Moduls V_0 selbst frei. Nach Proposition 2.1.9 gilt

$$[L : K] = \operatorname{Rang} V_0 \geq \operatorname{Rang} V = \dim_K(KV) = [L : K]. \qquad \square$$

Beispiel 2.3.9. Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ eine **quadratfreie Zahl**, d.h., in der Primfaktorzerlegung von d kommt jede Primzahl nur mit Potenz 1 vor. Sei $K = \mathbb{Q}\left(\sqrt{d}\right)$ und sei $\mathcal{O} = \mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$ in K, der **Ganzzahlring** von K. Dann ist $1, \omega$ eine Ganzheitsbasis, wobei

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4, \\ \sqrt{d} & \text{sonst.} \end{cases}$$

Beweis. Uebungsaufgabe. $\square$

Korollar 2.3.10. *Sei $L/\mathbb{Q}$ eine endliche Koerpererweiterung und $B \subset L$ ein Integritaetsring mit Ganzheitsbasis ueber $\mathbb{Z}$. Sei $b \in B$. Dann gilt*

$$|N_{K/L}(b)| = |B/bB|.$$

Beweis. Sei M_b die Matrix der b-Multiplikation in einer Ganzheitsbasis. Dann gilt

$$|B/pB| = |\mathbb{Z}^n/M\mathbb{Z}^n|$$

Nach dem Elementarteilersatz kann man $M = SDT$ schreiben, wobei $S, T \in \mathrm{GL}_n(\mathbb{Z})$ und D eine Diagonalmatrix $D = \operatorname{diag}(d_1, \ldots, d_n)$ ueber $\mathbb{Z}$ ist. Dann gilt $\det(S), \det(T) = \pm 1$ und daher

$$|N_{L/K}|(b)| = |\det(M)| = |\det(D)|.$$

Andererseits ist $T\mathbb{Z}^n = \mathbb{Z}^n$ und deshalb

$$|\mathbb{Z}^n/SDT\mathbb{Z}^n| = |\mathbb{Z}^n/SD\mathbb{Z}^n|.$$

Die Abbildung $\mathbb{Z}^n/SD\mathbb{Z}^n \to \mathbb{Z}^n/D\mathbb{Z}^n$, $x \mapsto S^{-1}x$ ist eine Bijektion. Damit folgt

$$\begin{aligned} |B/bB| = |\mathbb{Z}^n/D\mathbb{Z}^n| &= \left|\prod_{j=1}^{n} \mathbb{Z}/d_j\mathbb{Z}\right| = |d_1 \cdots d_n| \\ &= |\det(D)| = |\det(SDT)| = |\det(M)| = |N_{L/\mathbb{Q}}(b)|. \end{aligned} \qquad \square$$

Satz 2.3.11. *Sind $v_1, \dots, v_n$ und $v'_1, \dots, v'_n$ Basen von L/K mit Basiswechselmatrix $T = (a_{ij}) \in \mathrm{M}_n(K)$, also $v'_j = \sum_j a_{i,j} v_i$, dann gilt fuer die Diskriminante*

$$D(v'_1, \dots, v'_n) = (\det(T))^2 D(v_1, \dots, v_n).$$

Ist $K = \mathbb{Q}$ und $A = \mathbb{Z}$, so haben alle Ganzheitsbasen von einem gegebenen L dieselbe Diskriminante.

Beweis. Es gilt

$$\begin{aligned} D(v'_1, \dots, v'_n) &= \det(\sigma_k v'_j)^2 \\ &= \det(T(\sigma_k v_j))^2 = \det(T)^2 D(v_1, \dots, v_n). \end{aligned}$$

Ist $A = \mathbb{Z}$, so stellt T eine Basiswechselmatrix eines freien $\mathbb{Z}$-Moduls dar, liegt also in $\mathrm{GL}_n(\mathbb{Z})$, hat also Determinante ± 1. □

Definition 2.3.12. Ein **Zahlkoerper** K ist eine endliche Erweiterung von $\mathbb{Q}$. In diesem Fall sei

$$\mathcal{O}_K = \text{ ganzer Abschluss von } \mathbb{Z} \text{ in } K$$

der **Ganzzahlring** von K. Die **Diskriminante** D_K des Zahlkoerpers K ist die Diskriminante einer beliebigen Ganzheitsbasis.

Beispiel 2.3.13. Ist $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei und $K = \mathbb{Q}\left(\sqrt{d}\right)$, dann gilt

$$D_K = \begin{cases} d & d \equiv 1 \mod 4, \\ 4d & \text{sonst.} \end{cases}$$

Insbesondere folgt: ist K ein quadratischer Zahlkoerper (also $[K : \mathbb{Q}] = 2$), dann ist

$$K = \mathbb{Q}(\sqrt{D_K}),$$

also ist K durch die Diskriminante eindeutig festgelegt.

Satz 2.3.14. *Seien K ein Zahlkoerper und $\mathfrak{a} \subset \mathfrak{a}'$ zwei endlich-erzeugte $\mathcal{O}_K$-Untermoduln von K Sei die* **Diskriminante** *$D(\mathfrak{a})$ von $\mathfrak{a}$ definiert als die Diskriminante einer*

beliebigen $\mathbb{Z}$-Basis von $\mathfrak{a}$, welche nach Satz 2.3.8 existiert. Dann ist der Index $(\mathfrak{a}' : \mathfrak{a}) = |\mathfrak{a}'/\mathfrak{a}|$ endlich und es gilt

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

Beweis. Sei $v_1, \dots, v_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ und $v_1', \dots, v_n'$ eine von $\mathfrak{a}'$. Sei T die Basiswechselmatrix, dann gilt $D(\mathfrak{a}) = (\det T)^2 D(\mathfrak{a}')$. Es bleibt zu zeigen, dass $|\det(T)| = |\mathfrak{a}'/\mathfrak{a}|$ gilt. Da $\mathfrak{a}$ ein $\mathbb{Z}$-Untermodul von $\mathfrak{a}'$ ist, gilt $T \in \mathrm{M}_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{Q})$. Die obige Behauptung ist klar, wenn T Diagonalgestalt hat. Nach dem Elementarteilersatz kann man aber die Basen (v_j) und (v_j') so waehlen, dass T Diagonalgestalt bekommt. □

Satz 2.3.15. *Seien K, L zwei Galois-Erweiterungen von $\mathbb{Q}$, so dass $K \cap L = \mathbb{Q}$. Seien $a_1, \dots, a_m$ und $b_1, \dots, b_n$ Ganzheitsbasen von K bzw L. Nimm an, dass die Diskriminanten D_K und D_L teilerfremd sind. Dann ist $(a_i b_j)$ eine Ganzheitsbasis vom Kompositum KL und es gilt*

$$D_{KL} = D_K^n \, D_L^m.$$

Proof. Sei $\alpha = \sum_{i,j} \lambda_{ij} a_i b_j$ ein ganzes Element in KL mit $\lambda_{ij} \in \mathbb{Q}$. Wir schreiben

$$\begin{aligned}
\mathrm{Gal}(KL/L) &= \{\sigma_1, \dots, \sigma_m\}, \\
\mathrm{Gal}(KL/K) &= \{\tau_1, \dots, \tau_n\}, \\
\mathrm{Gal}(KL/\mathbb{Q}) &= \{\sigma_i \tau_j : 1 \le i \le m,\ 1 \le j \le n\}.
\end{aligned}$$

Die Matrix $T = \tau_j(b_i)$ erfuellt $\det T^2 = D_L$ und

$$\big(\tau_1\alpha, \dots, \tau_n\alpha\big)^t = T \left(\sum_i \lambda_{i,1} a_i, \dots, \sum_i \lambda_{i,n} a_i \right)^t.$$

Sei $T^\# = \det(T)\, T^{-1}$ die Adjunkte, dann folgt

$$T^\# \big(\tau_1\alpha, \dots, \tau_n\alpha\big)^t = \det(T) \left(\sum_i \lambda_{i,1} a_i, \dots, \sum_i \lambda_{i,n} a_j \right)^t.$$

Die linke Seite ist ein Vektor mit ganzen Elementen. Wir multiplizieren beide Seiten mit der ganzen Zahl $\det(T)$ und erhalten

$$D_L \sum_i \lambda_{ij}\, a_i \in \mathcal{O}_L, \quad \text{also } D_L \lambda_{ij} \in \mathbb{Z}.$$

Vertausche K und L und erhalte ebenso

$$D_K \lambda_{ij} \in \mathbb{Z}$$

und da nach Voraussetzung die Diskriminanten teilerfremd sind, ist $\lambda_{ij} \in \mathbb{Z}$ fuer alle i, j. Daher ist $(a_i b_j)$ eine Ganzheitsbasis. Berechnet man in dieser Basis die Diskriminante, sieht man auch die zweite Aussage. □

* * *

2.4 Kreisteilungskoerper

Fuer $n \in \mathbb{N}$ sei

$$C_n(x) = \prod_{\substack{0 \le j \le n-1 \\ ggT(j,n)=1}} (x - e^{2\pi i j/n})$$

das n-te **Kreisteilungspolynom** in $\mathbb{C}[x]$.

Der Grad des n-ten Kreisteilungspolynoms C_n ist gleich

$$\phi(n) = (\mathbb{Z}/n\mathbb{Z})^\times$$

die **Eulersche ϕ-Funktion**.

Lemma 2.4.1. *Die Eulersche ϕ-Funktion ist schwach multiplikativ, d.h., sind m und n in $\mathbb{N}$ teilerfremd, dann ist $\phi(mn) = \phi(m)\phi(n)$. Ist p eine Primzahl und $k \in \mathbb{N}$, dann gilt*

$$\phi(p^k) = p^k - p^{k-1}.$$

Beweis. Mit dem chinesischen Restsatz folgt fuer teilerfremde m, n, dass $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ und damit folgt die Multiplikativitaet. Die Elemente in $\mathbb{Z}/p^k\mathbb{Z}$, die nicht teilerfremd zu p^k sind, sind genau die Vielfachen von p und damit das Bild der injektiven Abbildung $\mathbb{Z}/p^{k-1}\mathbb{Z} \hookrightarrow \mathbb{Z}/p^k\mathbb{Z}$, $(n + p^{k-1}\mathbb{Z}) \mapsto (np + p^k\mathbb{Z})$. □

Sei μ_n die Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$. Diese Gruppe ist zyklisch und wird von $\zeta_n = e^{2\pi i/n}$ erzeugt. Eine Einheitswurzel $\zeta \in \mu_n$ heisst **primitive n-te Einheitswurzel**, wenn ζ die Gruppe μ_n erzeugt. Dies ist genau dann der Fall, wenn $\zeta = e^{2\pi ij/n}$ ist fuer ein j, das teilerfremd zu n ist. Daher sind die Nullstellen von C_n genau die primitiven n-ten Einheitswurzeln, also

$$C_n(x) = \prod_{\zeta \in \mu_n^{prim}} (x - \zeta),$$

wobei μ_n^{prim} die Menge der primitiven n-ten Einheitswurzeln bezeichnet.

Proposition 2.4.2. *Es gilt*

$$x^n - 1 = \prod_{d|n} C_d(x),$$

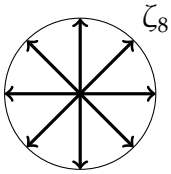
wobei das Produkt ueber alle $d \in \mathbb{N}$ laeuft, die n teilen. Die Kreisteilungspolynome liegen in $\mathbb{Z}[x]$, sind normiert und haben den konstanten Term 1.

Beweis. Das Polynom auf der linken Seite hat genau alle Elemente von μ_n als Nullstellen, jede ist eine einfache Nullstelle. Ist $\zeta \in \mu_n$ von Ordnung d, dann ist d ein Teiler von n und ζ ist einfache Nullstelle des Kreisteilungspolynoms C_d und keines anderen. Damit haben beide Seiten der behaupteten Gleichung dieselben Nullstellen, alle sind einfach, also sind die beiden Polynome gleich.

Wir beweisen nun, dass die Koeffizienten von C_n ganzzahlig sind. Durch Polynomdivision sieht man induktiv, dass sie Koeffizienten in $\mathbb{Q}$ haben. Die Behauptung folgt dann aus Proposition 1.1.8. □

Lemma 2.4.3. *Ist die primitive n-te Einheitswurzel ζ Nullstelle des irreduziblen normierten Polynoms $f \in \mathbb{Q}[x]$ und ist $p \nmid n$ eine Primzahl, dann ist auch ζ^p eine Nullstelle von f.*

Beweis. Sowohl ζ als auch ζ^p sind Nullstellen von $x^n - 1 = f(x)g(x)$ fuer ein normiertes Polynom $g(x)$. Nach Proposition 1.1.8 sind f und g beide in $\mathbb{Z}[x]$. **Angenommen**, $f(\zeta^p) \neq 0$, dann folgt $g(\zeta^p) = 0$, also ist ζ Nullstelle von $g(x^p)$. Da f das Minimalpolynom von ζ ist, gibt es ein Polynom $h \in \mathbb{Q}[x]$ so dass $g(x^p) = h(x)f(x)$. Wieder gilt $h \in \mathbb{Z}[x]$. Seien $\overline{f}, \overline{g}, \overline{h}$ die Bilder in $\mathbb{Z}/p\mathbb{Z}[x]$. Es ist dann $\overline{f}(x)\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p$. Daher folgt ueber dem endlichen Koerper $\mathbb{F}_p$, dass $x^n - 1 = \overline{f}\overline{g}$. Jeder irreduzible Faktor von $\overline{f}$ ist wegen $\overline{g}^p = \overline{fh}$ auch ein Faktor von $\overline{g}$ und damit hat $x^n - 1$ mehrfache Nullstellen. Das kann aber nicht sein, denn die Ableitung von $x^n - 1$ ist nx^{n-1} und die hat nur die Null als Nullstelle, **Widerspruch!** □



Satz 2.4.4 (Kreisteilungskoerper)**.** *Das Kreisteilungspolynom C_n ist irreduzibel. Die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist galoissch mit Galois-Gruppe isomorph zu $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Beweis. Sei ζ eine primitive n-te Einheitswurzel und f ihr Minimalpolynom. Wir muessen zeigen, dass $f = C_n$. Wir sind fertig, wenn wir zeigen koennen, dass jede andere primitive n-te Einheitswurzel ebenfalls Nullstelle von f ist. Sei dazu ε eine weitere Primitive n-te Einheitswurzel, dann ist $\varepsilon = \zeta^d$ mit $\mathrm{ggT}(d, n) = 1$. Es folgt $d = p_1 \cdots p_k$ mit zu n teilerfremden Primzahlen. Nach dem Lemma ist ζ^{p_1} eine Nullstelle von f und dann $\zeta^{p_1 p_2}$ und so fort bis zu $\zeta^d = \varepsilon$. Daher ist C_n irreduzibel.

$L = \mathbb{Q}(\zeta_n)$ ist der Zerfaellungskoerper von $x^n - 1$ und damit galoissch ueber $\mathbb{Q}$. Sei ζ eine n-te Einheitswurzel in L. Ist $\zeta \in \mu_n$ primitiv und $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, dann ist $\tau(\zeta)$ wieder primitiv. Ferner ist τ durch das Bild $\tau(\zeta)$ eindeutig festgelegt. Fixieren wir eine primitive n-te Einheitswurzel ζ_n, so erhalten wir also eine injektive Abbildung $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mu_n^{prim}$, $\tau \mapsto \tau(\zeta_n)$. Da aber C_n irreduzibel ist, ist es das Minimalpolynom von ζ und daher ist der Grad von $\mathbb{Q}(\zeta)$ ueber $\mathbb{Q}$ gleich dem Grad von C_n, also $|\mu_n^{prim}|$, so dass

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mu_n^{prim}$$

folgt. Die Abbildung $k \mapsto \zeta_n^k$ schliesslich ist ein Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mu_n^{prim}$. □

Proposition 2.4.5.

(a) *Seien $m, n \in \mathbb{N}$. Dann gilt fuer das Kompositum*

$$\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_k),$$

wobei k das kleinste gemeinsame Vielfache von m und n ist.

(b) *Die Einheitswurzeln im Koerper $\mathbb{Q}(\zeta_n)$ sind genau die Zahlen $\pm 1, \pm\zeta_n, \ldots, \pm\zeta_n^{n-1}$.*

Beweis. (a) Es seien $m = cd$ und $n = cf$, wobei c der ggT ist. Dann gilt $k = cdf$ und

$(d, f) = 1$. Ferner ist ζ_k^f eine m-te Primitive Einheitswurzel, also kann man $\zeta_k^f = \zeta_m$ annehmen und ebenso $\zeta_k^d = \zeta_n$, so dass die Inklusion "$\subset$" klar ist.

Fuer die andere Inklusion beachte, dass es wegen $(d, f) = 1$ ganze Zahlen x, y gibt, so dass $dx + fy = 1$. Dann folgt

$$\zeta_m^y \zeta_n^x = (\zeta_k^f)^y (\zeta_k^d)^x = \zeta_k^{dx+fy} = \zeta_k.$$

(b) Sei ζ_m eine primitive m-te Einheitswurzel, die in $\mathbb{Q}(\zeta_n)$ liegt. Nach Teil (a) folgt dann $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_k)$, wobei k das kleinste gemeinsame Vielfache von m und n ist. Dann gilt $n \mid k$ und $\phi(n) = \phi(k)$. Ist $n = \prod_p p^{v_p}$ die Primfaktorzerlegung und ist $k = \prod_p p^{v_p+k_p}$, dann gilt also

$$\prod_{p:v_p>0} p^{v_p-1}(p-1) = \prod_{p:v_p+k_p>0} p^{v_p+k_p-1}(p-1).$$

Da jeder Faktor links $\leq$ dem entsprechenden Faktor rechts ist, muessen alle diese Faktoren jeweils gleich sein, es gilt also

$$\begin{aligned} p^{v_p-1}(p-1) &= p^{v_p+k_p-1}(p-1) && \text{falls } v_p > 0, \\ 1 &= p^{k_p-1}(p-1) && \text{falls } v_p = 0,\ k_p > 0. \end{aligned}$$

Daraus ergibt sich $k_p = 0$, ausser wenn $p = 2$ und $v_2 = 0$. Im ersten Fall folgt $\zeta_m = \zeta_n$. Der zweite Fall tritt genau dann ein, wenn n ungerade und $k = 2n$ ist. In diesem Fall ist $\zeta_k = \zeta_{2n} = -\zeta_n^{\frac{n+1}{2}}$, wie aus der Gleichung $\frac{1}{2n} = \frac{\frac{n+1}{2}}{n} + \frac{1}{2}$ mit der Ientifikation $\zeta_{2n} = e^{2\pi i \frac{1}{2n}}$ folgt. Also folgt auch in diesem Fall die Behauptung. □

* * *

2.5 Ganzzahlringe in Kreisteilungskoerpern

Satz 2.5.1. *Sei ζ_n eine primitive n-te Einheitswurzel und $K = \mathbb{Q}(\zeta_n)$. Dann ist $O_K = \mathbb{Z}[\zeta_n]$. Insbesondere ist $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)-1}$ eine Ganzheitsbasis. Es gilt*

$$D_K = (-1)^{\frac{\phi(n)}{2}} \frac{n^{\phi(n)}}{\prod_{p|n} p}$$

Der Beweis ist nicht schwer, aber sehr detailreich. Wir lassen ihn aus.

* * *

3 Dedekind-Ringe

Vorbemerkung. Ernst Kummer hat im 19. Jahrhundert festgestellt, dass Ganzzahlringe im Allgemeinen nicht faktoriell sind, was als ein großes Übel empfunden wurde. Er ergaenzte die fehlende Faktorzerlegung durch (vorgestellte) ”ideale Zahlen” (im Sinne von imaginierte Zahlen) und rechnete damit.

Richard Dedekind zeigte, dass gewisse Zahlenmengen, die er ”Ideale” nannte, die von Kummer gewuenschten Eigenschaften haben. Er stelle also fest, dass in Ganzzahlringen alle Ideale als Produkte von Primidealen geschrieben werden koennen. Wir nennen dies die **Primidealzerlegungs-Eigenschaft** oder wir sagen, der Ring hat **Primidealzerlegung**.

Die Eigenschaft der Primidealzerlegung ist zwar fuer Anwendungen nuetzlich, aber es ist schwer, von einem gegebenen Ring nachzuweisen, dass er diese Eigenschaft besitzt. Daher ist folgende Aussage nuetzlich:

Ein Integritaetsring, der kein Koerper ist, hat genau dann Primidealzerlegung, wenn er

(a) **noethersch** ist,

(b) **ganzabgeschlossen** und

(c) wenn in ihm jedes Primideal $p \neq 0$ maximal ist.

Wir werden zunaechst die hier auftretenden Begriffe einfuehren und diese Aussage in Satz 3.2.14 beweisen.

* * *

3.1 Noethersche Ringe

Satz 3.1.1. *Sei R ein Ring. Dann sind aequivalent:*

(a) *Jedes Ideal a von R ist endlich-erzeugt.*

(b) *Jede aufsteigende Kette* $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$ *von Idealen wird stationaer, d.h., es existiert ein Index* k_0 *so dass* $\mathfrak{a}_k = \mathfrak{a}_{k_0}$ *fuer jedes* $k \geq k_0$ *gilt.*

Beweis. (a)⇒(b): Sei eine aufsteigende Kette $(\mathfrak{a}_k)_{k\in\mathbb{N}}$ gegeben und sei

$$\mathfrak{a} = \bigcup_{k\in\mathbb{N}} \mathfrak{a}_k.$$

Dann ist $\mathfrak{a}$ ein Ideal, also endlich-erzeugt, seien $u_1, \dots, u_n$ Erzeuger, dann liegt jedes u_i in einem $\mathfrak{a}_k$, also gibt es ein k_0, so dass alle u_i in $\mathfrak{a}_{k_0}$ liegen, also ist fuer jedes $k \geq k_0$

$$\mathfrak{a}_k = \mathfrak{a} = \mathfrak{a}_{k_0}.$$

(b)⇒(a): Sei $\mathfrak{a}$ ein Ideal, das nicht endlich erzeugbar ist. Dann existiert eine Folge $u_1, u_2, \dots$ von Elementen von $\mathfrak{a}$ so dass fuer die Ideale

$$\mathfrak{a}_n = Ru_1 + Ru_2 + \cdots + Ru_n$$

gilt $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$, was der aufsteigenden Kettenbedingung widerspricht. □

Definition 3.1.2. Ein Ring R heisst **noethersch**, wenn er den aequivalenten Bedingungen des Satzes genuegt.

Satz 3.1.3 (Hilbert)**.** *Ist* R *noethersch, dann auch jeder Quotient* $R/\mathfrak{a}$ *und der Polynomring* $R[x]$.

Proof. Ist $\overline{\mathfrak{a}}_1 \subset \overline{\mathfrak{a}}_2 \subset \dots$ eine aufsteigende Idealkette in $R/\mathfrak{a}$ und ist $\mathfrak{a}_j$ das Urbild von $\overline{\mathfrak{a}}_j$ in R, dann ist $\mathfrak{a} \subset \mathfrak{a}_1 \subset \dots$ eine aufsteigende Idealkette in R und da R noethersch ist, wird diese stationaer, also auch die Kette der Bilder in $R/\mathfrak{a}$.

Sei nun R noethersch und $\mathfrak{a}$ ein Ideal von $R[x]$. Sei S_n die Menge aller $a \in R$ so dass $a = 0$ oder es ein Polynom $ax^n + a_{n-1}x^{n-1} + \cdots + a_0$ gibt, das in $\mathfrak{a}$ liegt. Dann ist S_j ein Ideal in R. Esgilt $S_0 = R \cap \mathfrak{a}$. Ferner ist

$$S_0 \subset S_1 \subset \dots.$$

Denn: Ist $a \in S_n$, also $f(x) = ax^n + \dots$ in $\mathfrak{a}$, dann ist $xf(x) = ax^{n+1} + \dots$ in $\mathfrak{a}$, also $a \in S_{n+1}$. Da R noethersch ist, wird die Idealkette stationaer, es gibt also ein r so dass $S_r = S_{r+1} = \dots$. Seien

$$\begin{gathered} a_{01}, \dots, a_{0n_0} \text{ Erzeuger von } S_0, \\ \vdots \\ a_{r1}, \dots, a_{rn_r} \text{ Erzeuger von } S_r \end{gathered}$$

Sei jeweils f_{ij} ein Polynom in $\mathfrak{a}$ so dass a_{ij} der Leitkoeffizient von f_{ij} ist. Sei $\mathfrak{b}$ das Ideal, das von den endlich vielen f_{ij} erzeugt wird. Wir behaupten $\mathfrak{a} = \mathfrak{b}$, wobei $\mathfrak{b} \subset \mathfrak{a}$ klar ist. Sei $f \in \mathfrak{a}$ vom Grad d. Wir benutzen Induktion nach d um $f \in \mathfrak{b}$ zu zeigen. Der Fall $d = 0$ ist wegen $S_0 = \mathfrak{a} \cap R$ klar. Fuer $d > r$ liegt der Leitkoeffizient a von f in S_d und dieses Ideal wird von den Leitkoeffizienten von

$$x^{d-r} f_{r,1}, \dots, x^{d-r} f_{r,n_r}$$

erzeugt. Daher gibt es $c_1 \dots, c_{n_r} \in R$ so dass das Polynom

$$f - c_1 x^{d-r} f_{r1} - \dots - c_{n_r} x^{d-r} f_{rn_r}$$

einen Grad $< d$ hat, also in $\mathfrak{b}$ liegt, so dass induktiv $f \in \mathfrak{b}$ folgt. Im Fall $d \leq r$ finden wir Koeefizienten so dass

$$f - c_1 f_{d1} - \dots - c_{n_d} f_{dn_d}$$

vom Grad $< d$ ist und schliessen ebenso. □

Beispiel 3.1.4. Beispiel fuer einen nicht noetherschen Ring: $\mathbb{Z}[x_1, x_2, \dots]$ ein Polynomring in unendlich vielen Unbestimmten. Dann ist das Ideal $\mathfrak{a} = \langle x_1, x_2, \dots \rangle$, das von allen Unbestimmten erzeugt wird, nicht endlich erzeugt.

Satz 3.1.5. *Sei R ein noetherscher Ring und sei M ein endlich-erzeugter Modul. Dann ist jeder Untermodul von M ebenfalls endlich-erzeugt.*

Bewei. Da M endlich-erzeugt ist, gibt es einen surjektiven Modulhomomorphismus $\phi : R^n \to M$. Ist $L \subset M$ ein Untermodul, so reicht es zu zeigen, dass $\phi^{-1}(L)$ endlich-erzeugt ist. Das bedeutet, es reicht, den Satz fuer den Modul R^n zu zeigen. Wir

tun dies durch Induktion nach n. Der Fall $n = 1$ ist trivial. Nun also zu $n \to n+1$: Betrachte die exakte Sequenz

$$0 \to R^n \to R^{n+1} \xrightarrow{p} R \to 0,$$

wobei der erste Pfeil durch die Inklusion, genauer durch $x \mapsto (x, 0)$ gegeben und der zweite die Projektion auf die letzte Koordinate ist.

Zu jedem Untermodul $U \subset R^{n+1}$ assoziieren wir zwei Moduln $(U \cap R^n, p(U))$ und wir behaupten, dass zwei Untermoduln $U \subset R^{n+1}$ genau dann gleich sind, wenn ihre assoziierten Paare uebereinstimmen. Die eine Richtung ist trivial, es ist also zu zeigen, dass fuer zwei Untermoduln $U, W \subset R^{n+1}$ gilt

$$\left\{ \begin{array}{c} R^n \cap U = R^n \cap W \\ p(U) = p(W) \end{array} \right\} \quad \Rightarrow \quad U = W.$$

Sei $x \in W$, dann existiert ein $y \in U$ so dass $p(x) = p(y)$, also $x - y \in R^n \cap W = R^n \cap U$. Da $y \in U$, folgt $x \in U$. Damit also $W \subset U$. Die andere Inklusion folgt wegen Symmetrie.

Sei nun $U_1 \subset U_2 \subset \ldots$ eine aufsteigende Kette von Untermoduln von R^n. Nach Induktionsvoraussetzung werden die Ketten $R^n \cap U_j$ und $p(U_j)$ stationaer, also auch (U_j). □

* * *

3.2 Dedekind-Ringe

Satz 3.2.1. *Sei K ein Zahlkoerper mit Ganzzahlring $\mathcal{O}_K$. Dann ist $\mathcal{O}_K$ noethersch, ganzabgeschlossen und jedes Primideal $\mathfrak{p} \neq 0$ ist maximal.*

Beweis. Nach Satz 2.3.8 ist jedes Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul von endlichem Rang, also endlich erzeugt. Da $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$, ist er ganzabgeschlossen. Ist $\mathfrak{p}$ ein Primideal $\neq 0$, dann ist $\mathfrak{p}$ nach Satz 2.3.8 ein freier $\mathbb{Z}$-Modul vom gleichen Rang wie $\mathcal{O}_K$, also ist $\mathcal{O}_K/\mathfrak{p}$ endlich. Damit folgt der Satz aus dem naechsten Lemma. □

Lemma 3.2.2. *Ein endlicher Integritaetsring ist ein Koerper.*

Beweis. Sei R ein endlicher Integritaetsring und sei $r \in R \setminus \{0\}$. Dann ist $m_r : R \to R$, $x \mapsto rx$ injektiv, also, da R endlich ist, surjektiv. Es gibt also ein $s \in R$ mit $rs = 1$, d.h., r ist invertierbar. □

Definition 3.2.3. Ein noetherscher, ganzabgeschlossener Integritaetsring, der kein Koerper ist und in dem jedes Primideal $\mathfrak{p} \neq 0$ maximal ist, heisst **Dedekind-Ring**.

Definition 3.2.4. Ein Ring R heisst **lokaler Ring**, falls R genau ein maximales Ideal besitzt.

Ein lokaler Hauptidealring wird auch **diskreter Bewertungsring** genannt.

Erinnerung. (Lokalisierung) Sei R ein Integritaetsring, K sein Quotientenkoerper und sei $S \subset R \setminus \{0\}$ eine **multiplikativ abgeschlossene Menge**, also

$$1 \in S, \qquad a, b \in S \quad \Rightarrow \quad ab \in S,$$

dann ist $S^{-1}R$ der Ring aller Elemente von K mit Nennern in S, also

$$S^{-1}R = \left\{ \frac{a}{s} : a \in R,\ s \in S \right\}.$$

Beispiel 3.2.5. Sei A irgendein Ring und $\mathfrak{p} \subset A$ ein maximales Ideal. Dann ist die Lokalisierung

$$A_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1} A$$

ein lokaler Ring, wobei $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$ ist. Das einzige maximale Ideal von $A_{\mathfrak{p}}$ ist $S_{\mathfrak{p}}^{-1}\mathfrak{p}$. Ist A ein Hauptidealring, dann auch die Lokalisierung $A_{\mathfrak{p}}$, d.h., dann ist $A_{\mathfrak{p}}$ ein diskreter Bewertungsring.

Als Spezialfall betrachte $A = \mathbb{Z}$ und p eine Primzahl. Dann ist der Ring

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

ein diskreter Bewertungsring.

Satz 3.2.6. *Es gilt*

(a) *Ein Hauptidealring, der kein Koerper ist, ist ein Dedekind-Ring.*

(b) *Ist K ein Koerper, dann ist $K[x]$ ein Dedekind-Ring.*

(c) *Diskrete Bewertungsringe sind Dedekind-Ringe.*

Beispiel 3.2.7. Ist $E \subset \mathbb{Z}$ eine endliche Primzahlmenge und ist S die Menge aller natuerlichen Zahlen, die nur Primteiler in E haben, dann ist

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \in \mathbb{Q} : b \in S \right\}$$

ein Dedekind-Ring. Insbesondere gibt es unendlich viele Dedekind-Ringe R mit $\mathbb{Z} \subset R \subset \mathbb{Q}$.

Beweis des Satzes. (a) Sei A ein Haupridealring und kein Koerper, dann ist A ganzabegeschlossen und noethersch, also bleibt zu zeigen, dass jedes Primideal $\mathfrak{p} \neq 0$ maximal ist. Sei also $\mathfrak{p}$ ein Primideal. Da A ein Hauptidealring ist, gibt es ein $p \in A$ mit $\mathfrak{p} = pA$. Dann ist p ein Primelement. Wir zeigen, dass pA maximal ist. Sei $\mathfrak{q} \supset pA$ ein Ideal mit $\mathfrak{q} \neq A$. Dann ist auch $\mathfrak{q}$ ein Hauptideal, etwa $\mathfrak{q} = qA$. Insbesondere ist $p \in qA$, also $p = qa$ fuer ein $a \in A$. Da A als Hauptidealring faktoriell ist, sind p und q assoziiert, also ist $\mathfrak{p} = \mathfrak{q}$.

(b) $K[x]$ ist ein Hauptidealring und damit folgt die Behauptung nach Teil (a).

(c) folgt aus (a), da diskrete Bewertungsringe Hauptidealringe sind. □

Definition 3.2.8. Sind $\mathfrak{a}, \mathfrak{b}$ Ideale eines Rings R, so auch ihre Summe und Produkt:

$$\mathfrak{a} + \mathfrak{b} = \{a + b : a \in \mathfrak{a},\ b \in \mathfrak{b}\},$$
$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{j=1}^{n} : a_j b_j : a_j \in \mathfrak{a},\ b_j \in \mathfrak{b} \right\}.$$

Es ist leicht zu sehen, dass beide Operationen assoziativ und kommutativ sind und dass das Nullideal ein neutrales Element der Addition ist, also

$$\mathfrak{a} + 0 = \mathfrak{a}$$

gilt, sowie dass das Ideal R ein neutrales Element der Multiplikation ist, also

$$aR = a.$$

Wir sagen a **teilt** b, geschrieben $a \mid b$, falls $b \subset a$.

Also: die groesseren Ideale teilen die kleineren.

Lemma 3.2.9. *Sei R ein Ring. Ist p ein Primideal mit $p \supset ab$ fuer zwei Ideale a und b, dann gilt $p \supset a$ oder $p \supset b$. Wir schreiben dies suggestiv als*

$$p \mid ab \quad \Rightarrow p \mid \mathcal{A} \quad \textit{oder} \quad \mathcal{P} \mid b.$$

Beweis. Angenommen, dies ist nicht der Fall, dann gibt es ein $a \in a \setminus p$ und ein $b \in b \setminus p$. Dann ist aber $ab \in ab \subset p$. Da nun p ein Primideal ist, muss $a \in p$ oder $b \in p$ sein, Widerspruch! □

Lemma 3.2.10. *Sei R ein Dedekind-Ring. Zu jedem Ideal $a \neq 0$ gibt es Primideale p_j so dass $a \supset p_1 \cdots p_m$.*

Beweis. Sei S die Menge aller Ideale a, fuer die es solche p_j nicht gibt. **Angenommen** $S \neq \varnothing$. Dann ist S geordnet durch Inklusion. Da R noethersch ist, ist jede aufsteigende Idealkette endlich, daher hat jede Kette in S eine obere Schranke in S. Nach dem Lemma von Zorn gibt es ein maximales Element a in S. Dies ist selbst kein Primideal, also existieren $b_1, b_2 \in R$ mit $b_1 b_2 \in a$ aber $b_1 \notin a$ und $b_2 \notin a$. Sei $a_1 = a + b_1 R$ und $a_2 = a + b_2 R$. Es folgt $a \subsetneq a_j$ fuer $j = 1, 2$ und $a_1 a_2 \subset a$. Da a maximal in S, liegen a_1 und a_2 nicht in S, also gibt es $p_1, \ldots, p_r$ und $q_1, \ldots, q_s$ mit $p_1 \cdots p_r \subset a_1$ und $q_1 \cdots q_s \subset a_2$, also

$$p_1 \cdots p_r q_1 \cdots q_s \subset a_1 a_2 \subset a.$$

Widerspruch! Damit folgt die Behauptung des Lemmas. □

Lemma 3.2.11. *Sei R ein Dedekind-Ring und K der Quotientenkoerper von R. Ist p ein Primideal von R und*

$$p^{-1} = \{x \in K : xp \subset R\},$$

so ist $ap^{-1} \neq a$ fuer jedes Ideal $a \neq 0$. Ferner ist $pp^{-1} = R$.

Beweis. Wir zeigen zunaechst, dass $p^{-1} \notin R$ ist. Sei $0 \neq a \in p$ und $p_1 \cdots p_r \subset aR \subset p$ mit minimalem r. Dann ist nach Lemma 3.2.9 eines der p_j in p enthalten. Sei also $p_1 \subset p$. Da p_1 ein maximales Ideal ist, folgt $p = p_1$. Wegen der Minimalitaet von r gibt es ein

$b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ mit $b \notin (a)$, also $\mathfrak{p} b \subset (a)$ und damit $a^{-1}b \in \mathfrak{p}^{-1}$. Da aber $b \notin (a)$ folgt $a^{-1}b \notin R$, also $\mathfrak{p}^{-1} \not\subset R$.

Sei nun $\mathfrak{a} \neq 0$ ein Ideal von R und $\alpha_1, \ldots, \alpha_m$ ein Erzeugendensystem von $\mathfrak{a}$. **Angenommen,** $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Dann gilt fuer $x \in \mathfrak{p}^{-1}$, dass $x\alpha_i = \sum_j a_{ij}\alpha_j$ mit Koeffizienten $a_{i,j} \in R$. Betrachte die Matrix $A = x\mathfrak{a} - (a_{i,j})$. Es gilt $A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = 0$. Sei $d = \det(A)$, so folgt $d\alpha_1 = \cdots = d\alpha_m = 0$ und da R integer, ist $0 = d = \det(A) = \det(x\mathfrak{a} - (a_{ij}))$. Also ist x ganz ueber R und damit $x \in R$, **Widerspruch!** Damit ist die Hauptaussage des Lemmas gezeigt. Ferner gilt $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subset R$. Man stellt fest, dass $\mathfrak{p}\mathfrak{p}^{-1}$ ein Ideal ist, da $\mathfrak{p}$ maximal, folgt $\mathfrak{p}\mathfrak{p}^{-1} = R$. □

Definition 3.2.12. Sei R ein Integritaetsring mit Quotientenkoerper K. Ein **gebrochenes Ideal** von R ist ein R-Untermodul $\mathfrak{a}$ von K mit der Eigenschaft, dass es ein $\alpha \in K^\times$ gibt, so dass $\alpha\mathfrak{a} \subset R$. Ein gebrochenes Ideal, das in R liegt ist ein echtes Ideal von R, man spricht in diesem Fall von einem **ganzen Ideal**.

Lemma 3.2.13. *Sei R ein noetherscher Integritaetsring mit Quotientenkoerper K. Fuer einen R-Untermodul $\mathfrak{a}$ von K sind aequivalent:*

(a) $\mathfrak{a}$ *ist ein gebrochenes Ideal.*

(b) $\mathfrak{a}$ *ist als R-Modul endlich erzeugt.*

Proof. (a)⇒(b): Sei $\mathfrak{a}$ ein gebrochenes Ideal. Dann gibt es ein $\alpha \in K$, so dass $\alpha\mathfrak{a} \subset R$ ein Ideal ist. Da R noethersch ist, ist $\alpha\mathfrak{a}$ als Ideal, also als R-modul endlich-erzeugt, also ist auch $\mathfrak{a}$ endlich-erzeugt.

(b)⇒(a): Es sei $\mathfrak{a} \subset K$ ein endlich-erzeugter R-modul, es gelte also

$$\mathfrak{a} = Ra_1 + \cdots + Ra_n$$

mit $a_1, \ldots, a_n \in K$. Schreibe $a_j = \frac{\alpha_i}{\beta_j}$ mit $\alpha_j, \beta_j \in R$. Dann gilt $\beta\mathfrak{a} \subset R$ mit $\beta - \beta_1 \cdots \beta_n$. □

Satz 3.2.14. *Sei R ein Integritaetsbereich, der kein Körper ist. Aequivalent sind:*

(a) *R ist ein Dedekind-Ring.*

(b) *Die gebrochenen Ideale von R bilden eine Gruppe bzgl. der Multiplikation.*

Ist dies der Fall, dann kann jedes Ideal $\mathfrak{a} \neq 0$ *als Produkt von Primidealen geschrieben werden*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

wobei die $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{N}_0$, *fast alle Null eindeutig bestimmt sind.*

Bemerkung 3.2.15. Es kann auch gezeigt werden, dass auch der letzte Punkt zu den anderen aequivalent ist, dass also ein Ring genau dann ein Dedekind-Ring ist, wenn jedes Ideal eine Primidealzerlegung besitzt. Da dies aber kompliziert zu beweisen ist und im Folgenden nicht gebraucht wird, lassen wir es weg.

Beweis des Satzes. (a)⇒(b): In Lemma 3.2.11 wurde gezeigt, dass jedes Primideal invertierbar ist. Nach Teil (a) ist dann jedes Ideal invertierbar.

(b)⇒(a): Es gelte (b). Wir zeigen zuerst, dass R noethersch ist. Sei $\mathfrak{a} \subset R$ ein Ideal und $\mathfrak{a}^{-1}$ sein Invers es. Aus $\mathfrak{a}\mathfrak{a}^{-1} = R$ folgt die Existenz von $x_1, \dots, x_n \in \mathfrak{a}$ und $y_1, \dots, y_n \in \mathfrak{a}^{-1}$ mit $\sum_{j=1}^{n} x_j y_j = 1$. Fuer beliebiges $a \in \mathfrak{a}$ ist dann $a = \sum_{j=1}^{n} x_j (y_j a) \in \sum_j x_j R$, also ist $\mathfrak{a}$ von $x_1, \dots, x_n$ erzeugt.

Als naechstes zeigen wir, dass R ganz-abgeschlossen ist. Sei K der Quotientenkoerper $x \in K$ ganz ueber R, d.h. es gilt $x^n + x^{n-1}a_{n-1} + \cdots + a_0 = 0$ fuer geeignete $a_0, \dots, a_{n-1} \in R$. Damit liegt x^n in dem von $1, x, \dots, x^{n-1}$ erzeugten gebrochenen Ideal $\mathfrak{b}$. Es folgt $\mathfrak{b}^2 \subset \mathfrak{b}$ und da $\mathfrak{b}$ invertierbar ist, folgt $\mathfrak{b} \subset R$. Also ist $x \in R$ und R ganz-abgeschlossen.

Sei schliesslich $0 \neq \mathfrak{p} \subset R$ ein Primideal und sei $a \in R \setminus \mathfrak{p}$. Wir betrachten das Ideal $\mathfrak{c} = \mathfrak{p} + aR$. Dieses ist invertierbar, also wegen $\mathfrak{c}\mathfrak{c}^{-1}\mathfrak{p} = \mathfrak{p}$ gilt $\mathfrak{c}^{-1}\mathfrak{p} = R\mathfrak{c}^{-1}\mathfrak{p} \supset \mathfrak{c}\mathfrak{c}^{-1}\mathfrak{p} = \mathfrak{p}$ und $\mathfrak{c}^{-1}\mathfrak{p} \subset \mathfrak{c}^{-1}\mathfrak{c} = R$. Fuer beliebiges $y \in \mathfrak{c}^{-1}\mathfrak{p} = (\mathfrak{p} + aR)^{-1}\mathfrak{p}$ ist $ay \in \mathfrak{p}$. Da $a \notin \mathfrak{p}$ folgt $y \in \mathfrak{p}$ und damit $\mathfrak{p} = \mathfrak{c}^{-1}\mathfrak{p}$ und da die gebrochenen Ideale eine Gruppe bilden ist $\mathfrak{c}^{-1} = R$ also $\mathfrak{c} = R$ und damit ist $\mathfrak{p}$ maximal.

Nun zum Zusatz: Wir zeigen zunaechst, dass jedes Ideal als Produkt von Primidealen geschrieben werden kann. Sei S die Menge aller Ideale ohne Primzerlegung. **Angenommen**, $S \neq \emptyset$. Sei L eine linear geordnete Teilmenge von S und sei $\mathcal{A} = \bigcup_{\mathfrak{a} \in L} \mathfrak{a}$. Dann ist das Ideal $\mathcal{A}$ endlich erzeugt, es gibt dann ein $\mathfrak{a} \in L$, das alle Erzeuger enthaelt und damit ist $\mathfrak{a} = \mathcal{A}$ eine obere Schranke zu L. Nach dem Lemma von Zorn hat S ein maximales Element $\mathfrak{s}$. Das Ideal $\mathfrak{s}$ liegt in einem maximalen Ideal $\mathfrak{p}$. Nach Lemma

3.2.11 gilt

$$s \subsetneq sp^{-1} \subset pp^{-1} = R.$$

Da s maximal in S, has sp^{-1} eine Primidealzerlegung, also $sp^{-1} = p_1 \cdots p_r$ und damit

$$a = a\,p^{-1}p = p_1 \cdots p_r p,$$

ein **Widerspruch** zu der Tatsache $a \in S$.

Zur Eindeutigkeit: Seien $a = p_1 \cdots p_r = q_1 \cdots q_s$ zwei Zerlegungen. Dann teilt p_1 eines der q_j, sagen wir q_1. Da q_1 maximal ist, folgt $p_1 = q_1$. Multiplikation mit p_1^{-1} (Lemma 3.2.11) liefert $p_2 \cdots p_r = q_2 \cdots q_s$ und Iteration liefert die Behauptung. □

Korollar 3.2.16. *Sei R ein Dedekind-Ring, $n \in \mathbb{N}$ und p ein Primideal von R, dann hat R/p^n hat nur die Ideale $p^0, p, p^2, \ldots, p^n$ und jedes Ideal p^j wird von einem beliebigen Element $u \in p^j \setminus p^{j+1}$ erzeugt, ist also ein Hauptideal.*

Proof. Zwischen p^n und R gibt nur die Ideale $R = p^0, p, p^2, \ldots, p^n$, also hat R/p^n nur diese Ideale. Ist dann $u \in p^j \setminus p^{j+1}$, dann muss $uR = p^j$ sein. □

Definition 3.2.17. Wir schreiben $\mathcal{J}_R$ fuer die Gruppe der gebrochenen Ideale von R. Sie wird auch die **Idealgruppe** genannt.

Satz 3.2.18. *Sei R ein Dedekind-Ring. Dann gilt*

$$R \text{ faktoriell} \quad \Leftrightarrow \quad R \text{ Hauptidealring}.$$

Beweis. Sei R faktoriell. Da jedes Ideal Produkt von Primidealen ist, reicht es zu zeigen, dass jedes Primideal ein Hauptideal ist. Sei also p ein Primideal und sei $p \neq 0$. Da jedes Element ein Produkt von Primelementen ist, muss p ein Primelement p enthalten. Dann ist $0 \neq pR \subset p$ ebenfalls ein Primideal und da jedes Primideal $\neq 0$ schon maximal ist, ist $pR = p$, also ist R ein Hauptidealring. Die Umkehrung ist trivial. □

Proposition 3.2.19. *Ist A ein Dedekind-Ring mit Quotientenkoerper K, so ist jede Lokalisierung $S^{-1}A$, die nicht gleich K ist, ein Dedekind-Ring.*

Beweis. Sei $a \neq 0$ ein Ideal von $S^{-1}A$. Dann ist $I = a \cap A \neq 0$ ein Ideal von A. Daher existiert ein gebrochenes Ideal J, so dass $IJ = A$. Dann sind $S^{-1}I = a$ und $S^{-1}J$ gebrochene Ideale von $S^{-1}A$ und es gilt $a\left(S^{-1}J\right) = S^{-1}(IJ) = S^{-1}A$. □

Proposition 3.2.20. *Sei R ein Dedekind-Ring und sei $\mathfrak{p} \neq 0$ ein Primideal von R. Dann ist $k = R/\mathfrak{p}$ ein Koerper und fuer jedes $\nu \in \mathbb{N}$ ist $\mathfrak{p}^\nu/\mathfrak{p}^{\nu+1}$ ein k-Vektorraum der Dimension 1.*

Beweis. Es ist $\mathfrak{p}^\nu \supset \mathfrak{p}^{\nu+1}$ und wegen der Eindeutigkeit der Primidealzerlegung sind die beiden verschieden. Sei also $a \in \mathfrak{p}^\nu \setminus \mathfrak{p}^{\nu+1}$, dann gilt

$$\mathfrak{p}^\nu \supset (a, \mathfrak{p}^{\nu+1}) \supsetneq \mathfrak{p}^{\nu+1}.$$

Wegen der Eindeutigkeit der Primidealzerlegung folgt dann $\mathfrak{p}^\nu = (a, \mathfrak{p}^{\nu+1})$, also ist der k-Vektorraum $\mathfrak{p}^\nu/\mathfrak{p}^{\nu+1}$ von dem Element $a + \mathfrak{p}^{\nu+1}$ erzeugt. □

Korollar 3.2.21. *Sei R ein Dedekind-Ring.*

(a) *Jedes gebrochene Ideal kann als Quotient $\frac{\mathfrak{a}}{\mathfrak{b}} = \mathfrak{a}\mathfrak{b}^{-1}$ geschrieben werden mit ganzen Idealen $\mathfrak{a}, \mathfrak{b} \subset R$.*

(b) *fuer jedes Ideal $\mathfrak{a}$ gilt*

$$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subset R\}.$$

(c) *Die Idealgruppe ist die freie abelsche Gruppe erzeugt von den Primidealen $\mathfrak{p} \neq 0$.*

Beweis. (a) Sei $\mathfrak{m}$ ein gebrochenes Ideal. Dann existiert ein $\beta \in R$ mit $\beta\mathfrak{m} \subset R$. Seien dann $\mathfrak{a} = \beta\mathfrak{m}$ sowie $\mathfrak{b} = \beta R$. Dann sind $\mathfrak{a}$ und $\mathfrak{b}$ ganz und es gilt $\mathfrak{m} = \mathfrak{a}\mathfrak{b}^{-1}$.

(b) Sei $\tilde{\mathfrak{a}}$ die rechte Seite. Man sieht leicht, dass $\tilde{\mathfrak{a}}$ ein gebrochenes Ideal ist. Wegen $\mathfrak{a}^{-1}\mathfrak{a} = R$ gilt $\mathfrak{a}^{-1} \subset \tilde{\mathfrak{a}}$. Andererseits gilt $\tilde{\mathfrak{a}}\mathfrak{a} \subset R = \mathfrak{a}^{-1}\mathfrak{a}$. Multipliziert man mit $\mathfrak{a}^{-1}$, erhaelt man $\tilde{\mathfrak{a}} \subset \mathfrak{a}^{-1}$, also insgesamt $\mathfrak{a}^{-1} = \tilde{\mathfrak{a}}$.

(c) Es ist zu zeigen, dass jedes gebrochene Ideal $\mathfrak{m}$ eine Darstellung besitzt mit

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{v(\mathfrak{p})}$$

mit eindeutig bestimmten $v(\mathfrak{p}) \in \mathbb{Z}$. Die Existenz einer solchen Darstellung folgt aus Teil (a), da $\mathfrak{a}$ und $\mathfrak{b}$ Primidealzerlegungen besitzen. Fuer die Eindeutigkeit sei etwa

$$\mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_n^{k_n} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

fuer $k_j, r_j \in \mathbb{Z}$ und paarweise verschiedenen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Wir muessen zeigen, dass $k_j = r_j$ fuer jedes j gilt. Wir multiplizieren mit $\left(\mathfrak{p}_1 \cdots \mathfrak{p}_1\right)^m$ fuer ein $m \in \mathbb{N}$

und erhalten

$$\mathfrak{p}_1^{k_1+m}\cdots\mathfrak{p}_n^{k_n+m} = \mathfrak{p}_1^{r_1+m}\cdots\mathfrak{p}_n^{r_n+m}.$$

Ist m hinreichend gross, dann sind alle Potenzen ≥ 0 und die Eindeutigkeit der Primidealzerlegung liefert $k_j + m = r_j + m$ fuer jedes j. □

Definition 3.2.22. Die Hauptideale aR, $a \in K^\times$ definieren eine Untergruppe $\mathcal{H}_R \cong K^\times/R^\times$ von $\mathcal{J}_R$. Die Quotientengruppe

$$\mathcal{C}\ell_R = \mathcal{J}_R/\mathcal{H}_R$$

heisst die **Idealklassengruppe** von R. Es gibt eine natuerliche exakte Sequenz

$$1 \to R^\times \to K^\times \to \mathcal{J}_R \to \mathcal{C}\ell_R \to 1.$$

Definition 3.2.23. Ist K ein Zahlkoerper, so schreibt man auch $\mathcal{J}_K$ und $\mathcal{C}\ell_K$ statt $\mathcal{J}_{O_K}$ und $\mathcal{C}\ell_{O_K}$, sowie $\mathcal{H}_K$ statt $\mathcal{H}_{O_K}$.

* * *

3.3 Erweiterungen von Dedekindringen

Definition 3.3.1. Sei A ein Dedekind-Ring und $\mathfrak{p} \subset A$ ein Primideal $\mathfrak{p} \neq 0$. Dann ist

$$k_\mathfrak{p} := A/\mathfrak{p}$$

ein Koerper, den man den **Restklassenkoerper** am Ideal $\mathfrak{p}$ nennt. Die Charakteristik

$$\mathrm{char}(A/\mathfrak{p})$$

nennt man die **Restklassencharakteristik**.

Lemma 3.3.2. *Sei R/k eine endliche Ringerweiterung, wobei k ein Koerper ist und R integer. Dann ist R ebenfalls ein Koerper.*

Proof. Nach Voraussetzung ist R ein endlich-dimensionaler k-Vektorraum. Sei $r \in R \setminus \{0\}$. Da R integer ist, hat die k-lineare Abbildung $M_r : x \mapsto rx$ trivialen Kern, ist also injektiv und da $\dim_k(R) < \infty$, ist sie auch surjektiv. Es gibt also ein $r' \in R$, so dass $1 = M_r(r') = rr'$. Damit ist r invertierbar, R also ein Koerper. □

Satz 3.3.3. *Sei A ein Dedekind-Ring mit Quotientenkoerper K. Sei L/K eine endliche separable Erweiterung und sei B der ganze Abschluss von A in L. Dann ist auch B ein Dedekind-Ring.*

Als A-Modul ist B endlich-erzeugt.

Beweis. Wir zeigen zuerst, dass B noethersch ist. Sei $\alpha_1, \dots, \alpha_n$ eine Basis von L/K, die in B liegt. Sei $d = D(\alpha_1, \dots, \alpha_n)$ die Diskriminante. Nach Lemma 2.3.5 liegt B in dem endlich erzeugten A-Modul $A\frac{\alpha_1}{d} + \cdots + A\frac{\alpha_n}{d}$ und ist nach Satz 3.1.5 ein endlich-erzeugter A-Modul und nach demselben Satz ist B ein noetherscher A-Modul und damit erst recht noethersch als B-Modul. Nebenbei haben wir gesehen, dass B als A-Modul endlich-erzeugt ist.

Als ganzer Abschluss von A ist B ganzabgeschlossen. Sei nun $\mathcal{P} \neq 0$ ein Primideal von B. Wir zeigen, dass das Primideal $\mathfrak{q} = A \cap \mathcal{P}$ ungleich Null ist. Ist $0 \neq \alpha \in \mathcal{P}$ und ist $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ das Minimalpolynom von α, dann folgt $a_0 \neq 0$ und aus $f(\alpha) = 0$ folgt $a_0 \in A \cap \mathcal{P}$.
Dann ist also $\mathfrak{q} \neq 0$ und der Integritaetsring $R = B/\mathcal{P}$ ist eine endliche Ringerweiterung des Koerpers $k = A/\mathfrak{q}$, nach Lemma 3.3.2 also ein Koerper und damit ist $\mathcal{P}$ ein maximales Ideal in B. □

Lemma 3.3.4. *Ist $\mathfrak{q}$ ein Primideal von A, dann ist $\mathfrak{q}B \neq B$.*

Beweis. Sei $\pi \in \mathfrak{q} \setminus \mathfrak{q}^2$, dann ist $\pi A = \mathfrak{q}\mathfrak{a}$, wobei $\mathfrak{a}$ teilerfremd zu $\mathfrak{q}$ ist, also gilt $\mathfrak{q} + \mathfrak{a} = A$. Schreibe entsprechend $1 = a + b$ mit $b \in \mathfrak{q}$ und $a \in \mathfrak{a}$. Es folgt $a \notin \mathfrak{q}$ und $a\mathfrak{q} \subset \mathfrak{q}\mathfrak{a} = \pi A$. Waere nun $\mathfrak{q}B = B$, so folgte $aB = a\mathfrak{q}B \subset \pi B$, also $a = \pi x$ mit $x \in B$. Sei $K = \mathrm{Quot}(A)$, dann ist $x = \frac{a}{\pi} \in K$, also $x \in B \cap K = A$ und daher $a \in \pi A = \mathfrak{a}\mathfrak{q} \subset \mathfrak{q}$, also $a \in \mathfrak{q}$. Widerspruch! □

Definition 3.3.5. Es gibt also demnach eine eindeutig bestimmte Primidealzerlegung

$$\mathfrak{q}B = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_k^{e_k}.$$

Die Zahl k heisst dann der **Zerlegungsgrad** von $\mathfrak{q}$ in B.

Die Zahl e_i heisst der **Verzweigungsgrad** des Primideals $\mathcal{P}_i$ ueber $\mathfrak{q}$. Es folgt $\mathcal{P}_i \cap A = \mathfrak{q}$ und man sagt in diesem Fall $\mathcal{P}_i$ **liegt ueber** $\mathfrak{q}$.

Die Zahl

$$f_i = [B/\mathcal{P}_i : A/\mathfrak{q}]$$

heisst der **Traegheitsgrad** von $\mathcal{P}_i$ ueber $\mathfrak{q}$.

Definition 3.3.6. (a) Ein Primideal $\mathcal{P}_i$ ueber $\mathfrak{q}$ heisst **unverzweigt**, falls $e_i = 1$ und die Restklassenkoerpererweiterung $(B/\mathcal{P}_i)/(A/\mathfrak{q})$ separabel ist. (Die zweite Bedingung ist bei Zahlringen stets erfuellt, da die Restklassenkoerper dann endlich sind.) Andernfalls heisst $\mathcal{P}_i$ **verzweigt**.

(b) Das Ideal $\mathfrak{q}$ heisst **unverzweigt**, falls alle $\mathcal{P}_i$ ueber $\mathfrak{q}$ unverzweigt sind. Sonst heisst $\mathfrak{q}$ verzweigt.

(c) Ein Primideal p in A heisst **voll zerlegt**, wenn

$$\mathfrak{q}B = \mathcal{P}_1 \cdots \mathcal{P}_n$$

mit $n = [L : K]$ verschiedenen Primidealen in B, also wenn $e_i = f_i = 1$ fuer alle i.

(d) Das Primideal $\mathfrak{q}$ heisst **unzerlegt** in B, wenn der Zerlegungsgrad gleich 1 ist (Definition 3.3.5), wenn es also nur ein Primideal $\mathcal{P}$ von B ueber $\mathfrak{q}$ gibt, also wenn

$$\mathfrak{q}B = \mathcal{P}^e$$

fuer ein $e \in \mathbb{N}$ gilt.

Beispiel 3.3.7. Betrachte $R = \mathbb{Z}[i]/\mathbb{Z}$. Es gilt $2 = (1+i)(1-i)$ und $1 - i = -i(1+i)$, also ist das Ideal $2\,\mathbb{Z}[i]$ das Quadrat des Ideals $(1+i)\,\mathbb{Z}[i]$ und da $\mathbb{Z}[i]$ als $\mathbb{Z}$-Modul von 1 und $(1+i)$ erzeugt wird, gilt $\mathbb{Z}[i]/(1+i) = \{0, 1\} = \mathbb{F}_2 = \mathbb{Z}/2$. Damit ist fuer die Primzahl 2

$$\begin{aligned} \text{Traegheitsgrad } & f = 1, \\ \text{Zerlegungsgrad } & k = 1, \\ \text{Verzeigungsgrad } & e = 2. \end{aligned}$$

Sei nun p eine Primzahl $\neq 2$. Ist p in R verzweigt, dann gibt es $\alpha = a + bi \in R$ so dass $pR = \alpha^2 R$, also sind p und α^2 assoziiert, also $p = \alpha^2 u$ mit einer Einheit und damit

$$p^2 = N(p) = \underbrace{N(u)}_{1}\, N(\alpha)^2,$$

also $N(\alpha) = N(a + bi) = a^2 + b^2$. In dem Ring $\mathbb{Z}/4$ sind die Quadrate genau die Zahlen 0

und 1. Ist also $p \equiv 3(4)$, dann hat p keine solche Darstellung, in dem Fall ist p also weder verzweigt noch zerlegt, muss also traege sein. Ist hingegen $p \equiv 1(4)$, dann stellt man mit aehnlichen Methoden fest, dass p zerlegt sein muss.

Satz 3.3.8. *Ist L/K separabel vom Grad n, so gilt*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Beweis. Nach dem chinesischen Restsatz gilt

$$B/\mathfrak{q}B \cong \bigoplus_{i=1}^{r} B/\mathcal{P}_i^{e_i}.$$

Sei $k = A/\mathfrak{q}A$ und $k_i = B/\mathcal{P}_i$, dann ist k_i/k eine Koerpererweiterung vom Grad f_i. Mit $\mathcal{P} = \mathcal{P}_i$ und $e = e_i$ gilt dann fuer den k-Vektorraum $B/\mathcal{P}$:

$$B/\mathcal{P}^e \supset \mathcal{P}/\mathcal{P}^e \supset \cdots \supset \mathcal{P}^{e-1}/\mathcal{P}^e,$$

so dass sich die Dimension aus den konsekutiven Quotienten gewinnen laesst, also gilt

$$\begin{aligned}
\dim_k B/\mathcal{P}_i^{e_i} &= \dim_k B/\mathcal{P}_i + \dim_k \mathcal{P}_i/\mathcal{P}_i^2 + \cdots + \dim_k \mathcal{P}_i^{e_i-1}/\mathcal{P}_i^{e_i} \\
&= \left(\underbrace{\dim_{k_i} B/\mathcal{P}_i}_{=1} + \underbrace{\dim_{k_i} \mathcal{P}_i/\mathcal{P}_i^2}_{=1} + \cdots + \underbrace{\dim_{k_i} \mathcal{P}_i^{e_i-1}/\mathcal{P}_i^{e_i}}_{=1} \right) f_i \\
&= e_i f_i.
\end{aligned}$$

Der Satz folgt also, wenn wir zeigen, dass $\dim_k B/\mathfrak{q}B = n$ gilt. Wir wissen, dass B ein endlich erzeugter A-Modul ist. Demnach ist dann $B/\mathfrak{q}B$ ein endlich-dimensionaler $k = A/\mathfrak{q}A$-Vektorraum. Sei $\overline{\omega}_1, \ldots, \overline{\omega}_m$ eine Basis mit Urbildern $\omega_1, \ldots, \omega_m \in B$. Wir zeigen, dass dies eine Basis von L/K ist. Angenommen, es gilt

$$a_1\omega_1 + \cdots + a_m\omega_m = 0$$

mit $a_j \in K$, wobei wir annehmen koennen, dass alle a_j in A liegen. Sei $\mathfrak{a}$ das von $a_1, \ldots, a_m$ erzeugte Ideal in A. Waehle ein $a \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{q}$. Schreiben wir $A^{\times m} = A \times \cdots \times A$

(n-mal), dann ist $\mathfrak{q}^{\times m} \subset A^{\times m}$ und

$$(aa_1, \ldots, aa_m) \in A^{\times m} \setminus \mathfrak{q}^{\times m}.$$

Modulo $\mathfrak{q}$ heisst das, dass es ein j gibt mit $\overline{aa}_j \neq 0$, was der linearen Unabhaengigkeit von $\overline{\omega}_1, \ldots, \overline{\omega}_m$ widerspricht! Damit sind die $\omega_1, \ldots, \omega_m$ ueber K linear unabhaengig.

Es bleibt zu zeigen, dass sie L aufspannen. Es gilt

$$B = \underbrace{A\omega_1 + \cdots + A\omega_m}_{=:M} + \mathfrak{q}B.$$

Mit dieser Bezeichnung ist also

$$B = \mathfrak{q}B + M,$$

was soviel bedeutet wie

$$B/M = \mathfrak{q}B/M.$$

Sei also $N = B/M$ als A-Modul, dann folgt $\mathfrak{q}N = N$. Der A-Modul N ist endlich-erzeugt, seien $\beta_1, \ldots, \beta_s$ Erzeuger. Wegen $N = \mathfrak{q}N$ gilt dann

$$\beta_j = \sum_{i=1}^{s} a_{i,j}\beta_i$$

fuer bestimmte Koeffizienten $a_{ij} \in \mathfrak{q}$. Sei R die Matrix $\left(I - (a_{ij})\right)$. Dann ist $R \equiv I \mod \mathfrak{q}$. Es gilt $R \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_s \end{pmatrix} = 0$ und $R^{\#}R = d\mathfrak{a}$ mit $d := \det R \equiv 1 \mod \mathfrak{q}$, also $d \neq 0$ und $d \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_s \end{pmatrix} = 0$. Damit sind alle β_j gleich Null, also $N = 0$. Das bedeutet $B = M = A\omega_1 + \cdots + A\omega_m$, also $L = K\omega_1 + \cdots + K\omega_m$. Damit sind die ω_j eine Basis von L/K also folgt $m = n$. Wir haben also gezeigt $\dim_k B/\mathfrak{q}B = n$ und damit ist der Satz bewiesen. □

Beispiel 3.3.9. Sei $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ und $K = \mathrm{Quot}(\mathcal{O}) = \mathbb{Q}(\sqrt{2})$. Die Primzahl 2 ist offensichtlich verzweigt. Wir werden spaeter sehen, dass $\mathcal{O}$ ein Hauptidealring ist. Sei p eine ungerade Primzahl und $\mathbb{F}_p = \mathbb{Z}/p$ der endliche Koerper. Gauss hat gezeigt, dass

$$\sqrt{2} \in \mathbb{F}_p \quad \Leftrightarrow \quad p \equiv \pm 1 \mod 8.$$

Ist also $p \not\equiv \pm 1 (8)$ und ist $\mathfrak{P}$ ein Primideal von $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ ueber 2, dann hat der Koerper

$$\mathcal{O}/\mathfrak{P} = \mathbb{F}_p(\sqrt{2})$$

den Grad 2 ueber $\mathbb{Z}/p = \mathbb{F}_p$, also ist der Traegheitsgrad von 2 gleich dem Grad von K ueber $\mathbb{Q}$, also ist p unverzweigt und unzerlegt, also traege. Ist $p \equiv \pm 1$, dann ist der Traegheitsindex gleich 1, also ist p dann verzeeigt oder zerlegt. Wir werden spaeter lernen, dass nur solche Primzahlen verzweigt sind, die die Diskriminante teilen, also haben wir insgesamt:

$$p \text{ ist } \begin{cases} \text{verzweigt} & p = 2, \\ \text{zerlegt} & p \equiv \pm 1 (8), \\ \text{traege} & \text{sonst.} \end{cases}$$

Definition 3.3.10. Sei nun θ ein primitives Element, also $L = K(\theta)$, $\theta \in B$ mit Minimalpolynom $p(x) \in A[x]$ und sei

$$\mathcal{F}_\theta := \{b \in B : bB \subset A[\theta]\}$$

der **Fuehrer** von $A[\theta]$. Dann ist $\mathcal{F}_\theta$ ein Ideal von B.

Lemma 3.3.11. $\mathcal{F}_\theta \neq 0$.

Beweis. Sei $B = A\omega_1 + \cdots + A\omega_n$. Dann ist $A[\theta] \subset B$ ein A-Untermodul mit $K \cdot A[\theta] = K[\theta] = L$. Insbesondere liegt jedes ω_j in $K \cdot A[\theta]$, es folgt $\omega_j = k_j^{-1} a_j$ mit $a_j \in A[\theta]$ und $k_j \in K$. Also $k_j \omega_j \in A[\theta]$. Schreibt man $k_j = \frac{\alpha_j}{\beta_j}$ mit $\alpha_j, \beta_j \in A$, so folgt $\alpha_j \omega_j = \beta_j k_j \omega_j \in A[\theta]$ und daher $\alpha \omega_j \in A[\theta]$, wobei

$$0 \neq \alpha = \alpha_1 \cdots \alpha_n \in A.$$

Es ist $\alpha \in \mathcal{F}_\theta$ und die Behauptung folgt. □

Proposition 3.3.12. *Sei A ein Dedekind-Ring mit Quotientenkoerper K. Sei L/K endlich-separabel und B der ganze Abschluss von A in L. Nach dem Satz vom primitiven Element gibt es ein $\theta \in L$ so dass $L = K(\theta)$. Man kann $\theta \in B$ waehlen. Sei dann $m(x) \in A[x]$ das Minimalpolynom.*

Sei $\mathfrak{q}$ ein Primideal von A so dass $\mathfrak{q}B$ teilerfremd zum Fuehrer $\mathcal{F}_\theta$ von $A[\theta]$ ist. Sei

$$\overline{m}(x) = \overline{m}_1(x)^{e_1} \cdots \overline{m}_r(x)^{e_r}$$

die Zerlegung des Polynoms $\overline{m}(x)$ modulo $\mathfrak{q}$ in $k[x] = A/\mathfrak{q}[x]$ in verschiedene normierte irreduzible $\overline{m}_j$. Dann sind

$$\mathcal{P}_i = \mathfrak{q}B + m_i(\theta)B, \qquad i = 1, \ldots, r$$

die verschiedenen Primideale von B ueber $\mathfrak{q}$, wobei $m_i \in A[x]$ ein beliebiger Lift von $\overline{m}_i$ ist. Der Traegheitsgrad f_i von $\mathfrak{P}_i$ ist

$$f_i = \operatorname{grad}(\overline{m}_i)$$

und es gilt

$$\mathfrak{q}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Beweis. Sei $k = A/\mathfrak{q}$. Wir zeigen, dass die Abbildung $f(x) \mapsto f(\theta)$ einen Isomorphismus

$$\alpha : k[x]/\overline{m}(x) \xrightarrow{\cong} B/\mathfrak{q}B$$

induziert: Der Kern der natuerlichen Abbildung $A[x] \to B/\mathfrak{q}B$ gegeben durch $f(x) \mapsto f(\theta) + \mathfrak{q}B$ ist das Ideal $(\mathfrak{q}, m(x))$. Wegen $A[x]/(\mathfrak{q}, m(x)) = k[x]/\overline{m}(x)$ bleibt die Surjektivitaet zu zeigen. Da $\theta = \alpha(x)$ gilt, ist α surjektiv auf $A[\theta]/(A[\theta] \cap \mathfrak{q}B) \subset B/\mathfrak{q}B$. Wegen $\mathcal{F} + \mathfrak{q}B = B$ und $\mathcal{F} \subset A[\theta]$ gilt $A[\theta] + \mathfrak{q}B = B$, also $A[\theta]/(A[\theta] \cap \mathfrak{q}B) = B/\mathfrak{q}B$.

Nach Chinas Restsatz

$$k[x]/\overline{m}(x) \cong \bigoplus_{i=1}^{r} k[x]/\overline{m}_i(x)^{e_i}.$$

Die Primideale des Rings $R = k[x]/\overline{m}(x)$ sind also die Hauptideale $(\overline{m}_i)$ und $[R/\overline{m}_i : k] = \operatorname{grad} \overline{m}_i$. Der Isomorphismus $\alpha : f(x) \mapsto f(\theta)$ uebersetzt dies in die entsprechenden Aussagen ueber $B/\mathfrak{q}B$, also die Behauptung. □

Satz 3.3.13. *Sei A ein Dedekind-Ring mit Quotientenkoerper K und L/K endlich-separabel. Sei B der ganze Abschluss von A in L. Dann gibt es nur endlich viele verzweigte Primideale.*

Beweis. Sei $\theta \in B$ ein primitives Element, also $L = K(\theta)$ mit Minimalpolynom $m(x) \in A[x]$. Sei

$$d = D(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \in A$$

die Diskriminante, wobei die θ_j die Galois-Konjugate von θ sind. Dann ist jedes zu d und zum Fuehrer $\mathcal{F}$ teilerfremde Primideal unverzweigt, denn: Sei $\mathfrak{q}$ ein solches Ideal, dann ist $d \not\equiv 0 \mod \mathfrak{p}$, also hat $\overline{m}(x)$ keine mehrfachen Nullstellen. Nach Proposition 3.3.12 folgt $e_i = 1$ fuer jedes i. □

* * *

4 Minkowski-Theorie

4.1 Gitter

Sei V ein endlich-dimensionaler $\mathbb{R}$-Vektorraum. Eine Untergruppe $\Gamma \subset V$ der Gestalt

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n,$$

heisst **Gitter**, falls $v_1, \ldots, v_n$ eine Basis von V ist. Die Gruppe Γ operiert dann auf V und die Menge

$$\mathcal{F} = \left\{ x_1 v_1 + \cdots + x_n v_n : 0 \leq x_j < 1 \ \forall_j \right\}$$

ist ein Vertretersystem von V/Γ, eine sogenannte **Grundmasche** des Gitters.

Beispiel 4.1.1. Die Gruppe $\mathbb{Z}^n$ ist ein Gitter in $\mathbb{R}^n$. Jedes andere Gitter Γ ist von der Form

$$\Gamma = A\ \mathbb{Z}^n$$

fuer eine Matrix $A \in \mathrm{GL}_n(\mathbb{R})$. Man muss nur die Basisvektoren $v_1, \ldots, v_n$ als Spalten in die Matrix A schreiben.

Definition 4.1.2. Sei nun der Vektorraum V **euklidisch**, d.h., mit einem symmetrischen, positiven Skalarprodukt

$$\langle ., . \rangle : V \times V \to \mathbb{R}$$

ausgestattet. Sei $e_1, \ldots, e_n$ eine Orthonormalbasis. Die Grundmasche

$$\left\{ x_1 e_1 + \cdots + x_n e_n : 0 \leq x_j < 1 \ \forall_j \right\}$$

hat das Volumen 1. Fuer eine beliebige Basis $v_1, \ldots, v_n$ hat die Masche

$$\mathcal{F} = \left\{ x_1 v_1 + \cdots + x_n v_n : 0 \leq x_j < 1 \ \forall_j \right\}$$

das Volumen

$$\mathrm{vol}(\mathcal{F}) = |\det(A)|,$$

wobei A die Basiswechselmatrix von $e_1, \ldots, e_n$ zu $v_1, \ldots, v_n$ ist. Wegen

$$\begin{aligned}\langle v_i, v_j \rangle &= \sum_{k,l} a_{ik} a_{jl} \langle e_k, e_l \rangle \\ &= \sum_{k} a_{ik} a_{jk} = (AA^t)_{i,j}\end{aligned}$$

folgt

$$\mathrm{vol}(\mathcal{F}) = \left|\det\left(\langle v_i, v_j \rangle\right)\right|^{\frac{1}{2}}.$$

Das Volumen von $\mathcal{F}$ wird auch das **Covolumen** von Γ genannt:

$$\mathrm{covol}(\Gamma) = \mathrm{vol}(\mathcal{F}).$$

Diese Zahl ist von der Wahl der Basis und damit $\mathcal{F}$ unabhaengig, denn eine andere Basis von Γ hat eine Basiswechselmatrix in $\mathrm{GL}_n(\mathbb{Z})$ und jedes $A \in \mathrm{GL}_n(\mathbb{Z})$ erfuellt $\det(A) = \pm 1$.

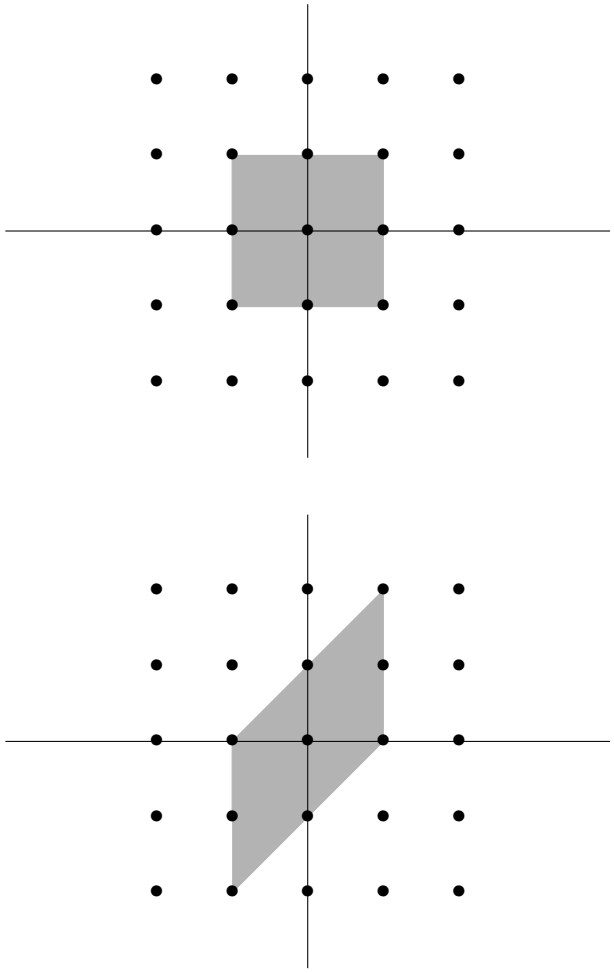
Definition 4.1.3. Eine Teilmenge $X \subset V$ heisst **symmetrisch**, falls $x \in X \Rightarrow -x \in X$. Ferner heisst sie **konvex**, falls sie mit zwei Punkten $x, y \in X$ auch deren Verbindungsstrecke $\overline{(x,y)}$ enthaelt, wenn also fuer je zwei $x, y \in X$ gilt

$$(1-t)x + ty \in X \qquad \forall_{0 \le t \le 1}.$$

Satz 4.1.4 (Minkowskischer Gitterpunktsatz)**.** *Sei $\Gamma \subset V$ ein Gitter, V euklidisch, $n = \dim V$. Sei X eine symmetrische abgeschlossene konvexe Teilmenge von V mit*

$$\mathrm{vol}(X) \ge 2^n \,\mathrm{covol}(\Gamma).$$

Dann enthaelt X mindestens ein $\gamma \in \Gamma \setminus \{0\}$.



Beweis. Sei X wie in der Voraussetzung. Fuer $\varepsilon > 0$ hat die Menge $X_\varepsilon = (1+\varepsilon)X$ Volumen $> 2^n \operatorname{covol}(\Gamma)$. Wenn wir zeigen, dass jedes X_ε einen Gitterpunkt $\gamma_\varepsilon \neq 0$ enthaelt, dann ist die Menge $\Gamma_\varepsilon = X_\varepsilon \cap \Gamma$ endlich und wegen $\Gamma_\delta \subset \Gamma_\varepsilon$ falls $\delta < \varepsilon$ muss die Menge $\Gamma \cap X \smallsetminus \{0\} = \bigcap_{\varepsilon>0} \Gamma_\varepsilon \smallsetminus \{0\}$ nichtleer sein.

Fuer den Beweis des Satzes reicht es also, anzunehmen, dass $\operatorname{vol}(X) > 2^n \operatorname{covol}(\Gamma)$ gilt. Wir zeigen zunaechst, dass es $\gamma_1 \neq \gamma_2$ in Γ gibt mit

$$\left(\gamma_1 + \frac{1}{2}X\right) \cap \left(\gamma_2 + \frac{1}{2}X\right) \neq \varnothing.$$

Waeren die Mengen $\gamma + \frac{1}{2}X$ alle paarweise disjunkt, so wuerde fuer eine Grundmasche

$\mathcal{F}$ gelten

$$\begin{aligned}\operatorname{vol}(\mathcal{F}) &\geq \sum_{\gamma\in\Gamma} \operatorname{vol}\left(\mathcal{F} \cap \left(\gamma + \frac{1}{2}X\right)\right) \\ &= \sum_{\gamma\in\Gamma} \operatorname{vol}\left(\left(\mathcal{F} - \gamma\right) \cap \frac{1}{2}X\right) \\ &= \operatorname{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\operatorname{vol}(X) > \operatorname{vol}(\mathcal{F}) \quad \text{Widerspruch!}\end{aligned}$$

Seien nun also $\gamma_1 \neq \gamma_2$ in Γ mit $\left(\gamma_1 + \frac{1}{2}X\right) \cap \left(\gamma_2 + \frac{1}{2}X\right) \neq \varnothing$. Waehle ein Element aus dem Durchschnitt, so erhalte

$$\gamma_1 + \frac{1}{2}x_1 = \gamma_2 + \frac{1}{2}x_2$$

mit $x_1, x_2 \in X$. Also folgt

$$0 \neq \underbrace{\gamma_1 - \gamma_2}_{\in\Gamma} = \frac{1}{2}(x_2 - x_1) \in \overline{(-x_1, x_2)} \subset X. \qquad \square$$

* * *

4.2 Anwendung des Gitterpunktsatzes

Definition 4.2.1. Sei K ein Zahlkoerper und sei

$$K_{\mathbb{C}} = \prod_{\tau\in\operatorname{Hom}(K,\mathbb{C})} \mathbb{C} = \mathbb{C}^{\operatorname{Hom}(K,\mathbb{C})}.$$

Beispiel 4.2.2. Wir haben $\mathbb{Q}_{\mathbb{C}} = \mathbb{C}$ und $\mathbb{Q}(i)_{\mathbb{C}} = \mathbb{C}^2$.

Definition 4.2.3. Sei $j : K \to K_{\mathbb{C}}$ die natuerliche Abbildung $j(x)_\tau = (\tau(x))$. Auf dem endlich-dimensionalen $\mathbb{C}$-Vektorraum $K_{\mathbb{C}}$ haben wir das Skalarprodukt

$$\langle u, v\rangle = \sum_\tau u_\tau \overline{v_\tau}.$$

Sei $F : \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation. F operiert auf den Faktoren von $K_{\mathbb{C}}$ aber auch auf $\operatorname{Hom}(K, \mathbb{C})$. Zusammen ergibt sich eine Involution $F : K_{\mathbb{C}} \to K_{\mathbb{C}}$ definiert durch

$$\left(F(z)\right)_\tau = \overline{z_{\overline{\tau}}}.$$

Es folgt $\langle Fx, Fy\rangle = \overline{\langle x, y\rangle}$. Sei $\mathrm{Tr} : K_{\mathbb{C}} \to \mathbb{C}$ die Spur, d.h.,

$$\mathrm{Tr}(x) = \sum_{\tau} x_{\tau}.$$

Es gilt dann

$$\mathrm{Tr}(Fx) = F\,\mathrm{Tr}(x) = \overline{\mathrm{Tr}(x)}.$$

Die Komposition

$$K \xrightarrow{j} K_{\mathbb{C}} \xrightarrow{\mathrm{Tr}} \mathbb{C}$$

hat Bilder in $\mathbb{Q}$ und ist gleich der ueblichen Spurabbildung $\mathrm{Tr}_{K/\mathbb{Q}}$.

Definition 4.2.4. Sei

$$\begin{aligned} K_{\mathbb{R}} = K_{\mathbb{C}}^{F} &= \left\{z \in K_{\mathbb{C}} : Fz = z\right\} \\ &= \left\{z \in K_{\mathbb{C}} : z_{\overline{\tau}} = \overline{z_{\tau}}\right\}. \end{aligned}$$

Dies ist ein $\mathbb{R}$-Vektorraum. Fuer $z = j(a)$, $a \in K$ gilt

$$z_{\overline{\tau}} = \overline{\tau}(a) = \overline{\tau(a)} = \overline{z_{\tau}},$$

also liegt $j(K)$ in $K_{\mathbb{R}}$. Die Einschraenkung von $\langle .,. \rangle$ ist ein Skalarprodukt

$$\langle .,. \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R},$$

denn fuer $x, y \in K_{\mathbb{R}}$ gilt $F\langle x, y\rangle = \langle Fx, Fy\rangle = \langle x, y\rangle$.

Beispiel 4.2.5. Sei $K = \mathbb{Q}(i)$. Dann ist

$$\begin{aligned} K_{\mathbb{C}} &= \mathbb{C} \times \mathbb{C}, & F(z, w) &= (\overline{w}, \overline{z}), \\ K_{\mathbb{R}} &= \left\{(z, \overline{z}) \in K_{\mathbb{C}}\right\} \end{aligned}$$

und

$$\langle (z, \overline{z}), (w, \overline{w})\rangle = z\overline{w} + \overline{z}w = 2\,\mathrm{Re}(z\overline{w}).$$

Definition 4.2.6. Der Raum $K_{\mathbb{R}}$ heisst der **Minkowski-Raum** zu K, das Skalarprodukt $\langle .,. \rangle$ auf $K_{\mathbb{R}}$ die **Minkowski-Metrik** und das zugehoerige Maß μ heisst das **Minkowski-Maß**.

Definition 4.2.7. Eine komplexe Einbettung $\tau : K \hookrightarrow \mathbb{C}$ heisst **reell**, falls $\tau(K) \subset \mathbb{R}$ und **imaginaer** sonst. Eine Einbettung τ ist genau dann reell, wenn $\overline{\tau} = \tau$ gilt.

Beispiele 4.2.8. (a) Ein Zahlkoerper, der nur reelle Einbettungen besitzt, heisst **total reell**. Beispiele sind $\mathbb{Q}$ oder **reellquadratische Zahlkoerper** $\mathbb{Q}(\sqrt{d})$, wobei $d \in \mathbb{N}$ kein Quadrat.

(b) Auf der anderen Seite gibt es auch Zahlkoeper, die keine reellen Einbettungen besitzen, wie die **imaginaerquadratischen Zahlkoerper** $\mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$, $d < 0$.

(c) In der Regel wird ein Zahlkoerper aber beides besitzen, wie zum Beispiel $\mathbb{Q}(\sqrt[3]{2})$, der 2 imaginaere und eine reelle Einbettung besitzt. Die Anzahl aller Einbettungen ist stets gleich $n = [K/\mathbb{Q}]$, da $K/\mathbb{Q}$ separabel ist.

Definition 4.2.9. Seien $\rho_1, \ldots, \rho_r : K \to \mathbb{R}$ die reellen und

$$\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$$

die imaginaeren Einbettungen, so dass also $n = r + 2s$ gilt. Der **Typ** des Zahlkoerpers K ist das Tupel (r, s).

Proposition 4.2.10. *Wir haben einen Isomorphismus reller Vektorraeume*

$$\begin{aligned} f : K_{\mathbb{R}} &\xrightarrow{\cong} \mathbb{R}^{r+2s}, \\ x &\mapsto (x_{\rho_1}, \ldots, x_{\rho_r}, \operatorname{Re} x_{\sigma_1}, \operatorname{Im} x_{\sigma_1}, \ldots, \operatorname{Re} x_{\sigma_s}, \operatorname{Im} x_{\sigma_s}). \end{aligned}$$

Die Minkowski-Metrik wird hierbei ueberfuehrt in

$$\langle x, y \rangle = \sum_{i=1}^{r} x_i y_i + 2 \sum_{i=r+1}^{r+2s} x_i y_i.$$

Beweis. Isomorphie klar, Rest durch Rechnung. □

Satz 4.2.11. *Ist $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}_K$, so ist $\Gamma = j(\mathfrak{a})$ ein Gitter in $K_{\mathbb{R}}$ mit Covolumen*

$$\operatorname{covol}(\Gamma) = \sqrt{|D_K|}\, \left|\mathcal{O}_K/\mathfrak{a}\right|.$$

Beweis. Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$, dann ist

$$\Gamma = \mathbb{Z} j(\alpha_1) + \cdots + \mathbb{Z} j(\alpha_n).$$

Seien $\tau_1, \dots, \tau_n : K \to \mathbb{C}$ die komplexen Einbettungen und sei A die Matrix $(\tau_i \alpha_j)_{i,j}$. Dann gilt nach Definition der Diskriminante

$$D(\mathfrak{a}) = D(\alpha_1, \dots, \alpha_n) = (\det(A))^2.$$

Nach Satz 2.3.14 gilt

$$D(\mathfrak{a}) = \left|O_K/\mathfrak{a}\right|^2 D_K.$$

Ferner gilt

$$\left(\left\langle j(\alpha_i), j(\alpha_j) \right\rangle \right)_{i,j} = \sum_{l=1}^{n} \tau_l(\alpha_i)\overline{\tau}_l(\alpha_j) = (A^t \overline{A})_{i,j}.$$

Also

$$\operatorname{covol}(\Gamma) = \left|\det\left(\left\langle j(\alpha_i), j(\alpha_j) \right\rangle\right)\right|^{\frac{1}{2}} = |\det(A)| = \sqrt{|D_k|}\ \left|O_K/\mathfrak{a}\right|. \qquad \square$$

Beispiele 4.2.12.

(a) Fuer $K = \mathbb{Q}(i)$ betrachten wir nur eine komplexe Einbettung und $\Gamma = O = \mathbb{Z}[i]$ ist ein Gitter in $\mathbb{C}$.

(b) Sei $K = \mathbb{Q}(\sqrt{2})$. Dann ist $K_{\mathbb{R}} = \mathbb{R} \times \mathbb{R}$ und O_K ist dann die Menge aller Vektoren der Form $(a - b\sqrt{2}, a + b\sqrt{2})$ mit $a, b \in \mathbb{Z}$. Eine Basis ist etwa $v_1 = (1, 1)$ und $v_2 = (-\sqrt{2}, \sqrt{2})$, so dass die Basiswechselmatrix von der Standard-Basis gleich

$$\begin{pmatrix} 1 & -\sqrt{2} \\ 1 & \sqrt{2} \end{pmatrix}$$

ist. Die Determinante ist $2\sqrt{2} = \sqrt{8} = \sqrt{D_K}$.

Satz 4.2.13. *Sei K ein Zahlkoerper vom Typ (r, s) und sei $0 \neq \mathfrak{a} \subset O_K$ ein Ideal. Fuer jedes $\tau \in \operatorname{Hom}(K, \mathbb{C})$ sei eine reelle Zahl $c_\tau > 0$ gegeben so dass $c_{\overline{\tau}} = c_\tau$ fuer jedes τ und*

$$\prod_{\tau \in \operatorname{Hom}(K,\mathbb{C})} c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}\ \left|O_K/\mathfrak{a}\right|$$

gilt. Dann gibt es ein $a \in \mathfrak{a} \setminus \{0\}$ mit

$$|\tau(a)| < c_\tau$$

fuer jedes $\tau \in \mathrm{Hom}(K, \mathbb{C})$.

Beweis. Die Menge $X = \left\{(z_\tau)_\tau \in K_{\mathbb{R}} : |z_\tau| < c_\tau\right\}$ ist symmetrisch und konvex. Fuer das Volumen gilt

$$\begin{aligned}
\mathrm{vol}(X) &= 2^s \,\mathrm{vol}_{\mathrm{Lebesgue}}(X) \\
&= 2^s \,\mathrm{vol}_{\mathrm{Lebesgue}}\left(\left\{(z_\tau) \in \prod_\tau \mathbb{R} : |z_\rho| < c_\rho,\ x_\sigma^2 + y_\sigma^2 < c_\sigma^2\right\}\right) \\
&= 2^s \prod_\rho (2c_\rho) \prod_\sigma \left(\pi c_\sigma^2\right) = 2^{r+s}\pi^s \prod_\tau c_\tau \\
&> 2^{r+2s}\sqrt{|D_K|}\ \left|\mathcal{O}_K/\mathfrak{a}\right| = 2^n \,\mathrm{covol}(\Gamma).
\end{aligned}$$

Nach dem Minkowskischen Gitterpunktsatz 4.1.4 folgt die Behauptung. □

Proposition 4.2.14. *Zu gegebenem* $N \in \mathbb{N}$ *und* $T > 0$ *gibt es nur endlich viele Zahlkoerper* K *vom Grad* $n \le N$ *und* $|D_K| \le T$.

Beweis. Sei K ein Zahlkoerper und sei $L = K\left(\sqrt{-1}\right) = K(i)$. Ist $L \neq K$, dann gilt $L = \mathbb{Q}(i)\ K$ und daher nach Satz 2.3.15:

$$D_L = 4^n D_K^2.$$

Ist also $D_K \le T$, dann ist $D_L \le 4^n T^2$. Der Koerper L ist rein imaginaer. Daher reicht es, zu zeigen, dass es nur endlich viele rein imaginaere Zahklkoerper K vom Grad $n \le N$ und $D_K \le T$ gibt.

Nach dem Gitterpunktsatz gibt es ein $C > 0$, so dass in jedem imaginaeren Zahlkoerper K ein $\alpha \in \mathcal{O}_K$ und eine Einbettung $\tau_0 : K \to \mathbb{C}$ existiert, so dass

$$|\mathrm{Im}(\tau_0(\alpha))| < C\sqrt{|D_K|}, \qquad |\mathrm{Re}(\tau_0(\alpha))| < 1, \qquad |\tau(\alpha)| < 1 \ \text{ fuer } \tau \neq \tau_0, \overline{\tau}_0. \qquad (*)$$

Dieses α ist dann ein primitives Element von K, also $K = \mathbb{Q}(\alpha)$, denn $\prod_\tau |\tau(\alpha)| = |N(\alpha)| \ge 1$ liefert $|\tau_0(\alpha)| > 1$, also $\mathrm{Im}(\tau_0(\alpha)) \neq 0$. Da $|\tau(\alpha)| < 1$ fuer $\tau \neq \tau_0, \overline{\tau}_0$, folgt $\tau_0(\alpha) \neq \tau(\alpha)$ fuer alle $\tau \neq \tau_0$, also $K = \mathbb{Q}(\alpha)$, denn andernfalls wuerde die Einschraenkung $\tau_0|_{\mathbb{Q}(\alpha)}$ eine Erweiterung $\tau \neq \tau_0$ nach K haben, was $\tau_0(\alpha) \neq \tau(\alpha)$ widerspricht. Alle Konjugierten $\tau(\alpha)$ von α erfuellen $(*)$, daher sind die Koeffizienten

des Minimalpolynoms beschraenkt durch Konstanten, die nur von N und T abhaengen. Also gibt es nur endlich viele solcher Polynome. □

* * *

4.3 Die Klassenzahl

Fuer ein Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}_K$ sei die **Norm** definiert durch

$$N(\mathfrak{a}) = \left|\mathcal{O}_K/\mathfrak{a}\right|.$$

Lemma 4.3.1. *Ist $\mathfrak{a}$ ein Hauptideal, also $\mathfrak{a} = (a) = a\mathcal{O}_K$, so gilt*

$$N(\mathfrak{a}) = |\mathrm{N}_{K/\mathbb{Q}}(a)|.$$

Dies rechtfertigt den Namen Norm.

Beweis. Ist $v_1, \ldots, v_n$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$, dann ist $av_1, \ldots, av_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$. Ist $A = (a_{ij}) \in \mathrm{M}_n(\mathbb{Z})$ die Basiswechselmatrix, also

$$av_j = \sum_i a_{ij} v_i,$$

so ist einerseits $|\det(A)| = \left|\mathcal{O}_K/\mathfrak{a}\right|$ und andererseits $\det(A) = \mathrm{N}_{K/\mathbb{Q}}(a)$ nach Definition. □

Satz 4.3.2. *Ist $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ die Primzerlegung eines Ideals $\mathfrak{a} \neq 0$ im Ganzzahlring $\mathcal{O}_K$ eines Zahlkoerpers, so gilt*

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{\nu_1} \cdots N(\mathfrak{p}_r)^{\nu_r}.$$

Beweis. Nach Chinas Restsatz ist

$$\mathcal{O}_K/\mathfrak{a} \cong \bigoplus_j \mathcal{O}/\mathfrak{p}_j^{\nu_j}.$$

Daher koennen wir $\mathfrak{a} = \mathfrak{p}^\nu$ annehmen. Sei dann k der endliche Koerper $\mathcal{O}_K/\mathfrak{p}$. Nach Proposition 3.2.20 ist $\dim_k \mathfrak{p}^\nu/\mathfrak{p}^{\nu+1} = 1$, also $|\mathfrak{p}^\nu/\mathfrak{p}^{\nu+1}| = N(\mathfrak{p})$. Es folgt also

$$N(\mathfrak{p}^\nu) = \left|\mathcal{O}_K/\mathfrak{p}^\nu\right| = \left|\mathcal{O}_K/\mathfrak{p}\right| \, \left|\mathfrak{p}/\mathfrak{p}^2\right| \cdots \left|\mathfrak{p}^{\nu-1}/\mathfrak{p}^\nu\right| = N(\mathfrak{p})^\nu. \qquad \square$$

Da die Primideale die Idealgruppe erzeugen, liefert die Norm damit also einen Homomorphismus der Idealgruppe

$$N : \mathcal{J}_K \to \mathbb{R}^\times.$$

Lemma 4.3.3. *Sei K ein Zahlkoerper vom Grad $n = r + 2s$.*

(a) *Sei*

$$X_T = \left\{(z_\tau) \in K_\mathbb{R} : \sum_\tau |z_\tau| \le T\right\}.$$

Dann gilt $\mathrm{vol}(X_T) = 2^{r+s}\pi^s \frac{T^n}{n!}$.

(b) *Jedes Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}_K$ enthaelt ein $a \neq 0$, so dass*

$$|N_{K/\mathbb{Q}}(a)| \le |\mathcal{O}_K/\mathfrak{a}| \, \frac{n!}{n^n}\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}.$$

Beweis. (a) Wir muessen zeigen, dass fuer

$$X_{r,s} = \left\{(x,z) \in \mathbb{R}^r \times \mathbb{C}^s : |x_1| + \cdots + |x_r| + 2|z_1| + \cdots + 2|z_s| < 1\right\}$$

gilt

$$\mathrm{vol}(X_{r,s}) = \frac{2^{r+s}\pi^s}{(r+2s)!}.$$

Wir zeigen dies durch Induktion nach r und s. Fuer $r = s = 0$ sind beide Seiten gleich 1.

$(r,s) \to (r+1,s)$:
Wir rechnen

$$\begin{aligned}\mathrm{vol}(X_{r+1,s}) &= \int_{-1}^{1} \mathrm{vol}((1-|t|)X_{r,s})\,dt = 2\int_0^1 t^{r+2s}\,\mathrm{vol}(X_{r,s})\,dt \\ &= 2\frac{2^{r+s}\pi^s}{(r+2s)!}\;\frac{t^{r+2s+1}}{r+2s+1}\Big|_{t=0}^{t=1} = \frac{2^{r+1+s}\pi^s}{(r+1+2s)!}.\end{aligned}$$

$(r,s) \to (r,s+1)$:

Sei $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$. Mit Polarkoordinaten rechnen wir

$$\begin{aligned}
\mathrm{vol}(X_{r,s+1}) &= \int_{\mathbb{D}} \mathrm{vol}\left((1-|z|)X_{r,s}\right)\, dx\,dy = \int_{\mathbb{D}} (1-|z|)^{r+2s}\ \mathrm{vol}\left(X_{r,s}\right)\, dx\,dy \\
&= \frac{2^{r+s}\pi^s}{(r+2s)!}\, 2\pi \int_0^1 t(1-t)^{r+2s}\, dt \\
&= \frac{2^{r+s}\pi^s}{(r+2s)!}\, 2\pi \int_0^1 t^{r+2s}(1-t)\, dt \\
&= \frac{2^{r+s+1}\pi^{s+1}}{(r+2s)!}\, \Big(\int_0^1 t^{r+2s}\, dt - \int_0^1 t^{r+1+2s}\, dt \Big) \\
&= \frac{2^{r+s+1}\pi^{s+1}}{(r+2s)!}\, \Big(\frac{1}{r+1+2s} - \frac{1}{r+2+2s} \Big) \\
&= \frac{2^{r+s+1}\pi^{s+1}}{(r+2(s+1))!}.
\end{aligned}$$

(b) Nach dem Satz von Minkowski enthaelt X_T ein Element a von $\mathfrak{a}$, falls $2^{r+s}\pi^s \frac{T^n}{n!} \geq 2^n |O/\mathfrak{a}| \sqrt{D_K}$. Man setzt nun $T^n = 2^n |O/\mathfrak{a}| \sqrt{D_K}\, n!\, 2^{-r-s}\pi^{-s} = \left(\frac{2}{\pi}\right)^s n!\, |O/\mathfrak{a}| \sqrt{D_K}$. Mit der Ungleichung

$$\frac{1}{n} \sum_\tau |z_\tau| \geq \left(\prod_\tau |z_\tau| \right)^{\frac{1}{n}}$$

folgt dann fuer dieses a, dass

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}}(a) = \prod_\tau |\tau(a)| &\leq \frac{1}{n^n} \left(\sum_\tau |\tau(a)| \right)^n \\
&\leq \frac{T^n}{n^n} = \frac{1}{n^n} \left(\frac{2}{\pi}\right)^s n! |O/\mathfrak{a}| \sqrt{D_K}
\end{aligned}$$

□

Satz 4.3.4 (Endlichkeit der Klassenzahl)**.** *Sei K ein Zahlkoerper vom Grad $n = r + 2s$. Jede Idealklasse enthaelt ein Ideal $\mathfrak{a}$ von $O = O_K$ mit*

$$N(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}.$$

Die Idealklassengruppe $\mathcal{CL}_K = \mathcal{J}_K/\mathcal{H}_K$ ist endlich. Ihre Kardinalitaet $h(K)$ wird die **Klassenzahl** *von K genannt.*

Beweis. Sei $\mathfrak{a}$ ein Repraesentant und sei $\gamma \in O_K$ mit $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subset O_K$. Dann gibt es nach

Lemma 4.3.3 ein $0 \neq b \in \mathfrak{b}$ mit

$$|\mathrm{N}_{K/\mathbb{Q}}(b)| \leq \frac{n!}{n^n}\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}N(\mathfrak{b}).$$

Dividieren wir durch $N(\mathfrak{b})$, wird das

$$|\mathrm{N}_{K/\mathbb{Q}}(b)|\, N\left(\mathfrak{b}\right)^{-1} = N\left(b\mathfrak{b}^{-1}\right) \leq \frac{n!}{n^n}\left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}.$$

Das Ideal $\mathfrak{a}_1 = b\mathfrak{b}^{-1} = b\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$ hat also die gewuenschte Eigenschaft.

Fuer die Endlichkeit der Klassenzahl sei $\mathfrak{p} \neq 0$ ein Primideal von $\mathcal{O}_K$ und sei p die Primzahl unter $\mathfrak{p}$, d.h., es gelte $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Dann ist der Koerper $\mathcal{O}_K/\mathfrak{p}$ eine endliche Erweiterung von $\mathbb{Z}/p\mathbb{Z}$. Sei f der Grad dieser Erweiterung. Es ist dann

$$N(\mathfrak{p}) = p^f.$$

Es gibt nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, da jedes solche $\mathfrak{p}$ ein Teiler des Hauptideals $p\mathcal{O}_K$ ist. Daher gibt es zu gegebenem $S > 0$ nur endlich viele Primideale $\mathfrak{p}$ mit $N(\mathfrak{p}) \leq S$. Wegen $N(\mathfrak{a}) = N(\mathfrak{p}_1)^{\nu_1} \cdots N(\mathfrak{p}_r)^{\nu_r}$ falls $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ gibt es nur endlich viele Ideale $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq S$. Fuer $S = \left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}$ folgt nach der ersten Aussage die Behauptung. □

Beispiele 4.3.5. (a) $K = \mathbb{Q}(\sqrt{2})$ hat Klassenzahl 1. Wir haben $s = 0$ und $D_K = 8$, also hat jede Idealklasse einen Vertreter $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq 1$ also $\mathfrak{a} = \mathcal{O}_K$ und das ist ein Hauptideal.

(b) $K = \mathbb{Q}\left(\sqrt{-7}\right)$ hat Klassenzahl 1.

Beweis. Da $-7 \equiv 1 \mod 4$, ist $\mathcal{O}_K = \mathbb{Z}[\alpha]$ mit $\alpha = \frac{\sqrt{-7}+1}{2}$ und $D_K = -7$. Es gilt $\alpha(\alpha - 1) = \frac{\sqrt{-7}+1}{2}\frac{\sqrt{-7}-1}{2} = \frac{-7-1}{4} = -2$. Also folgt $\alpha^2 - \alpha + 2 = 0$. Da $2 < \sqrt{7} < 3$, hat nach Satz 4.3.4 jede Idealklasse einen Vertreter $\mathfrak{a} \subset \mathcal{O}_K$ mit $N(\mathfrak{a}) \leq 1$, also $\mathfrak{a} = \mathcal{O}_K$ und das ist ein Hauptideal. □

(c) $K = \mathbb{Q}\left(\sqrt{13}\right)$ hat Klassenzahl 1.

Beweis. Da $13 \equiv 1 \mod 4$ ist $\mathcal{O} = \mathbb{Z}[\beta]$ mit $\beta = \frac{\sqrt{13}+1}{2}$ und $D_K = 13$. Es gilt $\beta(\beta - 1) = \frac{\sqrt{13}+1}{2}\frac{\sqrt{13}-1}{2} = 3$, also $\beta^2 - \beta - 3 = 0$. Da $3 < \sqrt{13} < 4$, hat nach Satz 4.3.4 jede Idealklasse einen Vertreter $\mathfrak{a} \subset \mathcal{O}$ mit $N(\mathfrak{a}) \leq 1$. Wieder folgt die Behauptung. □

(d) Liste einiger Zahlkoerper $\mathbb{Q}(\sqrt{d})$

d	-1	-2	-3	-5	-6
	1	1	1	2	2

d	2	3	5	6	7
	1	1	2	2	1

Bemerkung 4.3.6. Gauß vermutete, dass die einzigen Imaginaerquadratischen Zahlkoerper der Klassenzahl 1 die mit den Diskriminanten

$$-3, -4, -7, -8, -11, -19, -43, -67, -163$$

sind. Dies wurde 1967 von Harold Stark bewiesen. Gauß vermutete weiter, dass es nur endlich viele reell-quadratische Zahlkoerper mit Klassenzahl 1 gibt. Diese Vermutung ist noch offen.

Satz 4.3.7. *Fuer jeden Zahlkoerper $K \neq \mathbb{Q}$ gilt $|D_K| > 1$.*

Proof. Nach dem Lemma gibt es $a \in O \setminus 0$, so dass

$$1 \leq N_{K/\mathbb{Q}}(a) \leq \frac{n^!}{n^n} \left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}.$$

Also folgt

$$\sqrt{D_K} \geq \frac{n^n}{n!} \left(\frac{\pi}{2}\right)^s > 1.$$

□

* * *

4.4 Fermats letzter Satz

Fermats letzter Satz (FLT) wurde 1994 von Andrew Wiles bewiesen, nachdem er ueber 350 Jahre ein offenes Problem darstellte. Er besagt, dass es fuer $n \in \mathbb{N}$ mit $n \geq 3$ die Gleichung

$$a^n + b^n = c^n$$

keine Loesung mit $a, b, c \in \mathbb{Z} \setminus \{0\}$ besitzt. Fuer $n = 4$ wurde der Satz von Fermat selbst bewiesen. Wegen $a^{4m} = (a^m)^4$ folgt er dann auch fuer alle Vielfachen von 4. Ist $n \geq 3$

kein Vielfaches von 4, dann gilt $n = mp$ fuer eine ungerade Primzahl p. Daher reicht es, FLT fuer ungerade Primzahlen zu beweisen.

Definition 4.4.1. Eine ungerade Primzahl p heisst **regulaere Primzahl**, falls

$$p \nmid h\big(\mathbb{Q}(\zeta_p)\big).$$

Es wird vermutet, dass etwa 60% aller Primzahlen regulaer sind.

Wir schreiben $\zeta = \zeta_p$ und $K = \mathbb{Q}(\zeta)$, sowie $O = O_K$. Wir fassen K als Teilmenge von $\mathbb{C}$ auf und schreiben $z \mapsto \overline{z}$ fuer die komplexe Konjugation. Diese liegt in $\mathrm{Gal}(K/\mathbb{Q})$ und da diese Gruppe kommutativ ist, gilt $\overline{\sigma(z)} = \sigma(\overline{z})$ fuer jedes $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Nach Satz 2.5.1 ist $O = \mathbb{Z}[\zeta]$.

Lemma 4.4.2.

(a) *Sei $\alpha \in \mathbb{C}$ algebraisch und ganz ueber $\mathbb{Z}$. Alle Galois-Konjugierten von α seien vom komplexen Betrag 1. Dann ist α eine Einheitswurzel.*

(b) *Fuer $v \in \mathbb{Z}[\zeta]^\times$ ist $v/\overline{v}$ eine Einheitswurzel.*

Proof. (a) Das Minimalpolynom von α ist

$$\begin{aligned} m(x) &= \prod_\sigma \big(x - \sigma(\alpha)\big) \\ &= \big(x - \sigma_1(\alpha)\big)\big(x - \sigma_2(\alpha)\big)\cdots\big(x - \sigma_n(\alpha)\big) \\ &= a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n, \end{aligned}$$

wobei das Produkt ueber alle Einbettungen von $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ laeuft. Es gilt

$$\begin{aligned} |a_j| &= \left| (-1)^{n-j} \sum_{\substack{A \subset \{1,2,\ldots,n\} \\ |A| = n-j}} \prod_{i \in A} \sigma_i(\alpha) \right| \\ &\le \sum_A \underbrace{\left| \prod_{i \in A} \sigma_i(\alpha) \right|}_{= \prod |\sigma_i(\alpha)| = 1} = \binom{n}{n-j} = \binom{n}{j}. \end{aligned}$$

Sei $C_n = \max_{j=0}^n \binom{n}{j}$. Dann folgt $|a_j| \le C_n$ fuer alle solchen α, deren Minimalpolynom einen Grad $\le n$ hat. Daher gibt es nur endlich viele solcher Minimalpolynome und

also nur endlich viele solcher α, Insbesondere hat α nur endlich viele Potenzen, muss also von endlicher Ordnung sein.

(b) Fuer einen Galois-Homomorphismus σ ist $\sigma(v/\overline{v}) = \sigma(v)/\overline{\sigma(v)}$ und daher haben alle Konjugierten von $v/\overline{v}$ den Betrag 1. Damit folgt Teil (b) aus Teil (a). □

Fuer den folgenden Satz beachte man, dass FLT fuer die Priemzahl $p = 3$ leicht zu beweisen ist. Also brauchen wir nur Primzahlen ≥ 5 zu betrachten.

Satz 4.4.3. *Sei p eine regulaere Primzahl ≥ 5. Dann gilt Fermats letzter Satz fuer den Exponenten p.*

Beweis. Wir nehmen das Gegenteil an, es gebe also $x, y, z \in \mathbb{Z} \setminus \{0\}$ mit $x^p + y^p = z^p$. Wir beweisen den Satz nur in dem sogenannten **1. Fall**, d.h. unter der Bedingung, dass so dass xyz teilerfremd zu p ist. Der Beweis des zweiten Falls benutzt dieselben Methoden, ist aber zu lang fuer dieses Skript.

In dem Ganzzahlring $\mathbb{Z}[\zeta_p]$ gilt

$$z^p = x^p + y^p = (x + y)(x + \zeta y)\cdots(x + \zeta^{p-1} y)$$

Zwischenbehauptung: Die Faktoren rechts sind paarweise teilerfremd in $O = \mathbb{Z}[\zeta]$. Wir zeigen dies fuer die ersten beiden, durch Umbennenung folgt daraus der allgemeine Fall. Sei $\mathfrak{a}$ das von $x + y$ und $x + \zeta y$ erzeuge Ideal von O. Dann gilt

$$\begin{aligned} y(1 - \zeta) &= (x + y) - (x + \zeta y) \in \mathfrak{a} \\ x(1 - \zeta) &= (x + \zeta y) - \zeta(x + y) \in \mathfrak{a} \end{aligned}$$

Da x und y teilerfremd sind, liegt auch $1 - \zeta$ in $\mathfrak{a}$. Das p-te Kreisteilungspolynom ist

$$\begin{aligned} C_p(x) &= \prod_{j=1}^{p-1} (x - \zeta^j) \\ &= \frac{\prod_{j=0}^{p-1} (x - \zeta^j)}{x - 1} = \frac{x^n - 1}{x - 1} = 1 + x + \cdots + x^{p-1}. \end{aligned}$$

Also folgt

$$N(1 - \zeta) = C_p(1) = 1 + 1 + \cdots + 1 = p.$$

Daher ist $\left|\mathcal{O}/(1-\zeta)\mathcal{O}\right| = p$, also ist dieser Ring ein Koerper und daher ist $(1-\zeta)\mathcal{O}$ ein Primideal, also maximal. Damit folgt $\mathfrak{a} = \mathcal{O}$ oder $\mathfrak{a} = (1-\zeta)\mathcal{O}$. **Angenommen,** $\mathfrak{a} = (1-\zeta)\mathcal{O}$, dann gibt es $\alpha, \beta \in \mathcal{O}$ mit

$$x + y = \alpha(1-\zeta),$$
$$x + \zeta y = \beta(1-\zeta).$$

Loest man dieses Gleichungssystem nach x und y auf, erhaelt man

$$y = \alpha - \beta$$
$$x = \beta - \alpha\zeta.$$

Das heisst also, dass $\alpha - \beta$ in $\mathbb{Z}$ liegt. Schreibt man

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1},$$

folgt daraus

$$\beta = b_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}.$$

Nun ist

$$\alpha\zeta = a_{p-1} + a_0\zeta + \cdots + a_{p-2}\zeta^{p-1}.$$

Da auch $\beta - \alpha\zeta \in \mathbb{Z}$, folgt $a_0 = a_1, \ldots, a_{p-2} = a_{p-1}$, also

$$\alpha = a_0(1 + \cdots + \zeta^{p-1}) = 0.$$

Widerspruch! Damit folgt $\mathfrak{a} = \mathcal{O}$ und die Zwischenbehauptung ist gezeigt.

Nun ist das Produkt der Ideale $(x + y\zeta^j)$ gleich (z^p), also eine p-te Potenz. Die Eindeutigkeit der Primidealzerlegung impliziert, dass jedes $(x + y\zeta^j)\mathcal{O}$ selbst eine p-te Potenz ist. Es gilt also

$$(x + y\zeta)\mathcal{O} = \mathfrak{a}^p$$

fuer ein Ideal $\mathfrak{a}$. Damit ist $\mathfrak{a}^p$ trivial in der Klassengruppe $\mathcal{Cl}(K)$ und da p die Gruppenordnung nicht teilt, ist $\mathfrak{a}$ selbst trivial, also ein Hauptideal, sagen wir $\mathfrak{a} = (t)$. Damit ist

$$x + y\zeta = ut^p$$

fuer eine Einheit $u \in \mathbb{Z}[\zeta]^\times$. Schreiben wir $t = b_0 + b_1\zeta + \cdots + b_{p-1}\zeta^{p-1}$ mit $b_j \in \mathbb{Z}$, dann folgt

$$\begin{aligned} t^p &\equiv b_0^p + (b_1\zeta)^p + \cdots + (b_{p-1}\zeta^{p-1})^p \\ &\equiv b_0 + b_1 + \cdots + b_{p-1} \mod p\mathbb{Z}[\zeta], \end{aligned}$$

also $t^p \equiv \overline{t}^p \mod p\mathbb{Z}[\zeta]$, wobei $\overline{t}$ die komplex Konjugierte ist.

Nach Lemma 4.4.2 ist $u/\overline{u}$ eine Einheitswurzel und nach Proposition 2.4.5 ist $u/\overline{u} = \pm\zeta^j$ fuer ein j. Ist $u/\overline{u} = \zeta^j$, dann gilt

$$\begin{aligned} x + y\zeta = ut^p &= \zeta^j\overline{u}t^p \\ &\equiv \zeta^j\overline{u}\overline{t}^p && \mod p\mathbb{Z}[\zeta_p] \\ &\equiv \zeta^j(x + y\overline{\zeta}) && \mod p\mathbb{Z}[\zeta_p]. \end{aligned}$$

Daher

$$u/\overline{u} = \zeta^j \quad \Rightarrow \quad x + y\zeta - x\zeta^j - y\zeta^{j-1} \equiv 0 \mod p\mathbb{Z}[\zeta].$$

Ebenso erhaelt man

$$u/\overline{u} = -\zeta^j \quad \Rightarrow \quad x + y\zeta + y\zeta^{j-1} + x\zeta^j \equiv 0 \mod p\mathbb{Z}[\zeta].$$

Fasst man $\mathbb{Z}[\zeta]/(p)$ als $\mathbb{F}_p = \mathbb{Z}/p$-Vektorraum auf, dann zeigen diese Kongruenzen lineare Abhaengigkeit von $1, \zeta, \zeta^{j-1}$ und ζ^j. Die Potenzen von ζ sind aber linear unabhaengig, denn

$$\mathbb{Z}[\zeta]/(p) \cong \mathbb{Z}[X]/(p, \phi_p(X)) \cong \mathbb{F}_p[X]/(X-1)^{p-1}.$$

Ist also $j \neq 0, 1, 2$, dann folgt $x \equiv 0 \mod p$, was wir ausgeschlossen hatten.

(a) Ist $j = 0$, so folgt $y \equiv 0 \mod p$, also ebenfalls ein Widerspruch.

(b) Ist $j = 2$, folgt $x \cong 0 \mod p$, Widerspruch!

(c) Bleibt also der Fall $j = 1$ dann folgt aus der Kongruenz, dass $x - y \equiv 0$, also $x \equiv y \mod p$. Wiederholt man den Beweis mit fuer die Gleichung $x^p + (-z)^p = (-y)^p$, so erhaelt man, falls wieder der Fall $j = 1$ eintritt, die zusaetzliche Gleichung $x \equiv -z \mod p$. Dann ist aber

$$x^p + x^p + x^p = 3x^p \equiv 0 \mod p.$$

Da 3 modulo p invertierbar ist, folgt $x \equiv 0 \mod p$, Widerspruch!

Damit ist FTL fuer regulaere Primzahlen unter der Teilerfremdheitsbedingung gezeigt. □

* * *

4.5 Der Dirichletsche Einheitensatz

Sei K ein Zahlkoerper, $K_{\mathbb{C}}^{\times} = \prod_{\tau} \mathbb{C}^{\times}$ die Einheitengruppe des Rings $K_{\mathbb{C}}$. Sei $j : K^{\times} \to K_{\mathbb{C}}^{\times}$ die natuerliche Abbildung. Wir haben Normabbildung

$$\begin{aligned} \mathrm{N} : K_{\mathbb{C}}^{\times} &\to \mathbb{C}^{\times}, \\ z &\mapsto \prod_{\tau} z_{\tau}, \end{aligned}$$

die das Diagramm

$$\begin{array}{ccc} K^{\times} & \xrightarrow{j} & K_{\mathbb{C}}^{\times} \\ & \searrow^{\mathrm{N}_{K/\mathbb{Q}}} & \downarrow \mathrm{N} \\ & & \mathbb{C}^{\times} \end{array}$$

kommutativ macht. Ebenso macht die Spurabbildung

$$\begin{aligned} \mathrm{Tr} : K_{\mathbb{C}} &\to \mathbb{C}, \\ z &\mapsto \sum_{\tau} z_{\tau} \end{aligned}$$

das Diagramm

$$\begin{array}{ccc} K & \xrightarrow{j} & K_{\mathbb{C}} \\ & \searrow^{\mathrm{Tr}_{K/\mathbb{Q}}} & \downarrow \mathrm{Tr} \\ & & \mathbb{C} \end{array}$$

kommutativ. Der Logarithmus $\mathbb{C}^{\times} \to \mathbb{R}$, $z \mapsto \log |z|$ induziert einen surjektiven Gruppenhomomorphismus

$$\mathit{log} : K_{\mathbb{C}}^{\times} \to \prod_{\tau} \mathbb{R}, \quad \mathit{log}(z)_{\tau} = \log |z_{\tau}|.$$

Wir erhalten ein kommutatives Diagramm

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{C}}^\times & \xrightarrow{log} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{C}^\times & \xrightarrow{log} & \mathbb{R}. \end{array}$$

Ueberall operiert der Erzeuger F von $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$: auf $K^\times$ trivial, auf $K_{\mathbb{C}}$ wie gehabt durch $F(z)_\tau = \overline{z_{\overline{\tau}}}$ und auf $\prod_\tau \mathbb{R}$ durch $F(x)_\tau = x_{\overline{\tau}}$. Alle Abbildungen des Diagramms vertauschen mit F. Daher koennen wir zu den F-Fixmoduln uebergehen und erhalten

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{log} & (\prod_\tau \mathbb{R})^F \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{R}^\times & \xrightarrow{log} & \mathbb{R}. \end{array}$$

Sei $O_K^\times$ die Einheitengruppe, dann ist

$$O_K^\times = \left\{ x \in O_K : \mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1 \right\}.$$

Seien

$$S = \left\{ y \in K_{\mathbb{R}}^\times : N(y) = \pm 1 \right\},$$

$$H = \left\{ x \in \left(\prod_\tau \mathbb{R} \right)^F : \mathrm{Tr}(x) = \sum_\tau x_\tau = 0 \right\}.$$

Sei λ die komponierte Abbildung

$$\lambda : O_K^\times \xrightarrow{j} S \xrightarrow{log} H$$

und sei $\Gamma \subset H$ das Bild von λ.

Satz 4.5.1. *Die Sequenz*

$$1 \to \mu(K) \to O_K^\times \xrightarrow{\lambda} \Gamma \to 0$$

ist exakt. Hier ist $\mu(K) = \{x \in K : x^n = 1 \text{ fuer ein } n \in \mathbb{N}\}$ *die Gruppe der Einheitswurzeln in K. Diese ist stets endlich.*

Beweis. Da die Gruppe Γ keine Torsionselemente hat, ist $\mu(K) \subset \ker\lambda$. Sei andersrum $a \in \ker\lambda$, dann ist $|\tau(a)| = 1$ fuer jedes $\tau : K \to \mathbb{C}$. Da $j(O_K)$ ein Gitter in $K_\mathbb{R}$ ist, ist $\ker(\lambda)$ endlich. Sei q die Ordnung, es folgt $a^q = 1$, also $a \in \mu(K)$. □

Lemma 4.5.2. *Bis auf Assoziiertheit gibt es nur endlich viele Elemente* $a \in O_K$ *mit gegebener Norm* $\mathrm{N}_{K/\mathbb{Q}}(a) = k \in \mathbb{Z}$.

Beweis. Ist $N_{K/\mathbb{Q}}(a) = 0$, so folgt $a = 0$. Sei also $k \in \mathbb{Z} \setminus \{0\}$ gegeben. In jeder der endlich vielen Nebenklassen in O_K/kO_K gibt es bis auf Assoziiertheit hoechstens ein a mit $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = k$, denn: ist $b = a + k\gamma = a + N(a)\gamma$ ein zweites, so ist

$$\frac{b}{a} = 1 + \frac{\mathrm{N}(a)}{a}\gamma \in O_K,$$

da $\frac{N(a)}{a} \in O_K$. Ebenso ist $\frac{a}{a} \in O_K$, also sind a und b assoziiert. Es gibt also bis auf Assoziiertheit hoechstens $(O_K : kO_K)$ Elemente der Norm k. □

Satz 4.5.3. *Es gilt*

(a) *Die Gruppe* Γ *ist ein Gitter in dem* $(r+s-1)$*-dimensionalen reellen Vektorraum H, ist also isomorph zu* $\mathbb{Z}^{r+s-1}$.

(b) *Sei* $K^1_\mathbb{R}$ *die Menge aller* $x \in K_\mathbb{R}$ *fuer die gilt* $\prod_\tau |x_\tau| = 1$*, wobei das Produkt ueber alle* $\tau : K \to \mathbb{C}$ *laeuft. Dann ist* $O^\times$ *eine diskrete Untergruppe von* $K^1_\mathbb{R}$ *und der Quotient* $K^1_\mathbb{R}/O^\times$ *ist kompakt.*

Beweis. (a) Zeige zunaechst: Γ ist eine diskrete Untergruppe. Waere dies nicht der Fall, so gaebe es ∞-viele $a \in O_K^\times$ mit $|\log|\tau(a)|| < C$ fuer alle τ, also mit $\tau(a)$ in einem festen Kompaktum in $K_\mathbb{R}$. Da O_K ein Gitter in $K_\mathbb{R}$ ist, geht das nicht.

Als naechstes Zeigen wir, dass H/Γ kompakt ist. Waehle reelle Zahlen $c_\tau > 0$ fuer $\tau \in \mathrm{Hom}(K, \mathbb{C})$ mit $c_{\overline{\tau}} = c_\tau$ und

$$C := \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|D_K|}.$$

Sei

$$X := \left\{(z_\tau) \in K_{\mathbb{R}} : \forall_\tau \ |z_\tau| \le c_\tau\right\}.$$

Fuer $y \in S = \{y \in K_{\mathbb{R}}^\times : \mathrm{N}(y) = \pm 1\}$ ist

$$Xy = \{(z_\tau) \in K_{\mathbb{R}}^\times : |z_\tau| \le \underbrace{c_\tau |y_\tau|}_{=c'_\tau}\}.$$

Es gilt $c'_{\overline{\tau}} = c'_\tau$ und wegen $\prod_\tau |y_\tau| = 1$ gilt auch $C = \prod_\tau c'_\tau$. Nach Satz 4.2.13 gibt es ein $0 \neq a \in \mathcal{O}_K$ mit $j(a) \in Xy$. Nach Lemma 4.5.2 gibt es $\alpha_1, \ldots, \alpha_N$ so dass jedes $a \in \mathcal{O}_K$ mit $|\mathrm{N}_{K/\mathbb{Q}}(a)| \le C$ zu einem α_i assoziiert ist. Die Menge

$$T = S \cap \left(\bigcup_{i=1}^N Xj(\alpha_i)^{-1}\right)$$

ist kompakt und hat die Eigenschaft, dass ihr Bild unter $S \xrightarrow{log} H \to H/\Gamma$ gleich ganz H/Γ ist, damit ist H/Γ das Bild eines Kompaktums, also kompakt.

(b) Die Aussage folgt aus (a) durch Anwendug von log. □

Satz 4.5.4. *Es gilt*

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}.$$

Beweis. Wir haben eine exakte Sequenz

$$1 \to \mu(K) \to \mathcal{O}_K^\times \to \mathbb{Z}^{r+s-1} \to 0$$

und da die Gruppe $\mathbb{Z}^{r+s-1}$ ein freier $\mathbb{Z}$-Modul ist, spaltet diese Sequenz. □

Beispiel 4.5.5. Sei $2 \le d \in \mathbb{N}$ quadratfrei mit $d \equiv 2, 3 \mod 4$ und $K = \mathbb{Q}(\sqrt{d})$. Eine Einheit in $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{d}]$ ist eine Zahl $a + b\sqrt{d}$, die die Gleichung

$$1 = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

erfuellt. Nach dem Dirichletschen Einheitensatz gibt es eine kleinste Zahl $\varepsilon > 1$, die dies tut Sie wird die **Grundeinheit** des reell-quadratischen Zahlkoerpers K genannt. Die Einheitengruppe ist

$$O^{\times} = \left\{ \pm \varepsilon^{k} : k \in \mathbb{Z} \right\}.$$

* * *

5 Absolutbetraege

5.1 Definition

Definition 5.1.1. Sei K ein Koerper. Ein **Betrag** oder auch **Absolutbetrag** auf K ist eine Abbildung

$$|.| : K \to [0, \infty),$$

so dass

$$|xy| = |x||y|, \qquad |x + y| \leq |x| + |y|,$$

$$|x| = 0 \quad \Leftrightarrow \quad x = 0.$$

Diese Eigenschaften heissen **Multiplikativitaet**, **Dreiecksungleichung** und **Definitheit**.

Beispiele 5.1.2. (a) Auf $\mathbb{R}$ oder $\mathbb{C}$ liefert der uebliche Betrag einen Absolutbegtrag. Wir schreiben diesen jeweils als $|z|_\infty = \sqrt{z\bar{z}}$.

(b) Auf jedem Koerper K erhaelt man einen Betrag durch

$$|x|_{\text{triv}} = \begin{cases} 0 & x = 0, \\ 1 & x \neq 0. \end{cases}$$

Dies ist der **triviale Betrag**. Ab sofort sei dieser stets ausgeschlossen.

(c) Sei $K = \mathbb{Q}$ und sei p eine Primzahl. Eine rationale Zahl $x \neq 0$ laesst sich schreiben als $x = p^k \frac{a}{b}$, wobei $a, b \in \mathbb{Z} \setminus \{0\}$ teilerfremd zu p sind. Die Zahl $k \in \mathbb{Z}$ ist dann eindeutig bestimmt. Sei

$$|x|_p = p^{-k}.$$

Dann ist $|.|_p$ ein Betrag, wenn man zusaetzlich $|0|_p = 0$ setzt. Man nennt ihn den **p-adischen Betrag**.

Beweis. Multiplikativitaet und Definitheit sind klar. Fuer die Dreiecksungleichung seien $x = p^k \frac{a}{b}$ und $y = p^r \frac{c}{d}$ gegeben so dass $a, b, c, d \in \mathbb{Z}$ teilerfremd zu p sind. Indem man mit p-Potenzen multipliziert, kann man $k, r \geq 0$ annehmen. Ferner kann man nach Vertauschen von x und y auch $k \leq r$ annehmen. Es ist dann

$$x + y = \frac{p^k ad + p^r bc}{bd} = p^k \frac{ad + p^{r-k} bc}{bd} = p^{k+s} \frac{m}{bd},$$

wobei $m \in \mathbb{Z}$ teilerfremd zu p ist. Da bd teilerfremd zu p ist, folgt $s \geq 0$ und daher

$$|x+y|_p = p^{-k-s} \leq p^{-k} = \max(|x|_p, |y|_p) \leq |x|_p + |y|_p. \qquad \square$$

Definition 5.1.3. Das letzte Beispiel erfuellt sogar die sogenannte **scharfe Dreiecksungleichung**:

$$|x+y| \leq \max\big(|x|, |y|\big).$$

Lemma 5.1.4. *Sei $|.|$ eine Betrag auf dem Koerper K. Dann gilt*

(a) $|1| = |-1| = |\zeta| = 1$, *wobei $\zeta \in K$ eine beliebige Einheitswurzel ist, also eine Gleichung der Form $\zeta^d = 1$ erfuellt.*

(b) $|-x| = |x|$

(c) $|x|^{-1} = |x^{-1}|$ *fuer $x \in K^\times$,*

(d) $||x| - |y|| \leq |x-y|$,

(e) *Fuer jede natuerliche Zahl n gilt $|n| \leq n$.*

Proof. (a) Zunaechst betrachte $|1| = |1^2| = |1|^2$, woraus $|1| = 1$ folgt. Sei dann $\zeta^d = 1$ mit $d \geq 2$, dann folgt $|\zeta|^d = |\zeta^d| = |1| = 1$, woraus wegen $|\zeta| \geq 0$ ebenfalls $|\zeta| = 1$ folgt.

(b) Es gilt $|-x| = |(-1)x| = |-1||x| = |x|$ nach (a).

(c) folgt aus der Tatsache, dass $|.|$ ein Gruppenhomomorphismus $K^\times \to \mathbb{R}_+^\times$ ist.

(d) Es gilt $|x| = |x-y+y| \leq |x-y| + |y|$, also $|x| - |y| \leq |x-y|$. Durch Vertauschen von x und y erhaelt man auch $|y| - |x| \leq |x-y|$, also zusammen die Behauptung.

(e) Es ist $|n| = |1 + \cdots + 1| \leq |1| + \cdots + |1| = n$. $\square$

* * *

5.2 Aequivalenz von Betraegen

Definition 5.2.1. Ein Betrag $|.|$ auf einem Koerper K heisst **archimedisch**, falls die Menge $\mathbb{N}$ der natuerlichen Zahlen unbeschraenkt ist.

Lemma 5.2.2. *Ein Betrag $|.|$ auf einem Koerper ist genau dann nichtarchimedisch, wenn er die scharfe Dreiecksungleichung*

$$|x+y| \leq \max(|x|,|y|)$$

erfuellt.

Beweis. Sei $|.|$ nichtarchimedisch, also etwa $|\mathbb{N}| \leq N$. Dann gilt fuer $|x| \geq |y|$

$$\begin{aligned} |x+y|^n &= \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \\ &\leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k |y|^{n-k} \\ &\leq N(n+1)|x|^n, \end{aligned}$$

also gilt

$$|x+y| \leq N^{\frac{1}{n}}(n+1)^{\frac{1}{n}}|x|,$$

so dass fuer $n \to \infty$ folgt $|x+y| \leq \max(|x|,|y|)$.

Erfuellt umgekehrt $|.|$ die scharfe Dreiecksungleichung, so folgt

$$|n| = |1+\cdots+1| \leq \max(|1|,\ldots,|1|) = 1. \qquad \square$$

Lemma 5.2.3. *Sei $|.|$ ein nichtarchimedischer Betrag auf dem Koerper K. Es gilt dann*

$$|x| \neq |y| \quad \Rightarrow \quad |x+y| = \max(|x|,|y|).$$

Beweis. Wir nehmen $|x| > |y|$ an. Dann ist $|x+y| \leq \max(|x|,|y|) = |x|$. Andererseits ist wegen $|-y| = |y|$ auch $|x| = |x+y-y| \leq \max(|x+y|,|y|) \leq \max(|x|,|y|) = |x|$, so dass ueberall Gleichheit herrscht, also die Behauptung folgt. $\square$

Definition 5.2.4. Ist $|.|$ ein nichtarchimedischer Betrag, so ist die Abbildung

$$\begin{aligned} v : K^\times &\to \mathbb{R}, \\ x &\mapsto -\log|x| \end{aligned}$$

eine sogenannte **Bewertung**, d.h., es gilt

- $v(xy) = v(x) + v(y)$,
- $v(x+y) \geq \min(v(x), v(y))$.

Ist umgekehrt v eine Bewertung, so ist

$$|x| = \begin{cases} e^{-v(x)} & x \neq 0, \\ 0 & x = 0, \end{cases}$$

ein nichtarchimedischer Betrag. Das bedeutet, dass die Begriffe nichtarchimedische Betraege und Bewertungen gleichwertig benutzt werden koennen.

Lemma 5.2.5. *Ist $|.|$ ein Betrag auf K und ist $0 < s < 1$, dann ist die Abbildung $x \mapsto |x|^s$ ebenfalls ein Betrag. Der Betrag $|.|^s$ ist genau dann archimedisch, wenn $|.|$ es ist.*

Beweis. Nur die Dreiecksungleichung ist nicht-trivial. Sei zunaechst $a \geq 0$ fest gewaehlt und fuer $t \geq 0$ sei $f(t) = t^s + a^s - (a+t)^s$. Wir zeigen $f \geq 0$. Es ist $f(0) = 0$ und fuer $t > 0$ gilt

$$f'(t) = s\left(t^{s-1} - (a+t)^{s-1}\right) > 0.$$

Damit ist f monoton wachsend und es folgt $f \geq 0$. Fuer $x, y \in K$ setzen wir $a = |x|$, $t = |y|$ und aus $f(t) \geq 0$ erhalten wir die Dreiecksungleichung. □

Definition 5.2.6. Sei K ein Koerper. Wir nennen zwei Betraege $|.|_1$ und $|.|_2$ auf K **aequivalent**, falls es ein $s > 0$ gibt, so dass

$$|x|_1 = |x|_2^s$$

fuer jedes $x \in K$ gilt.

Bemerkung 5.2.7. Ein Betrag $|.|$ auf K definiert eine Metrik $d(x,y) = |x-y|$ und damit eine Topologie auf K. Man kann zeigen, dass zwei Betraege genau dann aequivalent sind, wenn sie dieselbe Topologie erzeugen, wenn sie also dieselben Folgen konvergent machen. Da dies aber fuer uns ohne Belang ist, lassen wir den Beweis weg.

Proposition 5.2.8. (a) *Sei $\mathbb{Q} \subset K \subset \mathbb{R}$ ein Koerper. Betrag $|.|$ auf K ist genau dann aequivalent zu $|.|_\infty$, falls*

$$|x| = |x|_\infty^s$$

fuer ein $0 < s \leq 1$.

(b) *Ist hingegen $\|.\|$ ein nichtarchimedischer Betrag, dann ist $\|.\|^s$ ein (nichtarchimedischer) Betrag fuer jedes $s > 0$.*

Proof. (a) Gilt die Gleichung, dann ist $|x|$ aequivalent zu $|.|_\infty$.

Umgekehrt zeigen wir, dass fuer $s > 1$ die Abbildung $N(x) = |x|_\infty^s$ kein Betrag ist. Waere es eine, so gölte fuer $0 < x, h \in K$, dass

$$\begin{aligned}\frac{(x+h)^s - x^s}{h} &= \frac{N(x+h) - N(x)}{h} \\ &\leq \frac{N(h)}{h} = h^{s-1}.\end{aligned}$$

Fuer $h \to 0$ geht die linke Seite gegen sx^{s-1} und die rechte gegen Null. Widerspruch!

(b) Die scharfe Dreiecksungleichung vererbt sich leichter als die normale. Dafuer braucht man nur die Monotonie der Abbildung $t \mapsto t^s$. □

* * *

5.3 Der Satz von Ostrowski

Satz 5.3.1 (Ostrowski). *Der Betrag $|.|_\infty$ von $\mathbb{R}$ und die p-adischen Betraege $|.|_p$ fuer Primzahlen p sind bis auf Aequivalenz genau alle Betraege auf dem Koerper $\mathbb{Q}$.*

Beweis. Da fuer eine Primzahl p die Folge p^n in $|.|_p$ gegen Null geht und dies in keinem anderen Betrag $|.|_q$ tut, folgt, dass die Betraege $|.|_p$ fuer $p \leq \infty$ paarweise inaequivalent sind.

Sei nun also $|.|$ irgendein Betrag auf $\mathbb{Q}$. *Erster Fall:* Es gebe eine natuerliche Zahl n_0 mit $|n_0| > 1$. Seien $1 < a, b \in \mathbb{N}$, dann kann man b^n in der Basis a darstellen $b^n = \sum_{i<m} c_i a^i$, wobei $c_i \in \{0, 1, \ldots, a-1\}$ und $m \leq n\frac{\log b}{\log a} + 1$. Wegen $|c_i| = c_i < a$ folgt

$$\begin{aligned}|b|^n = |b^n| &= \left|\sum_{i<m} c_i a^i\right| < am \max(|a|^{m-1}, 1) \\ &\leq a\Big(n\frac{\log b}{\log a} + 1\Big) \max\left(|a|^{n\frac{\log b}{\log a}}, 1\right).\end{aligned}$$

Hieraus folgt

$$|b| \leq \underbrace{\left[a\Big(n\frac{\log b}{\log a} + 1\Big)\right]^{\frac{1}{n}}}_{\to 1} \max\left(|a|^{\frac{\log b}{\log a}}, 1\right),$$

so dass

$$|b| \leq \max\left(|a|^{\frac{\log b}{\log a}}, 1\right).$$

Ist nun $|b| > 1$, so muss auch $|a| > 1$ sein, so dass wir $|b| \leq |a|^{\frac{\log b}{\log a}}$ oder $|b|^{\frac{1}{\log b}} \leq |a|^{\frac{1}{\log a}}$ erhalten. Wegen Symmetrie folgt dann Gleichheit. Damit existiert also eine Konstante c so dass $|a| = c^{\log a} = a^{\log c}$, so dass dieser Betrag zum Betrag von $\mathbb{R}$ aequivalent ist.

Zweiter Fall: Es gilt $|n| \leq 1$ fuer alle natuerlichen Zahlen $n \in \mathbb{N}$. Wir nehmen an, dass $|.|$ nichttrivial ist, dann muss es eine natuerliche Zahl n geben mit $|n| < 1$. Nach Primfaktorzerlegung folgt, dass es eine Primzahl p geben muss mit $|p| < 1$. Sei q eine zweite Primzahl, wir behaupten, dass dann $|q| = 1$ sein muss. Angenommen, das ist nicht so. Nach dem euklidischen Algorithmus existieren $m, n \in \mathbb{Z}$ so dass $mp + nq = 1$. Nach der scharfen Dreiecksungleichung (siehe Lemma 5.2.2) gilt

$$1 = |mp + nq| \leq \max(|m||p|, |n||q|) < 1$$

Widerspruch! Also ist p die einzige Primzahl mit $|p| < 1$. Sei $\alpha = |p|$ und sei $c = -\log \alpha / \log p$, dann gilt fuer eine beliebige rationale Zahl $r = p^k \frac{a}{b}$ mit zu p teilerfremden $a, b \in \mathbb{Z}$

$$|r| = |p|^k = \alpha^k = e^{k \log \alpha} = e^{-ck \log p} = |r|_p^c.$$ □

Lemma 5.3.2.

(a) *Eine Untergruppe* $0 \neq H \subset \mathbb{R}$ *der additiven Gruppe* $(\mathbb{R}, +)$ *liegt entweder dicht oder ist eine* **diskrete Untergruppe**, *also von der Form*

$$H = \alpha\mathbb{Z}$$

fuer ein $\alpha > 0$.

(b) *Eine Untergrupe* $1 \neq M \subset (0, \infty)$ *der multiplikativen Gruppe* $\mathbb{R}_+^\times$ *ist entweder dicht oder von der Form*

$$M = q^{\mathbb{Z}}$$

fuer ein $q > 1$.

Beweis. Die Exponentialabbildung $\exp : \mathbb{R} \to \mathbb{R}_+^\times$ ist ein Gruppenisomorphismus, der in beiden Richtungen stetig ist. Durch seine Anwendung und die seiner

Umkehrabbildung log sieht man, dass die beiden Aussagen (a) und (b) aequivalent sind. Wir beweisen daher (a). Sei also $0 \neq H \subset \mathbb{R}$ eine Untergruppe.

1. Fall. Es gibt ein $\varepsilon > 0$ so dass

$$H \cap (-\varepsilon, \varepsilon) = \{0\}.$$

Sei $\alpha > 0$ das Supremum ueber alle solchen $\varepsilon > 0$. Dann ist $\alpha < \infty$, denn sonst waere H trivial. Sei $0 < \varepsilon < \alpha$, so gibt es ein $h_1 \in H$ mit $\alpha \leq h_1 < \alpha + \varepsilon$, nach der Definition von α. Wir behaupten $h_1 = \alpha$. **Angenommen**, nicht, dann muss es ein $h_0 \in H$ geben mit $\alpha \leq h_0 < h_1$. Dann ist aber $h_1 - h_0 \in H$ und da $\alpha \leq h_0 < h_1 < \alpha + \varepsilon$, folgt $0 < h_1 - h_0 < \varepsilon$ oder $h_1 - h_0 \in (0, \varepsilon)$ was im **Widerspruch** zur Annahme steht. Es folgt also $\alpha \in H$. Ist nun $h \in H$ beliebig, dann gibt es ein $k \in \mathbb{Z}$ so dass

$$k\alpha \leq h < (k+1)\alpha.$$

Es folgt $0 \leq h - k\alpha < \alpha$ und da $h - k\alpha$ in H liegt, folgt $h - k\alpha = 0$, also $h = k\alpha \in \alpha\mathbb{Z}$. Zusammen haben wir also

$$H = \alpha\mathbb{Z}.$$

2. Fall. Fuer jedes $\varepsilon > 0$ ist $H \cap (-\varepsilon, \varepsilon) \neq \{0\}$. Sei $\varepsilon > 0$. Ist a in $H \cap (-\varepsilon, \varepsilon)$, so auch $-a$, so dass wir $H \cap (0, \varepsilon) \neq 0$ folgern koennen. Sei also $b \in H \cap (0, \varepsilon)$, so bildet die Menge $b\mathbb{Z}$ ein Gitter in $\mathbb{R}$ mit Abstand $b < \varepsilon$, es folgt, dass es zu jedem $x \in \mathbb{R}$ in der ε-Umgebung ein Element aus $b\mathbb{Z}$, also ein Element aus H gibt. Damit liegt H dicht in $\mathbb{R}$. □

Definition 5.3.3. Eine Betrag $|.|$ auf einem Koerper K heisst **diskret**, wenn die Gruppe $\{|x| : x \in K^\times\}$ eine diskrete Untergruppe von $\mathbb{R}^\times$ ist. Das bedeutet, dass es ein $q > 1$ gibt, so dass die Betraege in $q^{\mathbb{Z}} = \{q^k : k \in \mathbb{Z}\}$ liegen.

Beispiele 5.3.4.

- Der uebliche Betrag auf $\mathbb{R}$ ist nicht diskret. Auch seine Einschraenkung auf $\mathbb{Q}$ ist nicht diskret.
- Der p-adische Betrag auf $\mathbb{Q}$ fuer eine Primzahl p ist diskret, denn die Betraege liegen alle in $p^{\mathbb{Z}}$.

Satz 5.3.5. *Sei $|.|$ ein nichtarchimedischer Betrag auf einem Koerper K. Dann ist*

$$A = \{x \in K : |x| \leq 1\}$$

ein Unterring von K, der sogenannte **Bewertungsring** *von K. Der Koerper K ist der Quotientenkoerper zum Integritaetsring A.*

Der Ring A ist ein **lokaler Ring**, *d.h., er hat genau ein maximales Ideal, dieses ist*

$$\mathfrak{m} = \{x \in K : |x| < 1\}.$$

Dies ist genau dann ein Hauptideal, wenn |.| diskret ist, d.h., der Bewertungsring A ist genau dann ein diskreter Bewertungsring, wenn der Betrag |.| diskret ist. In diesem Fall spricht man von einer **diskreten Bewertung**

Beweis. Die Menge A enthaelt die Null und die Eins und ist abgeschlossen unter der Multiplikation. Wegen der scharfen Dreiecksungleichung ist die auch unter der Addition abgeschlossen, also ein Unterring. Fuer die letzte Aussage beachte, dass sogar noch schaerfer gilt: ist $x \in K$, dann ist $x \in A$ oder $x^{-1} \in A$.

Die Menge $\mathfrak{m}$ ist wegen der scharfen Dreiecksungleichung ein Ideal von A. Ihr Komplement $A \setminus \mathfrak{m}$ ist die Menge aller $x \in K$ mit $|x| = 1$, also folgt $A \setminus \mathfrak{m} = A^\times$, woraus folgt, dass $\mathfrak{m}$ maximal und dass $\mathfrak{m}$ das einzige maximale Ideal ist.

Ist nun $\mathfrak{m}$ ein Hauptideal, etwa $\mathfrak{m} = \pi A$ und sei $x \in \mathfrak{m}$ mit $x \neq 0$. Dann gibt es ein maximales $k \in \mathbb{N}$, so dass $x = \pi^k y$ fuer ein $y \in A$, denn es gilt fuer jede solche Darstellung von x, dass $0 < |x| = |\pi|^k |y| \leq |\pi|^k$. Da die Folge $|\pi|^k$ fuer $k \to \infty$ gegen Null geht, folgt die Existenz eines maximalen $k \in \mathbb{N}$ mit $x = \pi^k y$ fuer ein $y \in A$. Dann muss $y \in A \setminus \mathfrak{m} = A^\times$ sein, denn sonst waere $y = \pi y'$, $y' \in A$ und damit $x = \pi^{k+1} y'$, was der Maximalitaet von k widerspricht. Also ist $|y| = 1$ und damit $|x| = |\pi|^k$, so dass der Betrag diskret ist. Ist umgekehrt der Betrag diskret, so ist nach Lemma 5.3.2 die Gruppe $|K^\times| = q^{\mathbb{Z}}$ fuer ein $q > 1$. Dann ist jedes $\pi \in K$ mit $|\pi| = q^{-1}$ ein Erzeuger von $\mathfrak{m}$. □

Korollar 5.3.6. *Sei |.| ein diskreter Betrag auf einem Koerper K. Seien A der Bewertungsring und $\mathfrak{m}$ das maximale Ideal. Dann sind Addition und Multiplikation $K \times K \to K$ offene Abbildungen.*

Proof. Seien $W \subset K \times K$ offen und $(x, y) \in W$. Dann existiert ein $k \in \mathbb{N}$, so dass $\left(x + \mathfrak{m}^k\right) \times \left(y + \mathfrak{m}^k\right)$ in W liegt. Dann liegt $x + y + \mathfrak{m}^k$ in $\left(x + \mathfrak{m}^k\right) + \left(y + \mathfrak{m}^k\right)$ und damit ist die Addition offen. Ferner liegt $xy + \mathfrak{m}^{2k}$ in $\left(x + \mathfrak{m}^k\right) \cdot \left(y + \mathfrak{m}^k\right)$ und damit ist die Multiplikation offen. □

* * *

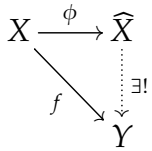
5.4 Vervollstaendigung

Erinnerung. In einem metrischen Raum (X, d) wird eine Folge $(x_n)_{n\in\mathbb{N}}$ **Cauchy-Folge** genannt, wenn es zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}$ gibt, so dass fuer alle $m, n \geq n_0$ gilt

$$d(x_m, x_n) < \varepsilon.$$

Jede konvergente Folge ist eine Cauchy-Folge. Der Raum heisst **vollstaendig**, wenn jede Cauchy-Folge auch konvergiert.

Jeder metrische Raum X besitzt eine **Vervollstaendigung**, also eine vollstaendigen Raum $\widehat{X}$ mit einer isometrischen Einbettung $\phi : X \hookrightarrow \widehat{X}$, so dass jede isometrische Abbildung $f : X \to Y$ in einen vollstaendigen Raum Y in eindeutiger Weise durch $\widehat{X}$ faktorisiert:



Hieraus folgt unter anderem, dass X dicht in $\widehat{X}$ liegt, also ist jedes Element von $\widehat{X}$ ein Limes von Elementen von X.

Zum Beispiel ist $\mathbb{R}$ die Vervollstaendigung von $\mathbb{Q}$.

Satz 5.4.1. *Sei $|.|$ ein Betrag auf einem Koerper K. Sei $\widehat{K}$ die Vervollstaendigung nach der induzierten Metrik $d(x, y) = |x - y|$. Dann setzen die Addition und Multiplikation $+, * : K \times K \to K$ in eindeutiger Weise fort zu stetigen Abbildungen $\widehat{K} \times \widehat{K} \to \widehat{K}$. Mit diesen Abbildungen ist $\widehat{K}$ wieder ein Koerper, also ist $\widehat{K}/K$ eine Koerpererweiterung.*

Beweis. Der Beweis ist derselbe wie im Uebergang von $\mathbb{Q}$ nach $\mathbb{R}$ (wenn man $\mathbb{R}$ als die Vervollstaendigung von $\mathbb{Q}$ einfuehrt).

Jedes Element $a \in \widehat{K}$ laesst sich als Limes $a = \lim_n a_n$ mit $a_n \in K$ schreiben. Wir definieren dann

$$\left(\lim_n a_n\right) + \left(\lim_n b_n\right) = \lim_n \left(a_n + b_n\right).$$

Fuer die Wohldefiniertheit dieser Definition seien $a'_n \to a$ und $b'_n \to b$ weitere Folgen in K. Dann sind $a_n - a'_n$ und $b_n - b'_n$ Nullfolgen und da

$$\left|\left(a_n + b_n\right) - \left(a'_n - b'_n\right)\right| \leq |a_n - a'_n| + |b_n - b'_n| \to 0,$$

ist auch $\left(a_n + b_n\right) - \left(a'_n - b'_n\right)$ eine Nullfolge, so dass die Limiten uebereinstimmen. Bei der Multiplikation geht das ebenso. Die Eindeutigkeit von $+, *$ als stetige Abbildungen ist klar, da sie als Limiten definiert wurden. Die Koerpereigenschaften vererben sich von K auf $\widehat{K}$. Wir zeigen exemplarisch das Assoziativgesetz der Addition:

$$\begin{aligned}
&\left(\left(\lim_n a_n\right) + \left(\lim_n b_n\right)\right) + \left(\lim_n c_n\right) \\
&= \lim_n \left(a_n + b_n\right) + \left(\lim_n c_n\right) \\
&= \lim_n (a_n + b_n) + c_n \\
&= \lim_n a_n + (b_n + c_n) \\
&= \left(\lim_n a_n\right) + \left(\left(\lim_n b_n\right) + \left(\lim_n c_n\right)\right).
\end{aligned}$$

□

* * *

5.5 Die p-adischen Zahlen

Definition 5.5.1. Sei nun $K = \mathbb{Q}$. Fuer jede Primzahl p haben setzen wir $v_p(p^k \frac{a}{b}) = k$ und definieren den entsprechenden Betrag

$$|a|_p = p^{-v_p(a)}.$$

Sei $\mathbb{Q}_p$ die Vervollstaendigung von $\mathbb{Q}$ nach dem Betrag $|.| + p$. Sei

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

der Bewertungsring von $\mathbb{Q}_p$. Dann ist $\mathbb{Z}_p$, da der Betrag diskret ist, ein lokaler Hauptidealring und die Ideale $\neq 0$ von $\mathbb{Z}_p$ sind genau $\mathbb{Z}_p, p\mathbb{Z}_p, \ldots, p^j\mathbb{Z}_p, \ldots$.

Sei $m \in \mathbb{N}$. Dann hat m eine eindeutig bestimmte Darstellung

$$m = \sum_{j=0}^{N} k_j p^j$$

wobei $k_0, k_1, \cdots \in \{0, 1, \ldots, p-1\}$.

Satz 5.5.2. (a) *Sei $z \in \mathbb{Z}_p$. Dann gibt es eindeutig bestimmte Koeffizienten $k_0, k_1, \cdots \in \{0, \ldots, p-1\}$ so dass*

$$z = \sum_{j=0}^{\infty} k_j p^j,$$

wobei die Summe in $\mathbb{Z}_p$ konvergiert. Addition und Multiplikation setzen die Operationen auf den endlichen Summen, also natuerlichen Zahlen, fort.

(b) *Der Ring $\mathbb{Z}_p$ ist ueberabzaehlbar.*

(c) *Der Unterring $\mathbb{Z}$ liegt dicht in $\mathbb{Z}_p$.*

Beweis. (a) Die Elemente $0, 1, \ldots, p-1$ in $\mathbb{Z}$ liefern genau alle Elemente von $\mathbb{F}_p = \mathbb{Z}/p = \mathbb{Z}_p/p\mathbb{Z}_p$. Also gibt es genau ein $k_0 \in \{0, \ldots, p-1\}$ und genau ein $c_0 \in \mathbb{Z}_p$, so dass

$$z - k_0 \in p\mathbb{Z}_p, \quad \text{also} \quad z = k_0 + pc_1.$$

Dasselbe gilt fuer c_1, also gibt es genau ein $k_1 \in \{0, \ldots, p-1\}$ und genau ein $c_2 \in \mathbb{Z}_p$, so dass

$$z = k_0 + pk_1 + p^2 c_2.$$

Wir wiederholen diesen Schluss und erhalten eindeutig bestimmte Folge $k_0, k_1, \ldots$ in $\{0, \ldots, p-1\}$ und $c_j \in \mathbb{Z}_p$ so dass

$$z = k_0 + pk_1 + \cdots + k_n p^n + c_{n+1} p^{n+1}.$$

Da $|c_n| \leq 1$, geht $c_{n+1} p^{n+1}$ gegen Null, also konvergiert die Reihe. Die Eindeutigkeit haben wir unterwegs geklaert.

(b) Die Ueberabzaehlbarkeit von $\mathbb{Z}_p$ folgt aus der Ueberabzaehlbarkeit der Menge

$$\{0, 1, \ldots, p-1\}^{\mathbb{N}_0}$$

aller Koeffizientenfolgen.

(c) Die endlichen Summen liegen dicht in $\mathbb{Z}_p$. □

Lemma 5.5.3. *Es gilt*

$$\mathbb{Q}_p^\times = \bigsqcup_{k\in\mathbb{Z}} p^k \mathbb{Z}_p^\times.$$

Also

$$\mathbb{Q}_p = \left\{ \sum_{j=k}^{\infty} a_j p^j : k \in \mathbb{Z},\ a_j \in \{0,1,\dots,p-1\} \right\}.$$

Beweis. "$\supset$" ist klar. Sei also $x \in \mathbb{Q}_p^\times$. Sei $k = v_p(x)$ und $y = xp^{-k}$, dann ist $v_p(y) = 0$, also $y \in \mathbb{Z}_p^\times$. □

Satz 5.5.4. *Für jedes $x \in \mathbb{Q}^\times$ gilt die* **Produktformel***:*

$$\prod_{p\le\infty} |x|_p = 1.$$

Hierbei läuft das Produkt über alle Primzahlen und über $p = \infty$. In dem Produkt sind fast alle Faktoren gleich 1.

Hierbei benutzen wir die Standard-Redeweise:

fast alle heißt *alle bis auf endlich viele*.

Proof. Schreibe x als teilerfremden Bruch und schreibe Zähler und Nenner als Produkt von Primzahlpotenzen dann ist

$$x = \pm p_1^{k_1} \cdots p_n^{k_n}$$

für verschiedene Primzahlen $p_1,\dots,p_n$ und $k_1,\dots,k_n \in \mathbb{Z}$. Es ist dann $|x|_p = 1$ falls p eine Primzahl ist, die mit keiner der p_j übereinstimmt. Also hat das Produkt wirklich nur endlich viele Faktoren $\neq 1$. Ferner gilt:

$$|x|_{p_j} = p^{-k_j} \qquad \text{und} \qquad |x|_\infty = p_1^{k_1} \cdots p_n^{k_n}.$$

Damit folgt

$$\prod_{p\le\infty} |x|_p = \Big(\prod_{j=1}^{n} p^{-k_j} \Big) \cdot p_1^{k_1} \cdots p_n^{k_n} = 1.$$ □

* * *

5.6 Hensels Lemma

Definition 5.6.1. Sei K ein Koerper mit einem Betrag und sei $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ ein Polynom. Dann setze

$$\|f\| = \max\left\{|a_j| : j = 0, \ldots, n\right\}.$$

Lemma 5.6.2. *Seien $f \in A[x]$ ein irreduzibles normiertes Polynom und sei $\alpha \in \overline{K}$ eine Nullstelle von f. Dann existiert ein $\delta > 0$ so das fuer jedes normierte Polynom g mit $\|f - g\| < \delta$ eine Nullstelle $\beta \in \overline{K}$ von g existiert, so dass $K(\alpha) = K(\beta)$.*

Beweis des Korollars. Sei L der Zerfaellungskoerper von f, versehen mit der Fortsetzung des Betrags. Sei $B = \left\{x \in L : |x| \leq 1\right\}$ der Bewertungsring umd $\mathfrak{m}_B = \left\{x \in L : |x| < 1\right\}$ das maximale Ideal.

Sei $n = \deg(f)$. Die Gruppe $\mathrm{Per}(n)$ operiert auf L^n durch Vertauschen der Koordinaten. Die Abbildung ϕ, die einem Vektor $v = (\alpha_1, \ldots, \alpha_n)$ das Polynom

$$\phi(v) = \prod_{j=1}^{n} (x - \alpha_j)$$

zuordnet, liefert eine Bijektion von $\mathrm{Per}(n)\backslash L^n$ in die Menge der normierten Polynome vom Grad n. Diese Abbildung ist stetig und offen (Korollar 5.3.6), also ein Homoeomorphismus. Der Korper $M = K(\alpha)$, sowie alle seine Unterkoerper sind abgeschlossene Teilmengen, also existiert eine offene Umgebung U von α, die leeren Schnitt mit allen echten Unterkoerpern von M hat. Das bedeutet, dass $M = K(u)$ fuer jedes $u \in U$ gilt. Wegen der Stetigkeit von ϕ^{-1} folgt damit die Behauptung. □

Satz 5.6.3 (Hensels Lemma)**.** *Der Koerper K sei vollstaendig bzgl dem nichtarchimedischen Betrag $|.|$ und $A = \left\{|x| \leq 1\right\}$ sei der Bewertungsring. Sei $\mathfrak{m} = \left\{|x| < 1\right\}$ das maximale Ideal von A und sei $f \in A[x]$ ein Polynom mit Reduktion $\overline{f} \in A/\mathfrak{m}[x]$. Gegeben sei eine Zerlegung*

$$\overline{f} = \tilde{g}\tilde{h}$$

in teilerfremde Polynome $\tilde{g}, \tilde{h} \in A/\mathfrak{m}[x]$. Dann besitzt f eine Zerlegung $f = gh$ in $A[x]$ mit

$$\begin{matrix}\overline{g} = \tilde{g}, \\ \overline{h} = \tilde{h}\end{matrix} \quad \textit{und} \quad \mathrm{grad}(g) = \mathrm{grad}\left(\tilde{g}\right).$$

Angewendet wird der Satz meist in folgender Form:

Korollar 5.6.4. *Hat das Polynom $f \in A[x]$ in $A/\mathfrak{m}$ eine Nullstelle α, dann hat es auch eine Nullstelle $a \in A$ mit $\overline{a} = \alpha$.*

Beweis des Korollars. Folgt durch Anwendung des Satzes auf den Fall $\tilde{g}(x) = (x - \alpha)^d$, wobei d die Nullstellenordnung ist. □

Beweis des Satzes. Seien $d = \text{grad}(f)$und $k = \text{grad}\,(\tilde{g})$, also $d \geq \text{grad}\left(\tilde{h}\right) + k$. Seien $g_0, h_0 \in A[x]$ beliebige Polynome mit $g_0 \equiv \tilde{g},\ h_0 \equiv \tilde{h} \mod \mathfrak{m}$, $\text{grad}(g_0) = k$, $\text{grad}(h_0) \leq d - k$. Da die Polynome $\tilde{g}, \tilde{h}$ teilerfremd sind, existieren $a(x), b(x) \in A[x]$ so dass $ag_0 + bh_0 \equiv 1 \mod \mathfrak{m}$.

Unter den Koeffizienten der beiden Polynome $f - h_0 g_0, ag_0 - bh_0 - 1 \in \mathfrak{m}[x]$ suche einen mit maximalem Betrag (der ist immer noch < 1) und nenne diesen Koeffizienten π. Wir machen den Ansatz

$$g = g_0 + p_1\pi + p_2\pi^2 + \ldots,$$
$$h = h_0 + q_1\pi + q_2\pi^2 + \ldots$$

mit $p_i, q_i \in A[x]$ vom Grad $< k$ bzw. $\leq d - k$. Wir bestimmen die p_i, q_i sukzessive so, dass mit

$$g_n = g_0 + p_1\pi + \cdots + p_n\pi^n,$$
$$h_n = h_0 + q_1\pi + \cdots + q_n\pi^n$$

gilt

$$f \equiv g_n h_n \mod (\pi^{n+1}).$$

Durch Grenzuebergang $n \to \infty$ ergibt sich dann $f = gh$ wie gewuenscht. **Konstruktion:** Fuer $n = 0$ ist die Forderung nach Wahl von π erfuellt. Sei die Forderung fuer $n - 1$ erfuellt. Die Aussage fuer n laeuft wegen

$$g_n = g_{n-1} + p_n\pi^n, \qquad h_n = h_{n-1} + q_n\pi^n$$

auf

$$f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\pi^n \mod \pi^{n+1}$$

hinaus, also auf

$$g_{n-1}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \equiv f_n \mod \pi,$$

wobei $f_n = \pi^{-n}(f - g_{n-1}h_{n-1}) \in A[x]$ ist. Wegen $g_0a + h_0b \equiv 1 \mod \pi$ gilt

$$g_0af_n + h_0bf_n \equiv f_n \mod \pi.$$

Wir wuerden jetzt $q_n = af_n$ und $p_m = bf_n$ setzen, wenn nicht die Grade zu gross sein koennten. Nach dem Prinzip der Polynomdivision kann man schreiben

$$b(x)f_n(x) = q(x)g_0(x) + p_n(x)$$

mit $\operatorname{grad}(p_n) < \operatorname{grad}(g_0) = m$. Wegen $g_0 \equiv \tilde{g} \mod \mathfrak{m}$ und $\operatorname{grad}(g_0) = \operatorname{grad}(\tilde{g})$ ist der hoechste Koeffizient von g_0 eine Einheit, so dass $q(x) \in A[x]$ und wir erhalten die Kongruenz

$$g_0(af_n + h_0q) + h_0p_n \equiv f_n \mod \pi.$$

Streichen wir nun aus dem Polynom $af_n + h_0q$ alle durch π teilbaren Koeffizienten heraus, so erhalten wir ein Polynom q_n mit $g_0q_n + h_0p_n \equiv f_n \mod \pi$, das wegen $\operatorname{grad}(f_n) \le d$, $\operatorname{grad}(g_0) = m$ und $\operatorname{grad}(h_0p_n) < (d-m) + m = d$ einen Grad $\le d - m$ hat, wie gewuenscht. □

Sei $|.|$ ein nichtarchimedischer Betrag. Fuer ein Polynom
$f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ sei

$$|f| = \max(|a_0|, \ldots, |a_n|).$$

Dann gilt

$$f \in A[x] \quad \Leftrightarrow \quad |f| \le 1.$$

Korollar 5.6.5. *Ist K vollstaendig und f irreduzibel, so gilt*

$$|f| = \max(|a_0|, |a_n|).$$

Insebesondere folgt:

$$a_0, a_n \in A \quad \Rightarrow \quad f \in A[x].$$

Beweis. Durch Multiplikation mit geeignetem $\alpha \in K$ erhalte $f \in A[x]$ und $|f| = 1$. Waere

nun $|a_0| < 1$ und $|a_n| < 1$, dann ist

$$\begin{aligned} f(x) &\equiv a_r x^r + \cdots + a_n x^n \\ &\equiv x^r (a_r + \cdots + a_{n-1} x^{n-r}) \mod \mathfrak{m}. \end{aligned}$$

Ist nun $|a_0|, |a_n| < 1$, dann ist $0 < r < n$, was nach Hensels Lemma zum Widerspruch zur Irreduzibilitaet fuehrt. □

* * *

5.7 Fortsetzung von Betraegen

Lemma 5.7.1. *Ist $|.|$ ein nichtarchimedischer Betrag auf dem Koerper L und B der Bewertungsring.*

(a) *Dann ist fuer jedes $\alpha \in L \setminus B$ der Ring $B[\alpha]$ gleich dem ganzen Koerper L.*

(b) *Ist $|.|_1$ eine weitere Bewertung mit Bewertungsring B_1. Gilt $B = B_1$, dann folgt $|.| = |.|_1^s$ fuer ein $s > 0$.*

Proof. (a) Sei $y \in L$. Da $|\alpha| > 1$, gibt es ein $k \in \mathbb{N}$, so dass $|\alpha|^k \geq |y|$, also $|y/\alpha^k| \leq 1$, d.h., $y/\alpha^k \in B$ und damit $y \in B[\alpha]$.

(b) Es gilt $|x| < 1 \Leftrightarrow |x|_1 < 1$. Waehle ein $\pi \in L$ mit $|\pi|, |\pi|_1 < 1$. Dann gibt es genau ein $s > 0$ mit $|\pi| = |\pi|_1^s$. □

Satz 5.7.2. *Sei K vollstaendig bezueglich des Betrags $|.|$. Sei L/K eine separable algebraische Koerpererweiterung, dann existiert genau eine Fortsetzung $\|.\|$ zu einem Betrag auf L. Ist L/K endlich vom Grad n, so gilt fuer diese Fortsetzung*

$$\|\alpha\| = |\mathrm{N}_{L/K}(\alpha)|^{\frac{1}{n}}.$$

Insbesondere ist diese Fortsetzung Galois-invariant, falls L/K galoisch ist.

Beweis. Ist $|.|$ archimedisch, dann gibt es nur eine nichttriviale Erweiterung: $\mathbb{C}/\mathbb{R}$. In diesem Fall ist die Behauptung eine Uebungsaufgabe. Sei also $|.|$ nichtarchimedisch.

Man kann voraussetzen, dass L/K endlich ist. Sei n der Grad. Sei $A \subset K$ der Bewertungsring und sei $B_g \subset L$ der ganze Abschluss von A in L. Wir zeigen

$$B_g = \{\alpha \in L : \mathrm{N}_{L/K}(\alpha) \in A\}.$$

"$\subset$": Bette L in einen algebraischen Abschluss $\overline{K}$ von K ein. Ist $\alpha \in B_g$, dann ist $\sigma(\alpha) \in B_g$ fuer alle $\sigma \in \mathrm{Hom}(L, \overline{K})$. Damit ist $\mathrm{N}_{L/K}(\alpha) = \prod_\sigma \sigma(\alpha) \in B_g \cap K = A$.
"$\supset$": Sei $\alpha \in L$ mit $\mathrm{N}_{L/K}(\alpha) \in A$. Sei

$$f(x) = a_0 + \cdots + a_{d-1}x^{d-1} + x^d$$

das Minimalpolynom von α. Dann ist $a_0 = (\pm 1)$ mal dem Produkt der Konjugierten von α, so dass $\pm a_0 = \mathrm{N}_{L/K}(\alpha) \in A$. Nach Korollar 5.6.5 folgt $f \in A[x]$.

Definiere nun

$$\|\alpha\| = |\mathrm{N}_{L/K}(\alpha)|^{\frac{1}{n}}, \quad \alpha \in L.$$

Es gilt

- $\|\alpha\beta\| = \|\alpha\|\,\|\beta\|$, $\alpha, \beta \in L$,
- $\|\alpha\| = 0 \;\Leftrightarrow\; \alpha = 0$,
- $\|\alpha + \beta\| \le \max(\|\alpha\|, \|\beta\|)$
  Beweis: Es reicht, $\alpha\beta \neq 0$ anzunehmen. Dividiere durch β und zeige $\|\alpha + 1\| \le \max(\|\alpha\|, 1)$, hierbei kann $\|\alpha\| \le 1$ angenommen werden, da man sonst die Rollen von α und β vertauscht. Aus $\|\alpha\| \le 1$ folgt $\alpha \in B$, so dass auch $\alpha + 1 \in B$, was soviel bedeutet wie $\|\alpha + 1\| \le 1 = \max(\|\alpha\|, 1)$.

Damit ist $|.|$ als nichtarchimedischer Betrag fortgesetzt. Sei $B_{\|.\|}$ der Bewertungsring dieser Fortsetzung.

Zur Eindeutigkeit: Wir koennen L/K als Galois-Erweiterung annehmen, da wir stets zur normalen Huelle uebergehen koennen. In diesem Fall ist $\|.\|$ Galois-invariant

Lemma 5.7.3. *Fuer jede Fortsetzung $|.|_1$ von $|.|$ nach L gilt $B_g = B_{|.|_1}$.*

Beweis des Lemmas. Die Behauptung folgt aus

1. $B_{\|.\|} \subset B_g$,
2. $B_g \subset B_{|.|_1}$,

3. $B_{|.|_1} \subset B_{\|.\|}$.

$B_{\|.\|} \subset B_g$: Sei $b \in B_{\|.\|}$ und $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ das Minimalpolynom. Da $\|.\|$ Galois-invariant ist, gilt $|a_0| = |N_{L/K}(b)| = \left\|N_{L/K}(b)\right\| = \prod_\tau \|\tau(b)\| \leq 1$. Nach Korollar 5.6.5 folgt $b \in B_g$.

$B_g \subset B_{|.|_1}$: Sei $a \in B_g$ und $f(x) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n \in A[x]$ das Minimalpolynom. Dann ist

$$\begin{aligned} |\alpha|_1^n = |\alpha^n|_1 &= |a_0 + \cdots + a_{n-1}\alpha^{n-1}|_1 \\ &\leq \max(|a_0|, |a_1|\,|\alpha|_1, \ldots, |a_{n-1}|\,|\alpha|_1^{n-1}) \\ &\leq \max(1, |\alpha|_1, \ldots, |\alpha|_1^{n-1}). \end{aligned}$$

Hieraus folgt $|\alpha|_1^n \leq |\alpha|_1^k$ fuer ein $0 \leq k < n$ und daher $|\alpha|_1^{n-k} \leq 1$, also $|\alpha|_1 \leq 1$ und damit $\alpha \in B_{|.|_1}$.

$B_{|.|_1} \subset B_{\|.\|}$: Sei $b \in B_{|.|_1}$. Waere $b \notin B_{\|.\|}$, dann goelte nach Lemma 5.7.1, dass $L = B_{\|.\|}[b] \subset B_g[b] \subset B_{|.|_1}$. Widerspruch! □

Zurueck zum Beweis des Satzes, also der Eindeutigkeit: Wenn wir zeigen koennen, dass $|.|_1$ Galois-invariant ist, folgt bereits die Behauptung, denn dann gilt

$$\begin{aligned} |b|_1 = \left((|b|_1)^n\right)^{\frac{1}{n}} &= \left(\prod_\tau |\tau(b)|_1\right)^{\frac{1}{n}} \\ &= \left(\left|\prod_\tau \tau(b)\right|_1\right)^{\frac{1}{n}} = \left(|\,\mathrm{N}_{L/K}(b)|_1\right)^{\frac{1}{n}} \\ &= \left(|\,\mathrm{N}_{L/K}(b)|\right)^{\frac{1}{n}} = \|b\|\,. \end{aligned}$$

Nach dem Lemma ist der Bewertungsring $B_{|.|_1} = B_g$ insbesondere Galois-invariant, also gilt $|\alpha|_1 \leq 1 \;\Leftrightarrow\; |\tau(\alpha)|_1 \leq 1$. Hieraus folgt sofort

$$|\alpha|_1 \leq |\beta|_1 \quad \Leftrightarrow \quad |\tau(\alpha)|_1 \leq |\tau(\beta)|_1.$$

Ist nun $|.|$ nicht diskret, dann liegt $|A^\times|$ dicht in $\mathbb{R}_{>0}$. Sei $\tau \in \mathrm{Gal}(L/K)$ und sei $b \in L^\times$. Dann ist $|b|_1$ durch die Menge aller $a \in A$ mit $|a| \leq |b|_1$ eindeutig festgelegt. Nun ist aber $|a| \leq |b|_1 \;\Leftrightarrow\; |a| \leq |\tau(b)|_1$, so dass $|b|_1 = |\tau(b)|_1$ folgt. Damit ist $|.|_1$ Galois-invariant.
Ist $|.|$ hingegen diskret, dann auch $|.|_1$ und B ist ein diskreter Bewertungsring, also ist das maximale Ideal ein Hauptideal und die Menge der Erzeuger ist Galois-invariant

und damit sieht man schnell ein, dass $|.|_1$ auch in diesem Fall Galois-invariant ist. □

Satz 5.7.4. *Sei L/K eine separable algebraische Erweiterung und sei $|.|$ ein nichtarchimedischer Betrag auf K. Dann existiert eine Fortsetzung nach L.*

Beweis. Bette K in die Vervollstaendigung K_v ein und L in das Kompositum LK_v. Nun wende den letzten Satz an. □

Beispiele 5.7.5. (a) Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{2})$. Dann gibt es zwei Einbettungen $L \hookrightarrow \mathbb{R}$ und beide liefern zwei verschiedene Fortsetzungen des reellen Betrages auf $\mathbb{Q}$.

(b) Die eindeutige Fortsetzung von $|.|_p$ nach $L = \overline{\mathbb{Q}}_p$ ist nicht diskret, da in L beliebige Wurzeln aus p existieren und ja gelten muss $|p^{\frac{1}{n}}|^n = |p|_p = p^{-1}$, so dass $|p^{1/n}| = 1/\sqrt[n]{p}$ folgt. Die von diesen Elementen erzeugte Untergruppe von $\mathbb{R}^\times$ ist dicht.

* * *

5.8 Lokale Koerper

Definition 5.8.1. Ein Koerper K mit Betrag $|.|$ heisst **lokaler Koerper**, falls K in der Metrik $|.|$ lokalkompakt ist. Dies ist aequivalent dazu, dass der abgeschlossene Einheitsball $\overline{B}_1(0)$ kompakt ist. Jeder lokale Koerper ist vollstaendig.

Beispiele 5.8.2.

(a) $\mathbb{R}$ und $\mathbb{C}$ sind lokale Koerper.

(b) $\mathbb{Q}_p$ ist ein lokaler Koerper.

(c) Ist K ein lokaler Koerper, dann ist jede endliche Erweiterung ebenfalls ein lokaler Koerper.

Beweis. Sei L/K endlich, dann ist als K-Vektorraum, $L \cong K^n$. Man zeigt dann wie in der Analysis, dass L die Produkttopologie traegt und L damit lokalkompakt ist. □

Definition 5.8.3. Sei K ein nichtarchimedischer lokaler Koerper mit Bewertungsring A. Ein Erzeuger π des maximalen Ideals wird auch ein **uniformisierendes Element** genannt.

Proposition 5.8.4. *Sei K vollstaendig in dem nichtarchimedischen Betrag $|.|$. Sei A der Bewertungsring und $\mathfrak{m}$ das maximale Ideal. Dann sind aequivalent:*

(a) *K ist ein lokaler Koeper.*

(b) *Der Restklassenkoerper $A/\mathfrak{m}$ ist endlich.*

Proof. (a)⇒(b): Sei $V \subset A$ ein Vertretersystem von $A/\mathfrak{m}$. Dann ist

$$A = \bigcup_{v \in V} v + \mathfrak{m}$$

eine offene Ueberdeckung des KOmpaktums $A = \overline{B}_1(0)$. Daher reicht eine endliche Teilueberdeckung. Da die Mengen $v + \mathfrak{m}$ aber paarweise disjunkt sind, ist V endlich.

(b)⇒(a): Sei (x_n) ein Folge in A. Wir muessen zeigen, dass sie eine konvergente Teilfolge hat. Da $A/\mathfrak{m}$ endlich ist, gibt es eine Restklasse $v_1 + \mathfrak{m}$, die unendlich viele Folgeglieder enthaelt, oder eine Teilfoilge $x_n^{(1)}$, die in $v_1 + \mathfrak{m}$ liegt. Da auch $A/\mathfrak{m}^2$ endlich ist, gibt es ebenso eine Teilfolge $x_n^{(2)}$ von $x_n^{(2)}$, die in $v_2 + \mathfrak{m}^2$ liegt fuer ein $v_2 \in A$ und so weiter. Im k-ten Schritt erhaelt man eine Teilfolge ($x_n^{(k)}$ die in $v_k + \mathcal{M}^k$ liegt fuer ein $v_k \in A$. Sei $y_n = x_n^{(n)}$. Da fuer $m \leq n$ gilt $y_m - y_n \in v_m + \mathfrak{m}^m$, ist y_n eine Cauchy-Folge, also konvergent. □

Satz 5.8.5. *Sei K ein nichtarchimedischer lokaler Koerper mit Bewertungsring A und Restklassenkoerper $\mathbb{F}_q$. Dann gilt $\mu(K) = \mu_{q-1}$. Es gilt*

$$K^\times \cong \pi^{\mathbb{Z}} \times \mu_{q-1} \times (1 + \pi A).$$

Die Gruppe $A^1 = 1 + \pi A$ heisst Gruppe der **Einseinheiten**.

Beweis. Wegen $K^\times \cong \pi^{\mathbb{Z}} \times A^\times$ reicht es, $A^\times \cong \mu_{q-1} \times A^1$ zu zeigen. Das Polynom $x^{q-1} - 1$ zerfaellt nach Hensels Lemma ueber A in Linearfaktoren, also folgt $\mu_{q-1} \subset K$. Der Homomorphismus $A^\times \to (A/\pi A)^\times$ hat den Kern A^1 und bildet μ_{q-1} bijektiv auf $(A/\pi A)^\times$ ab.

Es bleibt zu zeigen, dass jede Einseinheit unendliche Ordnung hat. Dazu nimm an, dass $(1 + \pi c)^n = 1$. Sei p die Charakteristik des endlichen Koerpers $A/\pi A$.

1. Fall: $p \nmid n$. Fuer gegebenes $k \in \mathbb{N}$ zeigen wir

$$(1 + c\pi^k)^n = 1 \quad \Rightarrow \quad c \equiv 0 \mod (\pi). \tag{$*$}$$

Aus $(*)$ folgt $1 = \sum_{j=0}^{n} \binom{n}{j} c^j \pi^{kj}$, also $nc\pi^k \equiv 0 \mod (\pi^{2k})$ und damit $c \equiv 0 \mod (\pi^k)$ und damit gilt $(*)$. Ist also $(1 + c\pi)^n = 1$, dann kann man $c = d\pi$ schreiben, hat also $(1 + d\pi^2) = 1$ und folgert $d \equiv 0 \mod (\pi)$ oder $c \equiv 1 \mod (\pi^2)$ und so weiter, so dass $c \equiv 0 \mod (\pi^k)$ fuer jedes k folgt und daher $c = 0$.

2. Fall: $p \mid n$, sagen wir $n = p^l m$ mit $p \nmid m$. Dann ist $1 = (1 + c\pi)^n = \left((1 + c\pi)^{p^l}\right)^m$, nach dem ersten Fall also $(1 + c\pi)^{p^l} = 1$. Es reicht dann, den Fall $l = 1$ zu betrachten. Da p die Binomialkoeffizienten $\binom{p}{k}$ teilt, folgt $p\pi c \equiv 0 \mod (p\pi^2)$, also $c \equiv 0 \mod \pi$. Man iteriert diesen Schluss wie im ersten Fall und erhaelt die Behauptung. □

* * *

5.9 Primstellen

Lemma 5.9.1. (a) *Ist $\rho : \mathbb{R} \to \mathbb{C}$ ein stetiger Ringhomomorphismus, dann ist $\eta = \mathrm{Id}$.*

(b) *Ist $\eta : \mathbb{C} \to \mathbb{C}$ ein stetiger Ringhomomorphismus, dann ist $\eta = \mathrm{Id}$ oder η ist die komplexe Konjugation.*

Beweis. (a) Schraenkt man ρ auf $\mathbb{Q}$ ein, dann ist $\rho = \mathrm{Id}$. Da ρ stetig und $\mathbb{Q}$ dicht ist, folgt die Behauptung.

(b) Aus Teil (a) folgt, dass $\eta|_{\mathbb{R}} = \mathrm{Id}$ gilt. Damit ist $\eta : \mathbb{C} \to \mathbb{C}$ eine $\mathbb{R}$-lineare Abbildung. Nun muss $\eta(i)^2 = \eta(i^2) = -1$ sein, also $\eta(i) = \pm i$. Zusammen mit der $\mathbb{R}$-Linearitaet folgt die Behauptung. □

Definition 5.9.2. Eine **Primstelle**, oder **Stelle** eines Zahlkoerpers K ist eine Aequivalenzklasse von Betraegen.

Man sagt von einer Stelle v auch

$$\begin{aligned} v \text{ ist endlich} &\quad\Leftrightarrow\quad v \text{ ist nichtarchimedisch,} \\ v \text{ ist unendlich} &\quad\Leftrightarrow\quad v \text{ ist archimedisch.} \end{aligned}$$

Im ersten Fall schreibt man $v < \infty$ oder $v \nmid \infty$ im zweiten $v|\infty$.

Jedes Primideal $\mathfrak{p}$ von $\mathcal{O} = \mathcal{O}_K$ liefert eine Stelle durch

$$|x|_{\mathfrak{p}} = p^{-k} \quad \Leftrightarrow \quad x \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1},$$

wobei p die Restklassencharakteristik $p = \mathrm{Char}(\mathcal{O}/\mathfrak{p})$ ist.

Satz 5.9.3. (a) *Die Zuordnung $\mathfrak{p} \mapsto |.|_{\mathfrak{p}}$ ist eine Bijektion zwischen der Menge aller Primideale und der Menge aller endlichen Stellen.*

(b) *Jede unendliche Stelle ist induziert von einer Einbettung $K \hookrightarrow \mathbb{C}$, die eindeutig bestimmt ist bis auf komplexe Konjugation.*

Beweis. (a) Sei $\phi : \mathfrak{p} \mapsto |.|_{\mathfrak{p}}$ diese Zuordnung. Es gilt $\mathfrak{p} = \{x \in K : |x|_{\mathfrak{p}} < 1\}$, woraus die Injektivitaet von ϕ folgt.

Fuer die Surjektivitaet sei $|.|$ ein nichtarchimedischer Betrag auf K. Die Einschraenkung von $|.|$ auf $\mathbb{Q}$ liefert einen nichtarchimedischen Betrag, der nach Satz 5.3.1 von der Form $|.|_p$ fuer eine Primzahl p gewaehlt werden kann. Sei $\widehat{K}$ die Vervollstaendigung von K nach $|.|$. Dann ist $\widehat{K}/\mathbb{Q}_p$ eine endliche Erweiterung lokaler Koerper. Nach Satz 5.7.2 gibt es nur eine Fortsetzung von $|.|_p$ nach $\widehat{K}$, also folgt fuer $x \in \widehat{K}$, dass $|x| = \left|N_{\widehat{K}/\mathbb{Q}_p}(x)\right|_p^c$ fuer ein $c > 0$ gilt. Insbesondere ist der Wertebereich von $|.|$ in $(0, \infty)$ diskret und das Primideal $\widehat{\mathfrak{p}} := \{x \in \widehat{K} : |x| < 1\}$ ist ein Hauptideal. Sei π ein Erzeuger. Man kann $|.|$ so waehlen, dass $|\pi| = 1/q$ mit $q = |\mathcal{O}/\mathcal{P}|$ ist. Dann gilt fuer $k \in \mathbb{Z}$,

$$\begin{aligned} x \in \mathfrak{p}^k \setminus \mathfrak{p}^k + 1 &\Leftrightarrow x = \pi^k u, \quad u \in \mathcal{O}_{\widehat{K}}^{\times} \\ &\Leftrightarrow |x| = |\pi|^k = q^{-k}. \end{aligned}$$

(b) Hier ist nur die Eindeutigkeit zu zeigen. Seien $\sigma, \tau : K \to \mathbb{C}$ zwei Einbettungen, die denselben Betrag induzieren, also $|\tau(x)| = |\sigma(x)|$ fuer jedes $x \in K$. Dann ist $\eta = \sigma \circ \tau^{-1} : \tau(K) \to \sigma(K)$ ein Koerperhomomorphismus zweier Teilkoerper von $\mathbb{C}$, der den Betrag erhaelt. Also setzt η zu einem stetigen Koerperhomomorphismus vom Abschluss $\overline{\tau(K)} = \mathbb{R}, \mathbb{C}$ nach $\mathbb{C}$ fort. Auf $\mathbb{Q}$ ist η die Identitaet, also auch auf $\mathbb{R}$. Damit ist ϕ eine $\mathbb{R}$-lineare Abbildung, die i auf $\pm i$ wirft, also ist η – Id oder die komplexe Konjugation. □

Satz 5.9.4 (Diskriminantenteiler)**.** *Sei $K \neq \mathbb{Q}$ ein Zahlkoerper. Fuer eine Primzahl p sind aequivalent:*

(a) *p ist verzweigt in K,*

(b) *p teilt die Diskriminante D_K.*

Beweis. Es reicht, dies fuer einen minimalen Unterkoerper zu beweisen (einmal verzweigt, immer verzweigt), also koennen wir annehmen, dass die Erweiterung K/Q keine Zwischenkoerper hat. Insbesondere ist jedes $\theta \in K \setminus \mathbb{Q}$ ein primitives Element.

Nach Satz 4.3.7 gilt $|D_K| > 1$. Sei p eine Primzahl. Wir schreiben $p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Sei $\mathfrak{q}$ ein Primideal von $\mathcal{O}$, teilerfremd zu $p\mathcal{O}$. Nach dem chinesischen Restsatz gibt es ein $\theta \in \mathfrak{q}$ mit $\theta \equiv 1 \mod p\mathcal{O}$. Liegt θ in $\mathbb{Z}$, ersetzt man es durch $\theta + pb$ mit einem $b \in \mathcal{O} \setminus \mathbb{Z}$ und erreicht, dass $\theta \notin \mathbb{Z}$ gilt. Dann folgt $K = \mathbb{Q}(\theta)$. Nach Satz 2.3.11 wird $D(\theta) = D(1, \theta, \ldots, \theta^{n-1})$ von D_K geteilt.

Wir erinnern an Definition 3.3.10. Der **Fuehrer** von θ ist

$$\mathcal{F}_\theta := \{b \in \mathcal{O} : b\mathcal{O} \subset \mathbb{Z}[\theta]\}.$$

Nun ist $\mathbb{Z}[\theta] = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \cdots \oplus \mathbb{Z}\theta^{n-1}$ Wir betrachten die $\mathfrak{q}$-adische Komplettierung $K_\mathfrak{q}$. Dann ist der Abschluss

$$\overline{\mathbb{Z}[\theta]} = \mathbb{Z}_q[\theta]$$

eine offene Nullumgebung, da $1, \theta, \ldots, \theta^{n-1}$ eine Basis von K ueber $\mathbb{Q}$ ist. Da $\theta \in \mathfrak{q}$, ist $|\theta|_\mathfrak{q} < 1$, also gibt es ein j_0, so dass fuer $j \geq j_0$ gilt

$$\theta^j \mathcal{O}_\mathfrak{q} \subset \overline{\mathbb{Z}[\theta]}.$$

Das bedeutet, dass $\theta^j \in \mathcal{F}_\theta$ gilt. Fuer $i = 1, \ldots, r$ gilt $\theta \notin \mathfrak{p}_i$, also $\theta^j \notin \mathfrak{p}_i$ und daher ist $\mathfrak{p}_i$ und schliesslich

$$p\mathcal{O} \text{ teilerfremd zu } \mathcal{F}_\theta.$$

Damit koennen wir Proposition 3.3.12 anwenden. Falls $p \mid D_K$, dann teilt p die Diskriminante $D(\theta)$ und daher hat das Minimalpolynom $m(x) \in \mathbb{Z}[x]$ von θ modulo p eine mehrfache Nullstelle. Nach Proposition 3.3.12 ist p verzweigt.

Schliesslich gelte $p \nmid D_K$, dann ist zu zeigen, dass p unverzweigt ist. Hierzu beachte, dass wegen $\theta \equiv 1 \mod p\mathcal{O}$ gilt $\mathcal{O} = \mathbb{Z}[\theta] + p\mathcal{O}$. Sei dann $v_j = a_j + b_j$ eine Ganzheitsbasis mit $a_j \in \mathbb{Z}[\theta]$ und $b_j \in p\mathcal{O}$. Dann ist $D_K = D(v_1, \ldots, v_n) \equiv D(\theta) \mod p$. Also wird $D(\theta)$ nicht von p geteilt, so dass nach Proposition 3.3.12 die Primzahl p unverzweigt ist. □

Satz 5.9.5. *Sei K ein Zahlkoerper, $v = |.| = |.|_v$ eine Stelle und sei K_v die Komplettierung an v. Dann ist jede endliche Erweiterung $\widehat{L}/K_v$ die Komplettierung einer endlichen Erweiterung L/K an einer Stelle w ueber v. Man kann L so waehlen, dass $\widehat{L}$ das Kompositum K_vL von K_v und L ist und dass $L \cap K_v = K$ gilt.*

Proof. Im archimedischen Fall ist $L = K$ oder $L = K(i)$ und damit ist die Sache klar.

Sei also $|.|$ nichtarchimedisch. Nach dem Satz vom Primitiven Element koennen wir $\widehat{L} = K_v[x]/f$ annehmen fuer ein normiertes irreduzibles Polynom $f(x) \in K_v[x]$. Da K dicht in K_v liegt, gibt es nach Lemma 5.6.2 ein $g(x) \in K[x]$ mit $\widehat{L} = K_v[x]/g$. Setzt man $L = K[x]/g$, so folgt die Behauptung. □