# Algebraische Zahlentheorie

Inoffizielles Vorlesungsskript im Sommersemester 2019/2020

Universität zu Köln

Dr. Stephan Ehlen

(Notizen von David Wambach)

Die Quelle für dieses Skript ist das handgeschriebene Vorlesungsskript der Vorlesung "Algebraische Zahlentheorie" von Dr. S. Ehlen aus dem Sommersemester 2019/2020 an der Universität zu Köln. Es wurde von einem Studenten zusammengefasst und erhebt keinen Anspruch auf Vollständigkeit oder Korrektheit. Weiterhin sind alle Resultate natürlich wohlbekannt und ich erhebe keinen Anspruch auf Originalität. *Bei Fragen, Kommentaren und insbesondere, falls sie die sicherlich vorhandenen (Tipp-)Fehler finden, wenden Sie sich bitte an uns.*



*Stand: 07. September 2019*; Dieses Skript wird während des Semesters laufend aktualisiert.

# Inhaltsverzeichnis

# Notationen

Liste einiger häufig benutzter Symbole:

| | |
|---|---|
| $\mathbb{N}$ | $= \{1,2,3,4,\dots\}$, die natürlichen Zahlen |
| $\mathbb{Z}$ | $= \{0,1,-1,2,-2,3,-3,\dots\}$, die ganzen Zahlen |
| $\mathbb{Q}$ | der Körper der rationalen Zahlen |
| $\mathbb{R}$ | der Körper der reellen Zahlen |
| $\mathbb{C}$ | der Körper der komplexen Zahlen |
| $\subset$ | Sind $A$ und $B$ Mengen, so bedeutet $A \subset B$, dass $A$ in $B$ enthalten ist und Gleichheit ist nicht ausgeschlossen (d.h. $(A \subset B) \Leftrightarrow (a \in A \Rightarrow a \in B)$) |
| $\subsetneq$ | $A \subset B$ und $A \neq B$ |
| $\lvert A \rvert$ | Die Anzahl der Elemente einer Menge A |
| $m \mid n$ | $m$ teilt $n$ (zum Beispiel in $\mathbb{Z}$: es ex. ein $x \in \mathbb{Z}$, so dass $mx = n$ gilt) |
| $m \nmid n$ | $m$ teilt nicht $n$ |
| $L/K$ | $K \subset L$ Körpererweiterung |
| $[L:K]$ | $= \lvert L/K \rvert$ der Grad der Körpererweiterung. |
| $K(\alpha)$ | $= \{a_0 \cdot \alpha^0 + a_1 \cdot \alpha^1 + a_2 \cdot \alpha^2 + \cdots \mid a_i \in K\}$ Körpererweiterung |
| $gH$ | $= \{g \cdot h \mid h \in H\}$ Restklasse von $g$ modulo $H$ |
| $G/H$ | $= \{gH \mid g \in G\}$ |
| $g \pmod H$ | $= gH \in G/H$ |
| $\mathbb{F}_p$ | $= \mathbb{Z}/p\mathbb{Z}$ Körper |
| Œ | Ohne Beschränkung der Allgemeinheit |

# 0. Motivation/Einleitung

Von Interesse in der Zahlentheorie: Lösen von Diophantischen Gleichungen:
polynomielle Gleichungen mit Koeffizienten in $\mathbb{Z}$ (oder in $\mathbb{Q}$) & dabei werden Ganzzahlige Lösungen gesucht.

Es kann hilfreich sein, hierzu in *Zahlkörpern* zu arbeiten, das sind endliche Körpererweiterungen von $\mathbb{Q}$.

**Beispiel** Welche $n \in \mathbb{N}$ lassen sich als Summe:

$$n = a^2 + b^2$$

mit $a,\ b \in \mathbb{Z}$ schreiben?

Etwas spezieller: Gibt es für ein $p \in \mathbb{N}$ Primzahl $a,\ b \in \mathbb{N}$ mit

$$p = a^2 + b^2 \ ?$$

| | |
|---|---|
| $2 = 1^2 + 1^2$ | ✓ |
| $3 \neq a^2 + b^2$ | X |
| $5 = 2^2 + 1^2$ | ✓ |
| ~~7~~ | X |
| ~~11~~ | X |
| $13 = 3^2 + 2^2$ | ✓ |

Beobachtung:
Ist $p \neq 2$ und $p = a^2 + b^2$ so folgt:

$$p \equiv 1 \pmod 4$$

Denn:

$$\begin{aligned}
\text{mod } 4: \quad 0^2 &\equiv 0 \pmod 4\\
1^2 &\equiv 1 \pmod 4\\
2^2 &\equiv 0 \pmod 4\\
3^2 &\equiv 1 \pmod 4\\
p = 0+0 &\Rightarrow 4 \mid p \ \lightning\\
p = 1+1 &\Rightarrow p \text{ gerade } \lightning
\end{aligned}$$

Es gilt auch die Umkehrung:

**Satz 0.1** Sei $p \neq 2$ eine Primzahl. Dann gilt:

Es existieren $a,\ b \in \mathbb{Z}$ mit $p = a^2 + b^2$ genau dann, wenn $p \equiv 1 \pmod 4$.

■ **Erinnerung** Die *Gaußschen ganzen Zahlen* sind der Ring

$$\mathbb{Z}[i] := \{a + bi \mid a,\ b \in \mathbb{Z}\}.$$

In *Algebra* haben wir gezeigt, dass $\mathbb{Z}[i]$ *euklidisch* („*Division mit Rest*“) ist, daraus folgt dass $\mathbb{Z}[i]$ *faktoriell* („*Eindeutige Primfaktorzerlegung*“) ist. *Gradabbildung* ist die Norm:

$$\begin{aligned}
N : \mathbb{Z}[i] &\longrightarrow \mathbb{N}_0\\
a + bi &\longmapsto a^2 + b^2.
\end{aligned}$$

Die Norm ist multiplikativ: $N(x \cdot y) = N(x) \cdot N(y)$.
Division mit Rest: Sei $b \in \mathbb{Z}[i] \setminus \{0\}$. Dann gilt: $\forall a \in \mathbb{Z}[i] :\ \exists\, q, r \in \mathbb{Z}[i]$ mit:

$$a = q \cdot b + r \text{ und } N(r) < N(b).$$

---

*Beweis von Satz 0.1:* Beweisstrategie:
„⇒“
Im Beispiel vorher gezeigt.

„⇐“
Sei $p = 1 \pmod 4$, so ist $p \in \mathbb{Z}[i]$ nicht prim ($\Leftrightarrow$ nicht irreduzibel).

$$\begin{aligned}
&\Rightarrow \exists\, x,\ y \in \mathbb{Z}[i] \setminus (\mathbb{Z}[i]^\times \cup \{0\}) \text{ mit:}\\
&\quad p = x \cdot y\\
&\text{Erinnerung: } \mathbb{Z}[i]^\times = \{\pm 1,\ \pm i\} = \{x \in \mathbb{Z}[i] \mid N(x) = 1\}\\
&\Rightarrow N(p) = p^2 = N(x \cdot y) = N(x) \cdot N(y), \text{ wobei gilt: } N(x) \neq 1 \neq N(y).\\
&\Rightarrow N(x) = N(y) = p\\
&\Rightarrow \text{Ist z.B.: } x = a + bi \in \mathbb{Z}[i], \text{ so folgt: } p = N(x) = a^2 + b^2.
\end{aligned}$$

Noch zu zeigen ist:
$p$ ist in $\mathbb{Z}[i]$ nicht prim.

## 0.1 Zahlentheorie

**Satz — Satz von Wilson.**

$$p \text{ Primzahl} \iff -1 \equiv (p-1)! \pmod{p}.$$

*Beweis:* „⇒“
Sei $p$ Primzahl.

$$\begin{aligned}(p-1)! &= (p-1)\cdot(p-2)\cdot(p-3)\cdot\dots\cdot 3\cdot 2\cdot 1\\ &\equiv (-1)\cdot(p-2)\cdot(p-3)\cdot\dots\cdot 3\cdot 2\cdot 1 \pmod{p}.\end{aligned}$$

Zu zeigen ist demnach: $(p-2)\cdot(p-3)\cdot\dots\cdot 3\cdot 2\cdot 1 \equiv 1 \pmod{p}$.
Die Menge der Faktoren $\{1,2,\dots,p-1\}$ entspricht genau den Einheiten in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Da $\mathbb{F}_p$ Körper ist, hat die Gleichung:

$$x^2 \equiv 1 \pmod{p}$$

modulo $p$ genau 2 Lösungen ($x \equiv \pm 1 \pmod{p}$).
Deshalb: Für $x \in \mathbb{F}_p$ mit $x \neq \pm 1$ gilt:

$$x \neq x^{-1}$$

$$\Rightarrow (p-2)\cdot(p-3)\cdot\dots\cdot 3\cdot 2 \equiv 1 \pmod{p},$$

da Inverse immer eindeutig sind und demnach hier immer Paare von Faktoren vorliegen, die 1 (mod $p$) ergeben.

„⇐“
Rückrichtung wird für den Beweis von Satz 0.1 nicht benötigt und hier nicht gezeigt. ∎

---

*Fortsetzung des Beweises von Satz 0.1:*
Zu zeigen ist noch: Ist $p \equiv 1 \pmod{4}$, so ist p nicht prim in $\mathbb{Z}[i]$.
Schreibe $p = 4n+1$ mit $n \in \mathbb{N}$.

Behauptung: $\exists\, x \in \mathbb{Z}$ mit $x^2 \equiv -1 \pmod{p}$.
Daraus würde folgen, dass $x^2 + 1 \equiv 0 \pmod{p} \Rightarrow p \mid (x^2+1)$.

Beweis:

$$\begin{aligned}-1 &\equiv (p-1)! \pmod{p} \quad (\textit{Satz von Wilson}).\\ &= (1\cdot 2\cdot\dots\cdot 2n)\cdot[(p-2n)\cdot(p-2n+1)\cdot\dots\cdot(p-2)\cdot(p-1)]\\ &= (2n)!\cdot[(p-2n)\cdot(p-2n+1)\cdot\dots\cdot(p-2)\cdot(p-1)]\\ &\equiv (2n)!\cdot[(-2n)\cdot(-2n+1)\cdot\dots\cdot(-2)\cdot(-1)] \pmod{p}\\ &= (2n)!\cdot[(-2n)\cdot(-(2n-1))\cdot\dots\cdot(-2)\cdot(-1)]\\ &= (2n)!\cdot(-1)^n\cdot(2n)!\\ &\equiv [(2n)!]^2 \pmod{p}\end{aligned}$$

$$\Rightarrow p \mid (x^2+1) = (x+i)(x-i) \in \mathbb{Z}[i]$$

Erinnerung: $p$ prim $\iff (p \mid \alpha \cdot \beta \Rightarrow p \mid \alpha \ \vee p \mid \beta)$
Aber: $p \nmid (x+i)$ und $p \nmid (x-i)$, denn $p \nmid x$. ∎

---

Standpunkt der Algebraischen Zahlentheorie:
$\mathbb{Z}[i]$ ist der *„Ring der ganzen Zahlen"* im quadratischen Zahlkörper $\mathbb{Q}[i] := \{a+bi \mid a,b \in \mathbb{Q}\}$.

**Satz 0.2**

$$\mathbb{Z}[i] = \{\alpha \in \mathbb{Q}[i] \mid \mathrm{Mipo}_\alpha \in \mathbb{Z}[X]\} \tag{1}$$
$$= \{\alpha \in \mathbb{Q}[i] \mid \exists\ m,n \in \mathbb{Z} :\ \alpha^2 + m\alpha + n = 0\} \tag{2}$$

*Beweis:* Es reicht, (2) zu zeigen: Sei $\alpha = a+bi \in \mathbb{Z}[i]$.

$$\alpha^2 - 2a(a+bi) + a^2 + b^2 = 0$$

Klar: $-2a \in \mathbb{Z},\ a^2+b^2 \in \mathbb{Z}$.
$\Rightarrow$ „$\subset$"

„$\supset$"
Angenommen $\alpha = a+bi \in \mathbb{Q}(i)$ mit $m := -2a \in \mathbb{Z}$ und $n := a^2+b^2 \in \mathbb{Z}$.

$$\begin{aligned}
&\Rightarrow m^2 + 4b^2 = 4n \\
&[\Rightarrow 4b^2 = 4n - m^2 \in \mathbb{Z}] \\
&\Rightarrow m^2 + (2b)^2 \equiv 0 \pmod 4 \\
&\Rightarrow m^2 \equiv (2b)^2 \equiv 0 \pmod 4 \quad (\text{denn: } \forall x \in \mathbb{Z} :\ x^2 \equiv 0,1 \pmod 4) \\
&\Rightarrow b \in \mathbb{Z} \\
&m^2 = (-2a)^2 \Rightarrow a \in \mathbb{Z}
\end{aligned}$$

∎

---

Ein weiteres Beispiel:

**Satz — Fermat's letzter Satz (vermutet 1637).**

$x^n + y^n = z^n$ hat für $n \geq 3$ keine ganzzahligen Lösungen mit $xyz \neq 0$.

Bewiesen 1994 durch Andrew Wiles (& viele Vorarbeiter), mit Elliptischen Kurven und Modulformen. Kummer: Beweis für $n = p$ reguläre Primzahl am Ende des Semesters.

**Beispiel** $x^2 + 2 = y^3$ hat nur die Lösungen $(\pm 5, 3)$.

*Beweis:* Übung. ∎

---

# 1. Ganze Algebraische Zahlen

**Definition 1.1**
- Ein Körper $K$ mit $\text{char}(K) = 0$ heißt *(algebraischer) Zahlkörper*, falls ${}^{K}/_{\mathbb{Q}}$ eine endliche Körpererweiterung ist.
- Eine algebraische Zahl $\alpha \in K$ wird *ganz* genannt, falls ein normiertes Polynom $f \in \mathbb{Z}[X]$ existiert, mit:

$$f(\alpha) = 0$$

- $\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ ganz}\}$ heißt *Ring der ganzen Zahlen in K*.

Allgemeiner (Im folgenden sind alle Ringe kommutativ mit 1):

**Definition 1.2** Sei $R \subset S$ Ringerweiterung
- $s \in S$ heißt *ganz über R*, falls es ein normiertes Polynom $f \in R[X]$ gibt, mit $f(s) = 0$.
- S heißt *ganz über R*, falls $s \in S$ ganz über R $\forall s \in S$.

Wir wollen zeigen: Der *ganze Abschluss von R in S*, $\overline{R} := \{s \in S \mid s \text{ ist ganz über } R\}$ ist ein Unterring von S.

## 1.1 Einschub zu Moduln

**Definition 1.3** Sei R ein Ring. Ein *R-Modul* ist eine abelsche Gruppe $(M, +)$ mit einer Skalarmultiplikation:

$$\begin{aligned} R \times M &\longrightarrow M \\ (r, m) &\longmapsto r \cdot m \end{aligned}$$

Mit $1 \cdot m = m$, so dass gilt:
1. $\forall r, s \in R,\ \forall m \in M: \quad r \cdot (s \cdot m) = (r \cdot s) \cdot m$
2. $\forall r, s \in R,\ \forall m \in M: \quad (r + s) \cdot m = r \cdot m + s \cdot m$
3. $\forall r \in R,\ \forall m, m' \in M: \quad r \cdot (m + m') = r \cdot m + r \cdot m'$

Genauso wie bei Vektorräumen definiert:
- R-Modul-Homomorphismus
- Untermoduln
- Restklassenmodul: $M/N$ $\quad (N \subset M$ Untermodul)

**Beispiel**
1. Sei $R$ Ring. Dann ist $R$ ein R-Modul. Die Untermoduln sind genau die Ideale in $R$. Ist $\mathfrak{a} \subset R$ Ideal $\Rightarrow R/\mathfrak{a}$ ist auch ein R-Modul.
2. Sei G abelsche Gruppe. Dann ist G ein $\mathbb{Z}$-Modul durch:

$$\mathbb{Z} \times G \longrightarrow G$$
$$(n,g) \longmapsto n \cdot g = \begin{cases} \sum_{i=1}^{n} g & \text{für } n \geq 0 \\ -(-n) \cdot g & \text{für } n < 0 \end{cases}$$

   Also: $\mathbb{Z}$-Moduln sind genau die abelschen Gruppen.
3. $K$ Körper, $V$ $K$-Vektorraum (Klar: $V$ ist $K$-Modul)
   Sei $\varphi \in \mathrm{End}_K(V)$. Dann ist $V$ ein $K[X]$-Modul durch:

$$K[X] \times V \longrightarrow V$$
$$(\sum_{i=0}^{n} a_i x^i, v) \longmapsto \sum_{i=0}^{n} a_i \varphi^i(v)$$

Übung:

$$\{(v,\varphi) \mid V \text{ } K\text{-Vektorraum}, \varphi \in \mathrm{End}_K(V)\} \longrightarrow \{V \mid V \text{ ist } K[X]\text{-Modul}\}$$

ist bijektiv

**Definition** Summen: Sei $M_i \subset M$ $(i \in I)$ eine Familie von Untermoduln. Dann heißt:

$$M' := \sum_{i \in I} M_i = \{\sum_{i \in I} x_i \mid x_i \in M_i,\ x_i = 0 \text{ für fast alle } i\}$$

*direkte Summe* der $M_i$, falls jedes $x \in M'$ eine eindeutige Darstellung $x = \sum_{i \in I} x_i$ hat.

■ **Bemerkung** $M' \subset M$ ist direkte Summe von $M_1 \subset M$ und $M_2 \subset M$
$\iff$ *i)* $M' = M_1 + M_2$ und *ii)* $M_1 \cap M_2 = \{0\}$

---

**Definition 1.4**
- Eine Familie $(x_i)_{i \in I} \subset M$ heißt *Erzeugendensystem* von M, falls

$$M = \sum_{i \in I} R \cdot x_i,$$

  wobei $R \cdot x_i := \{r \cdot x_i \mid r \in R\}$
- $M$ heißt *endlich erzeugt*, falls es ein Erzeugendensystem von $M$ gibt, das endlich ist.
- Die Familie $(x_i)_{i \in I}$ heißt *frei* (oder *linear unabhängig*), falls gilt:

$$\sum_{i \in I} r_i \cdot x_i = 0 \ \ (r_i \in R) \Rightarrow \forall i \in I : \ r_i = 0$$

- Ein freies Erzeugendensystem heißt *Basis*.
- Ein Modul, der eine Basis besitzt, heißt *frei*.

**Beispiel**
1. Der Modul $R^n$ ist endlich erzeugt und frei ($n \in \mathbb{N}$)
2. Sei $m \in \mathbb{N}$, $M := \mathbb{Z}/m\mathbb{Z}$ ist endlich erzeugter $\mathbb{Z}$-Modul aber nicht frei.
3. Allgemeiner: $R$ Ring, $\{0\} \neq \mathfrak{a} \subsetneq R$ Ideal $\Rightarrow R/\mathfrak{a}$ ist nicht frei.
4. $\frac{a}{b} \in \mathbb{Q}^\times$, $b \neq \pm 1$, $\mathrm{ggT}(a,b) = 1$
   $\Rightarrow \mathbb{Z}[\frac{a}{b}]$ ist nicht endlich erzeugt als $\mathbb{Z}$-Modul.

Ab jetzt: $R \subset S$ Ringerweiterung und sind $s_1, \ldots, s_n \in S$, so gilt:

$$R[s_1,\ldots,s_n] := \mathrm{Bild}(\, R[X_1,\ldots,X_n] \longrightarrow S)$$
$$f(X_1,\ldots,X_n) \longmapsto f(s_1,\ldots,s_n)$$

## 1.2 Charakterisierung ganzer Zahlen

**Satz 1.5** Die Elemente $s_1, \ldots, s_n \in S$ sind genau dann alle ganz über $R$, falls $R[s_1,\ldots,s_n]$ als $R$-Modul endlich erzeugt ist.

*Beweis:* „⇒“
$R' := R[s_1,\ldots,s_n]$, Induktion nach $n \in \mathbb{N}$:
$\underline{n = 1}$
$R' = R[s_1]$ mit $s_1$ ganz über R, sei $f \in R[X]$ normiert mit $f(s_1) = 0$.
Sei $\alpha \in R' \Rightarrow \exists\, g \in R[X]$ mit $\alpha = g(s_1)$. Division mit Rest: $g = f \cdot q + r$, $\mathrm{grad}(r) < \mathrm{grad}(f)$
$\Rightarrow \alpha = g(s_1) = 0 + r(s_1) \Rightarrow 1, s_1, s_1^2, \ldots, s_1^{n-1}$ ist ein Erzeugendensystem von $R[s_1]$

$\underline{n \mapsto n+1}$
$\widetilde{R} := R[s_1,\ldots,s_n]$, $R' = R[s_1,\ldots,s_{n+1}] = \widetilde{R}[s_{n+1}]$

$$\left.\begin{array}{l}\text{Induktionsanfang} \Rightarrow \widetilde{R} \text{ ist endlich erzeugt über } R \\ \underline{n=1} \Rightarrow R' \text{ ist endlich erzeugt über } \widetilde{R}\end{array}\right\} R' \text{ ist endlich erzeugt über } R$$

„⇐“
Annahme: $R' = R[s_1,\ldots,s_n]$ ist endlich erzeugt über $R$ mit Erzeugendensystem $\alpha_1, \ldots, \alpha_m \in R'$

$$\text{Sei } x \in R' \Rightarrow x \cdot \alpha_i = \sum_{j=1}^{m} a_{ij} \cdot \alpha_j \text{ mit } a_{ij} \in R. \qquad (\star)$$

$A := (a_{ij})_{i,j} \in R^{m \times m}$
$B := x \cdot E_m - A \in R^{m \times m}$, mit $E_m \in R^{m \times m}$ der Einheitsmatrix.
La-Place-Entwicklung:
$B^\star := (b_{ij}^\star)$ ist die komplementäre Matrix mit $b_{ij}^\star = (-1)^{i+j} \cdot \det(B_{ji})$. $B_{ji}$ entsteht durch Streichen der $j$-ten Zeile und $i$-ten Spalte.
$B \cdot B^\star = B^\star \cdot B = \det(B) \cdot E_m$, insbesondere: $B \cdot y = 0$ für $y \in R^m \Rightarrow \det(B) \cdot y = 0$

$$\Rightarrow B \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = 0, \text{ wegen } (\star)$$

$$\Rightarrow \det(B) \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = 0 \Rightarrow \det(B) \cdot \alpha_i = 0 \quad \forall i = 1,\ldots,m$$

$$1 = \sum_{i=1}^{m} c_i\alpha_i \Rightarrow \det(B) = \det(B)\cdot\sum_{i=1}^{m} c_i\alpha_i = \sum_{i=1}^{m} c_i\cdot\underbrace{(\det(B)\cdot\alpha_i)}_{\|\,0} = 0$$

$\Rightarrow f(X) := \det(X\cdot E_m - A) \in R[X]$ hat $x \in R'$ als Nullstelle. $\Rightarrow x$ ist ganz über $R$ ∎

---

**Korollar 1.6** Der ganze Abschluss $\overline{R} := \{s \in S \mid s \text{ ist ganz über } R\}$ ist ein Unterring von $S$

*Beweis:* $1 \in R \subset \overline{R}$ ✓
Seien $\alpha, \beta \in \overline{R} \Rightarrow R[\alpha,\beta]$ ist endlich erzeugt über $R$
$\Rightarrow R[\alpha,\beta,\alpha\pm\beta,\alpha\cdot\beta]$ ist endlich erzeugter $R$-Modul.
$\Rightarrow$ mit Satz (1.5): $\alpha\pm\beta,\ \alpha\cdot\beta \in \overline{R}$ ∎

---

(Speziell: $R = \mathbb{Z}$, $K/\mathbb{Q}$ Zahlkörper, $\mathcal{O}_K$ = Ring der ganzen Zahlen in $K = \overline{\mathbb{Z}} \subset K$ ist tatsächlich ein Ring)

**Korollar 1.7** Seien $R \subset S \subset T$ Ringerweiterungen und es sei $S$ ganz über $R$ sowie $T$ ganz über $S$. Dann ist auch $T$ ganz über $R$.

*Beweis:* Sei $t \in T$. Da $t$ ganz über $S$ ist, folgt:
$0 = t^n + a_{n-1}\cdot t^{n-1} + \cdots + a_1\cdot t + a_0$ mit $a_0,\ldots,a_{n-1} \in S$.
Da $S$ ganz über $R$ ist, sind $a_0,\ldots,a_{n-1}$ ganz über $R$.
$\overset{(1.5)}{\Longrightarrow}$ $R' := R[a_0,\ldots,a_{n-1}]$ ist endlich erzeugt als $R$-Modul.
$t$ ist ganz über $R'$ $\overset{(1.5)}{\Longrightarrow}$ $R'[t]$ ist endlich erzeugter $R'$-Modul
$\Rightarrow R'[t]$ endlich erzeugter $R$-Modul $\overset{(1.5)}{\Longrightarrow}$ $t$ ist ganz über $R$ ∎

---

**Definition 1.8** Sei $R \subset S$ Ringerweiterung. $R$ heißt *ganzabgeschlossen in $S$*, falls $\overline{R} = R$ gilt. Speziell: $R$ Integritätsring, $K = Q(R)$ der Quotientenkörper, dann heißt $\overline{R} \subset K$ auch *Normalisierung* von $R$. Falls in diesem Fall $\overline{R} = R$ gilt, so heißt $R$ *ganzabgeschlossen (schlechthin)*.

**Proposition 1.9** Jeder faktorielle Ring ist ganzabgeschlossen.

---

*Beweis:*
$K := Q(R)$, sei $x = \frac{a}{b} \in K$ (d.h. $a,b \in R$) ganz über R:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \quad \text{mit } a_0,\ldots,a_{n-1} \in R:$$
$$\overset{\cdot b^n}{\Longrightarrow} a^n + a_{n-1}\cdot b\cdot a^{n-1} + \cdots + a_1\cdot b^{n-1}\cdot a + a_0\cdot b^n = 0$$

Sei $p \in R$ prim mit $p \mid b \Rightarrow p \mid (a_{n-1}\cdot b\cdot a^{n-1} + \cdots + a_1\cdot b^{n-1}\cdot a + a_0\cdot b^n) = -a^n$
$\Rightarrow p \mid a^n \Rightarrow p \mid a \overset{p \text{ beliebig}}{\Longrightarrow} x = \frac{a}{b} \in R$ ∎

---

**Beispiel** $\mathbb{Z}$ ist ganzabgeschlossen (in $\mathbb{Q}$).

| | |
|---|---|
| Ab jetzt: $R$ ist ganzabgeschlossener Integritätsring (in $K$) | z.B: $R = \mathbb{Z}$ |
| $K = Q(R)$ | $K = \mathbb{Q}$ |
| $L/K$ ist endliche Körpererweiterung | $L/K$ Zahlkörper |
| $S = \overline{R} \subset L$ (der ganze Abschluss von $R$ in $L$) | $S = \mathcal{O}_L$ |

■ **Bemerkung** $S$ ist ganzabgeschlossen (in $Q(S)$) nach (1.7)

---

■ **Bemerkung** a) Ist $\alpha \in L \Rightarrow \exists\, r \in R,\ s \in S$ mit $\alpha = \frac{s}{r}$. Insbesondere: $L = Q(S)$
b) $\alpha \in L$ ganz über $R \iff$ das Minimalpolynom $f_\alpha$ hat Koeffizienten in $R$ ($f_\alpha \in R[X]$)

---

*Beweis:* a) Sei $\alpha \in L$ mit $a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + \cdots + a_1 \cdot \alpha + a_0 = 0$, wobei $a_0, \ldots, a_n \in R$ mit $a_n \neq 0$ (wird durch Ausmultiplizieren der Nenner erreicht)

$$\overset{\cdot a_n^{n-1}}{\Longrightarrow} \underbrace{a_n^n \cdot \alpha^n}_{\| \ (a_n\alpha)^n} + \underbrace{a_{n-1} \cdot a_n^{n-1} \cdot \alpha^{n-1}}_{\| \ a_{n-1}(a_n\alpha)^{n-1}} + \cdots + \underbrace{a_1 \cdot a_n^{n-1} \cdot \alpha}_{\| \ a_1 \cdot a_n^{n-2}(a_n \cdot \alpha)} + a_0 \cdot a_n^{n-1} = 0$$

$$a_n' := 1,\ a_{n-1}' := a_{n-1},\ a_{n-2}' := a_{n-2} \cdot a_n, \ldots,\ a_0' := a_0 \cdot a_n^{n-1} \in R$$

$\Rightarrow S \ni s := (a_n \cdot \alpha)$ ist ganz über R
$\Rightarrow \alpha = \frac{s}{r}$ mit $r = a_n \in R$

b) „$\Leftarrow$“ klar
„$\Rightarrow$“ Sei $\alpha \in L$ ganz über $R$ mit $g(\alpha) = 0$ mit $g \in R[X]$ normiert und sei $f_\alpha$ das Minimalpolynom von $\alpha$ über $K$.

$\Rightarrow f_\alpha \mid g$ in $K[X]$ $\qquad (\star)$

Sei $Z$ ein Zerfällungskörper von $f_\alpha$ über $L$.

$\Rightarrow f_\alpha(X) = (X - \alpha_1) \cdot \cdots \cdot (X - \alpha_m) \in Z[X]$

$\overset{(\star)}{\Longrightarrow}$ $\alpha_1, \ldots, \alpha_m$ sind Nullstellen von $g \Rightarrow \alpha_1, \ldots, \alpha_m$ sind ganz über R

Sei $f_\alpha(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0$ mit $a_0, \ldots, a_{m-1} \in K$

Da $\alpha_1, \ldots, \alpha_m$ ganz über $R$ sind folgt, dass $\underbrace{a_0, \ldots, a_{m-1}}_{\in R[\underbrace{\alpha_1, \ldots, \alpha_m}_{\text{ganz über } R}] \cap K}$ ganz über $R$ sind mit Korollar (1.6).

$$\Downarrow$$

$R[\alpha_1, \ldots, \alpha_m] \cap K = R$, da $R$ ganzabgeschlossen ist

$\Rightarrow f_\alpha \in R[X]$ ■

---

Speziell von Interesse für uns:
$R = \mathbb{Z}$, $K = \mathbb{Q}$, $L/\mathbb{Q}$ Zahlkörper, $S = \overline{\mathbb{Z}} =: \mathcal{O}_L$ Ring der ganzen Zahlen in $L$. Die Bemerkung sagt in diesem Fall:
a) Ist $\alpha \in L \Rightarrow \exists\, m \in \mathbb{Z}$ mit $m \cdot \alpha \in \mathcal{O}_L$
b) $\mathcal{O}_L = \{\alpha \in L \mid f_\alpha \in \mathbb{Z}[X]\}$

### 1.2.1 Spur, Norm und Diskriminante

**Definition 1.10** Sei $x \in L$. Betrachte die $K$-lineare Abbildung:

$$\begin{aligned} T_x : L &\longrightarrow L \\ \alpha &\longmapsto x \cdot \alpha \end{aligned}$$

Wir definieren die *Spur* und *Norm* von $x$ als:

$$\begin{aligned} Tr_{L/K}(x) &:= Tr(T_x) && \text{(Spur von } x := \text{ Spur von } T_x) \\ N_{L/K}(x) &:= \det(T_x) && \text{(Norm von } x := \text{ Norm von } T_x) \end{aligned}$$

■ **Erinnerung** $T_x \in \mathrm{End}_K(L)$, wobei $L$ als $K$-Vektorraum betrachtet wird.
Ist $B$ eine Basis von $L$ als $K$-VR, so ist

$$\begin{aligned} Tr(T_x) &:= Tr(M_B^B(T_x)), \text{ wobei } M_B^B(T_x) \text{ die Darstellungsmatrix von } T_x \text{ bzgl. } B \text{ ist.} \\ \det(T_x) &:= \det(M_B^B(T_x)) \end{aligned}$$

Aus der linearen Algebra ist bekannt, dass dies unabhängig ist von der Wahl der Basis $B$.

---

**Beispiel** $R = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $S = \mathcal{O}_L = \mathbb{Z}[i]$, Basis von $L/K$ ist: $B = (1, i)$
$x = i \in \mathbb{Q}(i)$. Dann hat $T_x = T_i$ die Abbildungsmatrix: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
Demnach folgt: $Tr_{\mathbb{Q}(i)/\mathbb{Q}}(i) = 0$, $N_{\mathbb{Q}(i)/\mathbb{Q}}(i) = 1$.
Für $x = a + b \cdot i \in \mathbb{Q}(i)$ ist die Matrix von $T_x$: $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.
$\Rightarrow Tr_{\mathbb{Q}(i)/\mathbb{Q}}(x) = 2 \cdot a$, $N_{\mathbb{Q}(i)/\mathbb{Q}}(x) = a^2 + b^2$

■ **Bemerkung 1.11** a) Ist $P_x(t) := \det(t \cdot \mathrm{Id}_L - T_x) = t^n - a_{n-1} \cdot t^{n-1} + \cdots + (-1)^n \cdot a_0 \in K[t]$ mit $n = [L : K]$ das charakteristische Polynom von $T_x$, so gilt:
$a_{n-1} = Tr_{L/K}(x)$
$a_0 = N_{L/K}(x)$
b) $\forall\, x, y \in L$ :
$T_{x+y} = T_x + T_x$ und $T_{x \cdot y} = T_x \circ T_y$
c) Deshalb definieren Spur und Norm (Gruppen-)Homomorphismen:
$Tr_{L/K} : L \longrightarrow K$ (additiv)
$N_{L/K} : L^\times \longrightarrow K^\times$ (multiplikativ)

---

*Beweis:* Lineare Algebra ■

---

**Satz 1.12** a) Sei $L = K(\beta)$ & $f_\beta = X^n - a_{n-1} \cdot X^{n-1} + \cdots + (-1)^n \cdot a_0 \in K[X]$ das Minimal-

polynom von $\beta$ über $K$. Dann gilt:

$$a_{n-1} = Tr_{L/K}(\beta), \quad a_0 = N_{L/K}(\beta)$$

b) Sei $L/K$ endlich, $\beta \in L$, $m := [L : K(\beta)]$. Dann ist:

$$Tr_{L/K}(\beta) = m \cdot Tr_{K(\beta)/K}(\beta), \quad N_{L/K}(\beta) = (N_{K(\beta)/K}(\beta))^m$$

*Beweis:* a) Übung $\rightsquigarrow$ Basis $(1, \beta, \beta^2, \ldots, \beta^{n-1})$
b) $B := \{b_1, \ldots, b_n\}$ Basis von $K(\beta)/K$, $C := \{c_1, \ldots, c_m\}$ Basis von $L/K(\beta)$
$\rightsquigarrow D := \{b_1c_1, b_2c_1, \ldots, b_nc_1, \ldots\ldots, b_1c_m, \ldots, b_nc_m\}$ Basis von $L/K$.

Ist $A \in K^{n\times n}$ Matrix (bezüglich $B$) von $T_\beta\big|_{K(\beta)}$, so ist $M := \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix} \in K^{mn\times mn}$ die Matrix von $T_\beta$ bzgl. Basis $D$.

$$\Rightarrow \det(M) = \det(A)^m \overset{a)}{=} (N_{K(\beta)/K}(\beta))^m$$
$$Tr(M) = m \cdot Tr(A) \overset{a)}{=} m \cdot Tr_{K(\beta)/K}(\beta)$$

■

**Satz 1.13** Sei nun $L/K$ separabel (und endlich). Es sei $N/L$ die normale Hülle von $L/K$. Seien $\sigma_1, \ldots, \sigma_n : L \to N$ die verschiedenen $K$-linearen Einbettungen von $L$ nach $N$. Dann gilt für $x \in L$ und $P_x(t) \in K[t]$ das charakteristische Polynom von $T_x$:

1. $P_x(t) = \prod_{i=1}^{n} (t - \sigma_i(x))$
2. $Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$
3. $N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$

■ **Bemerkung**
- Oft wird der Satz so formuliert: $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$ verschiedene Einbettungen von $L$ in den algebraischen Abschluss $\overline{K}$ von $K$ (äquivalent)
- Ist $L/K$ Galoiserweiterung $\rightsquigarrow \mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$
- $L/\mathbb{Q}$ Zahlkörper. Verstehe $\sigma_1, \ldots, \sigma_n : L \to \mathbb{C}$ als Einbettungen von $L$ nach $\mathbb{C}$.

*Beweis von Satz (1.13):* 1. Sei $x \in L \Rightarrow K(x)/K$ ist separabel, da $L/K$ separabel ist.
Ist $\mathrm{Hom}_K(K(x), N) = \{\tau_1, \ldots, \tau_m\}$, so folgt für $f_x \in K[t]$ das Minimalpolynom von x über K:

$$f_x(t) = \prod_{i=1}^{m} (t - \tau_i(x))$$
$$= t^m - a_{n-1} \cdot t^{m-1} + \cdots + (-1)^m \cdot a_0$$

Ist $d := [L : K(x)]$, so gilt:

$P_x(t) = (f_x(t))^d$ (nach der Argumentation von Satz 1.12 a) und b)).

$$d := [L : K(x)] = |\mathrm{Hom}_{K(x)}(L,N)| = |\mathrm{Hom}_\tau(L,N)| \quad \forall \tau \in \mathrm{Hom}_K(K(x),N)$$

$$P_x(t) = f_x(t)^d = \prod_{i=1}^{m}(t-\tau_i(x))^d = \prod_{i=1}^{m}[\prod_{\sigma\in \mathrm{Hom}_{\tau_i}(L,N)}(t-\sigma(x))] = \prod_{\sigma\in\mathrm{Hom}_K(L,N)}(t-\sigma(x)),$$

da $\mathrm{Hom}_K(L,N) = \dot\cup_{i=1}^{n} \mathrm{Hom}_{\tau_i}(L,N)$. *Bewiesen in Algebra, Lemma 4.4.* $\Rightarrow$ 1. ∎

---

**Beispiel** $L = \mathbb{Q}(\sqrt{D})$, $D$ quadratfrei. Galoiserweiterung $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sqrt{D} \mapsto -\sqrt{D}\}$.
Sei $x = a + b\cdot\sqrt{D} \in L$, $a,b \in \mathbb{Q}$.

$$\Rightarrow Tr_{L/\mathbb{Q}}(x) = 2a = (a+b\sqrt{D}) + (a-b\sqrt{D})$$
$$N_{L/\mathbb{Q}}(x) = (a+b\sqrt{D})\cdot(a-b\sqrt{D}) = a^2 - D\cdot b^2$$

**Korollar 1.14** Seien $K \subset L \subset M$ separable & endliche Körpererweiterungen. Dann gilt:

$$Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L} \quad \text{und} \quad N_{M/K} = N_{L/K} \circ N_{M/L}$$

*Beweis:* Übung ∎

---

**Proposition 1.15** Sei $R$ ganzabgeschlossener Integritätsring, $K = Q(R)$, $S = \overline{R} \subset L$, $L/K$ endliche und separable K-Erweiterung. Sei $x \in S$.

a) Dann sind $Tr_{L/K}(x) \in R$ und $N_{L/K}(x) \in R$.

b) Außerdem:

$$x \in S^\times \iff N_{L/K}(x) \in R^\times$$

---

*Beweis:* a) Hier für $Tr_{L/K}$:
Sei $\{\sigma_1,\dots,\sigma_n\} = \mathrm{Hom}_K(L,N)$, wobei $N$ die normale Hülle ist. Für $x \in S$ ($\Rightarrow x \in L$ & $x$ ganz über $R$) folgt:
$\Rightarrow \sigma_1(x),\dots,\sigma_n(x)$ ganz über R, da es alle Nullstellen von dem Minimalpolynom $f_x \in R[X]$ von $x$ über $K$ sind.
$\overset{\text{Satz (1.13)}}{\Rightarrow}$ $K \ni Tr_{L/K}(x)$ ganz über $R$, da der ganze Abschluss von $R$ Unterring von $N$ ist (selbes Argument mit Norm).
$\overset{R \text{ ganzabg.}}{\Rightarrow}$ $Tr_{L/K}(x) \in R$

b) „$\Leftarrow$“ Angenommen $N_{L/K}(x) \in R^\times$
$\Rightarrow \exists\, a \in R^\times$:

$$a\cdot N_{L/K}(x) = 1$$
$$= a\cdot\prod_{i=1}^{n}\sigma_i(x)$$
$$\underset{\sigma_1=\mathrm{id}_L}{\overset{\text{Ø}}{=}} x\cdot \underbrace{(\prod_{i=2}^{n}(\sigma_i(x))\cdot a)}_{\in L \text{ und ganz über } R \Rightarrow \in S}$$

Es folgt also:
$L \ni x^{-1} = \prod_{i=2}^{n}\sigma_i(x)\cdot a$, da $a \in R^\times$ & $\sigma_i(x)$ ganz über $R\ \forall\ i$

$\Rightarrow \prod_{i=2}^{n} \sigma_i(x) \cdot a \in S \Rightarrow x \in S^\times$

„⇒“

Ist $x \in S^\times \Rightarrow 1 = N_{L/K}(1) = N_{L/K}(x \cdot x^{-1}) = N_{L/K}(x) \cdot \underbrace{N_{L/K}(x^{-1})}_{\substack{\cap\!\!\!\cup \\ R}} \overset{\substack{S \\ \cup\!\!\!\cap}}{\Rightarrow} N_{L/K}(x) \in R^\times$ ∎

---

**Definition 1.16** Sei $L/K$ endl. und separable K-Erw., sei $B := (\alpha_1, \ldots, \alpha_n) \subset L$ Basis von $L/K$.
$N :=$ normale Hülle von $L/K$ und $\mathrm{Hom}_K(L,N) = \{\sigma_1, \ldots, \sigma_n\}$.
Die *Diskriminante* der Basis $B$ ist definiert als:

$$d(\alpha_1, \ldots, \alpha_n) := \left[\det\left((\sigma_i(\alpha_j))_{i,j}\right)\right]^2$$

∎ **Bemerkung**

1. Sei $A := \left(Tr_{L/K}(\alpha_i \cdot \alpha_j)\right)_{i,j} \in K^{n \times n}$. Es gilt:
   $Tr_{L/K}(\alpha_i \cdot \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i) \cdot \sigma_k(\alpha_j)$.
   Sei $B := \left(\sigma_k(\alpha_i)\right)_{k,i}$, dann ist also $A = B^T \cdot B$
   $\rightsquigarrow K \ni \det(A) = \det(B^T \cdot B) = \det(B)^2 = d(\alpha_1, \ldots, \alpha_n)$
   Also gilt:
   $$\boxed{d(\alpha_1, \ldots, \alpha_n) = \det\left(Tr_{L/K}(\alpha_i \cdot \alpha_j)\right) \in K}$$
2. Basiswechsel: Sind $B$ und $B'$ zwei Basen und $T$ die Basiswechselmatrix von $B$ nach $B'$
   $$\Rightarrow d(B') = \det(T)^2 \cdot d(B)$$

---

**Beispiel** $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$, $D$ quadratfrei. Basis von $L/K$: $B = (1, \sqrt{D}) =: (\alpha_1, \alpha_2)$
$\sigma_1 = \mathrm{id}$, $\sigma_2(\sqrt{D}) = -\sqrt{D}$

$$\Rightarrow d(B) = \left[\det\begin{pmatrix} 1 & \sigma_1(\alpha_2) = \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}\right]^2$$
$$= (-2 \cdot \sqrt{D})^2 = 4D$$

Zum Vergleich:

$$A := \left(Tr_{L/K}(\alpha_i \cdot \alpha_j)\right)_{i,j} = \begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix}$$
$$\Rightarrow \det(A) = 4D$$

<u>weil:</u>

$$A = \begin{pmatrix} Tr_{L/K}(\alpha_1 \cdot \alpha_1) & Tr_{L/K}(\alpha_1 \cdot \alpha_2) \\ Tr_{L/K}(\alpha_2 \cdot \alpha_1) & Tr_{L/K}(\alpha_2 \cdot \alpha_2) \end{pmatrix} = \begin{pmatrix} Tr_{L/K}(1) & Tr_{L/K}(\sqrt{D}) \\ Tr_{L/K}(\sqrt{D}) & Tr_{L/K}(D) \end{pmatrix}$$

Erinnerung: $Tr_{L/K}(a + b \cdot \sqrt{D}) = 2a$ (für $a, b \in \mathbb{Q}$)

## 1.3 Ganzheitsbasis

**Definition 1.17** Sei $R$ ganzabgeschlossener Integritätsring, $K = Q(R)$ Quotientenkörper, $L/K$ endliche K-Erw. und $S = \overline{R} \subset L$. Dann heißen die Elemente $s_1, \dots, s_n \in S$ *Ganzheitsbasis* von $S$ über $R$, falls sich jedes $s \in S$ eindeutig als Linearkombination $s = r_1 \cdot s_1 + \cdots + r_n \cdot s_n$ mit $r_i \in R \; \forall \; i$ schreiben lässt.
(Kürzer: Ganzheitsbasis ist Basis von $S$ als $R$-Modul, d.h. Ganzheitsbasis von $S$ über $R$ existiert $\iff$ $S$ ist frei als $R$-Modul)

---

Sei $K/\mathbb{Q}$ ein Zahlkörper und $\mathcal{O}_K \subset K$ der Ring der ganzen Zahlen in $K$. Ist $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ eine Ganzheitsbasis von $\mathcal{O}_K$ (über $\mathbb{Z}$), so heißt die Diskriminante:

$$d_K := d(\mathcal{O}_K) := d(\omega_1, \dots, \omega_n)$$

auch *Diskriminante von K*.

Noch zu zeigen:

1. Der Ring der ganzen Zahlen $\mathcal{O}_K$ hat immer eine Ganzheitsbasis
2. Unabhängigkeit von $d_K$ von der Wahl der Ganzheitsbasis.

---

2. ist einfach:
Sind $B = (\omega_1, \dots, \omega_n)$ und $B' = (\omega_1', \dots, \omega_n')$ zwei Ganzheitsbasen von $\mathcal{O}_K \Rightarrow \exists$ Basiswechselmatrix $T \in \mathbb{Z}^{n \times n}$ mit $(\omega_1', \dots, \omega_n') \cdot T = (\omega_1, \dots, \omega_n)$, genauso $\exists S \in \mathbb{Z}^{n \times n}$ mit $(\omega_1, \dots, \omega_n) \cdot S = (\omega_1', \dots, \omega_n')$

$$\Rightarrow S \cdot T = T \cdot S = E_n \Rightarrow S, T \in \mathrm{GL}_n(\mathbb{Z}) \Rightarrow \mathbb{Z}^\times \ni \det(T) = \pm 1 \Rightarrow \det(T)^2 = 1$$

$\Rightarrow$ Wohldefiniertheit von $d_K$ folgt aus der Transformationsformel

1. erfordert Vorarbeit:

**Lemma 1.20** Eine Ganzheitsbasis von $S$ über $R$ ist auch eine Basis von $L/K$. Insbesondere hat sie Länge $n = [L : K]$.

*Beweis:* Ist $s_1, \dots, s_n \in S$ Ganzheitsbasis und $x \in L$

$$\Rightarrow \exists \; s \in S, r \in R \text{ mit } x = \frac{s}{r}$$
$$\Rightarrow s = r_1 \cdot s_1 + \cdots + r_n \cdot s_n \Rightarrow x = \underbrace{\frac{r_1}{r}}_{\in K} \cdot s_1 + \cdots + \underbrace{\frac{r_n}{r}}_{\in K} \cdot s_n$$

■

---

Zurück nochmal zur Diskriminante:

■ **Bemerkung 1.18** Ist $L = K(\alpha)$, so ist $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ Basis von $L/K$ mit $n = [L : K]$. Dann gilt:

$$d(1, \alpha, \dots, \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

mit $\alpha_i := \sigma_i(\alpha)$, $\mathrm{Hom}_K(L, N) = \{\sigma_1, \dots, \sigma_n\}$, $N/L$ normale Hülle

---

*Beweis:*
Vandermonde-Determinante:

$$\det\big((\alpha_i^j)_{i,j}\big) = \det\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{pmatrix} = \prod_{i<j}(\alpha_i - \alpha_j)$$

■

---

**Satz 1.19** Sei $L/K$ separabel und $\alpha_1, \dots, \alpha_n$ Basis von $L/K$. Dann ist
$d(\alpha_1, \dots, \alpha_n) \in K^\times$. (insb. $\neq 0$).
Weiterhin definiert

$$(x,y) := Tr_{L/K}(x \cdot y)$$

eine nicht-ausgeartete symmetrische $K$-Bilinearform auf $L$.
Zusatz: Falls $\alpha_1, \dots, \alpha_n \in S$ sind, so ist $d(\alpha_1, \dots, \alpha_n) \in R \setminus \{0\}$.

■ **Bemerkung** Bilinearform:

$x \mapsto (x,y)$ linear
$y \mapsto (x,y)$ linear

nicht ausgeartet:

Ist $x \in L$ mit $(x,y) = 0 \; \forall \, y \in L \Rightarrow x = 0$

$(x,y)$ Bilinearform, $\alpha_1, \dots, \alpha_n$ Basis von $L/K$
$\rightsquigarrow \big((\alpha_i \cdot \alpha_j)_{i,j}\big) \in K^{n \times n}$ Gram-Matrix.
LA: $(x,y)$ nicht ausgeartet $\iff \det\big((\alpha_i \alpha_j)_{i,j}\big) \neq 0$

---

*Beweis von Satz (1.19):*

- Satz vom primitiven Element $\Rightarrow L = K(\alpha)$, $\quad 1, \alpha, \dots, \alpha^{n-1}$ Basis von $L/K$ mit $n = [L:K]$
  $\overset{\text{Bemerkung (1.18)}}{\Rightarrow} d(1, \alpha, \dots, \alpha^{n-1}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 \neq 0 \quad$ mit $\alpha_i := \sigma_i(\alpha)$,
  denn: $\alpha_i \neq \alpha_j \iff \sigma_i(\alpha) \neq \sigma_j(\alpha)$ ✓
  $\Rightarrow$ Für bel. Basis $\alpha_1, \dots, \alpha_n$ ist $d(\alpha_1, \dots, \alpha_n) = \det(T)^2 \cdot d(1, \alpha, \dots, \alpha^{n-1}) \neq 0$ für geeignetes $T \in \mathrm{GL}_n(K)$.
  $d(1, \alpha, \dots, \alpha^{n-1}) \in K$ : siehe oben
- (symm.) Bilinearform:
  1. symmetrisch: Klar, da $Tr_{L/K}(x \cdot y) = Tr_{L/K}(y \cdot x)$, da $y \cdot x = x \cdot y$
  2. $L \to K$, $x \mapsto (x \cdot y)$ ist K-Linearform:
     $\forall \, x_1, x_2, y \in L, \; \lambda \in L$ :
     - $(x_1 + x_2, y) = Tr[(x_1 + x_2) \cdot y] = Tr(x_1 y + x_2 y) = Tr(x_1 y) + Tr(x_2 y) = (x_1, y) + (x_2, y)$
     - $(\lambda \cdot x, y) = Tr(\lambda \cdot x \cdot y) = \lambda \cdot Tr(x \cdot y) = \lambda (x,y)$

- Zusatz: Sind $\alpha_1,\dots,\alpha_n \in S$, so ist $Tr_{L/K}(\alpha_i\cdot\alpha_j)$:
  1. Ganz über $R$
  2. in $K$

  $\Big\}$ $\overset{\text{Proposition (1.15)}}{\Rightarrow}$ $Tr_{L/K}(\alpha_i\cdot\alpha_j)\in R \Rightarrow \det(Tr_{L/K}(\alpha_i\alpha_j))\in R\setminus\{0\}$.

∎

---

**Beispiel** Seien $L=\mathbb{Q}(\sqrt{D})$, $D$ quadratfrei, $K=\mathbb{Q}$, $B=(1,\sqrt{D})$ Basis und $\sigma_1=\mathrm{id}$, $\sigma_2(\sqrt{D})=-\sqrt{D}$.
Aus Bemerkung (1.18) folgt: (mit $\alpha=\sqrt{D}$, $\alpha_i=\sigma_i(\alpha)$)

$$d(B)=(\alpha_1-\alpha_2)^2=(\sqrt{D}-(-\sqrt{D}))^2=4D$$

Bilinearform aus Satz (1.19):

$$\begin{aligned} L\times L &\longrightarrow K\\ (x,y)&\longmapsto (x,y):=Tr_{L/\mathbb{Q}}(x\cdot y)\end{aligned}$$

Gram-Matrix bzgl. Basis $B$:

$$\begin{pmatrix}2 & 0\\ 0 & 2D\end{pmatrix}=:A$$

$\Rightarrow$ Ist $x=a+b\cdot\sqrt{D}$, $y=c+d\cdot\sqrt{D}$, so ist:

$$\begin{aligned}(x,y)=Tr_{L/K}(x\cdot y)&=(a,b)\cdot A\cdot\begin{pmatrix}c\\ d\end{pmatrix}\\ &=Tr_{L/K}\big((a+b\cdot\sqrt{D})(c+d\cdot\sqrt{D})\big)\\ &=Tr_{L/K}(ac+bdD+(bc+ad)\cdot\sqrt{D})\\ &=2(ac+bdD)\end{aligned}$$

Ebenso ist:

$$(a\quad b)\cdot\begin{pmatrix}2 & 0\\ 0 & 2D\end{pmatrix}\cdot\begin{pmatrix}c\\ d\end{pmatrix}=(2a\quad 2bD)\cdot\begin{pmatrix}c\\ d\end{pmatrix}=2ac+2bdD \quad ✓$$

Zusatz: $d(B)\in\mathbb{Z}\setminus\{0\}$ ✓

Eine Ganzheitsbasis muss es nicht immer geben, aber: Ist $R$ ein Hauptidealring, so existiert stets eine Ganzheitsbasis von $S$ über $R$.
Hier: Spezialfall $R=\mathbb{Z}$

**Satz 1.21** Sei $K$ ein algebraischer Zahlkörper, $\mathcal{O}_K\subset K$ der Ring der ganzen Zahlen in $K$. Dann ist $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul vom Rang $n=[K:\mathbb{Q}]$.
(Insb.: Es gibt eine Ganzheitsbasis , $\mathcal{O}_K\cong\mathbb{Z}^n$)

*Beweis:*

1. Beh.: Es gibt eine Basis $(b_1,\dots,b_n)$ von $K/\mathbb{Q}$ mit $b_i\in\mathcal{O}_K\ \forall\ i$
   Bew.: Ist $(\widetilde{b_1},\dots,\widetilde{b_n})$ beliebige Basis von $K/\mathbb{Q}$, dann gibt es ein $m\in\mathbb{Z}$ mit $m\cdot\widetilde{b_i}=:b_i\in\mathcal{O}_K$
2. Sei nun $(b_1,\dots,b_n)$ so eine Basis wie in 1.
   Sei $U:=\mathbb{Z}\cdot b_1\oplus\dots\oplus\mathbb{Z}\cdot b_n\subset\mathcal{O}_K$ der von $(b_1,\dots,b_n)$ erzeugte $\mathbb{Z}$-Untermodul von $\mathcal{O}_K$. Dann

gilt $U \cong \mathbb{Z}^n$ mit:

$$\begin{aligned} \mathbb{Z}^n &\longrightarrow U \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} &\longmapsto \sum_{i=1}^{n} x_i \cdot b_i \end{aligned}$$

Unter allen Basen, die 1. erfüllen, sei $B = (\omega_1, \ldots, \omega_n)$ eine Basis, so dass $|d(B)| \in \mathbb{N}$ minimal sei. $(d(B) \in \mathbb{Z} \setminus \{0\})$

Beh.: $\Gamma := \bigoplus_{i=1}^{n} \mathbb{Z} \cdot \omega_i = \mathcal{O}_K$

Bew.: $B$ ist Basis von $K/\mathbb{Q}$ nach Lemma (1.20).

$\rightsquigarrow$ Sei $x \in \mathcal{O}_K \setminus \Gamma \Rightarrow \exists\, \lambda_1, \ldots, \lambda_n \in \mathbb{Q}$ mit:

$$x = \sum_{i=1}^{n} \lambda_i \cdot \omega_i$$

Œ: $\lambda_1 \notin \mathbb{Z} \rightsquigarrow$ neue Basis: $B' := (\underbrace{x - \lfloor \lambda_1 \rfloor \cdot \omega_1}_{\in \mathcal{O}_K}, \omega_2, \ldots, \omega_n) \subset \mathcal{O}_K$

lin. unabh.:

$\sum_{i=2}^{n} x_i \omega_i + x_1(x - \lfloor \lambda_1 \rfloor \omega_1) = 0 \Rightarrow x = -\sum_{i=2}^{n} \frac{x_i}{x_1} \omega_i + \lfloor \lambda_1 \rfloor \cdot \omega_1 \Rightarrow \lambda_1 = \lfloor \lambda_1 \rfloor \lightning \lambda_1 \notin \mathbb{Z}.$

Basiswechsel:

$$T \cdot B = B' \Rightarrow T = \begin{pmatrix} \lambda_1 - \lfloor \lambda_1 \rfloor & \lambda_2 & \lambda_3 & \ldots & \lambda_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

$\Rightarrow \det(T)^2 = (\lambda_1 - \lfloor \lambda_1 \rfloor)^2 \in (0,1) \Rightarrow |d(B')| = |\det(T)^2| \cdot |d(B)| < |d(B)| \lightning$

■

---

■ **Bemerkung** Der Satz (1.21) bleibt korrekt, falls der „Grundring“ $R$ ein Hauptidealring ist.

---

**Korollar 1.22** Sei $(0) \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal. Dann ist auch $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Rang $n = [K : \mathbb{Q}]$.

*Beweis:*

1. $\mathfrak{a}$ ist $\mathbb{Z}$-Untermodul von $\mathcal{O}_K \cong \mathbb{Z}^n$. Ist $U \subset \mathbb{Z}^n$ Untermodul $\Rightarrow U$ ist frei (Übung)
   $\Rightarrow \mathfrak{a}$ ist frei
2. Sei $x \in \mathfrak{a}$ mit $x \neq 0 \Rightarrow$ $\underbrace{x \cdot \mathcal{O}_K}_{=(x)=\text{Hauptideal von } x \text{ erzeugt}} \subset \mathfrak{a}$
   $x \cdot \mathcal{O}_K \cong \mathbb{Z}^n$ als $\mathbb{Z}$-Modul
   $\Rightarrow \text{Rang}(\mathfrak{a}) \geq n$. Außerdem gilt, da $\mathfrak{a} \subset \mathcal{O}_K$ : $\text{Rang}(\mathfrak{a}) \leq n$
   $\Rightarrow \text{Rang}(\mathfrak{a}) = n$

■

---

**Korollar 1.23** Ist $(0) \neq \mathfrak{a} \subset \mathcal{O}_K$ Ideal, so ist $\mathcal{O}_K/\mathfrak{a}$ endlich.

*Beweis:* Übung ∎

---

**Definition 1.24** Ist $(0) \neq \mathfrak{a} \subset \mathcal{O}_K$ Ideal, so definieren wir die *Norm* von $\mathfrak{a}$ als:

$$N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}| = [\mathcal{O}_K : \mathfrak{a}]$$

**Korollar 1.25** Der Ring $\mathcal{O}_K$ ist noethersch.

∎ **Erinnerung** $R$ noethersch $\Rightarrow$ Jede aufsteigende Kette von Idealen $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots \subset R$ wird stationär, d.h. es existiert ein $n \in \mathbb{N}$ mit $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$.
Äquivalent: Jedes Ideal von $R$ ist endlich erzeugt.

---

*Beweis von Korollar (1.25):* $(0) \neq \mathfrak{a} \subset \mathcal{O}_K$ Ideal.

Korollar (1.22) $\Rightarrow$ $\mathfrak{a}$ ist endl. erzeugt als $\mathbb{Z}$- Modul

$\Rightarrow$ $\mathfrak{a}$ ist endl. erzeugt als $\mathcal{O}_K$-Modul,

d.h. $\mathfrak{a} = \langle a_1, \ldots, a_m \rangle = \{\sum_{i=1}^{m} \lambda_i \cdot a_i \mid \lambda_i \in \mathcal{O}_K\}$

$\Leftrightarrow$ $\mathfrak{a}$ endl. erzeugt als Ideal

$\Rightarrow$ mit obiger Äquivalenz die Behauptung

∎

---

**Satz 1.26** Seien $\Gamma \subset \Gamma' \subset K$ zwei additive Untergruppen von K, die als $\mathbb{Z}$-Moduln frei vom Rang $n = [K : \mathbb{Q}]$ seien. Dann gilt:

$$d(\Gamma) = [\Gamma' : \Gamma]^2 \cdot d(\Gamma'),$$

wobei $d(\Gamma)$ bzw. $d(\Gamma')$ die Diskriminante einer Basis von $\Gamma$ bzw. $\Gamma'$ als $\mathbb{Z}$-Modul sind.

*Beweis:*
$B := (b_1, \ldots, b_n)$ Basis von $\Gamma$, $B' := (b'_1, \ldots, b'_n)$ Basis von $\Gamma'$. Dann ist $d(B) = d(\Gamma)$, $d(B') = d(\Gamma')$.

$$\begin{array}{ccccc}
\sum_{i=1}^{n} x_i \cdot b_i & \in & \Gamma \hookrightarrow \Gamma' & \ni & \sum_{i=1}^{n} y_i \cdot b'_i \\
\uparrow & & \uparrow \cong \quad \uparrow \cong & & \uparrow \\
\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \in & \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^n & \ni & \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}
\end{array}$$

Dann erfüllt $A \in \mathbb{Z}^{n \times n}$:

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

mit $\sum_{i=1}^{n} y_i \cdot b_i' = \sum_{i=1}^{n} x_i \cdot b_i$. In den Übungen wurde gezeigt, dass es Matrizen $S,T \in \mathrm{GL}_n(\mathbb{Z})$ gibt, mit

$$SAT = \begin{pmatrix} m_1 & & \\ & \ddots & \\ & & m_n \end{pmatrix},$$

$m_i \in \mathbb{Z}$.

$$\Rightarrow \Gamma'/\Gamma \cong \mathbb{Z}^n/\mathrm{Bild}(A) \cong \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$$

$$\Rightarrow |\Gamma'/\Gamma| = [\Gamma' : \Gamma] = \prod_{i=1}^{n} |m_i|$$

Andererseits: Sind die Basen so gewählt, dass $A = \begin{pmatrix} m_1 & & \\ & \ddots & \\ & & m_n \end{pmatrix}$, so gilt für $d(\Gamma)$:

$$d(\Gamma) = \det \begin{pmatrix} m_1 b_1' & m_1\sigma_2(b_1') & \dots & m_1\sigma_n(b_1') \\ \vdots & \vdots & & \vdots \\ m_n b_n' & m_n\sigma_2(b_n') & \dots & m_n\sigma_n(b_n') \end{pmatrix}^2$$

mit: $\{\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K,N)$ mit $N/K$ normale Hülle.

$$\begin{aligned} b_1 &= m_1 b_1' \\ b_2 &= m_2 b_2' \\ &\vdots \\ b_n &= m_n b_n' \end{aligned}$$

$$\Rightarrow d(\Gamma) = (\prod_{i=1}^{n} m_i)^2 \cdot \det \begin{pmatrix} b_1' & \sigma_2(b_1') & \dots & \sigma_n(b_1') \\ \vdots & \vdots & & \vdots \\ b_n' & \sigma_2(b_n') & \dots & \sigma_n(b_n') \end{pmatrix}^2 = [\Gamma' : \Gamma]^2 \cdot d(\Gamma') \qquad \blacksquare$$

**Beispiel** $K = \mathbb{Q}(\sqrt{5})$, $R = \mathbb{Z}[\sqrt{5}] \subset K$ Unterring mit $R \subset \mathcal{O}_K$, da alle Basiselemente ganz sind, wobei die Basis $B := (b_1, b_2) := (1, \sqrt{5})$ ist. Dann gilt:

$$d(R) = \det\Big(Tr_{K/\mathbb{Q}}(b_i \cdot b_j)\Big) = \det \begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix} = 20 = 2^2 \cdot 5,$$

da $Tr_{K/\mathbb{Q}}\big((a+b\sqrt{5})\big) = (a+b\sqrt{5})(a-b\sqrt{5}) = 2a$ $\qquad a,b \in \mathbb{Q}$
$\rightsquigarrow$Frage: Gibt es Elemente in $\mathcal{O}_K \setminus R$?
Suche wegen $2^2$ nach Elementen mit Nenner 2:
$\rightsquigarrow$ Ja! z.B.: $\frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$, denn:

$$Tr\left(\frac{1+\sqrt{5}}{2}\right) = 1 \in \mathbb{Z}\checkmark \qquad N\left(\frac{1+\sqrt{5}}{2}\right) = \frac{1-5}{4} = -1 \in \mathbb{Z}\checkmark$$

$B' := (1, \frac{1+\sqrt{5}}{2})$ Basis von $R' := \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \subset \mathcal{O}_K$

$$d(B') = \det \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} = 5 \Rightarrow R' = \mathcal{O}_K,$$

denn es gibt kein Quadrat, dass 5 teilt und $d(\mathcal{O}_K) \in \mathbb{Z}$

**Korollar 1.27** Sei $K$ Zahlkörper, $\mathcal{O}_K \subset K$ Ring der ganzen Zahlen, $n = [K : \mathbb{Q}]$, $\Gamma \subset \mathcal{O}_K$ freier $\mathbb{Z}$-Untermodul vom Rang $n$ mit Basis $B := (b_1, \ldots, b_n)$. Falls $\Gamma \neq \mathcal{O}_K$ gilt, so gibt es eine Primzahl $p \in \mathbb{N}$ mit $p^2 \mid d(\Gamma)$ und es gibt ein $x \in \mathcal{O}_K \setminus \Gamma$ von der Form:

$$x = \frac{1}{p} \cdot \sum_{i=1}^{n} \lambda_i b_i \qquad 0 \leq \underset{\in\mathbb{Z}}{\lambda_i} < p$$

und $\lambda_{i_0} = 1$ für ein $i_0 \in \{1, \ldots, n\}$.
Dann ist $\Gamma' := \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_{i_0-1} \oplus \mathbb{Z}x \oplus \mathbb{Z}b_{i_0+1} \oplus \cdots \oplus \mathbb{Z}b_n$ wieder $\mathbb{Z}$-Untermodul von $\mathcal{O}_K$ mit:

$$d(\Gamma') = \frac{d(\Gamma)}{p^2} \qquad \text{insb.: } \Gamma \subsetneq \Gamma'$$

*Beweis:* Es gelte: $\Gamma \neq \mathcal{O}_K \Rightarrow [\mathcal{O}_K : \Gamma] \neq 1$, sei $p \in \mathbb{N}$ prim mit $p \mid [\mathcal{O}_K : \Gamma]$

$\overset{\text{Cauchy}}{\Rightarrow}$ Es gibt in $\mathcal{O}_K/\Gamma$ ein Element $y + \Gamma$ der Ordnung $p$
$\Rightarrow p \cdot y \in \Gamma$ aber $y \notin \Gamma$
$\Rightarrow p \cdot y = \sum_{i=1}^{n} \mu_i b_i$ mit $\mu_i \in \mathbb{Z}$ und $\exists\, i_0 \in \{1, \ldots, n\}$ mit $p \nmid \mu_{i_0}$, da $y \notin \Gamma$
$\Rightarrow \mathrm{ggT}(\mu_{i_0}, p) = 1 \Rightarrow \exists\, a, b \in \mathbb{Z} :\ 1 = a\mu_{i_0} + bp$
$\Rightarrow p \cdot a \cdot y = \sum_{i=1}^{n} a\mu_i b_i = \sum_{i \neq i_0} a\mu_i b_i + (1 - bp) b_{i_0}$
$\Rightarrow pay + bpb_{i_0} = \sum_{i \neq i_0} a\mu_i b_i + b_{i_0} \in \Gamma$
Seien $\lambda_i \in \{0, \ldots, p-1\}$ mit $a\mu_i = \lambda_i + p \cdot c_i$ mit $c_i \in \mathbb{Z}$, wobei $a\mu_i \equiv \lambda_i \pmod{p}$
$\Rightarrow \lambda_{i_0} \equiv (1 - bp) \equiv 1 \pmod{p}$
$\Rightarrow \lambda_{i_0} = 1$

Es ist: $x := \frac{1}{p} \cdot \sum_{i=1}^{n} \lambda_i b_i = \frac{1}{p} \cdot \sum_{i=1}^{n} (a\mu_i - pc_i) b_i = \underbrace{ay}_{\in \mathcal{O}_K} - \underbrace{\sum_{i=1}^{n} c_i b_i}_{\in \Gamma \subset \mathcal{O}_K}$.

Aber: $x \notin \Gamma$, denn $\lambda_{i_0} = 1$. Sei nun $\Gamma'$ wie im Satz definiert, mit Basis $(b_1, \ldots, b_{i_0-1}, x, b_{i_0+1}, \ldots, b_n)$.
Zu zeigen bleibt: $\Gamma \subset \Gamma'$. Dazu reicht es zu zeigen, dass $b_{i_0} \in \Gamma'$.

$$b_{i_0} = p \cdot x - \sum_{i \neq i_0} \lambda_i b_i \in \Gamma' \ \checkmark$$

Zur Diskriminante:

$$\varphi : \Gamma' \longrightarrow \mathbb{Z}/p\mathbb{Z}$$
$$\sum_{i \neq i_0} m_i \cdot b_i + m_{i_0} \cdot x \longmapsto m_{i_0} \pmod{p}$$

ist ein surjektiver Gruppenhomomorphismus. Es gilt:
$\mathrm{Kern}(\varphi) = \Gamma$, da die $x$-Koordinate genau dann durch $p$ teilbar ist.

$$\overset{\text{Hom.-Satz}}{\Rightarrow} \Gamma'/\Gamma \cong \mathbb{Z}/p\mathbb{Z} \Rightarrow [\Gamma' : \Gamma] = p$$
$$\overset{\text{Satz (1.26)}}{\Rightarrow} d(\Gamma') = \frac{d(\Gamma)}{[\Gamma' : \Gamma]^2} = \frac{d(\Gamma)}{p^2}$$

■

---

**Beispiel** $K = \mathbb{Q}(\sqrt{2}, i)$ ist Galois über $\mathbb{Q}$ mit Galoisgruppe:

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1 = \mathrm{id},\ \sigma_2 = \begin{cases} \sqrt{2} & \mapsto -\sqrt{2} \\ i & \mapsto i \end{cases},\ \sigma_3 = \begin{cases} \sqrt{2} & \mapsto \sqrt{2} \\ i & \mapsto -i \end{cases},\ \sigma_4 = \sigma_2 \circ \sigma_3\}$$

Starte mit Basis $B := (b_1, b_2, b_3, b_4) := (1, \sqrt{2}, i, i\sqrt{2}) \subset \mathcal{O}_K$, $\Gamma := \bigoplus_{i=1}^{4} \mathbb{Z} b_i$

Dann gilt:

$$d(\Gamma) = d(B) = \det(Tr_{K/\mathbb{Q}}(b_i \cdot b_j)) = \det \begin{pmatrix} Tr(1) & Tr(\sqrt{2}) & Tr(i) & Tr(i\cdot\sqrt{2}) \\ Tr(\sqrt{2}) & Tr(2) & Tr(i\cdot\sqrt{2}) & Tr(2i) \\ Tr(i) & Tr(i\cdot\sqrt{2}) & Tr(-1) & Tr(-\sqrt{2}) \\ Tr(i\cdot\sqrt{2}) & Tr(2i) & Tr(-\sqrt{2}) & Tr(-2) \end{pmatrix}$$

Es gilt:

$$Tr_{K/\mathbb{Q}}(a) = 4a, \text{ für } a \in \mathbb{Z}$$
$$Tr_{K/\mathbb{Q}}(i) = i + i - i - i = 0$$
$$Tr_{K/\mathbb{Q}}(\sqrt{2}) = \sqrt{2} - \sqrt{2} + \sqrt{2} - \sqrt{2} = 0$$
$$Tr_{K/\mathbb{Q}}(i\cdot\sqrt{2}) = 0$$

Daraus folgt für die obere Matrix:

$$d(\Gamma) = \det \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & -8 \end{pmatrix} = 2^{10} \qquad \Rightarrow p = 2 \text{ ist die einzige Möglichkeit}$$

$x = \frac{1}{2} \cdot \sum_{i=1}^{4} \lambda_i b_i$, mit $\lambda_i \in \{0, 1\}$ und ein $\lambda_i = 1$.
z.B. für $\lambda_2 = \lambda_4 = 1,\ \lambda_1 = \lambda_3 = 0$ ergibt sich: $x = \frac{\sqrt{2}}{2}(1+i) \in \mathcal{O}_K$, denn $x^4 = -1 \Rightarrow x^4 + 1 = 0$

$$\Rightarrow B' = (b_1, b_2, b_3, x) \text{ und } \Gamma' = \langle B' \rangle \text{ mit } d(\Gamma') = 2^8$$

Suche also nach $x = \frac{1}{2}\left(\lambda_1 + \lambda_2\sqrt{2} + \lambda_3 i + \lambda_4 \frac{\sqrt{2}}{2}(1+i)\right)$ mit $x \in \mathcal{O}_K \setminus \{0\}$ und $\lambda_i \in \{0, 1\}$.
Muss also für Tupel $(\lambda_1, \ldots, \lambda_4) \in \{0,1\}^4$, $(\lambda_1, \ldots, \lambda_4) \neq (0, \ldots, 0)$ überprüfen, ob $x \in \mathcal{O}_K$ ist.
Dafür gibt es 3 verschiedene Möglichkeiten:

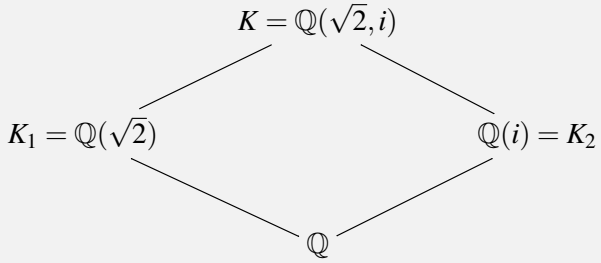
1. Notwendig & Hinreichend: Minimalpolynom ausrechnen.

$$\mathrm{Mipo}_x(t) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} (t - \sigma(x)) \in \mathbb{Z}[X]???$$

2. Notwendig:

   $$Tr_{K/\mathbb{Q}}(x), \mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}???$$

3. Notwendig: Relative Spuren/Normen. Betrachte hierzu folgendes Diagramm:




   z.B.: Ist $Tr_{K/K_1}(x) \in \mathcal{O}_{K_1}$???

Hier betrachten wir 3. mit $K/K_1 = K/\mathbb{Q}(\sqrt{2})$. $\mathcal{O}_{K_1} = \mathbb{Z}[\sqrt{2}]$ ist eine Übung. Die Galois-Gruppe ist: $\mathrm{Gal}(K/K_1) = \{\sigma_1, \sigma_3\}$.
Damit ergibt sich für die Spur:

$$\begin{aligned} Tr_{K/K_1}(x) &= \lambda_1 + \lambda_2\sqrt{2} + \frac{\lambda_4}{2}\sqrt{2} = \lambda_1 + \left(\lambda_2 + \frac{\lambda_4}{2}\right)\sqrt{2} \\ &\Rightarrow \lambda_4 = 0, \text{ da } \lambda_4 \in \{0,1\} \end{aligned}$$

Für die Norm ergibt sich:

$$\begin{aligned} N_{K/K_1}(x) &= \frac{1}{4}\left(\lambda_1 + \lambda_2\sqrt{2} + \lambda_3 \cdot i\right)\left(\lambda_1 + \lambda_2\sqrt{2} - \lambda_3 \cdot i\right) \\ &= \frac{1}{4}\left(\lambda_1^2 + 2\lambda_2^2 + \lambda_3^2 + 2\lambda_1\lambda_2\sqrt{2}\right) \\ &\Rightarrow \lambda_1 \cdot \lambda_2 = 0 \end{aligned}$$

$$\left.\begin{array}{l} \lambda_1 = 0 \Rightarrow \frac{2\lambda_2^2}{4} \in \mathbb{Z} \Rightarrow \lambda_2 = 0 \\ \lambda_2 = 0 \Rightarrow \frac{\lambda_1^2}{4} \in \mathbb{Z} \Rightarrow \lambda_1 = 0 \end{array}\right\} \Rightarrow \lambda_3 = 0 \Rightarrow x = 0$$

Damit ist man fertig, weil man gezeigt hat, dass es kein solches $x \in \mathcal{O}_K$ gibt.

■ **Bemerkung 1.28 — Algorithmus zur Bestimmung einer Ganzheitsbasis von $\mathcal{O}_K$.**

Algorithmus:

**Data:** ${}^K/_{\mathbb{Q}}$ alg. Zahlkörper vom Grad $n = [K : \mathbb{Q}]$, $B = (b_1, \ldots, b_n)$ Basis von ${}^K/_{\mathbb{Q}}$ mit $B \subset \mathcal{O}_K$, sowie $\Gamma = \bigoplus_{i=1}^{n} \mathbb{Z} \cdot b_i$
**Result:** Ganzheitsbasis von $\mathcal{O}_K$
**for** $\star$ *Alle Primzahlen* $p \in \mathbb{N}$ *mit* $p^2 \mid d(\Gamma)$ **do**
  **for** *alle Tupel* $(\lambda_1, \ldots, \lambda_n) \in \{0, \ldots, p-1\}^n$ *mit* $\lambda_{i_0} = 1$ *für ein* $i_0$ **do**
    **if** $x = \frac{1}{p} \cdot \sum_{i=1}^{n} \lambda_i b_i \in \mathcal{O}_K$ **then**
      neue Basis: Ersetze $b_{i_0}$ durch $x$;
      $\Gamma := \bigoplus_{i=1}^{n} \mathbb{Z} b_i$;
      Gehe zurück zu $\star$
    **else**
      Falls kein solches $x$ existiert gilt $\Gamma = \mathcal{O}_K$ und man ist fertig
    **end**
  **end**
**end**

# 2. Dedekindringe und Ideale

In diesem Kapitel ist $K$ ein algebraischer Zahlkörper und $\mathcal{O}_K \subset K$ der Ring der ganzen Zahlen in $K$.

Wir haben gesehen: $\mathcal{O}_K$ ist im Allgemeinen nicht faktoriell

**Beispiel** K=$\mathbb{Q}(\sqrt{-5})$ ,$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5}$

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

Aber: jedes Element kann in irreduzible Elemente zerlegt werden (da $\mathcal{O}_K$ noethersch)
$\rightsquigarrow$ Ideale: *(Kummer: „ideale Zahlen“)*
Im Beispiel: Es gibt Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4 \subset \mathcal{O}_K$ mit:

$$\underbrace{(6)}_{=6\cdot\mathcal{O}_K \text{ das von 6 erzeugte Hauptideal}} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_4 \qquad \text{und} \qquad (2) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$$

$$(3) = \mathfrak{p}_3 \cdot \mathfrak{p}_4$$
$$(1+\sqrt{-5}) = \mathfrak{p}_1 \cdot \mathfrak{p}_3$$
$$(1-\sqrt{-5}) = \mathfrak{p}_2 \cdot \mathfrak{p}_4$$

Mehr Details dazu in der Übung.
Also: Die Mehrdeutigkeit der Zerlegung von 6 in $\mathcal{O}_K$ wird schlicht zu einer Umordnung der Primidealfaktoren in der Faktorisierung von dem Ideal $(6)$.
Allgemeiner gilt die Existenz und Eindeutigkeit der Primidealfaktorisierung in Dedekindringen.

**Definition 2.1** Ein *Dedekindring* ist ein Integritätsring $R$ mit folgenden Eigenschaften

1. $R$ ist noethersch
2. $R$ ist ganzabgeschlossen
3. Ist $\mathfrak{p} \neq (0)$ Primideal in $R$, so ist $\mathfrak{p}$ maximal

**Satz 2.2** Sei $K$ alg. Zahlkörper, $\mathcal{O}_K \subset K$ Ring der ganzen Zahlen in $K$. Dann gilt:
Der Ring $\mathcal{O}_K$ ist ein Dedekindring.

*Beweis:*

1. noethersch ✓ Korollar (1.25)
2. ganzabgeschlossen ✓ Korollar (1.7)
3. Jedes Primideal $\mathfrak{p} \neq (0)$ ist maximal:
   (maximal: ist $\mathfrak{p} \subseteq \mathfrak{a} \subseteq \mathcal{O}_K \Rightarrow \mathfrak{a} = \mathfrak{p}$ oder $\mathfrak{a} = \mathcal{O}_K$. Äquivalent: $\mathcal{O}_K/\mathfrak{p}$ ist Körper)
   Beh.: $\mathfrak{p} \cap \mathbb{Z} = (p) \neq (0)$ ist ein Primideal in $\mathbb{Z}$

   Beweis: $\mathfrak{p} \cap \mathbb{Z}$ Primideal von $\mathbb{Z}$ ist klar, da $\mathfrak{p}$ Primideal ist:

   prim: Für $a, b \in \mathbb{Z}$ : Ist $a \cdot b \in \mathfrak{p} \cap \mathbb{Z}$, $\mathfrak{p}$ prim $\Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}$
   $\Rightarrow a \in \mathfrak{p} \cap \mathbb{Z} \vee b \in \mathfrak{p} \cap \mathbb{Z}$

   $\mathfrak{p} \cap \mathbb{Z} \neq (0)$ : $\mathfrak{p} \neq (0) \Rightarrow \exists\, x \in \mathfrak{p},\ x \neq 0$
   $\overset{x \in \mathcal{O}_K}{\Rightarrow}\ \exists\, a_{n-1}, \ldots, a_0 \in \mathbb{Z}$ mit $a_0 \neq 0$ und
   $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$
   $\Rightarrow a_0 = -(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x) \in \mathfrak{p}$
   $\Rightarrow 0 \neq a_0 \in \mathfrak{p} \cap \mathbb{Z}$

   ---

   Sei nun $\overline{\mathcal{O}} := \mathcal{O}_K/\mathfrak{p}$ Wir wollen zeigen, dass $\overline{\mathcal{O}}$ Körper ist.
   - $\overline{\mathcal{O}}$ ist endlich (Korollar (1.23))
   - Sei $\overline{\mathcal{O}} = \{\overline{x_1}, \ldots, \overline{x_m}\}$ mit der kanonischen Projektion $\pi : \mathcal{O}_K \to \overline{\mathcal{O}}$ und seien
     $x_1, \ldots, x_m \in \mathcal{O}_K$ mit $\pi(x_i) = \overline{x_i}$
     Sind $f_i \in \mathbb{Z}[X]$ normiert mit $f_i(x_i) = 0$
     Betrachte $\varphi : \mathbb{Z} \hookrightarrow \mathcal{O}_K \xrightarrow{\pi} \overline{\mathcal{O}}$

     $$\mathrm{Kern}(\varphi) = \mathfrak{p} \cap \mathbb{Z} = (p), \qquad p \in \mathbb{Z} \text{ Primzahl}$$

     $\rightsquigarrow$ Erhalte injektive Abbildung

     $$\overline{\varphi} : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to \overline{\mathcal{O}}$$

     Siehe also $\mathbb{F}_p$ als $\mathbb{F}_p \subset \overline{\mathcal{O}}$ als Teilmenge an, indem man $\mathbb{F}_p$ mit $\overline{\varphi}(\mathbb{Z}/p\mathbb{Z})$ identifiziert.

     Definiere $\overline{f_i} := f_i^{\pi} \in \mathbb{F}_p[X]$ durch Reduktion der Koeffizienten modulo $\pi$ (bzw. mod $p$)
     d.h.: ist $f_i = \sum a_{ij}x^j \rightsquigarrow f_i^{\pi} = \sum \underbrace{\pi(a_{ij})}_{=\varphi(a_{ij})} x^j$
     $\Rightarrow \overline{f_i}(\overline{x_i}) = \pi(f_i(x_i)) = \pi(0) = 0 \ \Rightarrow \overline{x_i}$ ist algebraisch über $\mathbb{F}_p$

     $\Rightarrow \overline{\mathcal{O}} = \mathbb{F}_p[\overline{x_1}, \ldots, \overline{x_m}]$ =Bild vom Einsetzungshomomorphismus:

     $$\mathbb{F}_p[t_1, \ldots, t_m] \longrightarrow \overline{\mathcal{O}}$$
     $$f(t_1, \ldots, t_m) \longmapsto f(\overline{x_1}, \ldots, \overline{x_m})$$

     $$\Rightarrow \overline{\mathcal{O}} = \mathbb{F}_p[\overline{x_1}, \ldots, \overline{x_m}] = \left[\left[(\mathbb{F}_p[\overline{x_1}])[\overline{x_2}]\right] \ldots [\overline{x_m}]\right]$$
     $$\overset{\text{Algebra: } \rightsquigarrow \overline{x_i} \text{ algebraisch}}{=} \left(\ldots\left(\left(\mathbb{F}_p(\overline{x_1})\right)(\overline{x_2})\right)\ldots(\overline{x_m})\right) \leftarrow \text{Körper}$$

In Algebra hatten wir nämlich gezeigt: Für $K$ Körper, $L/K$ Körpererweiterung und $\alpha \in L$ algebraisch über $K$ folgt:

$$\Rightarrow K[\alpha] = K(\alpha) \subset L \text{ ist ein Körper}$$

■

■ **Bemerkung 2.3** Sei $R$ Ring, $\mathfrak{a}, \mathfrak{b} \subset R$ Ideale

- Schreibe $\mathfrak{a} \mid \mathfrak{b}$ („$\mathfrak{a}$ teilt $\mathfrak{b}$“), falls $\mathfrak{b} \subseteq \mathfrak{a}$
- Demnach folgt: $a \mid b \iff (b) \subseteq (a)$ für alle $a, b \in R$
- $\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\} \subset R$ Ideal
- $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$
- $\mathfrak{a} \cdot \mathfrak{b} := \{\sum_{i=1}^{m} a_i b_i \mid m \in \mathbb{N},\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\} \subset R$ Ideal
- $\mathfrak{a} \cap \mathfrak{b} \subset R$ Ideal
- $\mathrm{kgV}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$
- $\mathfrak{p} \subset R$ Primideal $\iff (\mathfrak{p} \mid \mathfrak{a} \cdot \mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \text{ oder } \mathfrak{p} \mid \mathfrak{b})$

*Beweis:* Zum Beispiel:
zu $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b})$:
Per Definition gilt: $\mathfrak{g}$ heißt $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b})$, falls gilt:
$\mathfrak{g} \mid \mathfrak{a}$ & $\mathfrak{g} \mid \mathfrak{b}$ und ist $\mathfrak{c} \subset R$ Ideal mit $\mathfrak{c} \mid \mathfrak{a}$ sowie $\mathfrak{c} \mid \mathfrak{b} \Rightarrow \mathfrak{c} \mid \mathfrak{g}$

Nachprüfen: $\mathfrak{a} + \mathfrak{b} \mid \mathfrak{a}$, denn $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$ und $\mathfrak{a} + \mathfrak{b} \mid \mathfrak{b}$ (genauso)
Ist $\mathfrak{c} \subset R$ Ideal mit $\mathfrak{c} \mid \mathfrak{a}$ und $\mathfrak{c} \mid \mathfrak{b}$, so folgt:
$\forall\, a \in \mathfrak{a}\ \forall\, b \in \mathfrak{b}:\ a + b \in \mathfrak{c} \Rightarrow \mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c} \Rightarrow \mathfrak{c} \mid \mathfrak{a} + \mathfrak{b}$

■

## 2.1 Primidealzerlegung

Im Folgenden: $\mathcal{O}$ ist Dedekindring, $K = \mathrm{Quot}(R)$

**Satz 2.4** Sei $\mathfrak{a} \subset \mathcal{O}$ Ideal mit $(0) \neq \mathfrak{a} \neq (1) = \mathcal{O}$
Dann besitzt $\mathfrak{a}$ eine Zerlegung in Primideale:

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \qquad (\mathfrak{p}_1, \ldots, \mathfrak{p}_r \text{ Primideale})$$

Die Zerlegung ist (bis auf Reihenfolge) eindeutig.

**Lemma 2.5** Sei $\mathfrak{a} \neq (0)$ Ideal von $\mathcal{O}$. Dann existieren $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathcal{O}$ Primideale mit

$$\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \subset \mathfrak{a}$$

*Beweis:* (Übungen: Ex 3: E14)
Sei $M$ die Menge aller Ideale $\mathfrak{a} \neq (0)$ von $\mathcal{O}$ für die die Aussage falsch ist. Dann wollen wir zeigen, dass $M = \varnothing$. Angenommen $M \neq \varnothing$.

Sei dann $\mathfrak{a} \in M$ maximal bezüglich der Inklusion von Idealen. Das Maximum existiert, da $\mathscr{O}$ noethersch ist.
Klar: $\mathfrak{a}$ ist nicht prim

$$\Rightarrow \exists\, a,b \in \mathscr{O} \text{ mit } a \cdot b \in \mathfrak{a} \text{ aber } a \notin \mathfrak{a} \;\&\; b \notin \mathfrak{a}$$

Definiere $I := (a) + \mathfrak{a}$, $J := (b) + \mathfrak{a}$
Es gilt: $\mathfrak{a} \subsetneq I, J \Rightarrow I, J \notin M$

$$\Rightarrow \exists\, \mathfrak{p}_1, \ldots, \mathfrak{p}_r, \qquad \mathfrak{q}_1, \ldots, \mathfrak{q}_s \subset \mathscr{O} \text{ Primideale mit:}$$
$$\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \subset I \qquad \mathfrak{q}_1 \cdot \cdots \cdot \mathfrak{q}_s \subset J$$
$$\Rightarrow \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \cdot \mathfrak{q}_1 \cdot \cdots \cdot \mathfrak{q}_s \subset I \cdot J$$

Behauptung: $I \cdot J \subset \mathfrak{a}$ ($\Rightarrow \lightning\, \mathfrak{a} \in M$)
Beweis: Sei $x \in I \cdot J \rightsquigarrow x = \sum x_i y_i$ mit $x_i \in I,\ y_i \in J$

$$x_i = \underbrace{\alpha}_{\in \mathfrak{a}} + \underbrace{m_i}_{\in \mathscr{O}} \cdot a \qquad y_i = \underbrace{\beta}_{\in \mathfrak{a}} + \underbrace{n_i}_{\in \mathscr{O}} \cdot b$$

$$\Rightarrow x_i y_i = \underbrace{\alpha \cdot \beta}_{\in \mathfrak{a}} + \underbrace{\alpha n_i b}_{\in \mathfrak{a}} + \underbrace{\beta m_i a}_{\in \mathfrak{a}} + \underbrace{m_i n_i a b}_{\in \mathfrak{a}} \in \mathfrak{a} \Rightarrow x \in \mathfrak{a}$$ ∎

**Lemma 2.6** Sei $\mathfrak{p} \subset \mathscr{O}$ Primideal, $\mathfrak{p} \neq (0)$
Definiere $\mathfrak{p}^{-1} := \{x \in K \mid x \cdot \mathfrak{p} \subset \mathscr{O}\}$. Dann gilt für alle Ideale $(0) \neq \mathfrak{a} \subset \mathscr{O}$:

$$\mathfrak{a} \subsetneq \mathfrak{a} \cdot \mathfrak{p}^{-1} := \{\sum_{i=1}^{m} a_i x_i \mid m \in \mathbb{N}, a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\}$$

Insbesondere gilt:

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathscr{O}$$

*Beweis:* Sei $\mathfrak{p} \neq (0)$ Primideal. Sei $a \in \mathfrak{p},\ a \neq 0$. Dann gilt: $(a) \subset \mathfrak{p}$.
Nach Lemma (2.5) gibt es $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathscr{O}$ Primideale mit $\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$ und $r \in \mathbb{N}$ minimal.

1. Behauptung: Es gibt ein $i \in \{1, \ldots, r\}$ mit $\mathfrak{p}_i = \mathfrak{p}$
   Beweis: Es reicht zu zeigen, dass es ein $i$ gibt mit $\mathfrak{p}_i \subset \mathfrak{p}$, da $\mathfrak{p}_i$ prim $\overset{\mathscr{O} \text{ Dedekind}}{\Rightarrow}$ $\mathfrak{p}_i$ maximal.
   Angenommen $\mathfrak{p}_i \not\subset \mathfrak{p}\ \forall i \Rightarrow \forall i\ \exists\, a_i \in \mathfrak{p}_i$ mit $a_i \notin \mathfrak{p}$
   $$\Rightarrow a_1 \cdot \cdots \cdot a_r \in \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \subset (a) \subset \mathfrak{p} \Rightarrow \lightning\, \mathfrak{p} \text{ prim}$$
2. Œ: $\mathfrak{p} = \mathfrak{p}_1 \quad \Rightarrow \mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_r \not\subset (a)$, da $r$ minimal war
   $$\exists b \in \mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_r \text{ mit } b \notin (a)$$
   $\Rightarrow a^{-1} \cdot b \notin \mathscr{O}$. Wäre nämlich $\underbrace{a^{-1} \cdot b}_{=:c} \in \mathscr{O}$, so wäre $b = \underbrace{a \cdot c}_{\in (a) \lightning b \notin (a)} \in \mathscr{O}$
   Außerdem gilt: $b \cdot \mathfrak{p} \in \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \subset (a) \Rightarrow a^{-1} b \mathfrak{p} \subset \mathscr{O}$
   $$\Rightarrow a^{-1} \cdot b \in \mathfrak{p}^{-1}$$
   $\Rightarrow \mathfrak{p}^{-1} \neq 0$ (Klar: $\mathscr{O} \subset \mathfrak{p}^{-1}$)
   Dies ist die Aussage des Lemmas für $\mathfrak{a} = \mathfrak{p}$
   $$\mathfrak{p} \underset{\mathfrak{p}^{-1} \neq \mathscr{O}}{\subsetneq} \mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathscr{O} \qquad \text{weil } \mathfrak{p} \text{ maximal}$$

3. Sei $\mathfrak{a} \neq (0)$ Ideal von $\mathscr{O}$. $\mathfrak{a} = (\alpha_1, \ldots, \alpha_n)$ mit $\alpha_i$ Erzeugern.

   $\mathfrak{a} \subset \mathfrak{a} \cdot \mathfrak{p}^{-1}$, denn $1 \in \mathfrak{p}^{-1}$

   Angenommen es gelte $\mathfrak{a} = \mathfrak{a} \cdot \mathfrak{p}^{-1} \Rightarrow \forall x \in \mathfrak{p}^{-1}$ gilt: $x \cdot \alpha_i \in \mathfrak{a}$

   $$x \cdot \alpha_i = \sum_{j=1}^{m} \underbrace{a_{ij}}_{\in \mathscr{O}} \cdot \alpha_j$$

   Sei $A := \Big( (\delta_{ij} \cdot x - a_{ij})_{ij} \Big) \in \mathscr{O}^{m \times m}$

   $$\Rightarrow A \cdot \underbrace{\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}}_{\in \mathscr{O}^n \neq 0} = 0 \qquad \Rightarrow \det(A) = 0 \qquad (\mathscr{O} \text{ Integritätsring})$$

   $\Rightarrow f(t) := \det(t \cdot \delta_{ij} - a_{ij}) \in \mathscr{O}[t]$ ist normiert mit $f(x) = 0$

   $\Rightarrow x$ ganz über $\mathscr{O} \overset{\text{ganzabg.}}{\Rightarrow} x \in \mathscr{O} \Rightarrow \mathfrak{p}^{-1} = \mathscr{O}$ ↯2.

■

---

*Beweis von Satz (2.4):* Existenz: Sei $S$ Menge aller Ideale $\neq (0), (1)$ von $\mathscr{O}$, die keine solche Primfaktorzerlegung besitzen. Wir wollen zeigen, dass $S = \varnothing$. Angenommen $S \neq \varnothing$.
Sei $\mathfrak{a} \in S$ maximal bezüglich „$\subset$“. Es existiert (da $\mathscr{O}$ noethersch) ein maximales Ideal $\mathfrak{p}$ in $\mathscr{O}$ mit $\mathfrak{a} \subset \mathfrak{p} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$.
$\mathfrak{p}$ maximal $\Rightarrow \mathfrak{p}$ prim $\Rightarrow \mathfrak{p} \notin S \Rightarrow \mathfrak{a} \neq \mathfrak{p}$

$$\Rightarrow \mathfrak{a} \underset{\text{Lemma (2.6)}}{\subsetneq} \mathfrak{a} \cdot \mathfrak{p}^{-1} \underset{\mathfrak{a} \subset \mathfrak{p}}{\subset} \mathfrak{p} \cdot \mathfrak{p}^{-1} \underset{\text{Lemma (2.6)}}{=} \mathscr{O}$$

Da $\mathfrak{a} \in S$ maximal $\Rightarrow \mathfrak{a} \cdot \mathfrak{p}^{-1}$ hat eine Primfaktorzerlegung.
Sei $\mathfrak{a} \cdot \mathfrak{p}^{-1} = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \quad \Rightarrow \mathfrak{a} = \mathfrak{a} \cdot \underbrace{\mathfrak{p}^{-1} \cdot \mathfrak{p}}_{=\mathscr{O}} = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \cdot \mathfrak{p} \quad$ ↯ $\mathfrak{a} \in S$
$\Rightarrow S = \varnothing$
Eindeutigkeit: Erinnerung: Ist $\mathfrak{p} \subset \mathscr{O}$ Primideal und $\mathfrak{a}, \mathfrak{b} \subset \mathscr{O}$ Ideale, so gilt:

$$\mathfrak{p} \mid \mathfrak{a} \cdot \mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \vee \mathfrak{p} \mid \mathfrak{b}$$

Seien also $\mathfrak{a} = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r = \mathfrak{p}'_1 \cdot \cdots \cdot \mathfrak{p}'_s$ zwei Primfaktorzerlegungen von $\mathfrak{a}$.
Œ $r \geq s$. Da $\mathfrak{p}_1 \mid \mathfrak{a} \Rightarrow \mathfrak{p}_1 \mid \mathfrak{p}'_i$ für ein $i \in \{1, \ldots, s\}$
Œ $\mathfrak{p}_1 \mid \mathfrak{p}'_1 \underset{\text{Primideale sind maximal in } \mathscr{O}}{\Rightarrow} \mathfrak{p}_1 = \mathfrak{p}'_1$
$\Rightarrow \mathfrak{p}_1^{-1} \cdot \mathfrak{a} = \underbrace{\mathfrak{p}_1^{-1} \cdot \mathfrak{p}_1}_{=\mathscr{O}} \cdot \cdots \cdot \mathfrak{p}_r = \underbrace{(p'_1)^{-1} \cdot \mathfrak{p}'_1}_{=\mathscr{O}} \cdot \cdots \cdot \mathfrak{p}'_s$

$\overset{\text{induktiv}}{\underset{\text{ggf. umsortieren}}{\Rightarrow}} \mathfrak{p}_{s+1} \cdot \cdots \cdot \mathfrak{p}_r = \mathscr{O} \Rightarrow s = r$ und $\mathfrak{p}_i = \mathfrak{p}'_i \; \forall i \leq s$ ■

---

■ **Bemerkung** $\mathfrak{a} \cdot \mathfrak{p}^{-1}$ ist tatsächlich ein Ideal

---

*Beweis:*

- abg. unter „+“: Es reicht zu zeigen, dass $\mathfrak{p}^{-1}$ abgeschlossen ist unter „+“:
  Seien $x, y \in \mathfrak{p}^{-1} \Rightarrow (x+y)\mathfrak{p}^{-1} = x\mathfrak{p}^{-1} + y\mathfrak{p}^{-1} \subset \mathscr{O}$ ✓

- $\forall \alpha \in \mathcal{O}\ \forall x \in \mathfrak{p}^{-1}: \quad \alpha \cdot x \in \mathfrak{p}^{-1}$ ✓

■

---

■ **Bemerkung** Fasse mehrfach auftretende Faktoren in der Primfaktorzerlegung zusammen: Jedes $\mathfrak{a} \neq (0)$ lässt sich (bis auf Reihenfolge) eindeutig schreiben als:

$$\mathfrak{a} = \prod_{\substack{p \subset \mathcal{O} \\ \text{prim}}} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}, \qquad \nu_\mathfrak{p}(\mathfrak{a}) \in \mathbb{N}_0 \text{ mit } \nu_\mathfrak{p}(\mathfrak{a}) = 0 \text{ für fast alle } \mathfrak{p}$$

---

■ **Bemerkung**
Jeder Hauptidealring ist Dedekindring.
Jeder Hauptidealring ist faktoriell.

---

**Korollar 2.7** Sei $\mathcal{O}$ faktorieller Dedekindring. Dann ist $\mathcal{O}$ ein Hauptidealring.

*Beweis:* Übung. Idee: Benutze Primidealzerlegung und zeige, dass jedes Primideal ein Hauptideal ist. ■

---

**Korollar 2.8** Sei $\mathfrak{a} \subset \mathcal{O}$ Ideal, dann existieren $a, b \in \mathcal{O}$ mit $\mathfrak{a} = (a, b)$

*Beweis:* Übung: Idee: Benutze die Primfaktorzerlegung von $\mathfrak{a}$ und für $0 \neq a \in \mathfrak{a}$ gilt $\mathfrak{a} \mid (a)$ + chin. Restsatz + $b$ geschickt wählen. ■

---

## 2.2 Die Idealklassengruppe

Auf der Menge der Ideale ist die Multiplikation eine assoziative und kommutative Verknüpfung. Neutrales Element: $\mathfrak{a} \cdot \mathcal{O} = \mathcal{O} \cdot \mathfrak{a} = \mathfrak{a}$ für alle Ideale $\mathfrak{a} \subset \mathcal{O}$. Inverse Elemente? Schon gesehen: $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}$ für $\mathfrak{p} \subset \mathcal{O}$ prim mit $\mathfrak{p}^{-1} = \{x \in K \mid x \cdot \mathfrak{p} \subset \mathcal{O}\}$. Allgemeiner:

**Definition 2.9** Ein *gebrochenes Ideal* von $\mathcal{O}$ ist ein endlich erzeugter $\mathcal{O}$-Untermodul $\mathfrak{a} \subset K$ mit $\mathfrak{a} \neq (0)$.
Klar: $(0) \neq \mathfrak{a} \subset \mathcal{O}$ Ideal $\Rightarrow$ $\mathfrak{a}$ ist gebrochenes Ideal.
Ist $K$ algebraischer Zahlkörper, $\mathcal{O} = \mathcal{O}_K$ Ring der ganzen Zahlen, so folgt:

$\mathfrak{a} \subset \mathcal{O}_K$ heißt dann auch *ganzes Ideal* von $K$.

**Satz 2.10** Ist $(0) \neq \mathfrak{a} \subset K$ ein $\mathcal{O}$-Untermodul von $K$. Dann sind die folgenden Aussagen äquivalent:

1. $\mathfrak{a}$ ist gebrochenes Ideal
2. $\exists\, x \in \mathcal{O} \setminus \{0\}$ mit $x \cdot \mathfrak{a} \subset \mathcal{O}$ $\qquad (x \cdot \mathfrak{a} \subset \mathcal{O}$ Ideal$)$

*Beweis:* „1.⇒2.“
Sei $\mathfrak{a} \subset K$ gebrochenes Ideal mit $\alpha_1 = \frac{\beta_1}{\gamma_1}, \ldots, \alpha_n = \frac{\beta_n}{\gamma_n}$ Erzeugendensystem mit $\beta_i, \gamma_i \in \mathcal{O}$.
Für $x := \gamma_1 \cdot \cdots \cdot \gamma_n \in \mathcal{O}$ gilt: $x \cdot \alpha_i \in \mathcal{O}$
$\Rightarrow$ Ist $a \in \mathfrak{a}$: $a = \sum_{i=1}^{n} \lambda_i \alpha_i, \qquad \lambda_i \in \mathcal{O}$

$$\Rightarrow x \cdot a = \sum_{i=1}^{n} \lambda_i x \alpha_i \in \mathcal{O}$$

„2.⇒1.“
Ist $x \cdot \mathfrak{a} \subset \mathcal{O} \Rightarrow x \cdot \mathfrak{a}$ ist Ideal von $\mathcal{O}$.

$\mathcal{O}$ noethersch $\Rightarrow x \cdot \mathfrak{a}$ endlich erzeugt $\Rightarrow \mathfrak{a}$ endlich erzeugt

∎

---

Sind $\mathfrak{a}, \mathfrak{b} \subset K$ gebrochene Ideale, so ist

$$\mathfrak{a} \cdot \mathfrak{b} := \{\sum_{i=1}^{m} a_i b_i \mid m \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\} \qquad \text{ein gebrochenes Ideal.}$$

(Endl. erzeugt, da Produkte von Erzeugern von $\mathfrak{a}, \mathfrak{b}$ ein Erzeugendensystem sind.)

**Definition 2.11** Die Menge $I_{\mathcal{O}} := \{\mathfrak{a} \subset K \mid \mathfrak{a} \text{ gebr. Ideal von } \mathcal{O}\}$ heißt *Idealgruppe* von $\mathcal{O}$.
Falls $K$ algebraischer Zahlkörper, $\mathcal{O} = \mathcal{O}_K$, schreibe auch:

$$I_K := I_{\mathcal{O}_K}$$

**Satz 2.12** $I_{\mathcal{O}}$ wird mit

$$\begin{aligned} I_{\mathcal{O}} \times I_{\mathcal{O}} &\longrightarrow I_{\mathcal{O}} \\ (\mathfrak{a}, \mathfrak{b}) &\longmapsto \mathfrak{a} \cdot \mathfrak{b} \end{aligned}$$

zu einer abelschen Gruppe, mit neutralem Element $(1) = \mathcal{O}$ und inversen Elementen zu $\mathfrak{a} \in I_{\mathcal{O}}$:
$\mathfrak{a}^{-1} := \{x \in K \mid x \cdot \mathfrak{a} \subset \mathcal{O}\} \in I_{\mathcal{O}}$

*Beweis:* Es bleibt zu zeigen: $\mathfrak{a}^{-1} \in I_{\mathcal{O}}$ und $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathfrak{a}^{-1} \cdot \mathfrak{a} = \mathcal{O}\ \forall \mathfrak{a} \in I_{\mathcal{O}}$

1. Zunächst: $\mathfrak{a} \subset \mathcal{O}$ Ideal, $\mathfrak{a}^{-1}$ ist $\mathcal{O}$-Modul klar.
   Ist $0 \neq a \in \mathfrak{a} \Rightarrow a \cdot \mathfrak{a}^{-1} \subset \mathcal{O}$
   $\overset{\text{Satz (2.10)}}{\Rightarrow} \mathfrak{a}^{-1} \in I_{\mathcal{O}}$
   Ist nun $\mathfrak{a} = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r$ die Primfaktorzerlegung von $\mathfrak{a}$, definiere: $\mathfrak{b} := \mathfrak{p}_1^{-1} \cdot \dots \cdot \mathfrak{p}_r^{-1}$
   $\mathfrak{b} \in I_{\mathcal{O}}$ genauso wie für $\mathfrak{a}^{-1}$ und es gilt:

   $$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{p}_1 \mathfrak{p}_1^{-1} \cdot \dots \cdot \mathfrak{p}_r \mathfrak{p}_r^{-1} = \mathcal{O} \qquad \text{mit Lemma (2.6)}$$
   $$\Rightarrow \mathfrak{b} \subset \mathfrak{a}^{-1}, \quad \text{denn: ist } b \in \mathfrak{b}, \quad \text{so gilt:} b \cdot \mathfrak{a} \subset \mathcal{O}$$

   Zu zeigen bleibt, dass $\mathfrak{a}^{-1} \subset \mathfrak{b}$ ist:
   $\mathfrak{a}^{-1} = \mathfrak{a}^{-1} \cdot \mathfrak{a}\mathfrak{b} \Rightarrow$ Ist $a \in \mathfrak{a}^{-1}$ so folgt:
   $$\Rightarrow a = \sum_{i=1}^{m} \underbrace{\lambda_i b_i}_{\in \mathfrak{b}} \in \mathfrak{b} \text{ (mit } \lambda_i \in \mathfrak{a}\mathfrak{a}^{-1} \subset \mathcal{O})$$
   $$\Rightarrow \mathfrak{b} = \mathfrak{a}^{-1}$$

2. Sei nun $\mathfrak{a} \subset K$ gebrochenes Ideal.
   $\overset{\text{Satz (2.10)}}{\Rightarrow} \exists y \in \mathcal{O} \setminus \{0\}$ mit $y \cdot \mathfrak{a} \subset \mathcal{O}$ Ideal.
   $\overset{1.}{\Rightarrow} (y\mathfrak{a})^{-1} \in I_{\mathcal{O}}$ und $(y\mathfrak{a})^{-1}$ ist zu $(y\mathfrak{a})$ invers.

   $$\mathfrak{a} = \frac{1}{y}(y\mathfrak{a}) \qquad \text{und} \qquad \mathfrak{a}^{-1} = y \cdot \underbrace{(y\mathfrak{a})^{-1}}_{=\frac{1}{y}\mathfrak{a}^{-1}}$$

Behauptung: $(y\mathfrak{a})^{-1} = \frac{1}{y}\mathfrak{a}^{-1}$
„$\subseteq$“ Sei $x \in (y\mathfrak{a})^{-1}$
$\Rightarrow xy\mathfrak{a} \subset \mathcal{O} \Rightarrow xy \in \mathfrak{a}^{-1} \Rightarrow x \in y^{-1}\mathfrak{a}^{-1}$
„$\supseteq$“ Sei $x \in y^{-1}\mathfrak{a}^{-1}$
$\Rightarrow x = y^{-1} \cdot x'$, mit $x' \in \mathfrak{a}^{-1}$ (d.h. $x'\mathfrak{a} \subset \mathcal{O}$) $\Rightarrow x(y\mathfrak{a}) = (xy)\mathfrak{a} = x'\mathfrak{a} \subset \mathcal{O}$
$\Rightarrow x \in (y\mathfrak{a})^{-1}$

$\Rightarrow \mathfrak{a}^{-1} \in I_{\mathcal{O}}$ und $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \frac{1}{y}(y\mathfrak{a})y(y\mathfrak{a})^{-1} = \frac{1}{y}y(y\mathfrak{a})(y\mathfrak{a})^{-1} = \mathcal{O}$

■

---

**Korollar 2.13** Jedes gebrochene Ideal $\mathfrak{a} \subset \mathcal{O}$ kann eindeutig (bis auf Reihenfolge) geschrieben werden als

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

das Produkt über alle Primideale von $\mathcal{O}$, $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$, $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ für fast alle $\mathfrak{p}$.
Per Definition: $\mathfrak{p}^0 = \mathcal{O}$

**Definition 2.14** Ein *gebrochenes Hauptideal* von $\mathcal{O}$ ist ein gebrochenes Ideal der Form $\mathfrak{a} = x \cdot \mathcal{O}$ mit $x \in K^\times$.

$$P_{\mathcal{O}} := \{x\mathcal{O} \mid x \in K^\times\} \subset I_{\mathcal{O}} \text{ ist Untergruppe}$$

Die Faktorgruppe $Cl_{\mathcal{O}} := {}^{I_{\mathcal{O}}}/_{P_{\mathcal{O}}}$ heißt *Idealklassengruppe* von $\mathcal{O}$.
$h_{\mathcal{O}} := |Cl_{\mathcal{O}}|$ heißt *Klassenzahl* von $\mathcal{O}$.
Falls $K$ algebraischer Zahlenkörper ist und $\mathcal{O} = \mathcal{O}_K$ der Ring der ganzen Zahlen, schreibe auch:

$$Cl_K := Cl_{\mathcal{O}_K}$$
$$h_K := h_{\mathcal{O}_K}$$

**Satz 2.15** Sei $\mathcal{O}$ Dedekindring. Dann gilt:

$$h_{\mathcal{O}} = 1 \iff \mathcal{O} \text{ Hauptidealring} \iff \mathcal{O} \text{ faktoriell}$$

*Beweis:* 2. Äquivalenz wurde in Korollar (2.7) gezeigt.
1. Äquivalenz: „$\Leftarrow$“
Sei $\mathcal{O}$ Hauptidealring, $\mathfrak{a} \subset K$ gebrochenes Ideal.

$$\Rightarrow \exists x \in \mathcal{O} \setminus \{0\} \text{ mit } x\mathfrak{a} \subset \mathcal{O} \text{ Ideal } \overset{\mathcal{O} \text{ Hauptidealring}}{\Rightarrow} x\mathfrak{a} = (y) \text{ mit } y \in \mathcal{O}$$
$$\Rightarrow \mathfrak{a} = y \cdot x^{-1}\mathcal{O} \in P_{\mathcal{O}} \Rightarrow I_{\mathcal{O}} = P_{\mathcal{O}} \Rightarrow h_{\mathcal{O}} = 1$$

„$\Rightarrow$“ Sei $h_{\mathcal{O}} = 1 \Rightarrow I_{\mathcal{O}} = P_{\mathcal{O}}$. Ist also $\mathfrak{a} \subset \mathcal{O}$ Ideal, so ist $\mathfrak{a} \in P_{\mathcal{O}}$

$$\Rightarrow \exists x \in K^\times \text{ mit } \mathfrak{a} = x \cdot \mathcal{O}, \text{ aber da } \mathfrak{a} \subset \mathcal{O} \Rightarrow x \in \mathcal{O}$$

$\Rightarrow \mathfrak{a} = (x) \subset \mathcal{O} \Rightarrow \mathcal{O}$ ist Hauptidealring ■

---

Die Klassenzahl „misst“, wie weit $\mathcal{O}$ davon entfernt ist, ein Hauptidealring (/faktoriell) zu sein. Ist zum Beispiel $h_{\mathcal{O}} = m \in \mathbb{N}$, so folgt für $\mathfrak{a} \subset \mathcal{O}$ Ideal: $\mathfrak{a}^m$ ist ein Hauptideal.

**Beispiel**
1. $K = \mathbb{Q}(i),\ \mathcal{O}_K = \mathbb{Z}[i] \Rightarrow h_K = 1$, da $\mathcal{O}_K$ euklidisch und damit Hauptidealring ist.
2. $K = \mathbb{Q}(\sqrt{-5}),\ \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell. $\Rightarrow h_K \neq 1$. De facto ist $h_K = 2$.

**Satz 2.16 — Stark-Heegner.** $K_D = \mathbb{Q}(\sqrt{D})$, $D < 0$ quadratfrei ($K_D$ ist imaginär quadratischer Zahlkörper). Dann gilt:

$$h_{K_D} = 1 \iff D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$$

*In dieser Vorlesung wird dieser Satz nicht bewiesen.*
Vermutung: Es gibt unendlich viele reell-quadratische Zahlkörper ($D > 0$) mit Klassenzahl 1.

# 3. Die Endlichkeit der Klassenzahl

In diesem Kapitel ist $K$ ein algebraischer Zahlkörper und $\mathcal{O}_K \subset K$ der Ring der ganzen Zahlen in $K$.

Erinnerung: Wir hatten die Norm von einem Ideal $\mathfrak{a} \subset \mathcal{O}_K$ wie folgt definiert:

$$N(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}] = |{}^{\mathcal{O}_K}/_{\mathfrak{a}}| \in \mathbb{N}$$

**Satz 3.1** Sei $x \in \mathcal{O}_K \setminus \{0\}$, so gilt:

$$|\underbrace{N_{K/\mathbb{Q}}(x)}_{\substack{\text{Norm des}\\ \text{Elements}}}| = \underbrace{N((x))}_{\substack{\text{Norm des Hauptideals}\\ (x)=x\mathcal{O}}}$$

*Beweis:* Es gibt eine $\mathbb{Z}$-Basis $(\omega_1, \ldots, \omega_n)$ von $\mathcal{O}_K$, so dass es $m_1, \ldots, m_n \in \mathbb{Z}$ gibt mit $(m_1\omega_1, \ldots, m_n\omega_n)$ $\mathbb{Z}$-Basis von $(x) = x \cdot \mathcal{O}_K$ (mit Diagonalisierungsalgorithmus)

$$\Rightarrow N((x)) = [\mathcal{O}_K : (x)] = \Big|\prod_{i=1}^{n} m_i\Big|$$

Auf der anderen Seite: $x \cdot \omega_j = \sum_{i=1}^{n} \underbrace{(a_{ij}m_i)}_{\in \mathbb{Z}} \cdot \omega_i,$ $(\star)$

da $(m_1\omega_1, \ldots, m_n\omega_n)$ Basis von ${}^{K}/_{\mathbb{Q}}$ ist.

$$\begin{aligned}\big|N_{K/\mathbb{Q}}(x)\big| &\overset{\text{Def.}}{=} \big|\det\big((a_{ij}\cdot m_i)_{i,j}\big)\big| \\ &= \Big|\prod_{i=1}^{n} m_i \cdot \det\big((a_{ij})_{i,j}\big)\Big| \overset{(!)}{=} \Big|\prod_{i=1}^{n} m_i\Big|\end{aligned}$$

Das Ideal $(x) = x \cdot \mathcal{O}$ hat die $\mathbb{Z}$-Basen:

1. $\mathbb{Z}\cdot x\cdot\omega_1\oplus\cdots\oplus\mathbb{Z}\cdot x\cdot\omega_n\rightsquigarrow(x\omega_1,\ldots,x\omega_n)$
2. $(m_1\omega_1,\ldots,m_n\omega_n)$ Ist $\mathbb{Z}$-Basis von $(x)$

$\overset{(\star)}{\Rightarrow} a_{ij}\in\mathbb{Z}\ \forall i,j,$ da $(a_{ij})_{i,j}$ die Basiswechselmatrix ist

$\Rightarrow (a_{ij})_{i,j}\in \mathrm{GL}_n(\mathbb{Z})\Rightarrow \det(a_{ij})_{i,j}=\pm 1$

■

---

**Satz 3.2** Sei $(0)\neq\mathfrak{a}\subset\mathscr{O}_K$ Ideal mit Primfaktorzerlegung

$$\mathfrak{a}=\mathfrak{p}_1^{\nu_1}\cdot\cdots\cdot\mathfrak{p}_r^{\nu_r}$$

Dann gilt:

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

*Beweis:* gleich

**Satz 3.3** Sei $2s=$Anzahl der Einbettungen $\sigma:K\to\mathbb{C}$ mit $\sigma(K)\not\subset\mathbb{R}$ (*komplexe Einbettungen*). (Die Anzahl ist gerade, weil die komplex konjugierten Einbettungen auch wieder komplexe Einbettungen sind.)
Sei weiter $n=[K:\mathbb{Q}]$ und $d_K$ die Diskriminante von ${}^{K}/_{\mathbb{Q}}$.
Dann gilt:
Es gibt ein Repräsentantensystem von $Cl_K$ durch ganze Ideale $\mathfrak{a}\subset\mathscr{O}_K$ mit:

$$N(\mathfrak{a})\leq B_K:=\frac{n!}{n^n}\cdot\left(\frac{4}{\pi}\right)^s\cdot\sqrt{|d_K|}$$

**Satz 3.4** Die Klassenzahl $h_K=|Cl_K|$ eines algebraischen Zahlkörpers ist endlich

*Beweis:* Es reicht zu zeigen: Es gibt nur endlich viele Ideale $\mathfrak{a}\subset\mathscr{O}_K$ mit $N(\mathfrak{a})\leq B_K$ beziehungsweise $\leq$ irgendeiner festen Schranke. Nach Satz (3.2) reicht es zu zeigen, dass es nur endlich viele Primideale $\mathfrak{p}\subset\mathscr{O}_K$ gibt mit $N(\mathfrak{p})\leq B_K$.
Sei nun also $(0)\neq\mathfrak{p}\subset\mathscr{O}_K$ Primideal. Dann ist $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$ ein Primideal in $\mathbb{Z}$ mit einer Primzahl $p\in\mathbb{N}$.
$\Rightarrow {}^{\mathscr{O}_K}/_{\mathfrak{p}}$ ist ein $\mathbb{F}_p$-Vektorraum (als alg. Erweiterung von $\mathbb{F}_p$) mit Dimension $\leq n=[K:\mathbb{Q}]$

$$\Rightarrow N(\mathfrak{p})=|{}^{\mathscr{O}_K}/_{\mathfrak{p}}|=p^f\qquad\text{mit } f\leq n$$

Ist $p\in\mathbb{Z}$ Primzahl, so gibt es nur endlich viele Primideale $\mathfrak{p}\subset\mathscr{O}_K$ mit $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$. Denn:
$p\in\mathfrak{p}\Rightarrow p\mathscr{O}_K\subset\mathfrak{p}\Rightarrow\mathfrak{p}\mid p\mathscr{O}_K$ und die Primfaktorisierung von $p\mathscr{O}_K=\mathfrak{p}_1\cdot\cdots\cdot\mathfrak{p}_r$ ist endlich.
Es gibt nur endlich viele $p\in\mathbb{Z}$ mit $p\leq B_K$ und nur endlich viele $\mathfrak{p}\subset\mathscr{O}_K$ mit $\mathfrak{p}\mid p\mathscr{O}_K$. ■

---

■ **Bemerkung 3.5** $C_K:=\frac{n!}{n^n}\cdot\left(\frac{4}{\pi}\right)^s$ heißt *Minkowski-Konstante*.

$B_K:=C_K\cdot\sqrt{|d_K|}$ heißt *Minkowski-Schranke*.

Sei nun $n = [K : \mathbb{Q}] = r + 2s$ wobei $r$ die Anzahl der reellen Einbettungen und $2s$ die Anzahl der komplexen Einbettungen ist. Dann ergibt sich folgende Tabelle:

| $n$ | $r$ | $s$ | $C_K$ |
|---|---|---|---|
| 2 | 0 | 1 | $0,637\ldots$ |
| 2 | 2 | 0 | $0,500\ldots$ |
| 3 | 1 | 1 | $0,283\ldots$ |
| 3 | 3 | 0 | $0,222\ldots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| 100 | 100 | 0 | $0,93 \cdot 10^{-42}$ |

**Beispiel** 1. $K = \mathbb{Q}(i) \rightsquigarrow r = 0, s = 1, d_K = -4$
$\Rightarrow C_K \approx 0,637$
$d_K = -4 \Rightarrow B_K < 1,3 \Rightarrow$ Einzige Norm die kleiner $1,3$ ist:

$$N(\mathfrak{a}) = 1 \Rightarrow \mathfrak{a} = \mathcal{O}_K \Rightarrow h_{\mathbb{Q}(i)} = 1$$

2. $K = \mathbb{Q}(\sqrt{-5}) \rightsquigarrow r = 0, s = 1, d_K = -20 \Rightarrow B_K < 3$
$\Rightarrow$ Repräsentantensystem mit $N(\mathfrak{a}) \leq 2$

$(2) = \mathfrak{p}^2$ ist Primfaktorzerlegung von $(2)$ (Übung)
$\mathfrak{p} = (2, 1 + \sqrt{-5})$
$N(\mathfrak{p})^2 = N(\mathfrak{p}^2) = N((2)) = |N(2)| = 4$
$\Rightarrow N(\mathfrak{p}) = 2$ Norm prim$\Rightarrow \mathfrak{p}$ Primideal
$\Rightarrow Cl_K = \{[\mathcal{O}_K], [\mathfrak{p}]\} \Rightarrow h_K = 2$

*Beweis von Satz (3.2):* $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| = \left|\mathcal{O}_K/\prod_{k=1}^{r} \mathfrak{p}_k^{\nu_k}\right| \overset{\text{chin. Restsatz}}{=} \left|\prod_{k=1}^{r} \mathcal{O}_K/\mathfrak{p}_k^{\nu_k}\right| = \prod_{k=1}^{r} N(\mathfrak{p}_k^{\nu_k})$
Zu zeigen ist nur noch: $N(\mathfrak{p}^\nu) = N(\mathfrak{p})^\nu$ per Induktion:
$\underline{\nu = 1:}$ klar
$\underline{\nu \mapsto \nu + 1:}$

$$\mathcal{O}_K/\mathfrak{p}^\nu \cong {}^{(\mathcal{O}_K/\mathfrak{p}^{\nu+1})}\big/_{(\mathfrak{p}^\nu/\mathfrak{p}^{\nu+1})} \qquad \text{mit dem Isomorphiesatz aus Algebra}$$

$\Rightarrow N(\mathfrak{p}^{\nu+1}) = N(\mathfrak{p}^\nu) \cdot [\mathfrak{p}^\nu : \mathfrak{p}^{\nu+1}] \overset{\text{I.V.}}{=} N(\mathfrak{p})^\nu \cdot [\mathfrak{p}^\nu : \mathfrak{p}^{\nu+1}]$
Zu zeigen bleibt, dass $[\mathfrak{p}^\nu : \mathfrak{p}^{\nu+1}] = N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$
Sei $a \in \mathfrak{p}^\nu \setminus \mathfrak{p}^{\nu+1}$. Dann ist $\mathfrak{p}^\nu = (a) + \mathfrak{p}^{\nu+1} = \text{ggT}((a), \mathfrak{p}^{\nu+1})$
Definiere:

$$\begin{aligned} \varphi : \mathcal{O}_K &\longrightarrow \mathfrak{p}^\nu/\mathfrak{p}^{\nu+1} \\ x &\longmapsto x \cdot a + \mathfrak{p}^{\nu+1} \end{aligned}$$

$\varphi$ ist surjektiv, $\text{Kern}(\varphi) = \mathfrak{p}$
$\Rightarrow \varphi$ faktorisiert: $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^\nu/\mathfrak{p}^{\nu+1}$

$$|\mathcal{O}_K/\mathfrak{p}| = |\mathfrak{p}^\nu/\mathfrak{p}^{\nu+1}| = [\mathfrak{p}^\nu : \mathfrak{p}^{\nu+1}]$$

∎

# 4. Gitter

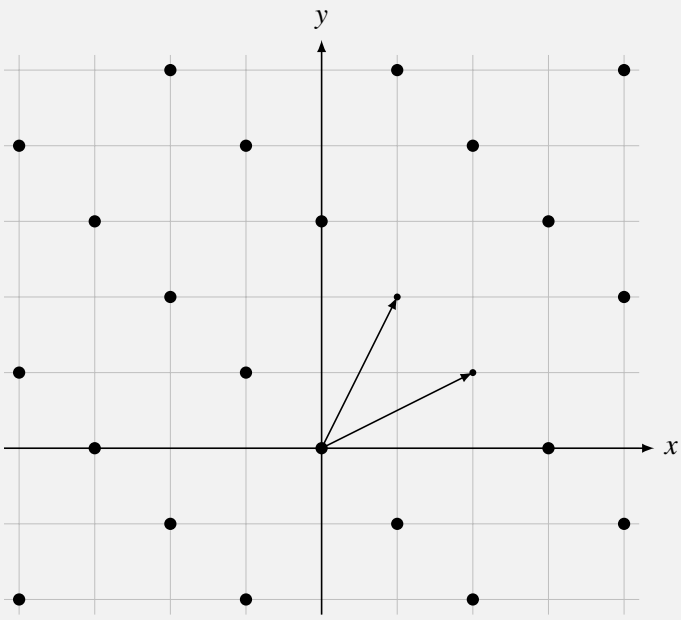
In diesem Kapitel ist $V$ ein endlich-dimensionaler $\mathbb{R}$-Vektorraum der Dimension $n$.

**Definition 4.1** Ein *Gitter* $L$ in $V$ ist eine Untergruppe $L \subset V$ von der Form:

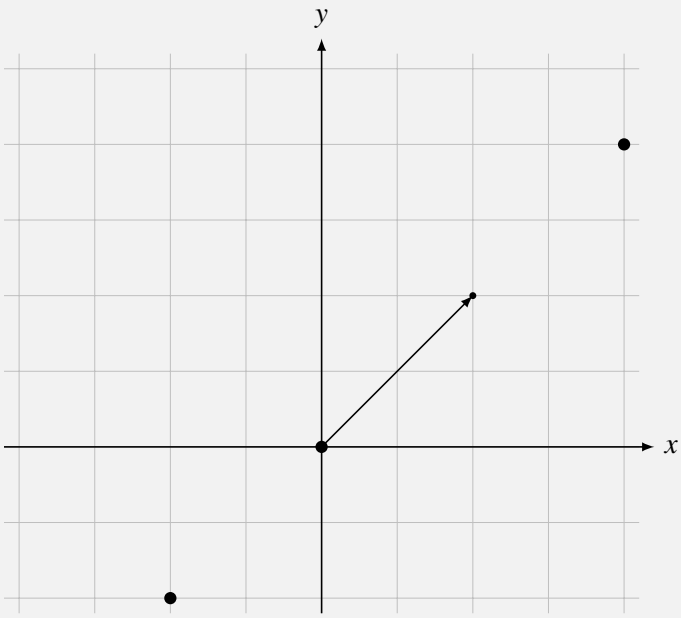
$$L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r \qquad \{v_1, \ldots, v_r\} \text{ reell linear unabhängig}$$

Falls $r = n$, so heißt $L$ *vollständiges Gitter*.

**Beispiel** Für $n = 2,\ r = 2$:



Für $n = 2,\ r = 1$:




■ **Bemerkung 4.2** Ein Gitter $L \subset V$ ist ein freier $\mathbb{Z}$-Modul vom Rang $r$. Die Umkehrung gilt nicht! z.B.: $\mathbb{Z} + \mathbb{Z} \cdot \sqrt{2} \subseteq \mathbb{R}$ hat als $\mathbb{Z}$-Modul Dimension 2, aber jedes Untergitter von $\mathbb{R}$ hat höchstens Dimension 1.

---

■ **Bemerkung 4.3** Seien $e_1, \ldots, e_n \in V$ Basis. Dann ist

$$\varphi : \mathbb{R}^n \longrightarrow V$$
$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \longmapsto \sum_{i=1}^{n} \lambda_i \cdot e_i$$

ein Isomorphismus. Da $V \cong \mathbb{R}^n$ erhält man eine Topologie auf $V$.

$$U \subset V \text{ offen} \iff \varphi^{-1}(U) \subset \mathbb{R}^n \text{ offen}$$

Diese hängt nicht von der Wahl der Basis ab.
(Jeder lineare Automorphismus $A \in \mathrm{GL}_n(\mathbb{R})$ ist ein Homöomorphismus , d.h. die Abbildung $x \mapsto Ax$ ist stetig und die Umkehrabbildung $x \mapsto A^{-1}x$ ist ebenfalls stetig.)

---

## 4.1 Charakterisierung von Gittern

**Definition** Eine Teilmenge $M \subset V$ ist diskret, falls jeder Punkt $x \in M$ eine offene Umgebung $U \subset V$ besitzt mit $U \cap M = \{x\}$ . (per Definition ist $M \subset V$ diskret, falls $M$ mit der induzierten Topologie diskret ist.)

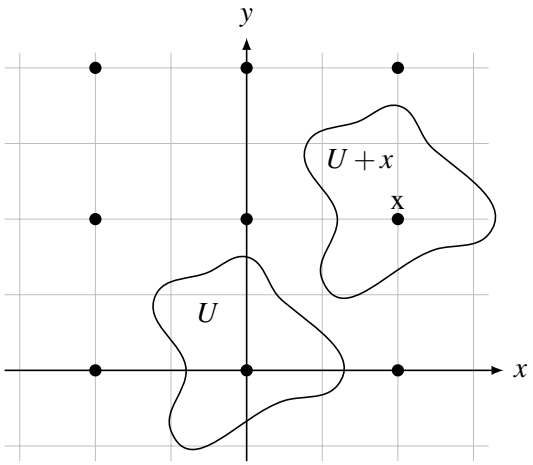
**Satz 4.4** Für eine Untergruppe $L \subset V$ sind äquivalent:

1. $L$ ist eine diskrete Untergruppe
2. Es gibt eine offene Menge $U \subset V$ mit $U \cap L = \{0\}$
3. $K \cap L$ ist endlich für alle kompakten Mengen $K \subset V$

4. $B \cap L$ ist endlich für jede beschränkte Menge $B \subset V$

*Beweis:* „1.⇒2.“ Klar.

„2.⇒1.“




$U \mapsto U + x =: \varphi_x$ (Translationsabbildung)

„1.⇒3.“
$L$ diskret ⇒ $L$ ist abgeschlossen ⇒ $K \cap L$ ist kompakt, diskret ⇒ $K \cap L$ endlich

„3.⇒4.“
Betrachte den Abschluss von $B \cap L$ ⇒ abgeschlossen und beschränkt ⇒ kompakt

„4.⇒2.“
Wähle eine beschränkte offene Menge um 0. Diese hat dann höchstens endlich viele Punkte. Die Menge ohne diese endlich vielen Punkte (außer der 0) ist immer noch offen. ∎

**Proposition 4.5** Eine Untergruppe $L \subset V$ ist genau dann ein Gitter, wenn $L$ diskret ist.

*Beweis:* „⇒“ Klar
„⇐“
Seien $\{e_1, \ldots, e_r\} \subseteq L$ maximal, reell linear unabhängig ($\Rightarrow L \subseteq \mathbb{R} \cdot e_1 + \cdots + \mathbb{R} \cdot e_r$)
Induktion nach $r$:
$\underline{r = 0}$ $L = 0$
$\underline{r = 1}$ $\Rightarrow L \subseteq \mathbb{R} \cdot e_1$
$L$ ist diskret $\rightsquigarrow$ Für jede Schranke $M > 0$ gilt:

$$\{a \cdot e_1 \mid |a| < M\} \cap L \text{ ist endlich.}$$

Deshalb gibt es ein $f \in L$ mit $f = a \cdot e_1$ mit $a > 0$ minimal. Wir wollen zeigen, dass $\mathbb{Z} \cdot f = L$:
Wenn dies nicht gilt, dann gibt es ein $\alpha \in L \setminus \mathbb{Z} \cdot f \Rightarrow \exists r \in \mathbb{R}$ mit:
$\alpha = r \cdot f = (m + b) \cdot f,\ m \in \mathbb{Z},\ 0 < b < 1$

$$L \ni \alpha - m \cdot f = b \cdot f = \underbrace{b \cdot a}_{<a} \cdot e_1 \qquad \lightning \text{ zu } a \text{ minimal}$$

$\underline{r>1}$ $L' := L \cap (\mathbb{R}e_1 + \cdots + \mathbb{R}e_{r-1})$, $L'$ ist diskrete Untergruppe in $\langle e_1, \ldots, e_{r-1} \rangle$.
Aus der Induktionsvoraussetzung folgt, dass $L'$ Gitter ist: Es gibt also $f_1, \ldots, f_{r-1}$ (reell linear unabhängig), sodass $L' = \mathbb{Z} \cdot f_1 + \cdots + \mathbb{Z} \cdot f_{r-1}$. Damit folgt für $\alpha \in L$ :
$\Rightarrow \alpha = a_1 \cdot f_1 + \cdots + a_{r-1} \cdot f_{r-1} + a \cdot e_r$. Definiere:

$$\begin{aligned} \varphi : L &\longrightarrow \mathbb{R} \\ \alpha &\longmapsto a \end{aligned} \qquad\qquad \varphi(L) =: L^\star$$

Es folgt: $\varphi\Big((a_1 - [a_1]) \cdot f_1 + \cdots + (a_{r-1} - [a_{r-1}]) \cdot f_{r-1} + a \cdot e_r\Big) = a$ (wobei $[a_i] \in \mathbb{Z}$).
Sei $|a| < M$. Es gilt: $L^\star \cap \{x \in \mathbb{R} \mid |x| < M\}$ ist endlich (da beschränkt und diskret).
$\overset{r=1}{\Rightarrow} L^\star$ ist Gitter von der Form: $\mathbb{Z} \cdot \varphi(f_r)$ mit $f_r \in L$.
Nun bleibt noch zu zeigen, dass $f_1, \ldots, f_{r-1}, f_r$ eine $\mathbb{Z}$-Basis von $L$ bilden:
Sei $\alpha \in L$. Dann gilt $\varphi(\alpha) = a \cdot \varphi(f_r)$ für ein $a \in \mathbb{Z}$.

$$\begin{aligned} &\Rightarrow \varphi(\alpha - a \cdot f_r) = 0 \\ &\Rightarrow \alpha - a \cdot f_r \in L' \\ \Rightarrow \alpha - a \cdot f_r &= a_1 f_1 + \cdots + a_{r-1} f_{r-1} \\ \Rightarrow \alpha &= a_1 f_1 + \cdots + a_{r-1} f_{r-1} + a f_r \\ \Rightarrow L &= \mathbb{Z} f_1 + \cdots + \mathbb{Z} f_r \end{aligned}$$

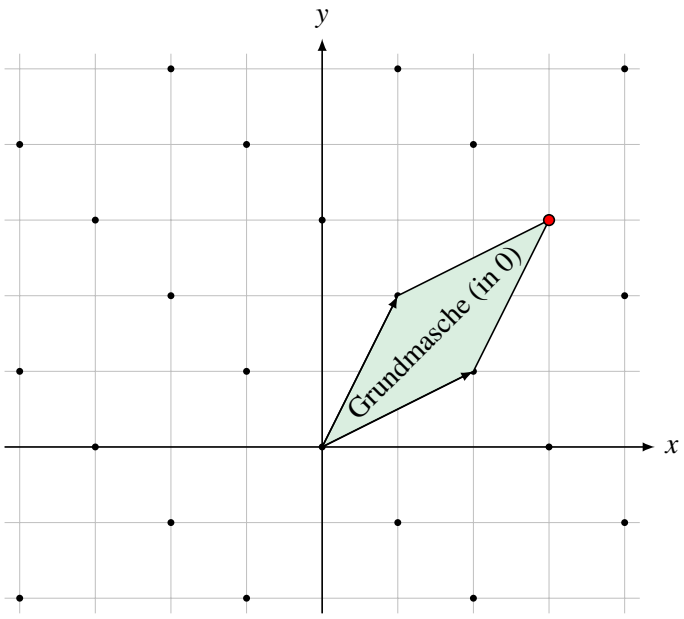
∎

## 4.2 Maßtheorie

**Definition 4.6** Sei $V$ reeller Vektorraum mit $\dim(V) = n$, $L \subset V$ ein vollständiges Gitter mit einer Basis $e_1, \ldots, e_n$ und $\lambda_0 \in L$.

$$D := \{\lambda_0 + \sum_{i=1}^{n} a_i \cdot e_i \mid 0 \leq a_i < 1\}$$

heißt *Grundmasche* von $L$ in $\lambda_0$.



■ **Bemerkung 4.7**

- Durch den Isomorphismus $\varphi : \mathbb{R}^n \to V$ erhalten wir (durch das Lebesgue-Maß auf dem $\mathbb{R}^n$ ein Maß $\mu$ auf $V$, das heißt ist $D \subset V$, so heißt $D$ *messbar* $\iff \varphi^{-1}(D) \subset \mathbb{R}^n$ messbar und es gilt:

  $$\mu(D) = \mu_{\text{Lebesgue}}(\varphi^{-1}(D))$$

- Ist $D$ Grundmasche von $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$, so gilt:

  $$\text{vol}(L) := \mu(D) = |\det(v_1, \ldots, v_n)|$$

  Dies ist unabhängig von der Wahl der Basis.

- Sind $L \subset M \subset \mathbb{R}^n$ zwei vollständige Gitter und $D_L$, $D_M$ Grundmaschen für $L$ beziehungsweise $M$, so gilt:

  $$\mu(D_L) = \mu(D_M) \cdot [M : L]$$

- Die obige Formel gilt auch (unabhängig von der Basiswahl von $V$) für zwei vollständige Gitter $L \subset M \subset V$

---

*Beweis:* Der erste und zweite Punkt wurden in Analysis bewiesen. Zum 3. Punkt: Es gibt eine Basis von $M$, $\{e_1, \ldots, e_n\}$ und eine weitere Basis $\{m_1 e_1, \ldots, m_n e_n\}$ von $L$.

$$\mu(D_M) = |\det(e_1, \ldots, e_n)| \quad \mu(D_L) = |\det(m_1 e_1, \ldots, m_n e_n)| = m_1 \cdot \cdots \cdot m_n \cdot \mu(D_M)$$

$$\left.\begin{aligned} M &= \bigoplus_{i=1}^{n} \mathbb{Z} \cdot e_i \\ L &= \bigoplus_{i=1}^{n} \mathbb{Z} \cdot m_i e_i \end{aligned}\right\} \Rightarrow {}^{M}\!/_{L} \cong \bigoplus_{i=0}^{n} {}^{\mathbb{Z}}\!/_{m_i \mathbb{Z}},$$

induziert durch kanonische Projektion und Korollar zum Homomorphiesatz.

$$[M : L] = m_1 \cdot \cdots \cdot m_n$$

■

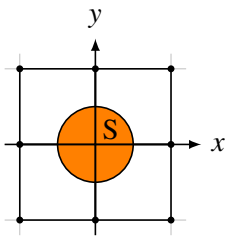
---

**Satz 4.8** Sei $D_0$ Grundmasche von (voll) $L \subset V$ im Punkt 0 und $S \subset \mathbb{R}^n$ messbar.
Falls $\mu(S) > \mu(D_0)$, so gilt:

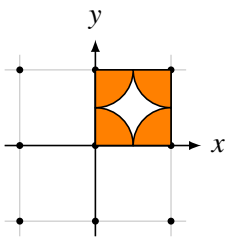
$$\exists\, \alpha, \beta \in S \text{ mit } \alpha \neq \beta \text{ und } \alpha - \beta \in L$$

*Beweis:* $S = \bigcup_{\lambda \in L} (S \cap \underbrace{(D_0 + \lambda)}_{=D_\lambda})$

$$\Rightarrow \mu(S) = \sum_{\lambda \in L} \mu(S \cap D_\lambda)$$




Idee: Verschiebe Alle Schnitte von $S$ mit den Grundmaschen in eine Grundmasche:




Verschiebe also die einzelnen Schnitte nach $D_0$. Dann muss es Überlappungen in $D_0$ geben, da sonst $\mu(S) \leq \mu(D_0)$ sein müsste.
$\Rightarrow \exists\, \alpha \in S \cap D_{\lambda_1}$ und $\exists\, \beta \in S \cap D_{\lambda_2}$, so dass

$$\alpha - \lambda_1 = \beta - \lambda_2$$

Das heißt, sie liegen nach der Verschiebung aufeinander. ∎

---

**Definition 4.9**

- $M \subset \mathbb{R}^n$ heißt *konvex*, falls für alle $x, y \in M$ auch gilt:

$$[x,y] := \{x \cdot (1-t) + y \cdot t \mid t \in [0,1]\} \subseteq M$$

- $M$ heißt *zentralsymmetrisch*, falls für alle $x \in M$ auch gilt: $-x \in M$.

**Satz 4.10 — Minkowski Gitterpunktsatz.** Sei $M \subset V \cong \mathbb{R}^n$ konvex, zentralsymmetrisch und kompakt. Sei weiter $L \subset V$ vollständiges Gitter mit Grundmasche $D$. Falls:

$$\mu(M) \geq 2^n \cdot \mathrm{vol}(L)$$

dann gilt:

$$\exists\, x \in M \cap L \text{ mit } x \neq 0$$

*Beweis:* $x, y \in M \Rightarrow \frac{1}{2} \cdot (x-y) \in M$. Wir setzen $S := \frac{1}{2} \cdot M$

$$\Rightarrow \mu(S) = \frac{1}{2^n} \cdot \mu(M) \overset{\mu(M) \geq 2^n \cdot \mathrm{vol}(L)}{\Rightarrow} \mu(S) \geq \mathrm{vol(L)}$$

Definiere $\widetilde{M} := (1+\varepsilon) \cdot M,\ \varepsilon > 0$, sowie $\widetilde{S} := \frac{1}{2} \cdot \widetilde{M}$. Dann folgt: $\mu(\widetilde{S}) > \mathrm{vol}(L)$.
$\overset{\text{Satz (4.8)}}{\Rightarrow} \exists\, \alpha, \beta \in \widetilde{S}$ mit $\alpha - \beta \in L \setminus \{0\}$

$$\Rightarrow \exists\, \alpha', \beta' \in \widetilde{M} \text{ sodass } \underbrace{\frac{1}{2}(\alpha' - \beta')}_{=:x} \in L$$

$$\Rightarrow \exists\, x \in L \setminus \{0\} \text{ mit } x \in \widetilde{M}$$

Es gibt nur endlich viele solche $x \in \widetilde{M}$, da $L$ diskret ist. Wenn kein $x \in L \setminus \{0\}$ existiert mit $x \in M$, so könnte man $\varepsilon$ klein genug wählen, so dass $\widetilde{M} \cap L = \{0\}$ ↯ ∎

---

Etwas Analysis: $V := \mathbb{R}^r \times \mathbb{C}^s$. Dann gilt $\dim_{\mathbb{R}}(V) = r + 2s =: n$.
kanonische Identifizierung: $V \cong \mathbb{R}^n$, indem $\mathbb{C}^s \cong \mathbb{R}^{2s}$ durch $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$

Wir definieren eine Norm $\|\cdot\|$ auf $V$:

$$\|x\| := \sum_{i=1}^{r} |x_i| + 2 \cdot \sum_{i=r+1}^{r+s} \underbrace{|z_i|}_{\text{komplexer Betrag}}$$

für $x = (x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s})^T \in V$

**Lemma 4.11** Sei $t \in \mathbb{R}$, $t > 0$ und $X(t) := \{x \in V \mid \|x\| \leq t\}$.
Es gilt:

$$\mu(X(t)) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{t^n}{n!}$$

*Beweis:* $X(t)$ ist symmetrisch bezüglich der $r$ reellen Achsen, d.h.:

$$\mu(X(t)) = 2^r \cdot \mu(Y(t)),$$

wobei $Y(t) = \{x \in V \mid \|x\| \leq t \text{ und } x_1, \ldots, x_r \geq 0\}$.
Für die komplexen $z_i$ nehmen wir Polarkoordinaten, d.h.:

$$z_i = x_i + i \cdot y_i = \frac{1}{2} \cdot \rho_i \cdot (\cos(\Theta_i) + i \cdot \sin(\Theta_i)$$

Determinante der Jacobimatrix des Koordinatenwechsels: Für jedes $z_i$ gibt es einen Faktor $\frac{\rho_i}{4}$. Damit folgt:

$$\mu(X(t)) = \int_{X(t)} 1 d\mu = 2^r \cdot 4^{-s} \cdot \int_{Z'} \rho_{r+1} \cdot \cdots \cdot \rho_{r+s}\, dx_1 \ldots dx_r\, d\rho_{r+1} \ldots d\rho_{r+s}\, d\Theta_{r+1} \ldots\, d\Theta_{r+s}$$

wobei $Z' := \{(X, \rho, \Theta) \in \mathbb{R}^{r+s+s} \mid x_i, \rho_i \geq 0,\ \sum x_i + \sum \rho_i \leq t,\ 0 \leq \Theta_i \leq 2\pi\}$

$$\Rightarrow \mu(X(t)) = 2^r \cdot 4^{-s} \cdot (2\pi)^s \cdot \int_{Z} \rho_{r+1} \cdot \cdots \cdot \rho_{r+s}\, dx_1 \ldots dx_r d\rho_{r+1} \ldots d\rho_{r+s}$$

wobei $Z = \{(X, \rho) \in \mathbb{R}^{r+s} \mid x_i, \rho_i \geq 0,\ \sum x_i + \sum \rho_i \leq t\}$.
Für den letzten Schritt des Beweises wird noch ein Lemma gebraucht:

**Lemma 4.12** Für $a_1, \ldots, a_m \in \mathbb{R}$ mit $a_i \geq 0$, sei $I(a_1, \ldots, a_m, t) := \int_{Z(t)} x_1^{a_1} \cdot \cdots \cdot x_m^{a_m}\, dx_1 \ldots dx_m$,
wobei $Z(t) := \{x \in \mathbb{R}^m \mid x_i \geq 0,\ \sum x_i \leq t\}$. Dann gilt:

$$I(a_1, \ldots, a_m, t) = t^{(\sum_{i=1}^m a_i + m)} \cdot \frac{\Gamma(a_1 + 1) \cdot \cdots \cdot \Gamma(a_m + 1)}{\Gamma(a_1 + \cdots + a_m + m + 1)}$$

wobei $\Gamma(x) := \int_0^\infty e^{-t} \cdot t^{x-1}\, dt$, mit den Eigenschaften: $\Gamma(x+1) = x \cdot \Gamma(x)$ und $\Gamma(n+1) = n!$

Setzt man dieses Lemma im Beweis von Lemma (4.11) ein, so folgt die Behauptung. ∎

**Lemma 4.13** Seien $a_1, \ldots, a_n \in \mathbb{R}_{\geq 0}$. Dann gilt:

$$\left(\prod_{i=1}^{n} a_i\right)^{\frac{1}{n}} \leq \frac{\sum_{i=1}^{n} a_i}{n} \qquad \text{oder:}$$

$$\prod_{i=1}^{n} a_i \leq \frac{\left(\sum_{i=1}^{n} a_i\right)^n}{n^n}$$

*Beweis:* Dies ist die *Jensen-Ungleichung* für den ln. ∎

# 5. Minkowski-Theorie (Teil 1)/Beweis von Satz (3.3)

In diesem Kapitel ist $K$ Zahlkörper vom Grad $n = [K : \mathbb{Q}]$.

**Definition** Ist $\sigma : K \to \mathbb{C}$ eine Einbettung, so heißt $\sigma$ *reell*, falls $\sigma(K) \subseteq \mathbb{R}$. Andernfalls heißt $\sigma$ *komplex*.

■ **Bemerkung**

- Mit $\sigma$ ist auch $\overline{\sigma} := \bar{\cdot} \circ \sigma$ eine Einbettung
- $\sigma$ reell $\Rightarrow \overline{\sigma} = \sigma$
- $\sigma$ komplex $\Rightarrow \overline{\sigma} \neq \sigma$
  $\rightsquigarrow$ Wir können die komplexen Einbettungen zu Paaren $(\sigma, \overline{\sigma})$ gruppieren
- $r$ ist Anzahl der reellen Einbettungen, $s$ die Anzahl der Paare der komplexen Einbettungen

  $$\rightsquigarrow r + 2s = n$$

- Wir erhalten eine Abbildung:

  $$\begin{aligned} \sigma : K &\longrightarrow V \\ x &\longmapsto (\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \ldots, \sigma_{r+s}(x)), \end{aligned}$$

  wobei bei den komplexen Einbettungen jeweils nur ein Vertreter pro Paar gewählt wurde.

---

**Beispiel** $K = \mathbb{Q}(\sqrt{D})$, $D$ quadratfrei.

1. $D > 0 \rightsquigarrow r = 2$

   $$\alpha \in K,\ \alpha = x + y \cdot \sqrt{D} \rightsquigarrow \sigma(\alpha) = (x + y\sqrt{D}, x - y\sqrt{D})$$

2. $D<0 \rightsquigarrow s=1$

$$\begin{aligned}\alpha &= x+y\cdot\sqrt{D}\\ &\rightsquigarrow \sigma_1(\alpha)=x+iy\sqrt{|D|},\ \sigma_2(\alpha)=\overline{\sigma_1(\alpha)}\\ &\quad \tau_1=\sigma_1(\alpha)\\ &\rightsquigarrow \sigma(\alpha)=\tau_1(\alpha)=\sigma_1(\alpha)\in\mathbb{C}\cong\mathbb{R}^2\end{aligned}$$

**Proposition 5.1** Sei $\mathfrak{a}\neq(0)$ ein ganzes Ideal. Dann ist $\sigma(\mathfrak{a})\subset\mathbb{R}^{r+2s}$ ein vollständiges Gitter. Die Grundmasche von $\sigma(\mathfrak{a})$ hat das Volumen:

$$\mu(\sigma(\mathfrak{a}))=2^{-s}\cdot N(\mathfrak{a})\cdot\sqrt{|d_K|}$$

---

*Beweis:* Wir wissen bereits: $\mathfrak{a}$ ist ein freier $\mathbb{Z}$-Modul vom Rang $n=r+2s$.
Wähle also eine $\mathbb{Z}$-Basis: $\alpha_1,\dots,\alpha_n\in\mathfrak{a}$.
Zeige: $\sigma(\alpha_1),\dots,\sigma(\alpha_n)$ sind $\mathbb{R}$-linear unabhängig.
Dazu: Sei $S:=\begin{pmatrix}\sigma(\alpha_1)\\ \vdots\\ \sigma(\alpha_n)\end{pmatrix}\in\mathbb{R}^{n\times n}$. Zeige, dass $\det(S)\neq 0$

$$S=\begin{pmatrix}\sigma_1(\alpha_1) & \dots & \sigma_r(\alpha_1) & \mathrm{Re}(\tau_1(\alpha_1)) & \mathrm{Im}(\tau_1(\alpha_1)) & \dots & \mathrm{Re}(\tau_s(\alpha_1)) & \mathrm{Im}(\tau_s(\alpha_1))\\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots\\ \sigma_1(\alpha_n) & \dots & \sigma_r(\alpha_n) & \mathrm{Re}(\tau_1(\alpha_n)) & \mathrm{Im}(\tau_1(\alpha_n)) & \dots & \mathrm{Re}(\tau_s(\alpha_n)) & \mathrm{Im}(\tau_s(\alpha_n))\end{pmatrix}$$

$$\rightsquigarrow\widetilde{S}=\begin{pmatrix}\sigma_1(\alpha_1) & \dots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1(\alpha_1)} & \dots & \tau_s(\alpha_1) & \overline{\tau_s(\alpha_1)}\\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots\\ \sigma_1(\alpha_n) & \dots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau_1(\alpha_n)} & \dots & \tau_s(\alpha_n) & \overline{\tau_s(\alpha_n)}\end{pmatrix}$$

$\widetilde{S}$ entsteht durch folgende Transformation pro Spaltenpaar $(x,y)$:

$$\begin{aligned}(x,y)&\mapsto(x+iy,y)\\ &\mapsto(x+iy,-2iy)\\ &\mapsto(x+iy,x-iy)\end{aligned}$$

$\Rightarrow\det(\widetilde{S})=(-2i)^s\cdot\det(S)$
Andererseits: $\det(\widetilde{S})^2=\det\big((\sigma_i(\alpha_j))_{i,j}\big)^2=d(\alpha_1,\dots,\alpha_n)=\underbrace{[\mathcal{O}_K:\mathfrak{a}]^2}_{=N(\mathfrak{a})^2}\cdot d_K\neq 0$

$\Rightarrow\det(S)\neq 0$

Genauer:

$$\mu(\underbrace{\sigma(\alpha)}_{\mathfrak{a}})=|\det(S)|=2^{-s}\cdot N(\mathfrak{a})\cdot\sqrt{|d_K|}$$

■

**Satz 5.2** Sei $\mathfrak{a} \subset \mathcal{O}_K,\ \mathfrak{a} \neq (0)$ ein ganzes Ideal. Dann gibt es ein $\alpha \in \mathfrak{a},\ \alpha \neq 0$ mit:

$$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot \sqrt{|d_K|} \cdot N(\mathfrak{a})$$

*Beweis:* Wir wollen Satz (4.10) anwenden für eine passende Menge $X(t) = \{x \in \mathbb{R}^r \times \mathbb{C}^s \mid \|x\| \leq t\}$.
$\mu(X(t)) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{t^n}{n!}$
$\mu(\sigma(\alpha)) = 2^{-s} \cdot N(\mathfrak{a}) \cdot \sqrt{|d_K|}$
Für Satz (4.10) braucht man: $\mu(X(t)) \geq 2^n \cdot \mu(\sigma(\alpha))$.
Dann existiert nach dem Satz ein $0 \neq \sigma(\alpha) \in X(t) \cap \sigma(\mathfrak{a})$.

$$\mu(X(t)) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{t^n}{n!} \overset{!}{\geq} 2^{r+2s} \cdot 2^{-s} \cdot N(\mathfrak{a}) \cdot \sqrt{|d_K|}$$
$$\Leftrightarrow t^n \geq \left(\frac{4}{\pi}\right)^s \cdot n! \cdot N(\mathfrak{a}) \cdot \sqrt{|d_K|} =: N$$

Wähle $t_0 := \sqrt[n]{N} \in \mathbb{R}$
$\overset{\text{Satz (4.10)}}{\Rightarrow} \exists\ \sigma(\alpha) \in X(t_0) \cap \sigma(\mathfrak{a})$ mit $\sigma(\alpha) \neq 0 \Rightarrow \alpha \neq 0$
Aus $\sigma(\alpha) \in X(t_0)$ folgt:

$$\|\sigma(\alpha)\| = \sum_{i=1}^{r} |\sigma_i(\alpha)| + 2 \cdot \sum_{i=1}^{s} |\tau_i(\alpha)| \leq t_0 = \sqrt[n]{N}$$
$$\overset{\text{Lemma (4.13)}}{\Rightarrow} \left( \prod_{i=1}^{r} |\sigma_i(\alpha)| \cdot \prod_{i=1}^{s} \underbrace{|\tau_i(\alpha)|^2}_{=\tau_i(\alpha)\cdot\overline{\tau_i(\alpha)}} \right)^{\frac{1}{n}} \leq \frac{\|\sigma(\alpha)\|}{n}$$
$$\Leftrightarrow \underbrace{\prod_{i=1}^{r} |\sigma_i(\alpha)| \cdot \prod_{i=1}^{s} |\tau_i(\alpha)|^2}_{=|N(\alpha)|} \leq \frac{\|\sigma(\alpha)\|^n}{n^n} \leq \frac{N}{n^n}$$

∎

---

*Beweis von Satz (3.3):* Sei $\mathfrak{a} \in I_K$ ein gebrochenes Ideal.
Wir wollen zeigen, dass es ein ganzes Ideal $\mathfrak{c} \subseteq \mathcal{O}_K$ gibt, mit $[\mathfrak{a}] = [\mathfrak{c}] \in Cl_K$ und
$N(\mathfrak{c}) \leq B_K = \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot \sqrt{|d_K|}$

Sei $x \in \mathcal{O}_K\, x \neq 0$ mit $x \cdot \mathfrak{a}^{-1} \subset \mathcal{O}_K$. Setze $\mathfrak{b} := x \cdot \mathfrak{a}^{-1}$

$$\overset{\text{Satz (5.2)}}{\Rightarrow} \exists\ \alpha \in \mathfrak{b} \text{ mit } |N_{K/\mathbb{Q}}(\alpha)| \leq B_K \cdot N(\mathfrak{b})$$

$\alpha \in \mathfrak{b} = x \cdot \mathfrak{a}^{-1} \Rightarrow \alpha = x \cdot y$ mit $y \in \mathfrak{a}^{-1}$
Setze $\mathfrak{c} := y \cdot \mathfrak{a} \subset \mathcal{O}_K$

$$\Rightarrow N(\mathfrak{c}) = N((y) \cdot \mathfrak{a}) = N((y)) \cdot N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(y)| \cdot N(\mathfrak{a})$$
$$= \left|\frac{N_{K/\mathbb{Q}}(\alpha)}{N_{K/\mathbb{Q}}(x)}\right| \cdot N(\mathfrak{a}) \underbrace{=}_{\mathfrak{b}^{-1}=x^{-1}\cdot\mathfrak{a}} |N_{K/\mathbb{Q}}(\alpha)| \cdot N(\mathfrak{b})^{-1} \leq B_K$$

und es gilt: $Cl_K \ni [\mathfrak{c}] = [(y) \cdot \mathfrak{a}] = [\mathfrak{a}]$. ∎

■ **Bemerkung** Sei $p \neq 2$ Primzahl.
Fermat $(\star)$: $x^p + y^p = z^p$ hat keine Lösungen $(x,y,z) \in \mathbb{Z}^3$ mit $xyz \neq 0$

---

Sei $\zeta_p \in \mathbb{C}$ eine $p$-te Einheitswurzel (primitiv). In $\mathbb{Z}[\zeta_p]$ ist $(\star)$ äquivalent zu:

$$y^p = z^p - x^p = (z-x)\cdot(z-\zeta_p x)\cdot\dots\cdot(z-\zeta_p^{p-1}x)$$

Falls $\mathbb{Z}[\zeta_p]$ faktoriell ist, kann man dies zum Widerspruch führen.
Problem: $\mathbb{Z}[\zeta_p]$ ist fast nie faktoriell.
Kummer: Falls $p \nmid h_{\mathbb{Q}(\zeta_p)}$, so kann man den Beweis-Ansatz retten.

---

Als nächstes: Studiere die Einheiten $\mathcal{O}_K^\times$

---

Die Sequenz:

$$\begin{array}{ccccccccc}
 & & & & & & \mathfrak{a}+P_K & & \\
 & & & & & & \| & & \\
 & & & & \mathfrak{a} & \longmapsto & [\mathfrak{a}] & & \\
 & & & & \cap & & \cap & & \\
1 & \hookrightarrow & \mathcal{O}_K^\times & \hookrightarrow & K^\times & \longrightarrow & I_K & \longrightarrow & Cl_K \longrightarrow 1 \\
 & & & & \cup & & \cup & & \\
 & & & & x & \longmapsto & x\cdot\mathcal{O}_K & &
\end{array}$$

ist exakt.

# 6. Dirichlet's Einheitensatz

Ziel: Verstehe die Einheitengruppe $\mathcal{O}_K^\times \subset \mathcal{O}_K$ besser mithilfe der Gittertheorie.
Problem: $\mathcal{O}_K^\times$ ist eine multiplikative Gruppe, d.h. $\sigma(\mathcal{O}_K^\times) \subset \mathbb{R}^r \times \mathbb{C}^s$ kann kein Gitter sein.
Betrachte:

$$\begin{array}{ccccc} K^\times & \xrightarrow{\sigma} & (\mathbb{R}^\times)^r \times (\mathbb{C})^s & \xrightarrow{\ell} & \mathbb{R}^{r+s} \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{R}^\times & \xrightarrow{x \mapsto \log(|x|)} & \mathbb{R} \end{array}$$

Hierbei:

$$\begin{aligned} \sigma : K &\longrightarrow \mathbb{R}^r \times \mathbb{C}^s \\ \alpha &\longmapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha)) \end{aligned}$$

mit $\sigma_1, \ldots, \sigma_r : K \to \mathbb{R}$ reelle Einbettungen und $\sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}} : K \to \mathbb{C}$ komplexe Einbettungen.
Außerdem: $\ell(x_1, \ldots, x_r, z_1, \ldots, z_s) = (\log(|x_1|), \ldots, \log(|x_r|), \log(|z_1|), \ldots, \log(|z_s|))$
sowie: $N(x_1, \ldots, x_r, z_1, \ldots, z_s) = \prod_{i=1}^{r} x_i \cdot \prod_{j=1}^{s} \underbrace{|z_j|^2}_{=z_j \cdot \overline{z_j}}$
und: $Tr(x_1, \ldots, x_{r+s}) = \sum_{i=1}^{r} x_i + 2 \cdot \sum_{i=1}^{s} x_{r+i}$
Damit kommutiert das Diagramm, alle Abbildungen sind Homomorphismen.

**Notation.**

$$\begin{aligned} \mu_K &:= \{\varepsilon \in K^\times \mid \exists\, n \in \mathbb{N} \text{ s.d. } \varepsilon^n = 1\} \subset \mathcal{O}_K^\times \\ &= \{\varepsilon \in \mathcal{O}_K^\times \mid \exists\, n \in \mathbb{N} \text{ s.d. } \varepsilon^n = 1\} \end{aligned}$$

*heißt Menge der Einheitswurzeln.*

Betrachte in der oberen Zeile des kommutativen Diagramms die Untergruppen:

$$\begin{aligned}\mathscr{O}_K^\times &= \{\varepsilon \in \mathscr{O}_K \mid \mathrm{N}_{K/\mathbb{Q}}(\varepsilon) = \pm 1\} \subset K^\times \\ S &:= \{v = (x_1,\dots,x_r,z_1,\dots,z_s) \in (\mathbb{R}^\times)^r \times (\mathbb{C})^s \mid \mathrm{N}(v) = \pm 1\} \subset (\mathbb{R}^\times)^r \times (\mathbb{C})^s \\ H &:= \{\underline{x} = (x_1,\dots,x_{r+s}) \in \mathbb{R}^{r+s} \mid Tr(\underline{x}) = 0\} \subset \mathbb{R}^{r+s}\end{aligned}$$

**Lemma 6.1** Es gilt: $\sigma(\mathscr{O}_K^\times) \subset S$ sowie $\ell(S) \subset H$.
Wir erhalten einen Gruppenhomomorphismus:

$$\begin{aligned}\lambda : \mathscr{O}_K^\times &\longrightarrow H \\ \alpha &\longmapsto \ell(\sigma(\alpha))\end{aligned}$$

**Satz 6.2** Sei $\Gamma := \lambda(\mathscr{O}_K^\times) \subset H$.
Die Sequenz

$$1 \hookrightarrow \mu_K \hookrightarrow \mathscr{O}_K^\times \xrightarrow{\lambda} \Gamma \to 0$$

ist exakt, d.h. an jeder Stelle

$$A \xrightarrow{\varphi} B \xrightarrow{\Psi} C$$

gilt: $\ker(\Psi) = \mathrm{Bild}(\varphi)$
D.h.: Hier ist die einzige Aussage, die zu zeigen ist, dass $\ker(\lambda) = \mu_K$

*Beweis:* „$\supseteq$“
Sei $\alpha \in \mu_K$ mit $\alpha^n = 1$

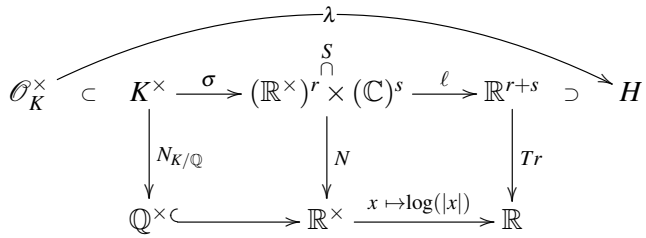
$$\begin{aligned}&\Rightarrow \sigma_i(\alpha)^n = 1 \quad \forall i \\ &\Rightarrow |\underbrace{\sigma_i(\alpha)}_{\in \mathbb{C}}| = 1 \Rightarrow \log(|\sigma_i(\alpha)|) = 0\end{aligned}$$

„$\subseteq$“

Sei $\alpha \in \ker(\lambda) \subset \mathscr{O}_K^\times$
$\lambda(\alpha) = \big(\log(|\sigma_1(\alpha)|),\dots,\log(|\sigma_r(\alpha)|),\log(|\sigma_{r+1}(\alpha)|),\dots,\log(|\sigma_{r+s}(\alpha)|)\big) = (0,\dots,0)$
$\Rightarrow \forall i:\ |\sigma_i(\alpha)| = 1$
$\sigma(\alpha) \in X(\underbrace{r+2s}_{=n})$, wobei $X(t) = \{x \in \mathbb{R}^r \times \mathbb{C}^s \mid \|x\| \le t\}$ und $X(r+2s)$ eine kompakte Teilmenge von $\mathbb{R}^{r+2s} \cong \mathbb{R}^r \times \mathbb{C}^s$ ist.
$\sigma(\alpha) \in \sigma(\mathscr{O}_K) \leftarrow$ Gitter in $\mathbb{R}^{r+2s}$
$\Rightarrow \sigma(\alpha) \cap X(n)$ ist endlich
$\Rightarrow \ker(\lambda) \subset \mathscr{O}_K^\times \subset K^\times$ ist endlich
$\Rightarrow$ jedes Element im $\ker(\lambda)$ hat endliche Ordnung
$\Rightarrow \ker(\lambda) \subset \mu_K$ ∎

**Satz 6.3** Die Gruppe $\Gamma \subset H$ ist ein vollständiges Gitter im $\mathbb{R}$-Vektorraum $H \cong \mathbb{R}^{r+s-1}$

*Beweis:* Erinnerung: Betrachte:




0. $H \cong \mathbb{R}^{r+s-1}$: $H = \ker(Tr(\mathbb{R}^{r+s}))$

$$Tr : \mathbb{R}^{r+s} \longrightarrow \mathbb{R}$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_{r+s} \end{pmatrix} \longmapsto \begin{pmatrix} 1 & \dots & 1 & 2 & \dots & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_{r+s} \end{pmatrix}$$

Kern hat eine Dimension weniger als der Vektorraum.

1. $\Gamma$ ist Gitter:
Kriterium: $\Gamma$ ist Gitter $\iff$ $\forall\, M \subset H$ beschränkt gilt: $\Gamma \cap M$ ist endlich
Sei dazu für $t > 0$ :

$$U(t) := \{x = (x_1, \dots, x_{r+s}) \in \mathbb{R}^{r+s} \mid |x_i| \leq t \ \forall i\}$$

$\Rightarrow \ell^{-1}(U(t)) = \{(x_1, \dots, x_r, z_1, \dots, z_s) \in (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \mid e^{-t} \leq |x_i| \leq e^t \ \forall i,\ e^{-t} \leq |z_i| \leq e^t \ \forall i\}$
$\Rightarrow \ell^{-1}(U(t))$ ist beschränkt $\Rightarrow \ell^{-1}(U(t)) \cap \sigma(\mathcal{O}_K^\times)$ ist endlich, denn $\sigma(\mathcal{O}_K)$ ist ein Gitter
$\Rightarrow U(t) \cap \underbrace{\ell(\sigma(\mathcal{O}_K^\times))}_{=\Gamma}$ ist endlich $\Rightarrow \Gamma$ ist ein Gitter

2. $\mathrm{Rang}(\Gamma) = r+s-1$ :
   (a) Dazu: Konstruiere eine beschränkte Menge $T \subset S$, so dass

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} T \cdot \sigma(\varepsilon)$$

Dann folgt:

$$H = \bigcup_{\gamma \in \Gamma} (\ell(T) + \gamma) \qquad \text{mit } \ell(T) \subset H \text{ beschränkt}$$

Konstruiere $T$ folgendermaßen:
Sei $x \in S$. Dann ist $x \cdot \sigma(\mathcal{O}_K) = \{x \cdot \sigma(\alpha) \mid \alpha \in \mathcal{O}_K\}$ (komponentenweise Multiplikation) ein Gitter in $\mathbb{R}^{r+2s}$ vom Volumen:

$$\mu(x \cdot \sigma(\mathcal{O}_K)) \overset{x \in S}{=} \mu(\sigma(\mathcal{O}_K)) = 2^{-s} \cdot \sqrt{|d_K|}$$

Die erste Gleichheit gilt, da der Skalierungsfaktor gerade der Betrag der Norm $|N(x)| \overset{x \in S}{=} 1$ beträgt, da der $i$-te Eintrag der $j$-ten Basisvektors mit $x_i$ multipliziert wird.

Sei $t \in \mathbb{R}^+$ mit $t^n \geq \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|d_K|} \cdot n!$

$$\Rightarrow \mu(X(t)) \geq 2^n \cdot \mu(x \cdot \sigma(\mathcal{O}_K))$$
$$\overset{\text{Satz (4.10)}}{\Rightarrow} \exists\, y \in x \cdot \sigma(\mathcal{O}_K) \cap X(t), \text{ mit } y \neq 0$$
$$\Rightarrow \exists\, 0 \neq \alpha \in \mathcal{O}_K \text{ mit } y = x \cdot \sigma(\alpha) \in X(t)$$
$$\Rightarrow |N_{K/\mathbb{Q}}(\alpha)| = |N(\sigma(\alpha))| = |\underbrace{N(x)}_{=1} \cdot N(\sigma(\alpha))| = |N(\underbrace{x \cdot \sigma(\alpha)}_{=y})| \leq t^n$$

weil $\forall x \in X(t):\ \|x\| \leq t \Rightarrow |x_i| \leq t,\ |z_i| \leq \frac{t}{2} \Rightarrow |N(x)| \leq \frac{t^{r+2s}}{2^{2s}}$

$$\Rightarrow |N_{K/\mathbb{Q}}(\alpha)| \leq t^n$$

Es gibt bis auf Assoziiertheit nur endlich viele $\alpha \in \mathcal{O}_K$ mit $|N_{K/\mathbb{Q}}(\alpha)| \leq t^n$, denn im Beweis von Satz (3.4) hatten wir gezeigt, dass es nur endlich viele Ideale $\mathfrak{a} \subset \mathcal{O}_K$ gibt, mit $N(\mathfrak{a}) \leq t^n$, insbesondere gibt es nur endlich viele Hauptideale $(\alpha) \subset \mathcal{O}_K$ mit $|N_{K/\mathbb{Q}}(\alpha)| = N((\alpha)) \leq t^n$ und:
$(\alpha) = (\beta) \iff \alpha = \varepsilon \cdot \beta \qquad \varepsilon \in \mathcal{O}_K^\times$

---

Seien nun also $\beta_1, \ldots \beta_N \in \mathcal{O}_K$ ein Vertretersystem (modulo Assoziiertheit) der Elemente von Norm $\leq t^n$
Ist dann $\gamma \in \mathcal{O}_K$ mit $x \cdot \sigma(\gamma) \in X(t)$, so gibt es also ein $i \in \{1, \ldots, N\}$ und ein $\varepsilon \in \mathcal{O}_K^\times$ mit $\gamma = \beta_i \cdot \varepsilon$

$$\Rightarrow \sigma(\beta_i^{-1}) \cdot X(t) \ni x \cdot \sigma(\varepsilon) = x \cdot \sigma(\beta_i^{-1}) \cdot \sigma(\gamma) = \underbrace{x \cdot \sigma(\gamma)}_{\in X(t)} \cdot \sigma(\beta^{-1})$$

Setze $T := \sigma(\beta_1^{-1}) \cdot X(t) \cup \cdots \cup \sigma(\beta_N^{-1}) \cdot X(t)$
Da $X(t)$ beschränkt ist, ist auch $T$ beschränkt. Es existiert also für alle $x \in S$ ein $\varepsilon = \varepsilon(x) \in \mathcal{O}_K^\times$ mit $x \cdot \sigma(\varepsilon) \in T \Leftrightarrow x \in T \cdot \sigma(\varepsilon^{-1})$ $(\star)$

(b)
- Falls $\underline{r+s-1=0:}$ ✓
- Nehme an, dass $\underline{r+s-1>0}$:
  Sei $M \in \mathbb{R}^+$ mit: $\forall x \in T:\ |x_i|,\ |z_i| \leq M$
  Seien $a_1, \ldots, \mathfrak{a}_{r+s} \in S$ mit $a_i = (a_{i,1}, \ldots, a_{i,r+s})$ und so, dass $|a_{i,j}| > M$ für $i \neq j$ und $a_{i,i}$ so, dass $a_i \in S$, das heißt $|N(a_i)| = 1$.

$$\overset{(\star)}{\Rightarrow} \underbrace{\varepsilon(a_1)}_{=\varepsilon_1}, \ldots, \underbrace{\varepsilon(a_{r+s})}_{=\varepsilon_{r+s}} \in \mathcal{O}_K^\times \text{ mit } \quad \underbrace{a_i}_{=\begin{pmatrix} a_{i,1} \\ \vdots \\ a_{i,r+s} \end{pmatrix}} \cdot \underbrace{\sigma(\varepsilon_i)}_{=\begin{pmatrix} \sigma_1(\varepsilon_i) \\ \vdots \\ \sigma_{r+s}(\varepsilon_i) \end{pmatrix}} \in T$$

$$\Rightarrow |\sigma_j(\varepsilon_i)| < 1 \quad i \neq j$$
$$\Rightarrow \log(|\sigma_j(\varepsilon_i)|) < 0 \quad i \neq j$$

$\underline{\text{Beh.:}}$ $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})$ sind $\mathbb{R}$-linear unabhängig

Sei $B := \begin{pmatrix} \log(|\sigma_1(\varepsilon_1)|) & \cdots & \log(|\sigma_r(\varepsilon_1)|) & 2\log(|\sigma_{r+1}(\varepsilon_1)|) & \cdots & 2\log(|\sigma_{r+s-1}(\varepsilon_1)|) \\ \vdots & & \vdots & \vdots & & \vdots \\ \log(|\sigma_1(\varepsilon_{r+s-1})|) & \cdots & \log(|\sigma_r(\varepsilon_{r+s-1})|) & 2\log(|\sigma_{r+1}(\varepsilon_{r+s-1})|) & \cdots & 2\log(|\sigma_{r+s-1}(\varepsilon_{r+s-1})|) \end{pmatrix}$

$B = (b_{ij})_{i,j} \in \mathbb{R}^{(r+s-1)\times(r+s-1)}$
Es gilt:

i. $b_{ij} < 0$ für $i \neq j$

ii. $\sum_{j=1}^{r+s-1} b_{ij} = \underbrace{Tr(\lambda(\varepsilon_i))}_{=0} - \begin{cases} 2 \cdot \log|\sigma_{r+s}(\varepsilon_i)| & \text{für } s > 0 \\ \log|\sigma_{r+s}(\varepsilon_i)| & \text{für } s = 0 \end{cases}$

$\Rightarrow \sum_{j=1}^{r+s-1} b_{ij} > 0 \qquad \forall i = 1, \ldots, r+s-1$

Für den Rest des Beweises benötigen wir das folgende Lemma:

---

**Lemma** Sei $B \in \mathbb{R}^{k \times k}$ mit $b_{ij} < 0 \; \forall i \neq j$, sowie $\sum_{j=1}^{k} b_{ij} > 0$. Dann ist $B$ invertierbar.

*Beweis:* Sei $x \in \mathbb{R}^k$ eine Lösung von $Bx = 0$. Angenommen $x \neq 0$. Sei $i_o \in \{1, \ldots, k\}$ mit $|x_{i_0}| = \max_i\{|x_i|\}$
Œ $x_{i_0} = 1$ (durch skalieren auf 1)
$\Rightarrow |x_i| \leq 1 \; \forall i$
$\Rightarrow$ der $i_0$-te Eintrag von $B \cdot x$ ist:

$$0 = \sum_{j=1}^{k} b_{i_0,j} \cdot x_j = b_{i_0,i_0} + \sum_{\substack{j=1 \\ j \neq i_0}}^{k} b_{i_0,j} \cdot x_j$$

$$\geq b_{i_0,i_0} + \sum_{\substack{j=1 \\ j \neq i_0}}^{k} b_{i_0,j} > 0 \; \lightning$$

∎

---

*Fortsetzung des Beweises von Satz 6.3:*
$\Rightarrow B$ ist invertierbar. Benutze den Isomorphismus

$$H \xrightarrow{\cong} \mathbb{R}^{r+s-1}$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_{r+s-1} \\ x_{r+s} \end{pmatrix} \longmapsto \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ 2x_{r+1} \\ \vdots \\ 2x_{r+s-1} \end{pmatrix}$$

$\Rightarrow \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r+s-1})$ sind linear unabhängig über $\mathbb{R}$.
$\text{Rang}(\Gamma) \geq r+s-1 \qquad (\Gamma \subset H \Rightarrow \text{Rang}(\Gamma) \leq r+s-1)$ ∎

---

**Satz 6.4 — Dirichlet's Einheitensatz.** Die Gruppe $\mathcal{O}_K^\times$ ist eine endlich erzeugte abelsche Gruppe von Rang $r+s-1$. Es gilt:

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}$$

Insbesondere gibt es also $r+s-1$ *Fundamentaleinheiten* $\varepsilon_1,\dots,\varepsilon_{r+s-1}\in\mathcal{O}_K^\times$, so dass gilt:

$$\mathcal{O}_K^\times=\{\omega\cdot\varepsilon_1^{n_1}\cdot\dots\cdot\varepsilon_{r+s-1}^{n_{r+s-1}}\mid\omega\in\mu_K,\ n_1,\dots,n_{r+s-1}\in\mathbb{Z}\}$$

*Beweis:* Satz (6.2) besagt, dass

$$1\longrightarrow\mu_K\longrightarrow\mathcal{O}_K^\times\xrightarrow{\lambda}\Gamma\longrightarrow 0$$

exakt ist. Mit dem Homomorphiesatz folgt:

$$\mathcal{O}_K^\times/\mu_K\cong\Gamma\overset{\text{Satz (6.3)}}{\cong}\mathbb{Z}^{r+s-1}$$

Seien $\gamma_1,\dots,\gamma_{r+s-1}\in\Gamma$ eine $\mathbb{Z}$-Basis von $\Gamma$ und $\varepsilon_1,\dots,\varepsilon_{r+s-1}\in\mathcal{O}_K^\times$ mit $\lambda(\varepsilon_i)=\gamma_i$.
Die Abbildung

$$\begin{aligned}\varphi:\Gamma&\longrightarrow\mathcal{O}_K^\times\\ \sum_{i=1}^{r+s-1}n_i\gamma_i&\longmapsto\prod_{i=1}^{r+s-1}\varepsilon_i^{n_i}\end{aligned}$$

ist ein Gruppenhomomorphismus mit $\lambda\circ\varphi=\mathrm{id}_\Gamma$.

$$\rightsquigarrow\ 1\longrightarrow\mu_K\longrightarrow\mathcal{O}_K^\times\underset{\varphi}{\overset{\lambda}{\rightleftarrows}}\Gamma\longrightarrow 0$$

Das heißt die Sequenz spaltet mittels $\varphi$.
$\mathrm{Bild}(\varphi)\cap\mu_K=\{1\}$, da die $\varepsilon_i$ unendliche Ordnung haben $\rightsquigarrow$ keine Einheitswurzeln sind.
Explizit: Betrachte $\varphi(\Gamma)\subset\mathcal{O}_K^\times$ Untergruppe. Es gilt $\varphi(\Gamma)\cap\mu_K=\{1\}$

$$\begin{aligned}\Gamma\times\mu_K\cong\varphi(\Gamma)\times\mu_K&\xrightarrow{\Psi}\mathcal{O}_K^\times\\ (\varepsilon,\omega)&\longmapsto\varepsilon\cdot\omega\end{aligned}$$

Zeige, dass diese Abbildung bijektiv ist:
$\Psi$ injektiv: $\Psi(\varepsilon_1,\omega_1)=\Psi(\varepsilon_2,\omega_2)$
$\Rightarrow\varepsilon_1\cdot\varepsilon_2^{-1}\cdot\omega_1\cdot\omega_2^{-1}=1\Rightarrow 0=\lambda(1)=\lambda(\varepsilon_1\cdot\varepsilon_2^{-1}\cdot\omega_1\cdot\omega_2^{-1})=\lambda(\varepsilon_1\cdot\varepsilon_2^{-1})$
$\Rightarrow\varepsilon_1\cdot\varepsilon_2^{-1}\in\mu_K=\mathrm{Kern}(\lambda)$ und $\varepsilon_1\cdot\varepsilon_2^{-1}\in\mathrm{Bild}(\varphi)\Rightarrow\varepsilon_1\cdot\varepsilon_2^{-1}=1\Rightarrow\varepsilon_1=\varepsilon_2$
$\Rightarrow\omega_1=\omega_2$ ✓

$\Psi$ surjektiv: Wir wissen: $\mathcal{O}_K^\times/\mu_K\cong\Gamma$
$\Rightarrow\mathcal{O}_K^\times=\bigcup_{\gamma\in\Gamma}\varphi(\gamma)\cdot\mu_K\Rightarrow$ Sei $\varepsilon\in\mathcal{O}_K^\times$, dann gibt es ein $\gamma\in\Gamma$ und $\omega\in\mu_K$ mit: $\varepsilon=\varphi(\gamma)\cdot\omega$ ∎

**Beispiel — Beispiel zu Fundamentaleinheiten.**

1. $K=\mathbb{Q}\Rightarrow r=1,\ s=0$ und $\mu_K=\{\pm1\}$

   $$\Rightarrow\mathbb{Z}^\times=\{\pm1\}=\mu_K$$

2. $K=\mathbb{Q}(\sqrt{D})$ mit $D$ quadratfrei.
   (a) $D<0$ (imaginär-quadratisch)

$\Rightarrow r = 0,\ s = 1 \Rightarrow r + s - 1 = 0$

$\Rightarrow \mathcal{O}_K^\times = \mu_K$ endlich

$$\text{und } \mu_K = \begin{cases} \{\pm 1\} & d_K < -4 \\ \{\pm 1,\ \pm i\} & d_K = -4 \\ \{\pm 1,\ \pm e^{\frac{2\pi i}{3}},\ \pm e^{\frac{4\pi i}{3}}\} & d_K = -3 \end{cases}$$

(b) $D > 0$ (reell-quadratisch)
$\Rightarrow r = 2,\ s = 0 \Rightarrow r + s - 1 = 1$ und $\mu_K = \{\pm 1\}$

$\Rightarrow \mathcal{O}_K^\times = \{\pm \varepsilon^n \mid n \in \mathbb{Z}\}$

wobei $\varepsilon$ Fundamentaleinheit ist.

- $D = 2 \qquad \varepsilon = 1 + \sqrt{2}$
- $D = 3 \qquad \varepsilon = 2 + \sqrt{3}$
- $D = 31 \qquad \varepsilon = 1520 + 273\sqrt{31}$
- $D = 94 \qquad \varepsilon = 2143295 + 221064\sqrt{94}$

  Aber:
- $D = 95 \qquad \varepsilon = 39 + 4\sqrt{95}$

Eine Fundamentaleinheit $\varepsilon \subset \mathcal{O}^\times_{\mathbb{Q}(\sqrt{D})}$ liefert eine Lösung der *Pellschen Gleichung*:

$$x^2 - D \cdot y^2 = \pm 4 \qquad (x, y \in \mathbb{Z})$$

Denn:

- Ist $d_K \equiv 0 \pmod 4$, das heißt $D = 2,3 \pmod 4$ und $\varepsilon = a + b\sqrt{D}$ mit $a, b \in \mathbb{Z}$ so folgt:

  $\Rightarrow N(\varepsilon) = a^2 - Db^2 = \pm 1$

  Wähle $x = 2a,\ y = 2b$.
- Ist $d_K = D \equiv 1 \pmod 4$, und $\varepsilon = \frac{a + b\sqrt{D}}{2}$ mit $a, b \in \mathbb{Z},\ a \equiv b \pmod 2$ so folgt:

  $$\Rightarrow \pm 1 = N(\varepsilon) = \frac{a^2}{4} - D\frac{b^2}{4}$$

  Wähle $x = a,\ y = b$

Mann kann die Fundamentaleinheit von $\mathbb{Q}(\sqrt{D}),\ D > 0$ z.B. mit Hilfe von Kettenbrüchen bestimmen.

## 6.1 Einschub: Kettenbrüche

**Definition 6.5** Ein *endlicher Kettenbruch* ist ein Ausdruck der Form

$$a_o + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots a_{n-1} + \frac{1}{a_n}}}} =: [a_0, a_1, \ldots, a_n]$$

*unendlicher Kettenbruch*:

$$\lim_{n \to \infty} [a_0, a_1, \ldots, a_n] \qquad \text{für eine Folge } (a_n)_{n \in \mathbb{N}} \subset \mathbb{R}$$

**Beispiel 6.6**

$$\begin{aligned}\sqrt{2} &= [1,2,2,\dots] =: [1,\overline{2}] \\ &= 1+(\sqrt{2}-1) = 1+\frac{1}{1+\sqrt{2}} = 1+\frac{1}{2+\frac{1}{1+\sqrt{2}}}\end{aligned}$$

(periodischer Kettenbruch)

**Definition** Bei einem unendlichen Kettenbruch $[a_0,a_1,\dots]$ mit $a_n \in \mathbb{Z}$ heißt:

$$[a_0,a_1,\dots,a_n] = \frac{p_n}{q_n}$$

der *n-te Näherungsbruch*.

■ **Bemerkung** Fakten:

- Jede reelle Zahl hat eine konvergente Kettenbruchentwicklung mit $a_n \in \mathbb{Z}$
- Endliche Kettenbrüche $\leftrightarrow \mathbb{Q}$
- Periodische Kettenbrüche $\leftrightarrow$ quadratische Irrationalzahlen: $x \in \mathbb{R}\setminus\mathbb{Q}$ Nullstellen vom Polynom $ax^2+bx+c$ mit $a,b,c \in \mathbb{Z}$
- Ist $d \in \mathbb{N}$, $d$ kein Quadrat und $p,q \in \mathbb{Z}$ mit $p^2-dq^2 = \pm 1$
  Dann ist $\frac{p}{q}$ ein Näherungsbruch der Kettenbruchentwicklung von $\sqrt{d}$.

---

Sei $\ell$ die minimale Periodenlänge der Kettenbruchentwicklung von $\sqrt{d}$ ($d>0$ quadratfrei) und $\frac{p}{q}$ der $(\ell-1)$-te Näherungsbruch.
Dann ist die eindeutig bestimmte Fundamentaleinheit $\varepsilon \in \mathcal{O}_K \subset \mathbb{Q}(\sqrt{d})$ mit $\varepsilon > 1$ gegeben durch:

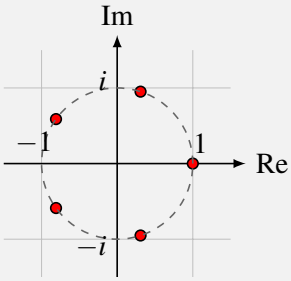
$$\begin{aligned} \varepsilon = p+q\sqrt{d} \qquad & \text{falls } d \equiv 2,3 \pmod 4 \text{ oder } d \equiv 1 \pmod 8 \\ \text{und } \varepsilon = p+q\sqrt{d} \text{ oder } \varepsilon^3 = p+q\sqrt{d} \qquad & \text{sonst } (d \equiv 5 \pmod 8)\end{aligned}$$

**Beispiel**

- $\sqrt{2} = [1,\overline{2}] \Rightarrow \ell = 1$
  0-ter Näherungsbruch: $1 \rightsquigarrow 1+\sqrt{2}$ ist Fundamentaleinheit
- $d=94$: $\sqrt{94} = [9,\overline{1,2,3,1,1,5,1,8,1,5,1,1,3,2,1,18}] \Rightarrow \ell = 16$
  15-ter Näherungsbruch: $\frac{p}{q} = \frac{2143295}{221064} \rightsquigarrow 2143295+221064\sqrt{94}$ ist Fundamentaleinheit
- $d=95$: $\sqrt{95} = [9,\overline{1,2,1,18}] \Rightarrow \ell = 4$
  3-ter Näherungsbruch: $\frac{p}{q} = \frac{39}{4} \rightsquigarrow 39+4\sqrt{95}$ ist Fundamentaleinheit

Damit können wir das *Beispiel zu Fundamentaleinheiten* erweitern:

**Beispiel** 3. Sei $[K:\mathbb{Q}] = 4$ mit $r=0$, $s=2 \rightsquigarrow r+s-1=1$
$\Rightarrow \operatorname{Rang}(\mathcal{O}_K^\times) = 1$
$\Rightarrow \mathcal{O}_K^\times = \{\omega\cdot\varepsilon^n \mid \omega \in \mu_K,\ n \in \mathbb{Z},\}$ und $\varepsilon$ ist eine Fundamentaleinheit
Beispielsweise: $K = \mathbb{Q}(\zeta_5)$, wobei $\zeta_5 = e^{\frac{2\pi i}{5}}$ primitive 5-te Einheitswurzel ist.
Mipo: $X^4+X^3+X^2+X+1$
$\mu_K = \{\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4, \zeta_5^5 = 1\}$




$\rightsquigarrow$ keine reellen Einbettungen
z.B.: $\varepsilon = 1 + \zeta_5$

# 7. Zerlegung von Primidealen in Erweiterungen

Ist $A \subset B$ eine Erweiterung von Dedekindringen und $\mathfrak{p} \subset A$ ein Primideal, so zerfällt $\mathfrak{p}$ in $B$:

$$\mathfrak{p} \cdot B = \mathfrak{Q}_1^{e_1} \cdot \dots \cdot \mathfrak{Q}_r^{e_r} \qquad (\mathfrak{Q}_i \subset B \text{ Primideal}, \ e_i \in \mathbb{N})$$

Hier: $K \subset L$ algebraischer Zahlkörper, $\mathcal{O}_K \subset \mathcal{O}_L$. Wie zerfallen Primideale $\mathfrak{p} \subset \mathcal{O}_K$ in $\mathcal{O}_L$?

**Proposition 7.1** Seien $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ und $(0) \neq \mathfrak{Q} \subset \mathcal{O}_L$ Primideale. Dann sind folgende Bedingungen äquivalent:

1. $\mathfrak{Q} \mid \mathfrak{p} \cdot \mathcal{O}_L$ d.h. $\mathfrak{p} \cdot \mathcal{O}_L \subset \mathfrak{Q}$
2. $\mathfrak{Q} \supset \mathfrak{p}$
3. $\mathfrak{Q} \cap \mathcal{O}_K = \mathfrak{p}$
4. $\mathfrak{Q} \cap K = \mathfrak{p}$

---

*Beweis:* „1. $\iff$ 2."
Klar, denn $\mathfrak{p} \subset \mathfrak{p} \cdot \mathcal{O}_L$ und $\mathfrak{Q} \subset \mathcal{O}_L$
„3.$\Rightarrow$ 2."
Klar
„3. $\iff$ 4."
$\mathfrak{Q} \cap K \subset \mathcal{O}_K$ wegen $\mathcal{O}_K$ ganzabgeschlossen.
„2.$\Rightarrow$ 3."
Sei also $\mathfrak{p} \subset \mathfrak{Q}$.
Klar: $\mathfrak{Q} \cap \mathcal{O}_K \supset \mathfrak{p} \cap \mathcal{O}_K = \mathfrak{p}$
Zu zeigen bleibt, dass $\mathfrak{Q} \cap \mathcal{O}_K \subset \mathfrak{p}$ ist:
Da $\mathfrak{p}$ maximal: Falls nicht $\mathfrak{Q} \cap \mathcal{O}_K \subset \mathfrak{p}$ ($\Rightarrow \mathfrak{Q} \cap \mathcal{O}_K \supsetneq \mathfrak{p}$), so ist $\mathfrak{Q} \cap \mathcal{O}_K = \mathcal{O}_K$
Ist aber $\mathfrak{Q} \cap \mathcal{O}_K = \mathcal{O}_K$, so folgt $\Rightarrow 1 \in \mathfrak{Q} \Rightarrow \mathfrak{Q} = \mathcal{O}_L$ $\lightning$ $\mathfrak{Q}$ Primideal ∎

---

**Definition** Falls eine der äquivalenten Bedingungen aus Proposition (7.1) erfüllt ist, so sagen wir:
$\mathfrak{L}$ *liegt über* $\mathfrak{p}$ beziehungsweise $\mathfrak{p}$ *liegt unter* $\mathfrak{L}$.

$$\begin{array}{ccc} \mathfrak{L} & \subset & \mathcal{O}_L \\ | & & | \\ \mathfrak{p} & \subset & \mathcal{O}_K \end{array}$$

**Proposition 7.2**
1. Jedes Primideal $(0) \neq \mathfrak{L} \subset \mathcal{O}_L$ liegt über genau einem Primideal $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$.
2. Ist $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ Primideal, so gibt es mindestens ein Primideal $(0) \neq \mathfrak{L} \subset \mathcal{O}_L$, das über $\mathfrak{p}$ liegt.

---

*Beweis:*

1. Sei $(0) \neq \mathfrak{L} \subset \mathcal{O}_L$ Primideal. Definiere $\mathfrak{a} := \mathfrak{L} \cap \mathcal{O}_K$. Wir haben bereits gesehen, dass $\mathfrak{a} \subset \mathcal{O}_K$ Primideal ist. $\mathfrak{a} \neq \mathcal{O}_K$ ist klar. Zu zeigen bleibt, dass $\mathfrak{a} \neq (0)$ ist:
   Sei $\alpha \in \mathfrak{L} \setminus \{0\}$
   $\Rightarrow$ Es existieren $a_{n-1}, \ldots, a_o \in \mathcal{O}_K$, $a_o \neq 0$ mit:
   $$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$
   $$\Rightarrow \mathcal{O}_K \ni a_0 = \underbrace{-\alpha}_{\in \mathfrak{L}} \cdot \underbrace{(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1)}_{\in \mathcal{O}_L} \in \mathfrak{L}$$
   $$\Rightarrow a_0 \neq 0 \in \mathfrak{L} \cap \mathcal{O}_K = \mathfrak{a}$$
2. Folgt aus der Primidealzerlegung, falls $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$.
   Angenommen $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$. Dann würde einerseits gelten:
   $$\mathfrak{p}^{-1}\mathfrak{p}\mathcal{O}_L = \mathcal{O}_K \cdot \mathcal{O}_L = \mathcal{O}_L$$
   Andererseits, da $\mathfrak{p}^{-1} \supsetneq \mathcal{O}_K$:
   $$\mathfrak{p}^{-1}\mathfrak{p}\mathcal{O}_L \supsetneq \mathcal{O}_K \cdot \mathfrak{p} \cdot \mathcal{O}_L = \mathcal{O}_K \cdot \mathcal{O}_L = \mathcal{O}_L \quad \lightning$$

∎

---

**Definition 7.3**
- Ist $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ ein Primideal mit:
  $$\mathfrak{p} \cdot \mathcal{O}_L = \mathfrak{L}_1^{e_1} \cdot \cdots \cdot \mathfrak{L}_r^{e_r},$$
  wobei $\mathfrak{L}_1, \ldots, \mathfrak{L}_r$ verschiedene Primideale in $\mathcal{O}_L$ sind.
  Dann heißen $e_1 =: e(\mathfrak{L}_1|\mathfrak{p}), \ldots, e_r =: e(\mathfrak{L}_r|\mathfrak{p})$ *Verzweigungsindizes* von $\mathfrak{p}$ in $\mathcal{O}_L$.
- Ist $e_1 = \cdots = e_r = 1$, so heißt $\mathfrak{p}$ *unverzweigt* in $\mathcal{O}_L$, sonst heißt $\mathfrak{p}$ *verzweigt*.

Weitere wichtige Invarianten: Trägheitsgrade:
Ist $\mathfrak{L} \subset \mathcal{O}_L$ ein Primideal über $\mathfrak{p}$, betrachte:

$$\mathcal{O}_K \hookrightarrow \mathcal{O}_L \xrightarrow{\pi} \mathcal{O}_L/\mathfrak{L} \qquad \text{mit dem Kern: } \mathfrak{p}$$

Erhalte eine Inklusion der Restklassenkörper:

$$\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{L}$$

Dies ist eine endliche Körpererweiterung.

**Definition 7.4** In dieser Situation wird der Grad der Körpererweiterung $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{Q}$ als *Trägheitsgrad* von $\mathfrak{Q}$ über $\mathfrak{p}$ bezeichnet. Notation: $f(\mathfrak{Q}|\mathfrak{p})$

**Beispiel 7.5** Für $\mathbb{Q}(i)/\mathbb{Q}$:

- $p = 2$:

$$2 = (1+i)(1-i) = \underbrace{-i}_{\in \mathbb{Z}[i]^\times} \cdot (1+i)^2$$

$\rightsquigarrow 2\mathbb{Z}[i] = ((1+i)\mathbb{Z}[i])^2$
$\rightsquigarrow$ Verzweigungsindex: $e\big((1+i)\mathbb{Z}[i]\big|2\mathbb{Z}\big) = 2$
Trägheitsgrad:

$$\begin{aligned}\left|\mathbb{Z}[i]/_{(1+i)\cdot\mathbb{Z}[i]}\right| &= N((1+i)\cdot\mathbb{Z}[i]) \\ &= |N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i)| = 2\end{aligned}$$

$\Rightarrow f\big((1+i)\cdot\mathbb{Z}[i]\big|2\mathbb{Z}\big) = 1$

- Ist $p \in \mathbb{Z}$ Primzahl mit $p \equiv 3 \pmod 4$
$p\cdot\mathbb{Z}[i]$ ist prim ($p$ ist *träge*)
$e(p\cdot\mathbb{Z}[i]|p\mathbb{Z}) = 1$

$$\left|\mathbb{Z}[i]/_{p\mathbb{Z}[i]}\right| = N(p\mathbb{Z}[i]) = |N_{\mathbb{Q}(i)/\mathbb{Q}}(p)| = p^2$$

$\Rightarrow f(p\mathbb{Z}[i]|p\mathbb{Z}) = 2$

- Ist $p \in \mathbb{Z}$ Primzahl mit $p \equiv 1 \pmod 4$
$\Rightarrow \exists\, a,b,\in \mathbb{Z}$ mit $p = a^2+b^2$

$$p\cdot\mathbb{Z}[i] = \mathfrak{p}\cdot\mathfrak{p}' \qquad \text{mit } \mathfrak{p} = (a+bi)\cdot\mathbb{Z}[i],\ \mathfrak{p}' = (a-bi)\cdot\mathbb{Z}[i]$$

$\mathfrak{p},\mathfrak{p}'$ nicht assoziiert. $e(\mathfrak{p}|p\mathbb{Z}) = e(\mathfrak{p}'|p\mathbb{Z}) = 1$

$$\begin{aligned}&p^2 = N(p\mathbb{Z}[i]) = N(\mathfrak{p}\mathfrak{p}') = N(\mathfrak{p})N(\mathfrak{p}') \\ &\Rightarrow N(\mathfrak{p}) = N(\mathfrak{p}') = p \\ &\Rightarrow f(\mathfrak{p}|p\mathbb{Z}) = f(\mathfrak{p}'|p\mathbb{Z}) = 1\end{aligned}$$

Beobachtung: $\sum_{i=1}^{r} e_i \cdot f_i = 2$

**Lemma 7.6** Sei $\mathfrak{p} \subset \mathcal{O}_K$ Primideal und $n = [L:K]$. Es gilt:

1. $N(\mathfrak{p}\cdot\mathcal{O}_L) = N(\mathfrak{p})^n$
2. Ist $\mathfrak{Q} \subset \mathcal{O}_L$ Primideal über $\mathfrak{p}$, so gilt:

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

*Beweis:*

- $\mathcal{O}_K \hookrightarrow \mathcal{O}_L \xrightarrow{\pi} \mathcal{O}_L/\mathfrak{p}\cdot\mathcal{O}_L \rightsquigarrow$ Man kann $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{p}\cdot\mathcal{O}_L$ auffassen. (Vorsicht: Im Allgemeinen ist das keine Körpererweiterung, aber: $\mathcal{O}_L/\mathfrak{p}\cdot\mathcal{O}_L$ ist $\mathcal{O}_K/\mathfrak{p}$-Vektorraum)
- $\mathcal{O}_L$ ist endlich erzeugter $\mathcal{O}_K$-Modul

$$\Rightarrow \dim_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{p}\cdot\mathcal{O}_L) < \infty$$

1. Behauptung: $\dim_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{p}\cdot\mathcal{O}_L)$

„$\leq$“: Sei $\overline{\omega_1},\dots,\overline{\omega_m}$ Basis von $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ über $\mathcal{O}_K/\mathfrak{p}$ und $\omega_1,\dots,\omega_m \in \mathcal{O}_L$ mit $\pi(\omega_i)=\overline{\omega_i}$.
Zeige $\omega_1,\dots,\omega_m$ sind linear unabhänig über $K$ (bzw. $\mathcal{O}_K$)
Angenommen, $\omega_1,\dots,\omega_m$ sind linear abhänig.
$\Rightarrow \exists\, a_1,\dots,a_m \in \mathcal{O}_K,\ (a_1,\dots,a_m)\neq(0,\dots,0)$ mit $\sum_{i=1}^{m} a_i\omega_i = 0$.
Sei $\mathfrak{a}=(a_1,\dots,a_m)\subset\mathcal{O}_K$ das von $a_1,\dots,a_m$ erzeugte Ideal.
Sei $x\in\mathfrak{a}^{-1}$ mit $x\notin\mathfrak{a}^{-1}\cdot\mathfrak{p}\Rightarrow x\cdot\mathfrak{a}\not\subseteq\mathfrak{p}$. (Wir finden so ein $x$, da $\mathfrak{a}^{-1}\supsetneq\mathfrak{a}^{-1}\cdot\mathfrak{p}$. Die Ungleichheit folgt aus der Eindeutigkeit der Primidealzerlegung. Weiter gilt für $\alpha\in\mathfrak{a}^{-1}\cdot\mathfrak{p}$ :
$\alpha=\sum_{\in\mathfrak{a}^{-1}}\widetilde{a}_i\ \cdot\underset{\in\mathfrak{p}}{b_i}\Rightarrow\alpha\cdot\mathfrak{a}=\sum\widetilde{a}_ib_i\mathfrak{a}=\sum_{\in\mathfrak{p}\subset\mathcal{O}_K}b_i\ \underset{\in\mathcal{O}_K}{(\widetilde{a}_i\mathfrak{a})}\subset\mathcal{O}_K\Rightarrow\alpha\in\mathfrak{a}^{-1}$).
$\Rightarrow xa_1,\dots,xa_m\in\mathcal{O}_K$ aber $\exists\, i_0\in\{1,\dots,m\}$ mit $x\mathfrak{a}_{i_0}\notin\mathfrak{p}$.
$0=\pi(x\cdot\sum_{i=1}^{m}a_i\omega_i)=\sum_{i=1}^{m}\underbrace{\pi(x\cdot a_i)}_{\in\mathcal{O}_K/\mathfrak{p}}\overline{\omega_i}$ und für $i_0$ : $\pi(x\cdot a_{i_0})\neq 0$ $\quad\lightning\ \overline{\omega_1},\dots,\overline{\omega_m}$ Basis

---

„$=$“: Sei nun $p\in\mathbb{Z}$ Primzahl mit $p\mathbb{Z}=\mathfrak{p}\cap\mathbb{Z}$ und $s=[K:\mathbb{Q}]$.
Für $K/\mathbb{Q}$ haben wir das Lemma schon gezeigt:

2. $N(\mathfrak{p})=|\mathcal{O}_K/\mathfrak{p}|=p^f$
1. $N(p\mathcal{O}_K)=|\mathcal{O}_K/p\mathcal{O}_K|=|N_{K/\mathbb{Q}}(p)|=p^s$

Sei $p\cdot\mathcal{O}_K=\mathfrak{p}_1^{e_1}\cdot\dots\cdot\mathfrak{p}_r^{e_r}$ mit $\mathfrak{p}=\mathfrak{p}_1,\mathfrak{p}_2,\dots,\mathfrak{p}_r\subset\mathcal{O}_K$ verschiedene Primideale.

$$\begin{aligned} p^s=N(p\mathcal{O}_K)&=\prod_{i=1}^{r}N(\mathfrak{p}_i)^{e_i}\\ &=\prod_{i=1}^{r}(p^{f_i})^{e_i}=p^{\sum_{i=1}^{r}e_if_i}\\ \Rightarrow\sum_{i=1}^{r}e_if_i&=s \end{aligned}$$

Sei $n_i=\dim_{\mathcal{O}_K/\mathfrak{p}_i}(\mathcal{O}_L/\mathfrak{p}_i\cdot\mathcal{O}_L)$. Zeige: $n_i=n\ \forall i$ (insbesondere $n_1=n$).

$$p^{n\cdot s}=N(\underbrace{p\cdot\mathcal{O}_L}_{=(p\mathcal{O}_K)\mathcal{O}_L})=\prod_{i=1}^{r}N(\mathfrak{p}_i\mathcal{O}_L)^{e_i}=\prod_{i=1}^{r}N(\mathfrak{p}_i)^{n_i\cdot e_i}=\prod_{i=1}^{r}p^{f_in_ie_i}=p^{\sum_{i=1}^{r}f_in_ie_i}$$

Wir wissen also:

$$\left.\begin{array}{c}\sum_{i=1}^{r}f_ie_in_i=n\cdot s\\ \sum_{i=1}^{r}e_if_i=s\\ n_i\leq n\ \forall i\end{array}\right\}\ n_i=n\ \forall i$$

$\Rightarrow\dim_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)=n$

2. $N(\mathfrak{Q})=p^{\dim_{\mathbb{F}_p}(\mathcal{O}_L/\mathfrak{Q})}$ und $N(\mathfrak{p})=p^{\dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})}$
$\dim_{\mathbb{F}_p}(\mathcal{O}_L/\mathfrak{Q})=\dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})\cdot\underbrace{\dim_{(\mathcal{O}_K/\mathfrak{p})}(\mathcal{O}_L/\mathfrak{Q})}_{f(\mathfrak{Q}|\mathfrak{p})}$ (Gradsatz)

∎

**Satz 7.7** Seien $K \subset L$ algebraische Zahlkörper, $n = [L:K]$. Sei $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ Primideal mit

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{Q}_1^{e_1} \cdot \dots \cdot \mathfrak{Q}_r^{e_r} \qquad (\mathfrak{Q}_1, \dots, \mathfrak{Q}_r \subset \mathcal{O}_L \text{ verschiedene Primideale}))$$

Dann gilt die fundamentale Gleichung:

$$\sum_{i=1}^{r} e_i f_i = n \qquad (f_i = f(\mathfrak{Q}_i|\mathfrak{p}))$$

*Beweis:* $N(\mathfrak{p}\mathcal{O}_L) \overset{\text{Lemma (7.6)}}{=} N(\mathfrak{p})^n$ und außerdem gilt:

$$N(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{r} N(\mathfrak{Q}_i)^{e_i} \overset{\text{Lemma (7.6)}}{=} \prod_{i=1}^{r} (N(\mathfrak{p})^{f_i})^{e_i} = N(\mathfrak{p})^{\sum_{i=1}^{r} e_i f_i}$$

∎

---

Frage: Wie bestimmt man die Zerlegung

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{Q}_1^{e_1} \cdot \dots \cdot \mathfrak{Q}_r^{e_r} \ ?$$

Idee: Angenommen $K = \mathbb{Q}$, $L = \mathbb{Q}(\Theta)$ $\mathcal{O}_L = \mathbb{Z}[\Theta]$.
Sei $g \in \mathbb{Z}[X]$ das Minimalpolynom von $\Theta$. Betrachte für eine Primzahl $p \in \mathbb{Z}$:

$$\begin{aligned} \mathbb{Z}[X] &\xrightarrow{\varphi_\Theta} \mathcal{O}_L = \mathbb{Z}[\Theta] \xrightarrow{\pi} \mathcal{O}_L/p\mathcal{O}_L \qquad \text{surjektiv} \\ f &\longmapsto f(\Theta) \end{aligned}$$

$\operatorname{Kern}(\varphi_\Theta) = (g) \subset \mathbb{Z}[X]$
$\operatorname{Kern}(\pi) = p\mathcal{O}_L$
$\rightsquigarrow \operatorname{Kern}(\pi \circ \varphi_\Theta) = \varphi_\Theta^{-1}(p\mathcal{O}_L) = (p,g) \subset \mathbb{Z}[X]$

$$\begin{array}{ccccc} \Rightarrow & \mathcal{O}_L/p\mathcal{O}_L & \overset{\text{Hom.-Satz}}{\cong} & \mathbb{Z}[X]/(p,g) & \overset{\text{Algebra: Lemma 3.3}}{\cong} \mathbb{F}_p[X]/(\overline{g}) \\ & \overset{\text{chin. Restsatz}}{\cong} & & & \cong \\ & (\mathcal{O}_L/\mathfrak{Q}_1^{e_1} \times \dots \times \mathcal{O}_L/\mathfrak{Q}_r^{e_r}) & \cong & \mathbb{F}_p[X]/(\overline{g_1}^{d_1}) \times \dots \times \mathbb{F}_p[X]/(\overline{g_s}^{d_s}) & \end{array}$$

wobei $\overline{g}$ die Reduktion mod $p$ von $g$ ist mit $\overline{g} = \overline{g_1}^{d_1} \cdot \dots \cdot \overline{g_s}^{d_s}$ Faktorisierung in $\mathbb{F}_p[X]$, wobei $\overline{g_1}, \dots, \overline{g_s}$ normiert und irreduzibel sind.
Die Idee suggeriert, dass es eine Verbindung zwischen $\mathfrak{Q}_i$ und $\overline{g_i}$ gibt.
Allgemeiner:

1. Falls $\mathcal{O}_L = \mathcal{O}_K[\Theta]$ ist, werden wir so die Zerlegung vollständig bestimmen können.
2. Falls $\mathcal{O}_L \supsetneq \mathcal{O}_K[\Theta]$ ist, so muss man endlich viele Primideale $\mathfrak{p} \subset \mathcal{O}_K$ aussparen.

---

Fixiere $(0) \neq \mathfrak{p} \subset \mathcal{O}_K$ Primideal. Sei $L = K(\Theta)$. Dies ist keine Einschränkung wegen des Satzes vom primitiven Element.
Sei $g \in \mathcal{O}_K[X]$ das Minimalpolynom von $\Theta$ und $\overline{g} \in (\mathcal{O}_K/\mathfrak{p}[X])$ die Reduktion der Koeffizienten von $g$ mod $\mathfrak{p}$. Weiterhin seien $\overline{g_1}, \dots, \overline{g_r} \in (\mathcal{O}_K/\mathfrak{p})[X]$ normiert und irreduzibel mit:

$$\overline{g} = \overline{g_1}^{e_1} \cdot \dots \cdot \overline{g_r}^{e_r}$$

**Satz 7.8** In dieser Situation nehmen wir an, dass die Primzahl $p \in \mathbb{Z}$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ die Ordnung von $\mathscr{O}_L/\mathscr{O}_K[\Theta]$ nicht teilt.
Es seien $g_1, \dots, g_r \in \mathscr{O}_K[X]$ normiert, so dass $\overline{g_i}$ die Reduktion modulo $\mathfrak{p}$ von $g_i$ ist. Dann gilt:

$$\mathfrak{p}\mathscr{O}_L = \mathfrak{Q}_1^{e_1} \cdot \dots \cdot \mathfrak{Q}_r^{e_r},$$

wobei $\mathfrak{Q}_i = \mathfrak{p}\mathscr{O}_L + g_i(\Theta) \cdot \mathscr{O}_L$ das von $\mathfrak{p}$ und $g_i(\Theta)$ erzeugte Ideal in $\mathscr{O}_L$ ist.
Dabei ist $f(\mathfrak{Q}_i|\mathfrak{p}) = \operatorname{grad}(g_i) = \operatorname{grad}(\overline{g_i})$ der Trägheitsgrad.

**Beispiel** $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathscr{O}_L = \mathbb{Z}[i]$, $g(X) = X^2 + 1$
Wende den Satz an:

1. $p = 2$:
   $\overline{g}(X) = X^2 + 1 = (\underbrace{X+1}_{=\overline{g_1}})^2 \in \mathbb{F}_2[X] \rightsquigarrow e_1 = 2$

   $$\Rightarrow 2\mathbb{Z}[i] = \mathfrak{Q}_1^2 \text{ mit } \mathfrak{Q}_1 = (2, \overline{g_1}(i)) = (2, 1+i) = (1+i)$$

2. $p \equiv 3 \pmod 4$:
   $\overline{g}(X) = X^2 + 1 \pmod p$, $\overline{g}$ ist irreduzibel falls $p \equiv 3 \pmod 4$:

   $\overline{g}$ ist irreduzibel $\iff$ $\overline{g}$ hat keine Nullstellen $\iff$ $-1$ ist quadratischer Nichtrest mod $p$ $\iff$ $\left(\frac{-1}{p}\right) = -1$

   Kurzer Bew/Bemerkung:
   $a \in \mathbb{F}_p^\times$ ist quadratischer Rest mod $p$ (d.h. $\exists\, b \in \mathbb{F}_p^\times$ mit $a = b^2$) $\iff$ $a^{\frac{p-1}{2}} = 1 \in \mathbb{F}_p$
   Beweis: „$\Rightarrow$“
   Sei $a$ quadratischer Rest $\Rightarrow \exists\, b \in \mathbb{F}_p^\times : \ a = b^2$

   $$\Rightarrow a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{(p-1)} \underset{|\mathbb{F}_p^\times| = p-1}{=} 1$$

   „$\Leftarrow$“
   Angenommen $1 = a^{\frac{p-1}{2}}$. $\mathbb{F}_p^\times$ ist zyklisch. Sei $\zeta \in \mathbb{F}_p^\times$ Erzeuger. $\Rightarrow \operatorname{ord}(\zeta) = p-1$.
   Es ist $a = \zeta^x$ für ein $x \in \{0, \dots, p-2\}$.

   $$\Rightarrow 1 = \zeta^{x \cdot \frac{p-1}{2}} \Rightarrow x \text{ gerade}$$

   Wähle $b = \zeta^{\frac{x}{2}} \in \mathbb{F}_p^\times \Rightarrow b^2 = a$ ∎

   Für $a = -1$: $\quad (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{für } p \equiv 1 \pmod 4 \\ -1 & \text{für } p \equiv 3 \pmod 4 \end{cases}$

   Es folgt also: $p \equiv 3 \pmod 4$ bleib prim in $\mathbb{Z}[i]$, d.h. $p\mathbb{Z}[i]$ ist Primideal und $f(p\mathbb{Z}[i]|p) = 2$.
3. $p \equiv 1 \pmod 4$:
   Wir haben gesehen, dass $\overline{g}(X) = X^2 + 1 \in \mathbb{F}_p[X]$ reduzibel ist, d.h. $\exists\, \overline{\alpha} \in \mathbb{F}_p^\times$ mit

   $$\overline{g}(X) = \underbrace{(X + \overline{\alpha})}_{=\overline{g_1}} \cdot \underbrace{(X - \overline{\alpha})}_{=\overline{g_2}}.$$

Für $\alpha \in \mathbb{Z}$ mit $\alpha \equiv \overline{\alpha} \pmod{p}$ ist dann:

$$p\mathbb{Z}[i] = \mathfrak{p}_1 \cdot \mathfrak{p}_2$$

$$\begin{aligned} \mathfrak{p}_1 &= (p, g_1(i)) & p_2 &= (p, g_2(i)) \\ &= (p, i+\alpha) & &= (p, i-\alpha) = (p, \alpha - i) \end{aligned}$$

Übersetzung zur bekannten Zerlegung:
Wir wissen: $p = a^2 + b^2$, $a, b \in \mathbb{Z}$

$$p\mathbb{Z}[i] = (a+bi)(a-bi)$$

ist $\widetilde{b} \in \mathbb{Z}$ mit $b \cdot \widetilde{b} \equiv 1 \pmod{p}$, so ist für $\alpha = a \cdot \widetilde{b} \in \mathbb{Z}$:

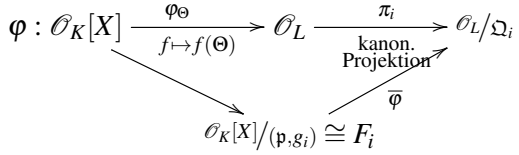
$$\begin{aligned} (X+\alpha)(X-\alpha) &= X^2 - \alpha^2 = X^2 - a^2\widetilde{b}^2 \\ &\equiv X^2 + 1 \pmod{p} \end{aligned}$$

Die letzte Gleichheit folgt, da $a^2 \cdot \widetilde{b}^2 = p \cdot \widetilde{b}^2 - b^2 \cdot \widetilde{b}^2 \equiv -1 \pmod{p}$.
$\Rightarrow \mathfrak{p}_1 = (p, \alpha + i) = (p, a\widetilde{b} + i) = (p, a + bi) = (a + bi) \subset \mathbb{Z}[i]$

*Beweis von Satz (7.8):* Die Aussage folgt aus den folgenden drei Punkten:

1. Für alle $i$ gilt: Entweder $\mathfrak{Q}_i = \mathcal{O}_L$ oder ${}^{\mathcal{O}_L}/_{\mathfrak{Q}_i}$ ist ein Körper mit $|{}^{\mathcal{O}_L}/_{\mathfrak{Q}_i}| = |{}^{\mathcal{O}_K}/_{\mathfrak{p}}|^{f_i}$ Elementen
2. Für $i \neq j$ gilt stets: $\mathfrak{Q}_i + \mathfrak{Q}_j = \mathcal{O}_L$
3. $\mathfrak{p}\mathcal{O}_L \mid \mathfrak{Q}_1^{e_1} \cdot \dots \cdot \mathfrak{Q}_r^{e_r}$

Beweis von 1.:
$F_i := {}^{(\mathcal{O}_K/\mathfrak{p})[x]}/_{(\overline{g_i})}$ ist ein Erweiterungskörper von ${}^{\mathcal{O}_K}/_{\mathfrak{p}}$ vom Grad $f_i := \operatorname{grad}(\overline{g_i}) = \operatorname{grad}(g_i)$.
Betrachte folgendes Diagramm:




$\mathfrak{Q}_i$ ist wie im Theorem definiert und $\varphi$ ist surjektiv, wie wir gleich zeigen werden.
Klar: $(p, g_i) \subset \mathcal{O}_K[X]$ ist im Kern$(\varphi)$ enthalten.

$$\varphi(p \cdot \mathcal{O}_K[X]) = \pi_i(\varphi_\Theta(\mathfrak{p} \cdot \mathcal{O}_K[X])) = \pi_i(\underbrace{\mathfrak{p} \cdot \mathcal{O}_K[\Theta]}_{\subset \mathfrak{p}\cdot\mathcal{O}_L \subset\, \mathfrak{Q}_i}) = \{0\}$$

$$\varphi(g) = \pi_i(\varphi_\Theta(g)) = \pi_i(\underbrace{g_i(\Theta)}_{\in \mathfrak{Q}_i}) = 0$$

Behauptung: $\varphi$ ist auch surjektiv.
$\varphi_\Theta(\mathcal{O}_K[X]) = \mathcal{O}_K[\Theta] \subset \mathcal{O}_L$.
Zeige: $\pi_i(\mathcal{O}_K[\Theta]) = \pi_i(\mathcal{O}_L)$
Zeige dazu: $\mathcal{O}_L = \mathcal{O}_K[\Theta] + \mathfrak{Q}_i$
bzw. sogar: $\mathcal{O}_L = \mathcal{O}_K[\Theta] + p \cdot \mathcal{O}_L$, wobei $p$ so gewählt ist, dass $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.
$p \cdot \mathcal{O}_L \subset \mathfrak{Q}_i$, da $p \in \mathfrak{p} \subset \mathfrak{Q}_i$.
Beweis:
$d := |{}^{\mathcal{O}_L}/_{(\mathcal{O}_K[\Theta] + p\cdot\mathcal{O}_L)}|$

$\overset{(\star)}{\Rightarrow} d \mid |\mathcal{O}_L/\mathcal{O}_K[\Theta]|$ und $d \mid \underbrace{|\mathcal{O}_L/p\cdot\mathcal{O}_L|}_{\substack{=N(p\cdot\mathcal{O}_L)\\=|N_{L/\mathbb{Q}}(p)|\\=p^{[L:\mathbb{Q}]}}} \Rightarrow d = 1$ nach Voraussetzung.

Beweis von $(\star)$:
Betrachte

$$\lambda : \mathcal{O}_L \longrightarrow \mathcal{O}_L/(\mathcal{O}_K[\Theta]+p\cdot\mathcal{O}_L) \qquad \text{kan. Projektion, surj.}$$

mit $\mathcal{O}_K[\Theta] \subset \ker(\lambda)$ (bzw. $p\cdot\mathcal{O}_L \subset \ker(\lambda)$).

$$\overset{\text{Hom.-Satz}}{\Rightarrow} \exists!\ \overline{\lambda} : \underbrace{\mathcal{O}_L/\mathcal{O}_K[\Theta]}_{=:G} \longrightarrow \mathcal{O}_L/(\mathcal{O}_K[\Theta]+p\cdot\mathcal{O}_L) \cong G/H \qquad \text{surj.}$$

mit $H := \ker(\overline{\lambda})$.
$\Rightarrow |G| = |H|\cdot[G:H] \Rightarrow \underbrace{|G/H|}_{=[G:H]} \mid |G|$

---

Für $p\mathcal{O}_L$ genauso.

---

Es folgt:

$$\pi_i(\mathcal{O}_K[\Theta]) \underset{\pi_i(\mathfrak{Q}_i)=0}{=} \pi_i(\mathcal{O}_K[\Theta]+\mathfrak{Q}_i) = \pi_i(\mathcal{O}_L)$$

$\Rightarrow \varphi$ ist surjektiv.

---

Außerdem ist die Abbildung:

$$\Psi : \mathcal{O}_K[X] \underset{\substack{\text{Red. der}\\\text{Koeffizienten}\\\text{mod } \mathfrak{p}}}{\longrightarrow} (\mathcal{O}_K/\mathfrak{p})[X] \longrightarrow (\mathcal{O}_K/\mathfrak{p})[X]/(\overline{g_i}) = F_i$$

surjektiv mit $\ker(\Psi) = (\mathfrak{p}, g_i)$ Übung Q30

$$\overset{\text{Hom.-Satz}}{\Rightarrow} F_i \cong \mathcal{O}_K[X]/(\mathfrak{p},g_i)$$

---

$\Rightarrow$ Entweder $\mathcal{O}_L/\mathfrak{Q}_i = \{0\} \Leftrightarrow \mathfrak{Q}_i = \mathcal{O}_L$ oder $\mathcal{O}_L/\mathfrak{Q}_i \cong F_i$,
da $\overline{\varphi} : F_i \to \mathcal{O}_L/\mathfrak{Q}_i$ ist injektiv, falls $\mathcal{O}_L/\mathfrak{Q}_i \neq \{0\}$, da $F_i$ Körper ist.

Beweis von 2.:

$$\mathfrak{Q}_i = \mathfrak{p}\mathcal{O}_L + g_i(\Theta)\cdot\mathcal{O}_L$$

Für $i \neq j$ sind $\overline{g_i}$ und $\overline{g_j}$ teilerfremd. Also existieren $\overline{h_i}$ und $\overline{h_j} \in (\mathcal{O}_K/\mathfrak{p})[X]$ mit:

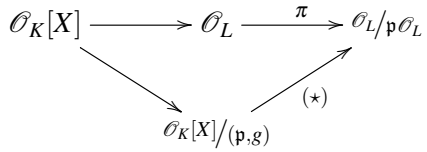
$$\overline{h_i}\cdot\overline{g_i} + \overline{h_j}\cdot\overline{g_j} = 1$$

Sind $h_i, h_j \in \mathcal{O}_K[X]$ mit $h_i \equiv \overline{h_i} \pmod{\mathfrak{p}}$ und $h_j \equiv \overline{h_j} \pmod{\mathfrak{p}}$, so folgt:

$$\begin{aligned}
&h_i\cdot g_i + h_j\cdot g_j \equiv 1 \pmod{\mathfrak{p}}\\
\Rightarrow &h_i\cdot g_i + h_j\cdot g_j - 1 \in \mathfrak{p}\cdot\mathcal{O}_K[X]\\
\Rightarrow &h_i(\Theta)\cdot g_i(\Theta) + h_j(\Theta)\cdot g_j(\Theta) - 1 =: \alpha \in \mathfrak{p}\cdot\mathcal{O}_L\\
\Rightarrow &1 = \underbrace{\underbrace{-\alpha}_{\in\mathfrak{p}\mathcal{O}_L} + \underbrace{h_i(\Theta)\cdot g_i(\Theta)}_{\in g_i(\Theta)\cdot\mathcal{O}_L}}_{\in\mathfrak{Q}_i} + \underbrace{h_j(\Theta)\cdot g_j(\Theta)}_{\substack{\in g_j(\Theta)\cdot\mathcal{O}_L\\\subset\mathfrak{Q}_j}}
\end{aligned}$$

$\Rightarrow 1 \in \mathfrak{Q}_i + \mathfrak{Q}_j \Rightarrow \mathfrak{Q}_i + \mathfrak{Q}_j = \mathcal{O}_L$

Beweis von 3.:
Wir wollen also zeigen, dass $\mathfrak{Q}_1^{e_1} \cdot \dots \cdot \mathfrak{Q}_r^{e_r} \subset \mathfrak{p}\mathcal{O}_L$ ist.
Klar: $\mathfrak{Q}_1^{e_1} \cdot \dots \cdot \mathfrak{Q}_r^{e_r} \subset (\mathfrak{p}, g_1(\Theta)^{e_1} \cdot \dots \cdot g_r(\Theta)^{e_r})$ (Ausmultiplizieren der Elemente)
Zeige also: $(\mathfrak{p}, g_1(\Theta)^{e_1} \cdot \dots \cdot g_r(\Theta)^{e_r}) \subset \mathfrak{p}\mathcal{O}_L$
Betrachte dazu wieder:




Dabei: $\mathcal{O}_K[X]/(\mathfrak{p},g) \cong (\mathcal{O}_K/\mathfrak{p})[X]/(\overline{g})$
Das Diagramm ist kommutativ, also:

$$\pi(g_1(\Theta)^{e_1} \cdot \dots \cdot g_r(\Theta)^{e_r}) = \underbrace{\overline{g_1}^{e_1}(\Theta) \cdot \dots \cdot \overline{g_r}^{e_r}(\Theta)}_{\overline{g}(\Theta)} = 0 \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$$

$(\star)$ kann als Einsetzungshomomorphismus $(\mathcal{O}_K/\mathfrak{p})[X]/(\overline{g}) \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ angesehen werden.

---

Beweis des Satzes aus 1.-3.:
1.: Œ: $\mathfrak{Q}_1, \dots, \mathfrak{Q}_s \neq \mathcal{O}_L$ Primideale mit:

$$|\mathcal{O}_L/\mathfrak{Q}_i| = |\mathcal{O}_K/\mathfrak{p}|^{f_i}, \qquad f_i = \operatorname{grad}(g_i) = \operatorname{grad}(\overline{g_i})$$

und $\mathfrak{Q}_{s+1}, \dots, \mathfrak{Q}_r = \mathcal{O}_L$.
Für $\mathfrak{Q}_1, \dots, \mathfrak{Q}_s$ gilt: $\mathfrak{Q}_i \mid \mathfrak{p}\mathcal{O}_L$ (per Definition)

$$f(\mathfrak{Q}_i|\mathfrak{p}) = f_i$$

Wegen 2. sind die $\mathfrak{Q}_i$ verschieden und wegen 3. gilt:

$$\mathfrak{p}\mathcal{O}_L \mid \mathfrak{Q}_1^{e_1 \cdot \dots \cdot \mathfrak{Q}_s^{e_s}}$$

$\Rightarrow$ Die Primidealzerlegung von $\mathfrak{p}\mathcal{O}_L$ ist von der Form:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{Q}_1^{d_1} \cdot \dots \cdot \mathfrak{Q}_s^{d_s} \qquad d_i \leq e_i$$

$$\overset{\text{Satz (7.7)}}{\Rightarrow} \sum_{i=1}^{s} d_i f_i = n = [L:K] = grad(g) = grad(\overline{g})$$

$$\overset{(\overline{g} = \overline{g_1}^{e_1} \cdot \dots \cdot \overline{g_r}^{e_r})}{=} \sum_{i=1}^{r} e_i f_i$$

$$\Rightarrow s = r \text{ und } d_i = e_i$$

■

---

■ **Bemerkung** Für die Übungen und weiterreichende Informationen empfehlen wir folgende Websites:

- LMFDB.ORG - Auf dieser Website sind zum Beispiel viele Informationen zu Zahlkörpern zusammengefasst.

- SAGEMATH.ORG - Sagemath ist eine Mathe-Software, die unter anderem viele Operationen im für uns relevanten Bereich der Zahlkörper umfasst.
- COCALC.COM - Cocalc ermöglicht es, online mit mehreren Personen zusammenzuarbeiten, z.B. in einem LaTeX-Dokument oder auch an einem Sagemath-Projekt.

# 8. Verzweigungstheorie

In diesem Kapitel ist $L/K$ eine Erweiterung algebraischer Zahlkörper. Nehme zusätzlich an, dass $L/K$ Galoiserweiterung ist. $\rightsquigarrow$ Das Zerlegungsverhalten von Primidealen wird „einfacher“.

**Satz 8.1** $G = \mathrm{Gal}(L/K)$. Sei $\mathfrak{p} \subset \mathcal{O}_K$ Primideal. Dann operiert $G$ transitiv auf der Menge $M := \{\mathfrak{Q} \subset \mathcal{O}_L \text{ Primideal} \mid \mathfrak{Q} \mid \mathfrak{p} \cdot \mathcal{O}_L\}$ der Primideale über $\mathfrak{p}$.

Zur Erinnerung:
transitiv bedeutet: Zu $\mathfrak{Q}, \mathfrak{Q}' \subset \mathcal{O}_L$ Primideale über $\mathfrak{p}$ gibt es ein $\sigma \in G$ mit $\sigma(\mathfrak{Q}) = \mathfrak{Q}'$
bzw.: Ist $\mathfrak{Q} \subset \mathcal{O}_L$ Primideal über $\mathfrak{p}$, so ist $M = \{\sigma(\mathfrak{Q}) \mid \sigma \in G\}$

---

*Beweis von Satz (8.1):*
Sei $\mathfrak{Q} \subset \mathcal{O}_L$ prim mit $\mathfrak{Q} \mid \mathfrak{p}\mathcal{O}_L$ und sei $\sigma \in G$. Dann:

- $\sigma(\mathfrak{Q}) \subset \mathcal{O}_L$ ist Primideal in $\mathcal{O}_L$ ($\subset \mathcal{O}_L$, da alle $\sigma(\alpha)$ Nullstellen des Minimalpolynoms sind)
- $\sigma(\mathfrak{p}) = \mathfrak{p}$
  $\Rightarrow \mathfrak{p} \subset \sigma(\mathfrak{Q}) \Rightarrow \sigma(\mathfrak{Q}) \mid \mathfrak{p}\mathcal{O}_L$

$\Rightarrow G$ operiert auf $M$.
Transitiv: Seien $\mathfrak{Q}, \mathfrak{Q}' \in M$. Angenommen es gelte für alle $\sigma \in G : \sigma(\mathfrak{Q}) \neq \mathfrak{Q}'$.
Nach dem chin. Restsatz gilt dann: $\exists x \in \mathcal{O}_L$ mit $x \equiv 0 \pmod{\mathfrak{Q}'}$ ($\Leftrightarrow x \in \mathfrak{Q}'$) und
$x \equiv 1 \pmod{\sigma(\mathfrak{Q})} \forall \sigma \in G$.

$$\left.\begin{aligned} \Rightarrow N_{L/K}(x) &= \prod_{\sigma \in G} \sigma(x) \in \mathcal{O}_K \\ &= x \cdot \prod_{\substack{\sigma \in G \\ \sigma \neq \mathrm{id}}} \sigma(x) \in \mathfrak{Q}' \end{aligned}\right\} N_{L/K} \in \mathcal{O}_K \cap \mathfrak{Q}' = \mathfrak{p} \subset \mathcal{O}_K.$$

Aber: $\forall \sigma \in G : x \notin \sigma(\mathfrak{Q}) \Rightarrow \sigma^{-1}(x) \notin \mathfrak{Q}$

$$\Rightarrow N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \overset{G = \{\sigma^{-1} \mid \sigma \in G\}}{=} \prod_{\sigma \in G} \sigma^{-1}(x) \notin \mathfrak{Q} \supset \mathfrak{p} \qquad \lightning\, N_{L/K}(x) \in \mathfrak{p}$$

∎

**Korollar 8.2** In dieser Situation gilt für alle $\mathfrak{Q}, \mathfrak{Q}' \subset \mathscr{O}_L$ über $\mathfrak{p}$:

$$e(\mathfrak{Q}|\mathfrak{p}) = e(\mathfrak{Q}'|\mathfrak{p})$$
$$f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}'|\mathfrak{p})$$

d.h. alle Verzweigungsindizes und Trägheitsgrade sind gleich.

*Beweis:* Nach Satz (8.1) existiert $\sigma \in G$ mit $\sigma(\mathfrak{Q}) = \mathfrak{Q}'$.
Also: $\mathfrak{Q}^e \mid \mathfrak{p}\mathscr{O}_L \Rightarrow \sigma(\mathfrak{Q}^e) = (\mathfrak{Q}')^e \mid \mathfrak{p}\mathscr{O}_L = \sigma(\mathfrak{p}\mathscr{O}_L)$

$$\Rightarrow e(\mathfrak{Q}|\mathfrak{p}) \leq e(\mathfrak{Q}'|\mathfrak{p})$$

genauso mit $\sigma^{-1}$: $e(\mathfrak{Q}'|\mathfrak{p}) \leq e(\mathfrak{Q}|\mathfrak{p}) \Rightarrow$ Gleichheit
Für die Trägheitsgrade:

$$\mathscr{O}_L \xrightarrow[\sigma(\mathfrak{Q})=\mathfrak{Q}']{\sigma} \mathscr{O}_L \xrightarrow{\pi} \mathscr{O}_L/\mathfrak{Q}'$$

ist surjektiv mit $\ker = \sigma^{-1}(\mathfrak{Q}') = \mathfrak{Q}$
$\rightsquigarrow \mathscr{O}_L/\mathfrak{Q} \cong \mathscr{O}_L/\mathfrak{Q}'$

$$\Rightarrow f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}'|\mathfrak{p})$$

∎

---

Also: Ist $L/K$ Galoiserweiterung, so ist $\mathfrak{p}\mathscr{O}_L = (\mathfrak{Q}_1 \cdot \dots \cdot \mathfrak{Q}_r)^e$ mit identischen Trägheitsgraden $f := f(\mathfrak{Q}_i|\mathfrak{p})$. Damit wird unsere Fundamentalgleichung zu:

$$[L:K] = n = r \cdot e \cdot f$$

1. Anwendung: Welche Primideale sind $\underbrace{\textit{verzweigt}}_{\text{mind. ein } e_i>1}$ ?

In der Übung gesehen: $K = \mathbb{Q}(\sqrt{d_K})$ wobei $d_K$ Diskriminante von $K$ ist so gilt:

$$p \text{ verzweigt} \iff p \mid d_K$$

**Satz 8.3** Sei $K$ algebraischer Zahlkörper und $p \in \mathbb{Z}$ Primzahl. Falls $p$ in $\mathscr{O}_K$ verzweigt ist, so gilt: $p \mid d_K$.

*Beweis:* Sei $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \cdot \dots \cdot \mathfrak{p}_r^{e_r}$ die Primidealzerlegung von $p$ in $\mathscr{O}_K$.
Sei $\mathfrak{p} = \mathfrak{p}_1 \subset \mathscr{O}_K$ ein Primideal über $p$ mit $e_1 = e(\mathfrak{p}|p\mathbb{Z}) > 1$
$\Rightarrow p\mathscr{O}_K = \mathfrak{p} \cdot \mathfrak{a}$ mit $\mathfrak{a} = \mathfrak{p}_1^{e_1-1} \cdot \mathfrak{p}_2^{e_2} \cdot \dots \cdot \mathfrak{p}_r^{e_r}$
$\Rightarrow p\mathscr{O}_K \subsetneq \mathfrak{a}$ (Eindeutigkeit der Primidealzerlegung)
Sei $\alpha \in \mathfrak{a} \setminus p\mathscr{O}_K$.
Sei weiterhin $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$ und $\alpha_1, \dots, \alpha_n \in \mathscr{O}_K$ eine Ganzheitsbasis.
Es existieren $m_1, \dots, m_n \in \mathbb{Z}$ mit

$$\alpha = m_1\alpha_1 + \dots + m_n\alpha_n$$

da $\alpha \notin p\mathscr{O}_K$, ex. $i \in \{1, \dots, n\}$ mit $p \nmid m_i$.
Œ$p \nmid m_1$

Aber: $\mathfrak{p} = \mathfrak{p}_1 \mid (\alpha), \ldots, \mathfrak{p}_r \mid (\alpha), \qquad$ da $\mathfrak{a} \mid (\alpha)$
Wir rechnen aus:

$$
\begin{aligned}
d_K = d(\alpha_1, \ldots, \alpha_n) &= [\det(\sigma_i(\alpha_j))]^2 \\
&= m_1^{-2} \cdot \left[ \det \begin{pmatrix} \sigma_1(m_1 \cdot \alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(m_1 \cdot \alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} \right]^2 \\
&\overset{\substack{\text{elementare} \\ = \\ \text{Spalten-} \\ \text{transformationen}}}{} m_1^{-2} \cdot \left[ \det \begin{pmatrix} \sigma_1(\alpha) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} \right]^2 \\
&= m_1^{-2} \cdot d(\alpha, \alpha_2, \ldots, \alpha_n) \\
\Rightarrow & d(\alpha, \alpha_2, \ldots, \alpha_n) = m_1^2 \cdot d_K
\end{aligned}
$$

Sei $L/K$ normale Hülle von $K/\mathbb{Q} \Rightarrow L/\mathbb{Q}$ Galoiserweiterung.
Seien $\sigma_1', \ldots, \sigma_n' \in \mathrm{Gal}(L/\mathbb{Q})$ Fortsetzungen von $\sigma_1, \ldots, \sigma_n$ auf $L$.
Sei weiter $\mathfrak{Q} \subset \mathcal{O}_L$ ein Primideal über $p$. Dann gilt:

1. $\alpha \in \mathfrak{Q}$, denn $\mathfrak{Q} \cap \mathcal{O}_K = \mathfrak{p}_i$ für ein $i \in \{1, \ldots, r\}$ und $\alpha \in \mathfrak{p}_i \forall i$
2. $\forall \sigma \in \mathrm{Gal}(L/\mathbb{Q}): \ \sigma(\alpha) \in \mathfrak{Q}$, denn: $\sigma^{-1}(\mathfrak{Q})$ ist Primideal über $p$ und wie in 1. folgt $\alpha \in \sigma^{-1}(\mathfrak{Q})$.

Damit folgt insbesondere:

$$\sigma_1'(\alpha) = \sigma_1(\alpha), \ldots, \sigma_n'(\alpha) = \sigma_n(\alpha) \in \mathfrak{Q}$$

$\Rightarrow d(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{Q}$
(Folgt mit einer Laplace-Entwicklung der Determinante nach der 1. Spalte. Jeder Summand ist von der Form: $\underbrace{\sigma_i(\alpha)}_{\in \mathbb{Q}} \cdot \underbrace{a_i}_{\in \mathcal{O}_L} \in \mathfrak{Q}$)
Außerdem ist $d(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$

$$
\begin{aligned}
&\Rightarrow d(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{Q} \cap \mathbb{Z} = p\mathbb{Z} \\
&\Rightarrow p \mid d(\alpha, \alpha_2, \ldots, \alpha_n) = m_1^2 \cdot d_K \\
p \nmid m_1 &\Rightarrow p \mid d_K
\end{aligned}
$$

■

■ **Bemerkung** Die Umkehrung des Satzes gilt auch, wird aber hier nicht bewiesen.

**Korollar 8.4** Es gibt nur endlich viele Primzahlen $p \in \mathbb{Z}$, die in $K$ verzweigt sind.

**Korollar 8.5** Ist $L/K$ eine Erweiterung algebraischer Zahlkörper, so gibt es nur endlich viele Primideale $\mathfrak{p} \subset \mathcal{O}_K$, die in $L$ verzweigt sind.

*Beweis:* Übung. ■

## 8.1 Mehr zur Galoistheorie/Verzweigungstheorie

Im Folgenden:

- $L/K$ Galoiserweiterung algebraischer Zahlkörper
- $G = \mathrm{Gal}(L/K)$ und $n = [L:K]$
- Sei $\mathfrak{p} \subset \mathcal{O}_K$ Primideal, $\mathfrak{p} \neq (0)$ mit $\mathfrak{p}\mathcal{O}_L = (\mathfrak{Q}_1 \cdot \dots \cdot \mathfrak{Q}_r)^e$, $f = f(\mathfrak{Q}_i|\mathfrak{p})$

**Definition 8.6** Für jedes Primideal $\mathfrak{Q} \subset \mathcal{O}_L$ über $\mathfrak{p}$ definieren wir:

$$G_{\mathfrak{Q}} := \{\sigma \in G \mid \sigma(\mathfrak{Q}) = \mathfrak{Q}\} \qquad \text{(Untergruppe)}$$

heißt *Zerlegungsgruppe* von $\mathfrak{Q}$ über $K$.
Der zugehörige Fixkörper

$$Z_{\mathfrak{Q}} := \{x \in L \mid \sigma(x) = x \;\forall\; \sigma \in G_{\mathfrak{Q}}\}$$

heißt *Zerlegungskörper* von $\mathfrak{Q}$ über $K$.

Erinnerung:

**Satz — Hauptsatz der Galoistheorie.**

$$\left\{\begin{smallmatrix}\text{Zwischenkörper}\\ K\subset Z\subset L\end{smallmatrix}\right\} \longleftrightarrow \left\{\begin{smallmatrix}U\subset G\\ \text{Untergruppen}\end{smallmatrix}\right\}$$
$$L^U = \{x \in L \mid \sigma(x) = x \;\forall \sigma \in U\} \longmapsto U$$
$$Z \longmapsto \mathrm{Gal}(L/Z)$$

Dabei sind die beiden Abbildungen inklusionsumkehrend und zueinander invers.
(Außerdem: $Z = L^U$ ist normal über $K \iff U \subset G$ Normalteiler)

■ **Bemerkung 8.7**

1. $\mathfrak{p}\mathcal{O}_L = \left[\prod_{\sigma \in G/G_{\mathfrak{Q}}} \sigma(\mathfrak{Q})\right]^e$ für ein festes (und beliebiges) $\mathfrak{Q} \subset \mathcal{O}_L$ mit $\mathfrak{Q} \mid \mathfrak{p}$.
   Also gilt auch $r = [G : G_{\mathfrak{Q}}]$.
2. Es gilt:
$$G_{\mathfrak{Q}} = \{\mathrm{id}\} \iff Z_{\mathfrak{Q}} = L$$
$$\iff p \text{ ist } \textit{voll zerlegt} \text{ in } L$$
   voll zerlegt: $r = n$ $(p\mathcal{O}_L = \mathfrak{Q}_1 \cdot \dots \cdot \mathfrak{Q}_n)$, $(e \cdot f \cdot r = n \Rightarrow e = f = 1)$
   Genauso:
$$G_{\mathfrak{Q}} = G \iff Z_{\mathfrak{Q}} = K$$
$$\iff p \text{ ist } \textit{unzerlegt} \text{ in } L$$
   unzerlegt: $r = 1$
3. Für $\sigma \in G$ ist:
$$G_{\sigma(\mathfrak{Q})} = \sigma \cdot G_{\mathfrak{Q}} \cdot \sigma^{-1}$$

---

*Beweis:*

1. generell: $G$ operiert transitiv auf $X$ ($X$ endlich)
$$\Rightarrow X = \{\sigma(x) \mid \sigma \in G/G_x\} = \{\sigma_1(x), \dots, \sigma_r(x)\} \qquad \text{für ein bel. (aber festes) } x \in X$$

und $\sigma_1, \dots, \sigma_r \in G$ Repräsentanten von $G/G_x$.
Denn: $G$ operiert transitiv $\Rightarrow$ ist $x \in X$, so gilt:

$$X = Gx = \{\sigma(x) \mid \sigma \in G\}.$$

Dann ist für $\sigma, \tau \in G$:

$$\begin{aligned} &\sigma(x) = \tau(x) \\ \Leftrightarrow &\tau^{-1} \circ \sigma(x) = x \\ \Leftrightarrow &\tau^{-1} \circ \sigma \in G_x \\ \Leftrightarrow &[\sigma] = [\tau] \in G/G_x \\ \Leftrightarrow &\tau G_x = \sigma G_x \end{aligned}$$

mit $G_x = \{\sigma \in G \mid \sigma(x) = x\} \subset G$ Untergruppe

3. Auch wieder generell bei Gruppenoperationen:

$$(\sigma \circ \underbrace{\tau}_{\in G_{\mathfrak{Q}}} \circ \sigma^{-1})(\sigma(\mathfrak{Q})) = \sigma(\tau(\mathfrak{Q})) = \sigma(\mathfrak{Q})$$

$$\Rightarrow \sigma \circ \tau \circ \sigma^{-1} \in G_{\sigma(\mathfrak{Q})}$$

Sei $\tau \in G_{\sigma(\mathfrak{Q})} \Rightarrow (\sigma^{-1} \circ \tau \circ \sigma)(\mathfrak{Q}) = \sigma^{-1}(\underbrace{\tau(\sigma(\mathfrak{Q}))}_{=\sigma(\mathfrak{Q})}) = \mathfrak{Q}$

$$\Rightarrow \sigma^{-1} \circ \tau \circ \sigma \in G_{\mathfrak{Q}} \Rightarrow \tau \in \sigma \cdot G_{\mathfrak{Q}} \cdot \sigma^{-1}$$

■

---

**Satz 8.8** Sei $\mathfrak{Q}_Z = \mathfrak{Q} \cap Z_{\mathfrak{Q}}$ das unter $\mathfrak{Q}$ liegende Primideal in $Z_{\mathfrak{Q}}$ $(\subset \mathscr{O}_{Z_{\mathfrak{Q}}})$.
Dann gilt:

1. $\mathfrak{Q}_Z$ ist unzerlegt in $L$
2. $e(\mathfrak{Q}|\mathfrak{Q}_Z) = e(\mathfrak{Q}|\mathfrak{p}), \qquad f(\mathfrak{Q}|\mathfrak{Q}_Z) = f(\mathfrak{Q}|\mathfrak{p})$

   $(\Rightarrow \mathfrak{Q}_Z \mathscr{O}_L = \mathfrak{Q}^e)$
3. $e(\mathfrak{Q}_Z|\mathfrak{p}) = f(\mathfrak{Q}_Z|\mathfrak{p}) = 1$

*Beweis:* 1.:
*Hauptsatz der Galoistheorie*:

$$G_{\mathfrak{Q}} = \mathrm{Gal}(L/Z_{\mathfrak{Q}})$$

$\Rightarrow$ Menge der Primideale über $\mathfrak{Q}_Z = \{\underbrace{\sigma(\mathfrak{Q})}_{=\mathfrak{Q}} \mid \sigma \in G_{\mathfrak{Q}}\} = \{\mathfrak{Q}\}$

2. und 3.:
Es gilt: $|G| = [L:K] = n = \underset{=e(\mathfrak{Q}|\mathfrak{p})}{e} \cdot \underset{=f(\mathfrak{Q}|\mathfrak{p})}{f} \cdot \underset{\substack{=|G/G_{\mathfrak{Q}}| \\ =[G:G_{\mathfrak{Q}}]}}{r}$

$$\Rightarrow e \cdot f = \frac{n}{r} = \frac{|G|}{[G:G_{\mathfrak{Q}}]} = |G_{\mathfrak{Q}}| \qquad (\star)$$

Sei $\mathfrak{p}\cdot\mathcal{O}_{Z_\mathfrak{Q}} = (\mathfrak{Q}_Z)^{e''}\cdot\ldots$ (weitere Primidealfaktoren)
$\mathfrak{Q}_Z\cdot\mathcal{O}_L = \mathfrak{Q}^{e'}$

$$\Rightarrow \mathfrak{p}\cdot\mathcal{O}_L = \mathfrak{Q}_Z^{e'\cdot e''}\cdot\ldots \text{ (weitere Primidealfaktoren)}$$
$$\Rightarrow e = e(\mathfrak{Q}|\mathfrak{p}) = e'\cdot e''$$
$$e'' = e(\mathfrak{Q}_Z|\mathfrak{p}), \qquad e' = e(\mathfrak{Q}|\mathfrak{Q}_Z)$$

Entsprechend gilt: $f = f(\mathfrak{Q}|\mathfrak{p}) = f'\cdot f''$

$$\overset{\text{Satz (7.7)}}{\Rightarrow} \quad \left.\begin{aligned}[L:Z_\mathfrak{Q}] &= e'\cdot f'\cdot 1\\ &= |G_\mathfrak{Q}| \overset{(\star)}{=} e\cdot f\end{aligned}\right\} \begin{array}{c}\text{Da } e'|e \text{ und}\\ f'|f \text{ folgt:}\\ e'=e \text{ und } f'=f\end{array}$$

$\Rightarrow e'' = f'' = 1$ ∎

---

∎ **Bemerkung** Sei $\sigma\in G_\mathfrak{Q}$. Dann induziert $\sigma$ einen Automorphismus:

$$\overline{\sigma} : \mathcal{O}_L/\mathfrak{Q} \longrightarrow \mathcal{O}_L/\mathfrak{Q}$$
$$x+\mathfrak{Q} \longmapsto \sigma(x)+\mathfrak{Q}$$

---

*Beweis:* Übung. ∎

---

**Notation.** *Ist $K$ in algebraischer Zahlkörper und $(0)\neq\mathfrak{p}\subset\mathcal{O}_K$ ein Primideal, so schreiben wir*

$$\kappa(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$$

*für den Restklassenkörper modulo $\mathfrak{p}$.*

**Satz 8.9** Die Erweiterung $\kappa(\mathfrak{Q})/\kappa(\mathfrak{p})$ ist normal (und damit Galoiserweiterung) und der Homomorphismus

$$G_\mathfrak{Q} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{p}))$$
$$\sigma \longmapsto \overline{\sigma}$$

ist surjektiv.

*Beweis:* normal(+separabel) folgen automatisch, da es sich um eine endliche Körpererweiterung endlicher Körper handelt.
Da separabel: Satz vom primitiven Element: Es gibt ein $\overline{\Theta}\in\kappa(\mathfrak{Q})$ mit

$$\kappa(\mathfrak{Q}) = \kappa(\mathfrak{p})(\overline{\Theta})$$

Sei $\overline{g}\in\kappa(\mathfrak{p})[X]$ das Minimalpolynom von $\overline{\Theta}$ über $\kappa(\mathfrak{p})$, sei $\Theta\in\mathcal{O}_L$ mit $\Theta\equiv\overline{\Theta} \pmod{\mathfrak{Q}}$ und sei $f\in\mathcal{O}_K[X]$ das Minimalpolynom von $\Theta$ über $K$.
Sei weiterhin $\Psi\in\mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{p}))$. Zu zeigen ist: Es gibt ein $\sigma\in G_\mathfrak{Q}$ mit $\overline{\sigma}=\Psi$.
$\Rightarrow \Psi(\overline{\Theta})$ ist Nullstelle von $\overline{g}$.
$\Rightarrow \Psi(\overline{\Theta})$ ist Nullstelle von $\overline{f} := f \mod \mathfrak{p}$.
$\Rightarrow$ Es gibt ein $\Theta'\in\mathcal{O}_K$ mit $f(\Theta')=0$ und $\Theta'\equiv\Psi(\overline{\Theta}) \pmod{\mathfrak{Q}}$.

Definiere: $\widetilde{\sigma}(\Theta) := \Theta'$, dies definiert $\widetilde{\sigma} : K(\Theta) \to L$ eindeutig.
Ist $\sigma$ irgendeine Fortsetzung auf ganz $L$, so erfüllt diese:

$$\begin{aligned} &\overline{\sigma}(\overline{\Theta}) = \Psi(\overline{\Theta}) \\ \underset{\kappa(\mathfrak{O})=\kappa(\mathfrak{p})(\overline{\Theta})}{\Rightarrow} \quad &\overline{\sigma} = \Psi \end{aligned}$$

∎

---

**Definition 8.10** Der Kern $I_{\mathfrak{O}} \subset G_{\mathfrak{O}}$ des Homomorphismus

$$\begin{aligned} G_{\mathfrak{O}} &\longrightarrow \mathrm{Gal}(\kappa(\mathfrak{O})/\kappa(\mathfrak{p})) \\ \sigma &\longmapsto \overline{\sigma} \end{aligned}$$

heißt *Trägheitsgruppe* von $\mathfrak{O}$ über $K$.
Der Fixkörper $T_{\mathfrak{O}} := \{x \in L \mid \sigma(x) = x \; \forall \sigma \in I_{\mathfrak{O}}\}$ heißt *Trägheitskörper* von $\mathfrak{O}$ über $K$.

Wir erhalten eine kurze exakte Sequenz:

$$1 \longrightarrow I_{\mathfrak{O}} \longrightarrow G_{\mathfrak{O}} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{O})/\kappa(\mathfrak{p})) \longrightarrow 1 \qquad (\star)$$

und entsprechend eine Körperkette

$$K \subset Z_{\mathfrak{O}} \subset T_{\mathfrak{O}} \subset L$$

(in dieser Reihenfolge, da der Isomorphismus inklusionsumkehrend ist nach Hauptsatz der Galoistheorie).

**Satz 8.11** Die Erweiterung $T_{\mathfrak{O}}/Z_{\mathfrak{O}}$ ist normal (und somit Galoiserweiterung) und es gilt:

1. $\mathrm{Gal}(T_{\mathfrak{O}}/Z_{\mathfrak{O}}) \cong \mathrm{Gal}(\kappa(\mathfrak{O})/\kappa(\mathfrak{p}))$; $\quad \mathrm{Gal}(L/T_{\mathfrak{O}}) = I_{\mathfrak{O}}$
2. $|I_{\mathfrak{O}}| = [L : T_{\mathfrak{O}}] = e(\mathfrak{O}|\mathfrak{p})$; $\quad [G_{\mathfrak{O}} : I_{\mathfrak{O}}] = [T_{\mathfrak{O}} : Z_{\mathfrak{O}}] = f(\mathfrak{O}|\mathfrak{p})$

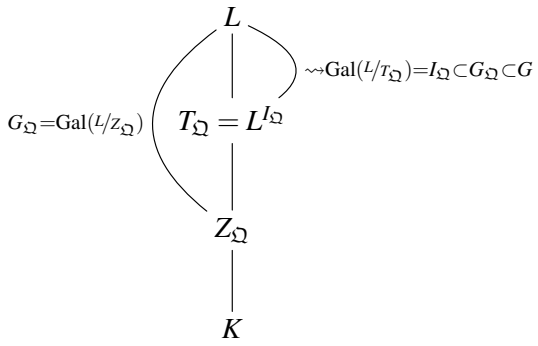
Sei $\mathfrak{O}_T := T_{\mathfrak{O}} \cap \mathfrak{O}$ das Primideal von $T_{\mathfrak{O}}$ unter $\mathfrak{O}$. Dann gilt:

3. $e(\mathfrak{O}|\mathfrak{O}_T) = e(\mathfrak{O}|\mathfrak{p})$; $\quad f(\mathfrak{O}|\mathfrak{O}_T) = 1$
4. $e(\mathfrak{O}_T|\mathfrak{O}_Z) = 1$; $\quad f(\mathfrak{O}_T|\mathfrak{O}_Z) = f(\mathfrak{O}|\mathfrak{p})$

Zusammenfassung: Für $\mathfrak{p}\mathcal{O}_L = (\mathfrak{Q}_1 \cdot \dots \cdot \mathfrak{Q}_r)^e = \Big(\prod_{\sigma \in G/G_{\mathfrak{Q}}} \sigma(\mathfrak{Q})\Big)^e$:

| Grad der Erweiterung | | Verzweigungsindizes | Trägheitsgrade |
|---|---|---|---|
| $e(\mathfrak{Q}\|\mathfrak{p}) = e$ | $L$ — $\mathfrak{Q}$ | $e$ | 1 |
| $f(\mathfrak{Q}\|\mathfrak{p}) = f$ | $T_{\mathfrak{Q}}$ — $\mathfrak{Q}_T$ | 1 | $f$ |
| Anzahl der Faktoren $= r$ | $Z_{\mathfrak{Q}}$ — $\mathfrak{Q}_Z$ | 1 | 1 |
| | $K$ — $\mathfrak{p}$ | | |

*Beweis von Satz (8.11):*




$\rightsquigarrow {}^{T_{\mathfrak{Q}}}/_{Z_{\mathfrak{Q}}}$ normal $\overset{\text{Hauptsatz der Galoistheorie}}{\Longleftrightarrow} I_{\mathfrak{Q}} \subset G_{\mathfrak{Q}}$ Normalteiler.
Letzteres gilt, da $I_{\mathfrak{Q}}$ Kern eines Homomorphismus ist.
1.
fast erledigt. Hauptsatz der Galoistheorie:

$$\mathrm{Gal}({}^{T_{\mathfrak{Q}}}/_{Z_{\mathfrak{Q}}}) \cong {}^{G_{\mathfrak{Q}}}/_{I_{\mathfrak{Q}}} \underset{(\star)}{\cong} \mathrm{Gal}({}^{\kappa(\mathfrak{Q})}/_{\kappa(\mathfrak{p})})$$

2.

$$\underbrace{|\mathrm{Gal}({}^{T_{\mathfrak{Q}}}/_{Z_{\mathfrak{Q}}})|}_{\substack{\| \text{ 1.} \\ [G_{\mathfrak{Q}}:I_{\mathfrak{Q}}]}} \overset{\text{Def.}}{=} f = f(\mathfrak{Q}|\mathfrak{p})$$

Außerdem: $|G_\mathfrak{Q}| = e \cdot f$.
Denn: $\underbrace{[L:K]}_{\substack{\| \\ e\cdot f\cdot r}} = |G| = |G_\mathfrak{Q}| \cdot \underbrace{[G:G_\mathfrak{Q}]}_{\substack{\| \\ r}}$

$\overset{\text{Lagrange}}{\Rightarrow} |I_\mathfrak{Q}| = e$ (Lagrange: $|G_\mathfrak{Q}| = |I_\mathfrak{Q}| \cdot [G_\mathfrak{Q} : I_\mathfrak{Q}]$)

3. und 4.
Betrachte die Erweiterung $L/T_\mathfrak{Q}$. Die Trägheitsgruppe von $\mathfrak{Q}$ über $\mathfrak{Q}_T$ ist auch gleich $I_\mathfrak{Q}$:
Der Kern von der Abbildung

$$\begin{aligned} I_\mathfrak{Q} &\longrightarrow \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{Q}_T)) \subset \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{p})) \\ \sigma &\longmapsto \overline{\sigma} \end{aligned}$$

ist auch gleich $I_\mathfrak{Q}$.
($I_\mathfrak{Q}$ ist auch Zerlegungsgruppe von $\mathfrak{Q}$ über $T_\mathfrak{Q}$).
Satz (8.9) $\Rightarrow I_\mathfrak{Q} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{Q}_T))$ ist surjektiv $\Rightarrow \mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{Q}_T)) = \{\mathrm{id}\}$
$\Rightarrow \kappa(\mathfrak{Q}) = \kappa(\mathfrak{Q}_T) \Rightarrow f(\mathfrak{Q}|\mathfrak{Q}_T) = 1$.
Gleichzeitig:

$$e(\mathfrak{Q}|\mathfrak{Q}_T) \cdot f(\mathfrak{Q}|\mathfrak{Q}_T) = [L : T_\mathfrak{Q}] = |I_\mathfrak{Q}| = e$$

4. folgt direkt aus der Multiplikativität von $e$ und $f$. ∎

---

∎ **Bemerkung**
- $I_\mathfrak{Q} = \{\mathrm{id}\} \iff T_\mathfrak{Q} = L \iff e = 1$, das heißt $\mathfrak{p}$ ist unverzweigt in $L$.
- In diesem Fall ist dann $\mathrm{Gal}(\kappa(\mathfrak{Q})/\kappa(\mathfrak{p})) \cong G_\mathfrak{Q} \subset G$ (eine Untergruppe von $G$).

---

∎ **Bemerkung** Sei $K \subset Z \subset L$ ein Zwischenkörper von $L/K$ und $\mathfrak{P} := \mathfrak{Q} \cap Z \subset \mathcal{O}_Z$ das unter $\mathfrak{Q}$ liegende Primideal von $\mathcal{O}_Z$.

1. Falls $e(\mathfrak{P}|\mathfrak{p}) = 1$ und $f(\mathfrak{P}|\mathfrak{p}) = 1$ ist, so gilt:
$$Z \subset Z_\mathfrak{Q}$$
2. Falls $e(\mathfrak{P}|\mathfrak{p}) = 1$ ist, so gilt:
$$Z \subset T_\mathfrak{Q}$$
3. Ist $\mathfrak{Q}$ das einzige Primideal über $\mathfrak{P} \subset \mathcal{O}_Z$, so ist
$$Z_\mathfrak{Q} \subset Z$$

---

*Beweis:* Übung. ∎

---

**Korollar 8.12** 1. Falls $G_\mathfrak{Q} \subset G$ ein Normalteiler ist, dann zerfällt $\mathfrak{p}$ in $Z_\mathfrak{Q}$ in $r = [Z_\mathfrak{Q} : K] = [G : G_\mathfrak{Q}]$ verschiedene Primideale:

$$\mathfrak{p}\mathcal{O}_{Z_\mathfrak{Q}} = \mathfrak{P}_1 \cdot \dots \cdot \mathfrak{P}_r, \qquad \mathfrak{P}_i \subset \mathcal{O}_{Z_\mathfrak{Q}} \text{ Primideale}$$

($\mathfrak{p}$ ist vollständig zerlegt in $Z_\mathfrak{Q}$).

2. Falls $I_{\mathfrak{Q}} \subset G$ zusätzlich Normalteiler ist, so bleiben $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ prim in $T_{\mathfrak{Q}}$ (sie sind „träge“). In $L$ werden die $\mathfrak{P}_i$'s zu $e-$ten Potenzen.

*Beweis:*

1. Hauptsatz der Galoistheorie: ${}^{Z_{\mathfrak{Q}}}/_{K}$ Galoiserweiterung
   $\Rightarrow$ Verzweigungsindizes und Trägheitsgrade sind alle identisch
   Also: Ist $\mathfrak{P} \subset \mathscr{O}_{Z_{\mathfrak{Q}}}$ Primideal über $\mathfrak{p}$, so ist
   $$\left.\begin{array}{l} e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{Q}_Z|\mathfrak{p}) = 1 \\ f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{Q}_Z|\mathfrak{p}) = 1 \end{array}\right\} \overset{\text{fundamentale Gleichung}}{\Rightarrow}$$ Anzahl der Primideale in $\mathscr{O}_{Z_{\mathfrak{Q}}}$ über $\mathfrak{p}$ ist gleich $r$.
2. In $L$ gibt es auch $r$ verschiedene Primideale über $\mathfrak{p}$. Somit ist dies auch in $T_{\mathfrak{Q}} \supset Z_{\mathfrak{Q}}$ der Fall ($T_{\mathfrak{Q}} \subset L$). Wie oben ist ${}^{T_{\mathfrak{Q}}}/_{K}$ Galoiserweiterung.
   $\Rightarrow$ alle Verzweigungsindizes sind gleich. $\Rightarrow e(\mathfrak{P}_i \cdot \mathscr{O}_{T_{\mathfrak{Q}}}|\mathfrak{P}_i) = e(\mathfrak{Q}_T|\mathfrak{Q}_Z) = 1$
   $\Rightarrow$ Die $\mathfrak{P}_i$ sind träge in $L$. ${}^{L}/_{T_{\mathfrak{Q}}}$ ist eine Galoiserweiterung, somit sind auch alle Verzweigungsindizes $= e$, d.h. $\mathfrak{P}_i \cdot \mathscr{O}_L = \mathfrak{Q}_i^e$ mit $\mathfrak{Q}_i \subset \mathscr{O}_L$ Primideal.

∎

# 9. Kreisteilungskörper und Fermat's letzter Satz

($n \in \mathbb{N}_{\geq 3}$). Betrachte den *n-ten Kreisteilungskörper* $K = \mathbb{Q}(\zeta)$, wobei $\zeta$ eine *primitive* $n$-te Einheitswurzel sei, d.h. $\zeta^n = 1$ aber $\zeta^m \neq 1 \; \forall 0 < m < n$ bzw. $\text{ord}(\zeta) = n$. (Denke dabei zum Beispiel an $\zeta = e^{\frac{2\cdot\pi\cdot i}{n}}$).
Wir wollen zeigen: $\mathcal{O}_K = \mathbb{Z}[\zeta]$.
Zunächst zur Erinnerung:

**Satz 9.1** $K/\mathbb{Q}$ ist Galoiserweiterung vom Grad $\varphi(n) := |\{m \in \mathbb{N} \mid 1 \leq m < n \text{ und } \text{ggT}(m,n) = 1\}|$ (*eulersche φ-Funktion*) und es gilt:

$$\begin{aligned} \text{Gal}(K/\mathbb{Q}) &\cong (\mathbb{Z}/n\mathbb{Z})^\times \\ (\sigma_a : \zeta \mapsto \zeta^a) &\leftrightarrow a \pmod{n} \end{aligned}$$

*Beweis:*

- Galoiserweiterung: Zerfällungskörper von $\underbrace{X^n - 1}_{\| \; \prod_{a=0}^{n-1}(X-\zeta^a)}$. (separabel, da $\text{char}(K) = 0$).
- Ist $\sigma \in \text{Gal}(K/\mathbb{Q})$, so ist $\sigma(\zeta)$ ebenfalls primitive $n$-te Einheitswurzel (da $\sigma$ Automorphismus ist).

  $\Rightarrow$ Minimalpolynom von $\zeta$ über $\mathbb{Q}$ :
  $$\Phi_n(X) = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} (X - \sigma(\zeta))$$

  (Also ist $\sigma(\zeta) = \zeta^a$ für ein $a \in \mathbb{N}$ mit $1 \leq a \leq n$ und $\text{ggT}(a,n) = 1$. Nicht klar ist jedoch, ob alle diese $a$ auftauchen)
  Zeigen nun: zu $a \in \mathbb{N}$ mit $1 \leq a \leq n$ und $\text{ggT}(a,n) = 1$ gibt es ein $\sigma_a \in \text{Gal}(K/\mathbb{Q})$, so dass $\sigma_a(\zeta) = \zeta^a$.
  Es reicht zu zeigen: Ist $p$ Primzahl, $1 < p < n$ mit $p \nmid n$, so gibt es $\sigma_p \in \text{Gal}(K/\mathbb{Q})$.

Sei dazu $\alpha := \zeta^k$ für $1 \leq k \leq n$ mit $\mathrm{ggT}(k,n) = 1$ und sei $f \in \mathbb{Z}[X]$ das Minimalpolynom von $\alpha$ über $\mathbb{Q}$.

$$\Rightarrow X^n - 1 = f(X) \cdot g(X) \qquad \text{mit } g \in \mathbb{Z}[X].$$

Klar: $\alpha^p$ ist Nullstelle von $X^n - 1$. Zu zeigen: $\alpha^p$ ist Nullstelle von $f$.
Angenommen $f(\alpha^p) \neq 0 \Rightarrow g(\alpha^p) = 0$

$$\Rightarrow f \mid g(X^p) \Rightarrow g(X^p) = f(X) \cdot \widetilde{g}(X) \qquad \text{mit } \widetilde{g} \in \mathbb{Z}[X].$$

Sei $\overline{g} \in (\mathbb{Z}/p\mathbb{Z})[X]$ die Reduktion modulo $p$ von $g$, $\overline{f} \in (\mathbb{Z}/p\mathbb{Z})[X]$ die Reduktion modulo $p$ von $f$.
$\Rightarrow \overline{f} \mid \overline{g}(X^p) = (\overline{g}(X))^p$ (Frobenius-Homomorphismus). Die Gleichheit gilt, da

$$\overline{g}(X^p) = \underbrace{\overline{a_0}}_{\| \; \overline{a_0}^p} + \overline{a_1}X^p + \cdots + \overline{a_m}X^{m \cdot p} = (\overline{a_0} + \overline{a_1}X + \cdots + \overline{a_m}X^m)^p$$

Da $(\mathbb{Z}/p\mathbb{Z})[X]$ faktoriell ist, folgt:
Ist $\overline{h} \in (\mathbb{Z}/p\mathbb{Z})[X]$ prim mit $\overline{h} \mid \overline{f}$, so gilt $\overline{h} \mid \overline{g}$

$$\Rightarrow \overline{h}^2 \mid \overline{f} \cdot \overline{g} = X^n - \overline{1}$$
$$\Rightarrow \overline{h} \text{ teilt die Ableitung von } X^n - 1 \text{ in } (\mathbb{Z}/p\mathbb{Z})[X]$$

Ableitung von $X^n - 1$ ist $\overline{n} \cdot X^{n-1}$.

$$\overset{\overline{n} \neq 0}{\Rightarrow} \underbrace{\overline{h} \mid X^{n-1}}_{\Downarrow \; \overline{h} = X^r} \qquad \not\downarrow \overline{h} \mid X^n - 1$$

$$\Rightarrow f(\alpha^p) = 0$$

$$\underset{k=1}{\Rightarrow} \Phi_n(X) = \prod_{\substack{a=1 \\ \mathrm{ggT}(a,n)=1}}^{n-1} (X - \zeta^a)$$

■

■ **Bemerkung** $\Phi_n$ heißt *n-tes Kreisteilungspolynom*.

**Korollar 9.2** 1. Ist $n$ gerade, so gilt:

$$\underbrace{\mu(K)}_{\substack{\text{Einheitswurzeln} \\ \text{in } K}} = \{X \in K \mid X^n = 1\}$$

(genau die $n$-ten Einheitswurzeln).
2. Ist $n$ ungerade, so gilt:

$$\mu(K) = \{X \in K \mid X^{2n} = 1\}$$

*Beweis:*

1. Übung.
2. $n$ ungerade $\Rightarrow \varphi(2n) = \varphi(n)$

$$\Rightarrow \mathbb{Q}\left(e^{\frac{2\cdot\pi\cdot i}{2n}}\right) = \mathbb{Q}\left(e^{\frac{2\cdot\pi\cdot i}{n}}\right)$$

„$\supseteq$“klar
„$\subseteq$“wegen Grad nach Satz (9.1)
Behauptung folgt auch aus 1.:
Man kann die Gleichheit auch so sehen:
$\zeta$ primitive $n$-te Einheitswurzel $\Rightarrow (-\zeta)^n = (-1)^n = -1$ ($n$ ungerade).

∎

---

**Satz 9.3** Sei $n \geq 3$, $K = \mathbb{Q}(\zeta)$ mit $\zeta$ primitiver $n$-ter Einheitswurzel. Dann ist:

$$\mathcal{O}_K = \mathbb{Z}[\zeta]$$

**Lemma 9.4** Für $n \geq 3$ gilt: $\mathbb{Z}[1-\zeta] = \mathbb{Z}[\zeta]$, sowie die Diskriminanten bezüglich $(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1})$ und $(1, 1-\zeta, \ldots, (1-\zeta)^{\varphi(n)-1})$ sind identisch.

*Beweis:* $\mathbb{Z}[1-\zeta] = \mathbb{Z}[\zeta]$, da $\zeta = -(1-\zeta)+1$ ist. Die Diskriminante hängt nicht von der Wahl der $\mathbb{Z}$-Basis ab. ∎

---

**Lemma 9.5** Für $n = p^r$ (mit $p \in \mathbb{N}$ Primzahl, $r \geq 1$) gilt:

$$p = \prod_{\substack{k=0 \\ p \nmid k}}^{n} (1-\zeta^k) \qquad (\zeta \text{ primitive } n\text{-te Einheitswurzel})$$

*Beweis:* $f(X) := \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \underbrace{1 + X^{p^{r-1}} + X^{2p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}}_{p \text{ Summanden}}$ $(\star)$

Es gilt: $\varphi(p^r) = (p-1)\cdot p^{r-1}$ und $f(\zeta^k) = 0$ für $p \nmid k$ (es gibt nur $\varphi(p^r)$ solche $k$'s)

$$\Rightarrow f(X) = \prod_{\substack{k=0 \\ p \nmid k}}^{n} (X-\zeta^k) \qquad \text{(normiertes Pol. vom Grad } \varphi(p^r) \text{ mit Nullstellen } \zeta^k \text{ für } p \nmid k)$$

$$(\star) \Rightarrow f(1) = p = \prod_{\substack{k=0 \\ p \nmid k}}^{n} (1-\zeta^k)$$ ∎

---

*Beweis von Satz (9.3):* Zunächst: $n = p^r$ Primzahlpotenz.
Wissen: $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta] \subset \mathcal{O}_K$
Wie in Übung *Q 29 i)*: Wenn $f \in \mathbb{Z}[X]$ das Minimalpolynom von $\zeta$ über $\mathbb{Q}$ ist, so gilt:

$$d := d(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(n)-1}) = (-1)^{\frac{m\cdot(m-1)}{2}} \cdot N_{K/\mathbb{Q}}(f'(\zeta)) \qquad \text{mit } m = \varphi(n)$$

Außerdem:

$$
\begin{aligned}
& X^n - 1 = f(X)\cdot g(X), \text{ mit } g \in \mathbb{Z}[X] \\
\Rightarrow & n\cdot X^{n-1} = f'(X)\cdot g(X) + f(X)\cdot g'(X) \\
\overset{X=\zeta}{\Rightarrow} & n\cdot \underbrace{\zeta^{n-1}}_{\| \ \zeta^{-1}} = f'(\zeta)\cdot g(\zeta) \\
\Rightarrow & n = f'(\zeta)\cdot g(\zeta)\cdot \zeta \\
\Rightarrow & \underbrace{N_{K/\mathbb{Q}}(n)}_{\| \ n^{\varphi(n)}} = N_{K/\mathbb{Q}}(\zeta\cdot g(\zeta))\cdot \underbrace{N_{K/\mathbb{Q}}(f'(\zeta))}_{\| \ \pm d} \\
\Rightarrow & d \mid n^{\varphi(n)} \Rightarrow d \text{ ist Potenz von } p
\end{aligned}
$$

Angenommen, $\mathbb{Z}[\zeta] \subsetneq \mathcal{O}_K \overset{\text{Korollar (1.27)}}{\Rightarrow} \exists\, x \in \mathcal{O}_K \setminus \underbrace{\mathbb{Z}[\zeta]}_{\| \ \mathbb{Z}[1-\zeta]}$ mit:

$$
x = \frac{1}{p}\cdot \sum_{j=0}^{\varphi(n)-1} \underbrace{m_j}_{\cap \ \mathbb{Z}} \cdot (1-\zeta)^j \qquad \text{mit } p \nmid m_{j_0} \text{ und } j_0 \in \{0,1,\ldots,\varphi(n)-1\} \text{ minimal.}
$$

$$
\Rightarrow y = \tfrac{1}{p}\cdot \sum_{j=j_0}^{\varphi(n)-1} m_j\cdot(1-\zeta)^j \in \mathcal{O}_K
$$

$$
\text{Lemma (9.5)} \Rightarrow \frac{p}{(1-\zeta)^{\varphi(n)}} = \prod_{\substack{k=0 \\ p\nmid k}}^{n} \frac{1-\zeta^k}{1-\zeta} \in \mathbb{Z}[1-\zeta]
$$

(vgl. (*E 38*) $\Rightarrow (1-\zeta) \mid (1-\zeta^k)$ in $\mathbb{Z}[1-\zeta]$).

$$
\begin{aligned}
& \Rightarrow \frac{p}{(1-\zeta)^j} \in \mathbb{Z}[1-\zeta] \qquad\qquad (j = 0,\ldots,\varphi(n)) \\
& \Rightarrow \underbrace{y\cdot \frac{p}{(1-\zeta)^{j_0+1}}}_{} \in \mathcal{O}_K \\
& \quad = \sum_{j=j_0}^{\varphi(n)-1} m_j\cdot(1-\zeta)^{j-j_0-1} = \frac{m_{j_0}}{1-\zeta} + \underbrace{\sum_{j=j_0+1}^{\varphi(n)-1} m_j\cdot(1-\zeta)^{j-(j_0+1)}}_{\cap \ \mathbb{Z}[1-\zeta]} \\
& \Rightarrow \frac{m_{j_0}}{1-\zeta} \in \mathcal{O}_K \\
& \quad \Rightarrow \underbrace{N_{K/\mathbb{Q}}\left(\frac{m_{j_0}}{1-\zeta}\right)}_{} \in \mathbb{Z} \\
& \quad\quad = \frac{N_{K/\mathbb{Q}}(M_{j_0})}{N_{K/\mathbb{Q}}(1-\zeta)} \overset{(9.5)}{=} \frac{m_{j_0}^{\varphi(n)}}{p} \qquad \lightning\, p \nmid m_{j_0}
\end{aligned}
$$

$\Rightarrow$ die Behauptung für $n = p^r$.

Einschub:
Sind $K, L$ Zahlkörper, dann ist ihr *Kompositum*:

$$KL = K(L),$$

der kleinste Zahlkörper, der $K$ und $L$ enthält. Es ist:

$$KL = \{\sum_{i=0}^{m} \alpha_i \cdot \beta_i \mid \alpha_i \in K,\ \beta_i \in L,\ m \in \mathbb{N}_0\}$$

Übung:
Seien $m = [K : \mathbb{Q}]$, $n = [L : \mathbb{Q}]$ und es gelte $[KL : \mathbb{Q}] = m \cdot n$ und es sei $d := ggT(d_K, d_L)$. Dann gilt:

$$\mathcal{O}_{KL} \subset \frac{1}{d} \cdot \mathcal{O}_K \cdot \mathcal{O}_L$$

Insbesondere, falls $d = 1$ ist, so gilt:

$$\mathcal{O}_{KL} = \mathcal{O}_K \cdot \mathcal{O}_L = \{\sum_{i=0}^{r} \alpha_i \cdot \beta_i \mid \alpha_i \in \mathcal{O}_K,\ \beta_i \in \mathcal{O}_L,\ r \in \mathbb{N}_0\}$$

*Ein Beweis findet sich zum Beispiel im Buch „Algebraische Zahlentheorie“ von Neukirch, oder auch im Buch „Number Fields“ von Marcus.*

---

Fortsetzung des Beweises:
Allgemeiner Fall: $n = p_1^{\nu_1} \cdot \dots \cdot p_r^{\nu_r}$ mit $p_i \neq p_j$ Primzahlen, $r \in \mathbb{N}$.
Induktion nach $r$:
$r = 1$: ✓
Induktionsschritt: Sei $n = n_1 \cdot n_2$, $\mathrm{ggT}(n_1, n_2) = 1$, $n_1, n_2 \neq 1$. Man erhält:

$$\begin{aligned} \zeta_1 &= \zeta^{\frac{n}{n_1}} & \zeta_2 &= \zeta^{\frac{n}{n_2}} \\ K_1 &= \mathbb{Q}(\zeta 1) & K_2 &= \mathbb{Q}(\zeta_2) \\ \mathcal{O}_{K_1} &= \mathbb{Z}[\zeta_1] & \mathcal{O}_{K_2} &= \mathbb{Z}[\zeta_2] \end{aligned}$$

nach Induktionsvoraussetzung

Es gilt: $\zeta = \zeta_1^{s_1} \cdot \zeta_2^{s_2}$ mit $s_1 n_1 + s_2 n_2 = 1 = \mathrm{ggT}(n_1, n_2)$, $(s_1, s_2 \in \mathbb{Z})$.
$\Rightarrow K = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1)\mathbb{Q}(\zeta_2) = K_1 K_2$ und $\mathbb{Z}(\zeta) = \mathbb{Z}(\zeta_1)\mathbb{Z}(\zeta_2)$.
Da $\mathrm{ggT}(n_1, n_2) = 1$ gilt $\varphi(n) = \varphi(n_1) \cdot \varphi(n_2)$. Wie oben zeigt man, dass $d_{K_i} \mid n_i^{\varphi(n_i)}$. Damit kann man die Übung anwenden:

$$\overset{\text{mit Übung}}{\Rightarrow} \mathcal{O}_K = \mathcal{O}_{K_1}\mathcal{O}_{K_2} = \mathbb{Z}[\zeta_1]\mathbb{Z}[\zeta_2] = \mathbb{Z}[\zeta]$$

∎

---

**Satz 9.6** Sei $n = \prod_p p^{\nu_p}$ die Primfaktorzerlegung von $n$. Für $p \in \mathbb{N}$ Primzahl sei $f_p \in \mathbb{N}$ minimal mit:

$$p^{f_p} \equiv 1 \pmod{\frac{n}{p^{\nu_p}}},$$

das heißt $f_p = \mathrm{ord}(p)$ in $(\mathbb{Z}/\frac{n}{p^{\nu_p}}\mathbb{Z})^\times$.
Dann gilt in $K = \mathbb{Q}(\zeta)$:

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_{r_p})^{\varphi(p^{\nu_p})},$$

wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_{r_p} \subset \mathcal{O}_K$ verschiedene Primideale mit Trägheitsgrad: $f(\mathfrak{p}_i|p) = f_p$ sind.
Fundamentale Gleichung:

$$\underbrace{\varphi(p^{\nu_p})}_{\substack{\| \\ e(\mathfrak{p}_I|p)}} \cdot f_p \cdot r_p = \varphi(n)$$

*Beweis:* $\mathcal{O}_K = \mathbb{Z}[\zeta] \Rightarrow$ Wir können stets Satz (7.8) anwenden.
Zeige:

$$\underset{\substack{n\text{-tes Kreisteilungs-} \\ \text{polynom}}}{\Phi_n(X)} \equiv (\overline{g_1}(X) \cdot \cdots \cdot \overline{g_{r_p}}(X))^{\varphi(p^{\nu_p})} \pmod{p}$$

mit $\overline{g_i} \in \mathbb{Z}/p\mathbb{Z}[X]$ irreduzibel, verschieden und $\mathrm{Grad}(\overline{g_i}) = f_p$.

---

Schreibe $n = p^{\nu_p} \cdot m$ mit $p \nmid m$.

$$\Rightarrow \Phi_n(X) = \prod_{k,l}(X - \xi^l \cdot \eta^l),$$

wobei $\xi^k$ die $m$-ten primitiven Einheitswurzeln durchläuft und $\eta^l$ die $p^{\nu_p}$-ten primitiven Einheitswurzeln.
Bemerke:

$$X^{p^{\nu_p}} - 1 \equiv (X-1)^{p^{\nu_p}} \pmod{p}$$

$\Rightarrow$ Ist $\mathfrak{p} \mid p\mathcal{O}_K$ Primteiler in $\mathcal{O}_K$, so gilt:

$$\eta^l \equiv 1 \pmod{\mathfrak{p}}$$

$$\Rightarrow \Phi_n(X) \equiv \prod_k (X - \xi^k)^{\varphi(p^{\nu_p})} = \Phi_m(X)^{p^{\nu_p}} \pmod{\mathfrak{p}}$$

$$\overset{\mathfrak{p}|p \text{ beliebig}}{\Rightarrow} \Phi_n(X) \equiv \Phi_m(X)^{p^{\nu_p}} \pmod{p}$$

$\Rightarrow$ Ⱡ $\quad p \nmid n$

---

Für $p \nmid n$ gilt:
$X^n - 1$ hat in $\mathcal{O}_K/\mathfrak{p}$ keine mehrfachen Nullstellen (für $\mathfrak{p} \mid p$), da die Ableitung $n \cdot X^{n-1}$ ist und $p \nmid n \Rightarrow \mathfrak{p} \nmid n$.
Sei $\mu_n = \{\zeta^a \mid a = 0, \ldots, n-1\} \subset \mathcal{O}_K$ die Gruppe der $n$-ten Einheitswurzeln und $\pi : \mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathfrak{p}$ die kanonische Projektion.
Dann ist $\pi(\mu_n)$ genau die Menge der Nullstellen von $X^n - 1$ in $\mathcal{O}_K/\mathfrak{p}$.
$\Rightarrow \pi\big|_{\mu_n} \longrightarrow \pi(\mu_n)$ ist bijektiv.
$\Rightarrow \mathcal{O}_K/\mathfrak{p}$ ist Körpererweiterung von $\mathbb{F}_p$, welche die $n$-ten Einheitswurzeln enthält.
Allgemein: Ist $\kappa/\mathbb{F}_p$ Körpererweiterung, $\xi \in \kappa$ primitive $n$-te Einheitswurzel

$$\Rightarrow \underset{\substack{\| \\ n}}{\mathrm{ord}(\xi)} \mid |\kappa^\times| = p^s - 1 \Rightarrow n \mid p^s - 1 \Rightarrow p^s \equiv 1 \pmod{n}$$

Umgekehrt: Falls $|\kappa| = p^s$ mit $p^s \equiv 1 \pmod{n} \Rightarrow \exists$ primitive $n$-te Einheitswurzel in $\kappa$, da $\kappa^\times$ zyklisch ist.

$\Rightarrow \mathbb{F}_{p^{f_p}}$ ist genau der Zerfällungskörper von $\underbrace{\Phi_n(X) \mod p}_{\vdots \; \overline{\Phi_n}(X)}$

Sei $\overline{\Phi_n}(X) = \overline{g_1}(X) \cdot \dots \cdot \overline{g_r}(X)$ mit $\overline{g_i}$ irreduzibel und verschieden.
$\Rightarrow \overline{g_i}(X) \in \mathbb{F}_p[X]$ ist das Minimalpolynom von einer primitiven $n$-ten Einheitswurzel $\overline{\xi} \in \mathbb{F}_{p^{f_p}}$.
$\Rightarrow \mathrm{Grad}(\overline{g_i}) = p^{f_p}$ ∎

---

**Korollar 9.7**
1. Eine ungerade Primzahl $p$ ist genau dann verzweigt in $\mathbb{Q}(\zeta_n)$, wenn $p \mid n$ gilt.
2. $p = 2$ verzweigt $\iff \mathrm{ggT}(4,n) \geq 4$ (d.h. $v_2 \geq 2$)
3. $p \neq 2$ voll zerlegt in $\mathbb{Q}(\zeta_n) \iff p \equiv 1 \pmod{n}$

*Beweis:* $n = \prod_p p^{v_p}$, $p\mathbb{Z}[\zeta_n] = (\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r)^{\varphi(p^{v_p})}$

1. $p \mid n \underset{p \text{ ungerade}}{\iff} \varphi(p^{v_p}) \neq \varphi(1) = 1$ für $p$ ungerade
2. $p = 2$:

$$\varphi(2^1) = 1, \quad \varphi(2^2) = 2, \dots$$

Falls $v_2 \leq 1$, so ist $p = 2$ unverzweigt, falls $v_2 > 1$, so ist $p = 2$ verzweigt.

3. voll zerlegt $\iff r_p = \varphi(n) \iff f_p = 1 \iff p \equiv 1 \pmod{n}$

∎

---

## 9.1 Das quadratische Reziprozitätsgesetz

**Definition 9.8** Sei $p \in \mathbb{N}$ ungerade Primzahl. Für $n \in \mathbb{Z}$ mit $p \nmid n$, definiere das *Legendre-Symbol*:

$$\underset{\text{„}n \text{ über } p\text{“}}{\left(\frac{n}{p}\right)} := \begin{cases} 1 & \text{falls } n \text{ ist quadratischer Rest modulo } p \\ -1 & \text{sonst} \end{cases}$$

($n$ quadratischer Rest modulo $p$ $:\iff \exists\, a \in (\mathbb{Z}/p\mathbb{Z})^\times : a^2 \equiv n \pmod{p}$)

∎ **Bemerkung**
- Das Legendre-Symbol ist multiplikativ:

$$\left(\frac{m \cdot n}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right)$$

- $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}$

---

**Satz 9.9 — Quadratisches Reziprozitätsgesetz; Gauß.** Für ungerade Primzahlen $p, q \in \mathbb{N}$, $p \neq q$ gilt:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Zusatz:

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
2. $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$

**Satz 9.10** Sei $n \in \mathbb{Z}$ quadratfrei und $p \in \mathbb{N}$ ungerade. Dann gilt:

$$\left(\frac{n}{p}\right) = 1 \iff p \text{ ist voll zerlegt in } K := \mathbb{Q}(\sqrt{n})$$

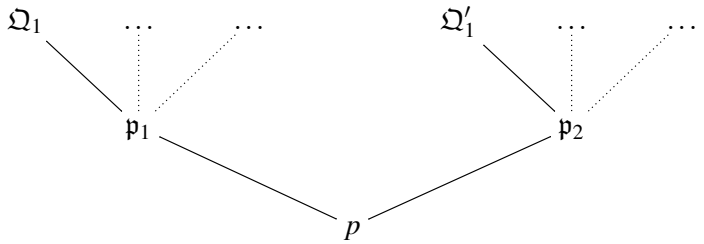
*Beweis:* $p \nmid |\mathcal{O}_K/\mathbb{Z}[\sqrt{n}]|$, da der Index maximal 2 ist.
$X^2 - n \mod p$ spaltet auf in $(X-a)(X+a)$ in $\mathbb{F}_p[X] \iff \left(\frac{n}{p}\right) = 1 \iff p$ voll zerlegt, d.h. $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$. ∎

---

**Satz 9.11** Seien $p, q$ ungerade Primzahlen, $p \neq q$. Sei $q^\star := (-1)^{\frac{q-1}{2}} \cdot q$ und $\zeta_q$ primitive $q$-te Einheitswurzel. Es gilt:

$$p \text{ ist voll zerlegt in } \mathbb{Q}(\sqrt{q^\star}) \iff p \text{ zerfällt in } \mathbb{Q}(\zeta_q) \text{ in eine gerade Anzahl an verschiedenen Primidealen}$$

*Beweis:* Wir wissen aus Aufgabe Q33: $\mathbb{Q}(\sqrt{q^\star}) \subset \mathbb{Q}(\zeta_q)$
„⇒" Sei $p$ voll zerlegt in $K := \mathbb{Q}(\sqrt{q^\star})$, $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ in $K$. Wir wissen: $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ ist galois
$\Rightarrow \mathbb{Q}(\zeta_q)/K$ ist galois.
$\Rightarrow G := \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ operiert transitiv auf den Primidealen über $p$.




Ist $\sigma \in G \Rightarrow \sigma|_K \in \mathrm{Gal}(K/\mathbb{Q})$. Sei also $\sigma \in G$ mit $\sigma(\mathfrak{Q}_1) = \mathfrak{Q}_1'$, wobei $\mathfrak{Q}_1 \mid \mathfrak{p}_1$ und $\mathfrak{Q}_1' \mid \mathfrak{p}_2$. Dann gilt: $\underbrace{\sigma(\mathfrak{p}_1)}_{\| \; \sigma(\mathfrak{Q}_1 \cap K)} = \underbrace{\mathfrak{p}_2}_{\| \; \mathfrak{Q}_1' \cap K}$. Daraus folgt, dass Primideale $\mathfrak{Q} \mid \mathfrak{p}_1$ unter $\sigma$ auf Primideale $\mathfrak{Q}' = \sigma(\mathfrak{Q}) \mid \mathfrak{p}_2$ abgebildet werden.
$\Rightarrow \sigma$ liefert eine Bijektion zwischen

$$\{\text{Primideale von } \mathbb{Q}(\zeta_q) \text{ über } \mathfrak{p}_1\} \leftrightarrow \{\text{Primideale von } \mathbb{Q}(\zeta_q) \text{ über } \mathfrak{p}_2\}$$

$\Rightarrow$ Die Anzahl der Primideale in $\mathbb{Q}(\zeta_q)$ über $p$ ist gerade.

„⇐" Angenommen, $p$ zerfällt in eine gerade Anzahl $r$ von Primidealen in $\mathbb{Q}(\zeta_q)$.
Sei $\mathfrak{Q} \subset \mathbb{Z}[\zeta_q]$ Primideal mit $\mathfrak{Q} \mid p$.

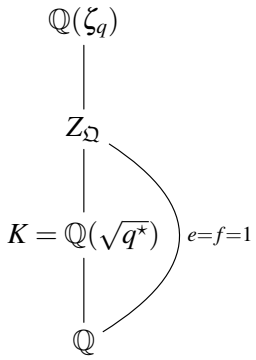
$r = [G : G_{\mathfrak{Q}}] \Rightarrow [\underbrace{Z_{\mathfrak{Q}}}_{\mathbb{Q}(\zeta_q)^{G_{\mathfrak{Q}}}} : \mathbb{Q}] = [G : G_{\mathfrak{Q}}] = r$ ist gerade.

$G$ ist zyklisch von Ordnung $p-1$. Sei $H \subset G$ mit $\mathbb{Q}(\zeta_q)^H = \mathbb{Q}(\sqrt{q^\star}) = K$. Da $[K : \mathbb{Q}] = 2$ ist, folgt daraus, dass $[G : H] = 2$ ist.
$\Rightarrow |G_{\mathfrak{Q}}|$ teilt $|H|$. $|G| = \underbrace{[G : H]}_{\| \; 2} \cdot |H| = [G : G_{\mathfrak{Q}}] \cdot |G_{\mathfrak{Q}}|$

$\overset{G\text{zyklisch}}{\Rightarrow} G_{\mathfrak{Q}} \subset H$

$\Rightarrow \mathbb{Q}(\sqrt{q^\star}) \subset Z_{\mathfrak{Q}}$.

Erinerrung: $f(\mathfrak{Q}_Z|p) = e(\mathfrak{Q}_Z|p) = 1$, wobei $\mathfrak{Q}_Z = Z_{\mathfrak{Q}} \cap \mathfrak{Q}$.




$\Rightarrow f(\mathfrak{Q} \cap K|p) = e(\mathfrak{Q} \cap K|p) = 1 \Rightarrow r = 2$, das heißt $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \Rightarrow p$ ist voll zerlegt in $K$. ∎

---

*Beweis von Satz (9.9):* (ohne Zusätze)
Zeige:

$$\left(\frac{q^\star}{p}\right) = \left(\frac{p}{q}\right) \qquad (q^\star := (-1)^{\frac{q-1}{2}} \cdot q)$$

Es gilt:

$$\left(\frac{q^\star}{p}\right) = 1 \overset{(9.10)}{\iff} p \text{ voll zerlegt in } \mathbb{Q}(\sqrt{q^\star})$$
$$\overset{(9.11)}{\iff} p \text{ zerfällt in } \mathbb{Q}(\zeta_q) \text{ in eine gerade } \underbrace{\text{Anzahl}}_{\| \; r \overset{(9.6)}{=} \frac{q-1}{f_p}} \text{ an Primidealen.}$$

mit $p^{f_p} \equiv 1 \pmod{q}$ $\qquad$ ($f_p$ minimal)
Also:

$$r \text{ gerade} \iff f_p \mid \frac{q-1}{2}$$
$$\iff p^{\frac{q-1}{2}} \equiv 1 \pmod{q}$$
$$\iff \left(\frac{p}{q}\right) = 1$$

∎

---

## 9.2 Fermat's letzter Satz

In diesem Abschnitt ist $p \in \mathbb{N}$ ungerade Primzahl, $K = \mathbb{Q}(\zeta) \subset \mathbb{C}$ mit $\zeta = e^{\frac{2\pi i}{p}}$ primitive $p$-te Einheitswurzel und $h = h_K$ ist die Klassenzahl von $K$.

**Definition 9.12** $p$ heißt *regulär*, falls $p \nmid h$

**Satz 9.13 — Fermat'sche Vermutung; Fermat's letzter Satz.** Sei $p$ ungerade, reguläre Primzahl. Dann besitzt

$$x^p + y^p = z^p$$

keine nicht-trivialen ganzzahligen Lösungen $x, y, z \in \mathbb{Z} \setminus \{0\}$.

■ **Bemerkung** Sei $G = \mathrm{Gal}(K/\mathbb{Q})$. Dann ist die komplexe Konjugation $w \mapsto \overline{w}$ ein Element von $G$.

---

**Lemma 9.14 — Kummer.** Sei $u \in \mathbb{Z}[\zeta]^\times$, dann ist $\frac{u}{\overline{u}}$ eine Einheitswurzel, das heißt:

$$\frac{u}{\overline{u}} = \pm\zeta^k \qquad \text{für } k \in \{0, \dots, p-1\}$$

(De facto gilt: $\frac{u}{\overline{u}} = \zeta^k$)

*Beweis:* Es gilt:

$$\left|\frac{u}{\overline{u}}\right| = 1$$

Außerdem: Sei $\sigma \in G$, dann ist $\sigma(\overline{u}) = \overline{\sigma(u)}$, weil $G$ abelsch ist.

$$\Rightarrow 1 = \left|\frac{\sigma(u)}{\overline{\sigma(u)}}\right| = \left|\frac{\sigma(u)}{\sigma(\overline{u})}\right| = \left|\sigma\left(\frac{u}{\overline{u}}\right)\right|$$

Also: Sei $\alpha := \frac{u}{\overline{u}}$, dann ist $|\sigma(\alpha)| = 1 \ \forall \sigma \in G$.
Damit liegt $\alpha$ im Kern der Abbildung $\lambda$ aus Satz 6.2 und liegt somit in $\mu_{\mathbb{Q}(\zeta)}$. Wir haben schon gesehen (in Korollar 9.2), dass dies genau die $2p$-ten Einheitswurzeln sind und hieraus folgt die Behauptung. ■

---

*Beweis von Satz (9.13):* Wir nehmen an, dass eine nicht-triviale Lösung existiert:

$$x^p + y^p = z^p \qquad x, y, z \neq 0$$

Œ: $\mathrm{ggT}(x, y, z) = 1$.
Fall 1: $p \nmid x \cdot y \cdot z$
Fall 2: $p$ teilt genau eine der Zahlen $x, y, z$.
Beweis des ersten Falls:

$$z^p = x^p + y^p = \prod_{j=0}^{p-1} (x + \zeta^j y) \qquad (\star)$$

wobei $\zeta = \zeta_p$ primitive $p$-te Einheitswurzel ist.
Übung E38:

1. $(1-\zeta)$ ist Primideal und $(1-\zeta)^{p-1} = (p)$

2. $1-\zeta = u_k \cdot (1-\zeta)^k$, für $u_k \in \mathbb{Z}[\zeta]^\times$ und $k = 1, \ldots, p-1$

Angenommen $\mathfrak{p} \mid (x+\zeta^j y)$ und $\mathfrak{p} \mid (x+\zeta^{j'} y)$ für $0 \le j < j' \le p-1$, wobei $\mathfrak{p} \subset \mathbb{Z}[\zeta]$ Primideal ist, $\mathfrak{p} \neq (0)$.

$$\begin{aligned}
\Rightarrow \mathfrak{p} \mid (x+\zeta^j y - (x+\zeta^{j'} y)) &= (\zeta^j y \cdot (1-\zeta^{j'-j})) \\
&\underset{\zeta^j \text{ Einheit}}{=} (y \cdot (1-\zeta^{j'-j})) \\
&\overset{2.}{=} (y \cdot (1-\zeta)) \\
\underset{\text{da } (1-\zeta) \mid (p)}{\overset{1.}{\Rightarrow}} \mathfrak{p} &\mid (y, p)
\end{aligned}$$

Außerdem: Wegen $(\star)$ gilt $\mathfrak{p} \mid (z)^p$.

Aber: $\operatorname{ggT}(yp, z) = 1 \qquad \nmid \mathfrak{p} = (1)$ einzige Möglichkeit

$\Rightarrow$ Alle Faktoren rechts in $(\star)$ sind paarweise teilerfremd.

$\underset{\text{Primidealzerlegung}}{\overset{\text{Eindeutigkeit der}}{\Rightarrow}} (x+\zeta^j y) = \mathfrak{a}_j^p$ mit $\mathfrak{a}_j \subset \mathbb{Z}[\zeta]$ Ideal und $\mathfrak{a}_i,\ \mathfrak{a}_j$ teilerfremd/koprim für $i \neq j$.

$p$ ist regulär ($p \nmid h_{\mathbb{Q}(\zeta)}$) impliziert, da $\mathfrak{a}_j^p$ Hauptideal ist, dass auch $\mathfrak{a}_j = (\alpha_j)$ ein Hauptideal ist.

Insbesondere: $\mathfrak{a}_1 = (\alpha_1) =: (\alpha)$ ist ein Hauptideal, $\alpha \in \mathbb{Z}[\zeta]$.

$$\Rightarrow \alpha^p \cdot u = x + \zeta y \qquad\qquad u \in \mathbb{Z}[\zeta]^\times$$

Schreibe $\alpha = \sum_{i=0}^{p-2} m_i \zeta^i$ mit $m_i \in \mathbb{Z}$.

$$\begin{aligned}
\Rightarrow \alpha^p = (\sum_{i=0}^{p-2} m_i \zeta^i)^p &\equiv \sum_{i=0}^{p-2} \underbrace{m_i^p}_{\| \| \| \; m_i} \cdot (\underbrace{\zeta^p}_{\| \; 1})^i \pmod{p} \\
&\equiv \sum_{i=0}^{p-2} m_i \pmod{p} \\
&\Rightarrow \alpha^p \equiv \overline{\alpha}^p \pmod{p}
\end{aligned}$$

Aus Lemma (9.14) folgt, dass $\frac{u}{\overline{u}} = \pm\zeta^k$ für ein $k \in \{0, \ldots, p-1\}$.

Falls $\frac{u}{\overline{u}} = +\zeta^k$, so gilt:

$$\begin{aligned}
x + \zeta y = u \cdot \alpha^p = \zeta^k \cdot \overline{u} \cdot \alpha^p &\equiv \zeta^k \cdot \overline{u} \cdot \overline{\alpha}^p \pmod{p} \\
&\equiv \zeta^k \cdot \overline{(u \cdot \alpha^p)} \equiv \zeta^k (x + \underbrace{\overline{\zeta}}_{\| \; \zeta^{-1}} y) \pmod{p}
\end{aligned}$$

$$\Rightarrow x + \zeta y - \zeta^k x - \zeta^{k-1} y \equiv 0 \pmod{p}$$

Genauso: Falls $\frac{u}{\overline{u}} = -\zeta^k$, so gilt:

$$x + \zeta y + \zeta^k x + \zeta^{k-1} y \equiv 0 \pmod{p}$$

Übung E34: $p \mid \left(\sum_{j=0}^{p-2} a_j \zeta^j\right) \qquad (a_j \in \mathbb{Z}) \iff p \mid a_j \ \forall j$

Eine kurze Fallunterscheidung führt zum Widerspruch, falls $k \neq 1$. Wir müssen also nur noch $k = 1$ betrachten:

$$\begin{aligned}
x \pm y + \zeta(y \pm x) \equiv 0 \pmod{p} \\
\Rightarrow p \mid x \pm y \\
\Rightarrow x \equiv \mp y \pmod{p}
\end{aligned}$$

Falls $x+y \equiv 0 \pmod{p}$, so folgt, dass $z^p = x^p + y^p \equiv (x+y)^p \equiv 0 \pmod{p}$ $\lightning$
Falls $x-y \equiv 0 \pmod{p}$, so folgt, dass $x \equiv y \pmod{p}$.
Genauso kann man folgern, da $p$ ungerade ist, dass $x \equiv -z \pmod{p}$, indem man die ursprüngliche Gleichung umstellt zu:

$$x^p + (-z)^p = (-y)^p$$

$\Rightarrow 0 = x^p + y^p + (-z)^p \equiv 3x^p \pmod{p}$
$\Rightarrow p = 3$ oder $\underbrace{p \mid x}_{\lightning}$
Wir müssen also nur noch den Fall $p = 3$ zum Widerspruch führen. Für $p = 3$ gilt:

$$x^3 + y^3 = z^3 \Rightarrow x^3 + y^3 \equiv z^3 \pmod{9}$$

Aber modulo 9 gilt:

$$\begin{aligned} 1^3 &\equiv 1 \quad 2^3 \equiv -1 \\ 4^3 &\equiv 1 \quad 5^3 \equiv -1 \\ 7^3 &\equiv 1 \quad 8^3 \equiv -1 \end{aligned}$$

$\Rightarrow$ die linke Seite $\equiv 0, 2, -2$, während die rechte Seite $\equiv \pm 1$ $\lightning$
$\Rightarrow$ Fall 1.
Fall 2:
$p$ teilt genau eine der Zahlen $x, y, z$.
Œ $x^p + y^p + z^p = 0$ und $p \mid z$ aber $p \nmid x$, $p \nmid y$.
Zerlege $z$ in:

$$z = p^r \cdot z_0 \qquad \text{mit } r \geq 1,\ p \nmid z_0$$

Wir wissen: $p = u \cdot (1-\zeta)^{p-1}$ für ein $u \in \mathbb{Z}[\zeta]^\times$.

$$\Rightarrow x^p + y^p + u^{r \cdot p} \cdot (1-\zeta)^{r \cdot (p-1)} \cdot z_0^p = 0 \qquad (\star\star)$$

und $p \nmid x \cdot y \cdot z_0 \Rightarrow (1-\zeta) \nmid x \cdot y \cdot z_0$
Mit dem folgenden Satz (9.15) folgt dann die Behauptung. ∎

---

**Satz 9.15** Sei $p \geq 3$ reguläre Primzahl. Dann hat die Gleichung:

$$a^p + b^p + \varepsilon \cdot (1-\zeta)^{p \cdot n} \cdot c^p = 0 \qquad (\star\star\star)$$

mit $\varepsilon \in \mathbb{Z}[\zeta]^\times$, $n \in \mathbb{N}$ und mit $(1-\zeta) \nmid a \cdot b \cdot c$, keine nicht-trivialen Lösungen $a, b, c \in \mathbb{Z} \setminus \{0\}$.

Aus dem Satz folgt, dass $(\star\star)$ keine Lösungen hat und damit die Behauptung des Satzes (9.13).
*Beweis:* Aus $(\star\star\star)$ folgt die Gleichheit der Ideale

$$\prod_{j=0}^{p-1} (a + \zeta^j \cdot b) = (1-\zeta)^{p \cdot n} \cdot (c)^p$$

$c \neq 0 \Rightarrow a + \zeta^j \cdot b \neq 0$
Es gilt: $1-\zeta \mid a + \zeta^j \cdot b$ für $j = 0, \ldots, p-1$ (vergleiche Übung E38), denn:

$$\left.\begin{array}{l} a + \zeta^j \cdot b \equiv a + b \pmod{(1-\zeta)} \\ 1-\zeta \text{ teilt mindestens einen der Faktoren} \end{array}\right\} \Rightarrow 1-\zeta \text{ teilt alle Faktoren.}$$

Behauptung:
Es existiert ein $j_0 \in \{0,\dots,p-1\}$ mit $(1-\zeta)^2 \mid a+\zeta^{j_0}\cdot b$
Beweis: Angenommen, $a+\zeta^j\cdot b \neq 0 \pmod{(1-\zeta)^2}\ \forall j$

$$\Rightarrow a+\zeta^j\cdot b \equiv \alpha_j\cdot(1-\zeta) \pmod{(1-\zeta)^2} \qquad \text{mit } \alpha_j \equiv 0$$

Beobachtung:

$$\mathbb{Z}[\zeta]/(1-\zeta)^2 \cong (\mathbb{Z}/p\mathbb{Z})[X]/(1-X)^2$$

$\Rightarrow$ Es gibt $p$ verschiedene Möglichkeiten für $\alpha_j$, davon sind $p-1$ Möglichkeiten $\neq 0$.
$\Rightarrow$ Es existieren $k,l \in \{0,\dots,p-1\}$, $0 \le k < l \le p-1$ mit:

$$\begin{aligned} &a+\zeta^k\cdot b \equiv a+\zeta^l\cdot b \pmod{(1-\zeta)^2} \\ \Rightarrow &(1-\zeta^{l-k})\cdot b \equiv 0 \pmod{(1-\zeta)^2} \end{aligned}$$

Da $1-\zeta^{l-k} = u_{l-k}\cdot(1-\zeta)$ mit $u_{l-k} \in \mathbb{Z}[\zeta]^\times$, folgt:

$$(1-\zeta) \mid b \qquad \lightning \text{ Widerspruch zur Annahme}$$

---

Also gibt es (genau ein) solches $j_0$.
$\Rightarrow$ die Behauptung des Satzes für $n=1$.
Für $n>1$, führe eine Induktion nach $n \in \mathbb{N}$ durch.
$\rightsquigarrow$ Ersetze $b$ durch $\zeta^{j_0}\cdot b \Rightarrow$ Œ$j_0 = 0$, das heißt:

$$a+b \equiv 0 \pmod{(1-\zeta)^2} \quad \text{und} \quad a+\zeta^j\cdot b \not\equiv 0 \pmod{(1-\zeta)^2} \text{ für } 1 \le j \le p-1$$

Wie im Fall 1 von Satz (9.13), (da waren alle $(x+\zeta^j\cdot y)$ koprim), erhält man:
$\mathrm{ggT}((a+\zeta^j\cdot b),(a+\zeta^{j'}\cdot b)) = \mathfrak{a}\cdot(1-\zeta)$, wobei $\mathfrak{a} = (a,b)$.

$$\begin{aligned} &\Rightarrow (a+\zeta^j\cdot b) = \mathfrak{a}\cdot(1-\zeta)\cdot\mathfrak{b}_j^p \qquad \text{für } j = 1,\dots,p-1 \\ &\quad (a+b) = \mathfrak{a}\cdot(1-\zeta)^{n\cdot p-(p-1)}\cdot\mathfrak{b}_0^p \end{aligned}$$

mit $1-\zeta \nmid \mathfrak{b}_j$ für alle $j = 0,\dots,p-1$.
$\Rightarrow \mathfrak{b}_k^p\cdot\mathfrak{b}_\ell^{-p}$ ist ein gebrochenes Hauptideal für alle $k$ und $\ell$.
Insbesondere für $\ell = 0$ folgt dann, da $p$ regulär ist, dass $\mathfrak{b}_k\cdot\mathfrak{b}_0^{-1} =: (\beta_k)$ ein gebrochenes Hauptideal, mit $\beta_k \in \mathbb{Q}(\zeta)^\times$, ist.
$\Rightarrow (a+\zeta^k\cdot b)\cdot(a+b)^{-1} = (\beta_k)^p\cdot(1-\zeta)^{-(n-1)\cdot p}$
$\Rightarrow$ Es existiert $\varepsilon_k \in \mathbb{Z}[\zeta]^\times$ für $k = 1,\dots,p-1$, mit

$$\frac{a+\zeta^k\cdot b}{a+b} = \frac{\varepsilon_k\cdot\beta_k^p}{(1-\zeta)^{p\cdot(n-1)}}$$

Schreibe $\beta_k$ als $\beta_k = \frac{x_k}{y_k}$, mit $x_k, y_k \in \mathbb{Z}[\zeta]$.

$$\Rightarrow (a+\zeta^k\cdot b)(1-\zeta)^{p\cdot(n-1)}\cdot y_k^p = \varepsilon_k\cdot x_k^p\cdot(a+b)$$

Damit folgt:
k=1: $$(1-\zeta)^{p\cdot(n-1)}\cdot(a+\zeta\cdot b)\cdot y_1^p = \varepsilon_1\cdot x_1^p\cdot(a+b) \tag{I}$$

k=2: $(1-\zeta)^{p\cdot(n-1)}\cdot(a+\zeta^2\cdot b)\cdot y_2^p=\varepsilon_2\cdot x_2^p\cdot(a+b)$ (II)
Berechne: $(-1)\cdot\big(y_1^p\cdot(\text{II})-y_2^p\cdot(1+\zeta)\cdot(\text{I})\big)$

$$\begin{aligned}\Rightarrow(1-\zeta)^{p\cdot(n-1)}\cdot(y_1y_2)^p\cdot\zeta\cdot(a+b)&=\varepsilon_1\cdot(x_1y_2)^p\cdot(a+b)\cdot(1+\zeta)-\varepsilon_2\cdot(x_2y_1)^p\cdot(a+b)\\&=(a+b)\cdot\big(\varepsilon_1\cdot(x_1y_2)^p\cdot(1+\zeta)-\varepsilon_2\cdot(x_2y_1)^p\big)\end{aligned}$$

Setze : $\varepsilon_2':=\frac{-\varepsilon_2}{\varepsilon_1\cdot(1+\zeta)}\in\mathbb{Z}[\zeta]^\times$ und $\varepsilon_3':=\frac{\zeta}{\varepsilon_1\cdot(1+\zeta)}\in\mathbb{Z}[\zeta]^\times$

$$\Rightarrow(x_1y_2)^p+\varepsilon_2'\cdot(x_2y_1)^p=\varepsilon_3'\cdot(1-\zeta)^{p\cdot((n-1)}\cdot(y_1y_2)^p$$

Wenn man nun $\varepsilon_2'$ los wird, so ist die Gleichung von der Form $(\star\star\star)$ aber mit $n-1$ statt mit $n$ und die Behauptung folgt per Induktion nach $n$. Für diesen Schritt benötigen wir das folgende Lemma.

---

**Lemma 9.16 — Kummer's Lemma.** Sei $p$ eine ungerade, reguläre Primzahl und $u\in\mathbb{Z}[\zeta_p]^\times$. Angenommen, es existiert ein $m\in\mathbb{Z}$ mit $u\equiv m\pmod p$.
Dann gibt es ein $v\in\mathbb{Z}[\zeta_p]^\times$, mit $u=v^p$

*Fortsetzung des Beweises von Satz (9.15):*
Es ist eine Übung zu zeigen, dass es ein $m\in\mathbb{Z}$ gibt, mit $\varepsilon_2'\equiv m\pmod p$.

$$\begin{aligned}&\overset{(9.16)}{\Rightarrow}\varepsilon_2'=v^p\qquad v\in\mathbb{Z}[\zeta]^\times\\&\Rightarrow(x_1y_2)^p+(vx_2y_1)^p+\varepsilon_3'\cdot(1-\zeta)^{p\cdot(n-1)}\cdot(-y_1y_2)^p=0\end{aligned}$$

mit $n-1\geq 1$, sowie $1-\zeta\nmid x_1y_1,\ vx_2y_1,-y_1y_2$
$\overset{\text{Induktion}}{\Rightarrow}$ die Behauptung des Satzes. ∎

---

# Literaturverzeichnis


1. J. Neukirch. *Algebraische Zahlentheorie*. Springer
2. D. A. Marcus. *Number Fields*. Springer
3. D. Zagier. *Zetafunktionen und Quadratische Zahlkörper*. Springer
4. S. Lang. *Algebraic Number Theory*. Addison-Wesley
5. J. Cassels, A. Fröhlich. *Algebraic Number Theory*. Thompson
6. H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer