Algebraische Zahlentheorie

Dr. Klaus Haberland

Setzer und Fehlerveranwortlicher: Stephan Wolf

Wintersemester 2014/15

Inhaltsverzeichnis

Literaturempfehlungen

1 BOREVICH, SHAFAREVICH Zahlentheorie

2 CASSELS, FRÖHLICH, Algebraic number theory, Academic Press 1990

3 FRÖHLICH, TAYLOR, Algebraic number theory, CUP 1993

4 LANG, S. Algebraic number theory, Springer 1994

5 MARCUS, D Numberfields, Springer 1995

6 NEUKIRCH, Algebraic number theory, Springer 2002

7 RAMAKRISHNAN, VALENZA, Fourier analysis on numberfields, Springer 1993

8 SWINNERTON-DYER, A brief guide to algebraic number theory, CUP 2001 (nur 147 S.)

Algebraische Voraussetzung

- Gruppe, Ring, Körper
- GALOIS-Theorie
- Struktursatz über endlich erzeugte Moduln über HIR
- Elementare Arithmetik: Kongruenzen, $\mathbb{F}_q^\times$ ist zyklisch

Siehe z.B. LANG, S.

§1 Ganze algebraische Zahlen

§1.1 Die Mutter aller Ringe: $\mathbb{Z}$

$\mathbb{Z}$ ist kommutativer Ring mit 1, integer (nullteilerfrei), Quotientenkörper ist $\mathbb{Q}$. Wegen des EUKLIDischen Algorithmus ist $\mathbb{Z}$ ein Hauptidealring, also faktoriell. Die Einheiten $\mathbb{Z}^\times$ sind ± 1, die Primelemente (= irred. Elemente) sind die Primzahlen und ihre Negativen. Es gibt unendlich viele Primzahlen. Der klassische Beweis von EUKLID ist bekannt. Es folgen zwei andere.

Beweis (EULER):

Die n-te **FERMAT-Zahl** ist

$$F_n = 2^{2^n} + 1$$

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ und $F_4 = 65537$ sind Primzahlen. Aber EULER 1732: $F_5 = 641 \cdot 6700417$, denn $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$. Also teilt 641 die Zahlen $5^4 \cdot 2^{28} + 2^{32}$ und $5^4 \cdot 2^{28} - 1$ (dritte binomische Formel) und daher auch die Differenz.

Zeigen nun: Alle zwei verschiedene F_n sind teilerfremd. Sei d Teiler von F_n und F_{n+k}, $k > 0$.

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \ldots - 1 \in \mathbb{N}$$

mit $x = 2^{2^n}$. Also teilt F_n die Zahl $F_{n+k} - 2$, und daher auch $d \mid F_{n+k} - 2$. Es folgt $d \mid (F_{n+k} - (F_{n+k} - 2)) = 2$. Da alle F_n ungerade sind, folgt $d = \pm 1$. Also sind je zwei FERMAT-Zahlen teilerfremd.

Folglich liefert jede FERMAT-Zahl mindestens einen neuen Primfaktor. Also muss es unendlich viele Primzahlen geben. □

Beweis (EULER):

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

bezeichnet die **RIEMANNsche Zetafunktion**. Sie konvergiert für $s > 1$. Also $\zeta : (1, \infty) \to \mathbb{R}$. Wir zeigen: $\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$.

$$\prod_{p \le x} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \le x} \sum_{m=0}^{\infty} \frac{1}{p^{ms}}$$

Das ist ein endliches Produkt von absolut konvergenten Reihen. Es lässt sich also ausmultiplizieren. Insgesamt erhält man so die Summe aller $\frac{1}{n^s}$, mit $n \in \mathbb{N}$ und $n = 1$ oder alle Primfaktoren p von n erfüllen $p \le x$. Es folgt daher folgende Abschätzung:

$$0 < \zeta(s) - \prod_{p \le x} \left(1 - \frac{1}{p^s}\right)^{-1} < \sum_{n > x} \frac{1}{n^s}$$

Im Grenzübergang folgt somit die Behauptung:

$$0 \le \lim_{x \to \infty} \zeta(s) - \prod_{p \le x} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s) - \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \le \lim_{x \to \infty} \sum_{n > x} \frac{1}{n^s} = 0$$

Wegen log stetig und $\log(1+x) = \sum_{i=0}^{\infty}(-1)^{i+1}\frac{x^i}{i}$, folgt

$$\log\zeta(s) = \sum_{p\in\mathbb{P}} \log\left(\left(1-\frac{1}{p^s}\right)^{-1}\right) = \sum_{p\in\mathbb{P}} \log\left(\left(1-\frac{1}{p^s}\right)^{-1}\right) = \sum_{p\in\mathbb{P}}\frac{1}{p^s} + \underbrace{\sum_{p\in\mathbb{P}}\sum_{n\geq 2}\frac{1}{np^{ns}}}_{(*)}.$$

Dabei ist $(*)$ für $s \to 1+0$ beschränkt, denn

$$\begin{aligned}\sum_{p\in\mathbb{P}}\sum_{n\geq 2}\frac{1}{np^{ns}} &< \sum_{p\in\mathbb{P}}\sum_{n\geq 2}\frac{1}{p^{ns}} = \sum_{p\in\mathbb{P}}\frac{1}{p^{2s}}\frac{1}{1-\frac{1}{p^s}} \\ &= \sum_{p\in\mathbb{P}}\frac{1}{p^s(p^s-1)} < \sum_{n=2}^{\infty}\frac{1}{n^s(n^s-1)} \\ &< \sum_{n\geq 2}\frac{1}{n(n-1)} < \infty\end{aligned}$$

Also folgt

$$\lim_{s\to 1+0}\sum_{p\in\mathbb{P}}\frac{1}{p^s} = \sum_{p\in\mathbb{P}}\frac{1}{p} = \infty.$$

Daher gibt es insbesondere unendlich viele Primzahlen. □

Fakt 1.1.1 (FERMAT)
Eine Primzahl p ist genau dann Summe zweier Quadratzahlen, wenn $p = 2$ oder $p \equiv 1 \pmod 4$.

Beweis: Sicher ist $2 = 1+1$. Für $p \equiv 3 \pmod 4$ hat man keine Chance, denn für alle $n \in \mathbb{Z}$ ist $n^2 \equiv 0$ oder $1 \pmod 4$ (0 für n gerade, 1 für n ungerade). Also ist $m^2 + n^2 \equiv 0, 1, 2 \pmod 4$.

Sei nun $p \equiv 1 \pmod 4$. $x^2+y^2 \equiv 0 \pmod p$ hat nichttriviale Lösungen genau dann, wenn $-1 = \square$, d.h. -1 ist Quadrat, in $\mathbb{F}_p$. $\mathbb{F}_p^\times$ ist zyklisch $\Rightarrow \mathbb{F}_p^\times = \langle g\rangle$. $g^{\frac{p-1}{2}} = -1$. Also $-1 = \square \Leftrightarrow \frac{p-1}{2}$ gerade $\Leftrightarrow p \equiv 1 \pmod 4$. Es existeren also $x, y \in \mathbb{Z}$ mit $x^2 + y^2 = mp$. Ohne Einschränkung sind $0 < x, y < \frac{p}{2}$, denn $\frac{p^2}{4}$ ist bereits größer als p, für $p \equiv 1 \pmod 4$. Nun ist $x^2 + y^2 < 2p^2/4 < p^2$, also o.B.d.A. $0 < m < p$.

Wir wählen m minimal und nehmen $m > 1$ an. m teilt nicht x und y gleichzeitig, da sonst $m^2 \mid x^2 + y^2 = mp$ ↯. Wähle a und b aus $\mathbb{Z}$, so dass

$$\begin{aligned} x_1 &= x - am & |x_1| &\leq \frac{1}{2}m, \\ y_1 &= x - bm & |y_1| &\leq \frac{1}{2}m. \end{aligned}$$

Dann ist $x_1^2 + y_1^2 > 0$ und $x_1^2 + y_1^2 \leq 2\cdot\left(\frac{1}{2}m\right)^2 = \frac{1}{2}m^2 < m^2$. Andererseits ist $x_1^2 + y_1^2 \equiv x^2 + y^2 \equiv 0 \pmod m$. Somit ist $x_1^2 + y_1^2 = m \cdot n$ mit $0 < n < m$.

Es folgt

$$\begin{aligned} m^2np = (x_1^2+y_1^2)(x^2+y^2) &= |x_1+iy_1|^2|x-iy|^2 \\ &= |(x_1+iy_1)(x-iy)|^2 \\ &= |(x_1x+yy_1)+i(xy_1-x_1y)|^2 \\ &= (x_1x+yy_1)^2+(xy_1-x_1y)^2 \\ xx_1+yy_1 &= x(x-am)+y(y-bm) \\ &= x^2+y^2-m(ax+by) =: mX \\ xy_1-x_1y &= x(y-bm)-(x-am)y \\ &= m(ay-bx) =: mY. \end{aligned}$$

Daher ist $X^2+Y^2 = n\cdot p$ und $0<n<m$ $\lightning$. Also ist $m=1$. □

§1.1.1 Die ganzen GAUSSschen Zahlen

Sei $K=\mathbb{Q}(i)$. Es gilt $[K:\mathbb{Q}]=2$, $K=\{\alpha+\beta i : \alpha,\beta\in\mathbb{Q}\}$ und

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \text{komplexe Konjugation}\}.$$

Definition 1.1.2
Die Menge der **ganzen GAUSSschen Zahlen** ist

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

Bemerkung 1.1.3
Eigenschaften der ganzen GAUSSschen Zahlen:

1) $\mathbb{Z}[i]$ ist kommutativ mit 1, integer und der QK ist $\mathbb{Q}(i)$.
2) Man hat die **Norm**

$$\mathrm{N}: \mathbb{Q}(i)\to\mathbb{Q},\ \alpha+\beta i \mapsto (\alpha+\beta i)(\alpha-\beta i) = \alpha^2+\beta^2.$$

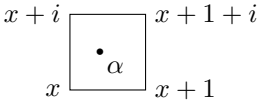
   Es gilt $\mathrm{N}(xy)=\mathrm{N}(x)\,\mathrm{N}(y)$. Für $x\in\mathbb{Z}[i]$ ist $\mathrm{N}(x)\in\mathbb{Z}$.
3) Die Einheiten sind $\pm1,\pm i$. *Beweis:* Ist $x\in\mathbb{Z}[i]^\times$, so existiert ein $y\in\mathbb{Z}^\times$ mit $xy=1$. Mit $x=a+bi$ und $y=c+di$ folgt

$$1=\mathrm{N}(xy)=\mathrm{N}(x)\,\mathrm{N}(y)=(a^2+b^2)(c^2+d^2).$$

   Also $a=\pm1$ und $b=0$ oder $a=0$ und $b=\pm1$. □

Lemma 1.1.4
Sei $\alpha\in\mathbb{Q}(i)$. Dann existiert ein $x\in\mathbb{Z}[i]$, so dass $\mathrm{N}(x-\alpha)<1$.

Beweis: α liegt in einem (höchstens in vier) $\mathbb{Z}[i]$-Kästchen (Quadrat),



hat also von einer der 4 Ecken einen Abstand $\leq \frac{1}{2}\sqrt{2}$. Also existiert ein $x \in \mathbb{Z}[i]$ mit $\mathrm{N}(x-\alpha) \leq \left(\frac{1}{2}\sqrt{2}\right)^2 = \frac{1}{2} < 1$. □

Folgerung 1.1.5 (EUKLIDischer Algorithmus für $\mathbb{Z}[i]$)
$\forall m \in \mathbb{Z}[i], q \in \mathbb{Z}[i] \setminus \{0\} \exists r, x \in \mathbb{Z}[i]$ mit:

(i) $m = xq + r$

(ii) $\mathrm{N}(r) < \mathrm{N}(q)$

Ende VL 1
21.10.14

Folgerung 1.1.6
$\mathbb{Z}[i]$ ist ein HIR, also faktoriell.

Beweis: Sei $\mathfrak{a} \subset \mathbb{Z}[i]$ ein Ideal $\neq (0)$. $0 \neq q \in \mathfrak{a}$ von minimaler Norm. Dann gilt: $(q) \subset \mathfrak{a}$. Sei $m \in \mathfrak{a}$, $m = xq + r$ mit $r \in \mathfrak{a}$ und $0 \leq N(r) < N(q)$. Es folgt $r = 0$, also $m \in (q)$. □

Bemerkung 1.1.7
- $\mathbb{Z}[i]$ hat die gleiche Arithmetik wie $\mathbb{Z}$: ggT (Eindeutig bis auf Einheiten), kgV, Primzahlen,...
- $a \mid b$ genau dann, wenn $\exists c : b = ac$.

Definition 1.1.8
Sei A ein kommutativer Ring, mit 1, integer. $p \in A$ heißt genau dann **irreduzibel**, wenn gilt

(i) $p \neq 0$, $p \notin A^\times$ (d.h. keine Einheit)

(ii) $p = a \cdot b \Rightarrow a \in A^\times$ oder $b \in A^\times$.

$p \in A$ heißt genau dann **prim**, wenn gilt

(i) $p \neq 0, p \notin A^\times$

(ii) $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$.

Mit anderen Worten: $A/(p)$ ist genau dann integer, wenn (p) Primideal ist.

Bemerkung 1.1.9
- Aus prim folgt irreduzibel

  p prim, $p = ab \Rightarrow p \mid ab$. O.B.d.A. $p \mid a$, also $a = p \cdot c$. Es folgt $ab = p = pbc \Rightarrow bc = 1 \Rightarrow b \in A^\times$.
- Ist A faktoriell (z.B. HIR), so folgt aus irred. sogar prim.

  Sei $p \in A$ irreduzibel, $p \mid ab$, also $pc = ab$. a und b haben Faktorisierung in irreduzible Faktoren. Also ist p einer dieser irreduziblen Faktoren. Folglich $p \mid a$ oder $p \mid b$.
- Für A nicht faktoriell gilt die vorherige Aussage im Allgemeinen nicht.

Fakt 1.1.10 (Primzahlen in $\mathbb{Z}[i]$) (i) Jede **GAUSSsche Primzahl** teilt in $\mathbb{Z}[i]$ genau eine orthodoxe Primzahl.

(ii) Die orthodoxen Primzahlen zerlegen sich wie folgt in $\mathbb{Z}[i]$.

(α) $p = 2$: $p = -i(1+i)^2$, $\pi_2 = 1 + i$ ist prim.

(β) $p \equiv 1 \pmod 4$: $p = \pi_p \cdot \overline{\pi}_p$ mit zwei assoziierten Primzahlen $\pi_p, \overline{\pi}_p$.

(γ) $p \equiv 3 \pmod 4$: p bleibt prim in $\mathbb{Z}[i]$.

Bemerkung 1.1.11 • Beispiele:

$$\begin{aligned} 2 &= (1+i)(1-i) = -i(1+i)^2 \\ 3 &= - \\ 5 &= (2+i)(2-i) \\ 7 &= - \\ 13 &= (3+2i)(3-2i) \end{aligned}$$

- Unter (ii) sind alle GAUSSschen Primzahlen aufgeführt, wegen (i).
- 2 heißt verzweigt (ramified), $p \equiv 1 \pmod 4$ heißt zerlegt (split) und $p \equiv 3 \pmod 4$ heißt träge (inert).

Beweis: Sei $\pi \in \mathbb{Z}[i]$ GAUSSsche Primzahl, dann ist $\mathrm{N}(\pi) = \pi\overline{\pi} = p_1 \cdot \ldots \cdot p_r \in \mathbb{Z}$ mit $p_i \in \mathbb{P}$. D.h. π teilt $p_1 \cdot \ldots \cdot p_r$, also auch einen der Faktoren. Gilt $\pi \mid p \in \mathbb{P}$ (Teilbarkeit in $\mathbb{Z}[i]$!) und $\pi \mid l \in \mathbb{P} \setminus \{p\}$, so folgt $\pi \mid 1$ ↯. (i)✓

Aus $\pi \mid p$ folgt $\mathrm{N}(\pi) \mid p^2$. $\mathrm{N}(\pi) = \pi\overline{\pi} = a^2 + b^2 \in \mathbb{Z}$ für $\pi = a + bi$. Also $\mathrm{N}(\pi) = p$ oder p^2.

Ist $\mathrm{N}(\pi) = p$ folgt $p = a^2 + b^2$, also $p = 2$ oder $p \equiv 1 \pmod 4$. Der Fall (α), also $p = 2$ ist klar. Sei p also $\equiv 1 \pmod 4$. Nach (i) existieren $a, b \in \mathbb{Z}$ mit

$$p = a^2 + b^2 = (a+bi)(a-bi) = \pi_p\overline{\pi_p}.$$

Das π_p ist prim, denn aus $\pi_p = \alpha\beta$ folgt $p = \mathrm{N}(\pi_p) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ und damit $\mathrm{N}(\alpha) = 1$ oder $\mathrm{N}(\beta) = 1$, also α oder β Einheit. $\pi, \overline{\pi}$ sind nicht assoziiert. Das zeigen wir indirekt. Angenommen $\overline{\pi} = \varepsilon\pi$ mit einer Einheit ε (also ε eine vierte Einheitswurzel).

$$\begin{aligned} \varepsilon = 1 &\Rightarrow a - bi = a + bi \Rightarrow b = 0 \Rightarrow a^2 \text{ prim } \lightning \\ \varepsilon = -1 &\Rightarrow a - bi = -a - bi \Rightarrow a = 0 \lightning \\ \varepsilon = i &\Rightarrow a - bi = ai - b \Rightarrow a = -b \lightning \\ \varepsilon = -i &\Rightarrow a - bi = -ai + b \Rightarrow a = -b \lightning \end{aligned}$$

Damit ist der Fall (β) klar. Sei schließlich $p \equiv 3 \pmod 4$ und $p = \alpha\beta$ in $\mathbb{Z}[i]$. $p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$. Sind α und β beide keine Einheit, so folgt $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p$. Aber p ist nicht Summe von zwei Quadraten ↯. □

Bemerkung 1.1.12
Der Fakt „Ist $p \equiv 1 \pmod 4$, so ist p nicht prim in $\mathbb{Z}[i]$“ folgt auch ohne FERMAT. *Beweis:* Wegen $p = 4n + 1$ ist -1 Quadrat $\pmod p$, denn

$$\begin{aligned} ((2n)!)^2 &\equiv (2n)!\underbrace{(p-1)(p-2)\cdot(p-2n)}_{2n \text{ Faktoren}} \pmod p \qquad (p - i = -i \pmod p, (-1)^{2n} = 1) \\ &\equiv (p-1)! \pmod p \qquad (p - 2n = 2n + 1) \\ &\equiv -1 \pmod p \qquad \text{nach Satz von Wilson.} \end{aligned}$$

Ohne Wilson: Anschaulich heben sich die Faktoren x, x^{-1} gegenseitig auf, lediglich die selbstinversen sind interessant. $x^2 = 1$ hat aber nur die Lösungen 1 und -1.

Also teilt p die Zahl $((2n)!)^2 + 1 =: N^2 + 1$. Folglich gilt $p \mid (N+i)(N-i)$. Angenommen p ist prim, dann folgt o.B.d.A.

$$\begin{aligned} p \mid N+i \Rightarrow \alpha p = N+i \Rightarrow \overline{\alpha} p = N-i \Rightarrow p \mid N-i \\ \Rightarrow p \mid 2N \Rightarrow p \mid N \Rightarrow p \mid i \lightning \end{aligned}$$

□

Fakt 1.1.13 (i) $\mathbb{Z}[i]/(\pi_2) = \mathbb{F}_2$

(ii) $\mathbb{Z}[i]/(\pi_p) = \mathbb{F}_p$ für $p \equiv 1 \pmod 4$

(iii) $\mathbb{Z}[i]/(\pi_p) = \mathbb{F}_{p^2}$ für $p \equiv 3 \pmod 4$

Bemerkung 1.1.14
$\mathbb{Z}[i]/(m) = \mathbb{Z}[i]/m\mathbb{Z} = m\mathbb{Z} + i \cdot m\mathbb{Z}$

Beweis: Sei $\pi \in \mathbb{Z}[i]$ prim, $(\pi) \supset (p)$ für ein $p \in \mathbb{P}$, also $\mathbb{Z}[i]/(\pi)$ Faktorring von $\mathbb{Z}[i]/(p)$. Letzterer hat p^2 Elemente. Also ist $\mathbb{Z}[i]/(\pi)$ ein endlicher integer Ring und daher ein Körper (denn ist A ein endlicher integer Ring, so ist für jedes $a \in A \setminus \{0\}$ die Abbildung $A \to A$, $x \mapsto ax$ eine Bijektion, also gibt es ein x mit $xa = 1$, also ist a invertierbar).

$\mathbb{Z}[i]/(\pi_2)$ ist ein echter Faktor von $\mathbb{Z}[i]/(2)$, wegen $(\pi_2) \neq (2)$, also $\mathbb{F}_2$

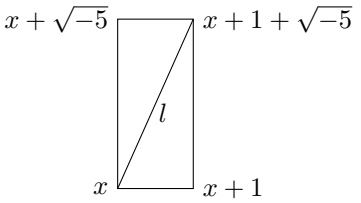
Für $p \equiv 3 \pmod 4$ folgt $\mathbb{Z}[i]/(p)$ ist Körper der Ordnung p^2, also $\mathbb{F}_{p^2}$

Für $p \equiv 1 \pmod 4$ ist $p = \pi_p \overline{\pi_p}$, also ist $\mathbb{Z}[i]/(\pi_p)$ ein echter Faktor von $\mathbb{Z}[i]/(p)$, also $\mathbb{F}_p$. □

§1.1.2 Der Ring $\mathbb{Z}[\sqrt{-5}]$

Sei $K := \mathbb{Q}[\sqrt{-5}]$, dann ist $[K : \mathbb{Q}] = 2$. Sei $A := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$.

A ist kommutativ, mit 1 und integer. Der QK ist K. Die Einheiten sind ± 1, denn ist ε Einheit gilt $\mathrm{N}(\varepsilon) = 1 = a^2 + 5b^2$. Betrachte ein „Kästchen“ in A.



Dann ist $\frac{1}{2}l = \frac{1}{2}\sqrt{6} > 1$. Daher funktioniert unser Argument für den EUKLIDischen Algorithmus nicht, wie bei es bei $\mathbb{Z}[i]$ der Fall war. Tatsächlich ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell, denn in A gilt $21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$. Dabei sind alle Faktoren prim.

Beweis: Ist $3 = xy$, so ist $9 = \mathrm{N}(x)\,\mathrm{N}(y)$. Ist $\mathrm{N}(x) = 1$, dann ist x Einheit. Also o.B.d.A. $\mathrm{N}(x) = \mathrm{N}(y) = 3$. Aber $\mathrm{N}(x) = a^2 + 5b^2 = 3$ hat keine Lösung in $\mathbb{Z}$ $\lightning$. Also 3 irreduzibel. Analog ist 7 irreduzibel, denn $a^2 + 5b^2 = 7$ hat keine Lösung in $\mathbb{Z}$.

Ist $4 + \sqrt{-5} = xy$ folgt $\mathrm{N}(4 + \sqrt{-5}) = 21 = \mathrm{N}(x)\,\mathrm{N}(y)$. Auch hier führen $\mathrm{N}(x) = 3$ oder $\mathrm{N}(x) = 7$ zum Widerspruch. Also $4 \pm \sqrt{-5}$ irreduzibel.

Wir zeigen: $3, 7$ und $4 \pm \sqrt{-5}$ sind alle nicht prim. Es genügt zu zeigen, dass für $x \in \{3, 7, 4 \pm \sqrt{-5}\}$ das Ideal (x) kein Primideal ist, also $A/(x)$ kein Körper ist.

$$\begin{aligned}\mathbb{Z}[\sqrt{-5}]/3\mathbb{Z}[\sqrt{-5}] &= \mathbb{F}_3 \oplus \sqrt{-5}\mathbb{F}_3 \\ &= \mathbb{F}_3[T]/(T^2+5) \\ &= \mathbb{F}_3[T]/(T^2-1)\,(5 = -1 \text{ in } \mathbb{F}_3) \\ &= \mathbb{F}_3 \oplus \mathbb{F}_3\end{aligned}$$

Analog für 7: $T^2 + 5 = T^2 - 2 = (T-3)(T+3)$ in $\mathbb{F}_7[T]$.

$(4 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ hat folgenden Index in $\mathbb{Z}[\sqrt{-5}]$:

$$\left| \det \begin{pmatrix} 4 & -5 \\ 1 & 4 \end{pmatrix} \right|,$$

denn der Index der Untergruppe ist gerade die Anzahl aller Elemente aus $\mathbb{Z}[\sqrt{-5}]$ („Volumen“) in einem $(4+\sqrt{-5})\mathbb{Z}[\sqrt{-5}]$-Kästchen. Dazu berechnen wir also die Determinante der Basistransformationsmatrix von

$$B = (1, \sqrt{-5}) \quad (\mathbb{Z}\text{-Basis von } \mathbb{Z}[\sqrt{-5}])$$

nach

$$C = (4 + \sqrt{-5}, \sqrt{-5}(4 + \sqrt{-5}) = -5 + 4\sqrt{-5}) \quad (\mathbb{Z}\text{-Basis von } (4 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]).$$

Also erhalten wir Index 21. Folglich hat $A/(4 + \sqrt{-5})A$ Ordnung 21 (analog für $4 - \sqrt{-5}$).

Es gibt keinen Körper der Ordnung 21, denn jeder endliche Körper hat einen Primkörper mit Primzahlcharakteristik p und bildet über diesem einen Vektorraum mit p^k Elementen. Aber $21 \neq p^k$. □

Bemerkung 1.1.15
In den nächsten Wochen beschäftigen wir uns damit die Eindeutigkeit der Zerlegung in solchen Ringen zu retten. KUMMERs Idee dazu war, ideale Zahlen zum Ring hinzuzufügen, sodass $3, 7$ und $4 \pm \sqrt{-5}$ weiter zerfallen und man die Eindeutigkeit der Primfaktorisierung zurück gewinnt.

Ende VL 2
22.10.14

§1.2 Ganze algebraische Zahlen

Definition 1.2.1
Sei A ein Ring (kommutativ, mit 1, integer) und $L \supset A$ Körper. Ein Element $x \in L$ heißt **ganz** in A (kurz : ganz $/A$) genau dann, wenn ein **unitäres Polynom**[1] $f \in A[X]$ mit $f(x) = 0$.

Bemerkung 1.2.2
x ganz $/A \Rightarrow x$ algebraisch $/\,\mathrm{QK}(A)$.

Beispiel 1.2.3 (i) $A = \mathbb{Z}$, $L = \mathbb{Q}$. $x \in \mathbb{Z}$ ist ganz $/\mathbb{Z}$. Wurzel von $T - x$. Sei $x \in \mathbb{Q}$ ganz $/\mathbb{Z}$, also

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0,\ a_j \in \mathbb{Z}.$$

[1] d.h. $\exists a_1, \ldots, a_n \in A$, $n \geq 1$, s.d. $f(x) = x^n + a_1 x^{n-1} + \ldots + a_0$

Sei nun $x = \frac{r}{s}$, $r, s \in \mathbb{Z}$, $s \neq 0$, ggT$(r, s) = 1$. Dann

$$r^n + a_1 r^{n-1} s + \ldots + a_n s^n = 0.$$

s teilt sicher die Summe $a_1 r^{n-1} s + \ldots + a_n s^n$, also auch r^n. Sei $p \mid s$, p prim $\Rightarrow p \mid r^n \Rightarrow p \mid r$. Ein Widerspruch. Also $s = \pm 1$ und damit $x \in \mathbb{Z}$.

(ii) $A = \mathbb{Z}$, $L = \mathbb{Q}(i)$. Sei $x = a + bi \in \mathbb{Z}[i]$. Wir bestimmen $c, d \in \mathbb{Z}$, s.d. $x^2 + cx + d = 0$ gilt. Dann $a^2 - b^2 + ac + d = 0$ und $2ab + bc = 0$. Also genügen $c = -2a$ und $d = a^2 + b^2$. Sei $x \in \mathbb{Q}(i)$ ganz $/\mathbb{Z}$, also $x^n + a_1 x^{n-1} + \ldots + a_0 = 0$, $a_j \in \mathbb{Z}$. Weiter wie für $\mathbb{Z}$.

(iii) $A = \mathbb{Z}$, $L = \mathbb{Q}(\sqrt{-5})$ liefert x ganz $/\mathbb{Z}$ genau dann, wenn $x \in \mathbb{Z}[\sqrt{-5}]$.

Fakt 1.2.4
Seien $L \supset A$ wie oben, dann ist $x \in L$ ganz $/A$ genau dann, wenn ein endlich erzeugter A-Modul $M \subset L$, $M \neq 0$ mit $xM \subset M$ existiert.

Beweis: Sei x ganz $/A$, also $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, $a_j \in A$. Bilde $M = A + Ax + \ldots + Ax^{n-1} \subset L$. Sei umgekehrt M ein endlich erzeugter A-Modul, also $M = Av_1 + \ldots + Av_n$. Es folgt

$$\begin{aligned} xv_1 &= a_{11} v_1 + \ldots + a_{1n} v_n \\ &\vdots \\ xv_n &= a_{n1} v_1 + \ldots + a_{nn} v_n \end{aligned}$$

also ist die Determinante

$$\det \begin{pmatrix} a_{11} - x & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - x & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - x \end{pmatrix} = 0.$$

Das ist Ganzheitsgleichung für x. □

Definition 1.2.5
Sei $A \subset L$ wie oben, die Menge B der $x \in L$, welche ganz $/A$ sind, heißt **ganzer Abschluss** von A in L.

A heißt **ganzabgeschlossen** in L, falls $B = A$ ist. A heißt ganzabgeschlossen, falls A ganzabgeschlossen im QK ist.

Beispiel 1.2.6 (i) $\mathbb{Z}$ ist ganzabg.

(ii) $\mathbb{Z}[i]$ ist der ganze algebraische Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(i)$.

(iii) $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$ ist nicht ganzabg.

Für $x = \frac{1+\sqrt{5}}{2}$ ist $x^2 - x - 1 = 0$, also x ganz in $\mathbb{Z}$, also erst recht ganz $/\mathbb{Z}[\sqrt{5}]$.

Definition 1.2.7
$A \subset B$ Ringe (kommutativ, mit 1, integer). B heißt **ganz** $/A$ genau dann, wenn alle Elemente aus B ganz $/A$ sind.

Fakt 1.2.8
Sei $A \subset L$ wie oben und B der ganze Abschluss von A in L. Dann ist B ein Ring in L, der A umfasst.

Beweis: Seien $x, y \in B$, $M, N \subset L$ endlich erzeute A-Moduln mit $xM \subset M$ und $yN \subset N$ ($M \neq 0 \neq N$). Dann ist $MN \subset L$ ein endlich erzeugter A-Modul $\neq 0$ und $(x+y)MN \subset MN$, also $xyMN \subset MN$. □

Bemerkung 1.2.9
$M = Av_1 + \ldots + Av_m$. $N = Aw_1 + \ldots + Aw_n$
$\Rightarrow MN = \sum Av_iw_j$

Fakt 1.2.10
Seien $A \subset B \subset C$ Ringe, B ganz $/A$, C ganz $/B$, dann ist C ganz $/A$.

Beweis: Sei $x \in C$, $x^n + b_1x^{n-1} + \ldots + b_n = 0$ Ganzheitsgleichung. $b_j \in B$. Sei $B_0 = A[b_1, \ldots, b_n]$, das ist endlich erzeugte A-Algebra. Wir zeigen durch Induktion über n, dass B_0 sogar endlich ist (d.h. endlich erzeugt als A-Modul). $A[b_1]$ ist endlich erzeugter A-Modul nach vorletzten Fakt. Nach IV ist $A[b_1, \ldots, b_{n-1}]$ endlich erzeugter A-Modul. b_n ist ganz $/A$, also erst recht ganz $/A[b_1, \ldots, b_{n-1}]$. Somit ist $B_0 = A[b_1, \ldots, b_n]$ endlich erzeugt als $A[b_1, \ldots, b_{n-1}]$-Modul. Das war der Induktionsschritt.

Nun zeigen wir x ganz $/A$. Mit B_0 ist auch $B_0[x]$ endlich erzeugter A-Modul, da x ganz $/B_0$ ist. Weiter gilt für $M = B_0[x]$: $xM \subset M$, also ist x ganz $/A$. □

Definition 1.2.11
Sei K algebraischer Zahlenkörper, d.h. endliche Erweiterung von $\mathbb{Q}$. Der **Ring der ganzen Zahlen** $\mathcal{O}_K$ ist definiert als der ganze Abschluss von $\mathbb{Z}$ in K:

$$\mathcal{O}_K = \{x \in K : x \text{ ganz } /\mathbb{Z}\}$$

Beispiel 1.2.12
Sei $K = \mathbb{Q}(e^{2\pi i/n})$. Dann $\mathcal{O}_K = \mathbb{Z}[e^{2\pi i/n}]$.

Bemerkung 1.2.13
- Nach dieser Definition hat man lange gesucht.
- $\mathcal{O}_K$ ist kommutativ, mit 1, integer, enthält $\mathbb{Z}$ und ist ganzabgeschlossen. Der QK ist K:

  Sei $x \in K \Rightarrow \exists \alpha_1, \ldots, \alpha_n \in \mathbb{Q}$:

  $$x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n = 0$$

  Dann existieren $a_0, \ldots, a_n \in \mathbb{Z}$ mit $a_0 \neq 0$, s.d.

  $$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0.$$

  Multipliziert man beide Seiten mit a_0^{n-1} folgt a_0x ganz $/\mathbb{Z}$, also aus $\mathcal{O}_K$. Mithin $x = \frac{a_0x}{a_0}$ mit $a_0x, a_0 \in \mathcal{O}_K$.

Beispiel 1.2.14 (Quadratische Zahlkörper)
$[K : \mathbb{Q}] = 2 \Leftrightarrow K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, $d \neq 0, 1$ sqf (squarefree). Solche K sind paarweise verschieden, denn ist $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{e})$, folgt $\sqrt{d} = \alpha + \beta\sqrt{e}$ und $\sqrt{e} = \gamma + \delta\sqrt{d}$ mit $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$. Es folgt $d = \alpha^2 + 2\alpha\beta\sqrt{e} + \beta^2 e \Rightarrow \alpha\beta = 0$. Ist $\beta = 0$, so ist $\sqrt{d} = \alpha \not\in$. Ist $\alpha = 0$ folgt $\sqrt{d} = \beta\sqrt{e}$, also $d = \beta^2 e$.

Für $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ ist Gal $= \{\mathrm{Id}, \sigma\}$. $\sigma(a+b\sqrt{d}) = a - b\sqrt{d}$. $\mathrm{N}(x) = x\sigma(x) = a^2 - db^2$. $\mathrm{Tr}(x) = x + \sigma(x) = 2a$. Wir zeigen $x \in \mathbb{Q}(\sqrt{d})$ ganz $/\mathbb{Z}$ (d.h. aus $\mathcal{O}_K$) genau dann, wenn $\mathrm{Tr}(x), \mathrm{N}(x) \in \mathbb{Z}$.

Beweis: Sei x ganz $/\mathbb{Z}$, d.h. x ist Wurzel eines unitären $\mathbb{Z}$-Polynoms $f \in \mathbb{Z}[T]$. Für $x \in \mathbb{Q}$ ist dann $x \in \mathbb{Z}$ (siehe oben). Sei $x \notin \mathbb{Q}$, $p(T) = \mathrm{Irr}(T, x, \mathbb{Q}) = T^2 - \mathrm{Tr}(x)T + \mathrm{N}(x)$. Dieses Polynom teilt f in $\mathbb{Q}(T)$. Nach GAUSS' Lemma, hat p Koeffizienten in $\mathbb{Z}$. Die andere Implikation ist trivial. □

Somit $a+b\sqrt{d} \in \mathcal{O}_K$ genau dann, wenn $2a \in \mathbb{Z}$ und $a^2 - db^2 \in \mathbb{Z}$. Also $a = \frac{r}{2}$, $r \in \mathbb{Z}$, $\frac{r^2}{4} - db^2 \in \mathbb{Z}$.

$b = \frac{s}{2}, s \in \mathbb{Z}$, $\frac{r^2 - ds^2}{4} \in \mathbb{Z}$ genau dann, wenn $r^2 \equiv ds^2 \pmod 4$. Ist $d \equiv 1 \pmod 4$, so gilt die Kongruenz genau dann, wenn $r \equiv s \pmod 2$. Ist $d \equiv 2, 3 \pmod 4$, so gilt die Kongruenz genau dann, wenn $r \equiv s \equiv 0 \pmod 2$. Damit haben wir folgenden Fakt:

Fakt 1.2.15
Sei $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, $d \neq 0, 1$ sqf. Dann ist

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{d}, a, b \in \mathbb{Z}\} & d \equiv 2, 3 \pmod 4 \\ \{\frac{a+b\sqrt{d}}{2}, a, b \in \mathbb{Z}, a \equiv b \pmod 2\} = \{a + b\frac{1+\sqrt{d}}{2}\} & d \equiv 1 \pmod 4 \end{cases}.$$

Fakt 1.2.16
Faktorielle Ringe sind ganzabgeschlossen.

Beweis: Sei K der QK von A, A faktoriell. Sei $x = \frac{r}{s} \in K$, $\mathrm{ggT}(r, s) = 1$, $r, s \in A$.

x ganz $/A$: $\left(\frac{r}{s}\right)^n + a_1 \left(\frac{r}{s}\right)^{n-1} + \ldots + a_n = 0$, $a_j \in A$.

$$r^n + a_1 r^{n-1} s + \ldots + a_n s^n = 0$$

$\Rightarrow s \mid r^n \Rightarrow s \in A^\times \Rightarrow x \in A$. □

Ende VL 3
28.10.14

§1.3 Die Ringe ganzer algebraischer Zahlen I - additive Struktur

L/K endlich, separabel (z.B. mit Charakteristik 0). L ist als K-VR endlich dimensional, $x \in L$ verursacht durch Multiplikation eine K-lineare Abbildung

$$A_x : L \to L : \; y \mapsto xy$$

$\mathrm{Tr}_K^L(x) := \mathrm{Tr}\, A_x$, $\mathrm{N}_K^L(x) = \det(A_x)$.

Ersatz für Galois-Gruppe ist $\mathrm{Hom}_K(L, \overline{K})$. Wegen Separabilität gilt $\#\,\mathrm{Hom}_K(L, \overline{K}) = [L : K] = n$. Sei

$$P_x := \det(T \cdot \mathrm{Id} - A_x),$$

dann gilt

$$\mathrm{Tr}_K^L(x) = - \text{ Koeffizient von } P_x \text{ bei } T^{n-1},$$
$$\mathrm{N}_K^L(x) = (-1)^n \text{ Koeffizient von } P_x \text{ bei } T^0.$$

Fakt 1.3.1
Sei L/K endlich und separabel, dann gilt

- $P_x(T) = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})}(T - \sigma x)$
- $\mathrm{Tr}_K^L(x) = \sum_\sigma \sigma x$
- $\mathrm{N}_K^L(x) = \prod_\sigma \sigma x$

Beweis: Sei zuerst $L = K(x)$, dann ist

$$f(T) = \prod_\sigma (T - \sigma x)$$

das irreduzible Polynom von x über K. Andererseits ist $P_x(x) = \det(x\,\mathrm{Id} - A_x) = 0$. Beide Polynome sind unitär, also $f = P_x$. Das war (i). (ii) und (iii) folgen trivial.

Der allgemeine Fall: $L/E/K$, $E = K(x)$. Wir zeigen $P_x(T) = \mathrm{Irr}(T, x, K)^{[L:E]}$. $L = \underbrace{E \oplus \ldots \oplus E}_{n\text{-mal}}$ als K-VR durch Wahl einer E-Basis von L. A_x lässt diese E invariant. Jede K-Einlagerung $\sigma : E \to \overline{K}$ hat genau n Fortsetzungen zu K-Einlagerungen von L. Also

$$\prod_{\tau \in \mathrm{Hom}_K(L,\overline{K})} (T - \tau x) = \prod_{\sigma \in \mathrm{Hom}_K(E,\overline{K})} (T - \sigma x)^n = \mathrm{Irr}(T, x, K)^n = P_x(T)$$

□

Fakt 1.3.2 (Turmsätze für Spur und Norm)
Seien $M/L/K$ endlich und separabel, dann gilt:

(i) $\mathrm{Tr}_K^M = \mathrm{Tr}_K^L \circ \mathrm{Tr}_L^M$

(ii) $\mathrm{N}_K^M = N_K^L \circ N_L^M$

Fakt 1.3.3
Sei L/K endlich und separabel, dann ist die **Spurform**

$$\mathrm{Tr}_K^L : L \times L \to K : (x, y) \mapsto \mathrm{Tr}_K^L(xy)$$

eine nichtausgeartete, symmetrische K-Bilinearform.

Satz 1.3.4 (Satz vom primitiven Element)
Sei L/K endlich und separabel. Dann gibt es ein $x \in L$ mit $L = K(x)$. In diesem Fall heißt die Erweiterung **einfach** und x **primitives Element**.

Beweis (vom vorherigen Fakt):

$L = K(\theta)$. Dann ist $1, \theta, \theta^2, \ldots, \theta^{n-1}$ ($n = [L : K]$) K-Basis von L. Der Spurform entspricht die Matrix

$$M = \left(\mathrm{Tr}_K^L(\theta^{i+j})\right)_{0 \le i,j \le n-1}.$$

Seien $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$ die K-Einbettungen von L (Anzahl $= n$ wegen separabel). Sei $\theta_i := \sigma_i \theta$ und

$$N = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_n \\ \vdots & \vdots & & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \ldots & \theta_n^{n-1} \end{pmatrix}.$$

Dann gilt $M = N \cdot N^T$, also $\det M = (\det N)^2$. $\det N \neq 0$, wegen θ_i alle verschieden (VANDERMONDE). □

Folgerung 1.3.5
Sei L/K endlich und separabel, $w_1, \ldots, w_n$ K-Basis von L. Die **Diskriminante** von $w_1, \ldots, w_n$ ist definiert als

$$d(w_1, \ldots, w_n) = \det(\sigma_i \omega_j)^2 = \det(\mathrm{Tr}(w_i w_j)).$$

Sie ist stets $\neq 0$

Satz 1.3.6 („Satz 1“: Additive Struktur der Ringe ganzer algebraischer Zahlen)
Sei K algebraischer ZK vom Grad n. Dann ist $\mathcal{O}_K$ freie abelsche Gruppe vom Rang n. D.h. es existieren $w_1, \ldots, w_n \in \mathcal{O}_K$, s.d. jede Zahl aus $\mathcal{O}_K$ sich eindeutig als $\mathbb{Z}$-Linearkombinationen der w_i schreiben lässt.

Definition 1.3.7
Solche $w_1, \ldots, w_n$ heißen **Ganzheitsbasen**.

Beweis: Sei $A = \mathcal{O}_K$, $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Q}$-Basis von K. O.B.d.A. $\alpha_i \in A$ (Mult. mit pos. nat. Zahl). Sei $\alpha_1', \ldots, \alpha_n'$ duale Basis bzgl. Spurform (d.h. $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha_i \alpha_j') = \delta_{ij}$). Wir wählen ein $c \in \mathbb{N} \setminus \{0\}$, s.d. $c\alpha_1', \ldots, c\alpha_n'$ ganz sind (d.h. aus A). Sei $x \in A$, dann sind alle $cx\alpha_i' \in A$. Es gilt $x = m_1\alpha_1 + \ldots + m_n\alpha_n$, $m_j \in \mathbb{Q}$. Dann ist

$$\begin{aligned}\mathrm{Tr}(cx\alpha_i') &= \sum_j \mathrm{Tr}(cm_j \alpha_j \alpha_i') \\ &= \sum_j cm_j \,\mathrm{Tr}(\alpha_j, \alpha_i') = cm_i.\end{aligned}$$

Dabei ist $\mathrm{Tr}(cx\alpha_i') \in \mathbb{Q}$ und ganz $/\mathbb{Z}$. Also $cm_i \in \mathbb{Z}$. D.h. x liegt in der endlich erzeugten abelschen Gruppe

$$B = \mathbb{Z}c^{-1}\alpha_1 + \ldots + \mathbb{Z}c^{-1}\alpha_n.$$

Additive Untergruppen in K sind torsionsfrei, also ist obige Gruppe B frei. A liegt in freier abelscher Gruppe B vom Rang $n = [K : \mathbb{Q}]$. Also ist auch A frei von endlichem Rang $\leq n$. A enthält freie abelsche Gruppe vom Rang n, nämlich $\mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Also hat auch A den Rang n. □

Beispiel 1.3.8
Sei $K = \mathbb{Q}(\zeta_p)$ mit $\zeta_p = e^{2\pi i/p}, p \in \mathbb{P}, p > 2$ (der sogenannte p-te **Kreisteilungskörper**).

$\mathrm{Irr}(T, \zeta_p, \mathbb{Q}) = \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \ldots + T + 1$, denn mit Substitution $T = S + 1$ folgt $\frac{(S+1)^p - 1}{S} = S^{p-1} + \binom{p}{1} s^{p-2} + \ldots + \binom{p}{p-1}$ ist EISENSTEIN-Polynom, also irreduzibel $/\mathbb{Q}$. Somit $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. $K/\mathbb{Q}$ ist normal, die GALOIS-Gruppe ist kanonisch so zu $(\mathbb{Z}/p\mathbb{Z})^\times$ isomorph, via $a \mapsto \sigma_a$, $\sigma_a \zeta_p = \zeta_p^a$. Wir zeigen nun, dass $1, \zeta_p, \ldots, \zeta_p^{p-2}$ eine Ganzheitsbasis ist. Äquivalent ist $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. Jedenfalls ist das eine $\mathbb{Q}$-Basis von K, die ζ_p^a sind alle ganz, also $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_K$. Der Index ist endlich, da beide abelsche Gruppen den Rang $p - 1$ haben[2] .

[2] $A \subset \mathbb{Z}^n$, A frei von $\mathrm{rk}\, A = n \Rightarrow (\mathbb{Z}^n : A) < \infty$: Sei $a_1, \ldots, a_n$ $\mathbb{Z}$-Basis von A. Dann $|\mathbb{Z}/A| = |\frac{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}{a_1\mathbb{Z} \oplus \ldots \oplus a_n\mathbb{Z}}| = |\mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_n\mathbb{Z}| = |\mathbb{Z}/a_1\mathbb{Z}| + \ldots + |\mathbb{Z}/a_n\mathbb{Z}| < \infty$.

Sei $\pi = 1 - \zeta_p$, wir zeigen: π ist irreduzibel in $\mathcal{O}_K$:

$$1 + T + \ldots + T^{p-1} = \prod_{a=1}^{p-1}(T - \zeta_p^a)$$

$T = 1 : p = \prod(1 - \zeta_p^a)$, $\mathrm{N}_{\mathbb{Q}}^K(\pi) = \prod(1 - \zeta_p^a) = p$, $\mathrm{N}_{\mathbb{Q}}^K(1 - \zeta_p^a) = p$ für alle $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Wäre $1 - \zeta_p^r = \alpha \cdot \beta \Rightarrow \mathrm{N}(\alpha)\,\mathrm{N}(\beta) = p$

Lemma 1.3.9 („Lemma 1“)
$\varepsilon \in \mathcal{O}_K$ ist Einheit $\Leftrightarrow \mathrm{N}_{\mathbb{Q}}^K(\varepsilon) = \pm 1$

Beweis: $\varepsilon \cdot \eta = 1 \Rightarrow \underbrace{\mathrm{N}(\varepsilon)}_{\in\mathbb{Z}}\underbrace{\mathrm{N}(\eta)}_{\in\mathbb{Z}} = 1 \Rightarrow \mathrm{N}(\eta) = \pm 1$. Ist $\mathrm{N}(\varepsilon) = \pm 1 = \prod_\sigma \sigma\varepsilon = \varepsilon \cdot \prod_{\sigma \neq \mathrm{Id}} \sigma\varepsilon$. Der zweite Faktor beseteht aus ganzen Zahlen, ist also aus $\mathcal{O}_K$, somit ist ε eine Einheit. □

$p = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$ impliziert $\mathrm{N}(\alpha) = \pm 1$ oder $\mathrm{N}(\beta) = \pm 1$. Also α oder β Einheit. Also sind alle π_r irreduzibel.

$$\pi_r = 1 - \zeta_p^r = \underbrace{(1 - \zeta_p)}_{\pi}(1 + \zeta_p + \ldots + \zeta_p^{r-1}).$$

Also ist $\pi_r = \pi \cdot \varepsilon_r$, $\varepsilon_r = 1 + \zeta_p + \ldots + \zeta_p^{r-1}$ ist Einheit. Die ε_r heißen **Kreiseinheiten**. Es folgt $p = \varepsilon_1\varepsilon_2 \ldots \varepsilon_{p-1}\pi^{p-1}$.

Lemma 1.3.10 („Lemma 2“)
Ist $c \in \mathbb{Z}$ in $\mathcal{O}_K$ durch π teilbar, so ist c in $\mathbb{Z}$ durch p teilbar ($\pi = 1 - \zeta_p$).

Beweis: $c = \pi x$, $x \in \mathcal{O}_K$.
$\mathrm{N}(c) = c^{p-1} = \mathrm{N}(\pi)\,\mathrm{N}(x) = p\underbrace{\mathrm{N}(x)}_{\in\mathbb{Z}}$. Also gilt $p \mid c^{p-1} \Rightarrow p \mid c$. □

Sei nun $x \in \mathcal{O}_K$, $x = a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2}$ mit $a_j \in \mathbb{Q}$.

$$\mathrm{Tr}_{\mathbb{Q}}^K(\zeta_p^r) = \begin{cases} -1 & r \not\equiv 0 \pmod p \\ p - 1 & r \equiv 0 \pmod p \end{cases}$$

Also ist $\mathrm{Tr}(\zeta_p x) = \sum_{j=0}^{p-2} a_j \,\mathrm{Tr}(\zeta_p^{j+1}) = -(a_0 + a_1 + \ldots + a_{p-2})$.

Ende VL 4
29.10.14

$$\begin{aligned} \mathrm{Tr}(\zeta_p^{-r}x) &= (p-1)a_r - \sum_{j\neq r} a_j \qquad \text{mit } 1 \le r \le p-2 \text{ oder } r = 0 \\ &= pa_r - \sum_{j=0}^{p-1} a_j \end{aligned}$$

Nun ist $\zeta_p^{-r}x - \zeta_p x \in \mathcal{O}_K$, also $\mathrm{Tr}(\zeta_p^{-r}x - \zeta_p x) \in \mathbb{Z}$ und folglich $pa_r \in \mathbb{Z}$. Somit

$$px = b_0 + b_1\zeta_p + \ldots + b_{p-2}\zeta_p^{p-2} \qquad b_j \in \mathbb{Z}.$$

Nun Substitution $\zeta_p = 1 - \pi$:

$$px = c_0 + c_1\pi + \ldots + c_{p-2}\pi^{p-2} \qquad c_j \in \mathbb{Z}.$$

π teilt c_0 in $\mathcal{O}_K \overset{L2}{\Longrightarrow} p \mid c_0$ in $\mathbb{Z}$.

$$\Rightarrow px - pd_0 = c_1\pi + \ldots + c_{p-2}\pi^{p-2} \qquad \text{mit } d_0 \in \mathbb{Z}$$

$\pi \mid c_1$ in $\mathcal{O}_K \Rightarrow p \mid c_1$ in $\mathbb{Z} \Rightarrow c_1 = pd_1$ usw. bis

$$px = p(d_0 + d_1\pi + \ldots + d_{p-2}\pi^{p-2}) \qquad d_j \in \mathbb{Z}.$$

Rücksubstitution: $\pi = 1 - \zeta_p \Rightarrow x \in \mathbb{Z}[\zeta_p]$. Wir halten das Ergebnis im folgenden Fakt fest.

Fakt 1.3.11
Sei $2 < p \in \mathbb{P}$, $\zeta_p = e^{2\pi i/p}$ und $K = \mathbb{Q}(\zeta_p)$. Dann $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. Insbesondere ist $1, \zeta_p, \ldots, \zeta_p^{p-2}$ Ganzheitsbasis.

Bemerkung 1.3.12
Mit etwas mehr Aufwand:

$m \geq 2$, $K = \mathbb{Q}(\zeta_m)$, $\zeta_m = e^{2\pi i/m}$, dann ist $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$. (Siehe NEUKIRCH, AlgZT, p. 62ff)

Fakt 1.3.13
Sei K algebraischer Zahlenkörper, $\omega_1, \ldots, \omega_n$ Ganzheitsbasis, dann heißt

$$d_K := \det(\sigma_i\omega_j)^2 = \det(\mathrm{Tr}(\omega_i\omega_j))$$

die **Diskriminante** von K. Sie ist unabhängig von der Wahl der Ganzheitsbasis.

Beweis: Sei $\omega_1', \ldots, \omega_n'$ eine andere Ganzheitsbasis, also $\omega_i' = \sum_j a_{ij}\omega_j$, $a_{ij} \in \mathbb{Z}$ und $\omega_i = \sum_j b_{ij}\omega_j'$, $b_{ij} \in \mathbb{Z}$.
$A = (a_{ij})$, $B = (b_{ij}) \Rightarrow AB = BA = I \Rightarrow \det A = \det B = \pm 1$.
Weiter ist $d(\omega_1', \ldots, \omega_n') = (\det A)^2 \cdot d(\omega_1, \ldots, \omega_n)$. □

Bemerkung 1.3.14
Man hat für beliebige $\omega_1, \ldots, \omega_n \in K$ die **Diskriminante**

$$d(\omega_1, \ldots, \omega_n) = \det(\sigma_i\omega_j)^2 = \det(\mathrm{Tr}(\omega_i\omega_j)).$$

Diese ist $\neq 0$ genau dann, wenn die ω_i $\mathbb{Q}$-linear unabhängig sind. Wie oben sieht man: d ist nur von $\mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ abhängig.

Fakt 1.3.15
Sind $M \subset N \subset K$ zwei additive Untergruppen vom Rang $n = [K : \mathbb{Q}]$, so gilt $d_M = (N : M)^2 d_N$.

Beweis: Sei $\omega_1, \ldots, \omega_n$ Basis von N, $\eta_1, \ldots, \eta_n$ Basis von M, $A = (a_{ij})$ sei definiert durch

$$\eta_i = \sum_j a_{ij}\omega_j, \ a_{ij} \in \mathbb{Z}.$$

Dann ist $d(\eta_1, \ldots, \eta_n) = \det(A)^2 d(\omega_1, \ldots, \omega_n)$. Wir zeigen $(N : M) = |\det(A)|$.

Elementare Zeilenoperationen:

- Vertauschung zweier Zeilen
- Addieren eines Vielfachen einer Zeile zu einer anderen

Das entspricht Linksmultiplikation mit $\mathbb{Z}$-Matrix der det ± 1. Analog kann man Spaltenoperationen mit Rechtsmultiplikationen von $\mathbb{Z}$-Matrizen realisieren. A besitzt betragsmäßig kleinstes Element $\neq 0$. Wir machen es zu a_{11}. Division mit Rest: Man kann in 1. Zeile und 1. Spalte alle Einträge betragsmäßig $< |a_{11}|$ machen: iterieren bis in 1. Zeile und 1. Spalte nur noch a_{11} und Nullen stehen. Nun so weiter: $\exists B, C \in \mathrm{GL}(n, \mathbb{Z})$, s.d.

$$BAC = \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix} = \mathrm{diag}(d_1, \ldots, d_n) = D.$$

Multiplikation mit B und C entspricht Wahl anderer Basen in M und N. Also $d_M = (\det D)^2 d_N$. $(N : M) = |\prod d_i|$ ist klar.

$$\left(\mathbb{Z}^n : \bigoplus_{i=1}^{n} d_i \mathbb{Z} \right) = \prod_{i=1}^{n} (\mathbb{Z} : d_i \mathbb{Z}) = \prod |d_i|$$

□

Folgerung 1.3.16
Sind $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ und $d(\omega_1, \ldots, \omega_n)$ ist quadratfrei, so ist dies Ganzheitsbasis.

Beispiel 1.3.17 (i) $K = \mathbb{Q}(\sqrt{d})$, $d \neq 0, 1$, sqf, $d \in \mathbb{Z}$.

- $d \equiv 1 \pmod 4$: $d_K = \det^2 \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix} = (-\sqrt{d})^2 = d$
- $d \equiv 2, 3 \pmod 4$: $d_K = \det^2 \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} = 4d$

d	-2	-1	2	3	5
d_K	-8	-4	8	12	5

(ii) $K = \mathbb{Q}(\zeta_p)$, $p > 2$ prim, $\zeta_p = e^{2\pi i/p}$

$d_K = \det(\mathrm{Tr}_{\mathbb{Q}}^K(\zeta_p^{i+j}))_{1 \leq i,j \leq p-1}$, denn mit $1, \zeta_p, \ldots, \zeta_p^{p-2}$ ist auch $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ eine Ganzheitsbasis.

$$\mathrm{Tr}(\zeta_p^r) = \begin{cases} -1 & r \not\equiv 0 \pmod p \\ p-1 & r \equiv 0 \pmod p \end{cases}$$

Also

$$d_K = \det \begin{pmatrix} -1 & -1 & \dots & p-1 \\ \vdots & \vdots & & \vdots \\ -1 & p-1 & \dots & -1 \\ p-1 & -1 & \dots & -1 \end{pmatrix} = (-1)^{p(p-1)/2} \det \begin{pmatrix} p-1 & \dots & -1 \\ \vdots & \ddots & \vdots \\ -1 & \dots & p-1 \end{pmatrix}$$

$$= (-1)^{(p-1)/2} \det(pI - A) \qquad \text{mit } A = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{pmatrix}$$

A hat $(p-2)$-fache Eigenwert 0, wegen Rang 1. Der letzte Eigenwert von A ist $p-1$, denn $A \cdot (1, \dots, 1)^T = (p-1)(1, \dots, 1)^T$. Somit ist $\det(\lambda I - A) = \lambda^{p-2}(\lambda - p + 1)$. Nun $\lambda = p$ einsetzen: $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$.

(iii) DEDEKIND

$f = T^3 - T^2 - 2T - 8$

(a) f ist irreduzibel /$\mathbb{Q}$: Angenommen $f(\alpha) = 0$ für ein $\alpha \in \mathbb{Q} \Rightarrow \alpha \in \mathbb{Z} \Rightarrow \alpha \mid 8$ $\Rightarrow \alpha = \pm 1, \pm 2, \pm 4, \pm 8$. Aber das sind alles keine Nullstellen von f.

Für jede Nullstelle $\alpha \in \mathbb{C}$ von f gilt $K = \mathbb{Q}(\alpha)$ hat Grad 3 über $\mathbb{Q}$.

(b) Die Diskriminante von $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$.

$$\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2$$

$$d(1, \alpha, \alpha^2) = \det \begin{pmatrix} \operatorname{Tr} 1 & \operatorname{Tr} \alpha & \operatorname{Tr} \alpha^2 \\ \operatorname{Tr} \alpha & \operatorname{Tr} \alpha^2 & \operatorname{Tr} \alpha^3 \\ \operatorname{Tr} \alpha^2 & \operatorname{Tr} \alpha^3 & \operatorname{Tr} \alpha^4 \end{pmatrix} = \begin{vmatrix} 3 & 1 & 5 \\ 1 & 5 & 31 \\ 5 & 31 & 49 \end{vmatrix} = -4 \cdot \underbrace{503}_{\in \mathbb{P}}$$

$$\begin{aligned} \operatorname{Tr}(1) &= 3 \\ \operatorname{Tr}(\alpha) &= \alpha + \alpha' + \alpha'' = -\text{Koeffizient an } T^2 = 1 \\ \operatorname{Tr}(\alpha^2) &= \alpha^2 + (\alpha')^2 + (\alpha'')^2 = (\alpha + \alpha' + \alpha'')^2 - 2(\alpha\alpha' + \alpha\alpha'' + \alpha'\alpha'') \\ &= 1 - 2(-2) = 5 \\ \operatorname{Tr}(\alpha^3) &= \operatorname{Tr}(\alpha^2 + 2\alpha + 8) = 5 + 2 + 24 = 31 \\ \alpha^4 &= \alpha^3 + 2\alpha^2 + 8\alpha = 3\alpha^2 + 10\alpha + 8 \\ \operatorname{Tr}(\alpha^4) &= 15 + 10 + 24 = 49 \end{aligned}$$

(c) $\beta = \frac{\alpha + \alpha^2}{2}$ ist ganz.

$$\begin{aligned}\beta^2 &= \frac{1}{4}(\alpha^2+2\alpha^3+\alpha^4) = \frac{1}{4}(\alpha^2+2\alpha^2+4a+16+3\alpha^2+10\alpha+8)\\ &= \frac{3}{2}\alpha^2+\frac{7}{2}\alpha+6 = 3\cdot\frac{\alpha+\alpha^2}{2}+2\cdot\alpha+6\\ &= 3\beta+2\alpha+6\\ \alpha\beta &= \frac{1}{2}(\alpha^3+\alpha^2) = \frac{1}{2}(2\alpha^2+2\alpha+8) = \alpha^2+\alpha+4\\ &= 2\beta+4\end{aligned}$$

Also gilt $\beta M \subset M$ für $M = \mathbb{Z}+\mathbb{Z}\alpha+\mathbb{Z}\beta$. Es folgt: Index ist 2 und $\mathcal{O}_K$ hat Ganzheitsbasis $1, \alpha, \frac{\alpha+\alpha^2}{2}$. $d_K = -503$.

(d) 2 ist ein außerwesentlicher Diskriminantenteiler. Für alle $\gamma \in \mathcal{O}_K \setminus \mathbb{Z}$ hat $\mathbb{Z}[\gamma]$ einen durch 2 teilbaren Index in $\mathcal{O}_K$. Insbesondere ist $\mathbb{Z}[\gamma] \neq \mathcal{O}_K$.

Sei dazu $\gamma = a+b\alpha+c\beta : a,b,c \in \mathbb{Z}$, b,c nicht beide $= 0$. Wir wissen $\beta^2 = 3\beta+2\alpha+6$, $\alpha\beta = 2\beta+4$, $\alpha^2 = 2\beta-\alpha$.

Übergangsmatrix zwischen $1,\alpha,\beta$ und $1,\gamma,\gamma^2$:

$$\begin{aligned}1 &= 1\\ \gamma &= a+b\alpha+c\beta\\ \gamma^2 &= a^2+2ab\alpha+ac\beta+b^2\alpha^2+2bc\alpha\beta+c^2\beta^2\\ &= (a^2+8bc+6c^2)+(2ab-b^2+2c^2)\alpha+(2ac+2b^2+4bc+3c^2)\beta\end{aligned}$$

$$\det\begin{pmatrix}1 & a & a^2+8bc+6c^2\\ 0 & b & 2ab-b^2+2c^2\\ 0 & c & 2ac+2b^2+4bc+3c^2\end{pmatrix} \equiv \det\begin{pmatrix}1 & a & a^2\\ 0 & b & b^2\\ 0 & c & c^2\end{pmatrix} \equiv bc(c-b) \equiv 0 \pmod 2$$

Ende VL 5
04.11.14

§1.4 Die Ringe ganzer algebraischer Zahlen II - mult. Struktur

Satz 1.4.1 („Satz 2“)
Sei K ein algebraischer ZK, $\mathcal{O}_K$ der Ring der ganzen algebraischen Zahlen. Dann ist $\mathcal{O}_K$ NOETHERsch, ganzabgeschlossen und jedes Primideal $\neq (0)$ ist maximal.

Beweis:

(i) Ganzabgeschlossen ist klar: $\mathcal{O}_K$ ist der ganze Abschluss von $\mathbb{Z}$ in K und ganz sein ist transitiv.

(ii) Sei $\mathfrak{a} \subset \mathcal{O}_K$ Ideal, dann ist $\mathfrak{a}$ additive Untergruppe in $\mathcal{O}_K$, frei von endlichem Rang, also auch $\mathfrak{a}$ frei von endlichem Rang. Somit ist $\mathfrak{a}$ als $\mathcal{O}_K$-Modul endlich erzeugt. Das liefert NOETHERsch.

(iii) Sei $\mathfrak{p} \subset \mathcal{O}_K$ Primideal $\neq (0)$. Dann enthält $\mathfrak{p}$ auch orthodoxe ganze Zahlen $\neq 0$. Sei $x \in \mathfrak{p} \setminus \{0\}$, $\mathrm{N}(x) = \prod \sigma x$ ist ganz und aus $\mathbb{Q}$, also aus $\mathbb{Z}$. Somit enthält $\mathfrak{p}$ positive natürliche Zahlen. Sei $m > 0$ die kleinste, dann gilt $(m) = m\mathcal{O}_K \subset \mathfrak{p} \subset \mathcal{O}_K$. Nun gilt

$$(\mathcal{O}_K : m\mathcal{O}_K) = m^{[K:\mathbb{Q}]}.$$

Also hat $m\mathcal{O}_K$ endlichen Index in $\mathcal{O}_K$, also auch $\mathfrak{p}$. Somit ist $\mathcal{O}_K/\mathfrak{p}$ endlicher, integer Ring, also ein Körper.

□

Bemerkung 1.4.2
Das sind geometrische Eigenschaften.

- ganzabgeschlossen bedeutet: ohne Singularität
- Primideal $\neq (0)$ sind maximal bedeutet Dimension von $\mathcal{O}_K$ ist 1
- „Schemata“ (GROTHENDIEK)

Definition 1.4.3
Ein integer, kommutativer Ring mit 1 heißt **DEDEKIND-Ring**, wenn er NOETHERsch, ganzabgeschlossen und der Dimension 1 ist, also jedes Primideal $\neq (0)$ ist maximal.

Satz 1.4.4 („Satz 3“: Primidealzerlegung in DEDEKIND-Ringen)
Jedes Ideal $\neq (0), (1)$ in einem DED-Ring besitzt eine Zerlegung in Primideale:

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n.$$

Diese ist bis auf Reihenfolge eindeutig bestimmt.

Beweis (VAN DER WAERDEN):

(i) Sei $\mathfrak{a} \neq (0)$ Ideal in DED-Ring A. Wir zeigen: $\exists \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ maximal, s.d. $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset \mathfrak{a}$.

Indirekt. Sei φ die Menge aller Ideale $\neq (0)$, für welche das nicht gilt. A NOETHERsch $\Rightarrow \varphi$ besitzt maximale Elemente, sei $\mathfrak{a}$ ein solches. $\mathfrak{a}$ selbst ist natürlich nicht prim. Also ex. $x, y \in A$ mit $x \notin \mathfrak{a}, y \notin \mathfrak{a}$, aber $xy \in \mathfrak{a}$. Seien $\mathfrak{a}_1 = (\mathfrak{a}, x)$, $\mathfrak{a}_2 = (\mathfrak{a}, y)$, dann ist $\mathfrak{a}_1 \supsetneq \mathfrak{a}$ und $\mathfrak{a}_2 \supsetneq \mathfrak{a}$ und $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$. Wegen der Maximalität von $\mathfrak{a}$ enthalten $\mathfrak{a}_1$ und $\mathfrak{a}_2$ Produkte von maximalen Idealen, also auch $\mathfrak{a}$ selbst. $\lightning$

(ii) Sei $\mathfrak{p}$ maximales Ideal in A. Wir definieren:

$$\mathfrak{p}^{-1} = \{x \in K : x\mathfrak{p} \subset A\}, \qquad K = \mathrm{QK}(A).$$

Es gilt $A \subset \mathfrak{p}^{-1}$, $\mathfrak{p}^{-1}$ ist abgeschlossen unter Addition und $y\mathfrak{p}^{-1} \subset \mathfrak{p}^{-1}$ für alle $y \in A$. D.h. $\mathfrak{p}^{-1}$ hat alle Eigenschaften eines A-Ideals, außer der in A zu liegen. Wir zeigen $\mathfrak{p}^{-1} \neq A$. Sei dazu $x \in \mathfrak{p}$, $x \neq 0$ und r die kleinste positive natürliche Zahl, s.d. $\exists \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ mit $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset (x)$. Dann muss wenigstens eines der $\mathfrak{p}_i$ in $\mathfrak{p}$ liegen: Gibt es $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ für alle i, so gilt $x_1 \ldots x_r \in \mathfrak{p}_1 \ldots \mathfrak{p}_r$, aber $x_1 \ldots x_r \notin \mathfrak{p}$. Ohne Einschränkung $\mathfrak{p}_1 \subset \mathfrak{p}$. Es folgt $\mathfrak{p}_1 = \mathfrak{p}$. Weiter ist $\mathfrak{p}_2 \ldots \mathfrak{p}_r \not\subset (x)$, wegen r minimal. Also existiert ein $y \in \mathfrak{p}_2 \ldots \mathfrak{p}_r$ mit $y \notin (x)$. Aber $y\mathfrak{p} \subset (x) \Rightarrow x^{-1}y\mathfrak{p} \subset A \Rightarrow x^{-1}y \in \mathfrak{p}^{-1}$. Nun ist $x^{-1}y \notin A$, denn wäre $x^{-1}y = a \in A$, so folgt $y = ax \in (x)$ $\lightning$. Also $\mathfrak{p}^{-1} \supsetneq A$.

(iii) Wir haben $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset A$ (wobei $\mathfrak{p}\mathfrak{p}^{-1} = \{\sum xy : x \in \mathfrak{p}, y \in \mathfrak{p}^{-1}\}$)

Da $\mathfrak{p}\mathfrak{p}^{-1}$ ein A-Ideal ist, folgt $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ oder $\mathfrak{p}\mathfrak{p}^{-1} = A$. Wir zeigen letzteres. Indirekt: Sei $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Also überführt jedes $x \in \mathfrak{p}^{-1}$ den endlich erzeugten A-Modul $\mathfrak{p}$ in sich selbst. $x\mathfrak{p} \subset \mathfrak{p}$. Also ist x ganz $/A$, also $x \in A$. $\lightning$.

(iv) Sei φ die Menge aller Ideale $\neq (0), (1)$ ohne Primidealzerlegung und sei $\mathfrak{a} \in \varphi$ maximal. Dann liegt $\mathfrak{a}$ im maximalen Ideal $\mathfrak{p}$. Also

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = A.$$

$\mathfrak{a}\mathfrak{p}^{-1}$ ist echt größer also $\mathfrak{a}$, da sonst $\mathfrak{p}^{-1}$ nur ganze Elemente enthielte. Weiter ist $\mathfrak{a}\mathfrak{p}^{-1}$ ein A-Ideal. Mithin besitzt $\mathfrak{a}\mathfrak{p}^{-1}$ die Zerlegung

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_m$$

in maximale Ideale. Es folgt $\mathfrak{a} = \mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_m \lightning$

(v) Eindeutigkeit. Ist $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$, so folgt $\mathfrak{a} \subset \mathfrak{p}$ oder $\mathfrak{b} \subset \mathfrak{p}$.

Ist $x \in \mathfrak{a} \setminus \mathfrak{p}$, $y \in \mathfrak{b} \setminus \mathfrak{p} \Rightarrow xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$ $\lightning$.

Ist $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$, so folgt $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \mathfrak{q}_1 \Rightarrow \mathfrak{p}_1 \subset \mathfrak{q}_1 \Rightarrow \mathfrak{p}_1 = \mathfrak{q}_1$. Multiplikation mit $\mathfrak{p}^{-1}$ gibt $\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s$. Nun IV benutzbar. IA: $\mathfrak{p}_1 \dots \mathfrak{p}_m = A \Rightarrow m = 0$.

□

Wir klären, was $\mathfrak{p}^{-1}$ ist:

Definition 1.4.5
Sei A DEDEKIND-Ring, K sein QK. Ein **gebrochenes Ideal** von A ist ein A-Modul $\mathfrak{a} \subset K$, s.d. ein $c \in A \setminus \{0\}$ existiert mit $c\mathfrak{a} \subset A$. Man schließt (0) aus.

Bemerkung 1.4.6
$c\mathfrak{a}$ ist dann gewöhnliches Ideal. Alle Ideale sind gebrochene Ideale: $c = 1$. Gebrochene Ideale sind endlich erzeugte A-Moduln.

Mantra: Die Nenner der Elemente aus gebrochene Ideal sind beschränkt.

Beispiel 1.4.7 (i) $\{\frac{a}{p} : a \in \mathbb{Z}\}$ ist gebrochenes Ideal von $\mathbb{Q}$. Aber $\{\frac{a}{p^m} : a \in \mathbb{Z}, m \in \mathbb{N}\}$ ist keins.

(ii) Ist A DED-Ring + HIR, dann sind die gebrochenene Ideale der Form $(x) = Ax$, $x \in K^\times$.

(iii) Gebrochene Hauptideale: Jedes $x \in K^\times$ erzeugt gebrochenes Ideal $(x) = Ax$.

(iv) Das $\mathfrak{p}^{-1}$ aus dem Beweis ist ein gebrochenes Ideal. Es ist A-Modul (klar) und für $c \in \mathfrak{p} \setminus \{0\}$ gilt $c\mathfrak{p}^{-1} \subset A$.

Bemerkung 1.4.8
Es gelten für gebrochene Ideale die selben Rechenregeln, wie für die üblichen Ideale.

Fakt 1.4.9
Sei A DEDEKIND-Ring, K der QK, $\mathfrak{a} \subset K$ gebrochenes Ideal, dann ist auch

$$\mathfrak{b} = \{x \in K : x\mathfrak{a} \subset A\}$$

ein gebrochenes Ideal und $\mathfrak{a}\mathfrak{b} = (1) = A$. D.h. die gebrochenen Ideale von A bilden bzgl. Multiplikation eine abelsche Gruppe Id_A. Man schreibt $\mathfrak{b} = \mathfrak{a}^{-1}$.

Beweis: Sei zuerst $\mathfrak{a}$ gewöhnliches Ideal in A. Dann gilt $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$. Setze $\mathfrak{c} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$. Es folgt $\mathfrak{a}\mathfrak{c} = A$, also $\mathfrak{c} \subset \mathfrak{b}$. Sei $x \in \mathfrak{b} \Rightarrow x\mathfrak{a} \subset A \Rightarrow x\mathfrak{a}\mathfrak{c} \subset \mathfrak{c} \Rightarrow xA \subset \mathfrak{c} \Rightarrow x \in \mathfrak{c} \Rightarrow \mathfrak{b} \subset \mathfrak{c}$.

$\mathfrak{c}$ ist gebrochenes Ideal, da die $\mathfrak{p}_i^{-1}$ es sind und Produkte gebrochener Ideale wieder gebrochene Ideale sind:

$$c\mathfrak{a} \subset A, d\mathfrak{b} \subset A \Rightarrow (cd)\mathfrak{a}\mathfrak{b} \subset A.$$

Sei nun $\mathfrak{a}$ gebrochenes Ideal, $c \in A \setminus \{0\}$, s.d. $c\mathfrak{a} \subset A$. $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$, genauer zeigen wir: $c(c\mathfrak{a})^{-1}$ ist reziprok zu $\mathfrak{a}$: $c(c\mathfrak{a})^{-1}\mathfrak{a} = A$. Das ist äquivalent zu $(c\mathfrak{a})^{-1}(c\mathfrak{a}) = A$, und das ist richtig. Somit $\mathfrak{a}^{-1} = c(c\mathfrak{a})^{-1}$, $(c\mathfrak{a})^{-1}$ ist gebrochenes Ideal, also auch $c(c\mathfrak{a})^{-1}$. □

Folgerung 1.4.10
Id_A ist freie abelsche Gruppe, jedes $\mathfrak{a} \in \mathrm{Id}_A$ hat eindeutige Darstellung

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})}$$

$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$, fast alle $= 0$ (alle bis auf endl. viele).

Ende VL 6
11.11.14

Beispiel 1.4.11

$$\mathrm{Id}_{\mathbb{Z}} = \prod_{p \in \mathbb{P}} \langle p \rangle$$

Beispiel 1.4.12
$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[-5]$, denn $-5 = 3 \pmod 8$. Es gilt $21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$. Wir haben gesehen, dass dies zwei Faktorisierungen in irreduzible Faktoren sind.

$$\begin{aligned}
\mathfrak{p}_1 &= (3) + (4 + \sqrt{-5}) = (3, 4 + \sqrt{-5}) \\
&= \{(a + b\omega)3 + (c + d\omega)(4 + \omega), a, b, c, d \in \mathbb{Z}\} \qquad \omega = \sqrt{-5} \\
\mathfrak{p}_2 &= (3, 4 - \omega) \\
\mathfrak{p}_3 &= (7, 4 + \omega) \\
\mathfrak{p}_4 &= (7, 4 - \omega)
\end{aligned}$$

Basis von $\mathcal{O}_K$ ist $1, \omega$. Wir bilden $I = \mathbb{Z} \cdot 3 + \mathbb{Z} \cdot (4 + \omega) \subset \mathfrak{p}_1$. Es gilt

$$\begin{aligned}
\omega \cdot 3 &= 3(4 + \omega) - 4 \cdot 3 \in I \\
\omega \cdot (4 + \omega) &= 4(4 + \omega) - 7 \cdot 3 \in I
\end{aligned}$$

$\Rightarrow (a + b\omega)3 + (c + d\omega)(4 + \omega) \in I \Rightarrow \mathfrak{p}_1 \subset I$.

Also ist 3, $4 + \omega$ eine Basis von $\mathfrak{p}_1$. Der Index von $\mathfrak{p}_1$ in $\mathcal{O}_K$ ist daher

$$\left| \det \begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix} \right| = 3$$

Somit ist $\mathcal{O}_K/\mathfrak{p}_1 = \mathbb{F}_3 \Rightarrow \mathfrak{p}_1$ maximal. Es folgt $\mathcal{O}_K/\mathfrak{p}_2 = \mathbb{F}_3$.

Wir zeigen 7, $4 + \omega$ ist $\mathbb{Z}$-Basis von $\mathfrak{p}_3$:

$$\begin{aligned}
\omega \cdot 7 &= 7(4 + \omega) - 4 \cdot 7 \in I \\
\omega \cdot (4 + \omega) &= 4(4 + \omega) - 3 \cdot 7 \in I
\end{aligned}$$

Also $(\mathcal{O}_K : \mathfrak{p}_3) = \left| \det \begin{pmatrix} 7 & 4 \\ 0 & 1 \end{pmatrix} \right| = 7 \Rightarrow \mathcal{O}_K/\mathfrak{p}_3 = \mathcal{O}_K/\mathfrak{p}_4 = \mathbb{F}_7$

Wir zeigen $\mathfrak{p}_1\mathfrak{p}_2 = (3) = 3 \cdot \mathcal{O}_K$: Jedenfalls ist $\mathfrak{p}_1\mathfrak{p}_2 \subset (3)$, denn es gilt:

$$(3x + (4+\omega)y)(3z + (4-\omega)w) = 9xz + 3(4-\omega)xw + 3(4+\omega)yz + 21yw$$

Dies ist Vielfaches von 3, also auch jede Summe solcher Elemente. Nun schauen wir uns spezielle Elemente an:

$$\begin{aligned} r :=& (3-(4+\omega))(3-(4-\omega)) = (-1-\omega)(-1+\omega) \\ =& (1-\omega^2) = 6 \\ s :=& (6-(4+\omega))(6-(4-\omega)) = (2+\omega)(2-\omega) \\ =& 4+5 = 9 \end{aligned}$$

$r, s \in \mathfrak{p}_1 \cdot \mathfrak{p}_2,\ s - r = 3\ \Rightarrow 3 \in \mathfrak{p}_1\mathfrak{p}_2\ \Rightarrow (3) \subset \mathfrak{p}_1\mathfrak{p}_2$.
Analog erhält man $\mathfrak{p}_3\mathfrak{p}_4 = (7)$, $\mathfrak{p}_1\mathfrak{p}_3 = (4+\omega)$ und $\mathfrak{p}_2\mathfrak{p}_4 = (4-\omega)$. Wir zeigen noch $\mathfrak{p}_1\mathfrak{p}_3 = (4+\omega)$:

$$(3x + (4+\omega)y)(7z + (4+\omega)w) = 21xz + 7(4+\omega)yz + 3(4+\omega)xw + (4+\omega)^2yw$$

Wegen $21 = (4+\omega)(4-\omega)$ folgt $\mathfrak{p}_1\mathfrak{p}_3 \subset (4+\omega)$. Spezielle Elemente:

$$\begin{aligned} r :=& (3-(4+\omega))(7-(4+\omega)) = (-1-\omega)(3-\omega) \\ =& -3+\omega-3\omega-5 = -8-2\omega = -2(4+\omega) \\ s :=& (6-(4+\omega))(7-2(4+\omega)) = (2-\omega)(-1-2\omega) \\ =& -2-4\omega+\omega-10 = -12-3\omega = -3(4+\omega) \end{aligned}$$

$\Rightarrow r - s = 4 + \omega \in \mathfrak{p}_1\mathfrak{p}_3\ \Rightarrow (4+\omega) \subset \mathfrak{p}_1\mathfrak{p}_3$.

Fakt 1.4.13
Sei A DED-Ring. Dann gilt:

$$A \text{ faktoriell } \Leftrightarrow A \text{ Hauptidealring}$$

Beweis: Ist A HIR, so folgt A faktoriell auch ohne DEDEKIND-Eigenschaft (Algebra 1). Sei nun A faktorieller DEDEKIND-Ring und $\mathfrak{p} \subset A$ Primideal. Sei $x \in \mathfrak{p}$, $x \neq 0$, dann gilt

$$x = \pi_1 \dots \pi_n \text{ mit irred. El. } \pi_i.$$

Dann existiert ein π_j mit $\pi_j \in \mathfrak{p}$, also $(\pi_j) \subset \mathfrak{p}$. (π) ist Primideal für irreduzibles π: $x, y \in A$, $xy \in (\pi)\ \Rightarrow xy = \pi z \Rightarrow \pi \mid xy\ \Rightarrow \pi \mid x$ oder $\pi \mid y$ (denn A faktoriell). Also (π_j) prim, $\neq (0)$ und somit $\mathfrak{p} = (\pi_j)$. □

§1.5 Die Idealklassengruppe

Sei K algebraischer Zahlkörper. Wir haben einen kanonischen Homomorphismus

$$K^\times \to \mathrm{Id}_K = \mathrm{Id}_{\mathcal{O}_K},\ x \mapsto x\mathcal{O}_K.$$

Fakt 1.5.1
Der Kern dieses HM ist die Einheitengruppe E_K (oder U_K) $= \mathcal{O}_K^\times$ von $\mathcal{O}_K$.

Beweis: Ist $\varepsilon \in \mathcal{O}_K$ Einheit, so ist $(\varepsilon) = (1) = \mathcal{O}_K$. Sei $\alpha \in K^\times$ und $(\alpha) = (1)$. D.h. es ex. $\beta \in \mathcal{O}_K$ mit $\alpha\beta = 1$. Nun ist auch $(\alpha^{-1}) = (1)$, also ex. $\gamma \in \mathcal{O}_K$ mit $\alpha^{-1}\gamma = 1 \Rightarrow \alpha \in \mathcal{O}_K$, aus $\alpha\beta = 1$ folgt $\alpha \in \mathcal{O}_K^\times$. □

Beispiel 1.5.2
Sei $K = \mathbb{Q}(\sqrt{2}) \supset \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ und $\varepsilon = 1 + \sqrt{2}$. Wegen $(1 + \sqrt{2})(1 - \sqrt{-2}) = -1$ folgt ε ist Einheit. ε hat unendliche Ordnung, wegen Betrag > 1. $\Rightarrow$ unendliche Einheitengruppe.

Definition 1.5.3
Der Cokern[3] dieses HM heißt **Idealklassengruppe** von K. Bezeichnung: Cl_K. Also

$$\mathrm{Cl}_K = \frac{\text{gebr. Ideale}}{\text{gebr. Hauptideale}}$$

Bemerkung 1.5.4
Cl_K misst also die Abweichung von $\mathcal{O}_K$ davon HIR zu sein. Cl_K ist abelsche Gruppe. Cl_K is die wichtigste und mysteriöseste Invariante eines algebraischen Zahlenkörpers.

Beispiel 1.5.5 (i) $\mathbb{Z}, \mathbb{Z}[i]$ sind HIR, also ist für $\mathbb{Q}$, $\mathbb{Q}(i)$ jeweils $\mathrm{Cl}_K = 1$.

(ii) $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell, also kein HIR. Also $\mathrm{Cl}_K \neq 1$.

Wir zeigen $\mathfrak{p}_1 = (3, 4 + \sqrt{-5})$ ist kein Hauptideal. Indirekt: $\mathfrak{p}_1 = (a + b\sqrt{-5}) \Rightarrow$ Jedes Element aus $\mathfrak{p}_1$ hat durch $a^2 + 5b^2$ teilbare Norm. Also teilt $a^2 + 5b^2$ die Norm $\mathrm{N}(3) = 9$ und $\mathrm{N}(4 + \sqrt{-5}) = 21$. Also teilt $a^2 + 5b^2$ die Zahl $3 = \mathrm{ggT}(21, 9)$. $\Rightarrow a = \pm 1$, $b = 0$ $\Rightarrow \mathfrak{p}_1 = \mathcal{O}_K$ ↯.

Definition 1.5.6
Sei K algebraischer Zahlkörper und $\mathfrak{a} \subset \mathcal{O}_K$ Ideal, $\mathfrak{a} \neq (0)$. Wir definieren die **Absolutnorm** $\mathbb{N}\mathfrak{a}$ durch

$$\mathbb{N}(\mathfrak{a}) := (\mathcal{O}_K : \mathfrak{a}) = \mathrm{card}\, \mathcal{O}_K/\mathfrak{a}.$$

Fakt 1.5.7 (Chinesischer Restsatz)
Sei A kommutativer Ring mit 1, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise verschiedene Primideale, $\mathfrak{a}_i + \mathfrak{a}_j = A$ für alle $i \neq j$. Dann ist der kanonische HM

$$A \to A/\mathfrak{a}_1 \oplus A/\mathfrak{a}_2 \oplus \ldots \oplus A/\mathfrak{a}_n$$

surjektiv, der Kern ist $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \ldots \mathfrak{a}_n$.

Bemerkung 1.5.8
Das ist ein Resultat der kommutativen Algebra, keine Zahlentheorie.

Beweis: Für zwei Ideale $\mathfrak{a}, \mathfrak{b}$, gilt sicher $\mathfrak{ab} \subset \mathfrak{a}, \mathfrak{b}$, also $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Sei $\mathfrak{a} + \mathfrak{b} = A$, dann folgt $\exists x \in \mathfrak{a}, y \in \mathfrak{b}$: $x + y = 1$. Ist $z \in \mathfrak{a} \cap \mathfrak{b}$, so ist $z = z(x + y) = zx + zy \in \mathfrak{ab}$. Daher $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. Das nehmen wir als Induktionsanfang und verallgemeinern: $\mathfrak{a}_i + \mathfrak{a}_n = A \Rightarrow \exists x_i \in \mathfrak{a}_i, y_i \in \mathfrak{a}_n$ mit

[3] Für einen Homomorphismus $f : A \to B$ ist $\mathrm{Coker}\, f = B/\mathrm{Img}\, f$. Damit erhält man die exakte Sequenz $0 \to \mathrm{Ker}\, f \to A \xrightarrow{f} B \to \mathrm{Coker}\, f \to 0$.

$x_i + y_i = 1$, für $i = 1, \ldots, n-1$. Sei $\mathfrak{b} = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_{n-1} = \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}$.

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{\mathfrak{a}_n}$$

Also ist $\mathfrak{b} + \mathfrak{a}_n = A$: $\prod_{i=1}^{n-1} x_i \in \mathfrak{b}$, $\prod_{i=1}^{n-1} x_i = 1 + y$ mit $y \in \mathfrak{a}_n \Rightarrow 1 = \prod_i x_i - y$. Nach Induktionsanfang folgt $\mathfrak{b} \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{b} \cdot \mathfrak{a}_n = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$.

Zur Surjektivität: Fixiere i: $\exists x_j \in \mathfrak{a}_i$, $y_j \in \mathfrak{a}_j$, $j \neq i$ mit $x_j + y_j = 1$. Sei $x = \prod_{j \neq i}(1 - x_j) \in A$. x liegt in jedem $\mathfrak{a}_j$ für $j \neq i$ und ist $\equiv 1 \pmod{\mathfrak{a}_i}$. Also hat x das Bild $(0, \ldots, 0, \underset{\substack{\uparrow \\ i\text{-te}}}{1}, 0, \ldots, 0)$. □

Bemerkung 1.5.9
Für DED-Ringe haben wir scheinbar zwei Definitionen für relativ prim (d.h. teilerfremd):

- $\mathfrak{a} + \mathfrak{b} = A$
- $\mathfrak{a}, \mathfrak{b}$ haben keine gemeinsamen Primidealteiler.

Wir zeigen deren Äquivalenz.

Beweis:

(i) $\mathfrak{p} \mid \mathfrak{a}$, $\mathfrak{p} \mid \mathfrak{b} \Rightarrow \mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{b} \subset \mathfrak{p} \Rightarrow \mathfrak{a} + \mathfrak{b} \subset \mathfrak{p} \Rightarrow \mathfrak{a} + \mathfrak{b} \subsetneq A$.

Also $\mathfrak{a} + \mathfrak{b} = A \Rightarrow \mathfrak{a}, \mathfrak{b}$ haben keine gemeinsamen Primteiler.

(ii) Ist $\mathfrak{a} + \mathfrak{b} \subsetneq A$, so existiert maximales Ideal $\mathfrak{p}$ mit $\mathfrak{a} + \mathfrak{b} \subset \mathfrak{p}$. Es folgt $\mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{b} \subset \mathfrak{p} \Rightarrow \mathfrak{p} \mid \mathfrak{a}, \mathfrak{b}$.

Also: Haben $\mathfrak{a}$ und $\mathfrak{b}$ keine gemeinsamen Primidealteiler, so folgt $\mathfrak{a} + \mathfrak{b} = A$.

Wir haben benutzt: $\mathfrak{p} \mid \mathfrak{a} \Leftrightarrow \mathfrak{a} \subset \mathfrak{p}$, was wir jetzt zeigen: $\mathfrak{p} \mid \mathfrak{a} \Rightarrow \exists \mathfrak{b} \subset A$ mit $\mathfrak{a} = \mathfrak{p} \cdot \mathfrak{b}$ $\Rightarrow \mathfrak{a} \subset \mathfrak{p}$. Ist $\mathfrak{a} \subset \mathfrak{p}$, so ist $\mathfrak{p}^{-1}\mathfrak{a} \subset A$, d.h. $\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{b}$ Ideal in A. Multiplikation mit $\mathfrak{p}$ gibt $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$.

□

Ende VL 7
12.11.14

Fakt 1.5.10
Sei K ein algebraischer ZK und $\mathfrak{a}, \mathfrak{b}$ Ideale in $\mathcal{O}_K \neq (0)$. Dann gilt $\mathbb{N}(ab) = \mathbb{N}(a)\mathbb{N}(b)$.

Beweis: g.z.z. $\mathbb{N}(\mathfrak{p}^e) = (\mathbb{N}\mathfrak{p})^e$

Wir betrachten $\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \ldots \supset \mathfrak{p}^e$. Sicher sind dabei alle Inklusionen echt.

$\mathcal{O}_K/\mathfrak{p}$ ist endlicher Körper, $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ist VR über $O_k/\mathfrak{p}$. Wir zeigen er hat Dimension 1. Sei dazu $x \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, $b := (x) + \mathfrak{p}^{i+1}$ ist Ideal in $\mathcal{O}_K$. Es gilt $\mathfrak{p}^i \supset b \supsetneq \mathfrak{p}^{i+1}$. Multiplikation mit $\mathfrak{p}^{-i}$ gibt $\mathcal{O}_K \supset b\mathfrak{p}^{-i} \supsetneq \mathfrak{p}$ maximal $\Rightarrow \mathcal{O}_K = b\mathfrak{p}^{-i} \Rightarrow b = \mathfrak{p}^i \Rightarrow x \pmod{\mathfrak{p}^i}$ ist Basis.

□

Folgerung 1.5.11
$\mathbb{N}$ setzt sich zu HM $\mathbb{N} : \mathrm{Id}_K \to \mathbb{R}_+^*$ fort, durch

$$\mathfrak{a} = \prod \mathfrak{p}^{\nu_\mathfrak{p}} \mapsto \mathbb{N}\mathfrak{a} = \prod (\mathbb{N}\mathfrak{p})^{\nu_\mathfrak{p}}$$

Bemerkung 1.5.12
In §1.4 hatten wir Diskriminanten für Ideale definiert: Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ ($n = [K : \mathbb{Q}]$), so ist

$$d(\mathfrak{a}) = \det^2(\sigma_i \alpha_j) = \det \mathrm{Tr}(\alpha_i \alpha_j).$$

d ist unabhängig von der Basiswahl. Für $\mathfrak{a} \supset \mathfrak{b}$ gilt $d(\mathfrak{b}) = (\mathfrak{a} : \mathfrak{b})^2 d(\mathfrak{a})$

Fakt 1.5.13
Sei $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, dann ist

$$\mathbb{N}((\alpha)) = |\,\mathrm{N}_{\mathbb{Q}}^K(\alpha)|.$$

Beweis: $d((\alpha)) = (\mathcal{O}_K : (\alpha))^2 d_K$. Ist $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ Ganzheitsbasis von $\mathcal{O}_K$, so ist $\alpha\omega_1, \ldots, \alpha\omega_n$ $\mathbb{Z}$-Basis von $(\alpha) = \alpha\mathcal{O}_K$. Somit

$$d((\alpha)) = \det^2(\sigma_i(\alpha\omega_j)) = \det^2(\sigma_i(\alpha)\sigma_i(w_j)) = \prod_i (\sigma_i \alpha)^2 \det^2(\sigma_i \omega_j) = (\mathrm{N}_{\mathbb{Q}}^K\, \alpha)^2 d_k.$$

□

Satz 1.5.14 („Satz 4“: Endlichkeit der Klassengruppe)
Für jeden alg. ZK K ist die Idealklassengruppe Cl_K endlich.

Beweis: Sei $n = [K : \mathbb{Q}]$, $\omega_1, \ldots, \omega_n$ Ganzheitsbasis. Sei weiter $\mathfrak{a} \subset \mathcal{O}_K$ Ideal.

$$S := \left\{ \sum_{i=1}^{n} a_i \omega_i : 0 \leq a_i \leq (\mathbb{N}\mathfrak{a})^{1/n} + 1, a_i \in \mathbb{Z} \right\}$$

Dann ist $\mathrm{card}\, S > \mathbb{N}\mathfrak{a} : \mathrm{card}\, S \geq ([(\mathbb{N}\mathfrak{a})^{1/n} + 1] + 1)^n > \mathbb{N}\mathfrak{a}$, wg. $[x + 1] > x$. Nach DIRICHLET-Schubfachschluss ex. also $\alpha, \beta \in S$, $\alpha \neq \beta$ mit $\alpha - \beta = \xi \in \mathfrak{a}$. Das heißt $(\xi) = \mathfrak{a} \cdot \mathfrak{b}$ mit ganzem Ideal $\mathfrak{b}$. Es gilt $|\,\mathrm{N}_{\mathbb{Q}}^K(\xi)| = \prod_\sigma |c_1 \sigma\omega_1 + \ldots + c_n \sigma\omega_n|$ mit $c_i \in \mathbb{Z}, 0 \leq |c_i| \leq (\mathbb{N}\mathfrak{a})^{1/n} + 1$. Man sieht $\exists C > 0$, s.d. $|\,\mathrm{N}(\xi)| \leq C\mathbb{N}(\mathfrak{a})$, daher hängt C nur von $\omega_1, \ldots, \omega_n$ ab, nicht von $\mathfrak{a}$. Wegen $(\xi) = \mathfrak{a}\mathfrak{b}$ folgt: $\mathbb{N}\mathfrak{b} \leq C$, $\mathfrak{b}$ liegt in der selben Idealklasse wie $\mathfrak{a}^{-1}$.

Wir haben gezeigt: In jeder Idealklasse gibt es ganze Ideale mit Absolutnorm $\leq C$. Nun zeigen wir: Es gibt in $\mathcal{O}_K$ nur endlich viele ganze Ideale mit Absolutnorm $\leq C$. Es g.z.z., dass es nur endlich viele solcher Primideale gibt. $\mathbb{N}\mathfrak{p}$ ist Potenz von p (Denn p = Charakteristik von $\mathcal{O}_K/\mathfrak{p}$).

Es gibt nur endlich viele Primzahlen $\leq C$. Zu jeder Primzahl p ex. nur endlich viele Primideale $\mathfrak{p}$ mit $\mathbb{N}\mathfrak{p} = p^e$: $\mathrm{char}(\mathcal{O}_K/\mathfrak{p}) = p \Rightarrow p = 0$ in $\mathcal{O}_K/\mathfrak{p} \Rightarrow p \in \mathfrak{p} \Rightarrow \mathfrak{p} \mid (p)$ wie jedes Ideal hat $(p) = p\mathcal{O}_K$ nur endlich viele Primteiler. □

§1.6 MINKOWSKI-Theorie

Sei K algebraischer ZK, $S = \mathrm{Hom}(K, \mathbb{C})$. $\#S = [K : \mathbb{Q}]$, $\sigma : K \to \mathbb{R}$ heißt **reelle Einlagerung**, sonst $\sigma(K) \not\subset \mathbb{R}$ **komplexe**. Letztere treten in Paaren $\sigma, \overline{\sigma}$ auf. Sei $r = r(K)$ die Anzahl der reellen, $2s = 2s(K)$ die Anzahl der komplexen Einlagerungen. Es gilt $r + 2s = n$.

Definition 1.6.1
Der **MINKOWSKI-Raum** $K_\mathbb{R}$ ist definiert als der $\mathbb{R}$-Vektorraum $\mathbb{R}^r \oplus \mathbb{C}^s$. Die *kanonische Einlagerung* $j : K \to K_\mathbb{R}$ ist definiert als

$$j(\alpha) = (\sigma_1\alpha, \ldots, \sigma_r\alpha, \tau_1\alpha, \ldots, \tau_s\alpha)$$

mit $\sigma_1, \ldots, \sigma_r$ die reellen $\sigma \in S$, die τ_j jeweils Repräsentanten der Paare komplex konjugierter Einlagerungen.

Bemerkung 1.6.2
Nicht sehr kanonisch[4]: $r!s!2^s$ Auswahlmöglichkeiten. Kanonisch: $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$, $j(\alpha) = \alpha \otimes 1$ (Tensorprodukt).

Beispiel 1.6.3 (i) $K = \mathbb{Q}(\sqrt{d}), d > 1$ sqf.

$r = 2, s = 0$, $j : K \to \mathbb{R}^2$: $\alpha + \beta\sqrt{d} \mapsto (\alpha + \beta\sqrt{d}, \alpha - \beta\sqrt{d})$

(ii) $K = \mathbb{Q}(\sqrt{d})$, $d < 0$ sqf.

$r = 0, s = 1$, $j : K \to \mathbb{C}$: $\alpha + \beta\sqrt{d} \mapsto \alpha + \beta\sqrt{d}$

(iii) $K = \mathbb{Q}(\zeta_p)$, $p > 2$ prim, $\zeta_p = e^{2\pi i/p}$

$r = 0$, $s = \frac{p-1}{2}$, $j : \zeta_p \mapsto (\zeta_p^a)_{a\in A}$ mit $A = \{a_1, \ldots, a_{(p-1)/2}\} \subset (\mathbb{Z}/p\mathbb{Z})^\times$ jeweils eines aus $\{a, -a\}$

Definition 1.6.4 (Skalarprodukt für $K_\mathbb{R}$)

$$\langle x, y\rangle := \sum_{i=1}^{r} x_{\sigma_i} y_{\sigma_i} + \sum_{j=1}^{s} (x_{\tau_j}\overline{y}_{\tau_j} + \overline{x}_{\tau_j} y_{\tau_j}).$$

Bemerkung 1.6.5 (i) $\mathbb{C}$ ist reeller Vektorraum der Dimension 2, $\langle u, v\rangle = u\overline{v} + \overline{u}v = 2\,\mathrm{Re}(u\overline{v})$ ist $\mathbb{R}$-Skalarprodukt.

(ii) Für $\alpha, \beta \in K$ gilt

$$\langle j(\alpha), j(\beta)\rangle = \sum_{\sigma\in \mathrm{Hom}(K,\mathbb{C})} \sigma(\alpha)\overline{\sigma(\beta)}.$$

(iii) ON-Basis von $K_\mathbb{R}$ ist

$$\begin{aligned} e_i &= (0, \ldots, 0, 1, 0, \ldots, 0) && 1 \le i \le r, \\ f_j &= (0, \ldots, 0, \tfrac{1}{\sqrt{2}}, 0, \ldots, 0) && r+1 \le j \le r+s, \\ g_j &= (0, \ldots, 0, \tfrac{i}{\sqrt{2}}, 0, \ldots, 0) && r+1 \le j \le r+s \end{aligned}$$

(iv) Wir haben noch $\mathbb{C} \to \mathbb{R}^2 : x + iy \mapsto (x, y)$, also

$$f : K_\mathbb{R} \to \mathbb{R}^n : x \mapsto (x_{\sigma_1}, \ldots, x_{\sigma_r}, \mathrm{Re}\, x_{\tau_1}, \mathrm{Im}\, x_{\tau_1}, \ldots, \mathrm{Re}\, x_{\tau_s}, \mathrm{Im}\, x_{\tau_s})$$

ist ein Isomorphismus von $\mathbb{R}$-VR. $\mathbb{R}^n$ trägt Standardskalarprodukt und hat Standardbasis $e_1, \ldots, e_n$ (Achtung: kleine Überladung). Dabei ist $f(e_i) = e_i$ für $1 \le i \le r$, $f(f_j) = \frac{1}{\sqrt{2}} e_{r+2j-1}$, $f(g_i) = \frac{1}{\sqrt{2}} e_{r+2j}$. f ist also keine Isometrie.

[4] „als alternativlos anzunehmen“

(v) Hat man EUKLIDischen VR V, so trägt V genau ein verschiebungsinvariantes Maß, welches auf

$$Q = \left\{ \sum t_i e_i : 0 \leq t_i \leq 1 \right\}, \qquad e_1, \ldots, e_n \text{ ON-Basis}$$

den Wert 1 hat.

Wir haben also auf $K_{\mathbb{R}}$ ein Maß μ und auf $\mathbb{R}^n$ das LEBESGUE-Maß λ. Für den Einheitsquader Q ist $\mu(Q) = 2^s \lambda(f(Q))$:

$$\begin{aligned} \lambda(f(Q)) &= \lambda\left(\left\{ \sum t_i c_i e_i : c_i = 1 \text{ für } 1 \leq i \leq r, c_i = \tfrac{1}{\sqrt{2}} \text{ für } r+1 \leq i \leq n \right\} \right) \\ &= \left(\frac{1}{\sqrt{2}} \right)^{2s} = s^{-2} \end{aligned}$$

Also gilt für alle messbaren Mengen $\Omega \subset K_{\mathbb{R}}$: $\mu(\Omega) = 2^s \lambda(f(\Omega))$.

(vi) Ist V ein EUKLIDischer VR, $v_1, \ldots, v_n \in V$, $n = \dim V$,

$$Q(v_1, \ldots, v_n) = \left\{ \sum_i t_i v_i : 0 \leq t_i \leq 1 \right\} = \textbf{Parallelotop},$$

so ist $\mu(Q) = \sqrt{\det(\langle v_i, v_j \rangle)}$.

Interludium:

Definition 1.6.6
Sei V endlich dimensionaler $\mathbb{R}$-VR. Eine Untergruppe $\Gamma \subset V$ heißt **Gitter** genau dann, wenn Γ diskret und cokompakt ist (d.h. V/Γ ist kompakt).

Beispiel 1.6.7 (i) $\mathbb{Z}^n \subset \mathbb{R}^n$ ist Gitter, denn $\mathbb{R}^n/\mathbb{Z}^n = (\mathbb{R}/\mathbb{Z})^n = (S_1)^n$.

(ii) $\mathbb{Q}^n \subset \mathbb{R}^n$ ist kein Gitter, da nicht diskret.

(iii) $\mathbb{Z}^m \times 0 \subset \mathbb{R}^n$ ist für $m < n$ kein Gitter, da nicht cokompakt.

Fakt 1.6.8
Sei $\Gamma \subset V$ ein Gitter. Dann existiert eine Basis $\omega_1, \ldots, \omega_n$ von V mit $\Gamma = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$. Umgekehrt ist jedes solche Γ ein Gitter.

Beweis: Sei $\Gamma = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ für Basis $\omega_1, \ldots, \omega_n$ von V. $U = \{\sum \lambda_i \omega_i : -\frac{1}{2} < \lambda_i < \frac{1}{2}\}$ ist offene Umgebung von 0 und enthält keine weiteren Punkte aus Γ. Sei $F = \{\sum t_i \omega_i : 0 \leq t_i \leq 1\}$ - Fundamentalmasche. F ist kompakt und wird surjektiv auf V/Γ abgebildet. Also ist V/Γ kompakt.

Sei nun Γ Gitter in V. Γ spannt Teilraum $V_0 = \operatorname{span} \Gamma$ auf. Sei V_1 komplementärer Raum, dann gilt: $V/\Gamma = V_0/\Gamma \oplus V_1$ ist nur kompakt für $V_1 = \{0\}$ (denn der einzige kompakte Vektorraum ist $\{0\}$). Also erzeugt Γ den Raum V und enthält somit Basis $\omega_1, \ldots, \omega_n$ von V. Sei $\Gamma_0 = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$ Gitter. Die Gruppe $\Gamma/\Gamma_0 \subset V/\Gamma_0$ ist diskret, also abgeschlossen, also kompakt und daher endlich[5].

$\Rightarrow (\Gamma : \Gamma_0) = N < \infty \Rightarrow N\Gamma \subset \Gamma_0 \Rightarrow \Gamma_0 \subset \Gamma \subset \frac{1}{N}\Gamma_0 \Rightarrow \Gamma$ freie abelsche Gruppe vom Rang n. □

[5] X kompakt genau dann, wenn jede offene Überdeckung enthält endliche Teilüberdeckung.

Ende VL 8
18.11.2014

Definition 1.6.9
Sei V endlichdimensionaler VR über $\mathbb{R}$, $\Omega \subset V$ heißt **konvex** genau dann, wenn mit $v, w \in \Omega$ das Verbindungsintervall $[v, w] = \{tv + (1-t)w : t \in [0,1]\}$ in Ω liegt.

Ω heißt **zentralsymmetrisch** genau dann, wenn aus $v \in \Omega$ $-v \in \Omega$ folgt.

Fakt 1.6.10 (MINKOWSKIs Gitterpunktsatz)
Sei V EUKLIDischer VR (endl. dim.), $\Gamma \subset V$ Gitter, $\Omega \subset V$ messbar, konvex, zentralsymmetrisch. Es gelte $\mathrm{vol}(\Omega) > 2^n \mathrm{vol}(\Gamma)$, $n = \dim(V)$. Dann enthält Ω neben 0 noch weitere Gitterpunkte.

Bemerkung 1.6.11
$\mathrm{vol}(\Gamma) = \mathrm{vol}(F)$, F Fundamentalmasche: $\Gamma = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$, $F = \{\sum_{i=1}^n t_i\omega_i : 0 \le t_i \le 1\}$. $\mathrm{vol}(\Gamma)$ ist unabhängig von der Wahl der Basis von Γ:

$$\mathrm{vol}(F) = \sqrt{|\det(\langle \omega_i, \omega_j \rangle)|}$$

Für eine ON-Basis $e_1, \ldots, e_n$ von V und A mit $\omega_i = Ae_i$, ist

$$\mathrm{vol}(F) = \mathrm{vol}(AF(e_1, \ldots, e_n)) = |\det A| \underbrace{\mathrm{vol}(F(e_1, \ldots, e_n))}_{=1},$$

$AA^T = (\langle \omega_i, \omega_j \rangle)$.

Beweis: Wir wählen die Fundamentalmasche vorsichtiger

$$F = \left\{ \sum_{i=1}^n t_i\omega_i : 0 \le t_i < 1 \right\}.$$

Dann gilt: $V = \bigsqcup_{\omega \in \Gamma} F + \omega$ (disjunkte Vereinigung). Also folgt $\frac{1}{2}\Omega = \bigsqcup (\frac{1}{2}\Omega \cap (F + \omega))$.
$\Rightarrow 2^{-n} \mathrm{vol}(\Omega) = \sum \mathrm{vol}(\frac{1}{2}\Omega \cap (F + \omega)) = \sum_{\omega \in \Gamma} \mathrm{vol}((\frac{1}{2}\Omega - \omega) \cap F)$
Die LHS ist $> \mathrm{vol}(F)$, also können die Mengen $\frac{1}{2}\Omega - \omega$ nicht alle disjunkt sein. $\exists \omega_1, \omega_2 \in \Gamma$ mit $\omega_1 \neq \omega_2$, $\exists v_1, v_2 \in \Omega$, s.d. $\frac{1}{2}v_1 + \omega + 1 = \frac{1}{2}v_2 + \omega_2$ gilt.
Somit ist $\frac{1}{2}(v_1 - v_2)$ aus $\Gamma \setminus \{0\}$. Mit v_2 ist auch $-v_2 \in \Omega$, also auch $\frac{1}{2}(v_1 - v_2) \in \Omega$. □

Folgerung 1.6.12
Ist Ω kompakt, so genügt schon $\mathrm{vol}(\Omega) \ge 2^n \mathrm{vol}(\Gamma)$ für den vorherigen Fakt.

Beweis: $\mathrm{vol}((1+\varepsilon)\Omega) > 2^n \mathrm{vol}(\Gamma) \Rightarrow$ man findet $\omega_\varepsilon \in \Gamma \setminus \{0\}$ in $(1+\varepsilon)\Omega$. Wähle $\varepsilon_n \downarrow 0$, $\omega_n = \omega_{\varepsilon_n} \in \Gamma \setminus \{0\}$. $\omega_n \in (1+\varepsilon)\Omega \subset 2\Omega$. Wg. Ω kompakt, besitzt (ω_n) konvergente Teilfolge. Da Γ diskret ist, muss diese konstant ab bestimmtem Index sein: $\omega_n = \omega_\infty$ für alle $n > n_0$, $\omega_\infty \neq 0$, $\omega_\infty \in \bigcap_n (1+\varepsilon_n)\Omega = \overline{\Omega}$ □

Bemerkung 1.6.13
Die Aussage ist bestmöglich:

$V = \mathbb{R}^n$, $\Omega = (-1,1)^n$, $\mathrm{vol}(\Omega) = 2^n$, $\Gamma = \mathbb{Z}^n$, $\mathrm{vol}(\Gamma) = 1$. Ω enthält nur den Gitterpunkt $(0, \ldots, 0)$. $\overline{\Omega}$ ist kompakt, zentralsymmetrisch, konvex und enthält $3^n - 1$ weitere Gitterpunkte.

Fakt 1.6.14
Sei K alg. ZK, $\mathfrak{a} \subset O_K$ Ideal $\neq (0)$. Dann ist $j(\mathfrak{a})$ ein Gitter in $K_\mathbb{R}$ und es gilt

$$\mathrm{vol}(j(\mathfrak{a})) = \mathbb{N}\mathfrak{a} \cdot \sqrt{|d_K|}.$$

Beweis: $K_\mathbb{R} = \mathbb{R}^r \oplus \mathbb{C}^s$ mit Skalarprodukt

$$\langle x, y\rangle = \sum_{i=1}^{r} x_{\sigma_i} y_{\sigma_j} + \sum_{j=1}^{s} (x_{\tau_j}\overline{y}_{\tau_j} + \overline{x}_{\tau_j} y_{\tau_j})$$

Es gilt $\langle j(\alpha), j(\beta)\rangle = \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} \sigma\alpha\overline{\sigma\beta}$. Sei $\omega_1, \ldots, \omega_n$ $\mathbb{Z}$-Basis von $\mathfrak{a}$, dann ist $j(\mathfrak{a}) = \mathbb{Z}j(\omega_1) + \ldots + \mathbb{Z}j(\omega_n)$. Nach Definition der Diskriminante ist $d(\mathfrak{a}) = \det^2(\sigma_i\omega_j)$. Andererseits ist $d(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})^2 d(\mathcal{O}_K) = (\mathbb{N}\mathfrak{a})^2 d_K$. Weiter ist

$$\mathrm{vol}(j(\mathfrak{a})) = \sqrt{|\det(\langle j(\omega_k), j(\omega_l)\rangle)|} = |\det(\sigma_i\omega_j)| = \mathbb{N}\mathfrak{a}\sqrt{|d_K|}.$$

□

Lemma 1.6.15
Sei K alg. ZK, $\lambda > 0$ reell.

$$\Omega(\lambda) := \left\{ x \in K_\mathbb{R} : \sum_{i=1}^{r} |x_{\sigma_i}| + 2\sum_{j=1}^{s} |x_{\tau_j}| \leq \lambda \right\}$$

Dann gilt $\mathrm{vol}(\Omega(\lambda)) = 2^r \pi^s \frac{\lambda^n}{n!}$

Beweis: Natürlich ist $\mathrm{vol}(\Omega(\lambda)) = \lambda^n \mathrm{vol}(\Omega(1))$.

$$f : K_\mathbb{R} \to \mathbb{R}^n : x_{\sigma_i} \mapsto x_{\sigma_i}, x_{\tau_j} \mapsto (\mathrm{Re}\, x_{\tau_j}, \mathrm{Im}\, x_{\tau_j})$$

Sei für $x \in \mathbb{R}^n$: $x = (x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s)$

$$f(\Omega(1)) = \left\{ \sum |x_i| + 2\sum |\sqrt{y_i^2 + z_i^2}| \leq 1 \right\}$$

Wir berechnen das LEBESGUE-Maß λ (Achtung: leichte Überladung mit $\lambda \in \mathbb{R}$) dieser Menge: Sei $y_j = r_j \cos\theta_j$, $z_j = r_j \sin\theta_j$.

$$\lambda(f(\Omega(1))) = \int_\Delta r_1 \cdot \ldots \cdot r_s dx_1 \ldots dx_r dr_1 \ldots dr_s d\theta_1 \ldots \theta_s$$

mit

$$\Delta = \left\{ (x, r, \theta) : \sum_{i=1}^{r} + 2\sum_{j=1}^{s} r_j \leq 1, r_j \geq 0, 0 \leq \theta_j \leq 2\pi \right\}.$$

Nimmt man nur die $x_i \geq 0$, so erhält man $2^r\lambda(f(\Omega(1)))$.

Wir setzen noch $y_j = 2r_j$, das gibt

$$\lambda(f(\Omega(1))) = 2^r(2\pi)^s 4^{-s} W_{r,s}(1)$$

mit

$$W_{r,s}(\mu) = \int_E dx_1 \dots dx_r y_1 \dots y_s dy_1 \dots dy_s \qquad \text{(FUBINI)},$$

wobei

$$E = \left\{ (x,y) \in \mathbb{R}_+^{r+s} : \sum_{i=1}^{r} + \sum_{j=1}^{s} y_j \leq \mu \right\}.$$

Es gilt wieder $W_{r,s}(\mu) = \mu^n W_{r,s}(1)$, $n = r + 2s$.

$$\begin{aligned} W_{r,s}(1) &= \int_0^1 W_{r-1,s}(1-x_1)dx_1 \\ &= W_{r-1,s}(1) \int_0^1 (1-x_1)^{n-1} dx_1 \\ &= \frac{1}{n} W_{r-1,s}(1) \end{aligned}$$

Es folgt

$$W_{r,s}(1) = \frac{1}{n(n-1)\dots(n-r+1)} W_{0,s}(1).$$

Analog folgt:

$$\begin{aligned} W_{0,s}(1) &= \int_0^1 W_{0,s-1}(1-y_1) \cdot y_1 dy_1 \\ &= W_{0,s-1}(1) \int_0^1 y_1 (1-y_1)^{2s-2} dy_1 \\ &\vdots \\ &= \frac{1}{2s(2s-1)} W_{0,s-1}(1) \end{aligned}$$

Insgesamt ergibt sich: $W_{r,s}(1) = \frac{1}{n!}$ (Beachte: $n - r = 2s$) und damit

$$\lambda(f(\Omega(1))) = 2^r 4^{-s} (2\pi)^s \tfrac{1}{n!}.$$

Es folgt $\mathrm{vol}(\Omega(1)) = 2^s \lambda(f(\Omega(1))) = 2^r \cdot \pi^s \cdot \frac{1}{n!}$. □

Bemerkung 1.6.16
$\Omega(1)$ ist kompakt, zentralsymmetrisch und konvex: Die ersten beiden Eigenschaften sieht man sofort. Konvex: Sind $x, y \in \Omega(1)$, $0 \leq t \leq 1$, so ist

$$|tx_0 + (1-t)y_0| \leq t|x_0| + (1-t)|y_0|.$$

Satz 1.6.17 („Satz 5“: MINKOWSKI)
Sei K alg. Zahlenkörper, $n = r + 2s = [K : \mathbb{Q}]$. $c_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s$ = **MINKOWSKI-Konstante**. Dann gibt es in jeder Idealklasse aus Cl_K ganze Ideale $\mathfrak{a}$ mit $\mathbb{N}\mathfrak{a} \leq c_K \sqrt{|d_K|}$.

Beweis: Sei $x \in \mathrm{Cl}_K$, $\mathfrak{b}$ ganzes Ideal aus x^{-1}. Wähle $\lambda > 0$ so groß, dass $\mathrm{vol}(\Omega(\lambda)) = 2^n \mathrm{vol}(j(\mathfrak{b})$ gilt. Das ist der Fall für $\lambda^n = 2^n \mathbb{N}\mathfrak{b}\sqrt{|d_K|}n!2^{-r}\pi^{-s}$. Dann existiert $\beta \in \mathfrak{b}$, $\beta \neq 0$ mit $j(\beta) \in \Omega(\lambda))$, also $\sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} |\sigma\beta| \leq \lambda$.

Es folgt $|N_{\mathbb{Q}}^K|^{1/n} \leq \frac{1}{n} \sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} |\sigma\beta| \leq \frac{\lambda}{n}$ (geometrisches Mittel $\leq$ arithmetisches Mittel).

$\Rightarrow |N_{\mathbb{Q}}^K(\beta)| \leq \frac{\lambda^n}{n^n} = \frac{n!}{n^n} 4^s \pi^{-s} \mathbb{N}\mathfrak{b}\sqrt{|d_K|}$. $(\beta) = \mathfrak{b} \cdot \mathfrak{a}$ für ein ganzes Ideal $\mathfrak{a}$, wg, $\beta \in \mathfrak{b}$. $\mathfrak{a}$ liegt dann in der Klasse x und $|N(\beta)| = \mathbb{N}\mathfrak{a} \cdot \mathbb{N}\mathfrak{b} \Rightarrow \mathbb{N}\mathfrak{a} \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$ □

Ende VL 9
19.11.2014

Folgerung 1.6.18 („Folgerung 1“)
Für jeden ZK $K \neq \mathbb{Q}$ ist $|d_K| > 1$

Beweis: $\sqrt{|d_K|} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s \Rightarrow |d_K| \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2} = c_n$

Für $n = 2$ ist $c_n = \left(\frac{\pi}{2}\right)^2 \frac{16}{4} = \frac{\pi^2}{4} > \frac{9}{4} > 1$.

Die Folge (c_n) ist monoton wachsend:

$$\frac{c_{n+1}}{c_n} = \frac{\pi}{4} \frac{(n+1)^{2n+2}}{n^{2n}} \frac{1}{(n+1)^2} = \frac{\pi}{4} \left(1 + \frac{1}{n}\right)^{2n}$$

Ana I: Der Grenzwert ist e^2. □

§1.7 Beispiele von Idealklassengruppen

§1.7.1 Imaginärquadratische ZK

$K = \mathbb{Q}(\sqrt{d})$, $d < 0$ sqf

$c_K = \frac{2!}{2^2} \frac{4}{\pi} = \frac{2}{\pi} < 0.6332$

$c_K \sqrt{|d_K|} < 2 \Leftrightarrow |d_K| < \pi^2$, also $\mathrm{Cl}_K = 1$ für $d_K = -3, -4, -7, -8$ ($d = -3, -1, -7, -2$). Man weiß, dass es nur noch die Diskriminanten $d_K = -11, -19, -43, -67, -163$ mit $h_K = 1$ gibt (HEEGNER, Problem der 10. Diskriminante, Beweis schwierig).

SIEGEL:

$$\lim_{-d \to \infty} \frac{\log h(\mathbb{Q}(\sqrt{d}))}{\log |d_K|} = \frac{1}{2}$$

Beispiel 1.7.1
$K = \mathbb{Q}(\sqrt{-163})$, $d_K = -163$ (prim), $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ mit $\omega = \frac{1+\sqrt{-163}}{2}$.

$$c_K \sqrt{163} = \frac{2!}{2^2} \frac{4}{\pi} \sqrt{163} < 8.128$$

Cl_K wird erzeugt von den Primidealen der Absolutnorm < 9. Jedes Primideal enthält natürliche Zahlen > 0. Ist $m \in \mathfrak{p}$, $m \in \mathbb{N} \setminus \{0\}$, so ist auch jeder Primteiler von m in $\mathfrak{p}$, $\mathfrak{p}$ enthält keine zwei Primzahlen $p, l \in \mathfrak{p}$, $p \neq l \Rightarrow 1 \in \mathfrak{p}$ ↯. Also liegt in $\mathfrak{p}$ genau eine Primzahl $p \in \mathfrak{p}$. Es folgt $p\mathcal{O}_K \subset \mathfrak{p} \subset \mathcal{O}_K$. Ist also $\mathfrak{p} \neq p\mathcal{O}_K$, so folgt $\mathbb{N}\mathfrak{p} = p$, ist $\mathfrak{p} = p\mathcal{O}_K$, so folgt $\mathbb{N}\mathfrak{p} = p^2$. Wir zeigen $p\mathcal{O}_K$ ist prim für $p = 2, 3, 5, 7$, denn daraus folgt $\mathrm{Cl}_K = 1$.

Wir betrachten $\mathcal{O}_K / p\mathcal{O}_K$. $\omega = \frac{1+\sqrt{-163}}{2} \Rightarrow \omega^2 = \frac{1}{4} + \frac{1}{2}\sqrt{-163} - \frac{163}{4} = \omega - 41$

Ist $\overline{\omega}$ das Bild von ω in $\mathcal{O}_K/p\mathcal{O}_K$, so ist

$$\begin{aligned} \overline{\omega}^2 &= 1+\overline{\omega} && p=2,3,7 \\ \overline{\omega}^2 &= -1+\overline{\omega} && p=5 \end{aligned}$$

Sei $\mathbb{F}_p[T] \to \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$: $T \mapsto \omega \mapsto \overline{\omega}$. Der Kern ist (T^2-T-1) für $p=2,3,7$ und (T^2-T+1) für $p=5$

x	0	1	2	3	4	5	6
x^2-x-1	-1	-1	1	5	11	19	29
x^2-x+1	1	1	3	7	13		

Also sind alle vier Ringe $\mathcal{O}_K/p\mathcal{O}_K$ Körper, d.h. $p\mathcal{O}_K$ ist maximales Ideal für $p=2,3,5,7$. Mithin $h_K=1$.

Beispiel 1.7.2
$K=\mathbb{Q}(\sqrt{-41})$

(i) $d_K=-4\cdot 41$, $\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\omega$ mit $\omega=\sqrt{-41}$.

$$c_K\sqrt{-41}=\frac{2!}{2^2}\frac{4}{\pi}\sqrt{41\cdot 4}=\frac{4}{\pi}\sqrt{41}<8,2$$

$\Rightarrow \mathrm{Cl}_K$ wird erzeugt von den Primidealen der Absolutnorm ≤ 8.

(ii) Wir zeigen $2\mathcal{O}_K=\mathfrak{p}_2^2$ (2 ist verzweigt)

Sei dazu $\mathfrak{p}_2:=\mathbb{Z}(1+\omega)+\mathbb{Z}\cdot 2$. Wir zeigen $\mathfrak{p}_2$ ist Ideal: $\omega(1+\omega)=\omega-41=\omega+1-21\cdot 2\in\mathfrak{p}_2$ und $\omega\cdot 2=2(\omega+1)-1\cdot 2\in\mathfrak{p}_2$. Also $\mathfrak{p}_2=(1+\omega,2)$.

$$\mathbb{N}\mathfrak{p}_2=\left|\det\begin{pmatrix}1&2\\1&0\end{pmatrix}\right|=2$$

Ein Kommutativer Ring mit 1 und 2 Elementen ist ein Körper. Also $\mathfrak{p}_2$ prim.

$\mathfrak{p}_2^2=((1+\omega)^2,2(1+\omega),4)$

$$(1+\omega)^2=1+2\omega-41=-40+2\omega=2(-20+\omega)$$

Also $\mathfrak{p}_2^2\subset 2\mathcal{O}_K=(2)$. $\mathbb{N}(\mathfrak{p}_2^2)=(\mathbb{N}\mathfrak{p}_2)^2=4$, $\mathbb{N}(2)=4$ $\Rightarrow \mathfrak{p}_2^2=(2)=2\mathcal{O}_K$

(iii) Wir zeigen: $3,5,7$ sind zerlegt (split): $p\mathcal{O}_K=\mathfrak{p}\overline{\mathfrak{p}}$, $\mathfrak{p}\neq\overline{\mathfrak{p}}$ und $\mathfrak{p}$,$\overline{\mathfrak{p}}$ prim.

Sei $\mathfrak{p}_3:=\mathbb{Z}(1+\omega)+\mathbb{Z}\cdot 3$. Das ist Ideal: $\omega(1+\omega)=\omega-41=(1+\omega)-14\cdot 3\in\mathfrak{p}_3$ und $\omega\cdot 3=3(1+\omega)-1\cdot 3\in\mathfrak{p}_3$.

$$\mathbb{N}\mathfrak{p}_3=\left|\det\begin{pmatrix}1&3\\1&0\end{pmatrix}\right|=3$$

$\Rightarrow \mathfrak{p}_3$ prim.

$\overline{\mathfrak{p}}_3=\mathbb{Z}(1-\omega)+\mathbb{Z}\cdot 3$. Angenommen $\overline{\mathfrak{p}}_3=\mathfrak{p}_3$, dann $1-\omega=a(1+\omega)+b\cdot 3$ mit $a,b\in\mathbb{Z}$. Dann folgt $a=-1$ und $a+3b=1$, also $3b=2$ $\lightning$. Somit $\mathfrak{p}_3\neq\overline{\mathfrak{p}}_3$. $\mathfrak{p}_3\cdot\overline{\mathfrak{p}}_3=\mathbb{Z}\cdot 3(1+\omega+\mathbb{Z}\cdot 3(1-\omega)+\mathbb{Z}\cdot 9+\mathbb{Z}\cdot 42\subset 3\cdot\mathcal{O}_K$.

$\mathbb{N}\mathfrak{p}_3\overline{\mathfrak{p}}_3=9=\mathbb{N}(3)$ $\Rightarrow 3\cdot\mathcal{O}_K=\mathfrak{p}_3\cdot\overline{\mathfrak{p}}_3$

$\mathfrak{p}_5 := \mathbb{Z}(2+\omega)+\mathbb{Z}5$ ist Ideal: $\omega(2+\omega) = 2\omega-41 = 2\omega+2-9\cdot 5 \in \mathfrak{p}_5$. $\omega\cdot 5 = 5(\omega+2)-2\cdot 5 \in \mathfrak{p}_5$.

$$\mathbb{N}\mathfrak{p}_5 = \left|\det \begin{pmatrix} 2 & 5 \\ 1 & 0 \end{pmatrix}\right| = 5$$

$\Rightarrow \mathfrak{p}_5$ prim.

Angenommen $\mathfrak{p}_5 = \overline{\mathfrak{p}}_5 \Rightarrow 2-\omega = a(2+\omega)+b\cdot 5$ mit $a, b \in \mathbb{Z}$. Dann ist $2 = 2a+5b$ und $-1 = a$, also $4 = 5b$ ↯. Wie oben folgt: $5\cdot \mathcal{O}_K = \mathfrak{p}_5 \cdot \overline{\mathfrak{p}}_5$.

Das $\mathfrak{p}_5$ ist gut konstruiert. Wählt man nämlich $A = \mathbb{Z}(1+\omega)+\mathbb{Z}\cdot 5$, so ist das kein Ideal: $\omega(1+\omega) = \omega - 41 = (\omega+1) - 42 \notin A$. Das Ideal $I = (1+\omega, 5)$ ist $\mathcal{O}_K$: $\omega(1+\omega)+9\cdot 5 = 3+(\omega+1) \in I$. Also ist $3 \in I$ und $5 \in I$, also $1 \in I$.

$\mathfrak{p}_7 := \mathbb{Z}(1+\omega)+\mathbb{Z}\cdot 7$ ist Ideal: $\omega(1+\omega) = \omega-41 = \omega+1-6\cdot 7 \in \mathfrak{p}_7$, $\omega\cdot 7 = 7\cdot(\omega+1)-7 \in \mathfrak{p}_7$.

$$\mathbb{N}\mathfrak{p}_7 = \left|\begin{pmatrix} 1 & 7 \\ 1 & 0 \end{pmatrix}\right| = 7$$

$\Rightarrow \mathfrak{p}_7$ prim.

Angenommen $\mathfrak{p}_7 = \overline{\mathfrak{p}}_7$. Dann $1-\omega = a(1+\omega)+b\cdot 7$ für $a, b \in \mathbb{Z}$. $\Rightarrow a = -1$, $1 = -1+7b$ und $7b = 2$ ↯. $\Rightarrow 7\cdot \mathcal{O}_K = \mathfrak{p}_7 \cdot \overline{\mathfrak{p}}_7$.

Alle ganzen Ideale mit $\mathbb{N} \leq 8$ sind: $(1), \mathfrak{p}_2, \mathfrak{p}_3, \overline{\mathfrak{p}}_3, \mathfrak{p}_2^2, \mathfrak{p}_5, \overline{\mathfrak{p}}_5, \mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2\overline{\mathfrak{p}}_3, \mathfrak{p}_7, \overline{\mathfrak{p}}_7, \mathfrak{p}_2^3$. Also $h_K \leq 12$. $\mathfrak{p}_2^2 = (2)$ mit Bild 1 in Cl_K, $\mathfrak{p}_2^3 = (2)\cdot \mathfrak{p}_2$ und $\mathfrak{p}_2$ haben das selbe Bild in Cl_K. Also $h_K \leq 10$. Diese 10 Ideale werden surjektiv auf Cl_K abgebildet, $\mathfrak{p}_3\cdot\overline{\mathfrak{p}}_3 = (3)$, also $\overline{\mathfrak{p}}_3 \cong \mathfrak{p}_3^{-1}$ in Cl_K, ebenso für $\mathfrak{p}_5, \mathfrak{p}_7$. Weiter $\mathfrak{p}_2^2 \cong 1$ in Cl_K. $\mathrm{N}(1+\omega) = 42 = 2\cdot 3\cdot 7 \Rightarrow (1+\omega) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7$ oder $\mathfrak{p}_2\overline{\mathfrak{p}}_3\mathfrak{p}_7$ oder $\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}}_7$ oder $\mathfrak{p}_2\overline{\mathfrak{p}}_3\overline{\mathfrak{p}}_7$. Also wird Cl_K erzeugt von $\mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_7$. $\mathrm{N}(2+\omega) = 45 = 3^2\cdot 5$, also $(2+\omega) = \mathfrak{p}_3^2\cdot\mathfrak{p}_5$ oder die anderen Möglichkeiten. $\Rightarrow \mathrm{Cl}_K$ wird erzeugt von $\mathfrak{p}_3$ und $\mathfrak{p}_7$. $\mathrm{N}(8+\omega) = 64+41 = 105 = 3\cdot 5\cdot 7 \Rightarrow (8+\omega) = \mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_7$ oder so ähnlich $\Rightarrow \mathrm{Cl}_K$ wird erzeugt von $\mathfrak{p}_3$.

Nun bestimmen wir die Ordnung von $\mathfrak{p}_3$ in Cl_K. Sie ist ≤ 10. $\mathfrak{p}_3^k = (a+b\omega) \Rightarrow 3^k = a^2+42b^2$. Ist umgekehrt $3^k = a^2+41b^2$, so folgt $(a+b\omega) = \mathfrak{p}_3^r\overline{\mathfrak{p}}_3^s$. Sind beide $r > 0$, $s > 0$, so steht rechts Faktor $\mathfrak{p}_3\overline{\mathfrak{p}}_3 = (3) = 3\mathcal{O}_K$, also $3 \mid a$, $3 \mid b$. Sind a, b nicht beide durch 3 teilbar, so ist $(a+b\omega) = \mathfrak{p}_3^k$ oder $= \overline{\mathfrak{p}}_3$. Wir suchen das minimale $k \geq 1$, s.d. $3^k = a^2+41b^2$ $\mathbb{Z}$-Lösungen hat, wir wissen $k \leq 10$.

$k = 1$	$3 = a^2+41b^2$ ↯
$k = 2$	$9 = a^2+41b^2$ ↯
$k = 3$	$27 = a^2+41b^2$ ↯
$k = 4$	$81 = a^2+41b^2$ ↯

usw. $k = 8$ liefert den ersten Treffer: $b = 11$, $a = 40$. $3^8 = 6561$, $a^2+41b^2 = 6561$.

Also $(40+11\omega) = \mathfrak{p}_3^8$ (oder $\overline{\mathfrak{p}}_3^8$?[6]). Somit: Die Idealklassengruppe von $\mathbb{Q}(\sqrt{-41})$ ist zyklisch der Ordnung 8, erzeugt von $\mathfrak{p}_3 = (1+\omega, 3)$

Ende VL 10
25.11.2014

[6] Tatsächlich ist letzteres der Fall, aber das benötigen wir nicht für unsere Aussage.

§1.7.2 Reell quadratische ZK

Sei $d > 1$, sqf, $c_K = \frac{2!}{2^2} = \frac{1}{2}$, $K = \mathbb{Q}(\sqrt{d})$, $r = 2$, $s = 0$.

$c_K \sqrt{|d_K|} < 2 \Leftrightarrow d_K < 4^2 = 16$ Also $\mathrm{Cl}_K = 1$ für $d_K = 5, 8, 12, 13$.

§1.7.3 Kreisteilungskörper

$K = \mathbb{Q}(\zeta_p)$, $p \in \mathbb{P}$, $p > 2$, $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$

$$c_K = \frac{(p-1)!}{(p-1)^{p-1}} \left(\frac{4}{\pi}\right)^{\frac{p-1}{2}}$$

$\mathrm{Cl}_K = 1$ für $p = 3$, $p = 5$ (ÜA)

Bisher verstehen wir die Idealklassengruppen der Kreisteilungskörper sehr schlecht. (S. LANG Cyclotomic fields I,II)

§1.8 Die Einheitengruppe

Wir wollen $E_K = U_K = \mathcal{O}_K^\times$ studieren. Das ist abelsche Gruppe. Diese kann unendlich sein: $K = \mathbb{Q}(\sqrt{2})$, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{2}$, $\varepsilon := 1 + \sqrt{2}$. Dann ist ε eine Einheit. $\varepsilon(1 - \sqrt{2}) = 1$. Dann ist $\varepsilon^n \uparrow \infty$.

Bemerkung 1.8.1
$(E_K)_{\mathrm{tor}}$ besteht genau aus den Einheitswurzeln $\mu(K)$ in K. Ihre Anzahl ist endlich, denn unter $j : K \to K_{\mathbb{R}}$ ist $j(E_K)$ diskret (wegen $j(O_K)$ =Gitter) und jede Komponente von $j(\zeta)$ ($\zeta \in \mu(K)$) hat Abssolutbetrag 1. Eine diskrete beschränkte Menge ist endlich.

Beispiel 1.8.2 • Einheiten in imaginärquadratischen ZK

$K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, sqf.

(i) $-d \equiv 2, 3 \pmod 4 \Rightarrow \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$

$\varepsilon \in \mathcal{O}_K$ Einheit $\Leftrightarrow \mathrm{N}\,\varepsilon = \pm 1$:

$$\varepsilon \cdot \eta = 1 \Rightarrow \mathrm{N}\,\varepsilon \cdot \mathrm{N}\,\eta = 1, \text{ wobei } \mathrm{N}\,\varepsilon, \mathrm{N}\,\eta \in \mathbb{Z}$$

Ist $\mathrm{N}\,\varepsilon = 1$, so gilt $\varepsilon \cdot \underbrace{\prod_{\sigma \neq \mathrm{Id}} \sigma\varepsilon}_{=\mathrm{N}\,\varepsilon = \eta} = 1$

$\eta \in K$ ist ganz, also aus $\mathcal{O}_K$. Somit $\varepsilon \in E_K$. Sei $\varepsilon = a + b\sqrt{-d}$, $\mathrm{N}\,\varepsilon = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + db^2 \geq 0$. $\mathrm{N}\,\varepsilon = 1 = a^2 + db^2$ hat Lösungen $(\pm 1, 0)$ außer $d = 1$, dann 4 Lösungen.

(ii) $-d \equiv 1 \pmod 4 \Rightarrow \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ mit $\omega = \frac{1+\sqrt{-d}}{2}$.

$$\begin{aligned} \mathrm{N}(a + b\omega) &= (a + b\tfrac{1+\sqrt{-d}}{2})(a + b\tfrac{1-\sqrt{-d}}{2}) \\ &= a^2 + ab + b^2 \tfrac{1+d}{4} \end{aligned}$$

$\Rightarrow 4\,\mathrm{N}(a+b\omega) = (2a+b)^2 + db^2 = \pm 4$, -4 geht nicht, also $(2a+b)^2 + db^2 = 4$. Ist $d > 4$, so nur triviale Lösungen: $b = 0$, $a = \pm 1$.

$d = 3$: $(2a+b)^2 + 3b^2 = 4$. Alle $\mathbb{Z}$-Lösungen sind $(\pm 1, 0), (0, \pm 1), (1, -1), (-1, 1)$, also 6 Lösungen.

$$2a + b = \pm 1 \;\Rightarrow\; \mu(\mathbb{Q}(\sqrt{-3})) = \mu_6$$

Definition 1.8.3

$$K_{\mathbb{R}}^{\times} = \{x \in K_{\mathbb{R}} : \text{ alle Komponenten sind } \neq 0\}$$

$$l : K_{\mathbb{R}}^{\times} \to \mathbb{R}^{r+s} : (x_{\sigma_1,\ldots,x_{\sigma_r},y_{\tau_1},\ldots,y_{\tau_s}}) \mapsto (\log|x_{\sigma_1}|, \ldots, \log|x_{\sigma_r}|, \log|y_{\tau_1}|^2, \ldots, \log|y_{\tau_s}|^2)$$

Wobei $\log = \ln$. Oder einheitlich: Für $\rho \in \mathrm{Hom}(K, \mathbb{C})$ sei

$$\mathrm{N}_\rho := \begin{cases} 1 & \rho \text{ reell} \\ 2 & \rho \text{ nicht reell} \end{cases}$$

Dann ist $l(x) = (\log|x_\rho|^{\mathrm{N}_\rho})_{\rho \in S}$, $S \subset \mathrm{Hom}(K, \mathbb{C})$ aus den Paaren komplex-konjugiertert wird eines ausgewählt

Es gilt $\sum_{\rho \in S} \log|x_\rho|^{\mathrm{N}_\rho} = \log \prod_{\rho \in S} |x_\rho|^{\mathrm{N}_\rho}$. Für $\alpha \in K^\times$ gilt $l(j(\alpha)) = \log|\,\mathrm{N}_{\mathbb{Q}}^K(\alpha)|$. (Deshalb die N_ρ)

Wir setzen noch $\lambda = l \circ j$, $\lambda : K^\times \to \mathbb{R}^{r+s}$. Das ist ein Homomorphismus:

$$\lambda(\alpha\beta) = l(j(\alpha\beta)) = l(j(\alpha)j(\beta)) = \lambda(\alpha) + \lambda(\beta)$$

Fakt 1.8.4 (i) Der Kern von $\lambda : E_K \to \mathbb{R}^{r+s}$ ist $\mu(K)$ = die Gruppe der Einheitswurzeln in K.

(ii) Das Bild von E_K ist diskret und liegt in der Hyperebende $H = \{x \in \mathbb{R}^{r+s} : \sum x_\rho = 0\}$

Beweis:

(i) Für $\zeta \in \mu(K)$ ist $\zeta^N = 1 \Rightarrow |\sigma\zeta| = 1$. $\forall \sigma \in S$, also $\log|\sigma\zeta| = 0 \Rightarrow \zeta \in \mathrm{Ker}\,\lambda$. Sei $\lambda(\alpha) = 0$, also $\log|\sigma\alpha| = 0 \forall \sigma \in S \Rightarrow \log|\sigma\alpha| = 0 \forall \sigma \in \mathrm{Hom}(K, \mathbb{C})$. Somit $|\sigma\alpha| = 1 \forall \sigma \in \mathrm{Hom}$. Somit liegt $j(\alpha)$ in beschränktem Gebiet in $K_{\mathbb{R}}$. Dasselbe gilt für alle Potenzen α^N von α. $j(\mathcal{O}_K)$ ist diskret, also ist die Menge $\{j(\alpha^N) : N \in \mathbb{N} \setminus \{0\}\}$ endlich. $\exists m > n > 0$ sd. $j(\alpha^m) = j(\alpha^n) = j(\alpha^{m-n}) = 1$. $\Rightarrow \alpha^{m-n}$ ist Eigenwert $\Rightarrow \alpha$ auch.

(ii) Für $\varepsilon \in E_K$ gilt $N_{\mathbb{Q}}^K(\varepsilon) = \pm 1 = \prod_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} \sigma(\varepsilon)$. Also

$$\sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} \log|\sigma\varepsilon| = \sum_{\rho \in S} \log|\rho\varepsilon|^{\mathrm{N}_\rho} = 0.$$

Somit liegt $\lambda(\varepsilon)$ in H.

Diskretheit: Sei $\Omega_c = \{(x_\rho) \in \mathbb{R}^{r+s} : |x_\rho| \leq c\}$. Dann ist $l^{-1}\Omega_c = \{(y_\rho) \in K_{\mathbb{R}} : e^{-c} < |y_\rho|^{\mathrm{N}_\rho} < e^c\}$. $l^{-1}\Omega_c \cap j(\mathcal{O}_K)$ ist endlich, da $l^{-1}\Omega_c$ beschränkt und $j(\mathcal{O}_K)$ diskret ist. Also erst recht $\Omega_c \cap \lambda(E_K)$ endlich.

□

Folgerung 1.8.5
E_K ist endlich erzeugt und $\operatorname{rk} E_K \leq r + s - 1$.

Beweis: $\lambda(E_K)$ ist diskrete Untergruppe in H, also Gitter in der linearen Hülle von $\lambda(E_K)$. □

Fakt 1.8.6
Sei K reellquadratisch, dann hat E_K den Rang 1. Es existiert also Einheit ε_K, s.d. $E_K = \mu_2 \times \langle \varepsilon_K \rangle$. ε_K ist eindeutig bestimmt durch $\varepsilon_K > 1$. Sie heißt **Fundamentaleinheit**.

Lemma 1.8.7 (DIRICHLET)
Sei $x \in \mathbb{R}$, $N > 1$ natürliche Zahl. Dann existieren $a, q \in \mathbb{Z}$, $0 < q \leq N$ mit $|x - \frac{a}{q}| < \frac{1}{Nq}$

Beweis: Unterteile $[0, 1)$ in N gleichlange Intervalle. Unter den Zahlen qx, $0 \leq q \leq N$ gibt es zwei verschiedene, welche $\pmod 1$ im selben Intervall liegen. Also

$$|q_1 x - q_2 x - a| \leq \frac{1}{N} \qquad a \in \mathbb{Z}, 0 \leq q_1, q_2 \leq N, q_1 \neq q_2.$$

Setze $q = |q_1 - q_2|$, dann gilt $0 < q \leq N$ und

$$|qx \pm a| < \frac{1}{N} \Rightarrow |x \pm \frac{a}{q}| < \frac{1}{qN}$$

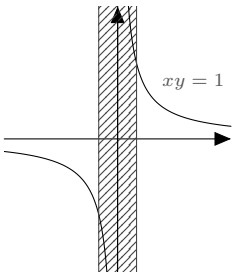
□

Beweis (des Fakts):

$K := \mathbb{Q}(\sqrt{d})$, $d > 1$ sqf, $K_{\mathbb{R}} = \mathbb{R} \oplus \mathbb{R}$. $j(a + b\sqrt{d}) = (a_b\sqrt{d}, a - b\sqrt{d})$. Sei $N > 1$, es existieren $q, a \in \mathbb{Z}$, s.d.

$$|a - q\sqrt{d}| < \frac{1}{N} \qquad 0 < q \leq N.$$

Das ist Streifen in $K_{\mathbb{R}}$



Es folgt $|a + q\sqrt{d}| \leq |a - q\sqrt{d}| + 2q\sqrt{d} < \frac{1}{N} + 2N\sqrt{d}$. Also ist $|\operatorname{N}(a + q\sqrt{d})| < 1 + 2\sqrt{d}$. Das ist also eine Schranke, die unabhängig von a, q, N ist. In solch einem Streifen zu N gibt es also stets Punkte aus $j(\mathcal{O}_K)$, deren Norm unabhängig von N beschränkten Betrag hat. Dann sind auch die Absolutnormen $\mathbb{N}((a + q\sqrt{d}))$ beschränkt.

Es gibt nur endliche viele ganze Ideale mit beschränkter Absolutnorm. Also existieren Ideale $(a + q\sqrt{d}), (b + r\sqrt{d})$ welche gleich sind, aber $(a, q) \neq (b, r)$. Dann gilt $a + q\sqrt{d} = \varepsilon(b + r\sqrt{d})$ mit

Einheit ε. Diese kann nicht -1 sein, wegen q, r positiv. D.h. $\varepsilon \neq 1, \neq -1$. Nun Fallunterscheidung:

$$\begin{aligned} 1 < \varepsilon &\Rightarrow e_K = \varepsilon \\ 0 < \varepsilon < 1 &\Rightarrow e_K = \frac{1}{\varepsilon} \\ -1 < \varepsilon < 1 &\Rightarrow e_K = -\frac{1}{\varepsilon} \\ \varepsilon < -1 &\Rightarrow e_K = -\varepsilon \end{aligned}$$

□

Bemerkung 1.8.8
Es folgt $E_K = \mu_2 \times$ unendliche zyklische Gruppe.

Satz 1.8.9 („Satz 6“ DIRICHLETscher Einheitensatz)
$\lambda(E_K)$ ist ein Gitter in H, d.h. $\operatorname{rk} E_K = r + s - 1$. Also $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$

Definition 1.8.10
Jede Menge von Einheiten $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$, welche E_K modulo Torsion erzeugt, heißt **System von Fundamentaleinheiten**.

Ende VL 11
26.11.2014

Beweis: Sei $S \subset \operatorname{Hom}(K, \mathbb{C})$ wie oben.

(i) Fixiere $\rho_0 \in S$, $x \in \mathcal{O}_K$, $x \neq 0$.

Wir zeigen: Es existiert $y \in \mathcal{O}_K$, $y \neq 0$, s.d.

(a) $|\operatorname{N}_{\mathbb{Q}}^K(y)| \leq \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$

(b) $\log |\rho y|^{\operatorname{N}_\rho} < \log |\rho x|^{\operatorname{N}_\rho}$ für alle $\rho \neq \rho_0$.

Sei dazu $\Omega \subset \mathbb{R}^n$ ($n = r+2s = [K : \mathbb{Q}]$) definiert durch $|x_\sigma| < c_\sigma$, σ reell, $y_\tau^2 + z_\tau^2 \leq c_\tau^2$, $\tau \in S$ komplex. Und die c so, dass $0 < c_\rho < |\rho x|^{\operatorname{N}_\rho}$ für alle $\rho \neq \rho_0$ und $\prod_{\rho \in S} c_\rho = \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$. Dann ist $\operatorname{vol}(\Omega) = 2^r \pi^s c_1 \ldots c_{r+s} = 2^n \operatorname{vol}(j(\mathcal{O}_K))$. Nach Satz oben: Es ex. $j(y) \neq 0$ in Ω.

(ii) Wir zeigen: Es existieren Einheiten $\varepsilon \in E_K$ mit $\log |\rho\varepsilon|^{\operatorname{N}_\rho} < 0$ für alle $\rho \neq \rho_0$. Dazu starten wir mit $\alpha_1 \in \mathcal{O}_K$, $\alpha_1 \neq 0$, nach (i) finden wir $\alpha_2, \ldots, \alpha_n \in \mathcal{O}_K \setminus \{0\}$, s.d.

(a) $\log |\rho\alpha_{j+1}| < \log |\rho\alpha_j|$ für alle $\rho \neq \rho_0$.

(b) $|\operatorname{N}_{\mathbb{Q}}^K(\alpha_j)| \leq c$

$\Rightarrow \mathbb{N}((\alpha_j)) \leq c$. Solche Ideale gibt es nur endlich viele, also existieren $k \neq l$, s.d. $(\alpha_k) = (\alpha_l)$. Es folgt $\alpha_k = \varepsilon\alpha_l$ mit $\varepsilon \in E_K$. Dann gilt

$$\log |\rho\alpha_k| = \log |\rho\varepsilon| + \log |\rho\alpha_l|.$$

Für $k > l$ folgt $\log |\rho\varepsilon| < 0$ für $\rho_0 \neq \rho$.

(iii) Wir finden also Einheiten $\varepsilon_r ho$, $\rho \in S$, s.d. in $\lambda(\varepsilon_\rho)$ alle Koordinaten negativ sind, bis auf die ρ-te.

□

Lemma 1.8.11
Sei A reelle $m \times m$-Matrix mit

(i) $a_{kl} < 0$ für alle $k \neq l$

(ii) Alle Zeilensummen sind $= 0$.

Dann gilt $\operatorname{rk} A = m - 1$

Beweis: Es folgt $a_{kk} > 0$. Wir zeigen: die ersten $m-1$ Spalten sind linear unabhängig. Sei $\sum_{i=1}^{m-1} \lambda_i s_i = 0$. Man darf annehmen: $\lambda_k = 1$, $\lambda_j \leq 1$ für alle $j \neq k$. Dann folgt

$$0 = \sum_{i=1}^{m-1} \lambda_i a_{ki} \geq \sum_{i=1}^{m-1} a_{ki} > \sum_{i=1}^{m} a_{ki} = 0 \lightning .$$

□

Fakt 1.8.12
Wir bilden die Matrix $M = (\log |\rho\varepsilon_i|^{\mathrm{N}_\rho})_{i=1,2,\ldots,r+s-1}$, $\rho \in S$ für ein Fundamentalsystem von Einheiten $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$. M hat $r+s-1$ Zeilen, $r+s$ Spalten. Die Determinanten der Minoren vom Format $(r+s-1) \times (r+s-1)$ sind $\neq 0$ und unterscheiden sich nur um Vorzeichen. Ihr Betrag heißt **Regulator** von K, geschrieben R_K.

Beweis: Seien $v_1, \ldots, v_{n+1} \in \mathbb{R}^n$, $\sum v_i = 0$. Dann ist

$$\det(v_1, \ldots, \hat{v_i}, \ldots, v_{n+1}) = \pm \det(v_1, \ldots, \hat{v_j}, \ldots, v_{n+1}),$$

wegen $\det(v_1, \ldots, v_i + v_j, \ldots, v_{n+1}) = 0$. □

§1.9 Beispiele für Einheiten

§1.9.1 Reell quadratische ZK

$K = \mathbb{Q}(\sqrt{d})$, $d > 1$, sqf, ε_K Fundamentaleinheit, es gilt $\mathrm{N}(\varepsilon_K) = \pm 1$. Sei $d \equiv 2, 3 \pmod 4$, dann produzieren die Einheiten die ganzzahligen Lösungen der **PELLschen Gleichunen**: $a^2 - db^2 = \pm 1$:

Genauer: Ist $\mathrm{N}(\varepsilon_K) = -1$, so erhält man die $\mathbb{Z}$-Lösungen der Nicht-PELLschen Gleichungen $a^2 - db^2 = -1$ aus $\varepsilon_K^m = a_m + b_m\sqrt{d}$, m ungerade und die der PELLschen Gleichung $a^2 - db^2 = 1$ aus ε_K^m, m gerade. Ist dagegen $\mathrm{N}(\varepsilon_K) = +1$, so hat die Nicht-PELLsche Gleichung keine $\mathbb{Z}$-Lösungen, ε_K^m produziert alle $\mathbb{Z}$-Lösungen der PELLschen Gleichung.

Analog für $d \equiv 1 \pmod 4$.

Bemerkung 1.9.1
Es gibt einen Kettenbruchalgorithmus zur Berechnung der Fundamentaleinheit, siehe z.B. BOREVICH, SHAFAREVICH.

§1.9.2 Kreiseinheiten

$K = \mathbb{Q}(\zeta_p)$, $p > 2$ prim, $\zeta_p = e^{2\pi i/p}$. $[K : \mathbb{Q}] = p - 1$, $r = 0$, $s = \frac{p-1}{2}$, $\operatorname{rk} E_K = \frac{p-3}{2}$. Sei $\varepsilon_r = \frac{1-\zeta_p^r}{1-\zeta_p} = 1 + \zeta_p + \ldots + \zeta_p^{r-1}$, $1 \leq r \leq p-1$. Dann ist $\varepsilon_r \in \mathcal{O}_K$, diese sind sogar Einheiten. $\varepsilon_r^{-1} = \frac{1-\zeta_p}{1-\zeta_p^r} = \frac{1-\zeta_p^{rs}}{1-\zeta_p^r} = 1 + \zeta^r + \ldots + \zeta_p^{(s-1)r} \in \mathcal{O}_K$, $rs \equiv 1 \pmod p$.

$\varepsilon_1 = 1, \varepsilon_{p-1} = \frac{1-\zeta_p^{p-1}}{1-\zeta_p} = 1 + \zeta_p + \ldots + \zeta_p^{p-1} = -\zeta_p^{p-1}$. Bleiben $\varepsilon_2, \ldots, \varepsilon_{p-2}$ - das sind $p-3$ viele.

$$\varepsilon_{p-r} = \frac{1-\zeta_p^{p-r}}{1-\zeta_p} = \zeta_p^{p-r}\frac{(\zeta_p^r - 1)}{1-\zeta_p} = -\zeta_p^{-r}\frac{1-\zeta_p^r}{1-\zeta_p} = -\zeta_p^{-r}\varepsilon_r.$$

Bleiben also $\varepsilon_2, \ldots, \varepsilon_{\frac{p-1}{2}}$. Man kann zeigen: Diese erzeugen Untergruppe von endlichem Index in E_K.

§1.9.3 Hilfsresultat

Fakt 1.9.2
Sei $f = X^n + a_1X^{n-1} + \ldots + a_n \in \mathbb{Z}[X]$ ein EISENSTEIN-Polynom. Für $p \in \mathbb{P}$: $p \mid a_j$ für alle j und $p^2 \nmid a_n$. Sei θ Wurzel von f, dann teilt p nicht den Index $(\mathcal{O}_K : \mathbb{Z}[\theta])$ für $K = \mathbb{Q}(\theta)$.

Beweis:

(i) Sei $x \in \mathbb{Z}[\theta]$, also $x = b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1}$, $b_j \in \mathbb{Z}$. Wir zeigen $\mathrm{N}(x) \equiv b_0^n \pmod p$.

$$\mathrm{N}(x) = \prod_{\rho \in \mathrm{Hom}(K,\mathbb{C})} (b_0 + b_1\rho(\theta) + \ldots + b_{n-1}\rho(\theta)^{n-1})$$

Sei $P = \prod_{j=1}^n (X_0 + X_1Y_j + X_2Y_j^2 + \ldots + X_{n-1}Y_j^{n-1}) \in \mathbb{Z}[X, Y]$. P ist symmetrisch in $Y_1, \ldots, Y_n$, also auch die $P_\alpha(Y)$ in $P = \sum P_\alpha(Y)X^\alpha$, $\alpha = (\alpha_0, \ldots, \alpha_{n-1})$. P_α ist homogen vom Grad $\deg(\alpha) = \sum_{j=0}^{n-1} j\alpha_j$. Somit sind alle Polynome in den elementarsymmetrischen Polynomen von $Y_1, \ldots, Y_n$. Außer für $\alpha = (n, 0, \ldots, 0)$ haben sie konstanten Term 0. Nun setze man $X_i = b_i$, $Y_j = \sigma_j\theta$, $\sigma_j \in \mathrm{Hom}(K, \mathbb{C})$. Es folgt $\mathrm{N}(x) \equiv b_0^n \pmod p$ wegen $a_j \equiv 0 \pmod p$.

(ii) Sei nun $x \in \mathbb{Z}[\theta]$ und $x = py$, $y \in \mathcal{O}_K$. Dann ist $\mathrm{N}(x) \equiv 0 \pmod p$, also $b_0 = pc_0$, $c_0 \in \mathbb{N}$ nach Punkt (i). Weiter ist

$$x - pc_0 = \theta(b_1 + b_2\theta + \ldots + b_{n-1}\theta^{n-2}).$$

$\Rightarrow \mathrm{N}(x - pc_0) = p^n \mathrm{N}(y - c_0) = \mathrm{N}(\theta)\,\mathrm{N}(b_1 + b_2\theta + \ldots + b_{n-1}\theta^{n-2})$. $\mathrm{N}(\theta) = \pm a_n$, also

$$p^{n-1}\,\mathrm{N}(y - c_0) = \underbrace{\pm\left(\frac{a_n}{p}\right)}_{\in\mathbb{Z},\ \text{prim zu } p}\ \mathrm{N}(b_1 + b_2\theta + \ldots + b_{n-1}\theta^{n-2})$$

$\mathrm{N}(b_1 + b_2\theta + \ldots + b_{n-1}\theta^{n-2}) \equiv b_1^n \pmod p$ wegen (i), also $p \mid b_1$, $b_1 = c_1 \cdot p$, $c_1 \in \mathbb{Z}$ usw.

Wir zeigten: $x \in \mathbb{Z}[\theta]$, $x = py$, $y \in \mathcal{O}_K \Rightarrow y \in \mathbb{Z}[\theta]$.

(iii) Hieraus folgt: p teilt den Index $(\mathcal{O}_K : \mathbb{Z}[\theta])$ nicht. Indirekt: p teilt den Index, d.h. in $\mathcal{O}_K/\mathbb{Z}[\theta]$ existiert eine Untergruppe $\overline{A}$ der Ordung p. Sei A Urbild von $\overline{A}$ in $\mathcal{O}_K$. Dann gilt $\mathcal{O}_K \supset A \supset \mathbb{Z}[\theta]$, $(A : \mathbb{Z}[\theta]) = p$. Es folgt, dass ein $y \in A \setminus \mathbb{Z}[\theta]$ mit $py \in \mathbb{Z}[\theta]$ existiert $\lightning$.

Sei $K = \mathbb{Q}(\sqrt[4]{2})$, $[K : \mathbb{Q}] = 4$, $\omega = \sqrt[4]{2} > 0$, $\mathrm{Irr}(T, \omega, \mathbb{Q}) = T^4 - 2$ irreduzibel.

$$
\begin{aligned}
d(1,\omega,\omega^2,\omega^3) &= \det{}^2 \begin{pmatrix} 1 & 1 & 1 & 1\,\omega & i\omega & -\omega & -i\omega \\ \omega^2 & -\omega^2 & \omega^2 & -\omega^2 & & & \\ \omega^3 & -i\omega^3 & -\omega^3 & i\omega^3 & & & \end{pmatrix} \\
&= 8\det{}^2 \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \\
&= 32 \cdot \overset{2}{\det}(-8i) = -2^{11}
\end{aligned}
$$

Nach dem Fakt von oben folgt: $1,\omega,\omega^2,\omega^3$ ist Ganzheitsbasis: $\mathcal{O}_K = \mathbb{Z}[\omega]$. $r = 2$, $s = 1$, $r+s-1 = 2$, $\operatorname{rk} E_K = 2$.

Sei $L = \mathbb{Q}(\sqrt{2})$, man hat $\mathrm{N}_L^K : E_K \to E_L$. Fundamentaleinheit in E_L ist $\varepsilon_L = 1+\sqrt{2}$ (denn $a^2 - 2b^2 = -1$ hat Lösung $(1,1)$). $\varepsilon \in E_K$, $\varepsilon = \alpha + \omega\beta$, $\alpha,\beta \in \mathcal{O}_L$, $\alpha = a + b\sqrt{2}$, $\beta = c + d\sqrt{2}$.

$$\mathrm{N}_L^K(\varepsilon) = \alpha^2 - \omega\beta^2 = (a^2 + 2b^2 - 4cd) + \sqrt{2}(2ab - c^2 - 2d^2)$$

Es gilt $\mathrm{N}_L^K(1+\omega) = (1+\omega)(1-\omega) = 1-\omega^2 = 1-\sqrt{2} = -\frac{1}{1+\sqrt{2}} = -\varepsilon_L^{-1}$

□

Ende VL 12
02.12.2014

D.h. im Bild von N_K^L liegt $-\varepsilon_L$, also hat das Bild Index 1 oder 2.

Es gibt keine Einheit in E_K mit Norm -1 in E_L:

$$
\begin{aligned}
\mathrm{N}_L^K(a + b\omega^2 + \omega(c + d\omega^2)) &= ((a + b\omega^2) + \omega(c + d\omega^2)) \\
&= ((a + b\omega^2) - \omega(c + d\omega^2)) \\
&= (a + b\omega^2)^2 - \omega^2(c + d\omega^2)^2 \\
&= a^2 + 2ab\omega^2 + 2b^2 - c^2\omega^2 - 4cd - 2d^2\omega^2 \\
&= (a^2 + 2b^2 - 4cd) + \omega^2(2ab - c^2 - 2d^2) \\
&\overset{!}{=} -1
\end{aligned}
$$

$$
\begin{aligned}
a^2 + 2b^2 - 4cd &= -1 && \Rightarrow a \text{ ungerade} \\
2ab - c^2 - 2d^2 &= 0 && \Rightarrow c \text{ gerade}
\end{aligned}
$$

Also $a^2 + 2b^2 - 4cd \equiv 1 + 0, 2 \pmod 8 \not\equiv -1 \pmod 8$

Es folgt: $\mathrm{N}_L^K(E_K) = \langle -\varepsilon_L \rangle$. Sei $\varepsilon_K := 1 + \omega$.

$$
\begin{aligned}
\mathrm{N}\,\frac{1+\omega}{1-\omega} &= \mathrm{N}\,\frac{(1+\omega)^2}{1-\omega^2} \\
&= \frac{1}{(1-\omega^2)^2}\,\mathrm{N}(1+\omega)^2 \\
&= \frac{1}{(1-\sqrt{2})^2}(1-\sqrt{2})^2 = 1
\end{aligned}
$$

$$\begin{aligned}\frac{1+\omega}{1-\omega} &= \frac{(1+\omega)^2}{1-\sqrt{2}} \\ &= \frac{(1+\omega)^2(1+\sqrt{2})}{-1} \\ &= -(1+2\omega+\omega^2+\omega^2+2\omega^3+2) \\ &= -(3+2\omega+2\omega^2+2\omega^3) = \eta_K\end{aligned}$$

Dann ist $\varepsilon_K = 1+\omega$, $\eta_K = 3+2\omega+2\omega^2+2\omega^3$ Fundamentalsystem von Einheiten: Dazu genügt es zu zeigen, dass η_K den Kern von N_L^K erzeugt (bis auf Vorzeichen): Sei $\theta \in E_K$ beliebig, dann ist $\mathrm{N}_L^K = (-\varepsilon_L)^m \Rightarrow \mathrm{N}_L^K(\theta) = \mathrm{N}_L^K(\varepsilon_K^m) \Rightarrow \mathrm{N}(\theta\varepsilon_K^{-m}) = 1 \Rightarrow \theta\varepsilon_K^{-m} = \eta_K^n \Rightarrow \theta = \varepsilon_K^m\eta_K^n$.

Sei $\eta \in E_K$ mit $\mathrm{N}_L^K(\eta) = 1$. Man findet Potenz η_K und Vorzeichen, s.d. $\pm\eta\eta_K^m$ zwischen 1 und η_K liegt. Sei dies jetzt das neue $\eta := \pm\eta\eta_K^m$.

$\eta = \alpha + \omega\beta$, $\alpha = a + b\sqrt{2}$, $\beta = c + d\sqrt{2}$. Also

$$1 \le \alpha + \beta\omega < \eta_K \Rightarrow \frac{1}{\eta_K} < \frac{1}{\alpha+\beta\omega} \le 1.$$

Nun ist $\frac{1}{\alpha+\beta\omega} = \alpha - \beta\omega$, wegen $\mathrm{N}\,\eta = 1$. $\Rightarrow \frac{1}{\eta_K} < \alpha - \beta\omega \le 1$.

$$1 + \frac{1}{\eta_K} < 2\alpha < 1 + \eta_K \tag{1}$$

Analog $-1 \le \beta\omega - \alpha < -\frac{1}{\eta_K} \Rightarrow$

$$0 \le 2\beta\omega < \eta_K - \frac{1}{\eta_K} \tag{2}$$

Nun ist $1 = \mathrm{N}_{\mathbb{Q}}^K(\eta) = \eta$, $\sigma^2\eta = |\sigma\eta|^2$

$\sigma : \omega \mapsto i\omega$, $\sigma^2 : \omega \mapsto -\omega$. $\sigma^2\eta = \frac{1}{\eta}\omega$, wegen $\eta\sigma^2\eta = \mathrm{N}_L^K(\eta) = 1$. $\Rightarrow |\sigma\eta|^2 = 1$

$\sigma\eta = (a - b\sqrt{2}) + i\omega(c - d\sqrt{2})$, $|\sigma\eta|^2 = (a - b\sqrt{2})^2 + \sqrt{2}(c - d\sqrt{2})^2 = 1 \Rightarrow -1 \le a - b\sqrt{2} \le 1$ (3), $\Rightarrow -\frac{1}{\sqrt{2}} \le c - d\sqrt{2} \le \frac{1}{\sqrt{2}}$ (4)

(1): $\frac{1}{2}(1 + \frac{1}{\eta_K}) < a + b\sqrt{2} < \frac{1}{2}(1 + \eta_K)$

(2): $0 \le c + d\sqrt{2} < \frac{1}{2\omega}(\eta_K - \frac{1}{\eta_K})$.

(1)+(3): $\frac{1}{2}(1 + \frac{1}{\eta_K}) - 1 < 2a < \frac{1}{2}(1 + \eta_K) + 1$

$\Rightarrow a = 1$, $b = 0$, $c - d = 0$ (via Taschenrechner)

§1.10 Primideale in Erweiterungen

Zunerst etwas kommutative Algebra:

Definition 1.10.1
Sei A integer Ring, $S \subset A$ heißt **multiplikativ**, falls

(i) $0 \neq S$, $1 \in S$

(ii) $x, y \in S \Rightarrow xy \in S$

Beispiel 1.10.2
Es gibt Kleinste: $\{1\}$ und größte: $A \setminus \{0\}$. Wichtigstes Beispiel: $S = A \setminus \mathfrak{p}$, für $\mathfrak{p}$ prim.

Definition 1.10.3
Die **Lokalisierung** von A nach S ist

$$S^{-1}A := \{a/s : a \in A, s \in S\} \subset K = QK(A).$$

Speziell: $S = A \setminus \mathfrak{p}$, $\mathfrak{p}$ prim, dann schreibt man $A_\mathfrak{p}$ und nennt $A_\mathfrak{p}$ die Lokalisierung von A an der Stelle $\mathfrak{p}$.

Bemerkung 1.10.4
$S^{-1}A$ ist wieder ein Ring mit 1, integer. Man hat kanonischen Ringhom. $A \to S^{-1}A$: $a \mapsto a/1$.

Beispiel 1.10.5 (i) $\mathfrak{p} = (0) = \{0\}$, also $S = A \setminus \{0\}$, dann ist $A_{(0)} = K = QK(A)$.

(ii) $A = \mathbb{Z}$, $\mathfrak{p} = (p)$, $p \in \mathbb{P}$.

$$\mathbb{Z}(p) = \{\tfrac{a}{b} \in \mathbb{Q} : \mathrm{ggT}(a, b) = 1, b > 0, p \nmid b\}$$

Definition 1.10.6
Ein **lokaler Ring** ist ein kommutativer Ring mit 1, welcher genau ein maximales Ideal besitzt.

Fakt 1.10.7
Sei $\mathfrak{p} \subset A$ Primideal. Dann ist $A_\mathfrak{p}$ lokaler Ring. Sein maximales Ideal ist $m_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Der Homomorphismus $A \to A_\mathfrak{p}$ induziert injektiven Homomorphismus $A/\mathfrak{p} \to A_\mathfrak{p}/m_\mathfrak{p}$. Danei ist $A_\mathfrak{p}/m_\mathfrak{p}$ der Quotientenkörper von $A/\mathfrak{p}$. Ist insbesondere $\mathfrak{p}$ maximal, so ist $A_\mathfrak{p}/m_\mathfrak{p} = A/\mathfrak{p}$.

Beweis: Zeuerst: $m_\mathfrak{p} \cap A = \mathfrak{p}$: Die Inklusion $\mathfrak{p} \subset m_\mathfrak{p} \cap A$ ist trivial. Sei $x \in A \cap m_\mathfrak{p}$, also $x = a/s$, $a \in \mathfrak{p}$, $s \in A \setminus \mathfrak{p}$. Somit ist $sx \in \mathfrak{p}$, aber $s \notin \mathfrak{p} \Rightarrow x \in \mathfrak{p}$.

Sei $y \in A_\mathfrak{p} \setminus m_\mathfrak{p}$, also $y = x/s$, $x \in A \setminus \mathfrak{p}$, $s \in A \setminus \mathfrak{p}$. Also ist y Einheit in $A_\mathfrak{p}$ und somit $m_\mathfrak{p}$. Weiter ist jedes Ideal $\neq (1)$ in $m_\mathfrak{p}$ enthalten. Also ist $A_\mathfrak{p}$ lokaler Ring.

Der Kern von $A \to A_\mathfrak{p} \to A_\mathfrak{p}/m_\mathfrak{p}$ ist $A \cap m_\mathfrak{p} = \mathfrak{p}$, also ist $A/\mathfrak{p} \to A_\mathfrak{p}/m_\mathfrak{p}$ injektiv (Homomorphiesatz). Jedes Element aus $A_\mathfrak{p}/m_\mathfrak{p}$ hat die Form als $+m_\mathfrak{p} = (a + \mathfrak{p})(s + m_\mathfrak{p})^{-1}$, also ist dies der QK von $A/\mathfrak{p}$. □

Fakt 1.10.8
Sei A ein DED-Ring, $S \subset A$ multiplikativ. Dann ist auch $S^{-1}A$ ein DED-Ring. Die Abbildung

$$\mathrm{Id}(A) \to \mathrm{Id}(S^{-1}A) : \mathfrak{a} \mapsto S^{-1}\mathfrak{a}$$

verursacht einen Isomorphismus zwischen $\mathrm{Id}(S^{-1}A)$ und der Untergruppe von $\mathrm{Id}(A)$, welche von den Primidealen $\mathfrak{p} \subset A$ erzeugt wird, die S nicht schneiden ($\mathfrak{p} \cap S = \emptyset$).

Beweis:

(i) $S^{-1}A$ ist NOETHERsch

Sei dazu $\mathfrak{a}_s$ ein Ideal in $S^{-1}A$ und $\mathfrak{a} := \mathfrak{a}_s \cap A$. Dann gilt $\mathfrak{a}_s = S^{-1}\mathfrak{a}$: $S^{-1}\mathfrak{a} \subset \mathfrak{a}_s$ ist trivial, sei also $x \in \mathfrak{a}_s$, $x = y/s$, $y \in A$, $s \in S$. Dann folgt $y = xs \in \mathfrak{a}_s \cap A = \mathfrak{a} \Rightarrow x \in S^{-1}\mathfrak{a}$.

Ist $\mathfrak{a} = (x_1, \ldots, x_n) \subset A$ Ideal, so ist $S^{-1}\mathfrak{a} = (x_1, \ldots, x_n) \subset S^{-1}A$.

(ii) $S^{-1}A$ ist ganzabgeschlossen: Sei K der QK von A, $x \in K$ ganz über $S^{-1}A$, d.h.

$$x^n + \frac{a_1}{s_1}x^{n-1} + \ldots + \frac{a_n}{s_n} = 0, a_j \in A, s_j \in S.$$

Sei $s = s_1 \cdot \ldots \cdot s_n$, Multiplikation mit s^n zeigt: sx ganz über A, also aus A. Mithin $x \in S^{-1}A$.

(iii) Jedes Primideal $\neq (0)$ ist maximal.

Sei $\mathfrak{p}_S \subset S^{-1}A$ prim und $\neq (0)$. Dann ist auch $\mathfrak{p} := \mathfrak{p}_S \cap A$ Primideal (wh. $A/\mathfrak{p} \to S^{-1}A/S^{-1}\mathfrak{p}$ und $S^{-1}\mathfrak{p} = \mathfrak{p}_S$). Also ist $\mathfrak{p}$ maximal in A, denn $\mathfrak{p} \neq (0)$. Sei $\mathfrak{p}_S \subset m_S \subset S^{-1}A$, dann folgt durch Schnitt mit A: $\mathfrak{p} \subset m_S \cap A \subset A$. Ist $m_S \cap A = A$, so folgt $1 \in m_S \Rightarrow m_S = S^{-1}A \lightning$ (maximale Ideale sind nie der ganze Ring nach Def.). Also $m_S \cap A = \mathfrak{p}$ und es folgt

$$S^{-1}(m_S \cap A) = m_S = S^{-1}\mathfrak{p} = \mathfrak{p}_S.$$

Somit ist $\mathfrak{p}$ maximal.

(iv) $\mathrm{Id}(A) \to \mathrm{Id}(S^{-1}A) : \mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ ist surjektiv: $\mathfrak{a}_S = S^{-1}(\mathfrak{a}_S \cap A)$. Wir hatten das für ganze Ideale gesehen. Es veralgemeinert sich sofort auf gebrochene Ideale wg. $S^{-1}(\mathfrak{a}\mathfrak{b}) = S^{-1}\mathfrak{a} \cdot S^{-1}\mathfrak{b}$ (Übungsaufgabe).

Der Kern besteht aus den gebrochenene Idealen $\mathfrak{a} \subset A$, für welche $S^{-1}\mathfrak{a} (= \mathfrak{a} \cdot S^{-1}A) = S^{-1}A$ gilt. Das ist genau dann der Fall, wenn $\exists a \in \mathfrak{a}, s \in S : a/s = 1 \Leftrightarrow a = s \Leftrightarrow \mathfrak{a} \cap S \neq \emptyset$.

□

Bemerkung 1.10.9 (i) Lokalisierung eliminiert Ideale.

(ii) Die maximalen Ideale von $S^{-1}A$ sind in Bijektion zu denjenigen A, welche S nicht schneiden via

$$m_S \mapsto m_S \cap A$$

und umgekehrt

$$m \mapsto S^{-1}m.$$

Ende VL 13
03.12.2014

Folgerung 1.10.10
Seu A DED-Ring, $\mathfrak{p} \subset A$, $\mathfrak{p} \neq (0)$ Primideal, $S = A \setminus \mathfrak{p}$. Dann ist $A_\mathfrak{p}$ ein DED-Ring mit genau einem maximalen Ideal $\mathfrak{m}_\mathfrak{p} = \mathfrak{p} \cdot A_\mathfrak{p}$. $A_\mathfrak{p}$ ist HIR, jedes gebrochene Ideal hat die Form $\mathfrak{m}_\mathfrak{p}^m$, $m \in \mathbb{Z}$ (falls Exponent nicht negativ, dann echtes Ideal).

Beweis: Jedes Primideal $\mathfrak{q} \neq \mathfrak{p}$ schneidet S. Also $\mathrm{Id}(A_\mathfrak{p}) = \langle m_\mathfrak{p} \rangle$. Sei $\pi \in m_\mathfrak{p} \setminus m_\mathfrak{p}^2$, dann ist $m_\mathfrak{p}^2 \subsetneq (\pi) \subset m_\mathfrak{p} \Rightarrow m_\mathfrak{p} = (\pi)$. □

Definition 1.10.11
Ein lokaler Ring, der HIR ist, heißt **diskreter Bewertungsring**.

Beispiel 1.10.12 (i) $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \setminus \{0\}, \mathrm{ggT}(a,b) = 1, p \nmid b\}$.

(ii) Diskrete Bewertungsringe sind nach den Körpern die einfachsten Ringe.

Bemerkung 1.10.13
Sei O dBR, $\mathfrak{m} = (\pi)$ sein maximales Ideal. Dann läss sich jedes $x \in K^\times$ ($K = QK(O)$) eindeutig

schreiben als $x = \pi^m \cdot u$, $m \in \mathbb{Z}$, $u \in O^\times$. Damit hat man

$$\nu_{\mathfrak{m}} : K^\times \to \mathbb{Z} : x \mapsto m = \mathrm{ord}_\pi(x).$$

Das ist eine sogenannte Exponentenbewertung auf K:

(i) $\nu(xy) = \nu(x) + \nu(y)$

(ii) $\nu(x+y) \geq \min(\nu(x), \nu(y))$

Fakt 1.10.14
Sei A ein DED-Ring, dann gilt in $K = QK(A)$: $A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$.

Beweis: Klar ist $A \subset \bigcap A_{\mathfrak{p}}$, sei also $0 \neq x \in \bigcap A_{\mathfrak{p}}$. Es gilt $(x) = \mathfrak{p}_1^{m_1} \cdot \ldots \cdot \mathfrak{p}_r^{m_r}$ für gewisse $m_j \in \mathbb{Z}$ und $\mathfrak{p}_i \neq \mathfrak{p}_j$ für alle $i \neq j$. Also $xA_{\mathfrak{p}_i} = \mathfrak{m}_i^{m_i} \Rightarrow m_i \geq 0$. Somit $x \in A$. □

Fakt 1.10.15
Hat der DED=Ring A nur endlich viele Primideale, so ist er ein HIR.

Beweis: Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_N$ alle maximalen Ideale in A, $\pi \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$. Wähle $x \in A$ mit $x \equiv \pi \pmod{\mathfrak{p}_1^2}$, $x \equiv 1 \pmod{\mathfrak{p}_j}$ für alle $j \in 1, \ldots, N$. Dann ist $(x) = \mathfrak{p}_1$. □

Nun wieder Arithmetik: Sei L/K eine endliche Erweiterung von ZK, mit $\mathfrak{p} \subset \mathcal{O}_K$ maximal ist $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$

Man studiert Zerlegungsverhalten von Primidealen in Erweiterungen alias Reziprozitätsgesetze.

Fakt 1.10.16
Sei L/K endliche, separabel, $A \subset K$ DED-Ring mit QK K, B der ganze Abschluss von A in L. Dann ist auch B ein DED-Ring.

Beweis: B ist ganzabgeschlossen, denn Ganzheit ist transitiv.

Sei $\mathfrak{P} \neq (0)$ Primideal in B. Dann ist $\mathfrak{P} \cap A = \mathfrak{p}$ ein Primideal in A, denn $A/\mathfrak{p} \to B/\mathfrak{P}$ ist injektiv. Wir zeigen: $\mathfrak{p} \neq (0)$. Ist $x \in \mathfrak{P} \setminus \{0\}$, so gilt

$$\mathrm{Irr}(T, x, K) = T^n + a_1 T^{n-1} + \ldots + a_n, \qquad a_j \in A.$$

Dieses Polynomm ist irreduzibel über K, also ist $a_n \neq 0$ und $a_n \in \mathfrak{P} \cap A$: $a_n = -x^n - a_1 x^{n-1} - \ldots - a_{n-1} x \in \mathfrak{P}$. B/FP ist integer. Sei M maximales Ideal in $B/\mathfrak{P}$, $\mathfrak{m} = M \cap A/\mathfrak{p}$. Dies ist nicht $A/\mathfrak{p}$, da sonst $1 \in M$. $A/\mathfrak{p}$ ist Körper, also ist $\mathfrak{m} = (0)$. Ist $M \neq (0)$, so haben wir also $\overline{x} \in M$, $\overline{x} \neq 0$, $x \in B$ Urbild. x ist ganz über A, also $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, $a_j \in A$. Also $\overline{x}^n + \overline{a_1 x}^{n-1} + \ldots + \overline{a_n} = 0$, d.h. $\overline{x}$ ist algebraisch über $A/\mathfrak{p}$. Bilde $\mathrm{Irr}(T, \overline{x}, A/\mathfrak{p}) = T^k + \alpha_1 T^{k-1} + \ldots + \alpha_k$, $\alpha_j \in A/\mathfrak{p}$. Dann ist $\alpha_k \neq 0$, wegen Irreduzibilität. α_k liegt in M: $\alpha_k = -\overline{x}^k - \alpha_1 \overline{x}^{k-1} - \ldots - \alpha_{k-1}\overline{x} \in M$. Also liegt α_k in $M \cap A/\mathfrak{p} = (0)$ ↯. Somit ist $\mathfrak{P}$ maximal.

Nun: B ist NOETHERsch. Sei $\omega_1, \ldots, \omega_n$ K-Basis von L, man darf annehmen $\omega_j \in B$. Sei $\omega_1', \ldots, \omega_n'$ duale Basis unter der Spurform $(\mathrm{Tr}_K^L(\omega_i \omega_j') = \delta_{ij})$. Man findet $c \in A$, $c \neq 0$, s.d. $c\omega_1', \ldots, c\omega_n'$ aus B sind. Sei $x \in B$, $x = a_1\omega_1 + \ldots + a_n\omega_n$. Dan ist $a_j = \mathrm{Tr}(x\omega_j')$, also $ca_j = \mathrm{Tr}(cx\omega_j') \in A$. Somit $B \subset Ac^{-1}\omega_1 + \ldots + Ac^{-1}\omega_n$. B ist also Untermodul eines endlich erzeugten A-Moduls. Ist A NOETHERsch, so ist jeder Untermodul eines endlich erzeugten Moduls selbst endlich erzeugt (Algebra 1). □

Bemerkung 1.10.17
B ist endlich erzeugter A-Modul, torsionsfrei, aber im Allgemeinen nicht frei.

Definition 1.10.18
Sei A ein DED-Ring, $\mathfrak{p} \subset A$ maximal. Ein maximales Ideal $\mathfrak{P} \subset B$ **liegt über** $\mathfrak{p}$ genau dann, wenn $\mathfrak{P} \cap A = \mathfrak{p}$.

Fakt 1.10.19 (i) $\mathfrak{P} \cap A = \mathfrak{p}$ ist maximales Ideal in A.

(ii) Für jedes $\mathfrak{p}$ existieren $\mathfrak{P}$ mit $\mathfrak{p} \cap A = \mathfrak{p}$,

(iii) deren Anzahl ist endlich.

Beweis:

(i) $\mathfrak{p} = \mathfrak{P} \cap A$ ist jedenfalls Primideal: $A/\mathfrak{p} \to B/\mathfrak{P}$ ist Einbettung. Ist $\mathfrak{p}$ nicht maximal, so bleibt nur $\mathfrak{p} = (0)$. Aber $\mathfrak{P} \neq (0)$ enthält Elemente aus $A \setminus 0$. $x \in \mathfrak{P}$, $\mathrm{Irr}(T, x, K) = T^n + \ldots + a_n$, $a_n \neq 0$, $a_n \in \mathfrak{P} \cap A$.

(ii) Wir zeigen $\mathfrak{p}B \neq B$. Sei dazu $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, also $(pi) = \mathfrak{p}\mathfrak{a}$ mit $\mathfrak{p} \nmid \mathfrak{a}$. Also sind $\mathfrak{p}$ und $\mathfrak{a}$ teilerfremd. $\mathfrak{p} \subsetneq \mathfrak{p} + \mathfrak{a}$, da sonst $\mathfrak{a} \subset \mathfrak{p} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$. Also $\mathfrak{p} + \mathfrak{a} = A$, somit existieren $p \in \mathfrak{p}$, $a \in \mathfrak{a}$ mit $p + a = 1$. Dabei ist $a \in \mathfrak{p}$, da sonst $1 \in \mathfrak{p}$ $\lightning$. Weiter gilt $a\mathfrak{p} \subset \mathfrak{a}\mathfrak{p} = \pi A$. Angenommen $\mathfrak{p}B = B$, dann folgt $aB = a\mathfrak{p}B \subset \mathfrak{a}\mathfrak{p}B = \pi B$. Also $a = \pi b$, $b \in B$. Außerdem $a \in A$, $\pi \in A$, also $b \in K$. Es gilt $B \cap K = A$ (A ganzabgeschlossen). Also ist $b \in A$. Aus $a = \pi b$ folgt $a \in \mathfrak{p}$ $\lightning$. Damit ist $\mathfrak{p}B \neq B$. Also existieren maximale Ideale $\mathfrak{P}$ mit $\mathfrak{p}B \subset \mathfrak{P} \subsetneq B$. $\mathfrak{P} \cap A$ enthält $\mathfrak{p}$ und ist Primideal in A, ist also gleich $\mathfrak{p}$.

(iii) Die Endlichkeitsaussage: $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$. Sei $\mathfrak{P} \subset B$ maximal und $\mathfrak{P} \cap A = \mathfrak{p}$. Es folgt $\mathfrak{p} \subset \mathfrak{p}$, also $\mathfrak{p}B \subset \mathfrak{p}$, also $\mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g} \subset \mathfrak{P} \Rightarrow \mathfrak{P} \mid \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g} \Rightarrow \mathfrak{P} = \mathfrak{P}_i$.

□

Bemerkung 1.10.20 (i) In DED-Ringen gilt $\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow \mathfrak{b} \mid \mathfrak{a}$, d.h. es existiert $\mathfrak{c}$ ganz mit $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ ($\mathfrak{c} = \{x \in K : x\mathfrak{b} \subset \mathfrak{a}\} \subset A$).

(ii) $\mathfrak{P} \mid \mathfrak{p} :\Leftrightarrow \mathfrak{P} \mid \mathfrak{p}B$

Definition 1.10.21
$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$, $e(\mathfrak{P}/\mathfrak{p})$ heißt **Verzweigungsindex**. Der Grad der Körpererweiterung $[B/\mathfrak{P} : A/\mathfrak{p}]$ heißt **Restklassengrad** $f(\mathfrak{P}/\mathfrak{p})$.

- $\mathfrak{p}$ heißt **verzweigt** in $L :\Leftrightarrow e(\mathfrak{P}/\mathfrak{p}) = 1$ für alle $\mathfrak{P} \mid \mathfrak{p}$
- $\mathfrak{p}$ heißt **voll zerlegt** in $L :\Leftrightarrow \mathfrak{p}$ unverzweigt und $f(\mathfrak{P}/\mathfrak{p}) = 1$ für alle $\mathfrak{P} \mid \mathfrak{p}$
- $\mathfrak{p}$ heißt **träge** in $L :\Leftrightarrow \mathfrak{p}$ ist unverzweigt in L und hat in L nur einen Primteiler, d.h. $\mathfrak{p}B = \mathfrak{P}$ maximal.

Bemerkung 1.10.22
Ist A DED-Ring mit QK K, L endlich, separable Erweiterung, B der ganze Abschluss von A in L, $\mathfrak{a} \subset A$ Ideal $\neq (0)$. Dann gilt $\mathfrak{a}B \cap A = \mathfrak{a}$.

Denn $\mathfrak{a} \subset \mathfrak{a}B \cap A$ ist klar, sei $\mathfrak{a} = \mathfrak{p}^r \cdot \mathfrak{q}$, $\mathfrak{p} \nmid \mathfrak{q}$. $b := \mathfrak{a}B \cap B$, $\mathfrak{b} = \mathfrak{p}^s q'$, $\mathfrak{p} \nmid \mathfrak{q}$, dann ist $s \leq r$. Wir haben zu zeigen $r = s$. Lokalisieren mit $S = A \setminus \mathfrak{p}$ liefert die Situation A dBR, $\mathfrak{a} = \mathfrak{p}^r = (\pi^r)$, $\mathfrak{a}B = \pi^r B = \{\pi^r B : b \in B\}$, $\mathfrak{a}B \cap A = \{\pi^r b : b \in B\} \cap A$. $\pi^r b \in K \Leftrightarrow b \in K$, also $\mathfrak{a}\mathfrak{b} \cap A = \pi^r A \Rightarrow r = s$. Folgelich ist $\mathrm{Id}(K) \to \mathrm{Id}(L)$ injektiv: $\mathfrak{a}B = \mathfrak{b}B \Rightarrow \mathfrak{a}B \cap A = \mathfrak{b}B \cap A \Rightarrow \mathfrak{a} = \mathfrak{b}$.

Satz 1.10.23 („Satz 7“)
Seien L/K, A, B wie oben, $\mathfrak{p} \subset A$ maximal. Dann gilt:

$$[L:K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p})$$

Ende VL 14
09.12.2014

Beweis (mittels Lokalisierung):

Sei $S = A \setminus \mathfrak{p}$, dann ist $S^{-1}A$ ein diskreter Bewertungsring, $S^{-1}B$ ist ein DED-Ring mit nur endlich vielen Ringidealen: Es kommen nur $\mathfrak{P} \cap S \neq \emptyset$ in Frage. $\Rightarrow \mathfrak{P} \cap A \subset \mathfrak{p} \Rightarrow \mathfrak{P} \cap A = \mathfrak{p}$, also $\mathfrak{P} \mid \mathfrak{p}$. Also ist $S^{-1}B$ HIR (nach chinesischem Restsatz). $S^{-1}B$ ist der ganze Abschluss von $S^{-1}A$ in L: Sei dazu $x \in B$, $s \in S \Rightarrow x/s \in L$ ganz über $S^{-1}A$:

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad a_j \in A$$

$\Rightarrow \left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \ldots + \frac{a_n}{s_n} = 0$ ist Ganzheitsgleichung für x/s über $S^{-1}A$. Sei $y \in L$ ganz über $S^{-1}A$, also

$$y^n + \frac{a_1}{s_1} y^{n-1} + \ldots + \frac{a_n}{s_n} = 0.$$

Multiplikation mit s^n, $s = s_1 \cdot \ldots \cdot s_n$ zeigt

$$(sy)^n + a_1'(sy)^{n-1} + \ldots + a_n' = 0 \qquad a_j' \in A.$$

Also ist sy ganz über $A \Rightarrow sy \in B \Rightarrow y \in S^{-1}B$.

Wir haben die Aufgabe nun vereinfacht: A dBR, B endlich erzeugter A-Modul, ist HIR und torsionsfrei als A-Modul, da B in einem Körper liegt. Algebra 1: Dann ist B freier A-Modul. Sei $b_1, \ldots, b_n$ eine Basis von B als A-Modul. Wir zeigen, dass dann die Bilder $\overline{b_1}, \ldots, \overline{b_n}$ in $B/\mathfrak{p}B$ linear unabhängig über $A/\mathfrak{p}$ sind. Sei $\sum \overline{a}_j \overline{b}_j = 0$, $\overline{a}_j \in A/\mathfrak{p}$. Nun folgt $\sum a_j b_j \in \mathfrak{p}B$ (a_j Urbild von $\overline{a}_j$ in A). $\Rightarrow \sum a_j b_j = \sum c_j b_j$, $c_j \in \mathfrak{p} \Rightarrow a_j = c_j \ \forall j \Rightarrow \overline{a_j} = 0$. Somit

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \mathrm{rk}_A B = [L:K].$$

(Letztes, weil eine A-Basis von B auch eine K-Basis von L ist.)

Sei $\mathfrak{p}B = \mathfrak{P}_1^{e+1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$. Wir haben Isomorphismus von $A/\mathfrak{p}$-VR

$$B/\mathfrak{p}B \to \bigoplus_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}.$$

Wir zeigen $\mathfrak{P}^r/\mathfrak{P}^{r+1} \cong B/\mathfrak{P}$ als $A/\mathfrak{p}$=VR: Sei $\mathfrak{P} = (\Pi)$, $B \to \mathfrak{P}^r/\mathfrak{P}^{r+1}$: $x \mapsto x\Pi^r + \mathfrak{P}^{r+1}$. Das ist surjektiver Homomorphismus von A-Moduln. Der Kern ist $(\Pi) = \mathfrak{P}$.

$$[L:K] = \dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{\mathfrak{P}|\mathfrak{p}} \dim_{A/\mathfrak{p}} B/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})} = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}).$$

□

Bemerkung 1.10.24 (i) Es fehlen noch die Formeln (Übungsaufgaben)

- $e(S^{-1}\mathfrak{P}/S^{-1}\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$
- $f(S^{-1}\mathfrak{P}/S^{-1}\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$

(ii)
- $S^{-1}(\mathfrak{ab}) = S^{-1}\mathfrak{a} \cdot S^{-1}\mathfrak{b}$
- $A/\mathfrak{p} = S^{-1}A/S^{-1}\mathfrak{p}$, $B/\mathfrak{p} = S^{-1}B/S^{-1}\mathfrak{P}$

(iii) Im Fall $K/\mathbb{Q}$ ist alles viel einfacher: $p \in \mathbb{P}$, $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$. $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ hat $\mathbb{F}_p$-Dimension $[K : \mathbb{Q}]$, $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \bigoplus \mathcal{O}_K/\mathfrak{p}_i^{e_i}$. $\operatorname{card} \mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}} = (\mathcal{O}_K : \mathfrak{p}^{e_\mathfrak{p}}) = \mathbb{N}(\mathfrak{p}^{e_\mathfrak{p}}) = (\mathbb{N}\mathfrak{p})^{e_\mathfrak{p}}$. Also $[K : \mathbb{Q}] = \sum_{\mathfrak{p}|p} e(\mathfrak{p}/p)f(\mathfrak{p}/p)$.

(iv) Der Satz zeigt: über $\mathfrak{p}$ liegen in B höchstens $[L : K]$ maximale Ideale.

Fakt 1.10.25 (Multiplikativität von e und f)
Seien $K \subset L \subset M$ endliche separable Erweiterungen, A DED-Ring in K, B sein ganzer Abschluss mit C = ganzer Abschluss in M. Sei Q Primideal in C über $\mathfrak{P}$ = Primideal in B über $\mathfrak{p}$ = Primideal in A. Dann gilt

(i) $e(Q/\mathfrak{p}) = e(Q/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$

(ii) $f(Q/\mathfrak{p}) = f(Q/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$

Beweis: Klar. □

Fakt 1.10.26
Sei L/K GALOIS-Erweiterung mit GALOISgruppe G. $A \subset K$ DED-Ring, B ganzer Abschluss in L. Sei $\mathfrak{p} \subset A$ maximales Ideal. Dann operiert G transitiv auf $\mathfrak{P}/\mathfrak{p}$ und es gilt $e(\mathfrak{P}/\mathfrak{p}), f(\mathfrak{P}/\mathfrak{p})$ sind gleich für alle $\mathfrak{P}/\mathfrak{p}$. Also

$$\mathfrak{p}B = \left(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}\right)^e$$

Beweis: Seien $\mathfrak{P}_1, \mathfrak{P}_2$ zwei Primteiler von $\mathfrak{p}$ und $\sigma\mathfrak{P}_1 \neq \mathfrak{P}_2$ für alle $\sigma \in G = \operatorname{Gal}(L/K)$. Dann folgt $\sigma\mathfrak{P}_1 \neq \tau\mathfrak{P}_2$ für alle $\sigma, \tau \in G$. Also ex. $x \in B$ mit $x \equiv 0 \pmod{\sigma\mathfrak{P}_1}$ für alle $\sigma \in G$ und $x \equiv 1 \pmod{\tau\mathfrak{P}_2}$ für alle $\tau \in G$ (chinesischer Restsatz). $\mathrm{N}_K^L(x) = \prod_{\sigma \in G} \sigma x$ liegt in A, da ganz und in K. Also $N(x) \in A \cap \mathfrak{P}_1 = \mathfrak{p}$. Andererseits ist $\sigma x \notin \mathfrak{P}_2$ für alle $\sigma \in G$. Somit auch $\mathrm{N}(x) \notin \mathfrak{P}_2 \Rightarrow \mathrm{N}(x) \notin \mathfrak{P}_2 \cap A = \mathfrak{p}$ ↯.

Die GALOISgruppe operiert also transitiv auf den $\mathfrak{P}/\mathfrak{p}$. $\sigma \in G$ verursacht Isomorphismus $B/\mathfrak{P} \to B/\sigma\mathfrak{P}$: $x + \mathfrak{P} \mapsto \sigma x + \sigma\mathfrak{P}$, also $f(\sigma\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$. $\mathfrak{p}B = \prod \mathfrak{P}^{e_\mathfrak{P}} = \prod(\sigma\mathfrak{P})^{e_\mathfrak{P}} \Rightarrow e_\mathfrak{P}$ ist dasselbe für alle $\mathfrak{P} \mid \mathfrak{p}$. □

Fakt 1.10.27
Sei K ein algebraischer ZK, dann ist $p \in \mathbb{P}$ in K verzweigt $\Leftrightarrow p$ teilt die Diskriminante d_K.

Beispiel 1.10.28
$K = \mathbb{Q}(i)$, nur $p = 2$ ist verzweigt: $2 = -i(1+i)^2$, $d_K = \det^2 \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} = -4$.

Beweis: $A = \mathcal{O}_K/p\mathcal{O}_K$ ist endliche $\mathbb{F}_p$-Algebra[7], kommutativ mit 1. p ist genau dann verzweigt, wenn A nilpotente Elemente enthält. Ist $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_g$ mit paarweise verschiedenen Faktoren, so ist

$$\mathcal{O}_K/p\mathcal{O}_K = \bigoplus_i \mathcal{O}_K/\mathfrak{p}_i = \bigoplus_i \mathbb{F}_{p_i^f}.$$

[7] K Körper, A ist K-Algebra $:\Leftrightarrow A$ ist K-Vektorraum und A hat Multiplikation, die sich mit der VR-Struktur verträgt, d.h. bilinear ist

Ist p verzeigt, so sitzt in A Teilalgebra $\mathcal{O}_K/\mathfrak{p}^e\mathcal{O}_K$, $e \geq 2$. Das Element $\overline{x}$ für $x \in \mathfrak{p} \setminus \mathfrak{p}^2$ ist nilpotent.

Wir definieren eine Spur auf A: $a \in A$, $\mathrm{Tr}^A_{\mathbb{F}_p}(a) = \mathrm{Tr}^A_{\mathbb{F}_p}(a : A \to A, x \mapsto ax)$. Es gilt $\mathrm{Tr}(a) \in \mathbb{F}_p$. Für $x \in \mathcal{O}_K$ und $\overline{x} \in A$ Bild von x gilt $\mathrm{Tr}^K_{\mathbb{Q}}(x) \equiv \mathrm{Tr}^A_{\mathbb{F}_p}(\overline{x}) \pmod p$(∗):

Ist $\omega_1, \ldots, \omega_n$ Ganzheitsbasis von $\mathcal{O}_K$, so ist $\overline{\omega}_1, \ldots, \overline{\omega}_n$ $\mathbb{F}_p$-Basis von A: sie erzeugen A als $\mathbb{F}_p$-Basis und $\dim_{\mathbb{F}_p} A = \mathrm{rk}_{\mathbb{Z}} \mathcal{O}_K = n$. Sei $x\omega_i = \sum m_{ij}\omega_j$, $m_{ij} \in \mathbb{Z}$, dann ist $\mathrm{Tr}^K_{\mathbb{Q}}(\overline{x}) = \sum m_{ii}$ und $\mathrm{Tr}^A_{\mathbb{F}_p}(\overline{x}) = \sum \overline{m}_{ii}$. Weiter hat A eine Zerlegung

$$A = \bigoplus_{\mathfrak{p}|p} A_{\mathfrak{p}},$$

wobei $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p}/p)}$, $A_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}^{e(\mathfrak{p}/p)}$ (chinesischer Restsatz). Dabei sind die $A_{\mathfrak{p}}$ invariant unter Multiplikation. Deshalb gilt $\mathrm{Tr}^A_{\mathbb{F}_p}(a) = \sum_{\mathfrak{p}|p} \mathrm{Tr}^{A_{\mathfrak{p}}}_{\mathbb{F}_p}(a)$. Sei $a_1, \ldots, a_n$ eine $\mathbb{F}_p$-Basis von A, d_A die Diskriminante: $d_A(a_1, \ldots, a_n) := \det(\mathrm{Tr}^A_{\mathbb{F}_p}(\omega_i\omega_j))$. Dann gilt für andere Basis $b_1, \ldots, b_n$: $d_A(b_1, \ldots, b_n) = c^2 d_A(a_1, \ldots, a_n)$, für ein $c \in \mathbb{F}_p^\times$. Aus (∗) folgt: Ist $a_1, \ldots, a_n$ Ganzheitsbasis, so ist $d_A(\overline{a}_1, \ldots, \overline{a}_n = 0$ in $\mathbb{F}_p \Leftrightarrow d_k \equiv 0 \pmod p$. Es gilt $d_{A\oplus B} = d_A \cdot d_B$:

$a_1, \ldots, a_k$ Basis von A, $b_1, \ldots, b_l$ Basis von B. Dann ist $\mathrm{Tr}() = \begin{pmatrix} \mathrm{Tr}(a_ia_j) & 0 \\ 0 & \mathrm{Tr}(b_rb_s) \end{pmatrix}$ (0, weil Spur von $(a_i, 0) \cdot (0, b_j) = (0, 0)$) .

Es folgt

$$d_A = \prod_{\mathfrak{p}|p} d_{A_{\mathfrak{p}}}.$$

Sei $A_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}^e$, $e \geq 2$. $A_{\mathfrak{p}}$ hat $A_{\mathfrak{p}}$-invariante Teilräume $A_{\mathfrak{p}} \supset \mathfrak{p}/\mathfrak{p}^e \supset \ldots \supset \mathfrak{p}^{e-1}/\mathfrak{p}^e$. Wähle $\mathbb{F}_p$-Basis von $\mathfrak{p}^{e-1}/\mathfrak{p}^e$, ergänze Basis zu Basis von $\mathfrak{p}^{e-2}/\mathfrak{p}^e$

In der obigen Basis sind also in der Matrix zu x die Diagonalelemente alle gleich 0. Also ist $\mathrm{Tr}^{A_{\mathfrak{p}}}_{\mathbb{F}_p}(x) = 0$. Die Matrix zu $d_{A_{\mathfrak{p}}}$ sieht also so aus:

$$\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}.$$

Es folgt $d_{A_{\mathfrak{p}}} = 0$, also $p \mid d_K$. Ist p unverzweigt, so ist $A_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ für alle $\mathfrak{p} \mid p$ eine endlich Erweiterung von $\mathbb{F}_p$, also $d_A \neq 0$, denn $\mathbb{F}_{p^n}/\mathbb{F}_p$ stets separabel:

$$T^{p^n} - T = f(T), f'(T) = -1$$

$\Rightarrow$ Spurform ist nichtausgerartet $\Rightarrow \det(\mathrm{Tr}(a_ia_j)) \neq 0$ für $\mathbb{F}_p$-Basen $a_1, \ldots, a_n$. □

Ende VL 15
10.12.2014

Folgerung 1.10.29
Sei L/K endliche Erweiterung von ZK, dann in $\mathcal{O}_K$ nur endlich viele Primideale verzweigt in $\mathcal{O}_L$.

Beweis: Mult. des Verzw.index. □

Folgerung 1.10.30
In $K/\mathbb{Q}$, $K \neq \mathbb{Q}$ gibt es stets verzweigte Primzahlen.

Beweis: $|d_K| > 1$. □

Beispiel 1.10.31 (E. ARTIN)
$f = T^5 - T + 1 \in \mathbb{Z}[T]$. Diskriminante: $d(T^5 + a^T + b) = A \cdot a^5 + B \cdot b^4$.

Gesucht: A, B. Wähle $a = -1$, $b = 0$. Wurzeln sind $0, \pm 1, \pm i$. Dann ist $d^8 = (1-i)^2 2^2 (1+i)^2 (-1+i)^2 (2i)^2 (-1-i)^2 1^2 i^2 (-1)^2 (-i)^2 = -2^8 = -A \Rightarrow A = 2^8$. Wähle $a = 0$, $b = -1$. Wurzeln sind $\zeta_5^r = e^{2\pi i r/5}$. Damit $d = \det(\sum_{k=0}^{5} \zeta_5^{ik} \zeta_5^{kj}) = \det \begin{pmatrix} 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \end{pmatrix} = 5^5$

$d(T^5 + aT + b) = 2^8 a^5 + 5^5 b^4$, $d(T^5 - T + 1) = 5^5 - 2^8 = 3125 - 256 = 19 \cdot 151$.

(i) f ist irred. modulo 5.

f hat keine Wurzeln in $\mathbb{F}_5$, aber auch keine in $\mathbb{F}_2 5$: Sei $\omega^2 = 2$, $\omega \in \overline{\mathbb{F}_5}$, dann ist $\mathbb{F}_2 5 = \{\alpha + \omega\beta : \alpha, \beta \in \mathbb{F}_5\}$. Sei $\theta = \alpha + \omega\beta$ Wurzel von f, $\theta^5 = a^5 + \beta^5 \omega^5 = \alpha + 4\beta\omega$, also $0 = \theta^5 - \theta = \alpha + 4\beta\omega - \alpha - \beta\omega + 1 = 1 + 3\beta\omega$ ↯ (denn $3\beta\omega = -1$ impliziert $\omega \in \mathbb{F}_5$ ↯).

Also ist f auch irreduzibel in $\mathbb{Z}[T]$. Sei $\theta \in \overline{\mathbb{Q}}$ Nullstelle von f und $K = \mathbb{Q}(\theta)$, dann ist $[K : \mathbb{Q}] = 5$. Weiter ist $\mathcal{O}_K = \mathbb{Z}[\theta]$, da $disc(1, \theta, \theta^2, \theta^3, \theta^4) = disc(f) = 19 \cdot 151$ quadratfrei ist.

(ii) f modulo 2.

$\overline{f}(T) = (T^2 + T + 1)(T^3 + T^2 + 1)$. Die Faktoren sind irreduzibel, da ohne Nullen in $\mathbb{F}_2$. Es gilt $\mathcal{O}_K = \mathbb{Z}[\theta] = \mathbb{Z}[T]/(f) \Rightarrow \mathcal{O}_K/2\mathcal{O}_K = \mathbb{F}_2[T]/(\overline{f}) = \mathbb{F}_2[T]/(\overline{g}) \oplus \mathbb{F}_2[T]/(\overline{h}) = \mathbb{F}_4 \oplus \mathbb{F}_8$. $\Rightarrow 2\mathcal{O}_K = \mathfrak{p}_2 \cdot \mathfrak{p}_2'$, $f(\mathfrak{p}_2) = 2$, $f(\mathfrak{p}_2') = 3$, $\mathbb{N}\mathfrak{p}_2 = 4$, $\mathbb{N}\mathfrak{p}_2' = 8$.

(iii) f modulo 3 $\overline{f} \in \mathbb{F}_3[T]$ ist irreduzibel: keine Wurzeln in $\mathbb{F}_3$, auch keine in $\mathbb{F}_9 = \{\alpha + \beta\omega : \alpha, \beta \in \mathbb{F}_3\}$, $\omega \in \overline{\mathbb{F}_3}$, $\omega^2 = 2$. Sei $\theta = \alpha + \beta\omega$ Wurzel, also $\theta^5 - \theta + 1 = 0 \Rightarrow \theta^6 = \theta^2 - \theta$.

$$\begin{aligned} \theta^6 = (\theta^2)^3 &= (\alpha^2 + 2\alpha\beta\omega + 2\beta^2)^3 \\ &= \alpha^2 + 2\beta^2 + 4\alpha\beta\omega \\ \theta^2 - \theta &= \alpha^2 + 2\beta^2 + 2\alpha\beta\omega - \alpha - \beta\omega \\ &\Rightarrow 4\alpha\beta\omega = -\alpha + (2\alpha - 1)\beta\omega \\ &\Rightarrow a = 0, 2\alpha\beta - \beta - 4\alpha\beta = 0 \Rightarrow \beta = 0 \text{ ↯} \end{aligned}$$

Somit ist $\mathcal{O}_K/3\mathcal{O}_K = \mathbb{F}_3[T]/(\overline{f})$ Körper $= \mathbb{F}_{3^5} = \mathbb{F}_{243} \Rightarrow 3\mathcal{O}_K = \mathfrak{p}_3$, $f(\mathfrak{p}_3/3) = 5$, $\mathbb{N}\mathfrak{p}_3 = 3^5 = 243$

(iv) f über $\mathbb{R}$

$f'(T) = 5T^4 - 1$ hat genau 2 reelle Nullstellen $\pm\frac{1}{\sqrt[4]{5}}$. Also liegen dort relative Extrema von f. $f''(T) = 20T^3$. $\Rightarrow$ bei $-\frac{1}{\sqrt[4]{5}}$ rel. Maximum und bei $\frac{1}{\sqrt[4]{5}}$ rel. Minimum. Schaut man sich deren Lage und das Verhalten im unendlichen an, wird klar: f hat genau eine reelle

[8] Produkt aller Differenzen von Wurzeln zum Quadrat

Nullstelle. Also $\mathrm{rk}(f) = 1$, $s(K) = 2$. Die MINKOWSKI-Konstante ist also

$$\frac{5!}{5^5}\left(\frac{4}{\pi}\right)^2 \sqrt{19 \cdot 151} < 4.$$

Also wird Cl_K erzeugt von ganzen Idealen der Absolutnorm < 4. Es gibt keine ganzen Ideale der Norm 2 oder 3 nach Punkt 2 und 3. Also ist $\mathrm{Cl}_K = 1$ und $h_K = 1$.

Man kann zeigen: Die GALOIS-Gruppe dieses Polynoms ist $\mathrm{Gal}(f) = S_5$. Sei E der Zerfällungskörper von f über $\mathbb{Q}$, dann liegt $\mathbb{Q}(\sqrt{19 \cdot 151})$ in E. ARTIN hat gezeigt: $E/IQ(\sqrt{(}19 \cdot 151))$ ist unverzweigt. Das ist eine unverzweigte A_5 Erweiterung.

Ende VL 16
16.12.2014

§1.11 Beispiele zum Zerlegungsverhalten

Der Prototyp ist hierbei $\mathbb{Q}(i)/\mathbb{Q}$.

Satz 1.11.1 (KUMMER)
Sei L/K eine endliche Erweiterung von Zahlkörpern, $p(X) = \mathrm{Irr}(X, \theta, K)$ und $\mathcal{O}_L = \mathcal{O}_K[\theta]$[9], $\mathfrak{p} \subset \mathcal{O}_K$ Primideal $\neq (0)$, $\overline{p}(X)$ die Reduktion von $p(X)$ modulo $\mathfrak{p}$, also $\overline{p}(X) \in \mathcal{O}_K/\mathfrak{p}[X]$. Sei $\overline{p}(X) = \overline{p_1}(X)^{e_1} \cdot \ldots \cdot \overline{p_g}^{e_g}$ die Zerlegung in irreduzible Polynome. Seien $p_i(X)$ Liftungen der $\overline{p}_i(X)$ zu unitären Polynomen in $\mathcal{O}_K[X]$ (Koeffizienten bei höchster Potenz von X ist 1). Dann sind

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + p_i(\theta)\mathcal{O}_L$$

die verschiedenen über $\mathfrak{p}$ liegenden Primideale in $\mathcal{O}_L$. Es gilt $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$, $f(\mathfrak{P}_i/\mathfrak{p}) = \deg \overline{p}_i(X)$ und $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$.

Beweis: $\mathcal{O}_K[X] \to \mathcal{O}_K/\mathfrak{p}[X]$: $f \mapsto \overline{f}$ hat als Kern $\mathfrak{p}\mathcal{O}_K[X]$.

$\mathcal{O}_K[X] \to \mathcal{O}_K/\mathfrak{p}[X] \to \mathcal{O}_K/\mathfrak{p}[X]/(\overline{p}(X))$ hat als Kern $\mathfrak{p}\mathcal{O}_K[X] + (p(X))$: Dieses Ideal wird auf 0 abgebildet, geht f auf 0, so ist $\overline{f} = \overline{p} \cdot \overline{q} \Rightarrow f - pg \in \mathfrak{p}\mathcal{O}_K[X]$. Der Homomorphismus ist surjektiv.

Man hat einen Isomorphismus $\mathcal{O}_K[X]/(p(X)) \to \mathcal{O}_K[\theta]$: $f \mapsto f(\theta)$: Der Kern von $\mathcal{O}_K[X] \to \mathcal{O}_K[\theta]$ besteht aus den f mit $f(\theta) = 0$. Also $f = g \cdot p$ mit $g \in K[X]$. $\Rightarrow g \in \mathcal{O}_K[X]$, da p unitär ist (Polynomdivision). $\Rightarrow f \in (p(X))$. Unter diesem Isomorphismus geht $\mathfrak{p}\mathcal{O}_K[X] + (p(X))$ auf $\mathfrak{p}\mathcal{O}_K[\theta]$. Nach Voraussetzung ist $\mathcal{O}_K[\theta] = \mathcal{O}_L$. Also haben wir einen Isomorphismus $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (\mathcal{O}_K/\mathfrak{p}[X])/(\overline{p}(X))$. Also

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \mathcal{O}_K[\theta]/\mathfrak{p}\mathcal{O}_K[\theta] \cong \mathcal{O}_K[X]/(\mathfrak{p}\mathcal{O}_K + (p(X))) \cong (\mathcal{O}_K/\mathfrak{p}[X])/(\overline{p}(X))$$

Chinesischer Restsatz: RHS ist isomorph zu $\bigoplus \mathcal{O}_K/\mathfrak{p}[X]/(\overline{p}_i(X)^{e_i})$, die Elementezahl $(\mathbb{N}\mathfrak{p})^n$ mit $n = [L : K] = \deg p(X)$. Ist $\overline{p}(X) = \prod_{j=1}^{g} \overline{p}_j(X)^{e_j}$, so sieht man rechts alle Primideale. Es sind genau die Hauptideale $(\overline{p}_j(X))$, ihre Bilder links sind die HI $(\overline{p}_j(\theta) =: \overline{\mathfrak{P}}_j)$. Der Körpergrad

$$[(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/\overline{\mathfrak{P}}_j : \mathcal{O}_K/\mathfrak{p}] = \deg \overline{p}_j(X),$$

denn $(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/\overline{\mathfrak{P}}_j = \mathcal{O}_K/\mathfrak{p}[X]/(\overline{p}_j(X))$. Sei $\mathfrak{P}_j$ das Urbild von $\overline{\mathfrak{P}}_j$ unter $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Dann

[9] Wir haben gesehen, dass so ein Element nicht immer existiert. Das ist also eine gewisse Einschränkung.

ist $\mathfrak{P}_j = \mathfrak{p}\mathcal{O}_L + p_j(\theta)\mathcal{O}_L$.

$$\prod_{j=1}^{g} \mathfrak{P}_j^{e_j} = \prod_j (\mathfrak{p}\mathcal{O}_L + p_j(\theta)\mathcal{O}_L)^{e_j}$$
$$\subseteq \mathfrak{p}\mathcal{O}_L + \underbrace{\prod p_j(\theta)^{e_j} \cdot \mathcal{O}_L}_{\equiv p(\theta) \equiv 0 \pmod{\mathfrak{p}\mathcal{O}_L}}$$

$\Rightarrow \prod \mathfrak{P}_j^{e_j} \subset \mathfrak{p}\mathcal{O}_L$.

Also teilt $\mathfrak{p}\mathcal{O}_L$ das Ideal $\prod_{j=1}^{g} \mathfrak{P}_j^{e_j}$. Mithin $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_j^{k_j}$, $k_j \leq e_j$.

$$(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/\overline{\mathfrak{P}}_j = (\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/(\mathfrak{P}_j/\mathfrak{p}\mathcal{O}_L) = \mathcal{O}_L/\mathfrak{P}_j$$

Also $f(\mathfrak{P}_j/\mathfrak{p}) = f_j = \deg \overline{p}_j(x)$. $(\mathcal{O}_L : \mathfrak{p}\mathcal{O}_L) = \mathbb{N}(\mathfrak{p}\mathcal{O}_L) = \prod(\mathbb{N}\mathfrak{P}_j)^{k_j} = (\mathbb{N}\mathfrak{p})^{\sum f_j k_j}$

Andererseits ist $\operatorname{card} k[X]/(\overline{p}(X)) = \prod \operatorname{card} k[X]/(\overline{p}_j(X))^{e_j}$ $(k = \mathcal{O}_K/\mathfrak{p}) = (\mathbb{N}\mathfrak{p})^{\sum e_j f_j}$ $\Rightarrow k_j = e_j$. □

Bemerkung 1.11.2
$K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, $d \neq 0, 1$ sqf.

Man kann zeigen:

$$p \text{ zerlegt} \Leftrightarrow \left(\frac{d_K}{p}\right) = 1$$
$$p \text{ träge} \Leftrightarrow \left(\frac{d_K}{p}\right) = -1$$

Satz 1.11.3 („Satz 9“ QRL - Quadratisches Reziprozitätsgesetz)
p, l ungerade PZ, $p \neq l$, dann gilt:

$$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}}$$

Folgerung 1.11.4
Das Zerlegungsverhalten von p in $\mathcal{O}_K$ hängt nur von p modulo $4|d_K|$ ab. $\Rightarrow$ der ARTIN-Führer ist $4|d_K|$.

Beispiel 1.11.5 (Kreisteilungskörper)
Wir manchen es uns leichter und betrachten nur $K = \mathbb{Q}(\zeta_p)$, $p > 2$ Primzahl, $\zeta_p = e^{2\pi i/p}$. $K/\mathbb{Q}$ ist GALOIS-Erweiterung, $\operatorname{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$ via $a \mapsto \sigma_a$, $\sigma_a\zeta_p = \zeta_p^a$, $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$, $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$. Also nur p verzweigt.

Fakt 1.11.6
Sei $l \neq p$ Primzahl, dann gilt $l\mathcal{O}_K = \mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_g$ mit $f(\mathcal{L}_i/l) = f$, $fg = \varphi(p) = p - 1$. Dabei ist f die Ordnung von l in $\mathbb{F}_p^\times$. Insbesondere ist l voll zerlegt $\Leftrightarrow l \equiv 1 \pmod{p}$ und l träge $\Leftrightarrow l$ ist Primitivwurzel modulo p ($\Leftrightarrow l$ erzeugt $\mathbb{F}_p^\times$). Somit hängt das Zerlegungsverhalten von l in $\mathcal{O}_K$ nur von l (modulo p) ab.

Beweis: Das Zerlegungsverhalten von l in $\mathcal{O}_K$ liest man ab aus dem von $p(X) = \frac{X^p-1}{X-1}$ in $\mathbb{F}_l[X]$ (Satz 8), resp. dem von X^p-1 in $\mathbb{F}_l[X]$. $\overline{p}(X) = X^p-1$ ist separabel über $\mathbb{F}_l$, wg. $\overline{p}'(X) = pX^{p-1}$. Der Zerfällungskörper von $\overline{p}$ über $\mathbb{F}_l$ ist die kleinste Erweiterung $\mathbb{F}_{l^f}$ von $\mathbb{F}_l$, welche die p-ten Einheitswurzeln enthält. Da $\mathbb{F}_{l^f}^\times$ zyklisch ist, geschieht das genau dann, wenn $e^f - 1$ durch p teilbar ist, wenn also f die Ordnund von l in $\mathbb{F}_p^\times$ ist. □

Bemerkung 1.11.7 (i) Wie verhalten sich die Primzahlen auf Restklassen? Ist a prim zu m ($m \geq 2$), wieviele Primzahlen sind $\equiv a \pmod{p}$.

DIRICHLET: In jeder Restklasse liegen unendlich viele Primzahlen. Sogar Summe der Reziproken ist ∞. $\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty$. DIRICHLET: $\sum_{p\equiv a \pmod{m}} \frac{1}{p} = \infty$.

(ii) Sei $f \in \mathbb{Z}[X]$ irreduzibel, betrachte $f_p \equiv f \pmod{p}$, also $f_p \in \mathbb{F}_p[X]$.

Ist $\mathrm{Gal}(f) \subset S_n$ ($n = \deg f$) abelsch, so zeigt die Klassenkörpertheorie: $\exists a \in \mathbb{N} \setminus \{0\}$ (ARTIN-Führer), s.d. die Anzahl der irred. Faktoren von f_p nur von $p \pmod{a}$ abhängt.

Ende VL 17
17.12.2014

§2 Lokale Zahlkörper

§2.1 Die reellen Zahlen

Was ist $\sqrt{2}$?

(i) $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots$

$\mathbb{N}$ = Kardinalität der endlichen Mengen

(ii) $\mathbb{Z}$ $(a-b) = (a,b) \sim (c,d) = (c-d) \Leftrightarrow a+d = b+c$

(iii) $\mathbb{Q}$ QK

(iv) Für $\mathbb{R}$ brauchen wir einen Absolutbetrag

$$|\cdot| : \mathbb{Q} \to \mathbb{Q}_+ = \{\alpha \in \mathbb{Q} : \alpha \geq 0\}$$

$$|\alpha| = \begin{cases} \alpha & \alpha \geq 0 \\ -\alpha & \alpha < 0 \end{cases}$$

mit

(a) $|\alpha| = 0 \Leftrightarrow \alpha = 0$

(b) $|\alpha + \beta| \leq |\alpha| + |\beta|$

(c) $|\alpha\beta| = |\alpha||\beta|$

Der Makel von $\mathbb{Q}$: Der Körper ist in der induzierten Metrik $dist(\alpha, \beta) = |\alpha - \beta|$ nicht vollständig.

Die Folge $x_0 = 2$, $x_{n+1} = x_n - \frac{x_n^2 - 2}{2x_n}$ ist CAUCHY-Folge ohne Grenzwert in $\mathbb{Q}$. Sei C der Ring aller Fundamentalfolgen (d.h. CAUCHY-Folgen) in $\mathbb{Q}$. Das ist kommutativer Ring mit 1, $\mathbb{Q}$ bettet sich in C ein, durch konstante Folgen. Sei $\mathfrak{m}$ das Ideal der Nullfolgen. Dies ist maximales Ideal: $(\alpha_n) \notin \mathfrak{m} \Rightarrow \exists \varepsilon > 0 \forall n_0 \exists n \geq n_0 : |\alpha_n| \geq \varepsilon$.

$\exists n_1 \forall m, n \geq n_1 : |\alpha_m - \alpha_n| < \frac{1}{2}\varepsilon$. Sei

$$\beta_n = \begin{cases} 0 & n < n_2 \\ \frac{1}{\alpha_n} n \geq n_2 & \end{cases}.$$

Dann ist (β_n) Fundamentalfolge:

$$|\beta_m - \beta_n| = \frac{\alpha_m - \alpha_n}{|\alpha_m||\alpha_n|} \leq \left(\frac{2}{\varepsilon}\right)^2 |\alpha_m - \alpha_n|$$

und es gilt $(\alpha_n)(\beta_n) = (\alpha_n \beta_n) \equiv 1 \pmod{m}$. Es folgt: $C/\mathfrak{m}$ ist ein Körper. Die Einbettung $\mathbb{Q} \to C$ überlebt. Wir bezeichnen $C/\mathfrak{m}$ mit $\mathbb{R}$.

Absolutbetrag auf $\mathbb{R}$:

$$|x| := \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Wobei $x > 0 \Leftrightarrow \alpha_n \geq \eta > 0$ $\forall n \geq n_0$, $(\alpha_n) \in x$. Es gelten die 3 Eigenschaften wie oben. Also ist $dist(x, y) = |x - y|$ Metrik auf $\mathbb{R}$

Fakt 2.1.1
$\mathbb{R}$ ist vollständig.

Beweis: Sei (x_n) Fundamentalfolge reeller Zahlen, also $\forall \varepsilon > 0 \exists n_0 \forall m, n \geq n_0 : |x_m - x_n| < \varepsilon$. Wir wählen $(\alpha_{nk}) \in x_n$.

$|x_m - x_n| < \varepsilon$ heißt $|\alpha_{mk} - \alpha_{nk}| < \varepsilon \ \forall k < k_0$. Wähle für jedes $r \in \mathbb{N} \setminus \{0\}$ einen Index $k_r \geq k$, s.d. $|\alpha_{rk_r} - \alpha_{rl}| < \varepsilon_r \ \forall l \geq k_r$ und $\varepsilon_r \downarrow 0$ (z.B. $\varepsilon = \frac{1}{r}$). Dann folgt:

$$\begin{aligned} |\alpha_{mk_m} - \alpha_{nk_n}| &\leq |\alpha_{mk_m} - \alpha_{ml}| + |\alpha_{ml} - \alpha_{nl}| + |\alpha_{nl} - \alpha_{nk_n}| \\ &< \varepsilon_m + \underbrace{|\alpha_{ml} - \alpha_{nl}|}_{<\varepsilon} + \varepsilon_n \end{aligned}$$

für l genügend groß. $\Rightarrow |\alpha_{mk_m} - \alpha_{nk_n}| < \varepsilon_m + \varepsilon + \varepsilon_n \Rightarrow (\alpha_{mk_m})$ ist Fundamentalfolge.

Sie definiert reelle Zahl x. Wir zeigen $x_n \to x$. Das ist äquivalent zu $x_n - x \to 0$, d.h. $|x_n - x| < \varepsilon \ \forall n \geq n_0 \Leftrightarrow |\alpha_{nl} - \alpha_{lk_l}| < \varepsilon \ \forall n \geq n_0, l \geq l_0 = l_0(n)$.

$|\alpha_{nl} - \alpha_{lk_l}| < \underbrace{|\alpha_{nl} - \alpha_{nk_n}|}_{<\varepsilon/2} + \underbrace{|\alpha_{nk_n} - \alpha_{lk_l}|}_{<\varepsilon_n}$ für genügend große n. □

Bemerkung 2.1.2
$\mathbb{Q}$ ist dicht in $\mathbb{R}$ (ÜA). Man betrachte $(\alpha_n) \in x \in \mathbb{R}$, x_n = Konstante Folge α_n. Dann gilt $x_n \to x$.

Was ist $\sqrt{2}$? Antwort: Die Äquivalenzklasse, in welcher die Folge (α_n) liegt mit $\alpha_0 = 2$, $\alpha_{n+1} = \alpha_n - \frac{\alpha_n^2 - 2}{2\alpha_n}$:

$\alpha_{n+1} = \frac{\alpha_n^2 + 2}{2\alpha_n} \Rightarrow \alpha_n > 0$.

$$\alpha_{n+1}^2 - 2 = \left(\frac{\alpha_n^2 + 2}{2\alpha_n} - 2 \right)^2 = \left(\frac{2 - \alpha_n^2}{2\alpha_n} \right)^2 = \left(\frac{\alpha_n^2 - 2}{2\alpha_n} \right)^2$$

$\Rightarrow \alpha_n^2 > 2$, $\alpha_n \downarrow$

$0 < \alpha_{n+1}^2 - 2 < \frac{(\alpha_n^2 - 2)^2}{16} \Rightarrow \alpha_n \to \sqrt{2}$, also ist (α_n) Fundamentalfolge.

§2.2 Bewertungen

Definition 2.2.1
Sei K ein Körper. Eine **Bewertung** von K ist eine Abbildung $|\cdot| : K \to \mathbb{R}_+$ mit

(i) $|x| = 0 \Leftrightarrow x = 0$

(ii) $|x + y| \leq |x| + |y|$

(iii) $|xy| = |x||y|$.

Beispiel 2.2.2 (i) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ mit ihren Absolutbeträgen.

(ii) Jeder Körper trägt die triviale Bewertung

$$|x| = \begin{cases} 0 & x = 0 \\ 1 & x \in K^\times \end{cases}.$$

Diese wird im Folgenden stets ausgeschlossen.

(iii) $p \in \mathbb{P}$, $0 < c < 1$, jedes $\alpha \in \mathbb{Q}^\times$ lässt sich schreiben als $\alpha = p^{\nu_p(\alpha)} \cdot \beta$, β prim zu p.

Sei $|\alpha|_p = c^{\nu_p(\alpha)}$ - ***p*-adische Bewertung**.

Dann $\nu_p(\alpha\beta) = \nu_p(\alpha)+\nu_p(\beta)$ zeigt (iii). $\nu_p(\alpha+\beta) \geq \min(\nu_p(\alpha), \nu_p(\beta))$ zeigt sogar $|\alpha+\beta|_p \leq \max(|\alpha|_p, |\beta|_p)$, also folgt (ii) (**ultrametrische Ungleichung**). $|\alpha|_p \neq 0$ für $\alpha \neq 0$ zeigt (i). Man nimmt gern $c = \frac{1}{p}$, also $|\alpha|_p = p^{-\nu_p(\alpha)}$.

Bemerkung 2.2.3
$dist(x, y) = |x - y|$ definiert eine Metrik auf bewertetem Körper.

Definition 2.2.4
Zwei Bewertungen eines Körpers heißen äquivalent genau dann, wenn eine der folgenen Aussagen gilt:

(i) Sie haben die selben offenen Mengen.

(ii) Sie haben die selben abgeschlossenen Mengen.

(iii) Sie haben die selben konvergenten Folgen

$$|x_n - x|_1 \to 0 \Leftrightarrow |x_n - x|_2 \to 0.$$

Fakt 2.2.5
Diese drei Eigenschaften sind äquivalent.

Beweis: (i) $\Leftrightarrow$ (ii) trivial.

(i) $\Rightarrow$ (iii): $|x_n - x| \to 0 \Rightarrow \{x_n : n \in \mathbb{N}\} \cup \{x\}$ ist abgeschlossen bezüglich $|\cdot|_1 \Rightarrow$ auch abgeschlossen bezüglich $|\cdot|_2 \Rightarrow x_n \to x$ bzgl. $|\cdot|_2$.

(iii) $\Rightarrow$ (i): Sei $E \subset K$ abgeschlossen bzgl $|\cdot|_1$, dann ist jeder Punkt aus E isoliert oder Häufungspunkt bzgl $|\cdot|_1$. $\Rightarrow$ das selbe bzgl. $|\cdot|_2 \Rightarrow E$ bzgl. $|\cdot|_2$ abgeschlossen. □

Fakt 2.2.6
Zwei Bewertungen $|\cdot|_1$, $|\cdot|_2$ eines Körper K sind genau dann äquivalent, wenn ein $c \in \mathbb{R}_+^\times$ mit $|\cdot|_2 = |\cdot|_1^c$ existiert.

Ende VL 18
06.01.2015

Beweis: Die Implikation $\Leftarrow$ ist trivial:

$$|x_n - x|_1 \to 0 \Rightarrow |x_n - x|_1^c \to 0$$

„$\Rightarrow$“ Sei $|x|_1 < 1$, dann ist (x^n) Nullfolge für $|\cdot|_1$, also auch für $|\cdot|_2$: $|x|_2^n \to 0 \Rightarrow |x|_2 < 1$. Mithin $|x|_1 < 1 \Leftrightarrow |x_2| < 1$.

Wir fixieren $y \in K^\times$ mit $|y|_1 > 1$ ($|\cdot|_1$ ist nicht trivial). Für jedes $x \in K^\times$ ist dann $|x|_1 = |y|_1^t$ mit $t = \frac{\log|x|_1}{\log|y|_1} \in \mathbb{R}$. Wir wählen Folge rationaler Zahlen $\alpha_i = \frac{a_i}{b_i}$, $b_i > 0$ mit $\alpha_i \downarrow t$. Dann gilt $|x|_1 = |y|_1^t < |y|_1^{a_i/b_i} \Rightarrow |x^{b_i}/y^{a_i}|_1 < 1 \Rightarrow |x^{b_i}/y^{a_i}|_2 < 1. \Rightarrow |x|_2 < |y|_2^{a_i/b_i}$. Für $i \to \infty$

folgt $|x|_2 \leq |y|_2^t$. Analog gibt $\beta_i \uparrow t$ die Abschätzung: $|x|_2 \geq |y|_2^t$. Somit $|x|_2 = |y|_2^t$. Es folgt $\log|x|_1 = t\log|y|_1$ und $\log|x|_2 = t\log|y|_2$.

$$\rightarrow \frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2} = c \quad \forall x \in K^\times$$

Nach Voraussetzung war $|y|_1 > 1$, also $|1/y|_1 < 1$. $\Rightarrow |1/y|_2 < 1 \Rightarrow |y|_2 > 1 \Rightarrow c > 0$. □

Interludium: Das 2015 - Paket

(i) $K = \mathbb{Q}(\sqrt{-2015})$

$-2015 \equiv 1 \pmod 4$, also $d_K = -2015 = -5 \cdot 13 \cdot 31$

MINKOVSKI-Konstante: $M_K = \frac{2!}{2}\frac{4}{\pi}\sqrt{2015} < 29$ (Taschenrechner)

Primzahlen < 29: verzweigt: $5, 13$. $5\mathcal{O}_K = \mathfrak{p}_5^2$, $13\mathcal{O}_K = \mathfrak{p}_{13}^2$

$-2015 \equiv 1 \pmod 8$ $\Rightarrow 2$ zerlegt: $2\mathcal{O}_K = \mathfrak{p}_2 \cdot \overline{\mathfrak{p}_2}$

$\left(\frac{-2015}{3}\right) = \left(\frac{-5}{3}\right) = \left(\frac{1}{3}\right) = 1$ $\Rightarrow 3$ zerlegt.

$\left(\frac{-2015}{23}\right) = \left(\frac{285}{23}\right) = \left(\frac{55}{23}\right) = \left(\frac{9}{23}\right) = 1$ $\Rightarrow 23$ zerlegt.

usw.

zerlegt	$2, 3, 7, 11, 17, 23$
träge	19
verzweigt	$5, 13$

Also: Cl_K wird erzeugt von $\mathfrak{p}_l$, $l = 2, 3, 5, 7, 11, 13, 17, 23$.

Ganzheitsbasis ist $1, \omega = \frac{1+\sqrt{-2015}}{2}$. $\mathrm{N}(a + b\omega) = \left(a + \frac{b}{2}\right)^2 + 2015 \cdot \frac{b^2}{4} = a^2 + ab + 504b^2$, $a, b \in \mathbb{Z}$.

Sei $b = 1$.

a	$a^2 + a + 504$
0	$504 = 2^3 \cdot 3^2 \cdot 7 \Rightarrow (\omega) = \mathfrak{p}_2^3\mathfrak{p}_3^2\mathfrak{p}_7$
1	$506 = 2 \cdot 11 \cdot 23$
2	$510 = 2 \cdot 3 \cdot 5 \cdot 17$
	$\vdots$
23	$1056 = 2^5 \cdot 3 \cdot 11$

Also fallen Erzeuger weg:

$a = 1$	$\mathfrak{p}_{23}$ weg
$a = 2$	$\mathfrak{p}_{17}$ weg
$a = 6$	$546 = 2 \cdot 3 \cdot 7 \cdot 13$, $\mathfrak{p}_{13}$ weg
$a = 7$	$560 = 2^4 \cdot 5 \cdot 7$, $\mathfrak{p}_7$ weg
$a = 9$	$594 = 2 \cdot 3^3 \cdot 11$, $\mathfrak{p}_{11}$ weg

Also wird Cl_K erzeugt von $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5$. $a = 23$ $\mathfrak{p}_3 \sim \mathfrak{p}_2^5\mathfrak{p}_1 1$ in Cl_K

Lücke:[$\mathrm{N}(17 + \omega) = 810 = 2 \cdot 3^4 \cdot 5$. $(17 + \omega) = \mathfrak{p}_2\mathfrak{p}_3^4\mathfrak{p}_5$ $\Rightarrow \mathrm{Cl}_K$ erzeugt von $\mathfrak{p}_3, \mathfrak{p}_5$, also $\mathrm{Cl}_K = \langle\mathfrak{p}_3\rangle \times \langle\mathfrak{p}_5\rangle$.

$\mathfrak{p}_5$ ist kein HIR: $\mathbb{N}\mathfrak{p}_5 = 5 = a^2 + ab + 504b^2$ $\Rightarrow 20 = (2a+b)^2 + 2016b^2$ ↯. $N(8+\omega) = 576 = 3^2 \cdot 2^6$ $\Rightarrow \mathfrak{p}_3$ hat in Cl_K Ordnung 13 oder 26. Für Ordnung 13 folgt $4 \cdot 13^{13} = (2a+b)^2 + 2016b^2$. Das geht nicht. Somit $\mathrm{Cl}_K \cong C_{26} \times C_2$, $h_K = 52$]

Also Cl_K erzeugt von $\mathfrak{p}_2$, $\mathfrak{p}_5$. $\mathfrak{p}_5^2 \sim 1$, aber $\mathfrak{p}_5$ nicht: $\mathfrak{p}_5 = (a + b\omega)$

$\Rightarrow 5 = \mathbb{N}\mathfrak{p}_5 = a^2 + ab + 504b^2$. $\Rightarrow b = 0$, $5 = a^2$ $\lightning$. Also $\mathfrak{p}_5$ kein Hauptideal.

$a = 17$: $810 = 2 \cdot 3^4 \cdot 5$ $\Rightarrow \mathfrak{p}_2 \cdot \mathfrak{p}_3^4 \cdot \mathfrak{p}_5 \sim 1$.

$a = 8$: $576 = 2^6 \cdot 3^2$

$\Rightarrow \mathfrak{p}_2^6 \cdot \mathfrak{p}_3^{\pm 2} \sim 1$ $\Rightarrow \mathfrak{p}_2^{24}\mathfrak{p}_3^{\pm 8} \sim 1$.

Für $+8$: $\mathfrak{p}_2^{24} \sim \mathfrak{p}_3^{-8}$, $\mathfrak{p}_3^{-8} \sim \mathfrak{p}_2^2 \sim \mathfrak{p}_5^2 \sim \mathfrak{p}_2^2$. Damit $\mathfrak{p}_2^{24} \sim \mathfrak{p}_2^2$ $\Rightarrow \mathfrak{p}_2^{22} \sim 1$.

Für -8: $\mathfrak{p}_2^{24} \sim \mathfrak{p}_2^{-2}$ $\Rightarrow \mathfrak{p}_2^{26} \sim 1$.

Annahme $\mathfrak{p}_2^{22} \sim 1$ $\Rightarrow 2^{22} = a^2 + ab + 504b^2$ $\Rightarrow 2^{24} = (2a + b)^2 + 2015b^2$.

$2^{24}/2015 \approx 8326,17$. Wurzel < 91. Ergebnis negativ: Mithin $\mathfrak{p}_2^{26} \sim 1$.

$\mathfrak{p}_2^2$ ist kein Hauptideal: $4 = a^2+ab+504b^2$, $16 = (2a+b)^2+2015b^2$. $\mathfrak{p}_2^2 = (2) = \mathfrak{p}_2\overline{\mathfrak{p}_2} \Rightarrow \mathfrak{p}_2 = \overline{\mathfrak{p}_2}$ $\lightning$

$\mathfrak{p}_2^{13} \sim 1$ $\Leftrightarrow \mathfrak{p}_2^{13} = (a + b\omega)$ $\Rightarrow$ $2^{15} = (2a + b)^2 + 2015b^2$. $2^{15}/2015 < 16,27$ $\Rightarrow b < 5$ - keine Lösungen.

Somit hat $\mathfrak{p}_2$ ind Cl_K die Ordnung 26. Angenommen $\mathfrak{p}_5 \sim \mathfrak{p}_2^a$ $\Rightarrow a = 13$. $5 \cdot 2^{15} = (2a + b)^2 + 2015b^2$, $b < 9$ - keine Lösungen.

Ergebnis: $\mathrm{Cl}_K = \langle \mathfrak{p}_2 \rangle \times \langle \mathfrak{p}_5 \rangle = C_{26} \times C_2$.

ÜA: $2^{28} = (2a + b)^2 + 2014b^2$ hat $\mathbb{Z}$-Lösungen. Welche?

(ii) Fundamentaleinheit von $\mathbb{Q}(\sqrt{2015})$

$K = \mathbb{Q}(\sqrt{2015})$, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, $\omega = \sqrt{2015}$, $d_K = 4 \cdot 2015$.

Kettenbruch von *omega*: $44 < \omega < 45$: $44^2 = 1936$, $45^2 = 2025$.

Also $\omega = 44 + (\omega - 44)$.

$\frac{1}{\omega-44} = \frac{\omega+44}{79} = 1 + \frac{\omega-35}{79}$

$\frac{79}{\omega-35} = \frac{79(\omega+35)}{790} = 7 + \frac{\omega-35}{10}$

$\frac{10}{\omega-35} = \frac{10(\omega+35)}{790} = 1 + \frac{\omega-44}{79}$

$\frac{79}{\omega-44} = \frac{79(\omega+44)}{79} = \omega + 44 = 88 + (\omega - 44)$

Ergebnis: $\sqrt{2015} = [44, \overline{1, 7, 1, 88}]$

n	0	1	2	3	4
a_n		44	1	7	1
p_n	1	44	45	359	404
q_n	0	1	1	8	9
$p_n^2 - 2015q_n^2$		-79	10	-79	1

$\Rightarrow \varepsilon_K = 404 + 9 \cdot \sqrt{2015}$, $\mathrm{N}\,\varepsilon_K = +1$.

(iii) Die Idealklassengruppe von $\mathbb{Q}(\sqrt{2015})$

$d_K = 4 \cdot 2015 = 2^2 \cdot 5 \cdot 13 \cdot 31$. $M_K = \frac{2!}{2^2} \cdot 2\sqrt{2}015 < 45$

Also verzweigt: $2, 5, 13, 31$.

$\left(\frac{2015 \cdot 4}{3}\right) = \left(\frac{2}{3}\right) = -1$ $\Rightarrow 3$ träge.

zerlegt	$17, 19$
träge	$3, 7, 11, 23, 29, 37, 41, 43$

Cl_K wird erzeugt von $\mathfrak{p}_l$, $l = 2, 5, 13, 17, 19, 31$.

$\mathrm{N}(a + b\omega) = a^2 - 2015b^2$. Sei $b = 1$:

a	$a^2 - 2015$
45	$10 = 2 \cdot 5$
48	$289 = 17^2$
39	$-494 = -2 \cdot 13 \cdot 19$
37	$-646 = -2 \cdot 17 \cdot 19$
31	$-1054 = -2 \cdot 17 \cdot 31$

$a = 48$ $\quad \mathfrak{p}_{17}^2 \sim 1$
$a = 45$ $\quad \mathfrak{p}_2 \sim \mathfrak{p}_5 \Rightarrow \mathfrak{p}_5$ weg
$a = 39$ $\quad \mathfrak{p}_{19}$ weg
$a = 37$ $\quad \mathfrak{p}_{17}$ weg
$a = 31$ $\quad \mathfrak{p}_{31}$ weg

$\Rightarrow \mathrm{Cl}_K$ wird erzeugt von $\mathfrak{p}_2$, $\mathfrak{p}_{13}$, beide der Ordnung ≤ 2.

Mit Geschlechtertheorie folgt sofort: Cl_K hat Ordnung 4.

Von Hand:

Man darf annehmen: $1 < a + b\omega < \varepsilon_K$ (a, b positiv).

$(a + b\omega)(a - b\omega) = \pm 2$. $-\frac{2}{a+b\omega} < a - b\omega < \frac{2}{a+b\omega} < 1$.

$\Rightarrow -1 < b\omega - a < 1 \Rightarrow 0 < 2b\omega < 1 + \varepsilon_K \Rightarrow 0 < b < \frac{1+\varepsilon_K}{\omega} = \frac{405+\omega}{\omega} = \frac{405}{\omega} + 1 < 19 \Rightarrow$ keine $\mathbb{Z}$-Lösungen.

Analog $\mathfrak{p}_3 \not\sim 1$. Fazit: $\mathrm{Cl}_K = \langle \mathfrak{p}_2 \rangle \times \langle \mathfrak{p}_{13} \rangle \cong C_2 \times C_2$.

Ende VL 19
07.01.2015

Fakt 2.2.7 (Schwacher Approximationssatz)
Seien $|\cdot|_1, \ldots, |\cdot|_n$ paarweise inäquivalente Bewertungen eines Körpers K und $a_1, \ldots, a_n \in K$. Dann existiert für alle $\varepsilon > 0$ ein $a \in K$, s.d. $|a - a_i|_i < \varepsilon$. D.h. die Diagonale $K \to K \times \ldots \times K$: $a \mapsto (a, \ldots, a)$ ist dicht.

Beweis: Es existiert $x \in K$ mit $|x|_1 < 1$, $|x|_n \geq 1$ und ein x' mit $|x'|_1 \geq 1$, $|x'|_n < 1$. Also gilt für $y = x'/x$: $|y|_1 > 1$, $|y|_n < 1$. Induktion über n: Es existiert $z \in K : |z|_1 > 1, |z|_2 < 1, \ldots, |z|_n < 1$. IA: $n = 2$ siehe oben. Sei also $|z|_1 > 1, |z|_2 < 1, \ldots, |z|_{n-1} < 1$. Ist $|z|_n \leq 1$, so ist $z^m y$ gut für $m >> 1$: $|z^m y| = |z|^m |y| > 1$, $|z|_j^m |y|_j < 1$ für $m >> 1$ und $2 \leq j \leq n-1$, $|z|_n^m |y|_n < 1$ wegen $|y|_n < 1$.

Der heikle Fall ist $|z|_n > 1$: Wir betrachten $t_m = \frac{z^m}{1+z^m}$, dann gilt $t_m \to 1$ in $|\cdot|_1$: $|t_m - 1|_1 = \frac{1}{|1+z^m|_1} \leq \frac{1}{|z|_1^m - 1} \to 0$.

Analog für $|\cdot|_n$: $|t_m - 1|_n \leq \frac{1}{|z|_n^m - 1} \to 0 \Rightarrow t_m \to 1$ in $|\cdot|_n$.

Für $2 \leq j \leq n-1$ gilt: $|t_m|_j = \frac{|z|_j^m}{|1+z^m|_j} \leq \frac{|z|_j^m}{1-|z|_j^m} \to 0$. Also ist (t_m) eine Nullfolge für diese $|\cdot|_j$. Aus $t_m \to 1$ in $|\cdot|_n$ folgt $|t_m|_n \to 1$: $||t_m|_n - 1| \leq |t_m - 1|_n \to 0$. Also leistet $t_m y$ das Gewünschte.

Sei nun $z \in K$, s.d. $|z|_1 > 1$, $|z|_j < 1$ für $j = 2, \ldots, n$. Dann gilt

$$\frac{z^m}{1+z^m} \to \begin{cases} 1 & \text{für } |\cdot|_1 \\ 0 & \text{für } |\cdot|_2, \ldots, |\cdot|_n \end{cases}.$$

Es folgt $\forall \eta > 0 \exists w \in K^\times$ mit $|w-1|_1 < \eta$, $|w|_j < \eta$ für alle $j = 2, \ldots, n$. Oder: $\forall j \forall \eta > 0 \exists w_j \in K^\times$ mit $|w_j - 1| < \eta$, $|w_j|_i < \eta$ für alle $i \neq j$.

Setze $a = \sum_{j=1}^n a_j w_j$. $a - a_j = \sum a_i w_i + a_j(w_j - 1)$. $\Rightarrow |a - a_j|_j \leq \sum_{i \neq j} |a_i|_j |w_i|_j + |a_j|_j |w_j - 1|_j \leq c \cdot \eta$. $\eta = \sum_{i \neq j} |a_i|_j$ □

Bemerkung 2.2.8 (i) Das ist eine Verallgemeinerung des chinesischen Restsatzes (Details später).

(ii) Starker Approximationssatz im Fall $\mathbb{Q}$: Ist ν_0 eine fixierte Bewertung von $\mathbb{Q}$, so kann man a so wählern, dass $|a|_\nu \leq 1$ für alle $\nu \neq \nu_0$.

Definition 2.2.9
Eine Bewertung heißt **nichtarchimedisch**, wenn $|n| \leq 1$ für alle $n \in \mathbb{N}$, sonst **archimedisch**.

Beispiel 2.2.10
Der übliche Absolutbetrag auf $\mathbb{Q}$ ist archimedisch, die p-adische Bewertungen sind nichtarchimedisch: $|a + b|_p \leq \max(|a|_p, |b|_p)$.

Fakt 2.2.11
$|\cdot|$ ist nichtarchimedisch $\Leftrightarrow |x + y| \leq \max(|x|, |y|)$ für alle $x, y \in K$.

Beweis: Aus der ultrametrischen Ungleichung folgt $|n| \leq \max(|1|, \ldots, |1|)$, $|1| = 1$, also $|n| \leq 1$ für alle $n \in \mathbb{N}$. Sei nun $n \leq 1$ für alle $n \in \mathbb{N}$. Seien $x, y \in K$, $|x| \leq |y|$.

$$|x+y|^n \leq \sum_{r \neq 0}^{n} |\binom{n}{r}| |x|^r |y^{n-r}| \leq \sum |x|^r |y^{n-r}| \leq (n+1)|y|^r$$

$\Rightarrow |x + y| \leq (n+1)^{1/n} |y|$ für alle $n \in \mathbb{N}$ $\Rightarrow |x + y| \leq |y|$. Also $|x + y| \leq \max(|x|, |y|)$. □

Satz 2.2.12 (OSTROWSKI)
Jede (nichttriviale) Bewertung von $\mathbb{Q}$ ist äquivalent zu $|\cdot|_\infty$ (Absolutbetrag) oder zu einer der p-adischen Bewertungen, $p \in \mathbb{P}$: $|\cdot|_p$.

Beweis: Sei $|\cdot|$ nichtarchimedische Bewertung von $\mathbb{Q}$. Dann ist also $|n| \leq 1$ für alle $n \leq IN$. Wäre $|n| = 1$ für alle $n \in \mathbb{N} \setminus \{0\}$, so würde dies auch für alle rationalen Zahlen außer 0 folgen. Also $|\cdot|$= triviale Bewertung. Also existiert eine Primzahl $p \in \mathbb{P}$ mit $|p| < 1$. Sei $I = \{a \in \mathbb{Z} : |a| < 1\}$ - das ist ein Ideal in $\mathbb{Z}$ und $p\mathbb{Z} \subset I \subsetneq \mathbb{Z}$, also $I = p\mathbb{Z}$. Für $m \in \mathbb{Z}$ gilt: $m = p^{\mathrm{ord}_p(m)} \cdot m_0$, $\mathrm{ggT}(p, m_0) = 1$. Also $|m| = |p|^r |m_0| = |p|^r$, $r = \mathrm{ord}_p(m)$. Das verallgemeinert sich sofort auf rationale Zahlern $\neq 0$. Also $|\alpha| = c^{\mathrm{ord}_p(\alpha)}$, $0 < c = |p| < 1$. D.h. $|\cdot| = |\cdot|_p$.

Sei $|\cdot|$ archimedisch, $m, n \in \mathbb{N}$ beide > 1, $m = a_0 + a_1 n + \ldots + a_r n^r$, $0 \leq a_j < n$, $a_r \neq 0$. Dann ist $n^r \leq m$, $|a_j| \leq n$, also $|m| \leq \sum_{j=0}^r |a_j| |n|^j \leq n(r+1) \max(1, |n|)^r$.

Nun ist $r \log n \leq \log m$, also $r \leq \frac{\log m}{\log n}$, und damit $|m| \leq n(1 + \frac{\log m}{\log n}) \max(1, |n|)^{\log m / \log n}$.

Ersetze m durch m^k, das gibt: $|m| \leq n^{1/k}(1 + k\frac{\log m}{\log n})^{1/k} \max(1, |n|)^{\log m / \log n}$. Für $k \to \infty$ folgt $|m| \leq \max(1, |n|)^{\log m / \log n}$. Die Bewertung ist archimedisch, also ex. $m \in \mathbb{N}$ mit $|m| > 1$.

$|0| = 0$, $|1| = 1 \Rightarrow m \geq 2$. Somit $1 < \max(1, |n|)^{\log m/\log n} \Rightarrow |n \geq 1|$ für alle $n \geq 2$. Es folgt $|m| \leq |n|^{\log m/\log n}$ oder $|m|^{1/\log m} \leq |n|^{1/\log n}$ für alle $m, n \geq 2$. Somit $|m|^{1/\log m} = |n|^{1/\log n}$ für alle $m, n \geq 2$. $|m|^{1/\log m} =: c = e^s$, $c > 1 \Rightarrow s > 0$. Also $|m| = e^{s \log m} = |m|_\infty^s$. Das gilt auch für $m = 0, 1$ und folgt dann für $\mathbb{Z}$ und $\mathbb{Q}^\times$. □

Fakt 2.2.13
Sei K eine Körper mit Bewertung $|\cdot|$, dann existiert ein Körper $\hat{K}$, eine Einbettung $K \to \hat{K}$, eine Fortsetzung $|\cdot|\hat{}$ von $|\cdot|$ auf $\hat{K}$ mit

(i) K ist dicht in $\hat{K}$.

(ii) $\hat{K}$ ist vollständig.

Darüber hinaus ist $\hat{K}$ bis auf Isometrie eindeutig bestimmt: Ist $\hat{L}$, $\|\cdot\|\hat{}$ weiterer solcher Körper, so existiert K-Isomorphismus $\sigma : \hat{K} \to \hat{L}$ mit $\|\sigma x\|\hat{} = |x|\hat{}$ für alle $x \in \hat{K}$.

Ende VL 20
13.01.2015

Beweis: C sei der Ring der CAUCHY-Folgen aus K. $\mathfrak{m}$ das Ideal der Nullfolgen, $\hat{K} := C/\mathfrak{m}$. Das ist ein Körper, da $\mathfrak{m}$ maximales Ideal ist: $(x_n) \notin \mathfrak{m} \Rightarrow |x_n| \geq \eta > 0$ für alle $n \geq n_0$.

$$y_n := \begin{cases} 1/x_n & n \geq n \\ 1 & n < n_0 \end{cases},$$

Dann ist $(x_n y_n) \equiv 1 \pmod{\mathfrak{m}}$. K bettet sich in $\hat{K}$ durch die konstanten Folgen ein. Wir setzen $|\cdot|$ fort auf $\hat{K}$ durch $|(x_n)| := \lim_{n\to\infty} |x_n|$. $(|x_n|)$ ist reelle Fundamentalfolge, wegen $||x_m| - |x_n|| \leq |x_m - x_n|$ also konvergent. Ist (y_n) Nullfolge, so ist $\lim_{n\to\infty} |x_n + y_n| = \lim_{n\to\infty} |x_n|$. Also wohldefinierte Abbildung:

$$|\cdot|\hat{}: \hat{K} \to \mathbb{R}_+^\times = [0, \infty).$$

Die 3 Eigenschaften von Bewertungen sind schnell überprüft. $|(x_n) + \mathfrak{m}| = 0 \Rightarrow \lim |x_n| = 0 \Rightarrow x_n \to 0 \Rightarrow (x_n) \in \mathfrak{m} \Rightarrow (x_n) + \mathfrak{m} = \mathfrak{m}$.

(i) K ist dicht in $\hat{K}$.

Sei $x \in \hat{K}, (x_n)$ Repräsentant in C. Sei y_n die Konstante Folge (x_n). Dann ist

$$|x - y_n|\hat{} = \lim_{k\to\infty} |x_k - x_n| \leq \varepsilon$$

für alle $n \geq n_0$. Also $y_n \to x$ in $\hat{K}$.

(ii) $\hat{K}$ ist vollständig.

Sei (x_n) FUndamentalfolge in $\hat{K}$. Nach (i) existiert $y_n \in K$, s.d. $|x_n - y_n|\hat{} \leq \frac{1}{n}$ (Wir identifizieren y_n mit der konstanten Folge y_n). Es gilt

$$|y_m - y_n|\hat{} \leq |y_m - x_m|\hat{} + |x_m - x_n|\hat{} + |x_n - y_n|\hat{} \leq \frac{1}{m} + |x_m - x_n|\hat{} + \frac{1}{n}.$$

$\Rightarrow (y_n)$ ist Fundamentalfolge aus K. Sie definiert also ein $x \in \hat{K}$, Nach (i) gilt $\lim_{n\to\infty} y_n = x$. Also

$$|x_n - x|\hat{} \leq |x_n - y_n|\hat{} + |y_n - x|\hat{} \to 0.$$

Somit gilt $\lim_{n\to\infty} x_n = x$

(iii) Die Eindeutigkeit

Wir haben $\hat{L} \overset{j}{\leftarrow} K \overset{i}{\rightarrow} \hat{K}$ mit Einbettungen i, j. Sei $x \in \hat{K}$ und $x = \lim_{n\to\infty} i(y_n)$, $y_n \in K$. (y_n) ist CAUCHY-Folge in K, also ist $j(y_n)$ eine solche in $\hat{L}$. Sei $\sigma(x) = \lim_{n\to\infty} j(y_n)$. Ist (z_n) eine weitere Folge aus K mit $x = \lim i(z_n)$, so ist $(y_n - z_n)$ Nullfolge, also auch $(j(y_n) - j(z_n))$ Nullfolge in $\hat{L}$. Somit ist $\sigma : \hat{K} \to \hat{L}$ wohldefiniert. Wegen $|x|\hat{} = \lim |y_n|$ und $\|\sigma\|\hat{} = \lim |y_n|$ ist $\|\sigma x\|\hat{} = |x|\hat{}$, also ist σ eine Isometrie. Das Bild $\sigma(\hat{K}) \subset \hat{L}$ enthält die dichte Teilmenge $j(K)$. Sei $x \in \hat{L}$, $x_n \in \sigma(\hat{K})$, $x_n \to x \Rightarrow (x_n)$ Fundamentalfolge $\Rightarrow x \in \sigma(\hat{K})$, wegen der Vollständigkeit von $\sigma(\hat{K})$. Also ist $\sigma(\hat{K})$ abgeschlossen in $\hat{L}$.

□

§2.3 Die p-adischen Zahlen

Definition 2.3.1
Sei $p \in \mathbb{P}$, dann heißt die Vervollständigung $\mathbb{Q}_p$ von $\mathbb{Q}$ bezüglich der p-adischen Bewertung der **Körper der p-adischen Zahlen**. Die Teilmenge

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

heißt **Ring der ganzen p-adischen Zahlen**.

Fakt 2.3.2 (i) $\mathbb{Z}_p$ ist ein dBR.

(ii) Jedes $x \in \mathbb{Z}_p$ besitzt eine eindeutige Darstellung $x = \sum_{j=0}^{\infty} a_j p^j$, $0 \leq a_j < p$, $a_j \in \mathbb{N}$.

(iii) Jedes $x \in \mathbb{Q}_p$ besitzt eine eindeutige Darstellung $x = \sum_{j>>-\infty} a_j p^p$, $0 \leq a_j < p$, $a_j \in \mathbb{N}$.

Beweis:

(i) Es gilt $|x + y|_p \leq \max(|x|_p, |y|_p)$, also ist $\mathbb{Z}_p$ ein Ring. Offensichtlich ist $\mathbb{Z}_p^\times = \{u \in \mathbb{Z}_p : |u|_p = 1\}$ und nach (ii) ist $\mathbb{Z}_p/p\mathbb{Z} = \mathbb{F}_p$. Also ist $(p) = p\mathbb{Z}_p$ maximales Ideal. Jedes andere Ideal $\neq \mathbb{Z}_p$ ist in diesem enthalten: Es enthält keine Einheiten. Somit ist $\mathbb{Z}_p$ ein lokaler Ring. Wir zeigen, dass jedes Ideal $\neq (0), \mathbb{Z}_p$ die Form $(p^n) = p^n\mathbb{Z}_p$ hat.

Sei $I \subset \mathbb{Z}_p$ solch ein Ideal und $x \in I$ habe maximale Bewertung ($|p|_p = \frac{1}{p}$). $x = p^m \cdot u$, $u \in \mathbb{Z}_p^\times$, wieder nach (ii), also $p^m \in I$. Jedes $y \in I$ erfüllt $|y|_p \leq |x|_p$, also $y = ax$ mit $a \in \mathbb{Z}_p \Rightarrow I = (p^m)$. Wir haben gezeigt: $\mathbb{Z}_p$ ist dBR.

(ii) Aus $\sum a_j p^j = \sum b_j p^j$ und $a_0 = b_0, \ldots, a_{r-1} = b_{r-1}$, $a_r \neq b_r$ folgt $a_r +$ (Norm<1) = $b_r +$(Norm<1) $\Rightarrow |a_r - b_r| < 1$ ↯

Alle solche Reihen konvergieren: $|\sum_M^N a_j p^j| \leq p^{-M}$.

Lemma 2.3.3
Sei $x \in \mathbb{Q}$ mit $|x|_p \leq 1$ (d.h. der Nenner ist prim zu p). Dann gilt: $\forall n \in \mathbb{N} \exists! m \in \{0, 1, \ldots, p^n - 1\} : |x - m|_p \leq \frac{1}{p^n}$.

Beweis: Sei $x = \frac{a}{b}$, ggT$(a, b) = 1$, $b > 0$, $p \nmid b$.

Also ggT$(b, p^n) = 1 \Rightarrow r, s \in \mathbb{Z}$: $rb + sp^n = 1$. Sei $m' := ar$, es folgt $|x - m'|_p = |\frac{a}{b} - ar|_p = |a|_p|\frac{1}{b} - r|_p = |a|_p|1 - br|_p$ ($|b|_p = 1$) $= |a|_p|sp^n|_p \leq \frac{1}{p^n}$. Das selbe gilt für alle $m' + p^n t$, $t \in \mathbb{Z}$, wg. der ultrametrischen Ungleichung.

Eindeutigkeit: $|x-m_1|_p < \frac{1}{p^n}$, $|x-m_2|_p < \frac{1}{p^n} \Rightarrow |m_1-m_2|_p < \frac{1}{p^n} \Rightarrow m_2-m_1$ ist durch p^n teilbar. $0 \le m_1, m_2 < p^n \Rightarrow m_1 = m_2$. Das war das Lemma. □ Sei $x \in \mathbb{Z}_p$, (α_n)

Fundamentalfolge aus x. $\forall k \ge 1 \exists N(k) \forall m,n \ge N(k) : |\alpha_m - \alpha_n|_p < \frac{1}{p^k}$.

Man darf voraussetzen, dass die Folge der $N(k)$ streng monoton wächst. Es gilt $|\alpha_n|_p \le \max\{|\alpha_n-\alpha_m|_p, |\alpha_m|_p\} \le \max\{\frac{1}{p}, |\alpha_m|_p\}$ für alle $m,n \ge N(1)$. Nun ist $\lim_{n\to\infty} |\alpha_m|_p = |x|_p \le 1$, also gilt $|\alpha_n|_p \le 1 \ \forall n \ge N(1)$. Wir wählen für jedes $\alpha_{N(k)}$ das $\beta_k \in \{0,1,\dots,p^k-1\}$ aus dem Lemma. Also $|\alpha_{N(k)-\beta_K}|_p \le \frac{1}{p^k}$. Dann ist $(\beta_k) \in x$, d.h. $\lim \beta_k = x$ und $|\beta_{k+1}-\beta_k| \le \max(|\alpha_{N(k+1)}-\alpha_{N(k)}|_p, |\alpha_{N(k+1)}-\beta_{k+1}|_p, |\alpha_{N(k)}-\beta_k|_p) \le \frac{1}{p^k}$. D.h. $\beta_{k+1}-\beta_k$ ist durch p^k teilbar. Wegen $0 \le \beta_k < p^k$, $0 \le \beta_{k+1} < p^{k+1}$ folgt $-p^k < \beta_{k+1}-\beta_k < p^{k+1}$, also $\beta_{k+1} \ge \beta_k$ und $\beta_{k+1} = \beta_k + a_k p^k$, $0 \le a_k < p$. Somit $\beta_k = \sum_{j=0}^{k} a_j p^j$, $k \to \infty$ gibt $x = \sum_{j=0}^{\infty} a_j p^j$.

(iii) folgt sofort: $x \in \mathbb{Q}_p^\times \Rightarrow p^N x \in \mathbb{Z}_p$ für geeignete $N \in \mathbb{N}$.

□

Folgerung 2.3.4 (i) $x \in \mathbb{Q}_p^\times \Rightarrow x = \frac{a_{-N}}{p^N} + \dots + \frac{a_{-1}}{p} + a_0 + a_1 p + \dots$, $a_{-N} \ne 0$ $(0 \le a_j < p)$ $\Rightarrow |x|_p = p^N$.

(ii) $\mathbb{Z}_p$ ist integer: ist klar, denn es liegt in einem Körper - alternativ: $xy = 0 \Rightarrow |xy|_p = 0$ $\Rightarrow |x|_p |y|_p = 0 \Rightarrow |x|_p = 0$ oder $|y|_p = 0 \Rightarrow x = 0$ oder $y = 0$.

(iii) $\operatorname{card} \mathbb{Z}_p = \operatorname{card} \mathbb{R}$

Beispiel 2.3.5
$p = 13$: $-\frac{1}{12} = \frac{1}{1-13} = \sum_{n=0}^{\infty} (13)^n$

Ende VL 21
14.01.2015

Fakt 2.3.6
$\mathbb{Z}_p$ ist kompakt, $\mathbb{Q}_p$ ist lokalkompakt, aber nicht kompakt.

Beweis:

$$\mathbb{Q}_p = \bigcup_{n=1}^{\infty} p^{-n} \mathbb{Z}_p$$

und $\mathbb{Z}_p$ ist offen in $\mathbb{Q}_p$. $\mathbb{Q}_p \setminus \mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \ge p\}$ abgeschlossen. Es gibt eine endliche Teilüberdeckung. Sei (x_n) Folge aus $\mathbb{Z}_p$, $\exists a_0 \in \{0,1,\dots,p-1\}$ s.d. unendlich viele der x_n mit a_0 beginnen. Unter denen gibt es unendlich viele, die mit $a_0 + a_1 p$ beginnen usw. $\Rightarrow$ es ex. eine Teilfolge $(x_{\mu(n)})$, s.d.

$$|x_{\mu(n)} - (a_0 + a_1 p + \dots + a_n p^n|_n < \frac{1}{p^n}.$$

Sei $x = \sum_{j=0}^{\infty} a_j p^j$, dann gilt $|x_{\mu(n)} - x|_p \le \frac{1}{p^n} \Rightarrow$ konvergente Teilfolge gefunden. □

Bemerkung 2.3.7 (i) $\mathbb{Z}_p$ ist offen und abgeschlossen in $\mathbb{Q}_p$ (clopen):

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \le 1\} = \{x \in \mathbb{Q}_p : |x|_p < p\}$$

Jeder topologische Raum ist disjunkte Vereinigung seiner Zusammenhangskomponenten. $\mathbb{R}$ ist zerlegt, $\mathbb{Q}$ ist total unzusammenhängend, d.h. jeder Punkt ist seine Zusammenhangskomponente: Sei $\alpha \in E \subset \mathbb{Q}$ zusammenhängend. Ist $\beta \in E \setminus \{\alpha\}$, so existiert $\gamma \in \mathbb{R} \setminus \mathbb{Q}$

zwischen α und β, es gilt

$$E = \underbrace{(E \cap \{x \in \mathbb{Q} : x < \gamma\})}_{\text{offen}} \sqcup \underbrace{(E \cap \{x \in \mathbb{Q} : x > \gamma\})}_{\text{offen}}.$$

$\Rightarrow E = \{\alpha\}$.

$\mathbb{Z}_p$ ist auch total unzusammenhängend: $\alpha \in \mathbb{Z}_p$ habe zusammenhängende Obermenge $E \subset \mathbb{Z}_p$. Enthält diese $\beta \neq \alpha$, so gilt

$$\alpha = \sum a_j p^j, \beta = \sum b_j p^j, \qquad a_0 = b_0, \ldots, a_{r-1} = b_{r-1}, a_r \neq b_r.$$

Nun ist

$$\mathbb{Z}_p = \bigsqcup_{0 \leq a < p^r} (a + p^r \mathbb{Z}_p)$$

disjunkte Zerlegung in clopen sets, α, β liegen in verschiedenen. Also $E = \{\alpha\}$.

(ii) $\mathbb{Q}_p$ ist wie $\mathbb{R}$ vollständig und lokalkompakt. Das sind Voraussetzungen für Analysis und co. Es gibt in allem Analogien für p-adische Körper: p-adische Mannigfaltigkeiten, p-adische DGLn, p-adische LIE-Algebren, p-adische LIE-Gruppen, p-adische Funktionalanalysis, p-adische transzendente Funktionen. p-adische Funktionentheorie ist schwieriger, als über $\mathbb{C}$: $[\mathbb{C} : \mathbb{R}] = 2$, aber $[\overline{\mathbb{Q}_p} : \mathbb{Q}_p] = \infty$. Überdies ist $\overline{\mathbb{Q}_p}$ nicht vollständig. $\widetilde{\overline{\mathbb{Q}_p}} := \mathbb{C}_p$ ist algebraisch abgeschlossen und vollständig (sog. TATE-Körper).

Über $\mathbb{Q}_p$ werden Träume wahr: $\sum a_n$ konvergiert $\Leftrightarrow a_n \to 0$.

Beispiel 2.3.8
Was ist $\sqrt{2}$?

In $\mathbb{Q}_2$ gibt es keine Zahl mit Quadrat 2: $x^2 = 2 \Rightarrow |x|_2^2 = \frac{1}{2} \Rightarrow |x|_2 = \frac{1}{\sqrt{2}}$ ↯.

Sei $p > 2$, wenn $x^2 = 2$ ist - mit $x \in \mathbb{Q}_p$, so folgt $y^2 \equiv 2 \pmod p$ hat Lösung. D.h. 2 ist Quadrat in $\mathbb{F}_p \Leftrightarrow \left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$. Also gibt es für $p \equiv \pm 5 \pmod 8$ keine Zahl mit Quadrat 2 in $\mathbb{Q}_p$.

Sei $p \equiv \pm 1 \pmod 8$, $\alpha_0 \in \mathbb{Z}_p$ so, dass $\alpha_0^2 \equiv 2 \pmod p$ gilt. Setze $\alpha_{n+1} := \alpha_n - \frac{\alpha_n^2 - 2}{2}$. Das ist korrekt definierte Folge: $|\alpha_0|_p = 1$, $|\alpha_0^2 - 2|_p < 1$, $|\alpha_0^2 + 2|_p = |\alpha_0^2 - 2 + 4|_p = 1$. Induktion: $|\alpha_{n+1}|_p = \left|\frac{\alpha_n^2 + 2}{2\alpha_n}\right|_p$

$$\alpha_{n+1}^2 - 2 = \frac{(\alpha_n^2 + 2)^2}{4\alpha_n^2} - 2 = \frac{(\alpha_n^2 - 2)^2}{4} \Rightarrow |\alpha_{n+1}^2 - 2|_p < 1$$

$\Rightarrow |\alpha_{n+1}^2 + 2|_p = |\alpha_{n+1}^2 - 2 + 4|_p = 1$.

Es folgt $|\alpha_{n+1} - \alpha_n| = |\alpha_n^2 - 2|$ und $|\alpha_{n+1}^2 - 2|_p = |\alpha_n^2 - 2|_p^2 \Rightarrow |\alpha_n^2 - 2| \to 0$.

Damit ist (α_n) CAUCHY-Folge, also konvergent gegen α say. Aus der Rekursionsformel folgt $\alpha = \alpha - \frac{\alpha^2 - 2}{2} \Rightarrow \alpha^2 = 2$.

Konkret für $p = 7$:

$$\alpha = a_0 + a_1 \cdot 7 + a_2 \cdot 49 + a_3 \cdot 243 + \ldots \qquad a_j \in \{0, 1, \ldots, 6\}$$

$a_0^2 \equiv 2 \pmod 7 \Rightarrow a_0 = 3$ oder $a_0 = 4$. Wir wählen $a_0 = 3$. $\alpha_1 = 3 - \frac{9-2}{6} = \frac{11}{6}$. Dann $\alpha_1^2 - 2 = \frac{121-72}{36} = \frac{49}{36}$.

$$\alpha_2 = \frac{11}{6} - \frac{49/36}{11/3} = \frac{11}{6} - \frac{49}{132} = \frac{242}{132} - \frac{49}{132} = \frac{195}{132}.$$

Damit $\alpha^2 - 2 = \frac{2401}{(132)^2} = \frac{7^4}{2^4 \cdot 3^2 \cdot 11}$

Beispiel 2.3.9
$y' = y$, Ansatz: $y = \sum_{j=0}^{\infty} a_j x^j$, damit $y' = \sum_{j=1}^{\infty} j a_j x^{j-1}$

$\Rightarrow a_j = (j+1)a_{j+1} \Rightarrow a_j = \frac{a_0}{j!}$. Also $y = c \cdot \exp(x) = c \sum_{n=0}^{\infty} \frac{x^n}{n!}$. $\operatorname{ord}_p(n!) = \frac{n - s(n)}{p-1}$ ($s(n) =$ Quersumme von n in p-adischer Darstellung).

Archimedische STIRLING-Formel:

$$\begin{aligned} \log(n!) &= n\log(n) - n + \frac{1}{2}\log(2\pi n) + \frac{\theta_n}{12n}, \qquad 0 < \theta_n < 1 \\ n! &= e^{n \log n - n + \ldots} \\ &= n^n e^{-n} \sqrt{2\pi n} e^{\theta_n / 12n} \end{aligned}$$

Konvergenzradius: $\limsup_n (\sqrt[n]{|n!|_p})^{-1} \Rightarrow$ konvergiert für $p > 2$ auf $p\mathbb{Z}_p$.

Beispiel 2.3.10
Die additive Gruppe von $\mathbb{Q}_p$ ist LCA (locally compact abellion). Solche Gruppen besitzen ein verschiebungsinvariantes BOREL-Maß, ein sog. HAAR-Maß. Das HAAR-Maß auf $\mathbb{Q}_p$ ist

$$\lambda(a + p^n \mathbb{Z}_p) = \frac{1}{p^n}$$

mit Normierung $\lambda(\mathbb{Z}_p) = 1$.

Ende VL 22
20.01.2015

Satz 2.3.11 („Satz 2“ HENSELSs Lemma)
Sei K vollständig in der nichtarchimedischen Bewertung $|\cdot|$, $\mathcal{O} = \{x \in K : |x| \leq 1\}$, $f \in \mathcal{O}[X]$, $x_0 \in \mathcal{O}$ approximative Nullstelle:

$$|f(x_0)| < |f'(x_0)^2|.$$

Dann besitzt f in $\mathcal{O}$ genau eine Wurzel $x \in \mathcal{O}$ mit $|x - x_0| < \frac{|f(x_0)|}{|f'(x_0)|}$.

Die Folge (x_n) mit $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ konvergiert gegen x.

Beweis: Setze $c_0 = |f(x_0)|/|f'(x_0)| < f'(x_0) \leq 1$, $c := |f(x_0)|/|f'(x_0)|^2 < 1$. Wir zeigen induktiv

(i) $|x_n| \leq 1$ (also $x_n \in \mathcal{O}$)

(ii) $|x_n - x_0| \leq c_0$

(iii) $|f'(x_n)| = |f'(x_0)|$

(iv) $|f(x_n)|/|f'(x_n)|^2 \leq c^{2^n}$.

Das ist klar für $n = 0$.

Der Induktionsschritt auf $n + 1$:

(i) Aus (iv) wissen wir nach Voraussetzung: $|x_{n+1} - x_n| = \frac{|f(x_n)|}{|f'(x_n)|} \leq c^{2^n}|f'(x_n)| < 1$. Also $|x_{n+1}| \leq \max(|x_n|, |x_{n+1} - x_n|)$.

(ii) $|x_{n+1} - x_0| \leq \max(|x_{n+1} - x_n|, |x_n - x_0|)$, $|x_n - x_0| \leq c_0$

$$|x_{n+1} - x_n| \leq c^{2^n}|f'(x_0)| = c^{2^n - 1}c_0 < c_0$$

$\Rightarrow |x_{n+1} - x_0| \leq c_0$

(iii) $f'(x_{n+1}) = f'(x_n) + \alpha\frac{f(x_n)}{f'(x_n)}$, $\alpha \in \mathcal{O}$, also

$$\frac{f'(x_{n+1})}{f'(x_n)} = 1 + \alpha\frac{f(x_n)}{f'(x_n)^2}.$$

$|\alpha\frac{f(x_n)}{f'(x_n)^2}| \leq c^{2^n} < 1 \Rightarrow \frac{f'(x_{n+1}}{f'(x_n)} = 1$

(iv) $f(x_{n+1}) = f(x_n) - f'(x_n)\frac{f(x_n)}{f'(x_n)} + \beta(\frac{f(x_n)}{f'(x_n)})^2$, $\beta \in \mathcal{O}$ (TAYLOR-Entwicklung) $\Rightarrow \left|\frac{f(x_{n+1})}{f'(x_{n+1})}^2\right| \leq \left|\frac{f(x_n)}{f'(x_n)^2}\right|^2 \leq (c^{2^n})^2 = c^{2^{n+1}}$

Es folgt $x_n \to x \in \mathcal{O}$. Aus der Rekursionsformel folgt $x = x - \frac{f(x)}{f'(x)} \Rightarrow f(x) = 0$. Aus (ii) folgt $|x - x_0| \leq c_0$. Angenommen f hat noch eine Wurzel $y \in \mathcal{O}$ mit $|y - x_0| \leq c_0$. Dann folgt $0 = f(y) = f(x) + f'(x)(x - y) + \gamma(y - x)^2$, $\gamma \in \mathcal{O}$. Also $|f'(x)| \leq |y - x| \leq c_0$. Aus (iii) folgt $|f'(x)| = |f'(x_0)|$. $c_0 = |f(x_0)|/|f'(x_0)| \Rightarrow |f'(x_0)|^2 \leq |f(x_0)|$ ↯ □

§2.4 Lokale Körper (mit Chrakteristik 0)

Definition 2.4.1
Eine Abbildung $\nu : K \to \mathbb{R} \cup \{\infty\}$ heißt **Exponentialbewertung** genau dann, wenn

(i) $\nu(x) = \infty \Leftrightarrow x = 0$,

(ii) $\nu(xy) = \nu(x) + \nu(y)$,

(iii) $\nu(x + y) \geq \min(\nu(x), \nu(y))$.

Bemerkung 2.4.2 (i) Durch $|x| = c^{\nu(x)}$, $0 < c < 1$, entsteht eine Bewertung von K. Diese ist nichtarchimedisch.

(ii) Die triviale Exponentenbewertung $\nu(x) = 0$ für alle $x \in K^\times$ wird ausgeschlossen.

Beispiel 2.4.3 (i) $K = \mathbb{Q}$, $p \in \mathbb{P}$, $\nu_p(x) = \mathrm{ord}_p(x)$. Sie induziert die p-adische Bewertung $|\cdot|_p$. Mann nimmt gern $c = \frac{1}{p}$.

(ii) Milde Verallgemeinerung: K alg. ZK, $\mathfrak{p} \subset \mathcal{O}_K$ maximales Ideal. $\nu_\mathfrak{p}(x) = \mathrm{ord}_\mathfrak{p}(x)$ ist Exponentialbewertung und führt zu Bewertung $|\cdot|_\mathfrak{p}$ auf K. Liegt $\mathfrak{p}$ über der Primzahl p, so ist $\mathbb{Q}_p \subset K_\mathfrak{p}$.

Definition 2.4.4
Eine Exponentialbewertung heißt **diskret** $\Leftrightarrow \nu(K^\times)$ ist bezüglich Addition diskrete Untergruppe von $\mathbb{R}$, d.h. $\nu(K^\times) \cong \mathbb{Z}$.

Beispiel 2.4.5
Die $\nu_{\mathfrak{p}}$ sind diskret.

Fakt 2.4.6
Sei ν eine diskrete Exponentenbewertung von K, $\mathcal{O}_\nu := \{x \in K : \nu(x) \geq 0\}$, $\mathfrak{m}_\nu := \{x \in K : \nu(x) > 0\}$.

Dann ist $\mathcal{O}_\nu$ ein diskreter Bewertungsring. $\mathfrak{m}_\nu$ sein maximales Ideal, es ist ein Hauptideal. Der Körper $\mathcal{O}_\nu/\mathfrak{m}_\nu$ heißt **Restklassenkörper**.

Beweis: $\mathcal{O}_\nu$ ist offensichtlich ein Ring, er ist integer (denn: in einem Körer), kommutativ, mit 1. Es gilt für $x \in K^\times$: $x \in \mathcal{O}_\nu$ oder $x^{-1} \in \mathcal{O}_\nu$. Weiter ist $\mathfrak{m}_\nu$ ein Ideal. Ist $x \in \mathcal{O}_\nu \setminus \mathfrak{m}_\nu$, so ist $\nu(x) = 0 \Rightarrow \nu(x^{-1}) = 0 \Rightarrow x^{-1}\mathcal{O}_\nu$. Also ist $\mathcal{O}_\nu$ lokaler Ring mit $\mathfrak{m}_\nu$ als einzigem maximalen Ideal. Sei $\pi \in \mathfrak{m}_\nu$ mit maximaler Exponentenbewertung (ν ist diskret). Dann ist $\nu(K^\times) = \nu(\pi)\mathbb{Z}$. Also ist jedes $x \in K^\times$ darstellbar als $x = \pi^{\nu(x)} \cdot u$, $u \in \mathcal{O}_\nu^\times$. Insbesondere ist $(\pi) = \mathfrak{m}_\nu$. □

Definition 2.4.7
Ein exponentenbewerteter Körper der Chrakteristik = 0 heißt **lokaler Körper** genau dann, wenn

(i) Die Exponentialbewertung ist diskret,

(ii) K ist vollständig (bzgl. der induzierten Bewertung),

(iii) der Restklassenkörper ist endlich.

Fakt 2.4.8
Lokale Körper sind lokalkompakt.

Beweis: Wir zeigen, dass $\mathcal{O}_\nu$ kompakt ist. Dann folgt die Aussage: $K = \bigcup_{n=0}^{\infty} \pi^{-n}\mathcal{O}_\nu$ (K ist lokalkompakt als Vereinigung abzählbarvieler kompakter Mengen).

Sei dazu (x_n) Folge aus $\mathcal{O}_\nu$. Dann ex. Teilfolge, deren Restklassen in $\mathcal{O}_\nu/\mathfrak{m}_\nu$ gleich sind. Wegen $\mathfrak{m}_\nu^n/\mathfrak{m}_\nu^{n+1} \cong \mathcal{O}_\nu/\mathfrak{m}_\nu$ (Isomorphismus = Multiplikation mit π^n) lässt sich das iterieren. $\Rightarrow$ Wir finden Teilfolge (y_n) mit $y_n \equiv y_{n+1} \pmod{\mathfrak{m}_\nu^n}$. Das ist Fundamentalfolge, also konvergent. Damit erhalten wir Folgenkompaktheit und damit Kompaktheit (metrischer Raum). □

Bemerkung 2.4.9
Ist K in der Bewertung $|\cdot|$ lokalkompakt, so ist K vollständig (ÜA).

Beispiel 2.4.10
Die $\mathbb{Q}_p$ sind lokale Körper: $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

Fakt 2.4.11
Sei K lokalkompakt in der Bewertung $|\cdot|$, L/K endliche Erweiterung, dann besitzt L höchstens eine Bewertung, welche $|\cdot|$ fortsetzt.

Beweis: K ist vollständig:

$\overline{\mathbb{D}}(0,r)$ ist Kompakt für $r << 1$, also auch $\overline{\mathbb{D}}(x,r)$, für alle $x \in K$. Ist (x_n) CAUCHY-Folge, so liegen alle x_n in $\overline{\mathbb{D}}(x_{n_0}, \varepsilon)$ für $n \geq n_0$. Es gibt also konvergente Teilfolge. Eine CAUCHY-Folge mit konvergenter Teilfolge ist konvergent.

Sei $|\cdot|_L$ Fortsetzung von $|\cdot|$ auf L. Wir konstruieren eine Art Norm auf L: Sei $\omega_1, \ldots, \omega_n$ K-Basis von L, für $x \in L$ gilt $x = \sum \alpha_i \omega_i$, $\alpha_i \in K$. Wir setzen $\|x\| := \max_{i=1}^n(|\alpha_i|)$. Eigenschaften:

(i) $\|x\| = 0 \Leftrightarrow x = 0$,

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

(iii) $\|\alpha x\| = |\alpha|\|x\|$

$K^n \to L : (\alpha_1, \ldots, \alpha_n) \mapsto \sum_{j=1}^n \alpha_j \omega_j$ ist Isometrie, falls links die Norm $|(\alpha_1, \ldots, \alpha_n)| := \max\{|\alpha_i|\}$ ist. Mit K ist auch K^n lokalkompakt. Also ist $S = \{x \in L : \|x\| = 1\}$ kompakt: yS liegt in präkompakter Umgebung der 0 für geeignete y. Wir vergleichen $|\cdot|_L$ und $\|\cdot\|$. $|x|_L \leq \sum |\alpha_i||\omega_i|_L \leq c\|x\|$ für ein $c > 0$. Wir zeigen $\exists c' > 0$, s.d. $\|x\| \leq c'|x|_L$.

Indirekt: Sei (x_n) Folge aus S mit $|x_n|_L \to 0$. Dann existiert eine Teilfolge (y_n) mit $y_n \to y \in S$ in $\|\cdot\|$, d.h. $\|y_n - y\| \to 0$. Es folgt

$$|y|_L \leq |y_n - y|_L + |y_n|_L \leq c\|y_n - y\| + |y_n|_L \to 0.$$

Somit $y = 0$ ↯. Also $\exists \varepsilon > 0 \forall x \in S : |x|_L \geq \varepsilon$. D.h. $\|x\| = 1 \Rightarrow |x|_L \geq \varepsilon \Rightarrow \|x\| \leq c'|x|_L$ für alle $x \in S$. Sei $x \in L^\times$, $x = \sum \alpha_i \omega_i$, $\|x\| = |\alpha_j| > 0 \Rightarrow \|\alpha_j^{-1} x\| = 1$.

$$\|x\| = |\alpha_j|\|\alpha_j^{-1}x\| \leq c'|\alpha_j||\alpha_j^{-1}x|_L = c'|x|_L.$$

Sind $|\cdot|_L$ und $|\cdot|'_L$ zwei Fortsetzungen von $|\cdot|$ auf L, so haben wir

$$|x|_L \leq c|x|'_L \text{ und } |x|'_L \leq c'|x|_L.$$

Ersetze x durch x^N, $N \to \infty \Rightarrow |x|_L = |x|'_L$ □

Ende VL 23
21.01.2015

Bemerkung 2.4.12 (i) Das eigentliche Problem ist die Existenz der Fortsetzung.

(ii) Die Fortsetzung ist äquivalent zu $\|\cdot\|$, falls sie existiert.

(iii) L ist in der Fortsetzung lokalkompakt, also vollständig.

Fakt 2.4.13
Sei L/K endlich, L bewertet, $\hat{K}$ sei lokalkompakt. Dann ist $\hat{L} = L \cdot \hat{K}$[10] und es gilt $[\hat{L} : \hat{K}] \leq [L : K]$.

Beweis: $L\hat{K} \subset \hat{L}$ und $L\hat{K}/\hat{K}$ ist endliche Erweiterung. Nach obigem Fakt ist $L\hat{K}$ vollständig, also abgeschlossen in $\hat{L}$. Nun ist $L \subset L\hat{K}$ dicht in $\hat{L}$, also $L\hat{K} = \hat{L}$. $[L\hat{K} : \hat{K}] \leq [L : K]$ ist Algebra I. □

Fakt 2.4.14
Jede endliche Erweiterung $K/\mathbb{Q}_p$ besitzt Fortsetzung von $|\cdot|_p$ auf K.

Beweis: $\mathbb{Z}_p$ ist dBR, einziges maximales Ideal ist $(p) = p\mathbb{Z}_p$, alle anderen Ideale sind (p^m), $m \geq 2$ und (0). Somit ist $\mathbb{Z}_p$ NOETHERsch, ganzabgeschlossen (da faktoriell), jedes Primideal $\neq 0$ ist maximal. Also $\mathbb{Z}_p$ DED-Ring. Sei $\mathcal{O}$ der ganze Abschluss von $\mathbb{Z}_p$ in K, dann ist auch $\mathcal{O}$ DED-Ring, $\mathcal{O}$ hat nur endlich viele Primideale. Also ist $\mathcal{O}$ ein HI-Ring, somit

$$p\mathcal{O} = (\pi_1^{e_1}) \cdot \ldots \cdot (\pi_m^{e_m}), \qquad e_j \geq 1$$

[10] Dieses Produkt ist nur definiert, falls ein Körper existiert, der beide Faktoren enthält (in diesem Fall leistet dies $\hat{L}$) und es ist der kleinste Körper, welcher beide Körper enthält.

mit maximalen Idealen $(\pi_1), \ldots, (\pi_m)$. Nach chinesischem Restsatz induzieren sie nichtäquivalente Bewertungsfortsetzungen auf K via $\nu_i(x) = \frac{1}{e_i} \operatorname{ord}_{\pi_i}(x)$. Nach Eindeutigkeitsaussage ist $m = 1$, also $p\mathcal{O} = \pi^e\mathcal{O} \Rightarrow p = u\pi^e$ mit $u \in \mathcal{O}^\times$. $\nu_\pi(x) := \frac{1}{e} \operatorname{ord}_\pi(x)$ induziert die Bewertungsfortsetzung

$$|x|_\pi = p^{-\nu_\pi(x)/e}.$$

Tatsächlich: $x \in \mathbb{Q}_p^\times \Rightarrow x = vp^m$, $v \in \mathbb{Z}_p^\times$.

$$|x|_\pi = p^{-\nu_p i(x)/e} = p^{-em/e} = p^{-m} = |x|_p$$

□

Folgerung 2.4.15
$|x|_\pi = |\operatorname{N}_{\mathbb{Q}_p}^K(x)|_p^{1/n}$, $n = [K : \mathbb{Q}_p]$

Beweis: Sei $L/\mathbb{Q}_p$ normale Hülle von $K/\mathbb{Q}_p$, $G = \operatorname{Gal}(L/\mathbb{Q}_p)$. Mit $x \mapsto |x|$ ist auch $x \mapsto |\sigma x|$ für $\sigma \in G$ eine Bewertung von L, also $|\sigma x| = |x|$. Es folgt $|\operatorname{N}_{\mathbb{Q}_p}^L(x)| = \prod_{\sigma\in G} |\sigma x| = |x|^{[L:\mathbb{Q}_p]}$. Ist $x \in K$, so folgt

$$\prod_{\sigma\in G} \sigma x = (\operatorname{N}_{\mathbb{Q}_p}^K(x))^{[L:K]}.$$

□

Bemerkung 2.4.16 (i) Es ist nicht offensichtlich, dass $x \mapsto |\operatorname{N}_{\mathbb{Q}_p}^K(x)|^{1/n}$ die Dreiecksungleichung erfüllt.

(ii) $|\cdot|_p$ auf $\mathbb{Q}_p$ setzt sich eindeutig auf $\overline{\mathbb{Q}}_p$ fort.

Fakt 2.4.17 (KRASNERs Lemma)
Sei $\alpha \in \overline{\mathbb{Q}}_p$ fixiert. Ist dann $\beta \in \overline{\mathbb{Q}_p}$ genügend nahe α (d.h. $|\alpha-\beta|$ klein), so folgt $\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$[11].

Beweis: Seien $\alpha = \alpha_1, \ldots, \alpha_n$ die Konjugierten von α, also die Wurzeln des irreduziblen Polynoms von α über $\mathbb{Q}_p$. Es gelte $|\alpha - \beta| < |\alpha - \alpha_i|$, $i = 2, \ldots, n$. Sei K der Zerfällungskörper von $\operatorname{Irr}(T, \alpha, \mathbb{Q}_p)$, d.h. $K = \mathbb{Q}_p(\alpha_1, \ldots, \alpha_n)$. Wir betrachten $K(\beta)/\mathbb{Q}_p(\beta)$, das ist Gal-Erweiterung. Sei $\sigma \in \operatorname{Gal}(K(\beta)/\mathbb{Q}_p(\beta))$, dann gilt

$$|\sigma\alpha - \sigma\beta| = |\sigma\alpha - \beta| = |\alpha - \beta|,$$

also $|\sigma\alpha - \alpha| \leq \max\{|\sigma\alpha - \beta|, |\beta - \alpha|\} = |\alpha - \beta| < |\alpha - \alpha_i|$. Es folgt $\sigma\alpha = \alpha$ ($\sigma\alpha = \alpha_j$), d.h. $\alpha \in \mathbb{Q}_p(\beta) \Rightarrow \mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$. □

Folgerung 2.4.18
Sind $\alpha, \beta \in \overline{\mathbb{Q}}_p$ genügend nahe, so gilt

$$\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta).$$

Satz 2.4.19 („Satz 3“)
Jede endliche Erweiterung von $\mathbb{Q}_p$ ist der Form $K_\mathfrak{p} = K \cdot \mathbb{Q}_p$ für einen geeigneten ZL K und eine $\mathfrak{p} \mid p$ von $\mathcal{O}_K$.

[11] Davon gibt es natürlich kein Äquivalent in $\mathbb{Q}$. „Wieder ein kleines Wunder der p-adik.“

Beweis: Sei E endliche Erweiterung von $\mathbb{Q}_p$, $E = \mathbb{Q}_p(\alpha)$ (Satz vom primitiven Element). $f = \mathrm{Irr}(X, \alpha, \mathbb{Q}_p)$ = unitäres Polynom über $\mathbb{Q}_p$. Wir wählen $g \in \mathbb{Q}[X]$ unitär vom selben Grad wie f, so dass die Koeffizienten von f und g nahe sind bzgl. $|\cdot|_p$. Wir zeigen, dass dann auch die Wurzeln von f und g nahe sind. D.h. Stetigkeit der Wurzeln, als Funktion der Koeffizienten.

Zuerst: $disc(f) \neq 0$, also auch $disc(g) \neq 0$. Somit hat auch g keine mehrfachen Wurzeln. Seien $\alpha = \alpha_1, \alpha_2 \ldots, \alpha_n$ die Wurzeln von f und $\eta > 0$ so, dass $|\alpha_i - \alpha_j| \geq \eta$ für alle $i \neq j$.

Seien $\beta_1, \ldots, \beta_n$ die Wurzeln von g. Aus $g(\beta_i) = 0$ folgt

$$|\beta_i|^n \leq C \max(1, |\beta_i|, \ldots, |\beta_i|^{n-1}).$$

Es gilt also $|\beta_i| \leq C$ und damit $|\beta_i - \beta_j| \leq C$. Es gilt $\prod_{i \neq j} |\beta_i - \beta_j|^2$ ist nahe $\prod_{i \neq j} |\alpha_i - \alpha_j|^2 = C_1$. Also $\exists \eta' > 0$, s.d. $|\beta_i - \beta_j| \geq \eta'$ für $i \neq j$.

Nun ist $|g(\alpha_1)| = |g(\alpha_1) - f(\alpha_1)|$ klein, also ist auch $\prod_{i=1}^n |\alpha_1 - \beta_i|$ klein. Alle Faktoren sind beschränkt, also muss wenigstens ein Faktor klein sein, say $|\alpha_1 - \beta_1|$ klein. Da die β_i Mindestabstand haben, ist nur $|\alpha_1 - \beta_1|$ klein.

KRASNERs Lemma zeigt: $\mathbb{Q}_p(\alpha_1) = \mathbb{Q}_p(\beta_1)$. Wir fanden also $K/\mathbb{Q}$ s.d. $K\mathbb{Q}_p = E$ für vorgelegtes E/IQ_p. Sei $\mathcal{O}_K$ der Ganzheitsring in K. $\mathcal{O}_E = \{x \in E : |x| \leq 1\}$. Dann ist $\mathcal{O}_K \subset \mathcal{O}_E$:

$$\begin{aligned} & x^n + a_1 x^{n-1} + \ldots + a_n = 0, a_j \in \mathbb{Z} \\ \Rightarrow & |x|^n \leq \max(1, |x|, \ldots, |x|^{n-1}) \\ \Rightarrow & |x| \leq 1 \end{aligned}$$

Sei $\mathfrak{m}_E = \{x \in \mathcal{O}_E : |x| < 1\}$. Das ist maximales Ideal in $\mathcal{O}_E$. $\mathfrak{p} := \mathcal{O}_K \cap \mathfrak{m}_E$ ist Primideal und $\neq (0)$, wg. $p \in \mathfrak{p}$ Für $m \in \mathbb{Z}$ gilt $|m|_{\mathfrak{p}} < 1 \Leftrightarrow |m|_p < 1$, also auch auf $\mathbb{Q}$. $\Rightarrow |\cdot|_{\mathfrak{p}}$ und $|\cdot|_p$ stimmen auf $\mathbb{Q}$ überein $\Rightarrow$ auf $\mathbb{Q}_p$ $\Rightarrow K_{\mathfrak{p}} = E$.

□

Ende VL 24
27.01.2015

Definition 2.4.20
Seien $L/K/\mathbb{Q}_p$ endliche Erweiterungen. $\mathfrak{m}_K = (\pi_K)$, $\mathfrak{m}_L = (\pi_L)$. Dann ist $\pi_K = u \cdot \pi_L^e$ mit $u \in \mathcal{O}_L^\times$ (oder äquivalent: $|\pi_K| = |\pi_L|^e$).

Dann heißt $e = e(L/K)$ **Verzweigungsindex**. Der **Restklassengrad** $f = f(L/K)$ ist der Grad der Restklassenkörpererweiterung

$$f = [\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}_K/\mathfrak{m}_K].$$

Bemerkung 2.4.21
Die beiden Turmformeln sind klar.

(i) $e(M/K) = e(M/L)e(L/K)$

(ii) $f(M/K) = f(M/L)f(L/K)$

Satz 2.4.22 („Satz 4“)
Seien $L/K/\mathbb{Q}_p$ endliche Erweiterungen. Dann gilt

$$[L : K] = e(L/K)f(L/K).$$

Insbesondere sind $\mathcal{O}_L/\mathfrak{m}_L$ und $\mathcal{O}_K/\mathfrak{m}_K$ endlich.

Beweis: Seien $\alpha_1, \ldots, \alpha_f \in \mathcal{O}_L$, s.d. $\overline{\alpha_1}, \ldots, \overline{\alpha_f} \in \mathcal{O}_L/\mathfrak{m}_L$ eine Basis des $\mathcal{O}_K/\mathfrak{m}_K$-Vektorraums $\mathcal{O}_L/\mathfrak{m}_L$ sind. Wir zeigen, dass die Vektoren $\alpha_i \pi_L^j$, $1 \leq i \leq f$, $0 \leq j < e$ K-linear unabhängig sind.

Sei $\sum \lambda_{ij} \alpha_i \pi_L^j = 0$, $\lambda_{ij} \in K$. O.B.d.A. $\lambda_{ij} \in \mathcal{O}_K$ und nicht alle aus $\mathfrak{m}_K$. Sei $\mu_j := \sum_{i=1}^f \lambda_{ij} \alpha_i \in \mathcal{O}_L$, diese sind nicht alle $= 0$:

$$\sum \overline{\lambda}_{ij} \overline{\alpha_i} = 0 \Rightarrow \overline{\lambda}_{ij} = 0 \lightning$$

Sei $\mu_r \neq 0$. Wir teilen durch die höchste Potenz s von π_K, welche alle π_{ir} teilt. Dann ist wenigstens ein Koeffizient eine Einheit. Deshalb ist die Reduktion modulo $\mathfrak{m}_L$ ungleich 0. Es folgt

$$\mu_r = \pi_K^s \cdot u_r, \text{ mit } u_r \in \mathcal{O}_L^\times \text{ wegen } \overline{u_r} \neq 0).$$

Also $\mu_r = v_r \pi_L^{es}$, $v_r \in \mathcal{O}_L^\times$.

In $\sum_{j=0}^{e-1} \mu_j \pi_L^j$ müssen 2 Summanden $\neq 0$ denselben Betrag haben, also dieselbe Potenz von π_L enthalten. Es gibt also $0 \leq a < b \leq e-1$ mit $|\mu_a \pi_L^a| = |\mu_b \pi_L^b|$. Nun ist $|\mu_a| = |\pi_L|^{es}$, $|\mu_b| = |\pi_L|^{et}$. Das gibt $e(s-t) = b - a \Rightarrow a = b$ $\lightning$

Wir haben gezeigt $e \cdot f \leq [L:K]$.

Setze $M := \sum_{i,j} \mathcal{O}_K \alpha_i \pi_L^j \subset \mathcal{O}_L$ und $N := \sum_j \mathcal{O}_K \cdot \alpha_i \subset \mathcal{O}_L$. Dann ist $M = N + \pi_L N + \ldots + \pi_L^{e-1} N$. Wir zeigen $\mathcal{O}_L = N + \pi_L \mathcal{O}_L$. Sei dazu $\alpha \in \mathcal{O}_L$, es folgt

$$\alpha \equiv \sum \lambda_i \alpha_i \pmod{\pi_L}$$

für gewisse $\lambda_i \in \mathcal{O}_K$. $\Rightarrow \alpha - \sum \lambda_i \alpha_i \in \pi_L \mathcal{O}_L$.

Iterieren: $\mathcal{O}_L = N + \pi_L(N + \mathcal{O}_L) = N + \pi_L N + \pi_L^2 \mathcal{O}_L$ usw. Es folgt $\mathcal{O}_L = M + \pi_L^e \mathcal{O}_L = M + \pi_K \mathcal{O}_L$.

Iterieren: $\mathcal{O}_L = M + \pi_K(M + \pi_K \mathcal{O}_L) = M + \pi_K M + \pi_K^2 \mathcal{O}_L$ ($\pi_K M \subset M$). Also $\mathcal{O}_L = M + \pi_K^2 \mathcal{O}_L$ usw. $\Rightarrow \mathcal{O}_L = M + \pi_K^N \mathcal{O}_L$ für alle $N \geq 1$.

Das zeigt: M ist dicht in $\mathcal{O}_L$. M ist stetiges Bild eines Kompaktums, also selbst kompakt und damit abgeschlossen in $\mathcal{O}_L$. Das zeigt $M = \mathcal{O}_L$. Es folgt: $\mathcal{O}_L$ ist freier $\mathcal{O}_K$-Modul mit Basis $\alpha_i \pi_L^j$, also vom Rang $e \cdot f$. Dies ist dann automatisch eine K-Basis von L. □

Folgerung 2.4.23 (aus dem Beweis)
$\mathcal{O}_L$ ist freier $\mathcal{O}_K$-Modul vom Ranf $[L:K]$.

Bemerkung 2.4.24
In Kapitel § I haben wir ähnliches durch Lokalisieren erreicht. Für Ringe ganzer Zahlen $\mathcal{O}_L/\mathcal{O}_K$. Für Zahlkörper L/K ist das falsch.

§2.5 Bewertung von Zahlkörpern

Satz 2.5.1 („Satz 5“)
Sei K algebraischer ZK.

(i) Jede Bewertung von K setzt eine p-adische oder die archimedische Bewertung von $\mathbb{Q}$ fort.

(ii) Die Fortsetzungen von $|\cdot|_\infty$ sind in Bijektion zu den Einlagerungen $\sigma : K \to \mathbb{R}$ (r Stück) und den Paaren $\tau, \overline{\tau} : K \to \mathbb{C}$ (s Stück).

(iii) Die Fortsetzungen von $|\cdot|_p$ sind in Bijektion zu den Primidealen $\mathfrak{p} \subset \mathcal{O}_K$ mit $\mathfrak{p} \mid p$ ($\Leftrightarrow \mathfrak{p} \cap \mathbb{Z} = (p)$)

(iv) Die Bijektion in (ii) ist $|x|_\rho := |\rho(x)|$.

(v) Die Bijektion in (iii) ist $|x|_\mathfrak{p} := p^{-\operatorname{ord}_\mathfrak{p}(x)/e(\mathfrak{p}/p)}$.

Beweis:

- Sei $|\cdot|$ nichttriviale Bewertung von K. Wir zeigen, dass die Einschränkung auf $\mathbb{Q}$ auch nichttrivial ist. Sei dazu $\omega_1, \ldots, \omega_n$ $\mathbb{Q}$-Basis von K. Sei $|\alpha| = 1$ für alle $\alpha \in \mathbb{Q}^\times$. Dann folgt $|x| \leq C$ für alle $x \in K^\times$ (Standardargument: Folge von Potenzen betrachten). Daraus folgt $|x| = 1$ für alle $x \in K^\times$. Der Satz von OSTROWSKI zeigt (i).

- Jede der Einlagerungen $\rho : K \to \mathbb{R}$ oder $\mathbb{C}$ definiert Fortsetzung von $|\cdot|_\infty$. Wir zeigen, dass sie (abgesehen von komplex konjugierten) inäquivalent sind. $j : K \to K_\mathbb{R}$ hat dichtes Bild, da $j(\mathcal{O}_K)$ Gitter ist: $j(K) = \bigcup_{m \in \mathbb{N}\setminus\{0\}} \frac{1}{m} j(\mathcal{O}_K)$.

  Sei $|\sigma x| = |\tau x|^s$ für alle $x \in K$, $x \in \mathbb{Q}$ zeigt $s = 1$. Sind σ, τ verschieden (auch nicht komplex konj.), so ex. Folgt (x_n) aus K mit $\sigma x_n \to 0$ und $\tau x_n \to 1$ (wegen der Dichtigkeit).

  Also $|\sigma x_n| \to 0$, $|\tau x_n| \to 1$ $\lightning$.

  Sei nun $|\cdot|$ eine Bewertung von K, welche $|\cdot|_\infty$ fortsetzt und sei $\hat{K}$ die Komplettierung. Dann haben wir $\hat{\mathbb{Q}} = \mathbb{R} \subset \hat{K}$, $\hat{K} = \mathbb{R} \cdot K$ mit $[\hat{K} : \mathbb{R}]$ endlich.

  $\mathbb{R}$ und $\mathbb{C}$ besitzen nur eine Fortsetzung, welche $|\cdot|_\infty$ von $\mathbb{Q}$ fortsetzen. Für $\mathbb{R}$ ist das klar, da $\mathbb{Q} \subset \mathbb{R}$ dicht ist. Für $\mathbb{C}$ so: Alle Normen als $\mathbb{R}$-VR sind äquivalent, d.h. $\|\cdot\|_1 \leq C \cdot \|\cdot\|_2$ und $\|\cdot\|_2 \leq C' \cdot \|\cdot\|_1$, also auch alle Bewertungen, die $|\cdot|_\infty$ auf $\mathbb{R}$ fortsetzen. Somit sind sie gleich. Also kommt jede solche Bewertung von K von einer Einlagerung $\rho : K \to \mathbb{R}$ oder $\mathbb{C}$

- Sei $|\cdot|$ nichtarchimedische Bewertung von alg. ZK K. $|\cdot|$ setze $|\cdot|_p$ auf $\mathbb{Q}$ fort. Sei

$$\mathcal{O} := \{x \in K : |x| \leq 1\},$$

$$\mathfrak{m} := \{x \in K : |x| < 1\}.$$

  Dann ist $\mathfrak{m}$ maximales Ideal: Jedes Element aus $\mathcal{O} \setminus \mathfrak{m}$ ist Einheit. $\mathcal{O}_K \cap \mathfrak{m}$ ist nichttriviales Primideal in $\mathcal{O}_K$: $p \in \mathcal{O}_K \cap \mathfrak{m}$. Also ist $\mathcal{O}_K \cap \mathfrak{m} = \mathfrak{p}$ maximales Ideal in $\mathcal{O}_K$. Wir haben $K \subset K_\mathfrak{p}$ = Vervollständigung von K in $|\cdot|_\mathfrak{p}$,

$$\mathcal{O}_K \subset S_\mathfrak{p}^{-1}\mathcal{O}_K \subset \mathcal{I} \subset \mathcal{O}_\mathfrak{p},$$

  $S_\mathfrak{p} = \mathcal{O}_K \setminus \mathfrak{p}$ Lokalisierung,

$$\mathfrak{p} \subset S^{-1}\mathfrak{p} \subset \mathfrak{m} \subset \mathfrak{m}_\mathfrak{p}.$$

  Klar ist $S^{-1}\mathcal{O}_K \subset \mathcal{O}$. Sei $x \notin S^{-1}\mathcal{O}_K$, dann folgt $\operatorname{ord}_\mathfrak{p}(x) < 0 \Rightarrow \operatorname{ord}_\mathfrak{p}(x^{-1}) > 0 \Rightarrow x^{-1}S^{-1}\mathfrak{p} \subset S^{-1}\mathfrak{m} = \mathfrak{m} \Rightarrow |x^{-1}| < 1 \Rightarrow |x| > 1 \Rightarrow x \notin \mathcal{O}$. Somit $S^{-1}\mathcal{O}_K = \mathcal{O}$.

  $S^{-1}\mathcal{O}_K$ ist dBR, sein maximales Ideal ist also HI: $S^{-1}\mathfrak{p} = (\pi)$. K ist der QK von $S^{-1}\mathcal{O}_K$ (Kapitel I). Es folgt $|\cdot| = |\cdot|_\mathfrak{p}$: $\mathfrak{m} = S^{-1}\mathfrak{p} = (\pi)$, alsi ist π für $|\cdot|$ ein Element maximaler Bewertung < 1. Jedes $x \in K^\times$ hat die Form $x = u \cdot \pi^m$, $m \in \mathbb{Z}$, u Einheit. $\Rightarrow |x| = |\pi|^m$. $p = \nu\pi^e$ mit $e = e(\mathfrak{m}/p) \Rightarrow |p| = \frac{1}{p} = |\pi|^e \Rightarrow |\pi| = \frac{1}{p^{1/e}} \Rightarrow |x| = \frac{1}{p^{m/e}}$, $m = \operatorname{ord}_\mathfrak{p}(x)$.

□

Ende VL 25
28.01.2015

Fakt 2.5.2
Sei L/K endliche Erweiterung von ZK, $\mathfrak{P}|\mathfrak{p}$. Dann gilt:

(i) $e(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = e(\mathfrak{P}/\mathfrak{p})$

(ii) $f(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = f(\mathfrak{P}/\mathfrak{p})$

(iii) $\mathcal{O}_K/\mathfrak{p} = \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{m}_{\mathfrak{p}}$

Beweis: $\mathcal{O} = S^{-1}\mathcal{O}_K$ ist dBR, sein maximales Ideal ist $\mathfrak{m} = (\pi)$, $S^{-1}\mathfrak{p} = \mathfrak{m}$, QK ist K. $p = u\pi^e$, $u \in \mathcal{O}^\times$, $e = e(\mathfrak{p}/p)$. Wir zeigen: $S^{-1}\mathcal{O}_K/S^{-1}\mathfrak{p}(= \mathcal{O}/\mathfrak{m}) = \mathcal{O}_K/\mathfrak{p}$: $\mathcal{O}_K \to S^{-1}\mathcal{O}_K \to S^{-1}\mathcal{O}_K/S^{-1}\mathfrak{p}$ hat den Kern $\mathcal{O}_K \cap S^{-1}\mathfrak{p} = \mathfrak{p}$ (siehe KapI). Wir zeigen die Surjektivität:

$x \in S^{-1}\mathcal{O}_K \Rightarrow x = y/s, y \in \mathcal{O}_K, s \in \mathcal{O}_K\backslash\mathfrak{p}$. $\exists t \in \mathcal{O}_K\backslash\mathfrak{p}$, s.d. $st \equiv 1 \pmod{\mathfrak{p}} \Rightarrow y/s \equiv yt \pmod{\mathfrak{p}}$ $\Rightarrow x \equiv yt \pmod{\mathfrak{p}}$. Also ist x Bild von $yt \in \mathcal{O}_K \pmod{S^{-1}\mathfrak{p}}$. Es folgt $f(\mathfrak{p}/p) = [\mathcal{O}/\mathfrak{m} : \mathbb{F}_p]$. Nach Turmformel folgt analoge Formel für $f(\mathfrak{P}/\mathfrak{p})$.

Beim Komplettieren ändert sich im nichtarchimedischen Fall die Wertegruppe der Bewertung nicht: Sie bleibt $\{p^{m/e} : m \in \mathbb{Z}\} \cup \{0\}$ wie auf K. Somit folgt aus $p = u \cdot \pi^{K_{\mathfrak{p}}/\mathbb{Q}_p}$, dass $e(K_{\mathfrak{p}}/\mathbb{Q}_p) = e(\mathfrak{p}/p)$. $p\mathcal{O}_K = \mathfrak{p}^{e(\mathfrak{p}/p)} \cdot \mathfrak{a}$, $\mathfrak{p} \nmid \mathfrak{a}$.

Es bleibt $\mathcal{O}/\mathfrak{m} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$. Wir haben

$$\mathcal{O} \to \mathcal{O}_{\mathfrak{p}} \to \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$$

hat Kern $\mathcal{O} \cap \mathfrak{m}_{\mathfrak{p}} = \mathfrak{m}$.

$\mathcal{O}_{\mathfrak{p}} \ni x = a_0 + a_1\pi + a_2\pi^2 + \ldots$ (a_j Repräsentantensystem von $\mathcal{O}_K$ modulo $\mathfrak{p}$)

$m_{\mathfrak{p}} = (\pi)$. Also $x \equiv a_0 \pmod{\mathfrak{m}_{\mathfrak{p}}}$. □

Bemerkung 2.5.3
Sei K algebraischer ZK, M_K Menge der Äquivalenzklassen nichttrivialer Bewertungen, $M_K = M_K^\infty \cup M_K^0$.

- M_K^∞ = archimedische Bewertungen
- $M_K^0 = M_K^f$ = nichtarchimedische Bewertungen
- $M_K^0 = Spec\mathcal{O}_K$ (fast)

Wir hatten sogenannte geometrische Abbildung

$$j : K \to \prod_{v \in M_K^\infty} K_v$$

mit K_v = Komplettierung von K an der Stelle v.

CHEVALLEY 1930

(i) Problem: $\prod_{v\in K} K_v$ ist zu groß - nicht lokalkompakt.

(ii) $\sum_{v\in K} K_v$ zu klein - K passt nicht diagonal hinein.

(iii) Sei $S \subset M_K$ endlich, $M_K^\infty \subset S$. Die S-Adele sind

$$\mathbb{A}_S = \prod_{v\in S} K_v \times \prod_{v \in M_K\backslash S} \mathcal{O}_{K_v}$$

Adele

Nun gilt $\mathbb{A}_K$ ist LCA (locally compact abelian) und K bettet sich diagonal ein.

Adele = adjoint elements

Die Einheiten $\mathbb{A}_K^\times$ heißen **Idele** = ideal elements ($J_K := \mathbb{A}_K^\times$).

§2.6 Unverzweigte Erweiterungen

Definition 2.6.1
Eine endliche Erweiterung von lokalen ZK L/K heißt **unverzweigt** genau dann, wenn $e(L/K) = 1$.

Bemerkung 2.6.2 (i) Sind l, k die Restklassenkörper von L, K, so gilt im unverzweigten Fall $[L : K] = [l : k]$.

(ii) Ist L/K endliche Erweiterung von Zahlkörpern, so sind nur endlich viele der lokalen Erweiterungen $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ verzweigt.

Fakt 2.6.3
$L/K/\mathbb{Q}_p$, L/K unverzweigt $\Leftrightarrow L = K(\zeta_n)$ mit ζ_n primitive n-te Einheitswurzel, $\mathrm{ggT}(p, n) = 1$.

Beweis:

(i) Sei L/K unverzweigt, dann ist $l = k(\theta)$, $\theta \in \overline{\mathbb{F}_p}$ primitive n-te Einheitswurzel mit $p \nmid n$. Sei $g = \mathrm{Irr}(X, \theta, k) \in k[X]$, $g \mid X^n - 1$. Nach HENSELs Lemma existiert eine Wurzel $\zeta \in \mathcal{O}_L$ von $X^n - 1$ mit $\zeta \equiv \theta \pmod{\mathfrak{m}_L}$. Dann ist ζ primitive n-te Einheitswurzel in L Sei $f = \mathrm{Irr}(X, \zeta, K) \in \mathcal{O}_K[X]$ (VIETAischer Wurzelsatz). Sei $\overline{f}$ die Reduktion von f (mod $\mathfrak{m}_K$), dann ist $\overline{f}(\theta) = 0$ (wg. $\zeta \mapsto \theta$). Also teilt g das Polynom $\overline{f}$ in $k[X]$. Nun ist $[K(\zeta) : K] = \deg f$, $[k(\theta) : k] = [l : k] = [L : K]$ (wegen Unverzweigtheit) $= \deg g$. Also $\deg f \leq \deg g$. Aber $g \mid \overline{f}$. Damit $\overline{f} = g$ und $L = K(\zeta)$.

(ii) Sei $L = K(\zeta_n)$ mit $zeta_n$ = primitive n-te Einheitswurzel, $p \nmid n$. Wir haben zu zeigen: L/K ist unverzweigt. Dann ist $l = \mathcal{O}_L/\mathfrak{m}_L$, $k = \mathcal{O}_K/\mathfrak{m}_K$. $l \supset k(\overline{\zeta}_n)$, $\overline{\zeta}_n$ = Bild von ζ_n in l (ζ_n ist ganz). Die Abbildung $\mu_n(L) \to \mu_n(l) : \zeta \mapsto \overline{\zeta} = \zeta \pmod{\mathfrak{m}_L}$ ist nach HENSELs Lemma Isomorphismus (Eindeutigkeit). Sei $f = \mathrm{Irr}(X, \zeta_n, K)$, $\overline{g} = \mathrm{Irr}(X, \overline{\zeta}_n, k)$. Dann gilt $\overline{g} \mid \overline{f}$.

Sei $\overline{f} = \overline{g} \cdot \overline{h}$ in $k[X]$, die Polynome $\overline{g}, \overline{h}$ sind teilerfremd, d.h. $X^n - 1 \in k[X]$ keine mehrfachen Nullstellen hat. Nach HENSELs Lemma-Variante folgt $f = gh$ mit $g \mapsto \overline{g}$, $h \mapsto \overline{h}$, $g, h \in \mathcal{O}_K[X]$. Aber f ist irreduzibel $\Rightarrow h = \overline{h} = 1$. Somit $[L : K] = \deg f = \deg \overline{g} = [k(\overline{\zeta}_n) : k] \leq [l : k] \leq [L : K] \overset{l:k}{\Longrightarrow} = [L : K] \Rightarrow L/K$ unverzweigt.

□

Ende VL 26
03.02.2015

Bemerkung 2.6.4 (Variante von HENSELs Lemma)
Sei K vollständig, bzgl. diskreter nichtarchimedischer Bewertung $|\cdot|$, $\mathcal{O}$ Bewertungsring, $\mathfrak{m}$ maximales Ideal, $k = \mathcal{O}/\mathfrak{m}$, $f \in \mathcal{O}[X]$ unitäres Polynom, $\overline{f} = \overline{g}\overline{h}$ in $k[X]$ mit $\overline{g}, \overline{h}$ teilerfremd. Dann existieren $g, h \in \mathcal{O}[X]$ unitär mit $g \mapsto \overline{g}$, $h \mapsto \overline{h}$ und $f = gh$.

Beweis: O.B.d.A. seien $\overline{g}, \overline{h}$ unitär. Seien $g_0, h_0 \in \mathcal{O}[X]$ Liftungen von $\overline{g}$, $\overline{h}$, unitär vom selben Grad. Also $f - g_0 h_0 \in \mathfrak{m}[X]$.

Ansatz:

$$g = g_0 + a_1\pi + a_2\pi^2 + \dots$$

$$h = h_0 + b_1\pi + b_2\pi^2 + \dots$$

mit $\mathfrak{m} = (\pi)$ und $a_j, b_j \in \mathcal{O}[X]$, sowie $\deg a_i < \deg \overline{g}$, $\deg b_i \leq \deg \overline{h}$. Beide Reihen konvergieren, g ist unitär wg. $\deg a_i < \deg \overline{g}$. Außerdem gilt $g \mapsto \overline{g}, h \mapsto \overline{h}$.

Sei $g_n = \sum_{i=0}^{n} a_i\pi^i$, $h_n = \sum_{i=0}^{n} b_i\pi^i$.

Induktionsanfang: $f \equiv g_0 h_0 \pmod{\pi}$

Seien a_i, b_i gefunden s.d. $f \equiv g_n h_n \pmod{\pi^{n+1}}$. Wir suchen Polynome $a_{n+1}, b_{n+1} \in \mathcal{O}[X]$, s.d. $g_{n+1} = g_n + a_{n+1}\pi^{n+1}$, $h_{n+1} = h_n + b_{n+1}\pi^{n+1}$.

$$\begin{aligned} f &\equiv g_{n+1}h_{n+1} \pmod{\pi^{n+2}} \\ &\equiv g_n h_n + (g_n b_{n+1} + a_{n+1}b_n)\pi^{n+1} \pmod{\pi^{n+2}} \end{aligned}$$

$f - g_n h_n \equiv 0 \pmod{\pi^{n+1}}$, also ist $f_{n+1} := \frac{f - g_n h_n}{\pi^{n+1}} \in \mathcal{O}[X]$ und wir haben zu sichern:

$$\overline{f}_{n+1} = \overline{g}\overline{b}_{n+1} + \overline{a}_{n+1}\overline{h} \in k[X]$$

Nach Voraussetzung ist $\mathrm{ggT}(\overline{g}, \overline{h}) = 1 \Rightarrow \exists \overline{c}, \overline{d} \in k[X]$ mit $1 = \overline{gc} + \overline{hd} \Rightarrow \overline{f}_{n+1} = \overline{gc}_1 + \overline{hd}_1 = \overline{g}(\overline{c}_1 + \overline{r}\overline{h}) + \overline{h}(\overline{d}_1 - \overline{r}\overline{g})$ für $\overline{r} \in k[X]$.

Also kann man erreichen, dass der Faktor bei $\overline{h}$ Grad $< \deg \overline{g}$ hat. □

Was hat das mit HENSELs Lemma zu tun? Sei $\overline{f} = (X - \overline{\lambda})\overline{h}(X)$, $\overline{\lambda} \in k \Rightarrow \overline{f}(\overline{\lambda}) = 0$. $\mathrm{ggT}(X - \overline{\lambda}, \overline{h}) = 1 \Rightarrow \overline{f}'(\overline{\lambda}) \neq 0 \Rightarrow |f(\lambda)| < 1, |f'(\lambda)| = 1$ (λ Liftung von $\overline{\lambda}$ nach $\mathcal{O}$).

Folgerung 2.6.5
Unverzweigte Erweiterungen sind normal.

Beweis: $K(\zeta_n) = K(\mu_n)$. □

Fakt 2.6.6 (i) M/L, L/K unverzweigt $\Rightarrow M/L$ unverzweigt

(ii) L/K, M/K unverzweigt (in $\overline{\mathbb{Q}}_p$) $\Rightarrow LM/K$ unverzweigt

(iii) L/K unverzweigt, E/K endlich (in $\overline{\mathbb{Q}}_p$) $\Rightarrow LE/E$ unverzweigt

Beweis:

(iii) $[L : L \cap E] = [LE : E]$

Analoges Bild für die Restklassenkörper $\Rightarrow f(le/e) = f(l/(l \cap e))$. Aus $e(L/K) = 1$ folgt $e(L/(L \cap E)) = 1$, somit $e(LE/E) = e(L/(L \cap E)) = 1$.

(i) folgt aus der Multiplikativität von E

(ii) folgt aus vorherigem Fakt: $L = K(\zeta_m)$, $M = K(\zeta_n), LM = K(\zeta_g)$, $g = \mathrm{kgV}(m, n)$ (prim zu p).

□

Folgerung 2.6.7
In jeder endlichen Erweiterung L/K gibt es maximale unverzweigte Erweiterungen $L/K^{nr}/K$ (nr - non ramified).

Folgerung 2.6.8
Die endlichen unverzweigten Erweiterungen in $\overline{K}/K$ sind in kanonischer Bijektion zu den endlichen Erweiterungen in $\overline{k}/k$.

Beweis: $\mathbb{F}_{q^n} = \mathbb{F}_q(\mu_{q^n-1})$, $K_n = K(\mu_{q^n-1})$. □

Fakt 2.6.9
Sei L/K endliche unverzweigte Erweiterung. Dann ist der kanonische Homomorphismus

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k)$$

ein Isomorphismus.

Beweis: Sei $\sigma : L \to L$ ein K-Automorphismus. $\sigma\mathcal{O}_L = \mathcal{O}_L$, $\sigma\mathfrak{m}_L = \mathfrak{m}_L$, wg. $|\sigma x| = |x|$. Also induziert σ einen k-Automorphismus von l. Das liefert den Homomorphismus

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k)$$

(Man muss sich die Existenz beider Gruppen klar machen, insbesondere die Separabilität von l/k (endl. Erweiterung endlicher Körper ist separabel).) Für geeignetes n prim zu p ($K \supset \mathbb{Q}_p$) ist $L = K(\zeta_n)$, $l = k(\overline{\zeta}_n)$. Die Abbildung $\mu_n(L) \to \mu_n(l)$ ist ein Isomorphismus. Ist also $\overline{\sigma} = Id$ auf $\mu_n(l)$, so auch $\sigma = Id$ auf $\mu_n(L)$. Also ist obiger Homomorphismus injektiv. Beide Gruppen haben dieselbe Ordnung $[L : K] = [l : k]$. □

§2.7 Zahm verzweigte Erweiterungen

Definition 2.7.1
Seien L/K lokale ZK (also endliche Erweiterungen von $\mathbb{Q}_p$)

(i) L/K heißt **vollverzweigt** $\Leftrightarrow f(L/K) = 1$

(ii) L/K heißt **zahm verzweigt** $\Leftrightarrow p \nmid e(L/K)$

(iii) L/K heißt **wild verzweigt** $\Leftrightarrow p \mid e(L/K)$

Fakt 2.7.2
Sei L/K vollverzweigt und zahm, $\mathfrak{m}_L = (\pi_L)$, dann ist π_L Wurzel eines EISENSTEIN-Polynoms vom Grad $e = e(L/K)$:

$$X^l + a_{l-1}X^{l-1} + \ldots + a_0$$

wobei alle $a_j \in \mathfrak{m}_K$ und $a_0 \notin \mathfrak{m}_K^2$. Es gilt $L = K(\pi_L)$. Umgekehrt erzeugt jede Wurzel eines solchen Polynoms eine vollverzweigte Erweiterung vom Grad e.

Beweis: Alle Konjugierten von π_L (= Wurzeln von $\mathrm{Irr}(X, \pi_L, K)$) haben diesselbe Bewertung in $\overline{\mathbb{Q}}_p$ (unter Automorphismen ändert sich die Bewertung nicht). Also sind die Koeffizienten von $\mathrm{Irr}(X, \pi_L, K)$ alle aus $\mathfrak{m}_K$. Der Absolutterm a_0 ist bis auf Vorzeichen das Produkt aller Konjugierter von π_L. Andererseits ist $\pi_K = u \cdot \pi_L^e$, π_L hat höchstens e Konjugierte, also $|a_0| = |\pi_L|^{e'}$, $a_0 = v \cdot \pi_K^r \Rightarrow |a_0| = |\pi_K|^r = |\pi_L|^{er} \Rightarrow e' = er$, $e' \leq e \Rightarrow r = 1$, $e' = e$. Also $a_0 \in \mathfrak{m} \setminus \mathfrak{m}_K^2$. Weiter folgt $[K(\pi_L) : K] = e \Rightarrow K(\pi_L) = L$.

Sei nun α Wurzel von f, dann ist $[K(\alpha) : K] = e$. Weiter gilt $|a_0| = |\alpha|^e \Rightarrow \alpha = \pi_L$ und die Erweiterung $K(\alpha)/K$ ist voll verzweigt. □

Ende VL 27
04.02.2015

Fakt 2.7.3
Sei L/K vollverzweigt und zahm, dann ex. $\pi_L \in \mathcal{O}_L$, $\pi_K \in \mathcal{O}_K$, s.d. π_L Wurzel eines Polynoms $X^e - \pi_K$ ist, $e = [L : K]$. Umgekehrt erzeugt jede Wurzel von $X^e - \pi_K$ mit $\mathrm{ggT}(e, p) = 1$ eine voll- und zahm verzweigte Erweiterung.

Beweis: Die 2. Aussage hatten wir gerade.

Sei $[L : K] = e = e(L/K)$, $\mathrm{ggT}(e, p) = 1$. Wähle $\pi_K \in \mathfrak{m}_K \setminus \mathfrak{m}_K^2$ und $\alpha \in \mathcal{O}_L$ mit $|\alpha|^e = |\pi_K|$, also $\mathfrak{m}_L = (\alpha)$, $\alpha = \pi_L$. Dann ist $L = K(\alpha)$, siehe oben. Wir wollen π_K abändern zu π'_K, s.d. eine Wurzel von $X^e - \pi'_K$ den Körper L über K erzeugt.

Es gilt $\alpha^e = \pi_K \cdot u$, $u \in \mathcal{O}_L^\times$. Wegen $l = k$ ($l = \mathcal{O}_L/Fm_L$, $k = \mathcal{O}_K/\mathfrak{m}_K$) gilt $u \equiv u_0 \pmod{\mathfrak{m}_L}$, $u_0 \in \mathcal{O}_K^\times$. Setze $\pi = u_0 \cdot \pi_K$, dann ist $|\pi| = |\pi_K|$. Sei $f(X) = X^e - \pi$ und $\alpha_1, \ldots, \alpha_e$ die Wurzeln von f. Sie sind verschieden, denn $f'(X) = eX^{e-1}$. Es gilt

$$|f(\alpha)| = \prod_{j=1}^{e} |\alpha - \alpha_j|,$$

sowie $|\alpha_j|^e = |\pi|$, also $|\alpha_j| = |\alpha| = |\pi_L| < 1$ für alle j. Andererseits ist

$$\alpha^e = u \cdot \pi_K = (u_0 + x)\pi_K$$

$x \in \mathfrak{m}_L = \pi + \pi y$, $y = xu_0^{-1} \in \mathfrak{m}_L$. Somit $|\alpha^e - \pi| = |\pi y| < |\pi|$, also $|f(\alpha)| < |\pi| \Rightarrow \prod_{j=1}^{e} |\alpha - \alpha_j| < |\pi| = |\pi_L|^e$. Weiter gilt $|\alpha - \alpha_j| \leq |\pi_L|$, wegen $\alpha, \alpha_j \in \mathfrak{m}_L$. Es ex. also ein j, s.d. $|\alpha - \alpha_j| < |\pi_L| = |\alpha_j|$. Nun gilt $|f'(\alpha_j)| = \prod_{i \neq j} |\alpha_i - \alpha_j| = |\alpha_j|^{e-1}$ und $|\alpha_i - \alpha_j| \leq |\alpha_j| = |\alpha|$, also $|\alpha_i - \alpha_j| = |\alpha_j|$.

Somit $|\alpha - \alpha_j| < |\alpha_i - \alpha_j|$ für alle $i \neq j$. Nach KRASNERs Lemma folgt $K(\alpha_j) \subset K(\alpha)$. Wegen $[K(\alpha_j) : K] = [K(\alpha) : K] = e$ folgt $K(\alpha_j) = K(\alpha)$. □

Fakt 2.7.4 (i) E/L, L/K zahm verzweigt $\Rightarrow E/K$ zahm verzweigt.

(ii) L/K zahm verzweigt, E/K endlich (in $\overline{\mathbb{Q}}_p$) $\Rightarrow EL/E$ zahm verzweigt.

(iii) E/K, F/K zahm verzweigt $\Rightarrow EF/K$ zahm verzweigt.

Beweis:

(i) klar

(ii) L/K zahm verzweigt $\Rightarrow \exists$ F/K, s.d. F/K unverzweigt, L/F voll- und zahm verzweigt. Also $L = F(\alpha)$, $\alpha^e = \pi_F$, $e = e(L/K)$ prim zu p. Dann ist $LE = E(\alpha)$ und α Wurzel eines Polynoms $X^e - \pi_F$, $p \nmid e$. Wir zeigen, dass solche Erweiterungen stets zahm verzweigt sind. Der Zerfällungskörper eines solchen Polynoms ist zweistufig metabelsch (Gruppe selbst und Faktorgruppe abelsch): 1. Schritt: Adjunktion mit der e-ten Einheitswurzel (hat abelsche GALOIS-Gruppe), 2. Schritt: Hat Grad, der e teilt: Gal(2. Schritt) $\hookrightarrow \mu_e$.

(iii) folgt formal aus (i) und (ii)

□

Folgerung 2.7.5
Jede endliche Erweiterung von lokalen ZK L/K zerlegt sich kanonisch in 3 Teile:

$$L/K^t/K^{nr}/K$$

mit

- K^{nr}/K maximal unverzweigt
- K^t/K^{nr} zahm und vollverzweigt
- L/K^t wild und vollverzweigt (Grad $= p^n$)

Beweis: K^t=Kompositum aller zahm verzweigten Erweiterungen in L/K. □

Lemma 2.7.6
Sei L/K Galerw. lokaler ZK, $\sigma \in \mathrm{Gal}(L/K)$, E Zwischenkörper, Dann gilt

$$e(\sigma E/K) = e(E/K),$$

$$f(\sigma E/K) = f(E/K).$$

Beweis: Sei $\mathfrak{m}_E = (\pi_E)$, dann ist $(\sigma\pi_E) = \sigma\mathfrak{m}_E$. $\pi_E^{e(E/K)} = u\pi_E \Rightarrow (\sigma\pi_E)^{e(E/K)} = v\pi_K$, $u, v \in \mathcal{O}_E^\times$. Es folgt $e(E/K) = e(\sigma E/K)$. Die Formel für f folgt aus $e \cdot f = [E : K]$ und $[\sigma E : K] = [E : K]$. □

Folgerung 2.7.7
Ist L/K Galoiserweiterung, so auch K^t/K.

§2.8 Galoistheorie der lokalen ZK

Sei L/K Galoiserweiterung lokaler ZK, dann lässt $G = \mathrm{Gal}(L/K)$ den Ring $\mathcal{O}_L$ invariant, wie auch das maximale Ideal $\mathfrak{m}_L$. Also induziert jedes $\sigma \in G$ einen Automorphismus von l/k, $l = \mathcal{O}_L/\mathfrak{m}_L$. Also haben wir einen HM $\mathrm{Gal}(L/K) \to \mathrm{Gal}(l/k)$.

Sei $M/K = K^{nr}/K$. Sie ist normal und der HM $\mathrm{Gal}(M/K) \to \mathrm{Gal}(m, k)$ ist Iso. Es gilt $l = m$.

Definition 2.8.1
Der Kern dieses Homomorphismus heißt **Trägheitsgruppe** (inertia group). Das ist die Galoisgruppe des vollverzweigten Schritts.

Fakt 2.8.2
Sei L/K wie oben, K^t/K die max. zahmverzweigte Erweiterung in L/K. Der Kern des HM $\mathrm{Gal}(L/K) \to \mathrm{Gal}(K^t/K)$ heißt **1. Verzweigungsgruppe**. Dies ist eine p-Gruppe. Also ist die $Gal(L/K)$ auflösbar.

Ende VL 28
10.02.2015

Beispiel 2.8.3 (d'apr´es WEIL, A. Exercise dyadiques Inv. Math. 27 (1974), 1-22)
Wir konstruieren eine S_4-Erweiterung von $\mathbb{Q}_2$.

1) Sei E der ZFK des Polynoms $X^3 - 2$. Es ist irreduzibel über $\mathbb{Q}_2$, die 3 Wurzeln sind $\pi, \zeta\pi, \zeta^2\pi$ mit π primitive 3. Einheitswurzel, $\pi^3 = 2$. Also ist $E = \mathbb{Q}_2(\zeta, \pi)$. $[\mathbb{Q}_2(\pi) : \mathbb{Q}_2] = 3$, voll verzweigt. $[\mathbb{Q}_2(\zeta) : \mathbb{Q}_2] = 2$, unverzweigt (2 prim zu 3). Also hat $E/\mathbb{Q}_2$ die Galois-Gruppe S_3, $e(E/\mathbb{Q}_2) = 3$, $f(E/\mathbb{Q}_2) = 2$.

   Die Trägeheitsgruppe ist A_3, max. unverzweigte Erweiterung ist $\mathbb{Q}_2(\zeta)/\mathbb{Q}_2$. $V = \{\mathrm{Id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ S_4, V ist Normalteiler und $S_4/V = S_3$. Wir suchen also zwei geeignete quadratische Erweiterungen von E.

2) Seinen $\alpha = \pi - 1$, $\beta = \zeta\pi - 1$, $\gamma = \zeta^2\pi - 1$. Das sind Einheiten in E, sie sind konjugiert unter der Galoisgruppe. Es gilt $\alpha\beta\gamma = (\pi-1)(\pi-\zeta)(\pi-\zeta^2) = \pi^3 - 1 = 1$. Keine der drei Zahlen α, β, γ ist Quadrat in E: Sei $u = \zeta(1+\pi x)$, $u^2 = \zeta^2(1 + 2\pi x + \pi^2 x^2)$, also $u^2 \equiv \zeta^2 \pmod{\pi^2}$. Aber $\alpha = \pi - 1 \equiv \pi + 1 \pmod{\pi^2}$, also ist $\alpha \neq u^2$. Damit sind β, γ keine Quadrate. Wegen $\alpha\beta\gamma = 1$ folgt α/β, β/γ, γ/α sind auch keine Quadrate: $\alpha/\beta = v^2 \Rightarrow \gamma = \frac{1}{\alpha\beta} = \frac{1}{(\beta v)^2}$ ↯. Somit ist $K = E(\sqrt{\alpha}, \sqrt{\beta}, \sqrt{gamma})/E$ von jeweils 2 der 3 Wurzeln erzeugt und ist Galoiserweiterung mit Galoisgruppe $V = C_2 \times C_2$ (diese hat 3 2-elementige Untergruppen). Die quadratischen Zwischenkörper sind also $E(\sqrt{\alpha})$, $E(\sqrt{\beta})$, $E(\sqrt{\gamma})$ (nach Galoistheorie).

Wir zeigen, dass $K/\mathbb{Q}_2$ normal ist. Betrachte

$$\begin{aligned} f(X) &= (X^2 - \alpha)(X^2 - \beta)(X^2 - \gamma) \\ &= X^6 - (\alpha\beta\gamma)X^4 + (\alpha\beta + \alpha\gamma + \beta\gamma)X^2 - 1 \end{aligned}$$

$$\begin{aligned} \alpha + \beta + \gamma &= (1 + \zeta + \zeta^2)\pi - 3 = -3 \\ \alpha\beta + \alpha\gamma + \beta\gamma &= \ldots = 3 \end{aligned}$$

Also $f(X) = X^6 + 3X^4 + 3X^2 - 1$. K enthält alle 6 Wurzeln $\pm\sqrt{\alpha}$, $\pm\sqrt{\beta}$, $\pm\sqrt{\gamma}$ von f, also den ZFK von f über $\mathbb{Q}_2$. Andererseits liegen im ZFK von f die Zahlen $\sqrt{\alpha}$, $\sqrt{\beta}$, $\sqrt{\gamma}$, also auch $\pi = 1 - (\sqrt{\alpha})^2$, $\zeta\pi$, $\zeta^2\pi$, also auch ζ.

D.h. K ist der ZFK von f über $\mathbb{Q}_2$, also normal. Die Galoisgruppe $G = \mathrm{Gal}(K/\mathbb{Q}_2)$ hat 24 Elemente, besitzt Normalteiler V, die Faktorgruppe ist S_3. Also Gruppenerweiterung

$$1 \to V \to G \to S_3 \to 1.$$

Das wird klassifiziert durch $H^2(S_3, V)$ (Homologie).

Seien $\sigma, \tau \in \mathrm{Gal}(E/\mathbb{Q}_2)$, s.d.

$$\begin{aligned} \sigma &: \pi \mapsto \zeta\pi, \zeta \mapsto \zeta \\ \tau &: \pi \mapsto \pi, \zeta \mapsto \zeta^2 \end{aligned}$$

Diese erzeugen $\mathrm{Gal}(E/\mathbb{Q}_2)$. Ist $\rho \in \mathrm{Gal}(E/\mathbb{Q}_2)$, so besitzt ρ genau 4 Liftungen nach $G = \mathrm{Gal}(K/\mathbb{Q}_2)$. Solch ein ρ permutiert α, β, γ die Liftungen sehen so auch:

$$\begin{aligned} \tilde{\rho} : \sqrt{\alpha} &\mapsto \pm\sqrt{\rho\alpha} \\ \sqrt{\beta} &\mapsto \pm\sqrt{\rho\beta} \\ \sqrt{\gamma} &\mapsto \pm\sqrt{\rho\gamma} \end{aligned}$$

Wir wählen links die Wurzeln so auch, dass $\sqrt{\alpha}\sqrt{\beta}\sqrt{\gamma} = 1$ gilt. Dann treten rechts nur 4 der 8 Vorzeichen-Kombinationen auf.

Betrachte $\theta = \sqrt{\alpha} + \sqrt{\beta} + \sqrt{\gamma} \in K$. θ besitzt unter $G = \mathrm{Gal}(K/\mathbb{Q}_2)$ genau 4 Konjugierte.

$$\begin{aligned} \theta_1 &= \theta = \sqrt{\alpha} + \sqrt{\beta} + \sqrt{\gamma}, \\ \theta_2 &= \sqrt{\alpha} - \sqrt{\beta} - \sqrt{\gamma}, \\ \theta_3 &= -\sqrt{\alpha} + \sqrt{\beta} - \sqrt{\gamma}, \\ \theta_4 &= -\sqrt{\alpha} - \sqrt{\beta} + \sqrt{\gamma}. \end{aligned}$$

Also ist θ Nullstelle eines Polynoms vom Grad 4 über $\mathbb{Q}_2$: $g(X) = (X - \theta_1)(X - \theta_2)(X - \theta_3)(X - \theta_4)$. Wir berechnen $g(X)$:

i) $\theta_1 + \theta_2 + \theta_3 + \theta_4 = 0$

ii) $\theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4 = 6$ (knallhart ausrechnen)

iii) Koeffizient bei X^1: 8 (rechnen)

iv) $\theta_1\theta_2\theta_3\theta_4 = -3$ (rechnen)

Somit gilt $g(X) = X^4 + 6X^2 - 8X - 3$. Sei $L \subset K$ der ZFK von $g(X)$. Aus $\theta_1 + \theta_4 = 2\sqrt{\gamma}$, $\theta_1 + \theta_2 = 2\sqrt{\alpha}$, $\theta_1 + \theta_3 = 2\sqrt{\beta}$ folgt $K \subset L$, mithin $L = K$. Es folgt $\mathrm{Gal}(K/\mathbb{Q}_2) = S_4$.

3) Wir zeigen K/E ist voll verzweigt. K/E besitzt 3 quadratische Zwischenkörper: $E(\sqrt{\alpha})$, $E(\sqrt{\beta})$, $E(\sqrt{\gamma})$. Sie sind konjugiert unter $\mathrm{Gal}(K/E)$, also gleichzeitig verzweigt oder unverzweigt. E besitzt genau eine unverzweigte quadratische Erweiterung, also sind alle drei verzweigt. Es folgt $e(K/E) = 4$, $f(K/E) = 1$ und $e(K/\mathbb{Q}_2) = 12$ und $f(K/\mathbb{Q}_2) = 2$.

Maximale unverzweigte Erweiterung ist $\mathbb{Q}_2(\zeta)$, maximale zahmverzweigte ist $E/\mathbb{Q}_2$, Trägheitsgruppe ist A_4, erste Verzweigungsgruppe ist V = KLEINsche Vierergruppe.

Ende VL 29
11.02.2015

§3 Aufgaben mit Lösungsvorschlägen

Aufgabe 1) Sei A kommutativer Ring mit 1. Ein A-Modul M heißt **NOETHERsch** genau dann, wenn eine der folgenden Bedingungen gilt:

i) Jeder Teilmodul ist endlich erzeugt.

ii) Jede strikt aufsteigende Folge von Teilmoduln $M_1 \subsetneq M_2 \subsetneq \dots$ ist endlich.

iii) Jede nichtleere Menge von Teilmoduln besitzt maximale Elemente.

Zeigen Sie die Äquivalenz der 3 Bedingungen.

Lösung:

(i) $\Rightarrow$ (ii) Sei $M_1 \subset M_2 \subset \dots$ eine aufsteigende Folge von Teilmoduln von M. Dann ist auch $\tilde{M} := \bigcup_i M_i$ Teilmodul von M. Nach (i) ist $\tilde{M}$ endlich erzeugt. $\Rightarrow \tilde{M} = \langle a_1, \dots, a_n \rangle$ $\Rightarrow$es existiert ein k mit $a_1, \dots, a_n \in M_k$, womit sich die Ausgangsfolge ab k stabilisiert.

(ii) $\Rightarrow$ (iii) Sei F eine nichtleere Familie von Teilmoduln von M und $K \subset F$ eine Kette (d.h. total geordnete Teilmenge) bezüglich Inklusion. Nach (ii) ist K endlich und besitzt somit ein maximales Element. Da K beliebig, besitzt F ein maximales Element nach ZORNs Lemma.

(iii) $\Rightarrow$ (i) Sei F die Familie aller endlich erzeugten Teilmoduln von M. Dann besitzt sie nach (iii) ein maximales Element N. Ist $N \neq M$, gibt es $a \in M \setminus N$ und $\tilde{N} := \langle N, a \rangle$ ist endlich erzeugt mit $N \subsetneq \tilde{N}$ im Widerspruch zur maximalität von N.

Aufgabe 2) Zeigen Sie: Jeder Teilmodul und jeder Faktormodul eines NOETHERschen Moduls ist auch NOETHERsch.

Lösung: Teilmoduln sind NOETHERsch: Sei N Teilmodul von M und L Teilmodul von N. Wegen Eigeschaft (i) und $L \subset N \subset M$ Teilmodul, ist L endlich erzeugt.

Faktormoduln sind NOETHERsch: Sei nun $\overline{L} \subset M/N$ Teilmodul und L Urbild in M. Dann ist L Teilmodul von M und somit endlich erzeugt. Die Bilder der Erzeuger von L erzeugen $\overline{L}$.

Aufgabe 3) Zeigen Sie: Ist $N \subset M$ Teilmodul und sind N und M/N NOETHERsch, so auch M.

Lösung: Sei L Teilmodul von M. $L \cap N \subset N$ ist Teilmodul, $\overline{L} := (L+N)/N \cong L/(L \cap N)$ (Isomorphiesatz). Dies liefert die kurze exakte Folge

$$0 \xrightarrow{d_1} L \cap N \xrightarrow{d_2} L \xrightarrow{d_3} \overline{L} \xrightarrow{d_4} 0,$$

also $\ker d_{i+1} = \operatorname{img} d_i$. $\Rightarrow d_2$ injektiv, d_3 surjektiv, wobei $L \cap N$, $\overline{L}$ nach Voraussetzung NOETHERsch sind.

Wir zeigen, dass für jede kurze exakte Folge $0 \to N' \xrightarrow{\varphi} N'' \xrightarrow{\psi} N''' \to 0$ aus N', N''' NOETHERsch auch N'' NOETHERsch folgt: Es ist $N' = Aa_1 + \dots Aa_s$ und $N''' = Ab_1 + \dots + Ab_t$. Seien $\overline{a_1}, \dots, \overline{a_s}$ und $\overline{b_1}, \dots, \overline{b_t}$ Bilder bzw. Urbilder unter φ bzw. ψ ($\overline{b_i}$ ggf. nicht eindeutig) und sei $x \in N''$. Dann ist $\psi(x) = \sum \lambda_i b_i$, also ist $x - \sum \lambda_i \overline{b_i} \in \ker \psi = \operatorname{img} \phi = \langle \overline{a_1}, \dots, \overline{a_s} \rangle$.

Aufgabe 4) Zeigen Sie: Ist A ein NOETHERscher A-Modul, so auch jeder endlich erzeugte A-Modul.

Lösung: Zunächst eine Hilfsaussage:

Lemma
Ist A NOETHERscher Ring, so ist auch A^n NOETHERscher A-Modul.

Beweis: Induktionsanfang: A^1 NOETHERsch. Induktionsschritt: $0 \to A \to A^{n+1} \to A^n \to 0$ ist kurze exakte Folge. □ Jeder endlich

erzeugte A-Modul M ist gegeben durch den Homomorphismus $A^n \xrightarrow{\varphi} M$ (span der Erzeuger). Also $M \cong A^n / \ker \varphi$ NOETHERsch nach Aufgabe 2.

Aufgabe 5) Beweisen Sie HILBERTs Basissatz: Mit A ist auch $A[X]$ NOETHERsch.

Lösung: Sei I ein Ideal in $A[X]$. Wir zeigen, dass I endlich erzeugt ist. Definiere $I_i := \{a_i : \exists f \in I : f(X) = a_i X^i + \ldots + a_1 X + a_0\}$ Leitkoeffizienten. Dies sind Ideale in A und es gilt $I_0 \subset I_1 \subset \ldots$ (z.B. durch Multiplikation mit X). Da A NOETHERsch ist, stabilisiert sich die Folge für ein $r \in \mathbb{N}$. Seien $a_{i1}, a_{i2}, \ldots, a_{in_i}$ Erzeuger von I_i für $0 \leq i \leq r$ und f_{ij} die zugehörigen Polynome aus I ($0 \leq i \leq r$, $1 \leq j \leq n_i$). Behauptung: $I = \langle f_{ij} \rangle$.

Betrachte $p \in I$ mit Grad d.

i) Fall $d > r$: Leitkoeffizient c von p in $I_d = I_r$. Also $c = \sum \lambda_j a_{rj}$ und somit können wir den Grad reduzieren. $\tilde{p} := p - \sum \lambda_j f_{rj} X^{d-r}$, also o.B.d.A. $d \leq r$.

ii) Fall $d \leq r$: Analog zu Fall 1 können wir den Grad reduzieren: $\tilde{p} := p - \sum \lambda_j f_{dj}$.

Induktiv folgt $\tilde{p} = 0$ und wir brauchen nur endlich viele Erzeuger.

Beispiel
Nicht-NOETHERsche Ringe:

i) Polynomring mit unendlich vielen Variablen $R[X_1, X_2, X_3, \ldots]$.

ii) $C(\mathbb{R})$ stetige Funktionen auf $\mathbb{R}$ mit punktweiser Addition und Multiplikation. Betrachte das Ideal $I_n = \{f \in C(\mathbb{R}) : \operatorname{supp} f \subset [-n, n]\}$.

Aufgabe 6) Bestimmen Sie die Einheiten in $\mathbb{Z}[\sqrt{2}]$

Lösung: Sei $a \in \mathbb{Z}[\sqrt{2}]^\times$. Also $ab = 1$ und $1 = \mathrm{N}(ab) = \mathrm{N}(a)\,\mathrm{N}(b)$. Mit $a = x + y\sqrt{2}$ führt dies zur PELLschen Gleichung $N(x + y\sqrt{2}) = x^2 - 2y^2 = \pm 1$. Diese hat Startlösung $\varepsilon = x_0 + \sqrt{2} y_0$ und jede weitere Lösung ergibt sich als $\pm\varepsilon^n$ mit $n \in \mathbb{Z}$:

Es ist $\varepsilon := 1 + \sqrt{2}$ Einheit, da $(1 + \sqrt{2})(1 - \sqrt{2}) = -1 \in \mathbb{Z}^\times$. Sei $\eta \neq \pm 1$ beliebige weitere Einheit. Ohne Einschränkung können wir $\eta > 1$ annehmen (sonst wählen wir $\pm\eta$ oder $\pm\frac{1}{\eta}$). Dann existiert ein $n \in \mathbb{N}$ mit $1 < \eta\varepsilon^{-n} \leq 1 + \sqrt{2}$. Sei $\eta\varepsilon^{-n} = \alpha + \sqrt{2}\beta$. Das ist also eine Einheit mit

$$1 < \alpha + \sqrt{2}\beta \leq 1 + \sqrt{2}. \tag{1}$$

Dann ist $\mathrm{N}(\alpha + \sqrt{2}\beta) = \alpha^2 - 2\beta^2 = \pm 1$. Damit ist $\alpha - \sqrt{2}\beta = \pm\frac{1}{\alpha + \sqrt{2}\beta}$. Wir wissen $\frac{1}{1+\sqrt{2}} \leq \frac{1}{a+\sqrt{2}b} < 1$.

i) Fall $\alpha - \sqrt{2}\beta = \frac{1}{\alpha+\sqrt{\beta}}$:

$$\frac{1}{1+\sqrt{2}} \leq \alpha - \sqrt{2}\beta < 1 \tag{2}$$

Addition von (1) und (2) liefert:

$$\underbrace{1 + \frac{1}{1+\sqrt{2}}}_{\in]0,2]} \leq 2\alpha < \underbrace{1+1+\sqrt{2}}_{\in [3,4]}$$

$\Rightarrow \alpha = 1 \Rightarrow \beta = 1$

ii) Fall $\alpha - \sqrt{2}\beta = -\frac{1}{\alpha+\sqrt{2}\beta}$

$$\frac{1}{1+\sqrt{2}} \leq \sqrt{2}\beta - \alpha < 1 \tag{3}$$

Analog folgt $\beta = 1$ und $\alpha = 1$.

Somit ist $\eta = \varepsilon^n(1+\sqrt{2}) = \varepsilon^{n+1}$ und die Einheiten sind genau alle $\pm\varepsilon^n$, $n \in \mathbb{Z}$ (wg. o.B.d.A.).

Aufgabe 7) Berechnen Sie die Galoisgruppe von $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}$, wobei $p_1, \ldots, p_n$ paarweise verschiedene Primzahlen sind.

Lösung: Wir haben den Turm

$$\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})/\ldots/\mathbb{Q}.$$

Das sind alles Erweiterungen des Grades max. 2. Somit ist die gesuchte Galoisgruppe 2-elementar-abelsch (d.h. C_2^k), weil jede Erweiterung abelsch von Grad 2 oder trivial ist. Es genügt zu zeigen, dass es 2^n verschiedene Zwischenkörper gibt. Dann ist $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) \cong C_2^n$.

Wir betrachten $\mathbb{Q}(\sqrt{p_{i_1} \cdot \ldots \cdot p_{i_r}}) = \mathbb{Q}(\sqrt{p_{j_1} \cdot \ldots \cdot p_{j_s}})$ mit $1 \leq i_1 < \ldots < i_r \leq n$, $1 \leq j_1 < \ldots < j_s \leq n$, welche klarer Weise innerhalb des Turms liegen. Dann ist

$$\begin{aligned}
&\sqrt{p_{i_1} \cdot \ldots \cdot p_{i_r}} = a + b\sqrt{p_{j_1} \cdot \ldots \cdot p_{j_s}} && a, b \in \mathbb{Q} \\
&\Rightarrow p_{i_1} \cdot \ldots \cdot p_{i_r} = a^2 + b^2 \cdot p_{j_1} \cdot \ldots \cdot p_{j_s} + 2ab\sqrt{p_{j_1} \cdot \ldots \cdot p_{j_s}} \\
&\Rightarrow ab = 0 && \text{da } \sqrt{p_{j_1} \cdot \ldots \cdot p_{j_s}} \text{ irrational} \\
&\Rightarrow a = 0 && \text{da } \sqrt{p_{i_1} \cdot \ldots \cdot p_{i_r}} \text{ irrational} \\
&\Rightarrow p_{i_1} \cdot \ldots \cdot p_{i_r} = b^2 \cdot p_{j_1} \cdot \ldots \cdot p_{j_s} \\
&\Rightarrow d^2 \cdot p_{i_1} \cdot \ldots \cdot p_{i_r} = c^2 \cdot p_{j_1} \cdot \ldots \cdot p_{j_s} && \text{mit } b = \frac{c}{d}, \mathrm{ggT}(c,d) = 1
\end{aligned}$$

Vergleich der Primfaktorzerlegung liefert $\{i_1, \ldots, i_r\} = \{j_1, \ldots, j_s\}$. Somit haben wir 2^n verschiedene Zwischenkörper gefunden und außerdem

$$\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1 \cdot \ldots \cdot p_n}).$$

Aufgabe 8) Sei $p > 2$ prim. Zeigen Sie, dass $2\sin\frac{2\pi}{p}$ ganz über $\mathbb{Z}$ ist, aber $\sin 2\pi p$ nicht.

Lösung: Wir betrachten $\zeta_p := e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Dies ist ganz als Nullstelle von $X^p - 1$, ebenso ζ_p^{-1}. Es gilt

$$\zeta_p - \zeta_p^{-1} = 2i\,\mathrm{Im}\,\zeta_p = 2i\sin\frac{2\pi}{p},$$

also ist $2\sin\frac{2\pi}{p}$ ganz. Weiter ist

$$\begin{aligned}
\mathrm{N}(\zeta_p - \zeta_p^{-1}) &= \underbrace{\mathrm{N}(\zeta_p^{-1})}_{=1}\,\mathrm{N}(\zeta_p^2 - 1) \\
&= \mathrm{N}(1 - \zeta_p^2) \\
&= \mathrm{N}(1 - \zeta_p) \qquad \zeta_p, \zeta_p^2 \text{ beide prim. } p\text{-te Einheitsw., da } \mathrm{ggT}(p,2) = 1 \\
&= \prod_{i=1}^{p-1}(1 - \zeta_p^i).
\end{aligned}$$

Dabei ist $1 - \zeta_p^i$ für $1 \le i \le p-1$ Nullstelle des Polynoms $1 + (1-Y) + (1-Y)^2 + \ldots + (1-Y)^{p-1}$ und das Produkt somit gleich dem Absolutglied. $\Rightarrow \mathrm{N}(\zeta_p - \zeta_p^{-1}) = p$, also $\mathrm{N}(\sin\frac{2\pi}{p}) = \frac{p}{2^{p-1}} \notin \mathbb{Z}$, also $\sin\frac{2\pi}{p}$ nicht ganz.

Aufgabe 9) Es sei e die EULERsche Zahl und $K = \mathbb{Q}(e)$. Bestimmen Sie den ganzen Abschluss von $\mathbb{Z}$ in K (verwenden Sie die Transzendenz von e).

Lösung: Sei $\alpha \in \mathbb{Q}(e)$ ganz, also $\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_0 = 0$ für gewisse $c_i \in \mathbb{Z}$. Weiter ist $\alpha = \frac{p(e)}{q(e)}$ für gewisse $p, q \in \mathbb{Q}[X]$, $\mathrm{ggT}(p,q) = 1$. Es ist also

$$0 = p(e)^n + c_{n-1}p(e)^{n-1}q(e) + \ldots + c_0 q(e)^n.$$

Somit ist $f(X) = p(X)^n + c_{n-1}p(X)^{n-1}q(X) + \ldots + c_0 q(X)^n$ Polynom in $\mathbb{Q}[X]$ mit Nullstelle e. Wegen e transzendent, ist $f = 0$. Nun teilt p die ersten n Summanden von f, also auch den letzten. Wegen $\mathrm{ggT}(p,q) = 1$ folgt $p \mid c_0$, also p konstant. Analog ist q konstant und somit $\alpha \in \mathbb{Q}$, also $\alpha \in \mathbb{Z}$.

Aufgabe 10) Ist $a = \frac{3+2\sqrt{6}}{1-\sqrt{6}}$ eine ganze algebraische Zahl?

Lösung: $a = \frac{(1+\sqrt{6})(3+2\sqrt{6})}{1-6} = -3-\sqrt{6} \Rightarrow a^2 = 15+6\sqrt{6} = -6a-3 \Rightarrow a^2+6a+3 = 0$ folge a ganz.

Aufgabe 11) Es seien $a, b \in \mathbb{Z}$ und $\alpha \in \mathbb{C}$ eine Nullstelle von $f(X) = X^3 + aX + b$. Weiter sei $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Berechnen Sie die Diskriminante von $1, \alpha, \alpha^2$.

Lösung: Wegen $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, ist f Minimalpolynom von α über $\mathbb{Q}$. Nach Definition ist die Diskriminante $d(\omega_1, \ldots, \omega_n) = \det(\mathrm{Tr}(\omega_i\omega_j))$. Weiter haben wir $\sigma_i \in$

$\mathrm{Gal}(\mathbb{Q}(\alpha):\mathbb{Q})$.

$$\begin{aligned}
\mathrm{Tr}(1) &= \sum \sigma_i 1 = 3\\
\mathrm{Tr}(\alpha) &= \sum \sigma_i \alpha \overset{\text{Vieta}}{=} -\text{Koeffizient von } X^2 \text{ im Minimal-Polynom}\\
&= 0\\
\mathrm{Tr}(\alpha^2) &= \sum \sigma_i \alpha^2 = \Big(\sum \sigma_i \alpha\Big)^2 - \sum_{i\neq j} \sigma_i\alpha\sigma_j\alpha\\
&= -\sum_{i<j} \sigma_i\alpha\sigma_j\alpha \overset{\text{Vieta}}{=} -2a\\
\mathrm{Tr}(\alpha^3) &= \mathrm{Tr}(-a\alpha - b) = -a\,\mathrm{Tr}(\alpha) - b\,\mathrm{Tr}(1) = -3b\\
\mathrm{Tr}(\alpha^4) &= \mathrm{Tr}(\alpha(-a\alpha - b)) = -a\,\mathrm{Tr}(\alpha^2) - b\,\mathrm{Tr}(\alpha) = 2a^2
\end{aligned}$$

Nun können wir die Determinante ausrechnen:

$$d(1,\alpha,\alpha^2) = \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2)\\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3)\\ \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha^3) & \mathrm{Tr}(\alpha^4)\end{vmatrix} = \begin{vmatrix} 3 & 0 & -2a\\ 0 & -2a & -3b\\ -2a & -3b & 2a^2\end{vmatrix} = -4a^3 - 27b^2.$$

Aufgabe 12) Sei $K = \mathbb{Q}(\alpha)$ mit $\alpha^3 - \alpha - 1 = 0$. Bestimmen Sie eine Ganzheitsbasis von $\mathcal{O}_K$.

Lösung: Jede Nullstelle von $f(X) = X^3 - X - 1$ aus $\mathbb{Q}$ liegt in $\mathbb{Z}$ und teilt das Absolutglied 1. Weder 1, noch -1 ist Nullstelle, also f irreduzibel. Mit der vorherigen Aufgabe folgt $d(1,\alpha,\alpha^2) = -4(-1)^3 - 27(-1)^2 = -23$.

Sei d_K die Diskriminante von K. Dann ist $-23 = m^2 d_K$ für ein $m \in \mathbb{Z}$. $\Rightarrow m^2 = 1$, da 23 als Primzahl quadratfrei ist. $\Rightarrow 1, \alpha, \alpha^2$ ist Ganzheitsbasis.

Aufgabe 13) Es sei $[K:\mathbb{Q}] = n$ und $M = \{\alpha \in K : \mathrm{Tr}(\alpha\mathcal{O}_K) \subset \mathbb{Z}\}$. Zeigen Sie, dass M ein freier $\mathbb{Z}$-Modul vom Rang n ist.

Lösung: Wir wissen $\mathcal{O}_K$ ist freier $\mathbb{Z}$-Modul vom Rang n. Idee: M ungefähr dual zu $\mathcal{O}_K$.

Sei $\alpha_1, \ldots, \alpha_n$ Ganzheitsbasis von $\mathcal{O}_K$. Es ist $\mathrm{Tr}(\alpha\mathcal{O}_K) \subset \mathbb{Z} \Leftrightarrow \forall i : \mathrm{Tr}(\alpha\alpha_i) \in \mathbb{Z}$. Sicher ist $\mathcal{O}_K \subset M$. Betrachte K als $\mathbb{Q}$-VR. Dann ist $\mathrm{Tr} : K^2 \to \mathbb{Q}$, $(x,y) \mapsto \mathrm{Tr}(xy)$ eine Bilinearform. Außerdem ist diese nicht ausgeartet (Beweis mittels Satz vom primitiven Element + Vandermondedeterminante). Weiter ist $\alpha_1, \ldots, \alpha_n$ auch $\mathbb{Q}$-Basis von K. Somit gibt es duale Basis $\chi_1, \ldots, \chi_n$, d.h. $\mathrm{Tr}(\chi_i\alpha_j) = \delta_{ij}$. Nun stellen wir α als $\sum \mu_i\chi_i$ mit $\mu_i \in \mathbb{Q}$ dar. Dann ist $\mathrm{Tr}(\alpha\alpha_j) = \mathrm{Tr}(\sum \mu_i\chi_i\alpha_j) = \sum \mu_i\delta_{ij} = \mu_j$, womit die Bedingung aus der Aufgabenstellung $\alpha \in M \Leftrightarrow \forall j : \mu_j \in \mathbb{Z}$ ist. Es ist also $\chi_1, \ldots, \chi_n$ $\mathbb{Z}$-Basis von M.

Aufgabe 14) Es sei $K/\mathbb{Q}$ eine quadratische Erweiterung und d_K die Diskriminante. Zeigen Sie $K = \mathbb{Q}(\sqrt{d_K})$.

Lösung: Sicher ist $K = \mathbb{Q}(\sqrt{d})$ für ein $d \in \mathbb{Z}$, quadratfrei, $\neq 0, 1$. Für die Diskriminante bestimmen wir die Struktur von $\mathcal{O}_K$. Sei $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$. Dieses ist genau dann ganz, wenn Spur und Norm ganz sind (Koeffizienten des Minimalpolynoms). Es ist $\mathrm{Tr}(\alpha) = a + b\sqrt{d} + a - b\sqrt{d} = 2a$. Also α ganz $\Leftrightarrow 2a, a^2 - db^2 \in \mathbb{Z}$. Dann ist auch $4(a^2 - db^2) \in \mathbb{Z}$ $\Rightarrow 4db^2 \in \mathbb{Z}$ $\Rightarrow 2b \in \mathbb{Z}$ (d quadratfrei). Also $a = \frac{a_1}{2}$, $b = \frac{b_1}{2}$ mit $a_1, b_1 \in \mathbb{Z}$.

i) Fall $d \equiv 2,3 \pmod 4$

$a^2 - db^2 \in \mathbb{Z} \Rightarrow a_1^2 - db_1^2 \equiv 0 \pmod 4$. Die einzigen Quadrate modulo 4 sind 0 und 1. Also $a_1, b_1 \equiv 0 \pmod 2$. Damit $a, b \in \mathbb{Z}$ und $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \langle 1, \sqrt{d} \rangle$.

$$d_K = \det{}^2(\sigma_i \omega_j) = \begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{vmatrix}^2 = 4d. \Rightarrow K = \mathbb{Q}(\sqrt{d_K})$$

ii) Fall $d \equiv 1 \pmod 4$

$a^2 - db^2 \in \mathbb{Z} \Rightarrow a_1^2 - b_1^2 \equiv 0 \pmod 4 \Rightarrow a_1 \equiv b_1 \pmod 2$. Also $\mathcal{O}_K = \{ \frac{a_1}{2} + b_1 2\sqrt{d} : a_1 \equiv b_1 \pmod 2 \} = \langle 1, \frac{1+\sqrt{d}}{2} \rangle$.

$$d_K = \begin{vmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d$$

Aufgabe 15) Beweisen Sie STICKELBERGERs Diskriminantensatz: Die Diskriminante eines algebraischen Zahlenkörpers K ist stets $\equiv 0$ oder $1 \pmod 4$.

Lösung: Es ist $\sqrt{d_K} = \det(\sigma_i \omega_j)$ für Ganzheitsbasen $\omega_1, \ldots, \omega_n$ und $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(K/\mathbb{Q})$. Wir zerlegen die Permutationsdarstellung der Determinante in gerade und ungerade Permutationen.

$$\det(\sigma_i \omega_j) = \alpha - \beta,$$

wobei $\alpha = \sum_{\pi \text{ ger.}} \prod_i \sigma_{\pi(i)} \omega_i$ und $\beta = \sum_{\pi \text{ ung.}} \prod_i \sigma_{\pi(i)} \omega_i$. Nun sind α und β ganz, also auch $\alpha + \beta$ und $\alpha \cdot \beta$. Diese sind nach Konstruktion invariant unter allen σ_i und liegen daher in $\mathbb{Q}$ und folglich in $\mathbb{Z}$. Somit ist

$$d \equiv (\alpha - \beta)^2 \equiv \underbrace{(\alpha + \beta)^2}_{\in \mathbb{Z}} - \underbrace{4\alpha\beta}_{\in \mathbb{Z}} \equiv 0, 1 \pmod 4.$$

Aufgabe 16) Zeigen Sie, dass $1, \sqrt[3]{2}, \sqrt[3]{4}$ eine Ganzheitsbasis von $\mathbb{Q}(\sqrt[3]{2})$ ist.

Lösung: Sei $\alpha = \sqrt[3]{2}$ und $K = \mathbb{Q}(\alpha)$. α hat Minimalpolynom $f(X) = X^3 - 2$ über $\mathbb{Q}$ und wir haben die 3 Homomorphismen $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \mathbb{Q}(\alpha, \zeta)) = \{\mathrm{id}, \sigma, \tau\}$, wobei $\zeta = e^{2\pi i/3}$, $\sigma(\alpha) = \alpha\zeta$ und $\tau(\alpha) = \alpha\zeta^2$. Nach Aufgabe 11 ist $d(\mathbb{Z}(\alpha)) = d(1, \alpha, \alpha^2) = -2^2 3^3$, also $-2^2 3^3 = [\mathcal{O}_K : \mathbb{Z}(\alpha)]^2 d_K$. Folglich $[\mathcal{O}_K : \mathbb{Z}(\alpha)] \in \{1, 2, 3, 6\}$. Wir zeigen $[\mathcal{O}_K : \mathbb{Z}(\alpha)] = 1$ und damit, dass $1, \alpha, \alpha^2$ Ganzheitsbasis von K ist.

Wäre $[\mathcal{O}_K : \mathbb{Z}(\alpha)] = k \in \{2, 3, 6\}$, folgte aus $x \in \mathbb{Z}[\alpha]$ auch $y = \frac{x}{k} \in \mathcal{O}_K$, also $y \in K$ ganz über $\mathbb{Z}$. Daher genügt es die Fälle $k = 2$ und $k = 3$ auszuschließen. Nun ist das Minimalpolynom von y über $\mathbb{Q}$ gerade $f(X) = X^3 - \mathrm{Tr}(y)X^2 + (y\sigma(y) + y\tau(y) + \sigma(y)\tau(y))X - \mathrm{N}(y)$ und wegen y ganz, ist $f \in \mathbb{Z}[X]$ (Algebra 1). Sei nun

$y = a + b\alpha + c\alpha^2$, mit $a = \frac{\tilde{a}}{k}$ $b = \frac{\tilde{b}}{k}$ und $c = \frac{\tilde{c}}{k}$ für $\tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{Z}$.

$$\begin{aligned}
\mathrm{Tr}(y) &= a + b\alpha + c\alpha^2 + \sigma(a + b\alpha + c\alpha^2) + \tau(a + b\alpha + c\alpha^2) \\
&= a + b\alpha + c\alpha^2 + a + b\alpha\zeta + c\alpha^2\zeta^2 + a + b\alpha\zeta^2 + c\alpha^2\zeta \\
&= 3a \\
y\sigma(y) + y\tau(y) + \sigma(y)\tau(y)) &= \text{Rechnerei...} \\
&= 2a^3 - 6bc + a^2 \\
\mathrm{N}(y) &= (a + b\alpha + c\alpha^2) \cdot (a + b\alpha\zeta + c\alpha^2\zeta^2) \cdot (a + b\alpha\zeta^2 + c\alpha^2\zeta) \\
&= a^3 + 2b^3 + 4c^3 - 6abc
\end{aligned}$$

Also $3a, 2a^3 - 6bc + a^2, a^3 + 2b^3 + 4c^3 - 6abc \in \mathbb{Z}$.

(a) $k = 2$

$3\frac{\tilde{a}}{2} \in \mathbb{Z} \Rightarrow \tilde{a}$ gerade $\Rightarrow a \in \mathbb{Z}$. Und aus $2a^3 - 6bc + a^2 \in \mathbb{Z}$ folgt $6bc \in \mathbb{Z}$.

$a^3 + 2b^3 + 4c^3 - 6abc \in \mathbb{Z} \Rightarrow \frac{\tilde{b}^3}{4} + \frac{\tilde{c}^3}{2} \in \mathbb{Z}$. Wegen $6bc \in \mathbb{Z}$ ist $\tilde{b}$ gerade oder $\tilde{c}$ gerade. Im ersten Fall folgt $\frac{\tilde{c}^3}{2} \in \mathbb{Z}$, also auch $\tilde{c}$ gerade. Im zweiten Fall folgt $\frac{\tilde{b}^3}{4} \in \mathbb{Z}$, also auch $\tilde{b}$ gerade.

Insgesamt also $a, b, c \in \mathbb{Z}$.

(b) $k = 3$

$2a^3 - 6bc + a^2 = \frac{1}{27}(2\tilde{a}^3 - 18\tilde{b}\tilde{c} + 3\tilde{a}^2) \in \mathbb{Z} \Rightarrow 3 \mid 2\tilde{a}^3 - 18\tilde{b}\tilde{c} + 3\tilde{a}^2 \Rightarrow 3 \mid 2\tilde{a}^3$ $\Rightarrow 3 \mid \tilde{a} \Rightarrow a \in \mathbb{Z}$. Also $6bc \in \mathbb{Z} \Rightarrow \frac{2}{3}\tilde{b}\tilde{c} \in \mathbb{Z}$ und somit $3 \mid \tilde{b}$ oder $3 \mid \tilde{c}$. Im ersten Fall folgt $b \in \mathbb{Z}$ und mit der Norm folgt $4c^3 - 6abc \in \mathbb{Z}$. Wegen $6c \in \mathbb{Z}$ folgt $4c^3 \in \mathbb{Z}$, also $c \in \mathbb{Z}$. Im zweiten Fall, also $c \in \mathbb{Z}$, folgt aus $2b^3 - 6abc \in \mathbb{Z}$ analog $b \in \mathbb{Z}$.

Insgesamt also $a, b, c \in \mathbb{Z}$.

Also $y \in \mathbb{Z}(\alpha)$ und $\mathcal{O}_K = \mathbb{Z}(\alpha)$. Damit ist alles gezeigt.

Aufgabe 17) Sei A eine DEDEKIND-Ring und $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ gebrochene Ideale von A. Zeigen Sie:

(a) $\mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\mathfrak{c}$

(b) $\mathfrak{ab} = \mathfrak{ba}$

(c) $\mathfrak{ab} = \mathfrak{a} \Leftrightarrow \mathfrak{b} = (1) = A$

Lösung:

(a)

$$\begin{aligned}
\mathfrak{a}(\mathfrak{b}\mathfrak{c}) &= \mathfrak{a}\left\{\sum_{i=1}^{n} b_i c_i : n \in \mathbb{N}, b_i \in \mathfrak{b}, c_i \in \mathfrak{c}\right\} \\
&= \left\{\sum_j a_j \sum_i b_{ij} c_{ij}\right\} \\
&= \left\{\sum_l (\sum_k (a_{kl} b_{kl}) c_l\right\} \qquad \text{(Umordnung endlicher Summe)} \\
&= \left\{\sum_k a_k b_k\right\} \mathfrak{c} \\
&= (\mathfrak{a}\mathfrak{b})\mathfrak{c}
\end{aligned}$$

(b) $\mathfrak{a}\mathfrak{b} = \{\sum_i a_i b_i\} = \{\sum b_i a_i\} = \mathfrak{b}\mathfrak{a}$

(c) $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \Leftrightarrow \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{a} \Leftrightarrow \mathfrak{b} = (1) = A$

Aufgabe 18) Zeigen Sie: Für gebrochene Ideale $\mathfrak{a}, \mathfrak{b}$ eines DED-Rings A ist auch $\mathfrak{a}+\mathfrak{b} := \{a+b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$ gebrochenes Ideal.

Lösung: Zunächst ist $\mathfrak{a}+\mathfrak{b}$ ein A-Modul: $\mathfrak{a}+\mathfrak{b}$ ist offensichtliche abgeschlossen unter Additon, also Gruppe nach Vererbung. Für $\lambda \in A$ und $a \in \mathfrak{a}, b \in \mathfrak{b}$ ist $\lambda(a+b) = \lambda a + \lambda b \in \mathfrak{a}+\mathfrak{b}$. Seien also $x, y \in A$ mit $x\mathfrak{a}$, $y\mathfrak{b}$ Ideale von A, dann $xy(\mathfrak{a}+\mathfrak{b}) = xy\mathfrak{a} + xy\mathfrak{b}$ Ideal von A. Also $\mathfrak{a}+\mathfrak{b}$ gebrochenes Ideal.

Aufgabe 19) Sei A eine DEDEKIND-Ring und $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ gebrochene Ideale von A. Zeigen Sie:

(a) $\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}$

(b) $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$

(c) $\mathfrak{a} + \mathfrak{b} = \mathfrak{a} \Leftrightarrow \mathfrak{b} \subset \mathfrak{a}$

(d) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$

Lösung:

(a) und (b) folgen aus Assoziativität bzw. Kommutativität der Addition im Ring A.

(c) „$\Leftarrow$“ klar, „$\Rightarrow$“ $\forall b \in \mathfrak{b} : b = 0 + b \in \mathfrak{a}$.

(d) folgt aus Distributivität im Ring A.

Aufgabe 20) Sei A eine DEDEKIND-Ring und $\mathfrak{a}, \mathfrak{b}$ Ideale von A. Zeigen Sie $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ und $\mathrm{kgV}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$.

Lösung: Wegen A DED-Ring, haben wir eine eindeutige Primfaktorzerlegung für Ideale.

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i}, \qquad \mathfrak{p} = \prod_i \mathfrak{p}_i^{b_i}.$$

Dann ist $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) = \prod_i \mathfrak{p}_i^{\min(a_i, b_i)}$ und $\mathrm{kgV}(\mathfrak{a}, \mathfrak{b}) = \prod_i \mathfrak{p}_i^{\max(a_i, b_i)}$. Sei nun $\mathfrak{p}$ Primteiler von $\mathfrak{a}$ und $\mathfrak{b}$, dann ist $\mathfrak{a}+\mathfrak{b} = \mathfrak{p}(\mathfrak{a}'+\mathfrak{b}')$. Iterieren liefert $\mathfrak{a}+\mathfrak{b} = \prod_i \mathfrak{p}_i^{\min(a_i.b_i)}(\tilde{\mathfrak{a}}+\tilde{\mathfrak{b}})$

mit Teilerfremden $\tilde{\mathfrak{a}}$ und $\tilde{\mathfrak{b}}$. Es bleibt zu zeigen: $(\tilde{\mathfrak{a}}+\tilde{\mathfrak{b}})=(1)$. Würde $\tilde{\mathfrak{a}}+\tilde{\mathfrak{b}}\subset\mathfrak{m}$, für ein maximales Ideal $\mathfrak{m}$, so würde $\mathfrak{m}$ nun $\tilde{\mathfrak{a}}+\tilde{\mathfrak{b}}$ teilen. Also $\mathfrak{a}+\mathfrak{b}=\prod_i \mathfrak{p}_i^{\min(a_i,b_i)}$.

Analog können wir $\mathfrak{a}\cap\mathfrak{b}=\prod_i \mathfrak{p}_i^{\min(a_i,b_i)}(\hat{\mathfrak{a}}\cap\hat{\mathfrak{b}})$ bilden, mit teilerfremden $\hat{\mathfrak{a}}$, $\hat{\mathfrak{b}}$. Wir zeigen: $\hat{\mathfrak{a}}\cap\hat{\mathfrak{b}}=\hat{\mathfrak{a}}\hat{\mathfrak{b}}$: „$\subset$“ ist klar. Oben haben wir $\hat{\mathfrak{a}}+\hat{\mathfrak{b}}=(1)$ gezeigt, also ist $1=a+b$ mit $a\in\hat{\mathfrak{a}}$, $b\in\hat{\mathfrak{b}}$. Für $x\in\hat{\mathfrak{a}}\cap\hat{\mathfrak{b}}$ ist nun $x=1x=ax+bx\in\hat{\mathfrak{a}}\hat{\mathfrak{b}}$. Also ist

$$\begin{aligned}\hat{\mathfrak{a}}\cap\hat{\mathfrak{b}}&=\prod_i \mathfrak{p}_i^{\min(a_i,b_i)}(\hat{\mathfrak{a}}\hat{\mathfrak{b}})\\&=\prod_i \mathfrak{p}_i^{\min(a_i,b_i)+a_i-\min(a_i,b_i)+b_i-\min(a_i,b_i)}\\&=\prod_i \mathfrak{p}_i^{a_i+b_i-\min(a_i,b_i)}\\&=\prod_i \mathfrak{p}_i^{\max(a_i,b_i)}\end{aligned}$$

Aufgabe 21) Sei A eine DEDEKIND-Ring und $\mathfrak{a},\mathfrak{b}$ Ideale von A. Zeigen Sie: $\mathfrak{ab}=\mathrm{ggT}(\mathfrak{a},\mathfrak{b})\,\mathrm{kgV}(\mathfrak{a},\mathfrak{b})$

Lösung: $\mathfrak{ab}=\prod_i \mathfrak{p}_i^{a_i+b_i}=\prod_i \mathfrak{p}_i^{\min(a_i,b_i)+\max(a_i,b_i)}=\mathrm{ggT}(\mathfrak{a},\mathfrak{b})\,\mathrm{kgV}(\mathfrak{a},\mathfrak{b})$.

Aufgabe 22) Sei A eine DEDEKIND-Ring und $\mathfrak{a},\mathfrak{b}$ Ideale von A. Zeigen Sie: $\mathrm{ggT}(\mathfrak{a},\mathfrak{b})=(1)\Leftrightarrow\mathfrak{ab}=\mathfrak{a}\cap\mathfrak{b}$

Lösung: Nach den vorherigen beiden Aufgaben haben wir: $\mathfrak{a}\cap\mathfrak{b}=\mathrm{kgV}(\mathfrak{a},\mathfrak{b})$ und $\mathfrak{ab}=\mathrm{ggT}(\mathfrak{a},\mathfrak{b})\,\mathrm{kgV}(\mathfrak{a},\mathfrak{b})$. Also Gleichheit $\Leftrightarrow\mathrm{ggT}(\mathfrak{a},\mathfrak{b})=(1)$.

Aufgabe 23) Bestimmen Sie die Klassenzahl von $K=\mathbb{Q}(\sqrt{-19})$.

Lösung: Wegen $-19\equiv 1\pmod 4$, ist $d_K=-19$ und $\mathcal{O}_K=\mathbb{Z}+\frac{1+\sqrt{-19}}{2}\mathbb{Z}$. Der Erweiterungsgrad ist $n=2=r+2s$, mit $r=0$ reellen und $s=1$ komplexen Einbettungen (modulo komplexer Konjugation) von $\mathbb{Q}$ in K. Daher ist die MINKOWSKI-Konstante

$$c_K=\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s=\frac{2}{\pi}.$$

Nach dem Satz von MINKOWSKI liegt in jeder Idealklasse ein ganzes Ideal mit Absolutnorm $\leq c_K\sqrt{|d_K|}=\frac{2}{\pi}\sqrt{19}<\frac{2}{3}\sqrt{19}=\frac{76}{9}<3$.

Wegen $\mathbb{N}\mathfrak{a}\in\mathfrak{a}$ und weil ein Primideal nicht 2 Primzahlen enthalten kann, verbleibt das Zerlegungsverhalten von $2\in\mathbb{P}$ zu untersuchen: Da $2\nmid d_K$ ist 2 unverzweigt, also $2\neq\mathfrak{p}^n$. Wir zeigen 2 ist träge: Setze $\omega:=\frac{1+\sqrt{-19}}{2}$, dann ist $\omega^2=\frac{-9+\sqrt{-19}}{2}=\omega-5$. Also $f(T)=T^2-T+5=\mathrm{Irr}(\omega,T,\mathbb{Q})$. Also $K=\mathbb{Q}[T]/(f(T))$ und $\mathcal{O}_K=\mathbb{Z}[T]/(f(T))$. Somit

$$\begin{aligned}\mathcal{O}_K/2\mathcal{O}_K&\cong\frac{\mathbb{Z}[T]/(T^2-T+5)}{2(\mathbb{Z}[T]/(T^2-T+5))}\\&\cong\underbrace{(\mathbb{Z}/2\mathbb{Z})}_{\mathbb{F}_2}[T]/(T^2-T+5).\end{aligned}$$

Darüber hinaus ist f irreduzibel in $\mathbb{F}_2[T]$, also $\mathcal{O}_K/2\mathcal{O}_K\cong\mathbb{F}_4$ ein Körper. Damit (2) Primideal in $\mathcal{O}_K$. $\mathbb{N}(2)=4>3$. Folglich ist $h_K=1$.

Aufgabe 24) Sei K ein algebraischer Zahlenkörper, h_K seine Klassenzahl und $\mathfrak{a}$ ein gebrochenes Ideal. Sei $\mathfrak{a}^n$ ein gebrochenes Hauptideal. Zeigen Sie: Sind n und h_K teilerfremd, so ist $\mathfrak{a}$ gebrochenes Hauptideal.

Lösung: Wegen $[\mathfrak{a}] \in \mathrm{Cl}_K$ und $\mathfrak{a}^n$ Hauptideal ist $[\mathfrak{a}]^n = 1$. Und wegen $h_K = \mathrm{ord}(Cl_K)$ ist $[\mathfrak{a}]^{h_K} = 1$. Der EUKLIDische Algorithmus liefert $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(n, h_k) = 1 = xn + yh_K$. Daher ist $[\mathfrak{a}]^1 = [\mathfrak{a}]^{xn+yh_K} = ([\mathfrak{a}]^n)^x([\mathfrak{a}]^{h_K})^y = 1$ und folglich $\mathfrak{a}$ Hauptideal.

Aufgabe 25) Es sei $\omega = \sqrt{-5}$ und $K = \mathbb{Q}(\omega)$. Seien weiter $\mathfrak{p} = (2, 1+\omega)$, $\mathfrak{q} = (3, 1+\omega)$ und $\mathfrak{r} = (3, 1-\omega)$. Zeigen Sie:

(a) $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ sind Primideale,

(b) $\mathfrak{p}^2 = (2)$, $\mathfrak{pq} = (1+\omega)$, $\mathfrak{qr} = (3)$, $\mathfrak{pr} = (1-\omega)$ und

(c) $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ sind keine Hauptideale.

(d) Berechnen Sie die Klassenzahl h_K.

Lösung:

(a) Bekanntlich ist $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$. Wir zeigen zunächst: $\mathfrak{p} = 2\mathbb{Z} + (1+\omega)\mathbb{Z}$, $\mathfrak{q} = 3\mathbb{Z} + (1+\omega)\mathbb{Z}$ und $\mathfrak{r} = 3\mathbb{Z} + (1-\omega)\mathbb{Z}$. Dazu genügt es zu zeigen, dass die rechten Seiten $\mathcal{O}_K$-Ideale sind.

$2\mathbb{Z} + (1+\omega)\mathbb{Z}$: $\omega \cdot 2 = 2(1+\omega) - 1 \cdot 2$ und $\omega \cdot (1+\omega) = \omega - 5 = (1+\omega) - 3 \cdot 2$.

$3\mathbb{Z} + (1+\omega)\mathbb{Z}$: $\omega \cdot 3 = 3(1+\omega) - 1 \cdot 3$ und $\omega \cdot (1+\omega) = \omega - 5 = (1+\omega) - 2 \cdot 3$.

$3\mathbb{Z} + (1-\omega)\mathbb{Z}$: $\omega \cdot 3 = 1 \cdot 3 - 3(1-\omega)$ und $\omega \cdot (1-\omega) = \omega + 5 = 2 \cdot 3 - (1-\omega)$.

Also

$$\mathbb{N}\mathfrak{p} = \left|\det \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\right| = 2,$$

$$\mathbb{N}\mathfrak{q} = \left|\det \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}\right| = 3,$$

$$\mathbb{N}\mathfrak{r} = \left|\det \begin{pmatrix} 3 & 1 \\ 0 & -1 \end{pmatrix}\right| = 3.$$

Folglich sind $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ Primideale.

(b) $\mathfrak{p}^2 = (2)$: $\mathfrak{p}^2 \subseteq (2)$, denn $2 \mid 2(1+\omega)$, $2 \mid 2 \cdot 2$, $2 \mid (1+\omega)^2 = 1 + 2\omega - 5 = 2\omega - 4$. $\mathbb{N}(\mathfrak{p}^2) = \mathbb{N}(\mathfrak{p})^2 = 4 = \mathbb{N}(2) \Rightarrow \mathfrak{p}^2 = (2)$.

$\mathfrak{pq} = (1+\omega)$: $\mathfrak{pq} \subseteq (1+\omega)$, denn $(1+\omega) \mid 2(1+\omega)$, $(1+\omega) \mid 3(1+\omega)$, $(1+\omega) \mid 2 \cdot 3 = 6 = (1-\omega)(1+\omega)$, $(1+\omega) \mid (1+\omega)^2$. Wegen $(1+\omega) \cdot 1 = 1+\omega$ und $(1+\omega)\omega = \omega - 5$ folgt $\mathbb{N}(1+\omega) = \left|\det \begin{pmatrix} 1 & -5 \\ 1 & 1 \end{pmatrix}\right| = 6$. Nun gilt $\mathbb{N}(\mathfrak{pq}) = \mathbb{N}\mathfrak{p} \cdot \mathbb{N}\mathfrak{q} = 2 \cdot 3 = 6 = \mathbb{N}(1+\omega)$. Also $\mathfrak{pq} = (1+\omega)$.

$\mathfrak{qr} = (3)$: $\mathfrak{qr} \subseteq (3)$, denn $3 \mid 3 \cdot (1+\omega)$, $3 \mid 3 \cdot 3$, $3 \mid 3(1-\omega)$, $3 \mid 6 = (1+\omega)(1-\omega)$. $\mathbb{N}(\mathfrak{qr}) = \mathbb{N}\mathfrak{p} \cdot \mathbb{N}\mathfrak{q} = 3 \cdot 3 = 9 = \mathbb{N}(3) \Rightarrow \mathfrak{qr} = (3)$.

$\mathfrak{pr} = (1-\omega)$: $\mathfrak{pr} \subseteq (1-\omega)$, denn $(1-\omega) \mid 2(1-\omega)$, $(1-\omega) \mid 3 \cdot 2 = (1+\omega)(1-\omega)$, $(1-\omega) \mid 3(1+\omega) = (-2+\omega)(1-\omega)$. Wegen $(1-\omega) \cdot 1 = 1-\omega$ und $(1-\omega)\omega = \omega + 5$

folgt $\mathbb{N}(1-\omega) = \left|\det \begin{pmatrix} 1 & 5 \\ -1 & 1 \end{pmatrix}\right| = 6$. Nun gilt $\mathbb{N}(\mathfrak{p}\mathfrak{r}) = \mathbb{N}\mathfrak{p} \cdot \mathbb{N}\mathfrak{q} = 2 \cdot 3 = 6 = \mathbb{N}(1-\omega)$. Also $\mathfrak{p}\mathfrak{r} = (1-\omega)$.

(c) $\mathbb{N}(a+b\omega) = |\,\mathrm{N}(a+b\omega)| a^2 + 5b^2 = 2$ oder $= 3$ hat keine $\mathbb{Z}$-Lösungen.

(d) Wie bereits gesehen, ist $d_K = 4 \cdot -5 = -20$, wegen $-5 \equiv 3 \pmod 4$. Satz von MINKOWSKI: $r = 0$, $s = 1$, $c_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s = \frac{2}{\pi}$. Also gibt es in jeder Idealklasse aus Cl_K ganze Ideale $\mathfrak{a}$ mit $\mathbb{N}\mathfrak{a} \leq c_K\sqrt{|d_K|} = \frac{2}{\pi}\sqrt{20} < \frac{2}{3}\sqrt{20} = \sqrt{\frac{80}{9}} < 3$. Da $(2) = \mathfrak{p}^2$, also $h_K = 2$. Damit $\mathrm{Cl}_K = \langle[\mathfrak{p}]\rangle \cong C_2$. 2 ist verzweigt, 3 ist zerlegt.

Aufgabe 26) Berechnen Sie die Klassenzahl von $\mathbb{Q}(\zeta_5)$, wobei $\zeta_5 = e^{2\pi i/5}$.

Lösung: Es ist $n = 4$ und $s = 2$ in der MINKOWSKI-Theorie. Also $c_K = \frac{3}{2\pi^2}$. Weiter ist $d_K = (-1)^{(5-1)/2}5^{5-2} = 125$. Damit folgt, dass in jeder Idealklasse in Cl_K ganze Ideale $\mathfrak{a}$ existieren mit $\mathbb{N}\mathfrak{a} \leq c_K\sqrt{|d_K|} = \frac{3}{2\pi^2}\sqrt{125} = \sqrt{\frac{9\cdot 125}{4\pi^4}} < \sqrt{\frac{125}{4\cdot 3^2}} < \sqrt{4} < 2$. $\Rightarrow h_K = 1$.

Aufgabe 27) Berechnen Sie die Klassenzahl von $K = \mathbb{Q}(\sqrt{-23})$. Benutzen Sie die Primideale $\mathfrak{p} = (2, \frac{1+\sqrt{-23}}{2})$, $\overline{\mathfrak{p}}$, $\mathfrak{q} = (3, \frac{1+\sqrt{-23}}{2})$, $\overline{\mathfrak{q}}$.

Lösung: Setze $\omega = \sqrt{-23}$ und $z = \frac{1+\omega}{2}$. $d_K = -23$ und $\mathcal{O}_K = \mathbb{Z} + z\mathbb{Z}$, wegen $-23 \equiv 1 \pmod 4$. $c_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right) = \frac{2}{\pi}$. Also wird Cl_K von Primidealen $\mathfrak{r}$ mit $\mathbb{N}\mathfrak{r} \leq \frac{2}{\pi}\sqrt{23} = \sqrt{\frac{46}{\pi}} < \sqrt{\frac{48}{3}} = 4$, also $\mathbb{N}\mathfrak{r} \leq 3$, erzeugt. Jedes Primideal $\mathfrak{r}$ enthält genau eine orthodoxe Primzahl r. Also $(r) = r\mathcal{O}_K \subset \mathfrak{r} \subset \mathcal{O}_K$. Ist $(r) = \mathfrak{r}$, so ist $\mathbb{N}\mathfrak{r} = \mathrm{N}_{\mathbb{Q}}^K(r) = r^2$ und sonst $\mathbb{N}\mathfrak{r} = r$. Also kommen nur Erzeuger in Frage, die 2 oder 3 enthalten.

Es gilt $\mathfrak{p} = 2\mathbb{Z} + z\mathbb{Z}$, $\overline{\mathfrak{p}} = 2\mathbb{Z} + \overline{z}\mathbb{Z}$, $\mathfrak{q} = 3\mathbb{Z} + z\mathbb{Z}$ und $\overline{\mathfrak{q}} = 3\mathbb{Z} + \overline{z}\mathbb{Z}$: Es genügt zu zeigen, dass die rechten Seiten $\mathcal{O}_K$-Ideale sind.

$$\begin{aligned} z \cdot 2 &= 2 \cdot z \\ z \cdot z &= \frac{1 + 2\omega - 23}{4} = z - 2 \cdot 3 \\ z \cdot 3 &= -3 \cdot \overline{z} - 2 \cdot 3 \\ z \cdot \overline{z} &= 6 = 2 \cdot 3 \end{aligned}$$

Damit folgt $\mathbb{N}\mathfrak{p} = \mathbb{N}\overline{\mathfrak{p}} = 2$ und $\mathbb{N}\mathfrak{q} = \mathbb{N}\overline{\mathfrak{q}} = 3$. Es ist $\mathfrak{p} \neq \overline{\mathfrak{p}}$ und $\mathfrak{q} \neq \overline{\mathfrak{q}}$: Ist $\frac{1+\omega}{2} = 2a + \frac{1-\omega}{2}b$ mit $a, b \in \mathbb{Z}$, folgt $b = -1$ und damit $2a = 1$ $\lightning$. Ist $\frac{1+\omega}{2} = 3a + \frac{1-\omega}{2}b$ mit $a, b \in \mathbb{Z}$, folgt $b = -1$ und $3a = 1$ $\lightning$.

Wir zeigen $(2) = \mathfrak{p}\overline{\mathfrak{p}}$, $(3) = \mathfrak{q}\overline{\mathfrak{q}}$: $2, 3 \mid \left(\frac{1+\omega}{2}\right)\left(\frac{1-\omega}{2}\right) = 6$ und $\mathbb{N}\mathfrak{p}\overline{\mathfrak{p}} = \mathbb{N}(2) = 4$, $\mathbb{N}\mathfrak{q}\overline{\mathfrak{q}} = \mathbb{N}(3) = 9$. Also sind 2 und 3 zerlegt. Insbesondere ist $[\mathfrak{p}] = [\overline{\mathfrak{p}}]^{-1}$ und $[\mathfrak{q}] = [\overline{\mathfrak{q}}]^{-1}$.

Weiter gilt $\mathfrak{p}\mathfrak{q} = (z)$: Die Norm passt jedenfalls: $\mathbb{N}\mathfrak{p}\mathfrak{q} = 6 = \mathbb{N}((z))$. Wir zeigen $\mathfrak{p}\mathfrak{q} \subset (z)$: $z \mid 2 \cdot 3 = 6 = z\overline{z}$, $z \mid 2z$, $z \mid 3z$, $z \mid z^2$. Damit ist $[\mathfrak{p}] = [\mathfrak{q}]^{-1}$.

Schließlich haben wir noch $\mathfrak{p}^3 = (\overline{z}+1)$ und $\mathfrak{p}^2$ ist kein Hauptideal: $\mathfrak{p}^3 = (8, 4z, 2z^2, z^3)$ und es ist $z^2 = z - 6$, also $z^3 = -5z - 6$. Damit $\mathfrak{p}^3 = (8, 4z, 2z - 12, 5z + 6)$. Wir

zeigen $\mathfrak{p}^3 \subset (\overline{z}+1)$, man beachte die Identität $z+\overline{z}=1$.

$$\begin{aligned}
&\overline{z}+1 \mid 8 = (z+1)(\overline{z}+1)\\
&\overline{z}+1 \mid 4z = (z-3)(\overline{z}+1)\\
&\overline{z}+1 \mid 2z-12 = -2\overline{z}-10 = (\overline{z}-4)(\overline{z}+1)\\
&\overline{z}+1 \mid 5z+6 = (2z-3)(\overline{z}+1)
\end{aligned}$$

Nun ist $\mathbb{N}((\overline{z}+1)) = 8 = \mathbb{N}\mathfrak{p}^3$, also $\mathfrak{p}^3 = (\overline{z}+1)$.

Angenommen $\mathfrak{p}^2 = (4, 2z, z^2) = (4, 2z, z-6) = (a+bz)$ für $a, b \in \mathbb{Z}$. Dann $\mathbb{N}((a+bz)) = a^2+ab+6b^2 = 4$, was nur die ganzzahligen Lösungen $(\pm 2, 0)$ besitzt. Aber $\mathfrak{p}^2 \neq (2)$, denn $2 \nmid z-6$. Also ist $\mathfrak{p}^2$ kein Hauptideal und es ergibt sich, dass Cl_K erzeugt ist durch $\mathfrak{p}$ und es gilt $h_K = 3$.

Aufgabe 28) Zeigen Sie, dass in einem algebraischen Zahlenkörper K nur endlich viele Einheitswurzeln liegen.

Lösung: Unter $j : K \to K_{\mathbb{R}}$ werden Einheitswurzeln injektiv auf Einheitswurzeln abgebildet (mit komponentenweiser Multiplikation in $K_{\mathbb{R}}$ und Einselement $(1, \ldots, 1)$). Also liegen die Bilder in einem beschränkten Gebiet, da jede einzelne Bildkomponente beschränkt ist (in $K_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$ hat jede Komponente einer Einheitswurzel Betrag 1). Gleichzeitig sind alle Einheitswurzeln ganz und $E_K = \mathcal{O}_K^\times$ wird auf ein Gitter abgebildet. Dieses kann nur endlich viele Punkte in beschränktem Gebiet haben.

Aufgabe 29) Welche Einheitswurzeln können in K (alg. ZK) liegen, falls $[K : \mathbb{Q}] = 4$ ist? Welche, falls $[K : \mathbb{Q}]$ ungerade?

Lösung: Für eine primitive m-te Einheitswurzel ζ_m ist $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$. Ist $\zeta_m \in K$, so gibt es einen Turm $K/\mathbb{Q}(\zeta_m)/\mathbb{Q}$ und es folgt $\varphi(m) \mid [K : \mathbb{Q}]$. Sei $m = \prod_i p_i^{e_i}$, dann ist $\varphi(m) = \prod_i (p_i - 1) p_i^{e_i - 1}$.

Im Fall $[K : \mathbb{Q}] = 4$, also $\varphi(m) \mid 4$, folgt, dass wir nur $p = 2, 3, 5$ betrachten müssen.

$$\begin{aligned}
&\varphi(m) = 1 \Leftrightarrow m \in \{1, 2\}\\
&\varphi(m) = 2 \Leftrightarrow m \in \{3, 4, 6\}\\
&\varphi(m) = 4 \Leftrightarrow m \in \{5, 8, 10, 12\}
\end{aligned}$$

Also können die Einheitswurzeln in K liegen.

Im Fall $[K : \mathbb{Q}]$ ungerade folgt auch $\varphi(m)$ ungerade. Damit kommt nur $m \in \{1, 2\}$ in Frage.

Aufgabe 30) Sei $K = \mathbb{Q}(\zeta_p)$, $p > 2$, $\zeta_p = e^{2\pi i/p}$. Zeigen Sie, dass die Zahlen $\varepsilon_r = (\zeta_p^r - 1)/(\zeta_p - 1)$ für $r = 1, \ldots, p-1$ Einheiten in $\mathcal{O}_K$ sind.

Lösung: Es ist $\varepsilon_r = \zeta_p^{r-1} + \ldots + \zeta_p + 1$, also ganz (als Summe ganzer Elemente). Einheit in $\mathcal{O}_K$: Zu zeigen ist $\varepsilon_r^{-1} \in \mathcal{O}_K$. Sei $s = r^{-1}$ in $\mathbb{F}_p$, dann ist $\zeta_p^{rs} = \zeta_p$. Damit folgt $\varepsilon_r^{-1} = \frac{\zeta_p - 1}{\zeta_p^r - 1} = \frac{\zeta_p^{rs} - 1}{\zeta_p^r - 1} = \zeta_p^{r(s-1)} + \zeta_p^{r(s-2)} + \ldots + \zeta_p^r + 1 \in \mathcal{O}_K$.

Aufgabe 31) Berechnen Sie die Fundamentaleinheiten von $K = \mathbb{Q}(\sqrt{d})$ für $d = 2, 3, 5, 6, 7, 10$ (NEUKIRCH p. 46). Hinweis: Die eindeutig bestimmte Lösung $(x_1, y_1) \in \mathbb{N}^2$ der Gleichung $x^2 - d_K y^2 = -4$, bzw. falls diese nicht existiert die Minimallösung der Gleichung $x^2 - d_K y^2 = 4$, führen zur Fundamentaleinheit $\varepsilon_1 = \frac{x_1 + \sqrt{d_K} y_1}{2}$.

Lösung: Wir berechnen d_K:

d	2	3	5	6	7	10
d_K	8	12	5	24	28	40

Nun probieren wir, wann $d_K y^2 \mp 4$ erstmalig ein Quadrat wird. Dabei lassen wir für jedes einzelne y dem Fall -4 stets den Vorrang:

$d_K \backslash d_K y^2 \mp 4$	$y=1$	$y=2$	$y=3$
8	4✓, 12		
12	8, 16✓		
5	1✓, 9		
24	20, 28	92, 100✓	
28	24, 32	108, 116	248, 256✓
40	36✓, 44		

Damit erhalten wir die Fundamentaleinheiten:

d	2	3	5	6	7	10
d_K	8	12	5	24	28	40
y	1	1	1	2	3	1
x	2	4	1	10	16	6
ε_K	$\frac{2+\sqrt{8}}{2} = 1+\sqrt{2}$	$2+\sqrt{3}$	$\frac{1+\sqrt{5}}{2}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$

§3.1 Interludium: Kettenbrüche

Definition 3.1.1
Es seien $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_m \in \mathbb{N}_+$, $m \in \mathbb{N} \cup \{\infty\}$. Dann ist $[a_0; a_1, \ldots, a_m]$ der **Kettenbruch**

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{}{a_{m-2} + \cfrac{1}{a_{m-1} + \cfrac{1}{a_m}}}}}.$$

Zu einem Kettenbruch $[a_0; a_1, \ldots, a_m]$ und $m \geq n \in \mathbb{N}$ heißt

$$\frac{p_n}{q_n} := [a_0; a_1, \ldots, a_n]$$

der n-te **Näherungsbruch**, wobei $p_n, q_n \in \mathbb{Z}$, $q_n > 0$ und $\mathrm{ggT}(p_n, q_n) = 1$.

Fakt 3.1.2
Die Näherungsbrüche lassen sich induktiv berechnen als: $p_{-1} := 1$, $q_{-1} := 0$, $p_0 = a_0$, $q_0 := 1$,

$$p_n = a_n p_{n-1} + p_{n-2}, \qquad q_n = a_n q_{n-1} + q_{n-2}.$$

Es gilt $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$.

Beweis: induktiv □

Definition 3.1.3
Sei $x \in \mathbb{R}$. Definiere induktiv: $r_0 := x$, $a_n := \lfloor r_n \rfloor$, $r_{n+1} = \frac{1}{r_n - a_n}$. Dann ist $[a_0; a_1, a_2, \ldots]$ der zu x gehörige Kettenbruch. Sei weiter $\frac{p_n}{q_n}$ der n-te Näherungsbruch von $[a_0; a_1, a_2, \ldots]$. Dann ist $\frac{p_n}{q_n}$ der zu x gehörige n-te Näherungsbruch.

Fakt 3.1.4
Sei $x \in \mathbb{R}$ und $\frac{p_n}{q_n}$ der zu x gehörige n-te Näherungsbruch. Dann ist

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(r_{n+1}q_n + q_{n-1})}.$$

Beweis: induktiv □

Bemerkung 3.1.5
$x = [a_0; a_1, a_2, \ldots, a_{n-1}, r_n]$ (der Einfachheit halber lassen wir nun $r_n \in \mathbb{R}^\times$ zu).

Fakt 3.1.6
Der zu $x \in \mathbb{R}$ gehörige Kettenbruch konvergiert gegen x. Es ist $|q_n x - p_n| < |q_{n-1}x - p_{n-1}|$.

Beweis: leicht, q_n streng monoton steigend, $r_i \geq 1$. □

Satz 3.1.7 (beste rationale Approximation)
Sei $x \in \mathbb{R}$, $\frac{p_n}{q_n}$ zugehöriger Näherungsbruch. Für $n \geq 2$ und $p, q \in \mathbb{Z}$ mit $0 < q \leq q_n$, sowie $\frac{p}{q} \neq \frac{p_n}{q_n}$ ist $|q_n x - p_n| < |qx - p|$. Weiter ist jeder Bruch $\frac{p'}{q'}$ mit dieser Eigenschaft ein Näherungsbruch.

Fakt 3.1.8
Von zwei aufeinanderfolgenden Näherungsbrüchen von x erfüllt einer die Ungleichung $|x - \frac{p}{q}| < \frac{1}{2q^2}$.

Beweis: (Idee) $|x - \frac{p_n}{q_n}| + |x - \frac{p_{n+1}}{q_{n+1}}| = \frac{1}{q_n q_{n+1}}$. □

Satz 3.1.9
(LAGRANGE) Eine irrationale, reelle Zahl ist genau dann Nullstelle eines quadratischen Polynoms über $\mathbb{Q}$, wenn ihre Kettenbruchentwicklung periodisch ist.

Satz 3.1.10
(GALOIS) Die Kettenbruchentwicklung von x ist rein periodisch ($[\overline{a_0; a_1, \ldots, a_n}]$) genau dann, wenn $x > 1$ und für jede konjugierte Nullstelle $\overline{x}$ gilt $-1 > \overline{x} > 0$. Ist $x = [\overline{a_0; a_1, \ldots, a_n}]$, so ist $-\frac{1}{\overline{x}} = [\overline{a_n; a_{n-1}, \ldots, a_0}]$.

Fakt 3.1.11
Sei $d \in \mathbb{N}$ sqf, dann ist die Kettenbruchentwicklung $\sqrt{d} = [\lfloor\sqrt{d}\rfloor, \overline{\underbrace{a_1, a_2, \ldots, a_2, a_1}_{\text{Palindrom}}, 2\lfloor\sqrt{d}\rfloor}]$

§3.2 Interludium: PELLsche Gleichung

Sei $d \in \mathbb{N}$ sqf. Wir wollen die **PELLsche Gleichung** $x^2 - dy^2 = 1$ in $\mathbb{Z}^2$ lösen.

Lemma 3.2.1
Seien r_n die Reste der Kettenbruchentwicklung von $\sqrt{d}$. Dann existieren $P_n, Q_n \in \mathbb{Z}$ mit $r_n = \frac{P_n + \sqrt{d}}{Q_n}$, $d - P_n^2 \equiv 0 \pmod{Q_n}$ und für $n \geq 2$ $p_{n-1}^2 - dq_{n-1}^2 = (-1)^n Q_n$, wobei $\frac{p_n}{q_n}$ der n-te Näherungsbruch von $\sqrt{2}$ ist.

Beweis (Skizze):

Induktiv P_n, Q_n richtig definieren, $r_0 = \frac{0+\sqrt{d}}{1}, r_1, \ldots$ + Kongruenz. Letzte Gleichung folgt aus $\sqrt{d} = \frac{r_n p_{n-1}+p_{n-2}}{r_n q_{n-1}+q_{n-2}}$. □

Satz 3.2.2
Die minimale positive Lösung der PELLschen Gleichung ist gegeben durch

$$(x_1, y_1) = \begin{cases} (p_{l-1}, q_{l-1}) & l \text{ gerade} \\ (p_{2l-1}, q_{2l-1}) & l \text{ ungerade} \end{cases},$$

wobei $\frac{p_n}{q_n}$ der n-te Näherungsbruch von $\sqrt{d}$ ist und l die Periodenlänge der Kettenbruchentwicklung ist. Alle weiteren Lösungen ergeben sich als

$$x_k + \sqrt{d}y_k = \pm(x_1 + \sqrt{d}y_1)^k, \qquad k \in \mathbb{Z}.$$

Aufgabe 32) Die Schlacht von Hastings (14.10.1066) [NEUKIRCH p. 46]

Harolds Mannen standen nach alter Gewohnheit dichtgedrängt in 13 gleichgroßen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx einbrechen zu wollen. ... Als aber Harold selbst auf dem Schlachtfeld erschien, formten die Sachsen ein einziges gewaltiges Quadrat mit ihrem König an der Spitze und stürmten mit den Schlachtrufen „Ut!", „Olicrosse!", „Godemite!" vorwärts. ... (vgl. „Carmen de Hastingae Proeho" von Guy, Bischof von Amiens).

Frage: Wie groß soll die Armee Harolds II. gewesen sein?

Lösung: Wir haben 13 Quadrate von jeweils y^2 Soldaten. Das Quadrat x^2 aller Soldaten zusammen mit Herold II., ergibt sich folglich als $x^2 = 13y^2 + 1$, was die PELLsche Gleichung

$$x^2 - 13y^2 = 1$$

liefert. Zur Lösung berechnen wir den Kettenbruch zu $\sqrt{13}$:

$$\begin{aligned}
\lfloor\sqrt{13}\rfloor &= 3 \\
\tfrac{1}{\sqrt{13}-3} &= \tfrac{3+\sqrt{13}}{4} \\
\lfloor\tfrac{3+\sqrt{13}}{4}\rfloor &= 1 \\
\tfrac{1}{\frac{\sqrt{13}+3}{4}-1} &= \tfrac{4}{\sqrt{13}-1} = \tfrac{4+4\sqrt{13}}{12} = \tfrac{1+\sqrt{13}}{3} \\
\lfloor\tfrac{1+\sqrt{13}}{3}\rfloor &= 1 \\
\tfrac{1}{\frac{1+\sqrt{13}}{3}-1} &= \tfrac{3}{\sqrt{13}-2} = \tfrac{6+3\sqrt{13}}{9} = \tfrac{2+\sqrt{13}}{3} \\
\lfloor\tfrac{2+\sqrt{13}}{3}\rfloor &= 1 \\
\tfrac{1}{\frac{2+\sqrt{13}}{3}-1} &= \tfrac{3}{\sqrt{13}-1} = \tfrac{3+3\sqrt{13}}{12} = \tfrac{1+\sqrt{13}}{4} \\
\lfloor\tfrac{1+\sqrt{13}}{4}\rfloor &= 1 \\
\tfrac{1}{\frac{1+\sqrt{13}}{4}-1} &= \tfrac{4}{\sqrt{13}-3} = \tfrac{12+4\sqrt{13}}{4} = 3+\sqrt{13} \\
\lfloor 3+\sqrt{13}\rfloor &= 6 \\
\tfrac{1}{3+\sqrt{13}-6} &= \tfrac{3+\sqrt{13}}{4} \qquad \text{(Periode)}
\end{aligned}$$

Also

$$\sqrt{13} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}}}}}$$

beziehungsweise $\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}]$.

Also ist die Periodenlänge $l = 5$ ungerade und damit der $(2l-1)$-te Näherungsbruch von Interesse. Nach Induktionsschema:

i	-1	0	1	2	3	4	5	6	7	8	9
a_i	$-$	3	1	1	1	1	6	1	1	1	1
p_i	1	3	4	7	11	18	115	133	248	381	629
q_i	0	1	1	2	3	5	33	38	71	109	180

Damit folgt: $629^2 - 13 \cdot 180^2 = 1$ und die Armee war, exklusive Herold II., $13 \cdot 180^2 = 421200$ Mann stark.

Aufgabe 32) Berechnen Sie die Fundamentaleinheiten von $K = \mathbb{Q}(\sqrt{d})$ für

(a) $d = 2010$,

(b) $d = 2012$,

(c) $d = 31$,

(d) $d = 46$ und

(e) $d = 71$.

(f) Warum wird nicht $d = 2011$ verlangt?

Lösung: Für jede Einheit $\varepsilon \in \mathcal{O}_K$ ist $\mathrm{N}(\varepsilon) \in \{-1, 1\}$. Für $d \equiv 2, 3 \pmod 4$ hat ε die Form $\varepsilon = a + b\sqrt{d}$, also $\mathrm{N}(\varepsilon) = a^2 - db^2 = \pm 1$. Ist $\mathrm{N}(\varepsilon) = -1$, so ist $\mathrm{N}(\varepsilon^2) = \mathrm{N}(\varepsilon)^2 = 1$. Wir können uns also zunächst auf den $+1$-Fall konzentrieren. Diese PELLsche Gleichung können wir mit Kettenbruchentwicklung lösen. Eine Lösung für den -1-Fall, falls existent, ist dann zu bevorzugen (weil sie die $+1$-Lösung erzeugt) und fällt automatisch bei der Berechnung ab.

(a) Wir entwickeln $\sqrt{2010}$:

$$\begin{aligned}
\sqrt{2010} &= 44 + (\sqrt{2010} - 44) \\
\tfrac{1}{-44+\sqrt{2010}} &= \tfrac{44+\sqrt{2010}}{2010-1936} = \tfrac{44+\sqrt{2010}}{74} = 1 + \tfrac{-30+\sqrt{2010}}{74} \\
\tfrac{74}{-30+\sqrt{2010}} &= \tfrac{74(30+\sqrt{2010})}{1110} = \tfrac{30+\sqrt{2010}}{15} = 4 + \tfrac{-30+\sqrt{2010}}{15} \\
\tfrac{15}{-30+\sqrt{2010}} &= \tfrac{15(30+\sqrt{2010})}{1110} = \tfrac{30+\sqrt{2010}}{74} = 1 + \tfrac{-44+\sqrt{2010}}{74} \\
\tfrac{74}{-44+\sqrt{2010}} &= \tfrac{74(44+\sqrt{2010})}{74} = 44 + \sqrt{2010} = 88 + (-44 + \sqrt{2010})
\end{aligned}$$

Das liefert $\sqrt{2010} = [44; \overline{1, 4, 1, 88}]$. Wegen Periode $l = 4$ gerade, ist der 3. Näherungsbruch von Interesse:

$$44 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1}}} = 44 + \cfrac{1}{1 + \cfrac{1}{5}} = 44 + \frac{5}{6} = \frac{269}{6}.$$

Also ist $269 + 6\sqrt{2010}$ Fundamentaleinheit.

(b) Es ist $\sqrt{2012} = [44; \overline{1, 5, 1, 10, 2, 1, 4, 22, 4, 1, 2, 10, 1, 5, 1, 88}]$. Also Periodenlänge $l = 16$ und wir betrachten den 15. Näherungsbruch. Wir verwenden das Iterationsschema:

i	p_i	q_i
0	44	1
1	45	1
2	269	6
3	314	7
4	3409	76
5	7132	159
6	10541	235
7	49296	1099
8	1095053	24413
9	4429508	98751
10	5524561	123164
11	15478630	345079
12	160310861	3573954
13	175789491	3919033
14	1039258316	23169119
15	1215047807	27088152

Also ist $1215047807 + 27088152\sqrt{2012}$ Fundamentaleinheit.

(c) $\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$, $l = 8$.

i	p_i	q_i
0	5	1
1	6	1
2	11	2
3	39	7
4	206	37
5	657	118
6	863	155
7	1520	273

Also $1520 + 273\sqrt{31}$ Fundamentaleinheit.

(d) $\sqrt{46} = [6; \overline{1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12}]$, $l = 12$.

i	p_i	q_i
0	6	1
1	7	1
2	27	4
3	34	5
4	61	9
5	156	23
6	997	147
7	2150	317
8	3147	464
9	5297	781
10	19038	2807
11	24335	3588

Also $24335 + 3588\sqrt{46}$ Fundamentaleinheit.

(e) $\sqrt{71} = [8; \overline{2, 2, 1, 7, 1, 2, 2, 16}]$, $l = 8$.

i	p_i	q_i
0	8	1
1	17	2
2	42	5
3	59	7
4	455	54
5	514	61
6	1483	176
7	3480	413

Also $3480 + 413\sqrt{71}$ Fundamentaleinheit.

(f) Die Kettenbruchentwicklung von $\sqrt{2011}$ hat eine Periode der Länge 96. Wir kennen im Moment kein Verfahren um dies leicht zu erkennen. Man kennt die obere Schranke $l \leq 2d$.

Aufgabe 32) Sei $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sqf. Sei $\mathfrak{p} \subset \mathcal{O}_K$ maximales Ideal. Zeigen Sie, dass $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl $p \in \mathbb{P}$ ist und $\mathbb{N}\mathfrak{p} \in \{p, p^2\}$.

Lösung: Jedes $\mathfrak{p}$ enthält orthodoxe ganze Zahlen für $x \in \mathfrak{p}$ zum Beispiel $\mathrm{N}\, x$. Also ist $\mathfrak{p} \cap \mathbb{Z} = (n)$ mit $n \in \mathbb{N}_+$, da $\mathbb{Z}$ HIR ($n \neq 1$, denn sonst $1 \in \mathfrak{p}$). Nach dem Homomorphiesatz hat man den Monomorphismus (inj.)

$$\mathbb{Z}/(n) \hookrightarrow \mathcal{O}_K/\mathfrak{p}$$

(via $\mathbb{Z} \hookrightarrow \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$), wobei das Ziel ein Körper ist (da $\mathfrak{p}$ maximal). Also ist $\mathbb{Z}/(n)$ integer, mithin $n \in \mathbb{P}$.

Somit haben wir $p\mathcal{O}_K \subset \mathfrak{p} \subsetneq \mathcal{O}_K$. Weiter ist $\mathbb{N}(p\mathcal{O}_K) = p^2$ ($\mathcal{O}_K$ ist Gitter), da K quadratischer ZK. $\Rightarrow \mathbb{N}\mathfrak{p} \mid p^2$ und $\mathbb{N}\mathfrak{p} \neq 1$.

Aufgabe 32) Sei $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sqf. Zeigen Sie, dass für $p \in \mathbb{P}$ genau einer der folgenden Fälle auftritt:

(a) $p\mathcal{O}_K$ ist prim in $\mathcal{O}_K$ (p träge),

(b) $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ mit $\mathfrak{p} \neq \mathfrak{p}'$ (p zerlegt),

(c) $p\mathcal{O}_K = \mathfrak{p}^2$ (p verzweigt).

Lösung: Im DEDEKIND-Ring haben wir eine Primidealzerlegung: $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$ und damit $p^2 = \mathbb{N}(\mathcal{O}_K) = \mathbb{N}(\mathfrak{p}_1) \cdot \ldots \cdot \mathbb{N}(\mathfrak{p}_n)$. Es folgt $n \leq 2$ und es ergeben sich die 3 Fälle.

Aufgabe 32) Sei $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sqf, $p \in \mathbb{P}$. Zeigen Sie:

(a) p träge $\Leftrightarrow \mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_{p^2}$,

(b) p zerlegt $\Leftrightarrow \mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_p \oplus \mathbb{F}_p$,

(c) p verzweigt $\Leftrightarrow \mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_p[T]/(T^2)$.

Lösung:

(a) $\mathcal{O}_K/p\mathcal{O}_K$ ist Körper $\Leftrightarrow p\mathcal{O}_K$ ist maximales Ideal $\Leftrightarrow p$ ist träge. Weiter hat $\mathcal{O}_K/p\mathcal{O}_K$ p^2 Elemente.

(b) „$\Rightarrow$“ p zerlegt, also $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. Chinesischer Restsatz:

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1 \oplus \mathcal{O}_K/\mathfrak{p}_2 \cong \mathfrak{p} \oplus \mathfrak{p}$$

„$\Leftarrow$“ $\mathcal{O}_K/p\mathcal{O}_K$ ist kein Körper, also p entwerder zerlegt oder verzweigt. Falls p verzweigt ist, so enthält $\mathcal{O}_K/p\mathcal{O}_K = \mathcal{O}_K/\mathfrak{p}^2$ nilpotente Elemente (aus $\mathfrak{p} \setminus \mathfrak{p}^2$), aber in $\mathbb{F}_p \oplus \mathbb{F}_p$ gibt es solche nicht.

(c) „$\Leftarrow$“ $\mathbb{F}_p[T]/(T^2)$ enthält nilpotente Elemente, also nach obiger Ausführung p verzweigt.

„$\Rightarrow$“ Es sei $p\mathcal{O}_K = \mathfrak{p}^2$ und $x \in \mathfrak{p} \setminus \mathfrak{p}^2$, sowie $\overline{x}$ das Bild von x in $\mathcal{O}_K/p\mathcal{O}_K$. Betrachte die Abbildung $\mathfrak{p}[T] \to \mathcal{O}_K/p\mathcal{O}_K$: $T \mapsto \overline{x}$. Dies ist ein surjektiver Homomorphismus und liefert die Isomorphie $\mathbb{F}_p[T]/\ker \cong \mathcal{O}_K/p\mathcal{O}_K$. Der Kern enthält (T^2) und kann nicht größer sein, da (T^2) Index p^2 hat.

Aufgabe 32) Sei $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sqf, $p \in \mathbb{P}$. Zeigen Sie: $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_p[T]/(f_p(T))$ mit

$$f_p(T) = \begin{cases} T^2 - d & d \equiv 2,3 \pmod 4 \\ T^2 - T - \frac{d-1}{4} & d \equiv 1 \pmod 4 \end{cases}.$$

Lösung: Sei $\omega = \sqrt{d}$ für $d \equiv 2,3 \pmod 4$, bzw. $\omega = \frac{1+\sqrt{d}}{2}$ für $d \equiv 1 \pmod 4$ aus der bekannten Ganzheitsbasis von $\mathcal{O}_K$ und $\overline{\omega}$ das Bild in $\mathcal{O}_K/p\mathcal{O}_K$. Sei weiter $f(T) = (T-\omega)(T-\sigma\omega)$ das Minimalpolynom von ω in $\mathbb{Q}[T]$ ($\sigma \in \mathrm{Gal}(K/\mathbb{Q})$) und f_p die Projektion nach $\mathbb{F}_p[T]$. Damit enthält der Kern des surjektiven Homomorphismus $\mathbb{F}_p[T] \to \mathcal{O}_K/p\mathcal{O}_K$: $T \to \overline{\omega}$ nun (f_p) mit Index p^2. Also $\mathbb{F}_p[T]/(f_p) \cong \mathcal{O}_K/p\mathcal{O}_K$. Weiter ist f_p wie gewünscht.

Aufgabe 32) Sei $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sqf, $p \in \mathbb{P}$. Zeigen Sie für $p > 2$:

(a) p träge $\Leftrightarrow p \nmid d_K$ und d_K ist kein Quadrat in $\mathbb{F}_p^\times$,

(b) p zerlegt $\Leftrightarrow p \nmid d_K$ und d_K ist Quadrat in $\mathbb{F}_p^\times$,

(c) p verzweigt $\Leftrightarrow p \mid d_K$.

Wie sieht es im Fall $p = 2$ aus?

Lösung: Sei $p > 2$. Wir verwenden die Ergebnisse und Bezeichnungen der vorherigen Aufgaben.

(a) p träge $\Leftrightarrow \mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_{p^2} \Leftrightarrow f_p$ irreduzibel $\Leftrightarrow p \nmid d_K$ und d_K kein Quadrat modulo p, denn sonst: $p \mid d_K \Rightarrow f_p = T^2$ ($d \equiv 2,3 \pmod 4$) bzw. $(T-\frac{1}{2})^2$ ($d \equiv 1 \pmod 4$); oder d_K Quadrat modulo $p \Rightarrow f_p = (T - \frac{\sqrt{d_K}}{2})(T + \frac{\sqrt{d_K}}{2})$, bzw. $f_p = (T - \frac{1+\sqrt{d_K}}{2})(T - \frac{1-\sqrt{d_K}}{2})$.

(b) $p \nmid d_K$ und d_K ist Quadrat in $\mathbb{F}_p^\times \Leftrightarrow f_p$ zerfällt in 2 verschiedene Faktoren $\Leftrightarrow \mathbb{F}_p[T]/(f_p) = \mathbb{F}_p \oplus \mathbb{F}_p \Leftrightarrow p$ zerlegt.

(c) $p \mid d_K \Leftrightarrow f_p = T^2$ bzw. $(T-\frac{1}{2})^2 \Leftrightarrow p$ verzweigt.

Sei nun $p = 2$. Im Fall $d \equiv 2,3 \pmod 4$ ist $f_2(T) = T^2 - d = T^2$ oder $= T^2 - 1 = (T-1)^2$. $\Rightarrow 2$ verzweigt. Im Fall $d \equiv 1 \pmod 4$ ist

$$f_2(T) = T^2 + T + \frac{1-d}{4} = \begin{cases} T^2+T & \Rightarrow 2 \text{ zerlegt} \quad d \equiv 1 \pmod 8 \\ T^2+T+1 & \Rightarrow 2 \text{ träge} \quad d \equiv 5 \pmod 8 \end{cases}.$$

Aufgabe 32) Sei $2 < p \in \mathbb{P}$. Das LEGENDRE-Symbol $\left(\frac{\cdot}{p}\right)$:$\mathbb{Z} \to \{0, \pm 1\}$ ist definiert durch:

$$\left(\frac{m}{p}\right) := \begin{cases} 0 & p \mid m \\ +1 & m \text{ ist Quadrat in } \mathbb{F}_p^\times \\ -1 & m \text{ ist kein Quadrat in } \mathbb{F}_p^\times \end{cases}.$$

Zeigen Sie:

(a) $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$

(b) $\left(\frac{x}{p}\right) \equiv x^{(p-1)/2} \pmod p$

(c) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

(d) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Lösung: Offensich impliziert (ii) die Punkte (i) und (iii). Wir zeigen (ii): Sei ζ ein Erzeuger der zyklischen Gruppe $\mathbb{F}_p^\times$. Diese hat $p-1$ Elemente, $\zeta, \zeta^2, \ldots, \zeta^{p-1} = 1$. Quadrieren dieser Liste liefert die Quadrate ζ^{2n}. Also für $p \nmid x$ (sonst trivial) ist

$$\left(\frac{x}{p}\right) = \left(\frac{\zeta^{n_x}}{p}\right) = (-1)^{n_x} \equiv (\zeta^{(p-1)/2})^{n_x} \equiv (\zeta^{n_x})^{(p-1)/2} \equiv x^{(p-1)/2} \pmod p.$$

(iv): In $\mathbb{Z}[i]$ haben wir die folgenden 2 Identitäten:

$$(1+i)^p \equiv 1 + i^p \pmod p$$

$$(1+i)^p \equiv (1+i)((1+i)^2)^{(p-1)/2} \equiv (1+i)(2i)^{(p-1)/2} \pmod p$$

Also $(1+i)\left(\frac{2}{p}\right) i^{(p-1)/2} \equiv (1+i)2^{(p-1)/2} i^{(p-1)/2} \equiv 1 + i^p \equiv 1 + i(-1)^{(p-1)/2} \pmod p$. Wir erhalten:

$$\left(\frac{2}{p}\right) i^{(p-1)/2} + \left(\frac{2}{p}\right) i^{(p+1)/2} \equiv 1 + i(-1)^{(p-1)/2} \pmod p$$

Koeffizientenvergleich:

Fall 1: $(p \equiv 1 \pmod 4)$

$$\left(\frac{2}{p}\right) i^{(p-1)/2} \equiv 1 \pmod p \Rightarrow \left(\frac{2}{p}\right) = (-1)^{(p-1)/4}$$

Fall 2: $(p \equiv 3 \pmod 4)$

$$\left(\frac{2}{p}\right) i^{(p+1)/2} \equiv 1 \pmod p \Rightarrow \left(\frac{2}{p}\right) = (-1)^{(p+1)/4}$$

Insgesamt:

$$\left(\frac{2}{p}\right) \equiv \begin{cases} +1 & p \equiv 1, 7 \pmod 8 \\ -1 & p \equiv 3, 5 \pmod 8 \end{cases},$$

was genau dem Verhalten von $(-1)^{(p^2-1)/8}$ in Abhängigkeit von p modulo 8 entspricht.

Aufgabe 32) Zeigen Sie für $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sqf:

(a) p träge $\Leftrightarrow \left(\frac{d_K}{p}\right) = -1$,

(b) p zerlegt $\Leftrightarrow \left(\frac{d_K}{p}\right) = 1$,

(c) p verzweigt $\Leftrightarrow \left(\frac{d_K}{p}\right) = 0$.

Lösung: Mit den Ergebnissen der vorherigen Aufgaben folgt das sofort:

(a) p träge $\Leftrightarrow p \nmid d_K$, d_K kein Quadrat in $\mathbb{F}_p^\times$ $\Leftrightarrow \left(\frac{d_K}{p}\right) = -1$,

(b) p zerlegt $\Leftrightarrow p \nmid d_K$, d_K ist Quadrat in $\mathbb{F}_p^\times$ $\Leftrightarrow \left(\frac{d_K}{p}\right) = 1$,

(c) p verzweigt $\Leftrightarrow p \mid d_K$ $\Leftrightarrow \left(\frac{d_K}{p}\right) = 0$.

Aufgabe 32) Beweisen Sie das quadratische Reziprozitätsgesetz: Für $p, q \in \mathbb{P} \setminus 2$, $p \neq q$ gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Lösung: Wir nutzen die GAUSSschen Summen. Wir arbeiten in $\mathbb{Z}[\zeta_q]$, $\zeta_q = e^{2\pi i/q}$. Sei $G = \sum_{x \in \mathbb{F}_q^\times} \left(\frac{x}{q}\right) \zeta_q^x$ (GAUSSsche Summe). Dann ist $G^2 = \sum_{x,y \in \mathbb{F}_q^\times} \left(\frac{xy}{q}\right) \zeta_q^{x+y}$. Die Substitution $y = tx$ liefert

$$G^2 = \sum_{x,t \in \mathbb{F}_q^\times} \left(\frac{tx^2}{q}\right) \zeta_q^{x(1+t)} = \sum_{t \in \mathbb{F}_q^\times} \left(\frac{t}{q}\right) \sum_{x \in \mathbb{F}_q^\times} \zeta_q^{x(1+t)}.$$

Die innere Summe ist $q-1$ für $t = -1$ und -1 sonst (die n-ten Einheitswurzeln summieren sich zu 0). Also

$$G^2 = \underbrace{-\sum_{t \in \mathbb{F}_q^\times} \left(\frac{t}{q}\right)}_{=0} + q\left(\frac{-1}{q}\right) = q(-1)^{(q-1)/2}.$$

Jetzt erhalten wir wiederum 2 Identitäten:

$$\begin{aligned} G^p &\equiv G(G^2)^{(p-1)/2} \equiv G(q\cdot(-1)^{(q-1)/2})^{(p-1)/2} \\ &\equiv G\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod p \\ G^p &\equiv \sum_{x\in\mathbb{F}_q^\times}\left(\frac{x}{q}\right)^p \zeta_q^{px} = \sum_{x\in\mathbb{F}_q^\times}\left(\frac{xp^2}{q}\right)\zeta_q^{px} = \left(\frac{p}{q}\right)\sum_{x\in\mathbb{F}_q^\times}\left(\frac{px}{q}\right)\zeta_q^{px} \\ &\equiv \left(\frac{p}{q}\right) G \pmod p \end{aligned}$$

Es folgt: $\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod p$, da G nicht verschwindet ($G^2 \neq 0$). Somit folgt die Behauptung.

Aufgabe 32) Sei $p \in \mathbb{P}$ unverzweigt in $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ sqf. Zeigen Sie: Das Zerlegungsverhalten von p hängt nur von $p \pmod{4|d_K|}$ ab.

Lösung: [unfertig] Es sei $|d_K| = 2^\varepsilon p_1 \cdot p_2 \cdot \ldots \cdot p_n$ mit $\varepsilon \in \{0,2,3\}$ (mehr nicht möglich, wegen d sqf) und paarweise verschiedenen Primzahlen $p_1,\ldots,p_n$. Nach einer der vorhergehenden Aufgaben, genügt es $\left(\frac{d_K}{p}\right)$ zu betrachten, um zwischen p träge und p zerlegt zu unterscheiden.

$$\left(\frac{d_K}{p}\right) = \left(\frac{2}{p}\right)^\varepsilon \prod_i \left(\frac{p_i}{p}\right) = \left(\frac{2}{p}\right)^\varepsilon \prod_i (-1)^{\frac{p-1}{2}\frac{p_i-1}{2}} \left(\frac{p}{p_i}\right)$$

- $\left(\frac{p}{p_i}\right)$ hängt nur von $p \pmod{p_i}$
- $\prod_i (-1)^{\frac{p-1}{2}\frac{p_i-1}{2}} = \left((-1)^{(p-1)/2}\right)^n (-1)^{\varepsilon\frac{p_i-1}{2}}$, n von $p \pmod 4$ abhängig
- $\left(\frac{2}{p}\right)^\varepsilon$ konstant, falls $\varepsilon = 0,2$; für $\varepsilon = 3$ folgt $\left(\frac{2}{p}\right)^\varepsilon = \left(\frac{2}{p}\right)$, also abhängig von $p \pmod 8$.

Aufgabe 32) Zeigen Sie, dass

$$\left|\frac{f(T)}{g(T)}\right| := c^{\deg g - \deg f}, \qquad 0 < c < 1,$$

eine Bewertung auf $K = k(T)$ (k Körper) definiert. Diese ist diskret und nichtarchimedisch. Welches ist die zugehörige Exponentenbewertung?

Lösung:

(a) $|ab| = |a||b|$

(b) $|a| = 0 \Leftrightarrow a = 0$

(c) $|a+b| \leq \max(|a|,|b|)$

(d) $\deg g - \deg f \in \mathbb{Z} \cup \{\infty\}$

Bemerkung: $\deg 0 = -\infty$, dann folgt (ii) und (iv). Zu (i):

$$\left|\frac{f(T)}{g(T)}\cdot\frac{\varphi(T)}{\gamma(T)}\right| = c^{\deg g\gamma - \deg f\varphi} = c^{\deg g + \deg\gamma - \deg f - \deg\varphi} = \left|\frac{f(T)}{g(T)}\right|\left|\frac{\varphi(T)}{\gamma(T)}\right|$$

Zu (iii): Es ist $\deg(f\gamma + g\varphi) \leq \max(\deg f\gamma, \deg g\varphi)$. Damit:

$$\begin{aligned}
\left|\frac{f(T)}{g(T)} + \frac{\varphi(T)}{\gamma(T)}\right| &= \left|\frac{f\gamma(T) + g\varphi(T)}{g\gamma(T)}\right| \\
&= c^{\deg g\gamma - \deg(f\gamma + g\varphi)} \\
&\leq c^{\deg g\gamma - \max(\deg f\gamma, \deg g\varphi)} \qquad (\text{wg.} c < 1) \\
&= c^{\min(\deg g\gamma - \deg f\gamma, \deg g\gamma - \deg g\varphi)} \\
&= \max\left(\left|\frac{f\gamma(T)}{g\gamma(T)}\right|, \left|\frac{g\varphi(T)}{g\gamma(T)}\right|\right) \\
&= \max\left(\left|\frac{f(T)}{g(T)}\right|, \left|\frac{\varphi(T)}{\gamma(T)}\right|\right)
\end{aligned}$$

Aufgabe 32) Sei $|\cdot|$ eine nichtarchimedische Bewertung des Körpers K und $\mathbb{D}(a,r)$ die offene Kugel um $a \in K$ mit Radius $r > 0$:

$$\mathbb{D}(a,r) = \{x \in K : |x - a| < r\}$$

Zeigen Sie:

(a) Ist $b \in \mathbb{D}(a,r)$, so ist $\mathbb{D}(b,r) = \mathbb{D}(a,r)$.

(b) Ist $\mathbb{D}(a,r) \cap \mathbb{D}(b,s) \neq \emptyset$ und $r \leq s$, so folgt $\mathbb{D}(a,r) \subset \mathbb{D}(b,s)$.

Lösung:

(a) Sei $x \in \mathbb{D}(a,r)$, so ist $|x - b| = |x - a + a - b| \leq \max(|x - a|, |a - b|) \leq r$ $\Rightarrow x \in \mathbb{D}(b,r)$ $\Rightarrow \mathbb{D}(a,r) \subset \mathbb{D}(b,r)$. Andere Inklusion analog.

(b) Es gibt $c \in \mathbb{D}(a,r) \cap \mathbb{D}(b,s)$. $\Rightarrow \mathbb{D}(a,r) = \mathbb{D}(c,r)$ und $\mathbb{D}(b,s) = \mathbb{D}(c,s)$. Mit $\mathbb{D}(c,r) \subset \mathbb{D}(c,s)$ folgt die Aussage.

Aufgabe 32) Sei K vollständig bezüglich der nichtarchimedischen Bewertung $|\cdot|$ und (a_k) Folge in K. Zeigen Sie: $\sum a_k$ konvergiert genau dann, wenn $a_k \to 0$. Geben Sie eine Formel für den Konvergenzradius an. Was passiert auf dem Rand?

Lösung: Da K vollständig ist, konvergiert eine Folge genau dann, wenn sie eine CAUCHY-Folge ist. Wir erhalten:

$$\begin{aligned}
&\sum a_k \text{ konvergiert} \\
\Leftrightarrow\ &\forall \varepsilon > 0 \exists N \forall n \geq m > N : \quad \underbrace{|\sum_{m}^{n} a_k|}_{=\max(|a_k| : m \leq k \leq n)} < \varepsilon \\
\Leftrightarrow\ &\forall \varepsilon > 0 \exists N \forall k \geq N : |a_k| < \varepsilon \\
\Leftrightarrow\ &a_k \to 0
\end{aligned}$$

Für den Konvergenzradius betrachten wir Potenzreihen der Form $f(X) = \sum_0^\infty a_k X^k$. Die Frage ist, für welche x diese Reihe konvergiert. Nach obiger Betrachtung ist das genau dann der Fall, wenn $a_k x^k \to 0$. Nun geht $|a_k x^k| = |a_k||x|^k$ genau dann gegen Null, wenn

$$|x| < \frac{1}{\limsup |a_k|^{1/k}} =: r \text{ (Konvergenzradius)} :$$

Sei $|x| = (1-\varepsilon)r$, dann sei N so, dass $|a_k|^{1/k} < \frac{1}{r}\frac{1}{1-\varepsilon/2}$ für alle $k > N$. Wir erhalten:

$$\begin{aligned} 0 \leq \lim |a_k x^k| &= \lim(|a_k|^{1/k}|x|)^k \\ &\leq \lim \left(\frac{1}{r}\frac{1}{1-\varepsilon/2} r(1-\varepsilon)\right)^k \\ &= \lim \left(\frac{1-\varepsilon}{1-\varepsilon/2}\right)^k \\ &= 0 \end{aligned}$$

Umgekehrt divergiert die Reihe für $|x| = (1+\varepsilon)r$. Zum Rand: Sei $|x| = r$. Ist $r = 0$ konvergiert die Reihe nur für $x = 0$, ist $r = \infty$ konvergiert die Reihe für alle $x \in K$. Sei $0 < r < \infty$. Nun ist $\lim |a_k x^k| = \lim |a_k| r^k$. Also konvergiert die Reihe genau dann auf dem Rand, wenn $\lim |a_k| r^k = 0$.

Aufgabe 32) Sei K ein bewerteter Körper. Zeigen Sie die Stetigkeit der Addition, Multiplikation und Reziprokenbildung.

Lösung: Wir benötigen $|(x,y)| \geq |x|, |y|$. Sei $\varepsilon > 0$. Wir konstruieren ein $\delta > 0$ mit $|(x,y) - (x',y')| < \delta \Rightarrow |(x+y) - (x'+y')| < \varepsilon$:

$|(x+y)-(x'+y')| = |(x-x')+(y-y')| \leq |x-x'|+|y-y'| \leq 2\max(|x-x'|, |y-y'|) \leq 2|(x-x', y-y')| < 2\delta := \varepsilon$. Also genügt $\delta := \varepsilon/2$.

Rest analog.

Aufgabe 32) Zeigen Sie, dass mit $|\cdot|$ auch $|\cdot|^s$, $0 < s \leq 1$, eine Bewertung ist.

Lösung: Nichttrivial ist nur die Dreiecksungleichung $a \leq b+c \Rightarrow a^s \leq b^s + c^s$: Sicher ist $a^s \leq (b+c)^s$, also zeigen wir $(b+c)^s \leq b^s + c^s$. Nun ist $(1+x)^s \leq 1+x^s$ für $x > 0$, da für $f(x) = (1+x)^s - 1 - x^s$ gilt: $f(0) = 0$ und $f'(x) = s(1+x)^{s-1} - sx^{s-1} < 0$. Setze $x = c/b$ und erhalte

$$\left(1 + \frac{c}{b}\right)^s \leq 1 + \frac{c^s}{b^s} \Rightarrow (b+c)^s \leq b^s + c^s.$$

Aufgabe 32) Zeigen Sie die Nichtäquivalenz von $|\cdot|_p$ und $|\cdot|_q$ auf $\mathbb{Q}$, für zwei verschiedene Primzahlen p, q.

Lösung: Es ist $|p^k|_p \overset{k\to\inf}{\longrightarrow} 0$, aber $|p^k|_q = 1$ für alle $k \in \mathbb{N}$.

Aufgabe 32) Zeigen Sie $\lim_{n\to\infty} \frac{x^n}{n!} = 0$, $x \in \mathbb{Q}$, genau dann, wenn $\mathrm{ord}_p(x) \geq 1$ für $2 < p \in \mathbb{P}$, bzw. $\mathrm{ord}_2(x) \geq 2$.

Lösung: Es ist $\mathrm{ord}_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \ldots$. Dies stellen wir in Termen der p-adischen Quersumme dar: Sei $n = a_0 + a_1 p + \ldots + a_k p^k$ ($a_i \in \{0, 1, \ldots, p-1\}$).

Dann ist

$$\begin{aligned}
\lfloor \frac{n}{p} \rfloor &= a_1 + a_2 p + \ldots + a_k p^k \\
\lfloor \frac{n}{p^2} \rfloor &= \quad + a_2 \ + \ldots + a_k p^{k-1} \\
&\vdots \\
\lfloor \frac{n}{p^k} \rfloor &= \qquad\qquad\qquad a_k
\end{aligned}$$

$$\begin{aligned}
\Rightarrow \operatorname{ord}_p(n!) &= a_1 + (1+p)a_2 + \ldots + (1+p+\ldots+p^{k-1})a_k \\
&= \frac{1}{p-1}\left(a_1(p-1) + a_2(p^2-1) + \ldots + a_k(p^k-1)\right) \\
&= \frac{1}{p-1}(n - \sum_{i=0}^{k} a_i)
\end{aligned}$$

Also

$$\operatorname{ord}_p(n!) = \frac{n - s_p(n)}{p-1},$$

wobei s_p die p-adische Quersumme ist. Nun ist $\operatorname{ord}_p(\frac{x^n}{n!}) = n \operatorname{ord}_p(x) - \frac{n-s_p(n)}{p-1}$. Für $p > 2$ geht dies nun genau dann gegen Unendlich, wenn $\operatorname{ord}_p(x) > 0$, also ≥ 1. Für $p = 2$ haben wir sicher eine Nullfolge für $\operatorname{ord}_2(x) \geq 2$ und sicher keine für $\operatorname{ord}_2(x) \leq 0$. Für $\operatorname{ord}_2(x) = 1$ ist $\operatorname{ord}_2\left(\frac{x^n}{n!}\right) = n - \frac{n-s_2(n)}{2-1} = s_2(n)$. Dies nimmt unendlich oft den Wert 1 an, wir haben also keine Nullfolge.

Aufgabe 32) Zeigen Sie: $a = \sum_{n \gg -\infty}^{\infty} a_n p^n$, $0 \leq a_n < p$ ist rational genau dann, wenn die a_n ab einem gewissen Index periodisch sind.

Lösung: „⇐“ Sei

$$a = \sum_{n=k}^{l-1} a_n p^n + \underbrace{\sum_{i=0}^{\infty} \sum_{n} = l + mi^{l+m(i+1)-1} a_{n-mi} p^n}_{=:P=\text{periodischer Teil}}.$$

Es genügt zu zeigen, dass $P \in \mathbb{Q}$. Nun ist $P - Pp^m = \sum_{n=0}^{m-1} a_{n+l} p^{i+1} \in \mathbb{Q}$. Also auch $P \in \mathbb{Q}$.

„⇒“ Sei a rational. Es genügt zu zeigen, dass $p^m \cdot a$ eine periodische Entwicklung für geeignetes m hat. Also o.B.d.A. $a = \frac{q}{r}$, $\operatorname{ggT}(q,r) = 1$, $p \nmid q, r$. Wir wollen $\underbrace{\frac{p^m q - q}{r}}_{=p^m a - a} \in \mathbb{Z} \setminus \{0\}$.

$$\begin{aligned}
&\Leftrightarrow p^m q - q \equiv 0 \pmod r, m \neq 0 \\
&\Leftrightarrow p^m \equiv 1 \pmod r, m \neq 0 \qquad \text{(wegen } \operatorname{ggT}(q,r) = 1\text{)} \\
&\Leftrightarrow m = k \cdot \operatorname{ord}_r(p)
\end{aligned}$$

Zum Beispiel $m = \mathrm{ord}_r(p)$ (ex. wegen $\mathrm{ggT}(p, r) = 1$). Dann ist $p^m a - a \in \mathbb{Z} \setminus \{0\}$. Ist $a = \sum_{n=k}^{\infty} a_n p^n$, dann ist also $\sum_{n=k}^{\infty} a_n p^n - \sum_{n=k+m}^{\infty} a_{n-m} p^n \in \mathbb{Z} \setminus \{0\}$. Es ist entweder $p^m a - a$ oder $a - p^m a$ positiv, hat also endliche Darstellung. Also exisitert eine N_0, sodass für alle $n > N_0$ gilt: $a_n - a_{n+m} \equiv 0 \pmod{p}$. $\Rightarrow a$ hat periodische Entwicklung.

Aufgabe 32) Berechnen Sie die ersten 4 Ziffern der 7-adischen Darstellung von $\sqrt{2} \in \mathbb{Q}_7$.

Lösung: Wegen $|2|_7 = 1$, ist $|\sqrt{2}|_7 = 1$, also $\sqrt{2} \in \mathbb{Z}_7$, also von der Form

$$\sqrt{2} = a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + a_3 \cdot 7^3 + \dots.$$

Folglich

$$2 = a_0^2 + 2a_0a_1 \cdot 7 + (2a_0a_2 + a_1^2) \cdot 7^2 + 2(a_0a_3 + a_1a_2) \cdot 7^3.$$

Diese Gleichung lösen wir sukzessive durch durch Betrachtungen modulo 7^k.

$$\begin{aligned}
&2 \equiv a_0^2 \pmod{7} \\
\Rightarrow &\text{Wählen } a_0 := 3
\end{aligned}$$

$$\begin{aligned}
&2 \equiv a_0^2 + 2a_0a_1 \cdot 7 \pmod{7^2} \\
\Rightarrow &2 \equiv 9 + 6a_1 \cdot 7 \pmod{7^2} \\
\Rightarrow &0 \equiv 7 + 6a_1 \cdot 7 \pmod{7^2} \\
\Rightarrow &0 \equiv 1 + 6a_1 \pmod{7} \\
\Rightarrow &\text{Wählen } a_1 := 1
\end{aligned}$$

$$\begin{aligned}
&2 \equiv a_0^2 + 2a_0a_1 \cdot 7 + (2a_0a_2 + a_1^2) \cdot 7^2 \pmod{7^3} \\
\Rightarrow &0 \equiv 7 + 6 \cdot 7 + (6a_2 + 1) \cdot 7^2 \pmod{7^3} \\
\Rightarrow &0 \equiv (6a_2 + 2) \cdot 7^2 \pmod{7^3} \\
\Rightarrow &0 \equiv 6a_2 + 2 \pmod{7} \\
\Rightarrow &\text{Wählen } a_2 := 2
\end{aligned}$$

$$\begin{aligned}
&2 \equiv a_0^2 + 2a_0a_1 \cdot 7 + (2a_0a_2 + a_1^2) \cdot 7^2 + 2(a_0a_3 + a_1a_2) \cdot 7^3 \pmod{7^4} \\
\Rightarrow &0 \equiv 7^2 + 13 \cdot 7^2 + (6a_3 + 4) \cdot 7^3 \pmod{7^4} \\
\Rightarrow &0 \equiv (6a_3 + 6) \cdot 7^3 \pmod{7^4} \\
\Rightarrow &0 \equiv 6a_3 + 6 \pmod{7} \\
\Rightarrow &\text{Wählen } a_3 := 6
\end{aligned}$$

Insgesamt: $\sqrt{2} = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \dots$.

Aufgabe 32) Zeigen Sie: $a \in \mathbb{Q}_p^\times$ ist p-adische Einheit genau dann, wenn a für alle n prim zu $p(p-1)$ eine n-te Wurzel in $\mathbb{Q}_p$ besitzt.

Lösung: „$\Rightarrow$“ Sei $a \in \mathbb{Z}_p^\times$. Da n prim zu $p-1$ ist, existiert eine Lösung von $x^n \equiv a \pmod{p}$ mit $a \not\equiv 0 \pmod{p}$. Weiter ist n prim zu p, also ist für $f(T) = T^n - a$ nun $|f(x)| < 1$ und $|f'(x)| = |nx^{n-1}| = 1$. Nach HENSELs Lemma existiert also eine n-te Wurzel von a in $\mathbb{Z}_p$.

„⇐“ Sei a keine p-adische Einheit, also $a = p^m u$ mit $u \in \mathbb{Z}_p^\times$ und $m \in \mathbb{Z} \setminus \{0\}$. Jetzt kann a aber nur n-te Wurzeln besitzen, falls n den Exponenten m teilt. Das sind aber nicht alle Zahlen, die prim zu $p(p-1)$ sind.

Aufgabe 32) Zeigen Sie: $\mathbb{Q}_p$ besitzt nur einen Körperautomorphismus - die Identität.

Lösung: Zuerst bemerken wir, dass jeder Körperautomorphismus ϕ auf dem Unterkörper $\mathbb{Q}$ stets die Identität ist. Weiterhin ist $\mathbb{Q}$ dicht in $\mathbb{Q}_p$, womit es genügt die Stetigkeit von ϕ zu zeigen, damit $\phi = \mathrm{id}$. Nun besitzt a genau dann eine n-te Wurzel, wenn $\phi(a)$ dies tut, wegen Homomorphie und Bijektivität. Nach vorheriger Aufgabe ist $a \in \mathbb{Z}_p^\times \Leftrightarrow \phi(a) \in \mathbb{Z}_p^\times$. Nun ist $\mathbb{Z}_p = \bigcup_{n=0}^\infty p^n \mathbb{Z}_p^\times$ und $\phi(p^n \mathbb{Z}_p^\times) = p^n \mathbb{Z}_p^\times$, also insbesondere $\phi(p^n \mathbb{Z}_p) \subset p^n \mathbb{Z}_p \Rightarrow \phi$ stetig.

Aufgabe 32) Zeigen Sie: $\mathbb{R}$ besitzt nur einen Körperautomorphismus - die Identität.

Lösung: Analog zur vorherigen Aufgabe, reicht es die Stetigkeit eines beliebigen Körperautomorphismus ϕ nachzuweisen. Für $x > 0$ gibt es y mit $y^2 = x \Rightarrow \phi(x) = \phi(y)^2$, also $\phi(x) > 0$. Es folgt $x > 0 \Leftrightarrow \phi(x) > 0$. Seien $v, w \in \mathbb{R}$ mit $|v - w| < \varepsilon \in \mathbb{Q}$. Dann ist ohne Einschränkung $-\varepsilon < v - w < \varepsilon$, also auch $-\varepsilon < \phi(v) - \phi(w) < \varepsilon$, womit ϕ stetig.

Aufgabe 32) In welchen $\mathbb{Q}_p$ ist -1 ein Quadrat? In welchen 2?

Lösung: Zu -1: Sei $p > 2$. Dann ist -1 ein Quadrat modulo p genau dann, wenn $p \equiv 1 \pmod 4$: Benutze HENSELs Lemma um Wurzel von $T^2 + 1$ in $\mathbb{Z}_p$ zu finden. Für $p = 2$ reicht modulo p nicht (Ableitung ist $2T$). Wir stellen fest: $x^2 + 1 \equiv 0 \pmod 4$ besitzt keine Lösung. Antwort: $p \equiv 1 \pmod 4$.

Zu 2: Sei $p > 2$. Dann ist $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Also 2 Quadrat modulo p, wenn $p \equiv \pm 1 \pmod 8$. Wieder liefert HENSELs Lemma eine Wurzel in $\mathbb{Z}_p$. Für $p = 2$ besitzt analog $x^2 \equiv 2 \pmod 4$ keine Lösung. Antwort: $p \equiv \pm 1 \pmod 8$.

Aufgabe 32) TEICHMÜLLER-Repräsentanten: Zeigen Sie, dass die $(p-1)$-ten Einheitswurzeln in $\mathbb{Q}_p$ ein Repräsentantensystem für $\mathbb{F}_p^\times = (\mathbb{Z}_p / p\mathbb{Z}_p)^\times$ bilden.

Lösung: Wir betrachten das Polynom $f(T) = T^{p-1} - 1$ mit den $(p-1)$-ten Einheitswurzeln als verschiedenen Nullstellen. Dies besitzt modulo p die approximativen Nullstellen $1, 2, \ldots, p-1$. Nach HENSELs Lemma liegen die $(p-1)$-ten Einheitswurzeln also in $\mathbb{Z}_p$. Außerdem verteilen sie sich wie gewünscht in die Restklassen. $\mathbb{F}_p^\times = (\mathbb{Z}_p / p\mathbb{Z}_p)^\times$.

Aufgabe 32) Zeigen Sie, dass $\mathbb{C}$ unendlich viele Automorphismen hat, von denen genau 2 stetig sind.

Lösung: Sei T eine Transzendenzbasis für $\mathbb{C}/\mathbb{Q}$ (d.h. ein algebraisch unabhängiges System mit $\mathbb{C}/\mathbb{Q}(T)$ algebraisch und $\mathbb{Q}(T)/\mathbb{Q}$ transzendent). Nun verursacht jede Permutation von T, welche 1 fest lässt (ohne Einschränkung $1 \in T$) einen Automorphismus von $\mathbb{Q}(T)$. Dieser setzt sich (nicht notwendigerweise eindeutig) zu einem Automorphismus von $\mathbb{C}$ fort, da $\mathbb{C}$ der algebraische Abschluss von $\mathbb{Q}(T)$ ist (das zu zeigen ist nicht trivial). Somit ist $|\mathrm{Aut}(\mathbb{C})| = \infty$. Ist ϕ stetig, folgt $\phi|_{\mathbb{R}} = \mathrm{id}$, wegen $\phi|_{\mathbb{Q}} = \mathrm{id}$. Somit ist $\phi \in \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \bar{\cdot}\}$.

Aufgabe 32) Sei K ein lokaler Körper (= endliche Erweiterung von $\mathbb{Q}_p$) und $\mathbb{U}_K = \mathcal{O}_K^\times$ die Einheitengruppe, $\mathbb{U}_K^{(1)} = \{u \in \mathbb{U}_K : u \equiv 1 \pmod{\mathfrak{m}_K}\}$ die Einseinheitengruppe,

$\mathfrak{m}_K = (\pi_K)$, $q = (\mathcal{O}_K : \mathfrak{m}_K)$. Zeigen Sie:

$$K^\times = \langle \pi_K \rangle \times \mu_{q-1} \times \mathbb{U}_K^{(1)}.$$

Lösung: Es ist $K^\times = \langle \pi_K \rangle \mathbb{U}_K$ nach allgemeiner Theorie. Weiter haben wir $\mathcal{O}_K/\mathfrak{m}_K \cong \mathbb{F}_q$ und somit einen Homomorphismus $\mathbb{U}_K \to \mathbb{F}_q^\times$. Dieser hat den Kern $\mathbb{U}_K^{(1)}$. Weiter ist analog zur vorletzten Aufgabe $\mu_{q-1} \subset \mathbb{U}_K$. Damit folgt die Behauptung.

Aufgabe 32) Zeigen Sie, dass durch

$$\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

eine stetige Abbildung $\mathbb{U}_K^{(1)} \to K$ definiert ist.

Lösung: Wir bestimmen den Konvergenzradius $r = \limsup_{n\to\infty} \sqrt[n]{|n|}$. Sei nun $n = p^k u$ mit $k \in \mathbb{Z}$, $\mathrm{ggT}(p,u) = 1$. Dann ist $\sqrt[n]{|n|} = \sqrt[n]{|u|} = p^{-k/n}$. Weiter ist $k \cdot \ln p \leq \ln n$ (ordinärer Logarithmus), also

$$\frac{k}{n} \leq \frac{\ln n}{n \ln p} \overset{n\to\infty}{\longrightarrow} 0.$$

Wir erhalten $\sqrt[n]{|n|} = p^{-k/n} \to 1 = r$. Also ist der neue Logarithmus für $|x| < 1$ wohldefiniert. Anders gesagt: $1 + x \in \mathbb{U}_K^{(1)}$.

Zur Stetigkeit: Es ist

$$\begin{aligned}
|\log(1+x) - \log(1+y)| &= |\sum (-1)^{n+1}(x^n - y^n)/n| \\
&\leq \sup_n \{|x^n - y^n|/|n||\} \quad \text{(ultrametrische Ungleichung)} \\
&= \sup_n \{\frac{1}{|n|}|x-y||x^{n-1} + x^{n-2}y + \ldots + y^{n-1}|\} \\
&\leq \sup_n \{\frac{|x|^{n-1}}{|n|}|x-y|\} \quad \text{(ult. Ungl. + o.B.d.A. } |x| < |y|) \\
&\leq |x-y| \quad \text{da } |x| < 1
\end{aligned}$$

und somit $\log(1+x)$ sogar Lipschitz-stetig.

Aufgabe 32) Berechnen Sie $(\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2)$.

Lösung: Es ist $\mathbb{Q}_p^\times = \langle p \rangle \times \mu_{p-1} \times \mathbb{U}_p^{(1)}$ nach obigen Betrachtungen. Also ist

$$(\mathbb{Q}_p^\times)^2 = \langle p^2 \rangle \times \underbrace{\mu_{(p-1)/2}}_{=\emptyset \text{ für } p=2} \times (\mathbb{U}_p^{(1)})^2.$$

Zuerst $p > 2$: Wir zeigen $(\mathbb{U}_p^{(1)})^2 = \mathbb{U}_p^{(1)}$. Sei dazu $u \in \mathbb{U}_p^{(1)}$, dann hat $f(T) = T^2 - u$ die approximative Nullstelle 1, da $|f(1)| < 1$ und $|f'(1)| = |2| = 1$. Also folgt mit HENSELs Lemma $(\mathbb{U}_p^{(1)})^2 = \mathbb{U}_p^{(1)}$ und somit $(\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2) = 4$.

Sei nun $p = 2$. Wir zeigen $(\mathbb{U}_2^{(1)})^2 = \mathbb{U}_2^{(3)} = \{u \in \mathbb{U}_2 : u \equiv 1 \pmod{2^3}\}$. Sei nun $u \in \mathbb{U}_2^{(3)}$, dann hat $f(T) = T^2 - u$ die approximative Nullstelle 1: $|f(1)| = |1-u| \leq \frac{1}{8}$,

$|f'(1)| = |2| = \frac{1}{2}$ und $\frac{1}{8} < \left(\frac{1}{2}\right)^2$. HENSELs Lemma liefert $\mathbb{U}_2^{(3)} = (\mathbb{U}_2^{(3)})^2$. Weiter ist für $u \in \mathbb{U}_2^{(1)}$ nun $u = 1 + 2x$, $x \in \mathbb{U}_2$. Quadrieren liefert $u^2 = 1 + 4x + 4x^2 = 1 + 4x(x+1) \equiv 1 \pmod 8$. Also $u^2 \in \mathbb{U}_2^{(3)}$. Insgesamt also $(\mathbb{U}_2^{(1)})^2 = \mathbb{U}_2^{(3)}$. Daher $(\mathbb{Q}_2^\times : (\mathbb{Q}_2^\times)^2) = 2(\mathbb{U}_2^{(1)} : \mathbb{U}_2^{(3)}) = 8$.

Aufgabe 32) Bestimmen Sie alle quadratischen Erweiterungen von $\mathbb{Q}_p$ (in einem fixierten algebraischen Abschluss).

Lösung: Jede quadratische Erweiterung hat die Gestalt $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ mit $\deg(\mathrm{Irr}(X, \alpha, \mathbb{Q}_p)) = 2$, also $\mathrm{Irr}(X, \alpha, \mathbb{Q}_p) = X^2 + q_1 X + q_2$ und damit $X = -\frac{q_1}{2} \pm \sqrt{\frac{q_1^2}{4} - q_2}$. Da $\frac{q_1}{2} \in \mathbb{Q}_p$, sind nur $\alpha = \sqrt{g}$, $g \in \mathbb{Q}_p$ interessant. Betrachten wir einen festen algebraischen Abschluss $\mathbb{Q}_p^A$ und dann

$$\mathbb{Q}_p^\times \underset{x \mapsto \sqrt{x}}{\longrightarrow} (\mathbb{Q}_p^A)^\times \longrightarrow (\mathbb{Q}_p^A)^\times / \mathbb{Q}_p^\times$$

mit Kern $(\mathbb{Q}_p^\times)^2$. So sehen wir, dass die quadratischen Erweiterungen von $\mathbb{Q}_p$ genau zu den nichttrivialen Restklassen in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ korrespondieren.

Mit der vorhergehenden Aufgabe kommen wir zu folgenden Schlüssen: Für $p > 2$ gibt es genau $4 - 1 = 3$ quadratischen Erweiterungen, nämlich $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{\zeta_{p-1}})$ und $\mathbb{Q}_p(\sqrt{p\zeta_{p-1}})$, wobei ζ_{p-1} primitive $p-1$-te Einheitswurzel ist. Für $p = 2$ sind die Elemente in $\mathbb{U}_2^{(1)}/\mathbb{U}_2^{(3)}$ repräsentiert durch $1, 3, 5, 7$. Die $8 - 1 = 7$ quadratischen Erweiterungen sind also $\mathbb{Q}_p(\sqrt{d})$ für $d = 3, 5, 7, 2, 6, 10, 14$.

Aufgabe 32) Zeigen Sie: Ein lokaler Zahlenkörper hat nur endlich viele Erweiterungen von festem Grad (in einem fixierten alg. Abschluss).

Lösung: Wir betrachten Erweiterungen $\overline{\mathbb{Q}}_p/L/K$ mit $[L : K] = n$ für gegebenes K und n. Da L/K separabel ist (Charakteristik 0), wird es nach dem Satz vom primitiven Element von einem $\theta \in L$ erzeugt ($L = K(\theta)$). Weiter können wir annehmen, dass θ ganz über K ist, da $K(\theta) = K(p^m\theta)$. Jedes solche θ hat ein Minimalpolynom des Grades $\leq n$, dessen Koeffizienten im Parameterraum $\mathcal{O}_K^n$ liegen. Nach KRASNERs Lemma gibt es wegen der Stetigkeit von Polynomen um jedes Minimalpolynom eine offene Umgebung, die die gleiche Erweiterung erzeugt. Da $\mathcal{O}_K$ kompakt ist, ist auch $\mathcal{O}_K^n$ kompakt und kann stets durch endlich viele dieser Koeffizientenvektor-Umgebungen überdeckt werden, womit es nur endlich viele verschiedene Köerperweiterungen gibt.

Aufgabe 32) Zeigen Sie: $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ ist GALOIS-Erweiterung vom Grad $\varphi(p^n)$ und die GALOIS-Gruppe ist isomorph zu $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Weiter ist $e = \varphi(p^n)$, $f = 1$.

Lösung: Sicher ist $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ algebraisch und separabel. Es verbleibt normal für GALOIS zu zeigen. Es ist

$$X^{p^n} - 1 = (X^{p^{n-1}} - 1)\left((X^{p^{n-1}})^{p-1} + \ldots + X^{p^{n-1}} + 1\right)$$

und somit

$$\phi(X) := \prod_\rho (X - \rho) = X^{(p-1)p^{n-1}} + \ldots + X^{p^{n-1}} + 1,$$

wobei ρ alle primitiven n-ten Einheitswurzeln durchläuft. Wir betrachten $\psi(X) :=$

$\phi(X+1)$. Dann ist ψ irred. als Eisensteinpolynom: $\psi(0) = \phi(1) = p$ und

$$\phi(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1} \equiv (X-1)^{p^n - p^{n-1}} \pmod{p}.$$

Also $\psi(X) \equiv X^{(p-1)p^{n-1}}$.

Da nun alle primitiven p^n-ten Einheitswurzeln durch $\zeta_{p^n}^a$ mit a prim zu p und $0 < a < p^n$ gegeben sind, ist also $\mathbb{Q}_p(\zeta_{p^n}/\mathbb{Q}_p)$ GALOIS mit Grad $(p-1)p^{n-1} = \varphi(p^n)$. Gleichzeitig liefert $\zeta_{p^n} \mapsto \zeta_{p^n}^a$ für jedes a prim zu p einen Automorphismus. Das sind $\varphi(p^n)$ viele, sodass

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Weiter ist $1-\zeta_{p^n}$ ein Element der Norm $\phi(1) = p$, also auch $1-\zeta_{p^n}^a$ und daher hat

$$\frac{1-\zeta_{p^n}^a}{1-\zeta_{p^n}} = 1 + \zeta_{p^n} + \ldots + \zeta_{p^n}^{a-1}$$

Norm 1. Es ist also $p = \prod_a (1-\zeta_{p^n}^a) = \eta(1-\zeta_{p^n})^{\varphi(p^n)}$ mit $\mathrm{N}\,\eta = 1$ und $1-\zeta_{p^n}$ Primelement. Wegen $e \cdot f = [L:K]$ folgt die Behauptung.

Aufgabe 32) Zeigen Sie: Ein lokaler Zahlkörper enhält nur endlich viele Einheitswurzeln.

Lösung: Sei $K/\mathbb{Q}_p$ endlich, fest aber beliebig. Wir betrachten $\mu_N \subset K$, die in K liegenden Einheitswurzeln, $N = p^m \cdot n$ mit n prim zu p. Nach obigen Betrachtungen erzeugt μ_{p^m} allein eine Erweiterung des Grades $\varphi(p^m) = (p-1)p^{m-1}$, womit m nach oben beschränkt ist. Betrachten wir $\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p$ ist dies unverzweigt nach Vorlesung.

Aufgabe 32) Wieviele quadratische Erweiterungen besitzt $\mathbb{Q}_p(\zeta_p)$?

Lösung: Analog zu einer vorangegangenen Aufgabe untersuchen wir $K^\times/(K^\times)^2$ für $K = \mathbb{Q}_p(\zeta_p)$. Für $p = 2$ ist $\mathbb{Q}_2(\zeta_2) = \mathbb{Q}_2$, also alles wie gehabt (7 quadratische Erweiterungen). Für $p > 2$ ist

$$K^\times \cong \langle 1-\zeta_p \rangle \times \mu_{p-1} \times \mathbb{U}_p^{(1)}.$$

Von hier an analog 3 quadratische Erweiterungen.

Aufgabe 32) Welche Erweiterung aus der vorherigen Aufgabe ist die unverzweigte für $p = 2$?

Lösung: Kandidaten: $\sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{2}, \sqrt{6}, \sqrt{10}, \sqrt{14}$. Wir stellen fest, dass genau $K = \mathbb{Q}_2(\sqrt{5})$ ungerade Diskriminante $d_K = 5$ hat (da $5 \equiv 1 \pmod 4$). Da 2 in allen anderen Fällen die Diskriminante teilt, ist 2 dort verzweigt.

Index