Algebraische Zahlentheorie
Sommersemester 2008

Prof. Dr. Annette Huber-Klawitter

Fassung vom 29. Juli 2008

Dies ist ein Vorlesungsskript und kein Lehrbuch.
Mit Fehlern muss gerechnet werden!

Math. Institut
Eckerstr.1
79104 Freiburg

0761-203-5560
annette.huber@math.uni-freiburg.de

Kapitel 0

Einleitung

Zahlentheorie beschäftigt sich mit Eigenschaften von Zahlen, d.h. Elementen von $\mathbb{Z}$. Damit ist sie eine der ältesten Wissenschaften überhaupt - die Königin der Mathematik. Wir wissen sehr viel, sehr vieles aber auch nicht. Unter

`http://www.ams.org/mathscinet`

finden Sie die "Mathematical Reviews", in denen alle wissenschaftlichen Arbeiten der Mathematik besprochen werden. Unter "MSC Primary" 11 sind die Arbeiten zur Zahlentheorie zu finden. (Kann als "Search Term" eingestellt werden!) Eine genauere Untergliederung können Sie nachlesen, wenn Sie den Links "Free Tools" und dann "Search MSC" folgen.
Heute sollen einige Teilgebiete der Zahlentheorie vorgestellt werden.

Elementare Zahlentheorie

Es werden nur die Mittel der Mittelstufe verwendet, d.h. Mathematik bis zum 17. Jahrhundert. Zum Beispiel:

Satz 0.1. *Eine ganze Zahl ist durch* 3 *teilbar genau dann, wenn ihre Quersumme durch* 3 *teilbar ist.*

Beweis: Sei $n = \sum_{n=0}^{m} a_i 10^i$ mit $0 \leq a_i < 10$. Wegen $10 \equiv 1 \mod 9$ folgt $n \equiv \sum_{n=0}^{m} a_i \mod 3$. □

Aber Vorsicht: elementar heißt nicht unbedingt einfach!

Satz 0.2 (Fermat)**.** *Jede natürliche Zahl ist Summe von vier Quadraten (*0 *ist als Summand zugelassen).*

Literatur: W. Scharlau, H. Opolka, Von Fermat bis Minkowski, Springer Verlag.

Analytische Zahlentheorie

Zahlentheoretische Information wird in Reihen kodiert und analytisch weiterverarbeitet.

Satz 0.3. *Es gibt unendlich viele Primzahlen.*

Beweis: Sei $\zeta(s) = \sum_{n\geq 1} 1/n^s$ die Riemannsche ζ-Funktion.

Behauptung. $\zeta(s)$ *konvergiert absolut und gleichmäßig in* $\mathrm{Re}s \geq \sigma > 1$.

$s = u + iv$ mit $u, v \in \mathbb{R}$.

$$|n^{-s}| = |n^{-u}| \cdot |n^{-iv}| = n^{-u}|\mathrm{e}^{-iv\log n}| = n^{-u}$$

Für $u \geq \sigma$ folgt (z.B. Integralvergleichskriterium)

$$\sum |n^{-s}| = \sum n^{-u} \leq \sum n^{-\sigma} < \infty$$

Behauptung.

$$\zeta(s) = \prod_{p\ prim} \frac{1}{1-p^{-s}}$$

Summenformel für die geometrische Reihe:

$$\frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + \dots$$

Beim Ausmultiplizieren kommt jeder Term

$$n^{-s} = (p_1^{n_1} p_2^{n_2} \dots p_k^{n_k})^{-s}$$

genau einmal vor. Sorgfältigeres Hinsehen zeigt auch die Grenzwertaussage, siehe: Hardy, Wright: An introduction to the Theory of Numbers, Theorem 280. Damit können wir nun den Satz beweisen. Gäbe es nur endliche viele Primzahlen, so wäre

$$\lim_{s\to 1} \prod_p \frac{1}{1-p^{-s}} = \prod_p \frac{1}{1-p^{-1}} \leq \infty$$

Der Grenzwert $\lim_{s\to 1} \zeta(s)$ existiert jedoch nicht (harmonische Reihe). □

Durch genaueres Studium der ζ-Funktion wurde das große Ergebnis der analytischen Zahlentheorie bewiesen.

Theorem 0.4 (Primzahlsatz)**.** *Sei $\pi(x)$ die Anzahl der Primzahlen kleiner gleich x. Dann gilt*

$$\pi(x) \sim \frac{x}{\log x}$$

(d.h. der Quotient geht gegen 1).

Diese Aussage wurde von Gauß ca. 1792 vermutet. Der erste Beweis stammt von Hadamard und de la Vallée-Poussin (unabhängig) 1896. Ein sehr kurzer Beweis stammt von Newman, vergleiche
D. Zagier, Newman's short proof of the prime number theorem, American Math. Monthly 104 (97) 705-708.

Vermutung 0.5 (Riemannsche Vermutung)**.** *Die Nullstellen von* $\zeta(s)$ *in* $\mathbb{C}$ *sind* $-2n$ *für* $n \in \mathbb{N}$ *oder haben* $\mathrm{Re}s = 1/2$.

Dies hat Folgen für den Fehlerterm im Primzahlsatz.

Algebraische Zahltheorie

Satz 0.6 (Euler)**.** *Die Gleichung* $x^3 + y^3 = z^3$ *hat keine Lösung in natürlichen Zahlen.*

Ansatz:

$$x^3 = z^3 - y^3 = (z - y)(z - \varrho y)(z - \varrho^2 y)$$

wobei $\varrho = \mathrm{e}^{2\pi i/3}$ eine dritte Einheitswurzel ist. Allgemeiner:

$$Z^3 - y^3 = (Z - y)(Z - \varrho y)(Z - \varrho^2 y) \in \mathbb{C}[Z]$$

da die Nullstellen übereinstimmen. Sei nun $K = \mathbb{Q}(\varrho)$, $R = \mathbb{Z}[\varrho]$. Die Körpererweiterung $K/\mathbb{Q}$ ist quadratisch, denn das Minimalpolynom von ϱ ist $Z^2 + Z + 1$. Es gilt

$$R = \{a + b\varrho \mid a, b \in \mathbb{Z}\} \ .$$

R ist ein Hauptidealring, darin ist $\lambda = 1 - \varrho$ eine Primzahl.
Man beweist allgemeiner:

Satz 0.7. *Die Gleichung* $x^3 + y^3 + \lambda^{3n} z^3 = 0$ *hat in* R *keine Lösungen mit* $xyz \neq 0$.

Beweis: Geschickte Teilbarkeitsargumente in R modulo λ, vergl. Hardy-Wright, Kapitel 13.4. □

Leider funktioniert dieselbe Idee nicht für

$$x^p + y^p = z^p$$

(p Primzahl), da $\mathbb{Z}[\zeta_p]$ mit $\zeta_p = \mathrm{e}^{2\pi i/p}$ im Allgemeinen kein Hauptidealring ist. Dennoch: Um Eigenschaften von $\mathbb{Z}$ zu studieren, lohnt es sich, endliche Erweiterungen von $\mathbb{Q}$ zu studieren. Diese *Zahlkörper* sind der Hauptgegenstand dieser Vorlesung.

Literatur:

(i) P. Samuel, Algebraic Theory of Numbers

(ii) S. Lang, Algebraic Number Theory

(iii) J. Neukirch, Algebraic Number Theory

(iv) A. Leutbecher, Zahlentheorie - eine Einführung in die Algebra

(v) Atiyah, MacDonald, Introduction to Commutative Algebra

Arithmetische Geometrie

In diesem Gebiet findet ein großer Teil der aktuellen Forschung der Zahlentheorie statt.
Gleichungen wie $x^p + y^p = z^p$ definieren eine Punktmenge in $\mathbb{R}^3$ oder $\mathbb{C}^3$. Dies ist ein Beispiel für eine algebraische Varietät. Sie können nun mit geometrischen Methoden studiert werden.

Theorem 0.8 (Mordell Vermutung, Faltings 1983)**.** *Sei C eine algebraische Kurve vom Geschlecht größer gleich 2 über $\mathbb{Q}$. Dann hat C nur endliche viele Punkte über jedem Zahlkörper.*

Beispiel. Für $n > 4$ definiert die Gleichung $X^n + Y^n = 1$ eine Kurve vom Geschlecht größer gleich 1. Also hat die Gleichung nur endlich viele rationale Lösungen, d.h. die Fermatgleichung hat nur endlich viele ganzzahlige Lösungen.

Theorem 0.9 (Wiles 1994)**.** *$x^n + y^n = z^n$ hat nur die trivialen Lösungen.*

Wiles benutzt die Methoden der arithmetischen Geometrie, insbesondere Geometrie von Modulformen. Der Beweis ist anspruchsvoll. Unsere algebraische Zahlentheorie ist hierfür das Einmaleins.

Kapitel 1

Ganze Ringerweiterungen

Zahlringe

Definition 1.1. *Ein Körper K der Charakteristik null mit $[K : \mathbb{Q}] < \infty$ heißt* Zahlkörper*. Der* Ganzheitsring *von K ist*

$$\mathcal{O}_K = \{\alpha \in K \mid \textit{es gibt } n \in \mathbb{N}, a_1, \ldots, a_n \in \mathbb{Z}, \alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0\}$$

Ringe von dieser Form heißen Zahlringe*.*

Entscheidend ist hierbei der Koeffizient 1 vor α^n!

Bemerkung. Fast alles, was wir in diesem Semester entwickeln, funktioniert genauso auch für endliche Erweiterungen von $\mathbb{F}_p(X)$, die sogenannten *Funktionenkörper*. Beide Klassen fasst man als *globale Körper* zusammen. Der Ring $\mathbb{F}_p[X]$ übernimmt die Rolle von $\mathbb{Z}$ in der Definition des Ganzheitsrings. Entscheidend ist, dass beides Hauptidealringe sind.

Beispiel. Sei $K/\mathbb{Q}$ quadratisch, d.h. $[K : \mathbb{Q}] = 2 \Rightarrow K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ keine Quadratzahl.

Satz 1.2. *Sei $K = \mathbb{Q}(\sqrt{d})$, d quadratfrei (d.h. kein doppelter Faktor in der Primfaktorzerlegung). Dann gilt:*

(i) Für $d \equiv 2, 3 \mod 4$ ist $\mathcal{O}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$,

(ii) Für $d \equiv 1 \mod 4$ ist $\mathcal{O}_K = \{1/2(u + v\sqrt{d}) \mid u, v \in \mathbb{Z}, u \equiv v \mod 2\}$.

Beweis: Es ist $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ mit $\sigma(\sqrt{d}) = -\sqrt{d}$. Sei $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$, d.h. Nullstelle von

$$P(X) = X^n + a_1X^{n-1} + \cdots + a_n = 0,\ a_i \in \mathbb{Z}\ .$$

Dann ist auch $\sigma(\alpha)$ eine Nullstelle von $P(X)$. Das Polynom

$$\begin{aligned} Q(\alpha) &= (X - \alpha)(X - \sigma(\alpha)) = X^2 - (\alpha + \sigma\alpha)X + \alpha\sigma\alpha \\ &= X^2 - (a + b\sqrt{d} + a - b\sqrt{d})X + (a + b\sqrt{d})(a - b\sqrt{d}) \\ &= X^2 - 2aX + (a^2 - b^2d) \in \mathbb{Q}[X] \end{aligned}$$

muss also $P(X)$ teilen. Nach dem Gauß-Lemma hat Q also ganze Koeffizienten (z.B. Bosch, 2.7 Kor.6). Es gilt also

$$2a, a^2 - b^2 d \in \mathbb{Z} \Rightarrow (2a)^2 - (2b)^2 d \in \mathbb{Z} \Rightarrow (2b^2)d \in \mathbb{Z} \ .$$

Wäre $2b \notin \mathbb{Z}$, so müssten sich die Primfaktoren des Nenners gegen Faktoren von d wegheben. Wegen $(2b)^2$ müsste der Faktor sogar doppelt in d vorkommen. Dies ist ein Widerspruch zur Wahl von d. Also:

$$\begin{gathered} a = \frac{u}{2}, b = \frac{v}{2} \text{ mit } u, v \in \mathbb{Z} \\ \Rightarrow \left(\frac{u}{2}\right)^2 - \left(\frac{v}{2}\right)^2 d = \frac{u^2 - v^2 d}{4} \in \mathbb{Z} \\ \Leftrightarrow 4 \mid u^2 - v^2 d \end{gathered}$$

Die Quadrate u^2 und v^2 können nur 0 oder 1 modulo 4 sein. Für $u^2 - v^2 d$ ergeben sich daher unterschiedliche Möglichkeiten je nach Restklasse von d. Man überprüft tabellarisch, dass für $d \equiv 2, 3$ nur $u^2 \equiv v^2 \equiv 0 \mod 4$ in Frage kommt, also beide gerade. Für $d \equiv 1$ ist $u^2 \equiv v^2 = 1 \mod 4$ ebenfalls möglich, also beide ungerade. □

Beispiel. Sei ζ_N eine primitive N-te Einheitswurzel. Der Ganzheitsring von $\mathbb{Q}(\zeta_N)$ ist $\mathbb{Z}[\zeta_N]$.

Der Beweis ist aufwändiger. Wir werden ihn später führen, wenn wir schon mehr über Zahlringe wissen.
In diesen Beispielen sieht man, dass $\mathcal{O}_K$ ein Ring ist. Für den allgemeinen Fall holen wir weiter aus.

Konvention: Alle Ringe sind kommutativ mit Eins. Alle Ringhomomorphismen bilden Eins auf Eins ab.

Definition 1.3. *Sei $A \subset B$ eine Ringerweiterung. Ein Element $b \in B$ heißt* ganz über A*, wenn es $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ gibt mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. Der* ganze Abschluss *von A in B ist die Menge der Elemente von B, die ganz über A sind. Die Ringerweiterung heißt* ganz*, wenn alle Elemente von b ganz über A sind.*

Beispiel. (i) $A = \mathbb{Z}$, $B = K$ endliche Körpererweiterung von $\mathbb{Q}$. Dann ist $\mathcal{O}_K$ nach Definition der ganze Abschluss von $\mathbb{Z}$ in K.

(ii) $A = K \subset L$ eine Körpererweiterung. Ein Element von L ist genau dann ganz über K, wenn es algebraisch über K ist. (Das Minimalpolynom kann normiert gewählt werden!).

Satz 1.4. *Sei $A \subset B$ eine Ringerweiterung. Dann ist der ganze Abschluss von A in B ein Ring.*

Insbesondere sind Zahlringe Ringe!

Bemerkung. Zum Beweis erinnern wir uns an den Fall von Körpererweiterungen. Warum ist der algebraische Abschluss ein Körper? Warum sind Summen/Produkte von algebraischen Elementen algebraisch? In der Algebra wurde dies auf die Theorie der *endlichen* Erweiterungen zurückgeführt - endliche Erweiterungen von endlichen Erweiterungen sind endlich, endliche Erweiterungen sind endlich. Endlich bedeutet hierbei *endlichdimensional* als Vektorraum.
Dieses Argument wollen wir mit Ringen wiederholen. Dafür müssen wir zuerst den Vektorraumbegriff auf Ringe übertragen!

Moduln

Definition 1.5. *Sei A ein Ring. Ein A-*Modul *M ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Skalarmultiplikation*

$$A \times M \to M$$

so dass für alle $a, b \in A$, $x, y \in M$ gilt:

(i) $a(x+y) = ax + ay$,

(ii) $(a+b)x = ax + bx$,

(iii) $a(bx) = (ab)x$,

(iv) $1x = x$.

Beispiel. $A = k$ ein Körper. Dann ist ein A-Modul das Gleiche wie ein k-Vektorraum.

Lemma 1.6. *Ein $\mathbb{Z}$-Modul ist das Gleiche wie eine abelsche Gruppe.*

Beweis: Sei M ein $\mathbb{Z}$-Modul, dann ist nach Definition M eine abelsche Gruppe. Interessant ist also die Gegenrichtung. Sei M eine abelsche Gruppe, $x \in M$, $n \in \mathbb{N}$. Wir definieren $nx = x + (n-1)x$. Für negative n setzen wir $nx = -(-n)x$. Die Modulaxiome gelten alle. Man beweist alles mit Induktion, z.B.

$$n(x+y) = (x+y) + (n-1)(x+y) = x + y + (n-1)x + (n-1)y = nx + ny\ .$$

□

Bemerkung. Man sieht an der Beispielrechung, dass die Kommutativität von M wirklich benötigt wird.

Definition 1.7. *Sei M ein A-Modul.*

(i) Ein System von Elementen $\{m_i | i \in I\}$ heißt Erzeugendensystem*, wenn es für jedes $m \in M$ ein $n \in \mathbb{N}$, endlich viele $i_1, \ldots, i_n \in I$ und $a_1, \ldots, a_n \in A$ gibt mit*

$$m = a_1 m_{i_1} + \cdots + a_n m_{i_n}$$

(ii) *M heißt* endlich erzeugt*, wenn es ein Erzeugendensystem mit endlich vielen Elementen gibt.*

(iii) *Ein System $\{m_i | i \in I\}$ heißt* linear unabhängig*, wenn aus*

$$0 = a_1 m_{i_1} + \cdots + a_n m_{i_n}$$

mit $n \in \mathbb{N}, i_1, \ldots, i_n \in I, a_1, \ldots, a_n \in A$ folgt, dass $a_1 = \cdots = a_n = 0$.

(iv) *Ein linear unabhängiges Erzeugendensystem heißt* Basis*.*

(v) *M heißt* frei*, falls es eine Basis gibt. Die Mächtigkeit einer Basis heißt* Rang *von M.*

Beispiel. (i) Wenn A ein Körper ist, so sind alle Moduln frei. (Basisexistenzsatz, Lineare Algebra). Der Rang ist nichts anderes als die Dimension.

(ii) Sei $A = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$. Dieser Modul ist nicht frei, denn für jedes Element gilt $2x = 0$. Es gibt keine linear unabhängigen Teilmengen!

(iii) A^2 ist frei vom Rang 2 mit Basis $\{(1,0),(0,1)\}$.

Die Wohldefiniertheit des Rangs werden wir noch zeigen.
Die Grundlagen der Theorie funktionieren wie in der linearen Algebra.

Definition 1.8. *(i)* *$N \subset M$ heißt* Untermodul*, wenn N abelsche Untergruppe von M ist und abgeschlossen unter Multiplikation mit A.*

(ii) *$f : N \to M$ heißt* Modulhomomorphismus*, wenn f ein Gruppenhomomorphismus ist und $f(am) = af(m)$. Die Menge der Modulhomomorphismen wird durch* $\mathrm{Hom}_A(M,N)$ *bezeichnet.*

Beispiel. A ist auch ein A-Modul. Die Untermoduln von A sind genau die Ideale. Ist $A \to B$ ein Ringhomomorphismus, so ist B ein A-Modul.

Lemma 1.9. *(i) Kern und Bild eines Modulhomomorphismus sind Untermoduln.*

(ii) Ist $N \subset M$ ein Untermodul, so ist M/N ein Modul mit der induzierten Skalarmultiplikation. Ist speziell $M = A$ der Ring, so ist A/N ein Ring falls $N \neq A$.

Beweis: Kern und Bild sind Untergruppen. Zu zeigen ist, dass sie von der Skalarmultiplikation respekiert werden. Sei $f : M \to N$ ein Modulhomomorphismus, $x \in \mathrm{Ker}\, f$, $a \in A$. Dann gilt

$$f(ax) = af(x) = a0 = 0 \ .$$

Sei $y = f(x)$ im Bild. Dann gilt

$$ay = af(x) = f(ax) \ .$$

Da M abelsch ist, ist N automatisch ein Normalteiler. Damit ist M/N als abelsche Gruppe definiert. Auch die Modulaxiome sind leicht zu überprüfen. Einzige Frage ist die Wohldefiniertheit der Skalarmultiplikation. Seien also $a \in A$, $x, y \in M$ in der selben Nebenklasse, d.h. $x - y \in N$. Dann gilt

$$a(x + N) = ax + N \; ; a(y + N) = ay + N \; .$$

Da N ein Untermodul ist, gilt $a(x-y) = ax-ay \in N$, also ist die Multiplikation wohldefiniert. Ist speziell $M = A$ der Ring, so ist N ein Ideal. Die Ringaxiome sind leicht zu überprüfen (oder vergleiche Algebra). □

Satz 1.10 (Homomorphiesatz, Noethersche Isomorphiesätze)**.** *Sei $f : M \to N$ ein A-Modulhomomorphismus. Dann ist die induzierte Abbildung*

$$\overline{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$$

ein Isomorphismus von A-Moduln. Sind $N, N' \subset M$ Untermoduldn, so ist

$$(N + N')/N \cong N'/(N \cap N')$$

ein kanonischer Isomorphismus. Sind $N' \subset N \subset M$ Untermoduln, so ist

$$(M/N')/(N/N') \cong M/N$$

ein kanonischer Isomorphismus.

Beweis: In der Algebra zeigt man diese Ausagen für abelsche Gruppen. Die Verträglichkeit mit der A-Modulstruktur ist leicht zu überprüfen. □

Satz 1.11. *Sei $M = A^n$ ein freier A-Modul. Dann ist der Rang wohldefiniert.*

Beweis: Sei $I \subset A$ ein maximales Ideal, d.h. $I \neq A$ und maximal mit dieser Eigenschaft. Solche Ideale existieren. (Satz der Algebra). Sei $N = IM$, d.h. der Untermodul, der von den ax mit $a \in I$, $x \in M = A^n$ erzeugt wird.

Behauptung. $N = I^n$ *(direktes Produkt von Moduln)*

Zunächst $N \supset I^n$. Sei $(x_1, \ldots, x_n) \in I^n$.

$$(x_1, \ldots, x_n) = (x_1, 0, \ldots, 0) + (0, x_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, x_n) = \\ x_1(1, 0, \ldots, 0) + \cdots + x_n(0, \ldots, 0, 1) \in N \; .$$

Für die zweite Inklusion sei $(a_1, \ldots, a_n) \in A^n$ und $x \in I$. Dann folgt $x(a_1, \ldots, a_n) = (xa_1, \ldots, xa_n) \in I^n$. Dann ist

$$M/N = A^n/I^n = (A/I)^n \; .$$

Die Zahl n ist die Dimension des $k = A/I$-Vektoraums M/N, also wohldefiniert. □

Lemma 1.12. *Sei R ein Ring, B eine quadratische Matrix mit Koeffizienten in B. Wenn das Gleichungssystem $By = 0$ eine nichttriviale Lösung $(\lambda_1, \ldots, \lambda_n)$ hat, so folgt $\lambda_i \det B = 0$ für alle i.*

Beweis: Ist R ein Körper, so gilt diese Aussage mit $\det B = 0$. (Lineare Algebra) Für den Ringfall gehen wir die Beweise durch: Die Determinante wird durch die Leibniz-Formel definiert. Sie ist multilinear und alternierend in den Zeilen und Spalten. Insbesondere bleibt sie unverändert, wenn man ein Vielfaches einer Spalte zu einer anderen addiert. Wir multiplizieren also die Spalte i mit λ_i (dies multipliziert die Determinante mit λ_i) und addieren dann das λ_j-fache der Spalte j für alle $j \neq i$. In der neuen Matrix verschwindet die i-te Spalte, also auch die Determinante. □

Ganze Ringerweiterungen

Satz 1.13. *Seien $A \subset R$ Ringe, $x \in R$. Dann sind äquivalent:*

(i) Es gibt $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$.

(ii) $A[x] = \left\{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0, a_i \in A\right\}$ ist ein endlich erzeugter A-Modul.

(iii) Es gibt einen Teilring $B \subset R$, der A und x enthält und der ein endlich erzeugter A-Modul ist.

(iv) x ist ganz über A.

Beispiel. Seien speziell $A \subset R$ Körper. Dann bedeuten die Bedingungen:

(i) x ist algebraisch über A.

(ii) $A[x]$ ist ein endlich dimensionaler A-Vektorraum.

(iii) $A, \{x\} \subset B$ und B ist ein endlich dimensionaler A-Vektorraum.

In dieser Form ist der Satz aus der Algebra bekannt. Der Beweis bleibt derselbe.

Beweis: $(i) \Rightarrow (ii)$: Sei $M \subset R$ der A-Modul, der von $1, x, \ldots, x^{n-1}$ erzeugt wird. Nach Vorraussetzung gilt

$$x^n = -a_1 x^{n-1} - \cdots - a_n \in M$$

Rekursiv erhält man also $x^{n+j} \in M$ für alle j. Es folgt $A[x] \subset M$. Die umgekehrte Inklusion ist klar. Insbesondere ist $A[x]$ endlich erzeugt.
$(ii) \Rightarrow (iii)$: Wähle $B = A[x]$.
$(iii) \Rightarrow (i)$: B werde von $y_1, \ldots, y_n$ also A-Modul erzeugt. Wegen $x \in B$ gilt $xy_i \in B$. Es gibt also Koeffizienten $a_{ij} \in A$ mit

$$xy_i = \sum_j a_{ij} y_j \Leftrightarrow \sum_j (a_{ij} - \delta_{ij} x) y_j = 0$$

Dies kann als ein lineares Gleichungssystem über dem Ring B für die y_j gelesen werden. Sei d die Determinante der Koeffizientenmatrix, also das charakteristische Polynom von (a_{ij}). Die Spalten der Koeffizientenmatrix sind linear abhängig. Nach Lemma 1.12 folgt $y_i d = 0$ für $i = 1, \ldots, n$. Da B von den y_i erzeugt wird, folgt $bd = 0$ für alle $b \in B$, insbesondere auch $1d = 0$. Das charakteristische Polynom ist die gesuchte Polynomialgleichung für x.
$(i) \Leftrightarrow (iv)$ gilt nach Definition. □

Beweis von Satz 1.4. Es gilt $x+y, x-y, xy \in A[x,y]$. Sei x ganz über A. Dann ist $A[x]$ ein A-Modul mit Erzeugern $\{x_1, \ldots, x_n\}$. Sei y ganz über A. Dann ist $A[y]$ ein A-Modul mit Erzeugern $\{y_1, \ldots, y_m\}$. Dann sind die Elemente $x_i y_j$ Erzeuger von $A[x,y]$, denn in $\alpha = \sum a_{kl} x^k y^l$ können x und y durch die x_i und y_j ausgedrückt werden. Durch Ausmultiplizieren erhält man eine Darstellung von α in Termen der $x_i y_j$. Also ist $A[x,y]$ endlich erzeugt. Nach Satz 1.13 sind dann alle Elemente von $A[x,y]$ ganz über A. □

Damit haben wir unser erstes Hauptziel erreicht.

Korollar 1.14 (Transitivität)**.** *Seien $A \subset B$, $B \subset C$ ganze Ringerweiterungen. Dann ist $A \subset C$ ganz.*

Beweis: Sei $x \in C$. Es erfüllt also eine Gleichung

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0 \ , b_i \in B$$

B ist ganz über A, also ist $A[b_i]$ endlich erzeugter A-Modul. Wie beim letzten Beweis folgt $A[b_1, \ldots, b_n]$ endlich erzeugter A-Modul. Wegen $x \in A[b_1, \ldots, b_n]$ ist x ganz über A (Satz 1.13). □

Korollar 1.15. *Sei B ein Integritätsring, $A \subset B$ ein Unterring, so dass B ganz über A ist. Dann gilt:*

$$B \text{ Körper } \Leftrightarrow A \text{ Körper}$$

Beweis: Sei A ein Körper, $0 \neq b \in B$. Nach Satz 1.13 ist $B' = A[b]$ ein endlichdimensionaler A-Vektorraum. Die Multiplikation mit B ist eine A-lineare Abbildung $B' \to B'$. Da B nullteilerfrei ist, ist diese Abbildung injektiv. Da B' endlich dimensional ist, ist sie dann auch surjektiv. Also hat b ein multiplikatives Inverses in $B' \subset B$.
Umgekehrt sei B ein Körper, $0 \neq a \in A$. Sei $b = a^{-1} \in B$. Dieses Element ist ganz über A, erfüllt also eine Gleichung

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \ a_i \in A \ .$$

Diese Gleichung wird mit a^{n-1} multipliziert.

$$b + a_1 + a_2 a + \ldots a_n a^{n-1} = 0 \ .$$

Alle Summanden außer dem ersten liegen in A, also auch b. □

Definition 1.16. *Sei A ein Integritätsring. A heißt* ganz abgeschlossen*, wenn A mit seinem ganzen Abschluss im Quotientenkörper übereinstimmt.*

Beispiel. Faktorielle Ringe (d.h. solche mit eindeutiger Primfaktorzerlegung, z.B. $\mathbb{Z}$, diskrete Bewertungsringe) sind ganz abgeschlossen.

Beweis: Sei A ein Hauptidealring, K der Quotientenkörper, $x \in K$ ganz über A. Dann ist

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,\ a_i \in A$$

Sei $x = a/b$ mit a und b teilerfremd. Die Gleichung wird mit b^n multipliziert:

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

b teilt jeden Summanden außer dem ersten, also folgt $b \mid a^n$. Dies ist ein Widerspruch zur Teilerfremdheit. Es folgt b invertierbar in A und damit $x \in A$. □

Korollar 1.17. *Zahlringe sind ganz abgeschlossen.*

Beweis: Sei $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$ in K, $\mathcal{O}'$ der ganze Abschluss von $\mathcal{O}_K$ in K. Wegen der Transitivität von ganzen Erweiterungen ist dann $\mathcal{O}'$ ganz über $\mathbb{Z}$, also $\mathcal{O}' \subset \mathcal{O}_K$. □

Kapitel 2

Moduln über Hauptidealringen

Unser nächstes großes Ziel ist der Beweis des folgenden Resultats.

Theorem 2.1. *Sei $K/\mathbb{Q}$ ein Zahlkörper, $\mathcal{O}_K \subset K$ der Ganzheitsring. Dann ist $\mathcal{O}_K \cong \mathbb{Z}^d$ mit $d = [K : \mathbb{Q}]$.*

Beispiel. (i) Für $K/\mathbb{Q}$ vom Grad zwei ist dies eine Übungsaufgabe.

(ii) Für $K = \mathbb{Q}(\zeta_n)$ gilt $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ (ohne Beweis). Als $\mathbb{Z}$-Modul hat dieser Ringe die Basis $1, \zeta_n x, \zeta_n^2, \ldots, \zeta_n^{\phi(n)-1}$, wobei $\phi(n)$ der Grad des Minimalpolynoms von ζ_n ist.

Bemerkung. Sei $\alpha \in \mathcal{O}_K$. Dann ist $\mathbb{Z}[\alpha]$ nach Satz 1.13 eine endlich erzeugte abelsche Gruppe. Ist $\mathbb{Z}[\alpha] \neq \mathcal{O}_K$, so nehmen wir $\beta \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha]$. Wieder nach Satz 1.13 ist $\mathbb{Z}[\alpha, \beta]$ ein endlich erzeugter $\mathbb{Z}[\alpha]$-Modul und damit eine endliche erzeugte abelsche Gruppe (vergleiche Beweis von Satz 1.4). Wenn dies nicht ganz $\mathcal{O}_K$ ist, dann ...
Es gibt zunächst keinen Grund, warum dieses Verfahren enden sollte.

Wir wenden uns den einfachen Reduktionen zu.

Moduln über Hauptidealringen

Satz 2.2. *Sei A ein Hauptidealring, M ein endlich erzeugter freier Modul, $N \subset M$ ein Untermodul. Dann ist N ebenfalls frei von kleinerem Rang als M.*

Proof. Es genügt $M = A^n$ zu betrachten. Der Beweis wird durch vollständige Induktion nach n geführt. Für $n = 1$ gilt die Aussage, da jedes Ideal ein Hauptideal ist, also frei vom Rang 1 oder 0.
Sei nun $n > 1$, $p : A^n \to A$ die Projektion auf die letzte Koordinate. Der Kern ist $A^{n-1} \times 0$, also frei vom Rang $n - 1$. Wir betrachten $\pi = p|_N$. Es gilt

$$\operatorname{Ker} \pi = N \cap \operatorname{Ker} p \subset \operatorname{Ker} p \cong A^{n-1}$$

also ist $\operatorname{Ker}\pi$ frei. Weiter gilt

$$\operatorname{Im}\pi \subset \operatorname{Im} p = A$$

Nach Induktionsvoraussetzung ist dieser Modul frei vom Rang höchstens 1.

Behauptung. $N \cong \operatorname{Ker}\pi \oplus \operatorname{Im}\pi$

Im Fall $\operatorname{Im}\pi = 0$ ist nichts zu zeigen. Sei nun y eine Basis von $\operatorname{Im}\pi$ und $\tilde{y}$ ein Urbild in N.

$$\phi : \operatorname{Ker}\pi \oplus \operatorname{Im}\pi \to N; \qquad (x, ay) \mapsto x + a\tilde{y}$$

Wie in der linearen Algebra rechnet man nach, dass diese Abbildung injektiv und surjektiv ist. Hier die Details: Sei $(x, ay) \in \operatorname{Ker}\phi$, d.h. $x = -a\tilde{y}$. Auf diese Relation wenden wir π an und erhalten $0 = -ay$. Wegen $y \neq 0$ folgt $a = 0$, somit $x = 0$. Für die Surjektivität sei $n \in N$. Sei $n' = \pi(x) = ay$. Dann ist $x = n - a\tilde{y} \in \operatorname{Ker}\pi$. Es gilt nach Konstruktion $n = \phi(x, a\tilde{y})$.
Dies beendet den Beweis. Als direkte Summe von freien Moduln ist N frei. □

Definition 2.3. *Ein A-Modul M heißt* torsionsfrei*, wenn $ax = 0$ für $a \in A, x \in M$ impliziert $a = 0$ oder $x = 0$.*

Besonders interessant ist der Fall $A = \mathbb{Z}$.

Beispiel. $\mathbb{Q}$-Vektorräume sind torsionsfreie abelsche Gruppen, denn $ax = 0, a \neq 0 \Rightarrow x = \frac{1}{a}ax = 0$. Alle Untergruppe von $\mathbb{Q}$-Vektoräumen sind torsionsfreie abelsche Gruppen, insbesondere unsere Ganzheitsringe $\mathcal{O}_K \subset K$.

Satz 2.4. *Sei A ein Hauptidealring. Torsionsfreie endlich erzeugte A-Moduln sind frei von endlichem Rang.*

Proof. Sei M ein endlich erzeugter torsionsfreier Modul. Seien $x_1, \ldots, x_N$ Erzeuger von M. Darin sei ohne Einschränkung $\{x_1, \ldots, x_n\}$ eine maximale linear unabhängige Teilmenge. Für $i > n$ gilt

$$a_i x_i + a_1 x_1 + \cdots + a_n x_n = 0$$

mit $a_i \neq 0$, denn sonst wäre $\{x_1, \ldots, x_n, x_i\}$ linear unabhängig. Mit anderen Worten: $a_i x_i \in < x_1, \ldots, x_n >_A$. Sei $a = \prod_{i=n+1}^{N} a_i$. Dann ist $ax_i \in < x_1, \ldots, x_n >_A$ für $i = 1, \ldots, N$. Wir definieren

$$\phi : M \to M \ ; \ x \mapsto ax \ .$$

M ist torsionsfrei, daher ist $\operatorname{Ker}\phi = \{x \in M \mid ax = 0\} = 0$. ϕ faktorisiert über $< x_1, \ldots, x_n >_A \cong A^n$. Der Untermodul $\phi(M)$ ist dann frei. □

Bemerkung. Wir haben hier einen Spezialfall des *Elementarteilersatzes* bewiesen. Jeder endlich erzeugte Modul über einem Hauptidealring hat die Form

$$A^n \times A/q_1 \times \ldots A/q_m$$

Für $n, m \in \mathbb{N}_0$ und Ideale $q_1 \subset \dot{\subset} q_m$. Für $A = \mathbb{Z}$ nennt man das Ergebnis auch *Struktursatz für endlich erzeugte abelsche Gruppen*. Für $A = k[X]$ (k Körper) ist es die *Jordansche Normalform*.

Vorüberlegungen zum Beweis des Theorems

$\mathcal{O}_K \subset K$ ist eine torsionsfreie abelsche Gruppe. Daher ist ist $\mathcal{O}_K$ endlich erzeugt genau dann, wenn $\mathcal{O}_K \cong \mathbb{Z}^N$ für ein N.

Lemma 2.5. *Sei $x \in K$. Dann gibt es $m \in \mathbb{Z}$ mit $mx \in \mathcal{O}_K$.*

Beweis: x erfüllt $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$ mit $a_i \in \mathbb{Q}$. Sei m der Hauptnenner der a_i. Multiplikation der Gleichung mit m^n ergibt

$$(mx)^n + a_1 m(mx)^{n-1} + \ldots m^n a_n = 0 \ .$$

Also gilt $mx \in \mathcal{O}_K$. □

Korollar 2.6. *$\mathcal{O}_K$ enthält eine freie Gruppe vom Rang $d = [K : \mathbb{Q}]$.*

Beweis: Sei $x_1, \ldots, x_d$ eine Basis von K über $\mathbb{Q}$. Seien $m_1, \ldots, m_d \in \mathbb{Z}$, so dass $m_i x_i \in \mathcal{O}$.

Behauptung. *$< m_1 x_1, \ldots, m_d x_d >$ hat Rang d.*

Wäre der Rang kleiner als d, so hätten wir eine Relation

$$n_1(m_1 x_1) + n_2(m_2 x_2) + \cdots + n_d(m_d x_d) = 0 \ ,$$

dies ist ein Widerspruch zu linearen Unabhängigkeit von $x_1, \ldots, x_d$ über $\mathbb{Q}$. □

Lemma 2.7. *Sei $M \subset K$ eine endlich erzeugte abelsche Gruppe. Dann gilt* $\mathrm{rg} M \leq d$.

Beweis: Sei $M_{\mathbb{Q}} = \{\frac{m}{s} \mid m \in M, s \in \mathbb{Z}\} \subset K$. Dies ist ein $\mathbb{Q}$-Vektorraum der Dimension höchstens d.

Behauptung. $\dim M_{\mathbb{Q}} = \mathrm{rg} M$.

Sei $x_1, \ldots, x_k$ eine Basis von M als $\mathbb{Z}$-Modul. Dies ist eine Basis von $M_{\mathbb{Q}}$ als $\mathbb{Q}$-Vektorraum, da ein linear unabhängiges Erzeugendensystem. □

Insgesamt: *Wenn $\mathcal{O}_K$* endlich erzeugt ist als abelsche Gruppe, *dann $\mathcal{O}_K \cong \mathbb{Z}^d$*. Wir fassen zusammen:

Lemma 2.8. *Für den Beweis von Theorem 2.1 genügt es zu zeigen, dass $\mathcal{O}_K \subset M \subset K$ wobei M eine endlich erzeugte abelsche Gruppe ist.*

Beweis: M endlich erzeugt, torsionsfrei $\Rightarrow$ M freier Z-Modul von endlichem Rang. $\mathcal{O}_K \subset M \Rightarrow \mathcal{O}_K$ frei von endlichem Rang. Die Gradaussage des Theorems folgt wie bereits bemerkt aus Korollar 2.6 und Lemma 2.7. □

Kapitel 3

Norm, Spur und Diskriminante

Erinnerung an Algebra

Sei L/K algebraisch und separabel, $\alpha \in L$. Das Minimalpolynom $\mathrm{Min}(\alpha)$ von α ist das normierte Polynom minimalen Grades mit Nullstelle α.

Beispiel. In Charakteristik Null sind alle Erweiterungen separabel. Erweiterungen von endlichen Körpern ebenfalls. Dies sind die beiden Fälle, die bei uns vorkommen werden.

Lemma 3.1. $\mathrm{Min}(\alpha)$ *ist das charakteristische Polynom* $\det(X\,\mathrm{id} - m_\alpha)$ *der* K*-linearen Multiplikationsabbildung* $m_\alpha : K(\alpha) \to K(\alpha)$ *mit* $x \mapsto \alpha x$*.*

Beweis: Sei P das charakteristische Polynom. Es hat den Grad $[K(\alpha) : K] = \deg \mathrm{Min}(\alpha)$. Es ist normiert. Es gilt (Satz von Cayley-Hamilton) $P(m_\alpha) = 0$ als Abbildung $K(\alpha) \to K(\alpha)$. Auswerten in 1 ergibt $P(\alpha) = 0$. Also erfüllt P alle Eigenschaften von $\mathrm{Min}(\alpha)$. □

Seien $\alpha_1, \ldots, \alpha_d$ die d verschiedenen (L/K separabel!) Nullstellen von $\mathrm{Min}(\alpha)$ in $\overline{K}$. Jedes α_i definiert einen Körperhomomorphismus $\sigma_i : K(\alpha) \to \overline{K}$ mit $\sigma_i(\alpha) = \alpha_i$. Dies sind alle Körperhomomorphismen $\sigma : K(\alpha) \to K$ mit $\sigma|_K = \mathrm{id}$.

Lemma 3.2. *Es gilt*

$$\mathrm{Min}(\alpha) = \prod_{i=1}^{d}(X - \alpha_i) = \prod_{i=1}^{d}(X - \sigma_i(\alpha)) \ .$$

Beweis: Klar □

Bemerkung. $K(\alpha)/K$ ist galois genau dann, wenn alle $\alpha_i \in K(\alpha)$. Dann ist $\{\sigma_1, \ldots, \sigma_d\} = \mathrm{Gal}(K(\alpha)/K)$.

Definition 3.3. *Sei L/K endliche Körpererweiterung, $\alpha \in L$. Das* charakteristische Polynom *von α ist*

$$P_\alpha(X) = \det(X \,\mathrm{id} - m_\alpha)$$

wobei $m_\alpha : L \to L$ die Multiplikationsabbildung mit α ist. Die Norm *von α ist*

$$N_{L/K}(\alpha) = \det(m_\alpha)$$

Die Spur *von α ist*

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

Bemerkung. Es gilt $P_\alpha(X) = X^{[L:K]} - \mathrm{Tr}(\alpha)X^{[L:K]-1} + \cdots + (-1)^{[L:K]}N(\alpha)$.

Lemma 3.4. *Sei L/K separable Körpererweiterung, $[L : K] = d$. Seien $\alpha_1, \ldots, \alpha_d$ die Nullstellen von* $\mathrm{Min}(\alpha)$*, jede mit Vielfachheit $[L : K(\alpha)]$. Seien*

$$\sigma_1, \ldots, \sigma_d : L \to \overline{K}$$

die Einbettungen mit $\sigma_i|_K = \mathrm{id}$. Dann gilt

$$\begin{aligned} P_\alpha(X) &= \mathrm{Min}(\alpha)^{[L:K(\alpha)]} = \prod_{i=1}^{d}(X - \alpha_i) = \prod_{i=1}^{d}(X - \sigma_i(\alpha)) \\ \mathrm{Tr}_{L/K}(\alpha) &= \sum \alpha_i = \sum \sigma_i(\alpha) \\ N_{L/K}(\alpha) &= \prod \alpha_i = \prod \sigma_i(\alpha)\ . \end{aligned}$$

Beweis: Es genügt, die Aussge für P_α zu zeigen. Es gilt

$$\{\alpha_1, \ldots, \alpha_d\} = \{\sigma_1(\alpha), \ldots, \sigma_d(\alpha)\}$$

als Mengen mit Vielfachheit, denn jede der $[K(\alpha) : K]$ vielen Einbettungen $K(\alpha) \to \overline{K}$ lässt sich auf $[L : K(\alpha)]$ viele Weisen nach L fortsetzen. Der Fall $L = K(\alpha)$ ist Lemma 3.1. Sei nun $r = [L : K(\alpha)]$.

Behauptung. $P_{L/K} = P^r_{K(\alpha)/K}$.

Sei $y_1, \ldots, y_r$ eine Basis von $L/K(\alpha)$, $z_1, \ldots, z_q$ eine Basis von $K(\alpha)/K$. Dann ist $\{y_i z_j \mid i = 1, \ldots, r, j = 1, \ldots, q\}$ eine Basis von L/K. Sei $M = (m_{jk})$ die Matrix der Multiplikation mit α bezüglich der z_j, d.h. $m_\alpha(z_j) = \sum_k m_{jk} z_k$. Dann gilt $m_\alpha(y_i z_j) = \sum_k m_{jk} y_i z_k$. Die Matrix von m_α bezüglich der Basis $y_i z_j$ ist eine diagonale Blockmatrix aus r Kopien von M. □

Korollar 3.5. *Sei L/K Erweiterung von Zahlkörpern, $\alpha \in \mathcal{O}_L$. Dann gilt $P_\alpha \in \mathcal{O}_K[X]$. Insbesondere ist $\mathrm{Tr}_{L/K}(\alpha), N_{L/K}(\alpha) \in \mathcal{O}_K$.*

Bemerkung. Falls $\mathcal{O}_L \cong \mathcal{O}_K^d$ (im Allgemeinen falsch!), so hat die Matrix von m_α Einträge in $\mathcal{O}_K$ und die Aussage ist klar.

Beweis: $P_\alpha(X) = \prod(X - \sigma(\alpha))$ mit σ wie im Lemma. Nach Vorraussetzung erfüllt α eine Gleichung

$$X^n + a_1 X^{n-1} + \cdots + a_0 = 0 \text{ mit } a_i \in \mathcal{O}_K$$

Dann erfüllt $\sigma(\alpha)$ dieselbe Gleichung, ist also ebenfalls ganz über $\mathcal{O}_K$. Damit sind alle Koeffizienten von P_α ganz über $\mathcal{O}_K$. Gleichzeitig liegen sie in K. Da $\mathcal{O}_K$ ganz abgeschlossen ist, liegen die Koeffizienten in $\mathcal{O}_K$. □

Beispiel. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{3})$, $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$. Wir wählen die Basis $1, \sqrt{3}$. Sei $\alpha = a + b\sqrt{3}$. Die Multiplikation mit α hat die Matrix

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

Also ist die Spur $2a$, die Norm $a^2 - 3b^2$, das charakteristische Polynom

$$P_\alpha(X) = X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) = X^2 - 2aX + (a^2 - 3b^2)$$

Für $b \neq 0$ ist dies das Minimalpolynom von α. Für $b = 0$ gilt $X^2 - 2aX + a^2 = (X - a)^2 = \mathrm{Min}(\alpha)^2$.

Definition 3.6. *Sei $A \subset B$ eine Ringerweiterung, B ein freier A-Modul vom Rang d. Die* Spurpaarung *ist die symmetrische A-bilineare Abbildung*

$$(\cdot, \cdot) : B \times B \to A \ , (x, y) = \mathrm{Tr}_{B/A}(xy) \ .$$

Sei $x_1, \ldots, x_d$ eine Basis von B. Dann heißt

$$D(x_1, \ldots, x_d) = \det(\mathrm{Tr}(x_i x_j)_{i,j})$$

Diskriminante *der Basis. Die* Diskriminante $\mathcal{D}_{B/A}$ *ist das Ideal, das $D(x_1, \ldots, x_d)$ erzeugt wird.*

Bemerkung. Uns interessiert vor allem L/K endliche Köpererweiterung, aber auch $\mathcal{O}_K/\mathbb{Z}$.

Beispiel. Sei $L = \mathbb{Q}[X]/(X^2 + pX + q)$ mit $p, q \in \mathbb{Q}$. Dies ist ein 2-dimensionaler $\mathbb{Q}$-Vektorraum, Basis $1, X$. Es gilt $\mathrm{Tr}(1) = 2$. Multiplikation mit X hat die Matrix

$$\begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$$

also, $\mathrm{Tr}(X) = -p$.
Es gilt

$$D(1, X) \ = \ \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(X) \\ \mathrm{Tr}(X) & \mathrm{Tr}(X^2) \end{pmatrix} \ = \ \det \begin{pmatrix} 2 & -p \\ -p & p^2 - 2q \end{pmatrix} \ = \ p^2 - 4q$$

Dies ist genau die Diskriminate der quadratischen Gleichung.

Lemma 3.7. *Sei $y_1, \dots, y_d \in B$ mit $y_i = \sum a_{ij} x_j$. Dann gilt*

$$D(y_1, \dots, y_d) = \det(a_{ij})^2 D(x_1, \dots, x_d)$$

Insbesondere ist $\mathcal{D}_{B/A}$ wohldefiniert.

Beweis: Es gilt

$$\mathrm{Tr}(y_p y_q) = \mathrm{Tr}\left(\sum_{i,j} a_{pi} a_{qj} x_i x_j \right) = \sum a_{pi} a_{qj} \mathrm{Tr}(x_i x_j)$$

Es folgt

$$(\mathrm{Tr}(y_p y_q))_{pq} = (a_{pi})_{pi} (\mathrm{Tr}(x_i x_j))_{ij} (a_q j)^t$$

wobei ^{t} die transponierte Matrix ist. Dies impliziert die Gleichheit der Determinanten. □

Exkurs in die bilineare Algebra

Sei $(\cdot, \cdot) : V \times V \to k$ eine symmetrische Bilinearform, (k Körper, V ein Vektorraum). Sei $v_1, \dots, v_d$ eine Basis von V, $M = (v_i, v_j)_{ij}$ die zugehörige symmetrische Matrix. Dann gilt für $v = \sum a_i v_i, w = \sum_j b_j v_j$

$$(v, w) = \left(\sum a_i v_i, \sum_j b_j v_j \right) = \sum_{i,j} a_i (v_i, v_j) b_j = (a_1, \dots, a_d)^t M (b_1, \dots, b_d)$$

Definition 3.8. *Die Bilinearform $(\cdot, \cdot)$ heißt nicht-degeneriert, wenn aus $(v, w) = 0$ für alle w die Gleichung $v = 0$ folgt.*

Lemma 3.9. *$(\cdot, \cdot)$ ist nichtdegeneriert genau dann, wenn die zugehörige Matrix M invertierbar ist, also genau dann, wenn $\det M \neq 0$.*

Beweis: Falls M nicht invertierbar ist, so gibt es v mit $v^t M = 0$, also auch $v^t M w = 0$ für alle w. Sei nun M invertierbar, $v = \sum a_i v_i$. Der Fall $d = 1$ ist trivial, also sei $d > 1$. Wähle $(c_1, \dots, c_d)$ mit

$$a_1 c_1 + \dots + a_d c_d \neq 0$$

Wir lösen das Gleichungssystem $Mw = (c_1, \dots, c_d)^t$. Dies ist möglich, da M invertierbar ist. Es folgt $v^t M w \neq 0$. □

Bemerkung. Die Diskriminante entscheidet also, ob die Spurpaarung nichtdegeneriert ist.

Beispiel. $K = \mathbb{Q}(\sqrt{3})/\mathbb{Q}$. Es gilt

$$D(1, \sqrt{3}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{3}) \\ \mathrm{Tr}(\sqrt{3}) & \mathrm{Tr}(3) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} = 12$$

Lemma 3.10. *Sei $(\cdot,\cdot)$ nicht-degenererierte symmetrische Bilinearform, $v_1,\dots,v_d$ eine Basis. Dann gibt es eine* duale Basis *$w_1,\dots,w_d$ mit $(v_i,w_j)=\delta_{ij}$.*

Beweis: Die Bestimmung von w_j bedeutet das Lösen eines linearen Gleichungssystems $Mw_j=(0,\dots,1,\dots,0)$ (mit 1 an der j-ten Stelle). Dies ist möglich, da M invertierbar ist. □

Satz 3.11. *Sei L/K separable endliche Körpererweiterung. Dann ist $\mathcal{D}_{L/K}\neq 0$. Die Spurpaarung ist nicht-degeneriert.*

Beweis: Es gilt $\mathrm{Tr}(\alpha)=\sum\sigma_i(\alpha)$, wobei $\sigma_i : L\to\overline{K}$ für $i=1,\dots,d$ die Einbettungen mit $\sigma_i|_K=\mathrm{id}$ durchläuft. (Hier benutzen wir die Separabilität.) Sei $x_1,\dots,x_d$ eine Basis von L über K. Es gilt

$$D(x_1,\dots,x_d)=\det\left(\mathrm{Tr}(x_iy_j)_{ij}\right)=\det\left(\sum_k\sigma_k(x_ix_j)\right)_{ij}$$
$$=\det\left(\sum_k\sigma_k(x_i)\sigma_k(x_j)\right)_{ij}=\det\left((\sigma_k(x_i))_{ik}(\sigma_k(x_j))_{kj}\right)=\det(\sigma_i(x_j))^2$$

Angenommen diese Determinante verschwindet. Dann gibt es $u_1,\dots,u_d\in\overline{K}$ mit $\sum_i u_i\sigma_i(x_j)=0$ für alle j. Da die x_j eine Basis sind, folgt $\sum u_i\sigma_i=0$ als Abbildungen $L^*\to\overline{K}$. Als Gruppenhomomorphismen $L^*\to\overline{K}^*$ sind die σ_i jedoch linear unabhängig nach Lemma 3.12. □

Lemma 3.12. *Sei G eine Gruppe, k ein Körper, $\sigma_i : G\to k^*$ für $i=1,\dots,m$ verschiedene Gruppenhomomorphismen. Dann sind sie linear unabhänging im k-Vektorraum* $\mathrm{Abb}(G,k)$.

Dies ist ein wesentlicher Schritt im Beweis des Hauptsatzes der Galoistheorie. Da das Lemma wichtig und einfach ist, führen wir den Beweis noch einmal.

Proof. Angenommen, die Aussage ist falsch. Dann gibt es eine minimale linear abhängige Teilmenge von $\{\sigma_1,\dots,\sigma_m\}$. Ohne Einschränkung besteht sie aus $\sigma_1,\dots,\sigma_n$ mit $n\leq m$. Es ist $n\geq 2$, denn $\sigma_1\neq 0$, da es Werte in k^* annimmt. Sei nun

$$a_1\sigma_1+\cdots+a_n\sigma_n=0$$

eine nichttriviale Relation in $\mathrm{Abb}(G,k)$. Wegen der Minimalität der Relation gilt $a_i\neq 0$ für alle i. Seien $g,h\in G$. Es gilt

$$\begin{aligned}0=&a_1\sigma_1(gh)+\cdots+a_n\sigma_n(gh)\\=&a_1\sigma_1(g)\sigma_1(h)+\cdots+a_n\sigma_n(g)\sigma_n(h)\end{aligned}$$

Da dies für alle h gilt, erhalten wir eine neue Relation

$$0=a_1\sigma_1(g)\sigma_1+\cdots+a_n\sigma_n(g)\sigma_n$$

Andererseits multiplizieren wir die ursprüngliche Relation mit $\sigma_1(g)$

$$0 = a_1\sigma_1(g)\sigma_1 + \cdots + a_n\sigma_1(g)\sigma_n$$

Durch Subtraktion ergibt sich

$$0 = 0 + a_2(\sigma_1(g) - \sigma_2(g))\sigma_2 + \cdots + a_n(\sigma_n(g) - \sigma_1(g))\sigma_n$$

Wir wählen speziell g mit $\sigma_1(g) \neq \sigma_2(g)$. Dies ist möglich wegen $\sigma_1 \neq \sigma_2$. Damit haben wir eine neue, kürzere nichttrivale Relation gefunden. Dies ist ein Widerspruch zur Wahl der σ_i. □

Beispiel. $L = \mathbb{Q}[X]/(X^2 + pX + q)$ hatte Diskriminante $p^2 - 4q$. Diese Zahl verschwindet genau dann, wenn $X^2 + pX + q$ eine doppelte Nullstelle hat, also wenn L kein Körper ist.

Beweis von Theorem 2.1. Sei $\mathcal{O}_K \subset K$ der Ganzheitsring. Nach Lemma 2.8 genügt es zu zeigen, dass $\mathcal{O}_K$ in einem endlich erzeugten $\mathbb{Z}$-Modul $M \subset K$ enthalten ist. Sei $x_1, \ldots, x_d$ eine Basis von $K/\mathbb{Q}$. Ohne Einschränkung gilt $x_i \in \mathcal{O}_K$. Sei $y_1, \ldots, y_d$ die duale Basis bezüglich der Spurpaarung.

Behauptung. $\mathcal{O}_K \subset < y_1, \ldots, y_d >_{\mathbb{Z}}$.

Sei $z \in \mathcal{O}_K$. Wir schreiben $z = \sum b_j y_j$ mit $b_j \in \mathbb{Q}$, da die y_j eine Basis bilden. Es gilt $x_i z \in \mathcal{O}_K$, da $\mathcal{O}_K$ ein Ring ist. Nach Korollar 3.5 ist $\mathrm{Tr}(x_i z) \in \mathbb{Z}$. Es folgt weiter

$$\mathrm{Tr}(x_i z) = \sum \mathrm{Tr}(x_i b_j y_j) = \sum b_j \mathrm{Tr}(x_i y_j) = b_i$$

□

Kapitel 4

Ideale von Ganzheitsringen

Dedekindringe

Definition 4.1. *Ein Ring A heißt* noethersch*, wenn jedes Ideal endlich erzeugt ist.*

Beispiel. Hauptidealringe sind noethersch, denn jedes Ideal wird von nur einem Element erzeugt.

Lemma 4.2. *Sei $\mathcal{O}_K$ ein Zahlring. Dann ist $\mathcal{O}_K$ noethersch.*

Beweis: Nach Theorem 2.1 ist $\mathcal{O}_K \cong \mathbb{Z}^d$ für $d = [K : \mathbb{Q}]$ (als abelsche Gruppe). Jedes Ideal I ist eine Untergruppe, nach Satz 2.2 ist I daher endlich erzeugt als Gruppe. Dann ist I erst recht endlich erzeugt als Ideal. □

Bemerkung. Nicht so leicht zu sehen, aber richtig: Ist k ein Körper, so ist $k[X_1, \ldots, X_n]$ noethersch.

Meist werden die folgenden Eigenschaften noetherscher Ringe ausgenutzt:

Lemma 4.3. *Sei A ein noetherscher Ring.*

(i)
$$I_1 \subset I_2 \subset I_3 \subset \ldots$$
eine Folge von Idealen. Dann wird diese stationär, d.h. es gibt $n_0 \in \mathbb{N}$, so dass $I_n = I_{n+1}$ für alle $n \geq n_0$.

(ii) Sei $\Phi \neq \emptyset$ eine Menge von Idealen von A. Dann hat Φ ein maximales Element.

Beweis: Wir betrachten eine Idealkette. Sei $I = \bigcup I_n$. Dies ist ein Ideal. Nach Vorraussetzung ist I endlich erzeugt. Seien $a_1, \ldots, a_m$ Erzeuger. Dann gibt es n_i für $i = 1, \ldots, m$, so dass $a_i \in I_{n_i}$. Sei $n_0 = \max n_i$. Dann gilt $a_i \in a_{n_0}$ für alle i. Dies bedeutet $I_{n_0} = I$, also auch $I_n = I_{n_0}$ für $n \geq n_0$.

Sei nun Φ ein Menge von Idealen von A. Angenommen, es gibt kein maximales Element. Sei $I_1 \in \Phi$. Da I_1 nicht maximal ist, gibt es $I_2 \in \Phi$ mit $I_1 \subsetneq I_2$. Da I_2 nicht maximal ist finden wir $I_3 \in \Phi$ mit $I_2 \subsetneq I_3$. Iterativ finden wir eine Kette von Idealen, die nicht stationär wird. Dies ist ein Widerspruch zu A noethersch. □

Definition 4.4. *Sei A ein Ring. Ein* Primideal *von A ist ein Ideal $\mathfrak{p} \subset A$, so dass gilt: $\mathfrak{p} \neq A$ und*

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$$

Beispiel. (i) Ist A ein Hauptidealring, so ist $I = (f)$ genau dann ein Primideal, wenn f ein Primelement (oder 0), denn

$$ab \in (f) \Leftrightarrow f|ab \Rightarrow f|a \text{ oder } f|b$$

(ii) A ist ein Integritätsbereich genau dann, wenn 0 ein Primideal ist:

$$ab \in 0 \Leftrightarrow ab = 0 \Rightarrow a = 0 \text{ oder } b = 0$$

Lemma 4.5. *Sei A ein Ring, I ein Ideal. I ist genau dann ein Primideal, wenn A/I ein Integritätsbereich ist.*

Beweis: Sei I ein Primideal, $a, b \in A$ mit $ab = 0 \mod I$. Dies bedeutet $ab \in I$, also ohne Einschränkung $a \in I$. Dies bedeutet wiederum $a = 0 \mod I$.
Sei umgekehrt A/I Integritätsbereich, $ab \in I$. Dann ist $ab = 0 \mod I$, also ohne Einschränkung $a = 0 \mod I$. Dies bedeutet $a \in I$. □

Korollar 4.6. *Maximale Ideale sind Primideale.*

Beweis: Sei $\mathfrak{m}$ maximales Ideal von A. Dann ist $A/\mathfrak{m}$ ein Körper, also ein Integritätsbereich. □

Definition 4.7. *Sei A ein Ring. Die* Krulldimension *von A ist die maximale Länge n einer Kette von Primidealen*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

Die Krulldimension kann auch unendlich sein, sogar in noetherschen Ringen.

Beispiel. (i) Körper haben Krulldimension Null.

(ii) Ein Hauptidealring, der kein Körper ist, hat Krulldimension 1. Ist p ein Primelement, so hat die Kette $0 \subset (p)$ keine Verfeinerung.

(iii) Schwierig: $k[X_1, \ldots, X_n]$ hat Dimension n.

Lemma 4.8. *Zahlringe sind eindimensional.*

Beweis: Sei $\mathcal{O}$ ein Zahlring. Sei $\mathfrak{p} \subset \mathcal{O}$ ein Primideal ungleich 0. Zu zeigen ist, dass $\mathfrak{p}$ maximal ist.
Auch $\mathfrak{p}' = \mathfrak{p} \cap \mathbb{Z}$ ist ein Primideal.

Behauptung. $\mathfrak{p}' \neq 0$.

Sei $x \in \mathfrak{p}$ mit

$$0 = x^n + a_1 x^{n-1} + \cdots + a_n = x(x^{n-1} + a_1 x^{n-2} + \ldots a_{n-1}) + a_n$$

und $a_i \in \mathbb{Z}$, ohne Einschränkung $a_n \neq 0$. Es folgt $a_n \in \mathfrak{p} \cap \mathbb{Z}$.
Es folgt $\mathfrak{p}' = (p)$ für eine Primzahl p. Die Abbildung

$$\mathbb{Z}/(p) \to \mathcal{O}/\mathfrak{p}$$

ist ein injektiver Ringhomomorphismus. Also ist der Integritätsring $\mathcal{O}/\mathfrak{p}$ eine ganze Erweiterung des Körpers $\mathbb{Z}/(p)$. Nach Lemma 1.15 ist dann auch $\mathcal{O}/\mathfrak{p}$ ein Körper, d.h. $\mathfrak{p}$ ist maximal. □

Definition 4.9. *Ein* Dedekindring *ist ein noetherscher, ganz abgeschlossener* 1*-dimensionaler Ring.*

Wir fassen zusammen:

Satz 4.10. *Sei $\mathcal{O}$ ein Zahlring. Dann ist $\mathcal{O}$ ein Dedekindring.*

Beweis: Lemma 4.2, Lemma 4.8 und Korollar 1.17. □

Strukturtheorie für Ideale von Dedekindringen

Definition 4.11. *Sei A ein Ganzheitsring mit Quotientenkörper K. Ein* gebrochenes *Ideal von A ist ein A-Untermodul $I \subset K$, so dass es $d \in A \setminus \{0\}$ gibt mit $dI \subset A$, d.h. ein gemeinsamer Hauptnenner.*

Bemerkung.

- Gebrochene Ideale heißen auch *invertierbare Ideale*
- Ein Ideal $I \subset A$ ist ein gebrochenes Ideal (mit $d = 1$). Zur Unterscheidung nennen wir sie auch *ganze* Ideale.
- Die Menge der gebrochenen Ideale hat eine Addition und Multiplikation

$$I + I' = \{a + b \mid a \in I, b \in I'\} \subset K$$
$$I \cdot I' = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in I' \right\} \subset K$$

  Wir werden zeigen, dass die gebrochenen Ideale ungleich 0 eine abelsche Gruppe bezüglich der Multiplikation bilden.

Lemma 4.12. *Ein Untermodul $I \subset K$ ist ein gebrochenes Ideal genau dann, wenn er endlich erzeugt ist.*
Ist $A = \mathcal{O}_K$ ein Zahlring, so ist I freie abelsche Gruppe vom Rang $[K : \mathbb{Q}]$.

Beweis: Sei $I =< x_1, \ldots, x_n >_A$, d der Hauptnenner der x_i, dann gilt $dI \subset A$. Ist umgekehrt $dI \subset A$, so ist dI ein Ideal eines noetherschen Rings, also endlich erzeugt. Dann ist auch I endlich erzeugt.
Sei nun $A = \mathcal{O}_K$ Zahlring. Als abelsche Gruppe ist I isomorph zu $dI \subset \mathcal{O}_K$. Als endlich erzeugte Untergruppe einer freien abelschen Gruppe ist er frei vom Rang höchstens $[K : \mathbb{Q}]$. Sei $a \in I$. Wegen $\mathcal{O}_K a \subset I$ ist der Rang mindestens $[K : \mathbb{Q}]$. □

Theorem 4.13. *Sei A ein Dedekindring. Dann ist jedes maximale Ideal invertierbar als gebrochenes Ideal, d.h. zu I existiert I^{-1} mit $I \cdot I^{-1} = A$.*

Bemerkung. Wäre A ein Hauptidealring, so wären alle gebrochenen Ideale von der Form Ab mit $b \in Q(A)$. Das inverse Ideal wäre einfach Ab^{-1}.

Lemma 4.14. *Sei A noetherscher Ring, $0 \neq I$ ein (ganzes) Ideal. Dann gibt es Primideale ungleich 0 mit $I \supset \mathfrak{p}_1 \ldots \mathfrak{p}_n$.*

Beweis: Sei Φ die Menge der Ideale $I \neq 0$ von A, für die das Lemma nicht gilt, d.h. die kein Produkt von Primidealen enthalten. Angenommen, $\Phi \neq \emptyset$. Da A noethersch ist, hat Φ ein maximales Element I_0. Das Ideal I_0 ist nicht prim, also gibt es $x, y \in A \setminus I_0$ mit $xy \in I_0$. Nach Voraussetzung

$$I_0 \subsetneq I_0 + (x), I_0 + (y) \Rightarrow I_0 + (x), I_0 + (y) \notin \Phi$$

Also gibt es Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$ ungleich null mit

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subset I_0 + (x), \mathfrak{q}_1 \ldots \mathfrak{q}_m \subset I_0 + (y) \Rightarrow$$
$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \mathfrak{q}_1 \ldots \mathfrak{q}_m \subset (I_0 + (x))(I_0 + (y)) = I_0$$

Dies ist ein Widerspruch. □

Beweis des Theorems: Sei $\mathfrak{m} \subset A$ maximal, $\mathfrak{m} \neq 0$. Sei

$$\mathfrak{m}' = \{x \in Q(A) \mid x\mathfrak{m} \subset A\}$$

Dies ist ein A-Untermodul von $Q(A)$. Für $0 \neq y \in \mathfrak{m}$ folgt $y\mathfrak{m}' \in A$, also ist dies ein gebrochenes Ideal. Schließlich gilt nach Definition $\mathfrak{m}\mathfrak{m}' \subset A$. Da $\mathfrak{m}$ ein Ideal ist, gilt $A \subset \mathfrak{m}'$. Es folgt

$$\mathfrak{m} = A\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m} \subset A$$

Da $\mathfrak{m}$ maximal ist, gilt

$$\mathfrak{m}'\mathfrak{m} = \mathfrak{m} \text{ oder } \mathfrak{m}'\mathfrak{m} = A$$

Behauptung. $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ *ist unmöglich.*

Angenommen, $\mathfrak{m} = \mathfrak{m}'\mathfrak{m}$. Sei $x \in \mathfrak{m}' \Rightarrow x\mathfrak{m} \subset \mathfrak{m}$. Iterativ folgt

$$x^2\mathfrak{m} = x(x\mathfrak{m}) \subset x(\mathfrak{m}) \subset \mathfrak{m} \Rightarrow \cdots \Rightarrow x^n\mathfrak{m} \subset \mathfrak{m} \text{ für alle } n \geq 1$$

Sei $0 \neq d \in \mathfrak{m}$, also $x^n d \in A$ für alle n. Dann ist $A[x]$ ein gebrochenes Ideal (mit Hauptnenner d), also endlich erzeugter A-Modul. Also ist x ganz über A. Dies

bedeutet wiederum, dass $x \in A$, da A ganz abgeschlossen ist. Also $\mathfrak{m}' \subset A$. Die Inklusion $A \subset \mathfrak{m}'$ war trivial, also haben wir $A = \mathfrak{m}'$ gezeigt. Insgesamt:

$$A = \{x \in Q(A) \mid x\mathfrak{m} \subset A\}$$

Sei nun $0 \neq a \in \mathfrak{m}$, also $(a) \neq 0$. Nach Lemma 4.14 gibt es Primideale ungleich null mit $\mathfrak{p}_1 \dots \mathfrak{p}_n \subset (a)$. Ohne Einschränkung sei n minimal. Es folgt

$$\mathfrak{m} \supset (a) \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$$

Angenommen, für alle i ist $\mathfrak{p}_i$ ist nicht in $\mathfrak{m}$ enthalten, d.h. es gibt $x_i \in \mathfrak{p}_i \setminus \mathfrak{m}$. Dann gilt $x_1 \dots x_n \in \mathfrak{p}_1 \dots \mathfrak{p}_n \subset \mathfrak{m}$. Dies ist ein Widerspruch zu $\mathfrak{m}$ Primideal. Also gibt es ein i mit $\mathfrak{p}_i \subset \mathfrak{m}$, z.B. $i = n$. Nach Definition ist $\mathfrak{p}_n \neq 0$. Da A eindimensional ist, folgt $\mathfrak{p}_n = \mathfrak{m}$. Damit:

$$\mathfrak{m} \supset (a) \supset \mathfrak{m}I \text{ mit } I = \mathfrak{p}_1 \dots \mathfrak{p}_{n-1}$$

I ist nicht in (a) enthalten, da n minimal gewählt war. Sei $b \in I \setminus (a)$. Wegen $\mathfrak{m}I \subset (a)$ folgt $\mathfrak{m}b \subset (a) = Aa$. Dies impliziert $\mathfrak{m}ba^{-1} \subset A$. Also nach Definition: $ba^{-1} \in \mathfrak{m}' = A \Leftrightarrow b \in (a)$. Dies ist ein Widerspruch zur Wahl des Elementes b. □

Theorem 4.15. *Sei A ein Dedekindring,* $\operatorname{Spm} A$ *die Menge der maximalen Idealevon A.*

(i) Jedes gebrochene Ideal ungleich Null schreibt sich eindeutig als

$$I = \prod_{\mathfrak{p} \in \operatorname{Spm} A} \mathfrak{p}^{v_\mathfrak{p}(I)}$$

mit $v_\mathfrak{p}(I) \in \mathbb{Z}$ fast alle null.

(ii) Es gilt $v_\mathfrak{p}(I) \geq 0$ für alle $\mathfrak{p}$ genau dann, wenn I ein ganzes Ideal ist.

(iii) Der Monoid der gebrochenen Ideale ungleich Null ist eine Gruppe.

Beweis: Zur Existenz: Es gilt $dI \subset A$, $I = (dI)(d^{-1})$. Daher genügt es, die Produktzerlegung für ganze Ideale zu zeigen, so dass gleichzeitig (ii) gilt. Sei Φ die Menge der Ideale, die keine Primidealfaktorisierung hat. Angenommen, $\Phi \neq \emptyset$. Da A noethersch ist, hat Φ ein maximales Element I. Es ist $I \neq A$, da $A = \prod_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}^0$. Also ist $I \subset \mathfrak{p}$ für ein maximales Ideal $\mathfrak{p}$. Sei $\mathfrak{p}' = \mathfrak{p}^{-1}$ das Inverse als gebrochenes Ideal. Wir betrachten $I' = I\mathfrak{p}'$. Es folgt

$$I \subset \mathfrak{p} \Rightarrow I' = I\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = A$$

d.h. auch I' ist ein ganzes Ideal. Wegen $A \subset \mathfrak{p}'$ gilt $I \subset I' = I\mathfrak{p}$.

Behauptung. $I \subsetneq I'$

Angenommen, die Ideale sind gleich. Sei $x \in \mathfrak{p}'$. Nach Annahme ist $xI \subset I$, also iterativ $x^n I \subset I$ für alle n. Ein Hauptnenner für I ist auch ein Hauptnenner für $A[x]$, also ist dieser Modul endlich erzeugt und x ganz über A. Damit ist $x \in A$. Wir haben $\mathfrak{p}' = A$ gezeigt, dies ist ein Widerspruch.

Nach Wahl von $I \in \Phi$ ist nun $I' \notin \Phi$. Es gilt

$$I' = \mathfrak{p}_1^{v_1} \dots \mathfrak{p}_n^{v_n} \Rightarrow I = \mathfrak{p}\mathfrak{p}' I = \mathfrak{p}\mathfrak{p}_1^{v_1} \dots \mathfrak{p}_n^{v_n}$$

Tatsächlich sind hierbei die Exponenten alle größer gleich 0.
Zur Eindeutigkeit: Sei $\prod \mathfrak{p}^{n_\mathfrak{p}} = \prod \mathfrak{p}^{m_\mathfrak{p}}$, also $\prod \mathfrak{p}^{n_\mathfrak{p} - m_\mathfrak{p}} = A$. Wir schreiben die Gleichung so um, dass alle Exponenten größer gleich Null und minimal sind. Wir erhalten also

$$\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k} = \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_l^{m_l}$$

mit $\mathfrak{p}_i \neq \mathfrak{q}_j$ für alle i, j und $n_i, m_j > 0$. Es gilt $\mathfrak{p}_1 \supset \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_l^{m_l}$. Also enthält $\mathfrak{p}_1$ eines der $\mathfrak{q}_j$ (wie im Beweis von Theorem 4.13). Da A ein Dedekindring ist, folgt $\mathfrak{p}_1 = \mathfrak{q}_j$, Widerspruch.
Die Behauptung über die Gruppenstruktur ist nun klar. □

Definition 4.16. *Die* Idealklassengruppe *oder Klassengruppe des Zahlkörpers K ist*

$$\mathrm{Cl}(K) = \frac{\textit{Gruppe der gebrochenen Ideale} \neq 0}{\textit{Hauptideale} \neq 0}$$

Die Klassenzahl *h ist die Anzahl der Elemente von* $\mathrm{Cl}(K)$.

Bemerkung. $h = 1$ bedeutet, dass jedes Ideal ein Hauptideal ist. Die Klassenzahl misst also, wie weit $\mathcal{O}_K$ davon abweicht, ein Hauptidealring zu sein. Sie ist endlich (tief! später)

Lemma 4.17. *Die Klassengruppe ist isomorph zur Halbgruppe der echten Ideale ungleich 0 mit Äquivalenzrelation $I(g) \sim I(f)$ für $f, g \in A \setminus \{0\}$.*

Beweis: Sei C' die im Lemma definierte Halbgruppe. Sie bildet sich in die Klassengruppe ab. Jedes gebrochene Ideal ist äquivalent zu einem echten Ideal, also ist die Abbildung surjektiv. Die Äquivalenzrelation ist offensichtlich die gleiche, also ist sie auch injektiv. □

Dieser Beschreibung sieht man die Existenz des Inversen nicht an! Man spart also keine Arbeit gegenüber unserem Ansatz.

Beispiel

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Es gilt $\mathcal{O} \cong \mathbb{Z}[X]/(X^2 + 5)$. Wir bestimmen die Primideale: Sei $\mathfrak{p} \subset \mathcal{O}$ prim, $(p) = \mathfrak{p} \cap \mathbb{Z}$ für $p \in \mathbb{Z}$ Primzahl.

(i) $p = 2$: Wir haben

$$\mathcal{O}/(2) = \mathbb{Z}[X]/(X^2 + 5, 2) = \mathbb{F}_2[X]/X^2 + 1 = \mathbb{F}_2[X]/(X + 1)^2$$

Also ist (2) selbst kein Primideal von $\mathcal{O}$. Es gibt genau ein Primideal, das 2 enthält. Modulo 2 wird es von $X + 1$ erzeugt, also $P_2 = (2, \sqrt{-5} + 1)$.

(ii) $p = 3$

$$\mathcal{O}/(3) = \mathbb{Z}[X]/(X^2+5,3) = \mathbb{F}_3[X]/(X^2-1) = \mathbb{F}_2[X]/(X+1)(X-1)$$
$$= \mathbb{F}_3[X]/(X-1) \times \mathbb{F}_3[X]/(X+1)$$

Es gibt zwei Primideale, die 3 enthalten, nämlich $P_3 = (3, \sqrt{-5}+1)$, $P_3' = (3, \sqrt{-5}-1)$. Es gilt $(3) = P_3 P_3'$ in $\mathcal{O}$. Wichtig für diese Berechnung war nur, dass -5 eine Quadratzahl modulo 3 war.

(iii) $p = 5$

$$\mathcal{O}/(5) = \mathbb{Z}[X]/(X^2+5,5) = \mathbb{F}_5[X]/X^2$$

$P_5 = (5, \sqrt{-5}) = (\sqrt{-5})$ ist das einzige Primideal, das 5 enthält. Es gilt $(5) = P_5^2$.

(iv) $p = 7$

$$\mathcal{O}/(7) = \mathbb{Z}[X]/(X^2+5,7) = \mathbb{F}_3[X]/(X^2-2) = \mathbb{F}_2[X]/(X+3)(X-3)$$
$$= \mathbb{F}_3[X]/(X-3) \times \mathbb{F}_3[X]/(X+3)$$

$P_7 = (7, \sqrt{-5} \pm 3)$ (wie Fall $p = 3$)

(v) $p = 11$ In diesem Fall ist 5 keine Quadratzahl modulo 11, das Ideal (11) ist prim in $\mathcal{O}$.

beim Rechnen modulo Hauptideale gilt also: $P_2^2 \sim 1$, $P_5 \sim 1$, $P_3 \sim (P_3')^{-1}$, $P_{11} \sim 1$ etc.
Frage: Ist P_2 ein Hauptideal? Falls $P_2 = (\alpha)$, so gibt es x, y mit

$$x\alpha = 2 \Rightarrow N(x)N(\alpha) = N(2) = 4$$
$$y\alpha = \sqrt{-5}+1 \Rightarrow N(y)N(\alpha) = N(\sqrt{-5}+1) = 6$$

Dies impliziert $N(\alpha) = 2$. Sei $\alpha = a_1 + a_2\sqrt{-5}$ $(a_i \in \mathbb{Z})$

$$a_1^2 + 5a_2^2 = 2$$

Dies führt also auf die Theorie der Lösbarkeit der quadratischen Gleichungen in $\mathbb{Z}$. Die obige ist nicht lösbar, also ist P_2 kein Hauptideal.

Man sieht bereits in diesem Beispiel: die Bestimmung der Klassengruppe ist schwierig, da sie unendlich viele Erzeuger und unendlich viele Relationen hat!

Die Frage nach Primidealen in $\mathbb{Z}[\sqrt{d}]$ führt auf die Frage, ob d eine Quadratzahl ist modulo p oder nicht. Dies wird durch Gauß' quadratisches Reziprozitätsgesetz zufriedenstellend beantwortet.

Folgerungen

Satz 4.18. *Sei A ein Dedekindring. Seien $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$ und $J = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(J)}$ ganze Ideale von A. Dann gilt*

$$I \cap J = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))}$$
$$I + J = \prod_{\mathfrak{p}} \mathfrak{p}^{\min(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))}$$

Beweis: Aus dem Struktursatz folgt, dass Enthaltenseinsrelationen sich in $\geq$-Relationen von die Exponenten $v_{\mathfrak{p}}$ übersetzen.
Wir betrachten $v_{\mathfrak{p}}(I \cap J)$. Wegen $I \cap J \subset I$ gilt $v_{\mathfrak{p}}(I \cap J) \geq v_{\mathfrak{p}}(I)$. Ebenso folgt $v_{\mathfrak{p}}(I \cap J) \geq v_{\mathfrak{p}}(J)$, also

$$I \cap J \subset \prod_{\mathfrak{p}} \mathfrak{p}^{\max(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))}$$

Die rechte Seite ist in I und J enthalten, also auch in $I \cap J$.
Die zweite Aussage wird analog gezeigt. □

Satz 4.19. *Sei A ein Dedekindring und $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$ ein ganzes Ideal. Dann gilt*

$$A/I \cong \prod A/\mathfrak{p}^{v_{\mathfrak{p}}(I)}$$

Beweis: Man beachte, dass die Produkte endlich sind, da fast alle $v_{\mathfrak{p}}(I) = 0$, fast alle $A/\mathfrak{p}^{v_{\mathfrak{p}}(I)} = 0$.
Die Ideale $\mathfrak{p}^{v_{\mathfrak{p}}(I)}$ für verschiedene maximale Ideale $\mathfrak{p}$ sind paarweise teilerfremd, d.h. $\mathfrak{p}_1^{v_1} + \mathfrak{p}_2^{v_2} = \mathcal{O}_K$ nach Satz 4.18. Ihr Schnitt ist I nach Satz 4.18. Die Aussage ist nun genau der Chinesische Restsatz. □

Lemma 4.20. *Sei A ein Dedekindring, $\mathfrak{p}$ ein maximales Ideal. Sei $\mathbb{F} = A/\mathfrak{p}$ der Restklassenkörper. Dann ist $\mathfrak{p}^v/\mathfrak{p}^{v+1}$ ein $\mathbb{F}$-Vektorraum der Dimension 1.*

Beweis: Die A-Operation auf $\mathfrak{p}^v/\mathfrak{p}^{v+1}$ faktorisiert durch $A/\mathfrak{p}$, dies definiert die Vektorraumstruktur. Wegen $\mathfrak{p}^v \neq \mathfrak{p}^{v+1}$ ist die Dimension wenigstens 1.

Behauptung. *Es gibt $y \in \mathfrak{p}^v$, das $\mathfrak{p}^v/\mathfrak{p}^{v+1}$ erzeugt.*

Sei $x \in \mathfrak{p} \setminus \mathfrak{p}^2$, also $(x) \subset \mathfrak{p}$, aber nicht $(x) \subset \mathfrak{p}^2$. Dies bedeutet $v_{\mathfrak{p}}(x) = 1$ und daher $v_{\mathfrak{p}}(x^v) = v$. Weiter ist nach Satz 4.18 $(x^v) + \mathfrak{p}^{v+1} = \mathfrak{p}^v$. Also ist x^v der gesuchte Erzeuger. □

Definition 4.21. *Sei $\mathcal{O}_K$ ein Zahlring, $I \subset \mathcal{O}_K$ ein ganzes Ideal ungleich Null. Dann heißt $N(I) = |\mathcal{O}_K/I|$* Idealnorm *von I.*

Beispiel. (i) Ist $\mathcal{O}_K = \mathbb{Z}$, so ist $I = (a)$ für $a \neq 0$. Es gilt also $N(I) = |\mathbb{Z}/(a)| = |a|$.

(ii) Ist $I = \mathfrak{p}$, so ist $\mathcal{O}_K/\mathfrak{p}$ eine ganze Erweiterung eines Körpers der Form $\mathbb{F}_p = \mathbb{Z}/(p)$, also ein endlicher Körper mit p^e Elementen.

(iii) Nach dem *Elementarteilersatz* gibt es eine Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ sowie ganze Zahlen $\lambda_1, \ldots, \lambda_n$, so dass $\lambda_1 x_1, \ldots, \lambda_n x_n$ eine Basis von I ist. Dann gilt (als Gruppe)

$$\mathcal{O}_K/I \cong \mathbb{Z}/(\lambda_1) \times \mathbb{Z}/\lambda_2 \times \cdots \times \mathbb{Z}/(\lambda_n)$$

Es folgt $N(I) = |\lambda_1 \ldots \lambda_n|$. Insbesondere ist die Idealnorm endlich.

Lemma 4.22. *Sei $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$. Dann gilt*

$$N(I) = \prod N(\mathfrak{p})^{v_{\mathfrak{p}}(I)}$$

Die Idealnorm ist multiplikativ. Ist $I = (x)$, so gilt $N(I) = |N_{K/\mathbb{Q}}(x)|$.

Beweis: Wegen des chinesischen Restsatzes genügt es, Ideale der Form $\mathfrak{p}^v$ zu betrachten. Für $v = 1$ gilt die Aussage. Wir schließen von v auf $v + 1$. Die Abbildung

$$\mathcal{O}_K/\mathfrak{p}^{v+1} \to \mathcal{O}_K/\mathfrak{p}^v$$

ist surjektiv mit Kern $\mathfrak{p}^v/\mathfrak{p}^{v+1}$. Nach Lemma 4.20 ist dies ein $\mathcal{O}_K/\mathfrak{p}$-Vektorraum der Dimension 1, hat also $N(\mathfrak{p})$-viele Elemente. Es gilt also $N(\mathfrak{p}^{v+1}) = N(\mathfrak{p}^v)N(\mathfrak{p})$.

Sei nun $I = (x)$. Nach dem Elementarteilersatz gibt es eine $\mathbb{Z}$-Basis $x_1, \ldots, x_n$ von $\mathcal{O}_K$ und ganze Zahlen $\lambda_1, \ldots, \lambda_n$, so dass $\lambda_1 x_1, \ldots, \lambda_n x_n$ eine Basis von I ist. Andererseits ist $xx_1, \ldots, xx_n$ ebenfalls eine Basis von I. Sei $u : K \to K$ durch $x_i \mapsto \lambda_i x_i$ gegeben. Sei $v : K \to K$ durch $x_i \mapsto x/\lambda_i x_i$ gegeben. Dann gilt $v \circ u = m_x$, also

$$N_{K/\mathbb{Q}}(x) = \det(v)\det(u) = \pm N(I)$$

denn v ist eine Basiswechselmatrix auf I. □

Kapitel 5

Gittertheorie

Unser Ziel ist es, die Endlichkeit der Klassengruppe zu zeigen.

Abstrakte Theorie

Definition 5.1. *Eine Untergruppe $H \subset \mathbb{R}^n$ heißt* diskret*, wenn für jede kompakte Teilmenge $K \subset \mathbb{R}^n$ der Schnitt $K \cap H$ endlich ist.*

Eine Teilmenge K ist kompakt, wenn jede offene Überdeckung eine endlich Teilüberdeckung hat. In $\mathbb{R}^n$ ist dies äquivalent dazu, dass jede Folge in K ein konvergente Teilfolge hat, oder dazu, dass sie beschränkt und abgeschlossen ist (Heine-Borel).

Beispiel. $\mathbb{Z} \subset \mathbb{R}$ ist diskret.

Satz 5.2. *Sei $H \subset \mathbb{R}^n$ diskret. Dann wird H von r Vektoren erzeugt, die linear unabhängig über $\mathbb{R}$ sind. Insbesondere gilt $H \cong \mathbb{Z}^r$ mit $\leq n$.*

Beweis: Seien $e_1, \ldots, e_r \in H$ eine maximale $\mathbb{R}$-linear unabhängige Teilmenge. Sei

$$P = \left\{ \sum \alpha_i e_i \mid 0 \leq \alpha_i \leq 1 \right\} \subset \mathbb{R}^n$$

Diese Menge ist kompakt, also $P \cap H$ endlich. Sei $x \in H$. Dann ist $x = \sum \lambda_i e_i$ mit $\lambda_i \in \mathbb{R}$. Sei $x_1 = x - \sum [\lambda_i] e_i$, wobei $[\alpha]$ die kleinste ganze Zahl kleiner gleich α ist (Gaußklammer), also $0 \leq \alpha - [\alpha] < 1$. Dies bedeutet $x_1 \in P \cap H$. Also erzeugen die e_i zusammen mit $P \cap H$ die Gruppe H. Wir konstruieren eine unendliche Folge $x_j \in H \cap P$, nämlich

$$x_j = jx - \sum [j\lambda_i] e_i$$

Da $P \cap H$ endlich ist, gibt es zwei Indices $j \neq k$ mit $x_j = x_k$. Es folgt

$$j\lambda_i - [j\lambda_i] = k\lambda_i - [k\lambda]_i \Leftrightarrow (j-k)\lambda_i = [j\lambda_i] - [k\lambda]$$

Insbesonder ist λ_i rational. Damit liegt die endlich erzeugte abelsche Gruppe H in dem $\mathbb{Q}$-Vektorraum, der von $e_1, \ldots, e_r$ erzeugt wird. Es folgt $H \cong \mathbb{Z}^r$. Die Erzeuger von H sind linear unabhängig über $\mathbb{R}$, da $e_1, \ldots, e_r$ es sind. $\square$

Definition 5.3. *Eine diskrete Untergruppe $H \subset \mathbb{R}^n$ vom Rang n heißt* Gitter. *Sei $e = \{e_1, \ldots, e_n\}$ eine Basis von H. Dann heißt*

$$P_e = \left\{ \sum \alpha_i e_i \mid 0 \leq \alpha_i < 1 \right\}$$

Fundamentalparallelogramm *von H.*

Beispiel. $\mathbb{Z}^n \subset \mathbb{R}^n$ ist ein Gitter.

Lemma 5.4. *Das Volumen von P_e bezüglich des Standardlebesgue-Maßes μ auf $\mathbb{R}^n$ ist unanhängig von der Wahl der Basis.*

Beweis: μ induziert ein Maß $\overline{\mu}$ auf $\mathbb{R}^n/H$. Es gilt $\overline{\mu}(\mathbb{R}^n/H) = \mu(P_e)$. Oder: zweite Basis in Termen der ersten ausdrücken. Sie und ihr Inverses sind ganzzahlig, also die Determinante ± 1. Der Absolutbetrag der Determinante taucht als Übergangsfaktor auf. (Forster Analysis 3, Bsp. (5.3)). □

Theorem 5.5 (Minkowski)**.** *Sei $H \subset \mathbb{R}^n$ ein Gitter, $S \subset \mathbb{R}^n$ messbar mit $\mu(S) > \mathrm{vol}(H)$. Dann gibt es $x, y \in S$, $x \neq y$ mit $x - y \in H$.*

Beweis: Sei $e_1, \ldots, e_n$ eine Basis von H, P_e das Fundamentalparallelogramm. Es gilt

$$S = \dot{\bigcup_{h \in H}} S \cap (h + P_e)$$

da $\mathbb{R}^n = \bigcup_h h + P_e$. Also gilt

$$\mu(S) = \sum_h \mu(S \cap (h + P_e) = \sum_h \mu((-h + S) \cap P_e) > \mu(P_e)$$

Also können die $(-h+S) \cap P_e)$ nicht paarweise disjunkt sein. Es gibt $h \neq h' \in H$ mit

$$P_e \cap (-h + S) \cap (-h' \cap S) \neq \emptyset$$

Also gibt es $x, y \in S$ mit $-h + x = -h' + y$. Wegen $x - y = h' - h$ liegt die Differenz in H und ist ungleich 0. □

Korollar 5.6. *Sei $H \subset \mathbb{R}^n$ ein Gitter, S messbare Teilmenge von $\mathbb{R}^n$, symmetrisch bezüglich 0 (d.h. $x \in S \Leftrightarrow -x \in S$) und konvex. Sei entweder*

(i) $\mu(S) > 2^n \mathrm{vol}(H)$ *oder*

(ii) $\mu(S) \geq 2^n \mathrm{vol}(H)$, *$S$ kompakt*

Dann enthält $S \cap H$ einen Punkt ungleich 0.

Beweis: Erster Fall: Sei $S' = \frac{1}{2} S$, also

$$\mu(S') = \frac{1}{2^n} \mu(S) > \mathrm{vol}(H)$$

Nach dem Theorem von Minkowski gibt es $x, y \in S'$ mit $0 \neq z = x - y \in H$. Es gilt $z = \frac{1}{2}(2x + (-2y)) \in S \cap H$ wie gewünscht.
Zweiter Fall: Wende den ersten Fall an auf $(1+\varepsilon)S$ mit $\varepsilon > 0$. Es folgt

$$(H \setminus \{0\}) \cap (1+\varepsilon)S \neq \emptyset$$

Dabei ist der Schnitt endlich, da H diskret und S kompakt. Dann ist auch

$$\bigcap_{\varepsilon > 0} (H \setminus \{0\}) \cap (1+\varepsilon)S \neq \emptyset$$

Ein Element im Schnitt liegt in $H \setminus \{0\}$ und in $\bigcap_{\varepsilon>0}(1+\varepsilon)S = S$. □

Die kanonische Einbettung

Sei $K/\mathbb{Q}$ ein Zahlkörper, $n = [K : \mathbb{Q}]$. Dann gibt es n verschiedene Körperhomomorphismen

$$\sigma_i : K \to \mathbb{C}$$

Beispiel. $K = \mathbb{Q}(\sqrt{d})$, $\sigma_i(\sqrt{d}) = \pm\sqrt{d}$.

Zwei Fälle sind zu unterscheiden: $\sigma_i = \overline{\sigma_i}$ (komplexe Konjugation) genau dann, wenn $\sigma_i(K) \subset \mathbb{R}$. In diesem Fall heißt σ_i *reelle Einbettung.*
Andernfalls ist $\overline{\sigma_i} = \sigma_j$ für ein $j \neq i$. In diesem Fall heißt σ_i *komplexe Einbettung.* σ_i und σ_j sind konjugiert.

Bemerkung. Jedes σ_i induziert eine Absolutbetrag auf K via $|x| = |\sigma_i(x)|$. Die Komplettierung von K bezüglich dieses Absolutbetrages ist dann $\mathbb{R}$ bzw. $\mathbb{C}$ für reelle bzw. komplexe Einbettungen.

Sei r_1 die Anzahl der reellen Einbettungen von K, r_2 die Anzahl der Paare von komplexen Einbettungen, also $n = r_1 + 2r_2$. Wir nummerieren die σ_i so, dass σ_i reell für $i \leq r_1$, σ_{r_1+i} konjugiert zu $\sigma_{r_1+r_2+i}$. Wir schreiben $r = r_1 + r_2$.

Beispiel. $K = \mathbb{Q}(\sqrt{d})$ $n = 2$. Falls $d > 0$: $r_1 = 2, r_2 = 0, r = 2$. Falls $d < 0$: $r_1 = 0, r_2 = 1, r = 1$.

Definition 5.7. *Die* kanonische Einbettung *ist*

$$\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$$

via $\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha))$.

Bemerkung. σ ist ein injektiver Ringhomomorphismus.

Satz 5.8. *Sei $M \subset K$ freier $\mathbb{Z}$-Untermodul vom Rang n, $x_1, \ldots, x_n$ Basis von M. Dann ist $\sigma(M)$ ein Gitter in $\mathbb{R}^n$ mit Volumen*

$$\mathrm{vol}(\sigma(M)) = 2^{-r_2} |\det(\sigma_i(x_j)_{i,j=1}^n)|$$

Beweis: $\sigma(x_i)$ ist der Vektor

$$(\sigma_1(x_i), \dots, \sigma_{r_1}(x_i), \mathrm{Re}\sigma_{r_1+1}(x_i), \mathrm{Im}\sigma_{r_1+1}(x_i), \dots, \mathrm{Re}\sigma_r(x_i), \mathrm{Im}\sigma_r(x_i))$$

Zu berechnen $\mathrm{vol}(\sigma(M)) = |\det(\sigma(x_i))|$. Falls diese Zahl ungleich 0 ist, sind die $\sigma(x_i)$ linear unabhängig über $\mathbb{R}$ und ein Gitter.
Es gilt $\mathrm{Re}z = \frac{1}{2}(z + \overline{z}), \mathrm{Im}z = \frac{1}{2i}(z - \overline{z})$. Es folgt

$$\begin{aligned}(\mathrm{Re}\sigma_{r_1+j}(x_i), \mathrm{Im}\sigma_{r_1+j}(x_i)) &= \left(\frac{1}{2}(\sigma_{r_1+j}(x_i) + \overline{\sigma_{r_1+j}(x_i)}), \frac{1}{2i}(\sigma_{r_1+j}(x_i) - \overline{\sigma_{r_1+j}(x_i)})\right) \\ &= \left(\frac{1}{2}(\sigma_{r_1+j}(x_i) + \sigma_{r+j}(x_i)), \frac{1}{2i}(\sigma_{r_1+j}(x_i) - \sigma_r(x_i))\right)\end{aligned}$$

Hieraus berechnen wird den Absolutbetrag der Determinante via Multilinearlität. Im ersten Schritt ignorieren wir den Faktor $\frac{1}{i}$, der den Betrag 1 hat. Dann beachten wir

$$\det(\dots, \frac{1}{2}(a+b), \frac{1}{2}(a-b), \dots) = -\frac{1}{2}\det(\dots, a, b, \dots)$$

und schließlich sortieren wir die σ_i um. Wir erhalten

$$|\det(\sigma(x_i)) = |\frac{1}{2^{r_2}}\det(\sigma_j(x_i))|$$

Diese Determinante ist ungleich 0, da die Charaktere σ_j linear unabhängig sind. □

Korollar 5.9. *Sei $\mathcal{O}_K \subset K$ der Ganzheitsring. Dann ist $\sigma(\mathcal{O}_K) \subset \mathbb{R}^n$ ein Gitter mit Volumen*

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-r_2} d^{1/2}$$

wobei $(d) = \mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}$, $d \in \mathbb{N}_0$ die absolute Diskriminante *ist.*

Beweis: Im Beweis von Satz 3.11 haben wir

$$D(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$$

gezeigt. $D(x_1, \dots, x_n) = \det(\mathrm{Tr}_{\mathcal{O}/\mathbb{Z}}(x_i x_j))$ war die Diskriminante, $\mathcal{D}_{\mathcal{O}/\mathbb{Z}}$ das von ihre erzeugte Hauptideal. □

Korollar 5.10. *Sei $I \subset \mathcal{O}_K$ ein Ideal ungleich 0. Dann ist $\sigma(I)$ ein Gitter mit Volumen*

$$\mathrm{vol}(\sigma(I)) = 2^{r_2} d^{1/2} N(I)$$

wobei $N(I) = |\mathcal{O}_K/I|$ die Norm des Ideals ist.

Beweis: $I \subset \mathcal{O}_K$ ist freier $\mathbb{Z}$-Modul vom Rang n. Auch $\sigma(I)$ ist ein Gitter. Wir wählen eine Basis $x_1, \dots, x_n$ von $\mathcal{O}_K$ nach dem Elementarteilersatz so, dass gleichzeitig $\lambda_1 x_1, \dots, \lambda_n x_n$ für gewisse $\lambda_i \in \mathbb{N}$ eine Basis von I ist. Damit gilt

$$N(I) = \lambda_1 \dots \lambda_n$$

Andererseits ist

$$\mathrm{vol}(\sigma(I)) = \frac{1}{2^{r_2}} |\det(\sigma(\lambda_i x_i))| = \frac{1}{2^{r_2}} |\lambda_1 \dots \lambda_n \det(\sigma(x_i))| = N(I)\mathrm{vol}(\sigma(\mathcal{O}))$$

□

Satz 5.11. *Sei K ein Zahlkörper vom Grad n über $\mathbb{Q}$, r_1 die Anzahl der reellen, r_2 die Anzahl der Paare von komplexen Einbettungen, d die Diskriminante über $\mathbb{Q}$. Sei I ein Ideal des Ganzheitsrings. Dann enthält I ein Element $x \neq 0$ mit*

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} d^{1/2} N(I)$$

Beweis: Wir betrachten die kanonische Einbettung $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Sei $t > 0$ reell,

$$B_t = \left\{ (y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum |y_i| + 2 \sum |z_j| \leq t \right\}$$

ist kompakt, konvex, symmetrisch bezüglich 0.

Behauptung. $\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$

Diese Formel wird durch Induktion nach r_1, r_2 gezeigt. Sei $V(r_1, r_2, t) = \mu(B_t)$.

(i) Es gilt

$$V(1,0,t) = \mu(\{y_1 \mid |y_1| \leq t\}) = 2t = 2^1 (\pi/2)^0 \frac{t^1}{1!}$$
$$V(0,1,t) = \mu(\{z_1 \mid 2|z_1| \leq t\}) = \pi(t/2)^2 = 2^0 (\pi/2)^1 \frac{t^2}{2!}$$

(ii) $r_1 \mapsto r_1 + 1$

$$\begin{aligned} V(r_1+1, r_2, t) &= \mu(\{(y_0, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \mid \dots\} \\ &= \int_{\mathbb{R}} V(r_1, r_2, t - |y_0|) dy_0 \\ &= \int_{-t}^{t} 2^{r_1} (\pi/2)^{r_2} \frac{(t-|y_0|)^n}{n!} dy_0 \\ &= 2^{r_1} (\pi/2)^{r_2} \frac{2}{n!} \int_0^t (t - y_0)^n dy_0 \\ &= 2^{r_1+1} (\pi/2)^{r_2} \frac{1}{n!} \left. \frac{-(t-y_0)^{n+1}}{n+1} \right|_0^t \\ &= 2^{r_1+1} (\pi/2)^{r_2} \frac{t^{n+1}}{(n+1)!} \end{aligned}$$

(iii) $r_2 \mapsto r_2 + 1$

$$\begin{aligned} V(r_1, r_2+1, t) &= \mu(\{(y_1, \dots, y_{r_1}, z_0, \dots, z_{r_2}) \mid \dots\} \\ &= \int_{\mathbb{C}} V(r_1, r_2, t - 2|z_0|) d\mu(z_0) \\ &= \int_{|z_0| \le t/2} V(r_1, r_2, t - 2|z_0|) d\mu(z_0) \\ &= \int_0^{t/2} \int_0^{2\pi} 2^{r_1} (\pi/2)^{r_2} \frac{(t-2\varrho)^n}{n!} \varrho d\varrho d\theta \\ &= 2^{r_1} (\pi/2)^{r_2} \frac{2\pi}{n!} \int_0^{t/2} (t-2\varrho)^n \varrho d\varrho \\ &= 2^{r_1} (\pi/2)^{r_2+1} \frac{t^{n+2}}{(n+2)!} \end{aligned}$$

wobei in Polarkoordinaten $z_0 = \varrho e^{i\theta}$, $d\mu(z_0) = \varrho d\varrho d\theta$, und in der letzten Zeile partielle Integration $\int u'v = uv - \int uv'$ benutzt wird

$$\begin{aligned} \int_0^{t/2} (t-2\varrho)^n \varrho d\varrho &= \int_0^x (t-x)^n x/2 dx/2 \\ &= 1/4 \left[\frac{-(t-x)^{n+1}}{n+1} x \Big|_0^x - \int_0^x \frac{-(t-x)^{n+1}}{(n+1)} dx \right] \\ &= 1/4 \left[0 - \frac{(t-x)^{n+2}}{(n+1)(n+2)} \Big|_0^x \right] \\ &= 1/4 \frac{t^{n+2}}{(n+1)(n+2)} \end{aligned}$$

Damit ist die Formel für das Volumen verifiziert. Wähle nun t so, dass $\mu(B_t) = 2^n \mathrm{vol}(\sigma(I))$, d.h.

$$2^{r_1} (\pi/2)^{r_2} \frac{t^n}{n!} = 2^{n-r_2} d^{1/2} N(I) \Rightarrow t^n = 2^{n-r_1} \pi^{-r_2} n! d^{1/2} N(I)$$

Aus dem Theorem von Minkowski, genauer Korollar 5.6 folgt die Existenz eines $0 \neq x \in I$ mit $\sigma(x) \in B_t$ so dass

$$\begin{aligned} |N(x)| = \prod_{i=1}^n |\sigma_i(x)| &= \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2 \\ &\le \left[1/n \sum_{i=1}^n |\sigma_i(x)| + 2/n \sum_{i=r_1+1}^{r_1+r_2} |\sigma_j(x)| \right]^n \\ &\le (t/n)^n \\ &= 2^{n-r_1} \pi^{-r_2} n! / n^n d^{1/2} N(I) \end{aligned}$$

da das geometrische Mittel kleiner ist als das arithmetische Mittel. □

Korollar 5.12. *Jede Idealklasse von K enthält ein ganzes Ideal J mit*

$$N(J) \leq (4/\pi)^{r_2} \frac{n!}{n^n} d^{1/2}$$

Beweis: Sei J' ein Ideal, ohne Einschränkung ist $I = J'^{-1}$ ein ganzes Ideal. Sei x wie im Satz, $J = xJ' = xI^{-1}$. Es gilt

$$N(J) = N(x)N(I)^{-1} \leq (4/\pi)^{r_2} \frac{n!}{n^n} d^{1/2} \frac{N(I)}{N(I)}$$

□

Theorem 5.13 (Dirichlet)**.** *Die Klassengruppe eines Zahlkörpers ist endlich.*

Beweis: Nach Korollar 5.12 genügt es, Klassen von Idealen zu betrachten, deren Norm kleiner gleich einer Konstante C ist. Also genügt es zu zeigen, dass es nur endlich viele Ideale mit $N(J) = q < C$ gibt für ein festes q. Es gilt

$$N(J) = |\mathcal{O}_K/J| = q \Rightarrow q \in J$$

Die Ideale von $\mathcal{O}_K$ mit $q \in J$ entsprechen genau den Idealen von $\mathcal{O}_K/(q)$. Dies ist ein endlicher Ring, hat also auch nur endlich viele Ideale. □

Beispiel. $K = \mathbb{Q}(\sqrt{-5})$, $r_1 = 0$, $r_2 = 1$, $n = 2$, Basis $1, \sqrt{-5}$. Also folgt

$$d = |\det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}|^2 = |-\sqrt{-5} - \sqrt{-5}|^2 = 4 \cdot 5 = 20$$

Die Konstante aus dem Beweis ist also

$$C = \frac{4}{\pi} \frac{2}{4} 2\sqrt{5} = 4/\pi\sqrt{5} = 2,847\ldots$$

Für $1 \in J$ ist $J = A$ das triviale Element. Ideale mit $2 \in J$ entsprechen den Idealen von $\mathbb{Z}[\sqrt{-5}]/(2) = \mathcal{O}/P_2^2$ wobei P_2 das eindeutige Primideal ist, das 2 enthält. Die Klassengruppe wird also von P_2 erzeugt. Es gilt $P_2^2 = (2)$, also die Relation $P_2^2 \sim 1$. Da $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring ist, ist die Klassengruppe isomorph zu $\mathbb{Z}/2$.

Korollar 5.14. *Sei K ein Zahlkörper vom Grad n über $\mathbb{Q}$ und Diskriminante d. Für $n \geq 2$ gilt*

$$d \geq \frac{\pi}{3} \left(\frac{(3\pi}{4} \right)^{n-1}$$

Der Quotient $n/\log d$ wird durch eine Konstante unabhängig von K beschränkt.

Beweis: Sei wie im Beweis des Theorems J ein ganzes Ideal mit

$$N(J) \leq (4/\pi)^{r_2} \frac{n!}{n^n} d^{1/2}$$

Wegen $N(J) \geq 1$ folgt

$$\begin{aligned} d^{1/2} &\geq (\pi/4)^{r_2} n^n/n! \Rightarrow \\ d &\geq (\pi/4)^{2r_2} n^{2n}/(n!)^2 \geq (\pi/4)^n n^{2n}/(n!)^2 = a_n \end{aligned}$$

da $n \geq 2r_2$ und $\pi/4 < 1$.

Behauptung. $a_n \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$.

Wir zeigen dies induktiv. Für $n = 2$ gilt wie gewünscht

$$a_2 = \pi^2/4^2 \cdot 2^4/2^2 = \pi^2/4 \ .$$

Nun $a_n \mapsto a_{n+1}$:

$$\begin{aligned} \frac{a_{n+1}}{a_n} &= \frac{\pi}{4} \cdot \frac{(n+1)^{2(n+1)} n!^2}{n^{2n}(n+1)^2} \\ &= \pi/4 \cdot \frac{(n+1)^{2n}}{n^{2n}} = \pi/4(1+1/n)^{2n} \\ &\geq \pi/4 \cdot (1 + 2n \cdot 1/n) = \pi/4 \cdot 3 \end{aligned}$$

Die zweite Aussage folgt durch Logarithmieren der Ungleichung. □

Theorem 5.15 (Hasse-Minkowski)**.** *Sei $K \neq \mathbb{Q}$ ein Zahlkörper. Dann ist seine Diskriminante ungleich* 1*.*

Beweis: $d \geq \pi/3 \cdot (3\pi/4)^{n-1} > 1$ □

Bemerkung. Wir werden später darauf zurückkommen, warum diese Aussage wichtig ist, Stichwort Verzweigung. Das Theorem besagt, dass alle Zahlkörper verzweigt über $\mathbb{Q}$ sind.

Theorem 5.16 (Hermite)**.** *Bis auf Isomorphie gibt es nur endlich viele Zahlkörper mit gegebenener Diskriminante.*

Beweis: Nach Korollar 5.14 gilt $n \leq \alpha \log d$ für eine Konstante α, d.h. der Grad ist beschränkt. Es genügt also zu zeigen, dass es nur endlich viele Körper mit gegebenem d, n, r_1, r_2 gibt. Sei zunächst $r_1 > 0$. Wir betrachten $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definiert durch

$$\{|y_1| \leq C/2, |y_i| \leq 1/2 \text{ für } i = 2, \ldots, r_1, |z_j| \leq 1/2 \text{ für } j = 1, \ldots, r_2\}$$

wobei $C = (\pi/4)^{-r_2} 2^{n-r_2} d^{1/2}$. Die Menge B ist konvex, kompakt und punktsymmetrisch bezüglich 0. Das Volumen ist

$$\mu(B) = C(1)^{r_1-1}(\pi/4)^{r_2} = 2^n \mathrm{vol}(\sigma(\mathcal{O}))$$

nach Wahl von C. Nach Korollar 5.6 gibt es $0 \neq x \in \mathcal{O} \cap B$.

Behauptung. $K = \mathbb{Q}(x)$

Nach Voraussetzung ist $|\sigma_i(x)| \leq 1/2$ für alle $i \neq 1$. Wegen

$$N(x) = \prod_{i=1}^{n} |\sigma_i(x)| \geq 1$$

folgt $\sigma_1(x) \geq 1$, insbesondere $\sigma_1(x) \neq \sigma_i(x)$ für alle $i \neq 1$. Wäre x nicht primitiv, so käme jedes Element in der Menge der $\sigma_i(x)$ mehrfach vor, also auch $\sigma_1(x)$. Folglich gilt $[\mathbb{Q}(x) : \mathbb{Q}] = n$. Dies zeigt die Behauptung.
Wegen $\sigma(x) \in B$ sind die $\sigma_i(x)$ beschränkt und damit auch alle Koeffizienten des Minimalpolynoms von x. Es gibt nur endlich viele Polynome in $\mathbb{Z}[X]$ vom Grad n mit beschränkten Koeffizienten, also auch nur endliche viele mögliche x.
Es bleibt der Fall $r_1 = 0$. In diesem Fall benutzen wir

$$B = \{|\mathrm{Im} z_1| \leq C, |\mathrm{Re} z_1| \leq 1/2, |z_i| \leq 1/2 \text{ für } i = 2, \ldots, r_2\}$$

so dass $\mu(B) = 2^n \mathrm{vol}(B)$. Wie im ersten Fall finden wir $x \in \sigma(\mathcal{O}) \cap B$ mit $|\sigma_1(x)| \geq 1$. Wiederum ist $\sigma_1(x) \neq \sigma_i(x)$ für $i \neq 1$. Wegen $\mathrm{Re}\sigma_1(x) \leq 1/2$ ist $\mathrm{Im}\sigma_1(x) \neq 0$, also ist auch $\sigma_1(x) \neq \overline{\sigma}_1(x)$. Wieder ist x primitives Element. $\square$

Kapitel 6

Die Einheitengruppe

Definition 6.1. *Sei K ein Zahlkörper. Die* Einheiten *von K sind die invertierbaren Elemente des Ganzheitsrings.*

Beispiel. $1, -1, i, -i$ sind Einheiten von $\mathbb{Q}(i)$. In $\mathbb{Q}(\sqrt{3})$ ist $2+\sqrt{3}$ eine Einheit mit Inversem $2-\sqrt{3}$.

Lemma 6.2. *$x \in K$ ist eine Einheit genau dann, wenn x ganz ist und $N(x) = \pm 1$.*

Beweis: Ist x eine Einheit, so ist $1 = N(xx^{-1}) = N(x)N(x)^{-1}$. Da die Norm eines ganzen Elementes ganz ist, folgt $N(x) = \pm 1$. Sei umgekehrt $x \in \mathcal{O}_K$ mit $N(x) = \pm 1$. Das charakteristische Polynom

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

hat ganze Koeffizienten, speziell $a_0 = \pm N(x) = \pm 1$. Es folt

$$\pm x(x^{n-1} + \cdots + a_1) = 1$$

Damit ist x eine Einheit. □

Theorem 6.3 (Dirichlet)**.** *Sei K ein Zahlkörper, r_1 die Zahl der reellen und r_2 die Zahl der komplexen Einbettungen, $r = r_1 + r_2$. Die Gruppe $\mathcal{O}_K^*$ der Einheiten von K ist isomorph zu*

$$\mathcal{O}_K^* \cong \mathbb{Z}^{r-1} \times G$$

wobei G die Gruppe der Einheitswurzeln in K ist, insbesondere eine endliche, zyklische Gruppe.

Beispiel. Für $K = \mathbb{Q}(i)$ gilt $\mathcal{O}_K^* \cong G = \{\pm 1, \pm i\}$, da $r = 0+1$. Für $K = \mathbb{Q}(\sqrt{3})$ gilt $\mathcal{O}_K^* \cong \{\pm 1\} \times \mathbb{Z}$, da $r = 2 + 0$. Tatsächlich ist $2 + \sqrt{3}$ ein Erzeuger der freien Untergruppe. Die Frage nach Erzeugern von $\mathbb{Q}(\sqrt{d})$ für $d > 0$ führt auf die Theorie der *Pellschen Gleichung*, die mit der Theorie der Kettenbrüche behandelt werden kann.

Beweis: Seien wie bisher $\sigma_1, \ldots, \sigma_{r_1}$ die reellen Einbettungen, $\sigma_{r_1}, \ldots, \sigma_r$ nichtkonjugierte komplexe Einbettungen. Die *logarithische Einbettung* $L : K^* \to \mathbb{R}^r$ ist

$$L : x \mapsto (\log|\sigma_1|, \ldots, \log|\sigma_r|) \in \mathbb{R}$$

L ist ein Gruppenhomomorphismus.
Sei $B \subset \mathbb{R}^r$ kompakt, $B' = L^{-1}(B) \cap \mathcal{O}_K^*$. Dann gibt es eine Konstante C, so dass für alle $x \in B'$ und $i = 1, \ldots, n$ gilt

$$|\sigma_i(x)| \leq C$$

Damit sind die Koeffizienten von

$$P(X) = (X - \sigma_1(x))(X - \sigma_2(x)) \ldots (X - \sigma_n(x))$$

beschränkt. Gleichzeitig sind sie ganz, da $x \in \mathcal{O}_K$. Es gibt also nur endliche viele mögliche P, daher ist B' endlich.
Dies gilt insbesondere für $G = L^{-1}(0) \cap \mathcal{O}_K^*$. Dies ist eine endliche Gruppe, besteht also nur aus endlich vielen Einheitswurzeln. Insbesondere ist sie zyklisch (Algebra). Ist umgekehrt ω eine Einheitswurzel, so gilt $|\sigma_i(\omega)| = 1$ für alle i. Damit liegt ω im Kern von L.
Nun studieren wir das Bild von $L(\mathcal{O}_K^*) \subset \mathbb{R}^r$. Nach unserer Vorüberlegung ist dies eine diskrete Untergruppe, also $L(\mathcal{O}_K^*) \cong \mathbb{Z}^s$ für $s \leq r$.

Behauptung. $s \leq r - 1$.

Für $x \in \mathcal{O}_K^*$ gilt

$$\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_2} \sigma_i(x)\overline{\sigma_i(x)}$$

Hieraus folgt

$$L(x) \in W = \left\{ (y_1, \ldots, y_r) \in \mathbb{R}^r \mid \sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_2} y_j = 0 \right\}$$

W hat Dimension $r - 1$, $L(\mathcal{O}^*)$ ist eine diskrete Untergruppe, also $s \leq r - 1$.

Behauptung. $L(\mathcal{O}^*)$ *enthält* $r - 1$ *linear unabhängige Elemente.*

Äquivalent: Für jede lineare Abbildung $f : W \to \mathbb{R}$ mit $f \neq 0$ gibt es $u \in \mathcal{O}_K^*$ mit $f(L(u)) \neq 0$. Wir identifizieren $W \cong \mathbb{R}^{r-1}$ via des Isomorphismus $(y_1, \ldots, y_r) \mapsto (y_1, \ldots, y_{r-1})$. Also schreibt sich $f(y_1, \ldots, y_r) = c_1 y_1 + \ldots c_{r-1} y_{r-1}$ für $c_i \in \mathbb{R}$. Wir wählen

$$\alpha \geq \left(\frac{2}{\pi}\right)^{r_2} d^{1/2}, \qquad \beta > \sum_{i=1}^{r-1} c_i \log \alpha$$

Wir werden eine Folge $x_h \in \mathcal{O}_K \setminus \{0\}$ konstruieren mit

$$|f(L(x_h)) - 2\beta h| < \beta, |N(x_h)| \leq \alpha$$

Aus der ersten Bedingung folgt $(2h-1)\beta < f(L(x_h)) < (2h+1)\beta$, also sind die $f(L(x_h))$ paarweise verschieden. Die $|N(x_h)|$ sind beschränkt und ganz, also gibt es nur endliche viele Ideale (x_h). Also gibt es zwei Indizes h, h' mit $(x_h) = (x_{h'})$. Dies bedeutet, dass es $u \in \mathcal{O}_K^*$ gibt mit $x_h = ux_{h'}$. Außerdem

$$f(L(u)) = f(L(x_h)) - f(L(x_{h'})) \neq 0$$

Damit wäre das Theorem gezeigt.
Wir konstruieren nun die x_h. Wähle $\lambda_1, \ldots, \lambda_r$ mit

$$\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r} \lambda_j^2 = \alpha, \qquad \sum_{i=1}^{r-1} c_i \log \lambda_i = 2\beta h$$

Dies ist möglich für $r \geq 2$. Im Fall $r = 1$ ist $s = 0$, und es ist nichts zu zeigen. Sei nun

$$B = \{(y_i, z_j) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_i| \leq \lambda_i, |z_j| \leq \lambda_{j+r_r}\}$$

Diese Menge ist kompakt, symmetrisch und konvex. Sie hat das Maß

$$\begin{aligned}\mu(B) = \prod_{i=1}^{r_1}(2\lambda_i) \prod_{j=1}^{r_2} \pi\lambda_j^2 &= 2^{r_1}\pi^{r_2}\alpha \\ &\geq 2^{r_1}\pi^{r_2}\left(\frac{2}{\pi}\right)^{r_2} d^{1/2} = 2^{n-r_2}d^{1/2} = 2^n \mathrm{vol}(\sigma(\mathcal{O}_K))\end{aligned}$$

Nach dem Theorem von Minkowski, Korollar 5.6 gibt es $x \in \mathcal{O}_K$, $x \neq 0$ mit $|\sigma_i(x)| \leq \lambda_i$ für alle i. Andererseits

$$|\sigma_i(x)| = \frac{|N(x)|}{\prod_{j\neq i} |\sigma_j(x)|} \geq \frac{1}{\prod_{j\neq i} \lambda_j} = \alpha^{-1}\lambda_i$$

Also

$$\begin{aligned}\lambda_i\alpha^{-1} \leq |\sigma_i(x)| \leq \lambda_i \Rightarrow \\ \log\lambda_i - \log\alpha \leq \log|\sigma_i(x)| \leq \log\lambda_i \Rightarrow \\ \log\alpha \geq \log\lambda_i - \log|\sigma_i(x)| \geq 0\end{aligned}$$

Wir überprüfen nun die gewünschten Eigenschaften von x:

$$|f(L(x)) - 2\beta h| = \left|\sum_{i=1}^{r-1} c_i \log|\sigma_i(x)| - \sum_{i=1}^{r-1} c_i \log\lambda_i\right| \leq \sum_{i=1}^{r-1} |c_i| \log\alpha < \beta$$

$$|N(x)| = \prod_{i=1}^{n} |\sigma_i(x)| \leq \prod_{i=1}^{n} \lambda_i = \alpha$$

□

Die analytische Klassenzahlformel

Definition 6.4. *Sei K Zahlkörper vom Grad n mit r_1 reellen und r_2 imaginär Einbettungen, $r = r_1 + r_2$. Seien $\varepsilon_1, \ldots, \varepsilon_{r-1}$ eine Basis des freien Anteils von $\mathcal{O}_K^*$. Seien $\sigma_1, \ldots, \sigma_r : K \to \mathbb{C}$ paarweise verschiedene und paarweise nicht konjugierte Einbettungen. Sei $N_i = 1$ falls σ_i reell und $N_i = 2$, falls σ_i imaginär. Dann heißt*

$$R_K = \left|\det(N_i \log|\sigma_i(\varepsilon_j)|_{i,j=1}^{r-1}\right|$$

Dirichlet-Regulator *von K.*

Bemerkung. Die letzte Einbettung σ_r bleibt also unberücksichtigt!

Definition 6.5. *Sei K Zahlkörper, s eine komplexe Variable.*

$$\zeta_K(s) = \sum_I \frac{1}{N(I)^s}$$

(hierbei durchlauft I die ganzen Ideale ungleich 0) heißt Dedekindsche Zeta-Funktion *von K.*

Beispiel. $K = \mathbb{Q}$, dann durchäuft I die Menge (n) für $n \in \mathbb{N}$, also

$$\zeta_{\mathbb{Q}}(s)) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

die Riemannsche Zeta-Funktion.

Theorem 6.6. *ζ_K konvergiert absolut und lokal gleichmäßig für* $\mathrm{Re}\, s > 1$ *und hat eine holomorphe Fortsetzung nach $\mathbb{C} \setminus \{1\}$. In 1 hat die Funktion einen einfachen Pol. Sie erfüllt eine Funktionalgleichung, die s und $1 - s$ verbindet.*

Beweis: Z.B. Neukirch, Algebraic Number theory, Chapter VII, §5, Lang Algebraic Number theory VIII, §2. □

Theorem 6.7 (Analytische Klassenzahlformel)**.** *Sei K Zahlkörper vom Grad n mit r_1 reellen und r_2 komplexen Einbettungen. Sei w die Anzahl der Einheitswurzeln in K. Dann ist*

$$\mathrm{Res}_1\, \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_k h}{w d^{1(2}}$$

Beweis: Man betrachtet die partiellen Zeta-Funktionen, bei denen über die Ideale einer festen Klasse summiert wird. Dann heißt es sorgfältig abschätzen in unseren bisherigen Überlegungen. Wieder siehe Neukirch, Lang o.ä. □

Bemerkung. Die Formel wird einfacher für $s = 0$. Dort hat ζ_K meist eine Nullstelle. Der führende Koeffizient der Taylorentwicklung ist

$$-\frac{hR}{w}$$

Die Klassenzahlformel wird - sowohl theoretisch, als auch praktisch - benutzt, um die Klassenzahl zu berechnen. Alle anderen Terme, auch das Residuum sind leichter zu berechnen als die Klassenzahl.

Kapitel 7

Verzweigung

Sei L/K eine Erweiterung von Zahlkörpern, $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, $\mathcal{O}_L\mathfrak{p}$ das von $\mathfrak{p}$ erzeugte Ideal von $\mathcal{O}_L$. Nach Theorem 4.15 gilt

$$\mathcal{O}_L\mathfrak{p} = \prod_{i=1}^{k} \mathfrak{P}_i^{e_i}$$

wobei die $\mathfrak{P}_i$ Primideale von $\mathcal{O}_L$ sind, nämlich genau diejenigen, die $\mathfrak{p}$ enthalten.

Definition 7.1. $\mathfrak{P}_i$ *heißt* Primideal von L über $\mathfrak{p}$. *Wir sagen auch,* $\mathfrak{P}_i|\mathfrak{p}$ *(* $\mathfrak{P}_i$ *teilt* $\mathfrak{p}$*). Der Exponent* $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ *heißt* Verzweigungsgrad von L/K in $\mathfrak{P}_i$. *Die Erweiterung* L/K *heißt* unverzweigt*, wenn* $e(\mathfrak{P}/\mathfrak{p}) = 1$ *für alle Primideale* $\mathfrak{p}$ *von* K *und alle* $\mathfrak{P}|\mathfrak{p}$. *Der Körper* $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ *heißt* Restklassenkörper *von* K *in* $\mathfrak{p}$. *Die Zahl* $f(\mathfrak{P}_i/\mathfrak{p}) = [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})]$ *heißt* Restklassengrad *von* L/K *in* $\mathfrak{P}_i$.

Satz 7.2 (Gradformel)**.** $[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p})$.

Beweis, erster Versuch: Sei zunächst $K = \mathbb{Q}$, also $\mathcal{O}_K = \mathbb{Z}$, $\kappa((p)) = \mathbb{F}_p$. Dann ist $[L : \mathbb{Q}] = \mathrm{rg}\mathcal{O}_L = \dim_{\mathbb{F}_p} \mathcal{O}_L/(p)$.

$$\mathcal{O}_L/(p) = \mathcal{O}_L/\prod_{i=1}^{k} \mathfrak{P}_i^{e_i}$$

Wegen der Multiplikativität der Norm von Idealen gilt

$$N((p)) = |\mathcal{O}_L/(p)| = \prod_{i=1}^{k} N(\mathfrak{P}_i)^{e_i}$$

Gleichzeitig handelt es sich um $\mathbb{F}_p$-Vektorräume mit

$$|\mathcal{O}_L/(p)| = p^{\dim_{\mathbb{F}_p} \mathcal{O}_L/(p)}, \qquad N(\mathfrak{P}_i) = p^{\dim \mathcal{O}_L/\mathfrak{P}_i}$$

Mit anderen Worten, $p^{[L:\mathbb{Q}]} = \prod_{i=1}^{k} p^{e_i f_i}$.
Für allgemeines K funktioniert dieser Beweis nicht, denn i.a. ist $\mathcal{O}_L$ kein freier $\mathcal{O}_K$-Modul. □

Satz 7.3. *Sei A ein Dedekindring, $K = Q(A)$, $\mathfrak{p} \subset A$ ein Primideal, $S = A \setminus \mathfrak{p}$. Dann ist*

$$A_{\mathfrak{p}} = S^{-1}A = \left\{ \frac{a}{s} \in K \mid a \in A, s \in S \right\}$$

ein Hauptidealring mit einem einzigen Primideal, nämlich $\mathfrak{P} = S^{-1}\mathfrak{p}$. Es gilt $A/\mathfrak{p} = A_{\mathfrak{p}}/\mathfrak{P}$.

Hauptidealringe mit nur einem Primideal heißen auch *diskrete Bewertungsringe*.

Beweis: $A_{\mathfrak{p}}$ ist ebenfalls ein Dedekindring, wie man leicht sieht.

(i) (Integritätsring) $a/s \cdot a'/s' = aa'/(ss') = 0$ genau dann wenn $aa' = 0$, also $a = 0$ oder $a' = 0$.

(ii) (ganz abgeschlossen) $x \in Q(A_{\mathfrak{p}}) = Q(A) = K$, ganz über $\mathfrak{p}$. Dann genügt es einer Gleichung

$$x^n + \frac{a_1}{s_1}x^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

mit $a_i \in A$, $s_i \in S$. Sei $s = s_1 \dots s_n$. Dann ist sx ganz über A, also $sx \in A$, da A ganz abgeschlossen ist. Es folgt $x = sx/s \in A_{\mathfrak{p}}$.

(iii) (noethersch) Sei $I \subset A_{\mathfrak{p}}$ ein Ideal, $I' = A \cap I$. Als Ideal von A ist I' endlich erzeugt.

Behauptung. $S^{-1}I' = I$.

Die Inklusion $\subset$ ist klar. Sei umgekehrt $x = a/s \in I$. Dann liegt $a = sx \in A \cap I$, und daher $x = \frac{sa}{x} \in S^{-1}I$.

(iv) (Dimension 1) Sei nun $I \subset A_{\mathfrak{p}}$ prim, also $I' = A \cap I$ ein Primideal von A. Dann ist I' entweder 0 oder maximal. Hieraus folgt, dass auch $S^{-1}I'$ entweder 0 ist oder maximal.

Wir bestimmen nun die Menge Primideale von $A_{\mathfrak{p}}$:

$$\operatorname{Spec} A_{\mathfrak{p}} = \{S^{-1}\mathfrak{q} \mid \mathfrak{q} \subset A \text{ prim } \}$$

Sei nun $\mathfrak{q} \neq \mathfrak{p}$ ein maximales Ideal, d.h. $\mathfrak{q} \setminus \mathfrak{p} \neq \emptyset$. Sei $s \in \mathfrak{q} \setminus \mathfrak{p} \subset S$. Dann gilt

$$1 = s/s = 1/s \cdot s/1 \in S^{-1}\mathfrak{q} \Rightarrow S^{-1}\mathfrak{q} = A_{\mathfrak{p}}$$

Also ist $A_{\mathfrak{p}}$ lokal mit maximalem Ideal $\mathfrak{P} = S^{-1}\mathfrak{p}$. Nach Theorem 4.15 hat jedes Ideal von $A_{\mathfrak{p}}$ die Form $\mathfrak{P}^n$ mit $n \in \mathbb{N}_0$. Sei $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, d.h.

$$\mathfrak{P} \supset (\pi) \supset \mathfrak{P}^2$$

Wegen $(\pi) \neq \mathfrak{P}^2$ folgt $\mathfrak{P} = (\pi)$, denn andere Ideale gibt es nicht. Damit ist $A_{\mathfrak{p}}$ ein Hauptidealring. Schließlich betrachten wir $A/\mathfrak{p} \to A_{\mathfrak{p}}/\mathfrak{P}$. Dies ist ein wohldefinierter Körperhomomorphismus. Sei $a/s \in A_{\mathfrak{p}}$. Wegen $s \in A \setminus \mathfrak{p}$ gilt $\overline{s} \neq 0$ in $A/\mathfrak{p}$. Dann ist $\overline{s}^{-1}a$ ein Urbild von a/s. Die Abbildung ist surjektiv, also bijektiv. □

Beweis von Satz 7.2. Sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, L/K eine Erweiterung und

$$\mathcal{O}_L\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$$

Sei $S = \mathcal{O}_K \setminus \mathfrak{p}$, $\mathcal{O}_{K,\mathfrak{p}} = S^{-1}\mathcal{O}_K \to S^{-1}\mathcal{O}_L$ ist eine Erweiterung von Dedekindringen. Wegen $S^{-1}(II') = (S^{-1}I)(S^{-1}I')$ folgt

$$S^{-1}\mathcal{O}_L\mathfrak{p} = \prod (S^{-1}\mathfrak{P}_i)^{e_i}$$

Der Verzweigungsgrad kann also auch nach Lokalisieren an S berechnet werden, ebenso wie die lokalen Körpergrade f_i.

Behauptung. *$S^{-1}\mathcal{O}_L$ ist freier $S^{-1}\mathcal{O}_K$-Modul vom Rang $[L:K]$.*

$S^{-1}\mathcal{O}_L$ ist der ganze Abschluss von $S^{-1}\mathcal{O}_K$ in L. Da $\mathcal{O}_L$ ein endlich erzeugter $\mathcal{O}_K$-Modul ist (sogar endlich erzeugt über $\mathbb{Z}$), ist auch $S^{-1}\mathcal{O}_L$ endlich erzeugt über $S^{-1}\mathcal{O}_K$. Wie im Beweis von Theorem 2.1 mit dem Hauptidealring $S^{-1}A_\mathfrak{p}$ statt $\mathbb{Z}$ folgt die Behauptung.
In dieser lokalen Situation kann das Argument aus unserem ersten Beweisversuch angewendet werden. □

Diskriminante

Wir erinnern: Sei A ein Hauptidealring, $A \to B$ eine Ringerweiterung mit $B \cong A^n$, Basis $x_1, \ldots, x_n$.

$$d_{B/A} = (\det(\mathrm{Tr}(x_i x_j)_{i,j}))$$

Speziell für $A = \mathbb{Z}$, $B = \mathcal{O}_K$ heißt der positive Erzeuger von $d_{B/A}$ absolute Diskriminante von K.

Satz 7.4. *Sei K ein Zahlkörper. Dann ist eine Primzahl $p \in \mathbb{Z}$ unverzweigt in K, genau dann wenn $p \nmid d$.*

Beweis: $\mathcal{O}_K \cong \mathbb{Z}^n$ mit $n = [K:\mathbb{Q}]$. Sei p Primzahl, $(p) = \prod \mathfrak{P}_i^{e_i}$. Die Erweiterung ist unverweigt über p, wenn $\mathcal{O}_K/(p) = \prod \mathcal{O}_K/\mathfrak{P}^{e_i}$ (chinesischer Restsatz) ein Produkt von Körpern ist. Sei $x_1, \ldots, x_n$ eine Basis von $\mathcal{O}_K$ als $\mathbb{Z}$-Modul. Dann ist $\overline{x_1}, \ldots, \overline{x_n}$ eine Basis von $\mathcal{O}_K/(p)$ als $\mathbb{Z}/(p) = \mathbb{F}_p$-Vektorraum. Nach Definition ist $d = \det(\mathrm{Tr}(x_i x_j))$, also ist $\overline{d} = \det(\mathrm{Tr}(\overline{x}_i \overline{x}_j))$ die Diskriminante von $\mathbb{F}_p \to \mathcal{O}_K/(p)$. Die Bedingung $p \nmid d$ ist äquivalent zu $\overline{d} \neq 0$. Zu zeigen ist also:

Behauptung. *$\mathbb{F}_p \to B = \mathcal{O}_K/(p)$ eine Ringerweiterung. Dann ist $d_{B/\mathbb{F}_p} \neq 0$ genau dann, wenn B ein Produkt von Körpern ist.*

Sei zunächst $B = \prod k_i$ wobei k_i endliche Körpererweiterungen von $\mathbb{F}_p$ sind. Es gilt $d_{B/\mathbb{F}_p} = \prod d_{k_i/\mathbb{F}_p}$ (rechne in Basen der k_i). Nach Satz 3.11 ist $d_{k_i/\mathbb{F}_p} \neq 0$.
Sei umgekehrt $B = \prod \mathcal{O}_K/\mathfrak{P}_i^{e_i}$ kein Produkt von Körpern. Dann enthält B ein nilpotentes Element $x \neq 0$. Ergänze $x = x_1$ zu einer Basis $x_1, \ldots, x_n$ von B. Die Produkte $x_1 x_i$ sind nilpotent, also ist Multiplikation mit $x_1 x_i$ eine nilpotente Abbildung. Daher sind alle Eigenwerte 0 und $\mathrm{Tr}(x_1 x_j) = 0$. Dann verschwindet auch die Diskriminante. □

Theorem 7.5 (Hasse-Minkowski)**.** *gibt keine Erweiterung $K/\mathbb{Q}$, die überall unverzweigt ist.*

Beweis: $K \neq \mathbb{Q} \Rightarrow d \neq 1$ nach Theorem 5.15. Also gibt es Teiler von d, also verzweigte Primzahlen. □

Korollar 7.6. *Sei L/K Erweiterung von Zahlkörpern. Dann sind nur endlich viele Primideale verzweigt.*

Beweis: $\mathbb{Z} \subset \mathcal{O}_K \subset \mathcal{O}_L$. Sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal, das in L/K verzweigt, d.h. $\mathcal{O}_L\mathfrak{p} = \prod \mathfrak{P}_i^{e_i}$ mit einem $e_i > 1$. Sei $(p) = \mathfrak{p} \cap \mathbb{Z}$. Es folgt

$$e(\mathfrak{P}_i/(p)) = e_i e(\mathfrak{p}/(p))$$

Also genügt es, $K = \mathbb{Q}$ zu betrachten. Dann sind die verzweigten Primideale die Teiler von d, also gibt es nur endlich viele. □

Bemerkung. Allgemeiner besagt *Klassenkörpertheorie*: $K/\mathbb{Q}$ ein Zahlkörper. Dann gibt es eine Erweiterung H/K, den *Klassenkörper* mit

(i) H ist maximale unverzweigte Erweiterung von K

(ii) $\mathcal{O}_H$ ist ein Hauptidealring

(iii) $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$

Literatur: Lang, "algebraic number theory", part II, Neukirch, Ch. 4-6, Cassels-Fröhlich, Ch.VII

Für allgemeine L/K ist $\mathcal{O}_L$ kein freier $\mathcal{O}_K$-Modul, daher ist die Diskriminante bisher nicht definiert worden.

Definition 7.7. *Sei L/K Erweiterung von Zahlkörpern. Dann ist ist das* Diskriminantenideal *definiert als*

$$\mathcal{D}_{L/K} = \prod \mathfrak{p}^{v(\mathfrak{p})} \subset \mathcal{O}_K$$

mit $d_{\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}}} = \mathfrak{p}_{\mathfrak{p}}^{v(\mathfrak{p})} \subset \mathcal{O}_{K,\mathfrak{p}}$.

Bemerkung. Da $\mathcal{O}_{K,\mathfrak{p}}$ ein Hauptidealring ist, ist die Diskriminante von $\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}}$ definiert. Da fast alle Primideale unverzweigt sind, ist $v(\mathfrak{p}) = 0$ fast immer.

Korollar 7.8. *L/K unverzweigt in $\mathfrak{p}$ genau dann, wenn $\mathcal{D}_{L/K} \nmid \mathfrak{p}$.*

Beweis: Verzweigung ist eine lokale Eigenschaft, ebenso die Teilbarkeit von Idealen. Wir lokalisieren also in $\mathfrak{p}$. Danach ist der Beweis der gleiche wie in 7.4 mit $\mathcal{O}_{K,\mathfrak{p}}$ statt $\mathbb{Z}$. □

Beispiele

Sei $K/\mathbb{Q}$ quadratisch, $(p) = \prod_{i=1}^{g} \mathfrak{p}_i$ Dann gibt es in $2 = \sum_{i=1}^{g} e_i f_i$ nur drei Möglichkeiten:

$$\begin{cases} g = 1, e = 2, f = 1 & p \text{ ist } \textit{rein verzweigt} \\ g = 2, e = 1, f = 1 & p \text{ ist } \textit{zerlegt} \\ g = 1, e = 1, f = 2 & p \text{ ist } \textit{träge} \end{cases}$$

Wir bestimmen die verzweigten Primzahlen: Sei $K = \mathbb{Q}(\sqrt{\delta})$ mit $\delta = 2, 3 \mod 4$, also $\mathcal{O}_K = \mathbb{Z}[\sqrt{\delta}]$, $d = 4\delta$. Die Erweiterung ist verzweigt in 2 und Teilern von δ.
Für $\delta = 1 \mod 4$ ist $1, (1 + \sqrt{\delta})/2$ eine Basis von $\mathcal{O}_K$.

$$d = \det \begin{pmatrix} 1 & 1 \\ (1+\sqrt{\delta})/2 & (1-\sqrt{\delta})/2 \end{pmatrix}^2 = [(1-\sqrt{\delta})/2 - (1-\sqrt{\delta})/2]^2 = \delta$$

In diesem Fall ist also 2 unverzweigt.
Beispiele für träge und zerlegte Primzahlen haben wir bereits gesehen: In $\mathbb{Q}(\sqrt{-5})$ ist 3 zerlegt und 11 träge. Das quadratische Reziprozitätsgesetz impliziert, dass es das Zerlegungsverhalten nur von den Restklassen von $p \mod 5$ abhängt. Nach dem *Dirichletschen Dichtesatz* hat enthält jede Restklasse $\mod 5$ (ungleich 0) unendliche viele Primzahlen. Beide Fälle kommen also unendlich oft vor.

Galoistheorie

Sei nun L/K eine Galoiserweiterung von Zahlkörpern, d.h.

$$[L : K] = \mathrm{Gal}(L/K) \Leftrightarrow L^{\mathrm{Gal}(L/K)} = K$$

wobei $\mathrm{Gal}(L/K) = \{\sigma : L \to L \mid \sigma|_K = \mathrm{id}\}$. Dies ist äquivalent dazu, dass L/K normal ist, d.h. für $\alpha \in L$ liegen alle Nullstellen des Minimalpolynoms in L.

Lemma 7.9. *Sei L/K eine Galoiserweiterung von Zahlkörpern. Dann operiert $\mathrm{Gal}(L/K)$ auf $\mathcal{O}_L$, auf den Primidealen von $\mathcal{O}_L$ und auf den Primidealen von $\mathcal{O}_L$ über $\mathfrak{p} \subset \mathcal{O}_K$.*

Beweis: Sei $\sigma \in \mathrm{Gal}(L/K)$, $x \in \mathcal{O}_L$, d.h. es gibt eine Polynomgleichung

$$x^n + a_1 x^{n-1} + \ldots a_n = 0 \qquad a_i \in \mathcal{O}_K$$

Anwenden von σ auf diese Gleichung ergibt

$$\sigma(x)^n + a_1 \sigma(x)^{n-1} + \cdots + a_n = 0$$

Damit ist auch $\sigma(x)$ ganz.
Sei nun $\mathfrak{q} \subset \mathcal{O}_L$ ein Primideal. Wir betrachten $\sigma(\mathfrak{q})$. Dies ist offensichtlich ein Ideal. Sei $ab \in \sigma(\mathfrak{q})$, also $\sigma^{-1}(a)\sigma^{-1}(b) \in \mathfrak{q}$. Da $\mathfrak{q}$ ein Primideal ist, folgt $\sigma^{-1}a \in \mathfrak{q}$ oder $\sigma^{-1}b \in \mathfrak{q}$, also $a \in \sigma(\mathfrak{q})$ oder $b \in \sigma(\mathfrak{q})$.
Schließlich sei $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. Dann gilt $\sigma(\mathfrak{q}) \cap \mathcal{O}_K = \mathfrak{p}$, denn σ lässt Elemente von $\mathcal{O}_K$ invariant. □

In dieser Situation heißen $\mathfrak{q}$ und $\sigma(\mathfrak{q})$ *konjugiert*. Verzweigungsindex und Restklassengrad von konjugierten Idealen stimmen überein.

Lemma 7.10. *Sei L/K Galoiserweiterung von Zahlkörpern. Je zwei Primideale von $\mathcal{O}_L$ über $\mathfrak{p} \subset \mathcal{O}_K$ sind konjugiert. Es gilt*

$$[L : K] = gfe$$

wobei g die Anzahl der Primideale über $\mathfrak{p}$ ist, e der Verzweigungsindex, f der Restklassengrad.

Beweis: Die Formel folgt aus der ersten Aussage mit der Gradformel. Seien $\mathfrak{q}, \mathfrak{q}'$ über $\mathfrak{p}$ nicht konjugiert, also $\sigma(\mathfrak{q}')$ nicht in $\mathfrak{q}$ enthalten für alle σ. Seien $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_k$ die Konjugierten von $\mathfrak{q}'$. Wir wählen $x_{ij} \in \mathfrak{q}'_j \setminus \mathfrak{q}'_i$ für $i \neq j$ und $x_i \in \mathfrak{q} \setminus \mathfrak{q}'_i$. Sei

$$x = x_1 \prod_{1 \neq j} x_{1j} + x_2 \prod_{2 \neq j} x_{2j} + \cdots + x_k \prod_{k \neq j} x_{kj}$$

Es gilt $x \in \mathfrak{q}$, da $x_i \in \mathfrak{q}$. Andererseits ist $x \notin \mathfrak{q}'_j$, denn jeder Summand außer dem zu j enthält einen Faktor in $\mathfrak{q}'_j$ (nämlich x_{ij}). In dem Summanden zu j ist kein Faktor in $\mathfrak{q}'_j$. Es folgt

$$N(x) = \prod \sigma(x) \in \mathcal{O}_K \cap \mathfrak{q} = \mathfrak{p} \subset \mathfrak{q}'$$

Also liegt ein $\sigma(x) \in \mathfrak{q}'$ und $x \in \sigma^{-1}\mathfrak{q}'$. Dies ist ein Widerspruch. □

Definition 7.11. *Sei L/K Galoiserweiterung von Zahlkörpern, $\mathfrak{q}$ ein Primideal von $\mathcal{O}_L$, $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{q}$. Die* Zerlegungsgruppe *von $\mathfrak{q}$ ist*

$$D_\mathfrak{q} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

Die natürliche Abbildung $\phi : D_\mathfrak{q} \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ ist ein Gruppenhomomorphismus. Die Trägheitsgruppe *$I_\mathfrak{q}$ ist der Kern von ϕ, d.h.*

$$I_\mathfrak{q} = \{\sigma : L \to L \mid \sigma(\alpha) = \alpha \mod \mathfrak{q} \text{ für alle } \alpha \in \mathcal{O}_L\}$$

Lemma 7.12. *Es gilt $|D_\mathfrak{q}| = ef$, $e = |I_\mathfrak{q}|$. Die Abbildung ϕ ist surjektiv.*

Beweis: Wie vorher sei g die Anzahl der Konjugierten von $\mathfrak{q}$, d.h. $|G|/|D_\mathfrak{q}|$, denn G operiert transitiv mit Standgruppe $D_\mathfrak{q}$. Also

$$g = n/|D_\mathfrak{q}| = gef/|D_\mathfrak{q}|$$

Sei nun $E = L^{D_\mathfrak{q}} \subset L$. Nach dem Hauptsatz der Galoistheorie ist $\mathrm{Gal}(L/E) = D_\mathfrak{q}$. Sei $\mathfrak{p}_E = \mathfrak{q} \cap \mathcal{O}_E$. Nach Definition liegt $\mathfrak{q}$ über $\mathfrak{p}_E$. Das Primideal $\mathfrak{q}$ wird von allen Elementen auf $D_\mathfrak{q}$ festgelassen, also ist die Zerlegungsgruppe von $\mathfrak{q}$ in L/E ganz $D_\mathfrak{q}$. Damit liegt nur ein Primideal von L über $\mathfrak{p}_E$ (nämlich $\mathfrak{q}$). Es folgt

$$ef = |D_\mathfrak{q}| = [L : E] = e(\mathfrak{q}/\mathfrak{p}_E) f(\mathfrak{q}/\mathfrak{p}_E)$$

Verzweigungsgrad und Restklassenindex sind multiplikativ in Körpertürmen, also folgt

$$e = e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p}_E), \qquad f = f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p}_E)$$

Dies bedeutet $\kappa(\mathfrak{p}_E) = \kappa(\mathfrak{p})$.
Nach dem Satz vom primitiven Element ist $\kappa(\mathfrak{q}) = \kappa(\mathfrak{p})(\overline{\alpha})$ für ein $\alpha \in \mathcal{O}_L$. Sei $P \in \mathcal{O}_E[X]$ das normierte Minimalpolynom von α. Es stimmt mit dem charakteristischen Polynom von α überein. Dann ist $\overline{P} \in \kappa(\mathfrak{p}_E)[X]$ eine Potenz des Minimalpolynoms von $\overline{\alpha}$. Sei $\overline{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}_E))$, also $\overline{\sigma}(\overline{\alpha})$ eine Nullstelle von $\overline{P}$. Dann muss es $\sigma \in \mathrm{Gal}(L/E) = D_\mathfrak{q}$ geben mit $\sigma(\alpha) = \overline{\sigma}(\overline{\alpha})$. Dann ist $\overline{\sigma} = \phi(\sigma)$, d.h. ϕ ist surjektiv. Es folgt $f(\mathfrak{q}/\mathfrak{p}_E) = |\mathrm{Im}\phi| = |D_\mathfrak{q}|/|I| = ef/|I|$. □

Korollar 7.13. *Sei L/K Galoisweiterung von Zahlkörpern, $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Dann ist $\mathfrak{p}$ unverzweigt genau dann, wenn $|I_\mathfrak{q}| = 1$ für ein $\mathfrak{q} \mid \mathfrak{p}$. Allgemein ist $L^{I_\mathfrak{q}}/K$ unverzweigt über $\mathfrak{p}$.*

Lemma 7.14. *Sei $\mathfrak{q}, \sigma(\mathfrak{q}) \mid \mathfrak{p}$. Dann gilt $D_{\sigma\mathfrak{q}} = \sigma D_\mathfrak{q} \sigma^{-1}$, $I_{\sigma\mathfrak{q}} = \sigma I_\mathfrak{q} \sigma^{-1}$. Insbesondere sind diese Gruppen isomorph.*

Proof. Die Aussage für D_σ ist die Formel für die Standgruppe von zwei Elementen derselben Bahn. Die Aussage für die Trägheitsgruppe rechnet man leicht nach. □

Bemerkung. Ist die Galoisgruppe abelsch, so gilt $D_\mathfrak{q} = D_{\sigma\mathfrak{q}}$. Wir schreiben dann auch $D_\mathfrak{p}$ und $I_\mathfrak{p}$.

Körpertürme

Seien $L/E/K$ Erweiterungen von Zahlkörpern, $\mathfrak{p}_L|\mathfrak{p}_E|\mathfrak{p}_K$ Primideale von L, E, K. Dann ist nach Definition

$$e(\mathfrak{p}_L/\mathfrak{p}_K) = e(\mathfrak{p}_L/\mathfrak{p}_E)e(\mathfrak{p}_E/\mathfrak{p}_K)$$
$$f(\mathfrak{p}_L/\mathfrak{p}_K) = f(\mathfrak{p}_L/\mathfrak{p}_E)f(\mathfrak{p}_E/\mathfrak{p}_K)$$

Besonders interessant ist der Fall $L = E_1E_2$ für $E_1, E_2/K$ Erweiterungen von Zahlkörpern.

Satz 7.15. *Seien $E, E'/\mathbb{Q}$ Galoiserweiterungen von Zahlkörpern. Die Diskriminanten d, d' seien teilerfremd. Dann ist $\mathcal{O}_E\mathcal{O}_{E'} = \mathcal{O}_{EE'}$. Die Körpererweiterung $EE'/\mathbb{Q}$ verzweigt genau in den Primzahlen, die dd' teilen. Es gilt $d_{EE'} = d^{n'}d'^{n}$.*

Proof. Der Körper $E \cap E'$ ist eine unverzweigte Erweiterung von $\mathbb{Q}$, also nach Theorem 7.5 gleich $\mathbb{Q}$.
Sei $n = [E : \mathbb{Q}]$, $n' = [E' : \mathbb{Q}]$. Dann ist $[EE' : \mathbb{Q}] = nn'$. Es gilt $\mathrm{Gal}(EE'/\mathbb{Q}) = G(E/\mathbb{Q}) \times G(E'/\mathbb{Q})$. Sei $x_1, \ldots, x_n$ eine Basis von $\mathcal{O}_E$ und $x'_1, \ldots, x'_{n'}$ eine Basis von E'. Dann ist $\{x_i x'_j | i = 1, \ldots, n, j = 1, \ldots, n'\}$ eine $\mathbb{Q}$-Basis von EE'. Sei nun $\alpha \in \mathcal{O}_{EE'}$,

$$\alpha = \sum a_{ij} x_i x'_j$$

Behauptung. $a_{ij} \in \mathbb{Z}$.

Sei $G = \mathrm{Gal}(E/K) = \{\sigma_1, \ldots, \sigma_n\}$, $G' = \mathrm{Gal}(E'/K) = \{\sigma'_1, \ldots, \sigma'_{n'}\}$. Dann gilt

$$\mathrm{Gal}(EE'/K) = \{\sigma_k \sigma'_l | k = 1, \ldots, n, l = 1, \ldots, n'\}$$

Wir betrachten die Matrix $T = (\sigma'_l x'_j)$. Es gilt $d' = \det(T)^2$. Sei $a = (\sigma_1 \alpha, \ldots, \sigma_{n'} \alpha)^t$. Dann gilt

$$a = Tb$$

mit $b = (\sum_i a_{i1} x_i, \sum_i a_{i2} x_i, \ldots, \sum_i a_{in} x_i)^t$. Sei $T^* = \det(T) T^{-1}$. Nach der Cramerschen Regel hat sie Einträge in $\mathcal{O}_{E'}$. Daher hat

$$T^* a = \det(T) b$$

Einträge in $\mathcal{O}_{EE'}$. Hieraus folgt, dass $\sum_i d' a_{ij} x_i$ ganz für alle j. Da $x_1, \ldots, x_n$ eine Basis von $\mathcal{O}_E$ ist, folgt $d' a_{ij} \in \mathbb{Z}$ für alle i, j.
Dieselbe Überlegung mit vertauschten Rollen von E und E' impliziert $d a_{ij} \in \mathbb{Z}$ für alle i, j. Da d, d' teilerfremd sind, ist $a_{ij} \in \mathbb{Z}$.
Ist p verzweigt in E oder E', dann offensichtlich auch in $EE'/\mathbb{Q}$. In der expliziten Basis, die wir gefunden haben, können wir auch die Diskriminate von $E_1 E_2/\mathbb{Q}$ leicht berechnen. □

Beispiel. (i) Sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{5})$. Der erste Körper hat Diskriminante 8, der zweite hat Diskriminante 5. Es folgt nach dem Satz $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]\mathcal{O}_{\sqrt{5}}$ mit der Basis $1, \sqrt{2}, (1+\sqrt{5})/2, \sqrt{2}(1+\sqrt{5})/2$.

(ii) Sei $K = \mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3})\mathbb{Q}(\sqrt{7})$. Der erste Körper hat Diskriminante 12, der zweite hat Diskriminante 28. Der Satz lässt sich nicht anwenden.

Kapitel 8

Zyklotomische Körper

Erinnerung

$\zeta \in \overline{\mathbb{Q}}$ heißt n-te Einheitswurzel, wenn $\zeta^n = 1$. Es heißt *primitive* n-te Einheitswurzel, wenn $\zeta^m \neq 1$ für $m < n$. Die Gruppe der n-ten Einheitswurzeln ist eine endliche zyklische Gruppe der Ordnung n. Die primitiven n-ten Einheitswurzeln sind gerade ihre Erzeuger. Es gibt also $\phi(n)$ viele primitive n-te Einheitswurzeln (Eulersche ϕ-Funktion).
Sei $\zeta_n \in \overline{\mathbb{Q}}$ primitive n-te Einheitswurzel. Dann hat das Minimalpolynom $\Phi(n)$ von ζ_n den Grad $\phi(n)$. Die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist galois mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^*$. Wir erhalten den Isomorphismus wie folgt: Sei $a \in \mathbb{Z}$ teilerfremd zu n. Dann definiert

$$\sigma_a : \zeta_n \mapsto \zeta_n^a$$

ein Element von $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Es hängt nur von der Restklasse $a \in \mathbb{Z}/n\mathbb{Z}$ ab, von dieser aber dann wirklich. Es gibt $\phi(n)$ solche Restklassen, daher hat die Galoisgruppe mindestens $\phi(n)$ Elemente. Dann ist die Erweiterung galois und unsere Zuordnung surjektiv. Man beachte, dass σ_a unabhängig von der Wahl von ζ_n ist! Die zyklotomischen Körper sind also Beispiele von *abelschen Erweiterungen*, Galoiserweiterungen mit abelscher Galoisgruppe.

Der Ganzheitsring

Sei ζ_n eine primitive n-te Einheitswurzel. Einheitswurzeln sind ganz, also gilt $\mathbb{Z}[\zeta_n] \subset \mathcal{O}_{\mathbb{Q}(\zeta_n)}$. Wir wollen Gleichheit zeigen und beginnnen langsam.

Satz 8.1. *Sei $n = l$ Primzahl. Dann ist*

$$\mathbb{Z}[\zeta_l] = \mathcal{O}_{\mathbb{Q}(\zeta_l)}$$

Proof. Sei $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\zeta_l)}$, $\zeta = \zeta_l$ Sei $x = a_0 + \cdots + a_{l-2}\zeta^{l-2} \in \mathcal{O}$ mit $a_i \in \mathbb{Q}$. Wegen $x(1-\zeta) \in \mathcal{O}$ folgt $\mathrm{Tr}(x(1-\zeta)) = a_0 p \in \mathbb{Z}$. Andererseits gilt

$$\mathrm{Tr}(x(1-\zeta)) = \sum_\sigma \sigma(x)(1-\sigma(\zeta))$$

mit $\sigma(\zeta) = \zeta^j$, also $1-\sigma(\zeta) = (1-\zeta)(1+\zeta+\cdots+\zeta^{j-1}$. Damit gilt $\mathrm{Tr}(x(1-\zeta)) \in \mathcal{O}(1-\zeta) \cap \mathbb{Z}$.

Behauptung. $\mathcal{O}(1-\zeta) \cap \mathbb{Z} = l\mathbb{Z}$

Mit $x = 1$ und $\mathrm{Tr}(1-\zeta) = l$ gilt $\supset$. Wäre Gleichheit falsch, so müsste $1 \in \mathcal{O}(1-\zeta)$ liegen, also $1-\zeta$ eine Einheit sein. Die Norm von $1-\zeta$ ist aber

$$N(1-\zeta) = \prod_{j=1}^{l-1}(1-\zeta^j) = \prod(X-\zeta^j)(1) = (1+X+\cdots+X^{l-1})(1) = l$$

also ist dies nicht der Fall.
Somit gilt $la_0 \in p\mathbb{Z}$, d.h. $a_0 \in \mathbb{Z}$. Dann ist auch $a_1\zeta + \ldots a_{p-2}\zeta^{p-2} = \zeta(a_1 + \ldots a_{p-2}\zeta^{p-3} \in \mathcal{O}$. ζ ist eine Einheit. Wir wiederholen nun das Argument und erhalten $a_1 \in \mathbb{Z}$ und iterativ $a_i \in \mathbb{Z}$ für alle i. Damit ist die Berechnung von $\mathcal{O}$ abgeschlossen. □

Lemma 8.2. *Sei $n = l^\nu$ eine Primzahlpotenz, $\lambda = (1-\zeta_n)$, $d = \phi(l^\nu)$. Dann ist (λ) ein Primideal mit Restklassengrad* 1. *gilt*

$$(l) = (\lambda)^d \subset \mathcal{O}_{\mathbb{Q}(\zeta_{l^\nu})}$$

l ist rein verzweigt. Es gilt

$$D(1, \zeta_n, \ldots, \zeta_n^{d-1}) = \pm l^s \text{ mit } s = l^{\nu-1}(\nu l - \nu - 1)$$

Proof. Sei $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\zeta_n)}$, $\zeta = \zeta_n$. Es gilt

$$\Phi_{l^\nu}(X) = \frac{X^{l^\nu}-1}{X^{l^{\nu-1}}-1} = X^{(l-1)l^{\nu-1}} + \cdots + X^{l^{\nu-1}} + 1$$

Einsetzen von 1 ergibt

$$l = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*}(1-\zeta^a)$$

Es ist

$$1-\zeta^a = (1+\zeta+\cdots+\zeta^{a-1})(1-\zeta)$$

Der Vorfaktor ist also ganz. Wegen $N(1-\zeta^a) = N(1-\zeta)$ hat er Norm 1, ist also eine Einheit in $\mathcal{O}$. Dies bedeutet $(1-\zeta) = (1-\zeta^a)$ als Ideale. Damit haben wir die Idealidentität gezeigt. Wegen $N(l) = l^d$ folgt $N(\lambda) = l$. Damit ist dies ein Primideal. Wegen $d = efg$ mit $g = 1, e = d$ ist $f = 1$.
Seien $\zeta_1, \ldots, \zeta_d$ die Konjugierten von ζ. Dann gilt

$$D(1, \zeta, \ldots, \zeta^{d-1}) = \pm \begin{vmatrix} 1 & \zeta_1 & \ldots & \zeta_1^{d-1} \\ 1 & \zeta_2 & \ldots & \zeta_2^{d-1} \\ & & \ldots & \\ 1 & \zeta_d & \ldots & \zeta_d^{d-1} \end{vmatrix}^2$$

$$= \prod_{i<j}(\zeta_i - \zeta_j)^2$$

Das von diesem Ausdruck in $\mathcal{O}$ erzeugte Ideal ist nach dem Obigen eine Potenz von (λ). Da es gleichzeitig eine ganze Zahl ist, erhalten wir (bis auf Vorzeichen) eine Potenz von l. Den Exponenten lesen wir ab. □

Satz 8.3. *Sei $n = l^\nu$ eine Primzahlpotenz. Dann ist $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. In $\mathbb{Q}(\zeta_n)$ ist l rein verzweigt, alle anderen Primideale sind unverzweigt.*

Proof. Sei $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\zeta_n)}$, $\zeta = \zeta_n$. Wir wissen $\mathbb{Z}[\zeta] \subset \mathcal{O}$. Sei l^s die Diskriminante. Nach Lemma 8.2 gilt $\mathbb{Z}/l\mathbb{Z} \cong \mathcal{O}/(\lambda)$ (Restklassengrad 1), also

$$\mathcal{O} = \mathbb{Z} + \lambda\mathcal{O} \Rightarrow \mathcal{O} = \mathbb{Z}[\zeta] + \lambda\mathcal{O}$$

Wir multiplizieren mit λ und setzen das Ergebnis ein. Es gilt also

$$\mathcal{O} = \mathbb{Z}[\lambda] + \lambda^2\mathcal{O} \Rightarrow \ldots \mathcal{O} = \mathbb{Z}[\lambda] + \lambda^s\mathcal{O}$$

Behauptung. $l^s\mathcal{O} \subset \mathbb{Z}[\zeta]$

Allgemeiner gilt $\Delta\mathcal{O} \subset< x_1, \ldots, x_d >$, wenn $x_1, \ldots, x_d \in \mathcal{O}$ mit $D(x_1, \ldots, x_d) = \Delta$. Sei $y_1, \ldots, y_d$ die duale Basis von $x_1, \ldots, x_d$ bezüglich der Spurpaarung. Wir wissen, dass

$$\mathcal{O} \subset< y_1, \ldots, y_d >_{\mathbb{Z}}$$

Es genügt also zu zeigen, dass $\Delta y_i \in< x_1, \ldots, x_d >_{\mathbb{Z}}$. Wir schreiben die y_i mit Hilfe der Cramerschern Regel in Termen der x_j hin. Als Nenner taucht nur Δ auf. □

Satz 8.4. *Sei $n \in \mathbb{N}$. Dann ist $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ verzweigt genau in den Primteilern von n.*

Proof. Dies ist eine Anwendung von Satz 7.15. □

Beispiel. Wir betrachten wieder den Fall $n = l$ ungerade Primzahl. Dann ist $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \cong \mathbb{F}_l^*$ zyklisch der Ordnung $l - 1$. Sei H die Untergruppe der Ordnung $(l-1)/2$. Wir betrachten $E = \mathbb{Q}(zeta_l)^H$. Dies ist eine quadratische Erweiterung von $\mathbb{Q}$. Welche? In $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ ist nur die Primzahl l verzweigt, also ist auch in $E/\mathbb{Q}$ höchstens l verzweigt. Es folgt

$$E = \begin{cases} \mathbb{Q}(\sqrt{l} & l = 1 \mod 4 \\ \mathbb{Q}(\sqrt{-l} & l = -1 \mod 4 \end{cases}$$

Satz 8.5. *Sei $d \in \mathbb{Z}$ quadratfrei. Dann gibt es N mit $\mathbb{Q}(\sqrt{d} =\subset \mathbb{Q}(zeta_N)$.*

Das minimale N mit dieser Eigenschaft heißt *Führer* von $\mathbb{Q}(\sqrt{d})$.

Proof. Beachte, dass $i = \zeta_4$. Wir beginnen mit $d = p$ Primzahl. Ist $p = 1 \mod 4$, so gilt nach dem Beispiel $\mathbb{Q}(\sqrt{p} \subset \mathbb{Q}(\zeta_p)$. Für $p = 3 \mod 4$ gilt nach dem Beispiel

$$\mathbb{Q}(\sqrt{p}) \subset\subset \mathbb{Q}(i, \sqrt{-p}) \subset \mathbb{Q}(i, \zeta_p) = \mathbb{Q}(\zeta_{4p}) \ .$$

Für $p = 2$ beachten wir $\zeta_8 = \sqrt{i} = \sqrt{2}^{-1} + i\sqrt{2}^{-1}$, also $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$.
Ist $d \in \mathbb{Z}$ quadratfrei, so gilt $d = \pm p_1 \dots p_n$ für verschiedene Primzahlen. Wir setzen die Fälle von vorher zusammen. Demnach gilt

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\zeta_8, \zeta_{p_1}, \dots, \zeta_{p_n}) \subset \mathbb{Q}(\zeta_{8d})$$

□

Tatsächlich gilt viel allgemeiner:

Theorem 8.6 (Kronecker-Weber)**.** *Sei $K/\mathbb{Q}$ endlich abelsche Erweiterung. Dann gibt es N mit $K \subset \mathbb{Q}(\zeta_N)$.*

Dies ist ein Spezialfall von Klassenkörpertheorie. Wir wollen versuchen, das Theorem bis Ende des Semesters zur beweisen. Offensichtlich ist ein Hauptproblem, den richtigen Kandidaten für N zu finden. Er wird vom Verzweigungsverhalten von K diktiert.

Zyclotomische Einheiten

Sei in diesem Abschnitt $n \in \mathbb{N}, n \neq 2 \mod 4$. Wir betrachten Einheiten von $\mathbb{Q}(\zeta_n)$. (Die Einschränkung wird wegen des Sonderfalls $\zeta_2 \in \mathbb{Q}$ nötig.)

Definition 8.7. *Sei V_n die multiplikative Untergruppe von $\mathbb{Q}(zeta_n)^*$ erzeugt von $\pm\zeta_n$ und $1 - \zeta_n^a$ für $a = 1, \dots, a-1$. Sei*

$$C_n = V_n \cap \mathbb{Z}[\zeta_n]^*$$

die Gruppe der zyklotomischen Einheiten.

Beispiel. (i) Ist $n = l^\nu$ Primzahlpotenz, so haben wir gezeigt, dass $(1 - \zeta_n)/(1 - \zeta_n^a)$ für $a \in (\mathbb{Z}/n\mathbb{Z})^*$ eine zyklotomische Einheit ist.

(ii) Ist $n = pq$ Produkt von zwei Primzahlen, so gilt $N(1 - \zeta_n)) = \Phi_n(1)$ und

$$\begin{aligned}
\Phi_n(X) &= \frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)} = \frac{X^{pq+1} - X^{pq} - X + 1}{X^{p+q} - X^p - X^q + 1} \\
\Phi_n(1) &= \frac{(pq+1)X^{pq} - pqX^{pq-1} - 1}{(p+q)X^{p+q-1} - pX^{p-1} - qX^{q-1}}(1) \\
&= \frac{(pq+1)pqX^{pq-1} - pq(pq-1)X^{pq-2}}{(p+q)(p+q-1)X^{p+q-2} - p(p-1)X^{p-2} - q(q-1)X^{q-2}}(1) \\
&= \frac{(pq+1)pq - pq(pq-1)}{(p+q)(p+q-1) - p(p-1) - q(q-1)} \\
&= \frac{2pq}{p^2 + q^2 + 2pq - p - q + 1 - p^2 + p - q^2 + q} = 1
\end{aligned}$$

Also ist dies eine zyklotomische Einheit.

Man zeigt allgemein, dass die zyklotomischen Einheiten eine Untergruppe von vollem Rang in $\mathbb{Z}[\zeta_n]^*$ bilden. Der Index ist im wesentlichen die Klassenzahl.
Iwasawa-Theorie beschäftigt sich mit dem System der Klassengruppe und dem System der zyklotomischen Einheiten für den ganzen Turm $\mathbb{Q}(\zeta_{np^\nu})$ für $\nu = 1, 2, \ldots$. Die Situation hat eine überraschend einfache Asymptotik.
Literatur: L. Washington, Introduction to Cyclotomic Fields, Graduate Text in Mathematics 83, Springer Verlag.
S. Lang, Cyclotomotic Fields I, II, Graduate Text in Mathematics, Springer Verlag.
Neukirch, Schmidt, Wingberg, Cohomology of Number Fields, Grundlehren der Mathemtik, Springer Verlag.

Kapitel 9

Bewertungstheorie und lokale Körper

Definition 9.1. *Sei k ein Körper. Ein* Absolutbetrag *v ist ein Abbildung*

$$k \to \mathbb{R} \qquad\qquad x \mapsto |x|_v$$

so dass

(i) $|x|_v \geq 0$ *und* $|x|_v = 0 \Leftrightarrow x = 0$.

(ii) Für alle $x, y \in k$ *gilt* $|xy|_v = |x|_v |y|_v$.

(iii) $|x + y|_v \leq |x|_v + |y|_v$.

Ein Absolutbetrag definiert eine Topologie via: $U \subset k$ heißt offen, falls für alle $x \in U$ ein $\varepsilon > 0$ existiert, so dass $\{y \in k \mid |y - x|_v < \varepsilon\} \subset U$.

Beispiel.

- $\mathbb{R}, \mathbb{C}$ mit dem gewöhnlichen Absolutbetrag, ebenso $\mathbb{Q}$.
- Für $p \in \mathbb{Q}$ eine Primzahl $|x|_p = p^{-v(x)}$, wobei $v(x)$ die Vielfachheit von p in x ist. Dies ist der *p-adische Betrag.*

Definition 9.2. *Sei k ein Körper. Eine* diskrete Bewertung *ist eine Abbildung* $v : k \to \mathbb{R} \cup \{\infty\}$ *mit*

(i) $v(x) = \infty \Leftrightarrow x = 0$.

(ii) $v(xy) = v(x) + v(y)$.

(iii) $v(x + y) \geq \min(v(x), v(y))$

und $v(k^*)$ diskrete Untergruppe von $\mathbb{R}$ vom Rang 1.

Wir können jede diskrete Bewertung ohne Einschränkung so normieren, dass $v(k^*) = \mathbb{Z}$.

Lemma 9.3. *Sei v eine diskrete Bewertung, $a > 1$ fest. Dann ist $|x|_v = a^{v(x)}$ ein Absolutbetrag.*

Beweis: Die Eigenschafte (i) und (ii) sind klar.
Dreiecksungleichung:

$$a^{-v(x+y)} \leq a^{\min(v(x),v(y))} \leq a^{-v(x)} + a^{-v(y)}$$

□

Beispiel. Sei $\mathcal{O}$ ein Dedekindring, $\mathfrak{p}$ ein Primideal, K der Quotientenkörper von $\mathcal{O}$. Für $x \in K^*$ sei $(x) = \prod \mathfrak{q}^{v_\mathfrak{q}(x)}$ die Produktzerlegung in Primideale. Dann ist die Abbildung $v : K^* \to \mathbb{Z}$ mit $x \mapsto v_\mathfrak{p}(x)$ eine diskrete Bewertung.

Allgemein:

Definition 9.4. *Ein Dedekindring mit genau einem maximalen Ideal heißt* diskreter Bewertungsring.

Satz 9.5. *Sei A ein Ring. Äquivalent sind:*

(i) A ist ein diskreter Bewertungsring.

(ii) A ist Hauptidealring mit genau einem maximalen Ideal.

(iii) A ist von der Form $\{x \in k | v(x) \geq 0\}$ für eine diskrete Bewertung eines Körpers k.

Es gilt dann $k = Q(A)$ und das maximale Ideal ist $\mathfrak{m} = \{x \in x | v(x) > 0\}$.

Beweis: Die Äquivalenz der ersten beiden Aussagen folgt wie wir bereits gesehen haben aus der Strukturtheorie von Dedekindringen. Wie im Beispiel wird die Bewertung auf $k = Q(A)$ definiert. Sie hat Wertebereich $\mathbb{Z} \cup \infty$. Sei nun umgekehrt $v : k \to \mathbb{Z} \cup \infty$ eine diskrete Bewertung, A und $\mathfrak{m}$ wie in (iii).

Behauptung. *A ist ein Ring mit maximalem Ideal $\mathfrak{m}$ und Quotientenkörper k.*

Sei $a, b \in A$. Dann ist $v(a + b) \geq \min(v(a), v(b)) \geq 0$, also $a + b \in A$. Ebenso $v(ab) = v(a)v(b) \geq 0$. Ebenso folgt, dass $\mathfrak{m}$ ein Ideal ist. Alle Elemente $u \in A \setminus \mathfrak{m}$ haben $v(u) = 0$, also $v(u^{-1}) = 0$ und daher $u^{-1} \in A$. Sie sind invertierbar. Jedes echte Ideal muss daher in $\mathfrak{m}$ enthalten sein, es ist maximal. Ist $x \in k$ mit $v(x) < 0$, so gilt $v(x^{-1}) > 0$, also $x^{-1} \in A$. Insbesondere ist k der Quotientenkörper von A.
Der Wertebereich von v ist diskret. Sei $\pi \in \mathfrak{m}$ mit $v(\pi)$ minimal. Ohne Einschränkung ist $v(\pi) = 1$, d.h. $v(k^*) = \mathbb{Z}$.

Behauptung. *Jedes Element von k^* hat die Form $u\pi^v$ mit $u \in A^*$, $v \in \mathbb{Z}$.*

Sei $x \in k^*$, $v = v(x)$, $u = x\pi^{-v}$. Dann gilt $v(u) = v(x) - v = 0$, also $u \in A^*$. □

Definition 9.6. *Sei* $\operatorname{Char} k = 0$. *Ein Betrag heißt* kanonisch, *wenn seine Einschränkung auf $\mathbb{Q}$ mit $|\cdot|$ oder einem $|\cdot|_p$ übereinstimmt.*

Wir interessieren uns nur für die kanonischen Beträge.

Definition 9.7. *Zwei Absolutbeträge heißen* äquivalent*, wenn sie dieselbe Topologie induzieren. Eine Äquivalenzklasse von Absolutbeträgen auf einem Körper heißt* Stelle *des Körpers.*

Lemma 9.8. *Seine $|\cdot|_1$ und $|\cdot|_2$ äquivalente Absolutbeträge. Dann gibt es $\lambda > 0$, so dass $|x|_1 = |x|_2^\lambda$.*

Beweis: Wir betrachten

$$\{x \in k \mid |x|_1 < 1\} = \{x \mid \lim_{n\to\infty} x^n = 0\}$$

Dies ist die gleiche Menge wie für $|\cdot|_2$, da Grenzwerte nur von der Topologie abhängen. Also:

$$|x|_1 > 1 \Leftrightarrow |x|_2 > 1$$

Wenn $|x|_1 = 1$ für alle $x \neq 0$, dann ist die Topologie diskret. Die Aussage gilt dann trivialerweise.
Sei also $y \in k$ mit $a = |y|_1 > 1$. Sei $b = |y|_2$. Für $x \in k^*$ gibt es $\alpha \geq 0$ mit $|x|_1 = a^\alpha$. Seien $m, n \in \mathbb{N}$ mit $m/n \geq \alpha$. Dann folgt

$$|x|_1 < |y|_1^{m/n} \Rightarrow \left|\frac{x^n}{y^m}\right|_1 < 1 \Rightarrow \left|\frac{x^n}{y^m}\right|_2 < 1 \Rightarrow |x|_2 < b^{m/n}$$

Ebenso argumentiert man für $m/n < \alpha \Rightarrow |x|_2 > b^{m/n}$. Da die Ungleichungen für alle m, n gelten, erhalten wir $|x|_2 = b^\alpha$. Mit anderen Worten

$$|x|_1 = a^\alpha = b^{\alpha \log_b a} = |x|_2^{\log_b a}$$

Dies beweist die Behauptung mit $\lambda = \log_b a$. □

Ein Körper heißt *vollständig*, wenn jede Cauchy-Folge konvergiert. Ist k ein Körper mit Absolutbetrag v, dann ist k_v (der Körper der Cauchy-Folgen in k modulo Nullfolgen) ein vollständiger Körper bezüglich der Fortsetzung von v. Dieser Körper k_v heißt *Komplettierung* von k. (Beweise wie in Analysis).

Beispiel. $\mathbb{R}$ ist die Komplettierung von $\mathbb{Q}$ bezüglich $|\cdot|$. Sei $\mathbb{Q}_p$ die Komplettierung von $\mathbb{Q}$ bezüglich $|\cdot|_p$. Dies ist der Körper der p-adischen Zahlen.

Definition 9.9. *Sei* $\operatorname{Char} k = 0$*. k heißt* lokaler Körper*, wenn er Komplettierung eines Zahlkörpers bezüglich eines kanonischen Betrages ist.*

Diese Körper wollen wir klassifizieren. Es gilt übrigens eine glattere Charakterisierung:

Theorem 9.10. *Sei* $\operatorname{Char} k = 0$*. Dann ist k lokal genau dann, wenn k vollständig, lokalkompakt und nicht-diskret.*

Beweis: vergl. Weil, Basic number theory §3. □

Zur Erinnerung: ein metrischer Raum ist lokalkompakt, wenn jede beschränkte Folge eine konvergente Teilfolge hat.

Satz 9.11. *Sei K ein Zahlkörper, $\mathfrak{p}$ ein Primideal, $|\cdot|_v$ der Absolutbetrag zur $\mathfrak{p}$-adischen Bewertung $v_\mathfrak{p} : K^* \to \mathbb{Z}$. Sei K_v die Komplettierung von $K_\mathfrak{p}$ bezüglich v.*

(i) $v_\mathfrak{p}$ ist eine diskrete Bewertung auf K_v.

(ii) Der topologische Abschluss $\mathcal{O}_v$ von $\mathcal{O}_K$ in K_v ist $\{x \in K_v \mid |x| \leq 1\}$, ein diskreter Bewertungsring mit Restklassenkörper $\mathcal{O}_K/\mathfrak{p}$.

(iii) $\mathcal{O}_v$ ist kompakt, K_v ist lokalkompakt.

Beweis: Sei $x \in K_v$, $x = \lim x_i$ mit $x_i \in K$. D.h. für alle $\varepsilon > 0$ gibt es N, so dass $|x_i - x_j| < \varepsilon$ für alle $i, j > N$. Also

$$|x_i| = |x_i - x_j + x_j| \leq \max(|x_i - x_j|, |x_j|) \leq \max(\varepsilon, |x_j|)$$

1. Fall: $x = 0$. Dann bilden die x_j eine Nullfolge.
2. Fall: $x \neq 0$, die x_i bilden keine Nullfolge. Dann gibt es $\varepsilon_0 > 0$, so dass es für jedes N ein $i > N$ gibt mit $|x_i| > \varepsilon_0$. Für alle $\varepsilon < \varepsilon_0$ folgt dann $|x_i| \leq |x_j|$. Also wird $|x_i|$ konstant.
$|x| = |x_i|$ für großes i hat denselben Wertebereich wie der Betrag auf K, insbesondere ist er diskret. Ebenso ist $v(x) = \lim v(x_i)$ konstant, die Bewertung auf K_v ist diskret.
Sei

$$\mathcal{O}_v = \{x \in K_v \mid |x| \leq 1\} = \{x \in K_v \mid v(x) \geq 0\}$$

Sei $\mathcal{O}_\mathfrak{p} = \{a/s \in K \mid a \in \mathcal{O}, s \in \mathcal{O} \setminus \mathfrak{p}\}$ die Lokalisierung des Ganzheitsrings in $\mathfrak{p}$.

Behauptung. *$\mathcal{O}_v$ ist der topologische Abschluss von $\mathcal{O}_\mathfrak{p}$.*

$\mathcal{O}_\mathfrak{p}$ ist ein lokaler Hauptidealring (vergleiche Satz 7.3). Das einzige Primideal wird erzeugt von $\pi \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Nach Definition ist $v(\pi) = 1$. Jedes Element von K^* ist von der Form $u\pi^r$ mit $u \in \mathcal{O}_\mathfrak{p}^*$ und $r \in \mathbb{Z}$. Es gilt $\mathcal{O}_\mathfrak{p} \subset \mathcal{O}_v$, denn $v(a/s) = v(a) - v(s) = v(a) \geq 0$. Sei $x \in \mathcal{O}_v$, also $x = \lim x_i$, $x_i \in K$, $v(x) \geq 0$. Hieraus folgt, wie wir gesehen haben $v(x_i) > 0$ für i groß genug.
Offensichtlich ist $K \cap \mathcal{O}_v = \mathcal{O}_\mathfrak{p}$. Sei $x \in K_v^*$, $r = v(x) \in \mathbb{Z}$. Dann ist $x = u\pi^r$ mit $v(u) = 0$, also $u \in \mathcal{O}_v^*$. Demnach ist auch $\mathcal{O}_v$ ein Hauptidealring, einziges Primideal (π).

Behauptung. *$\mathcal{O}_K$ ist dicht in $\mathcal{O}_\mathfrak{p}$.*

Sei $x = a/s$ mit $s \in \mathcal{O}_K \setminus \mathfrak{p} = \mathcal{O}_K \cap \mathcal{O}_v^*$. Sei $N \geq 0$. π^N und s sind teilerfremd, d.h. $(\pi^N, s) = 1$. Es gibt $b, c \in \mathcal{O}_K$ mit

$$b\pi^N + sc = 1 \Rightarrow sc - ss^{-1} = -b\pi^N \Rightarrow |c - s^{-1}| = |s(c - s^{-1})|_v \leq |\pi|_v^{-N}$$

Damit wird s^{-1} (und dann auch as^{-1}) durch ein Element von $\mathcal{O}_K$ approximiert.

Beachte (Satz 7.3)

$$\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \to \mathcal{O}_v/(\pi)$$

Die Abbildung ist injektiv, da es ein Körperhomomorphismus ist.

Behauptung. *Die Abbildung ist surjektiv.*

Sei $x = \lim x_i$ mit $x_i \in \mathcal{O}_\mathfrak{p}$. Es gilt $v(x - x_i) \to \infty$, insbesondere $v(x - x_i) \geq 1$ für i groß genug, d.h. $\pi \mid x - x_i$. Hieraus folgt $x = x_i$ modulo π, also liegt x modulo π im Bild von $\mathcal{O}_\mathfrak{p}$.
Dies beendet den Beweis von (ii).
Sei x_i eine Folge in $\mathcal{O}_v$. Seien $\overline{x}_i$ die Bilder in $\mathcal{O}_v/(\pi)$. Dies ist ein endlicher Körper. Nach dem Schubfachprinzip enthält eine Restklasse unendlich viele Elemente, d.h. eine Teilfolge ist konstant modulo π. Iteration dieses Argumentes liefert Teilfolgen, die konstant sind modulo π^2, dann modulo π^3. Die Diagonalfolge wird für i groß genug konstant modulo π^n, d.h. $v(x_i - x_j) \geq n$ für i, j groß genug. Die x_i bilden eine Cauchy-Folge. Der Grenzwert existiert dann in $\mathcal{O}_v$.
Abgeschlossene Kugeln in K_v sind von der Form $x + \pi^r \mathcal{O}_v$, also kompakt. □

Satz 9.12. *Sei k ein vollständiger, lokalkompakter Körper mit Absolutbetrag, E/k endlich. Dann setzt sich der Betrag von k auf höchstens eine Weise nach E fort. E ist bezüglich dieses Betrages vollständig und lokalkompakt.*

Beweis: Seien $|\cdot|_1$ und $|\cdot|_2$ zwei Fortsetzungen nach E. Wie in der reellen Analysis zeigt man, dass E vollständig und lokalkompakt ist. Ebenso zeigt man (nur Lokalkompaktheit geht ein), dass sie äquivalent sind, d.h. dieselbe Topologie induzieren. Nach Lemma 9.8 gilt dann $|\cdot|_1 = |\cdot|_2^\lambda$. Setzt man $x \in k$ ein, so folgt $\lambda = 1$. □

Bemerkung. Insbesondere gilt für alle $\sigma \in \mathrm{Gal}(E/k)$ die Gleichung $|\sigma(x)| = |x|$, da $|\sigma \cdot|$ ein neuer Betrag ist.

Satz 9.13. *Sei K ein Zahlkörper, k der Abschluss von K bezüglich eines Betrages, der $|\cdot|_p$ fortsetzt. Dann ist k eine endliche Erweiterung von $\mathbb{Q}_p$.*

Beweis: Wir betrachten das Kompositum $K\mathbb{Q}_p$, den Teilkörper von K_v, der von K und $\mathbb{Q}_p$ erzeugt wird. Er ist endlich über $\mathbb{Q}_p$. Da $\mathbb{Q}_p$ lokalkompakt ist, ist es nun auch $K\mathbb{Q}_p$ (Satz 9.12) lokalkompakt und vollständig. Damit ist $K\mathbb{Q}_p = K_v$, also ist dieser Körper endlich. □

Lemma 9.14. *Sei $k/\mathbb{Q}_p$ endlich, $\mathcal{O}_p$ der ganze Abschluss von $\mathbb{Z}_p$ in k.*

(i) $\mathcal{O}_p$ ist diskreter Bewertungsring mit maximalem Ideal $\mathfrak{p}$.

(ii) Der p-adische Betrag auf $\mathbb{Q}_p$ setzt sich nach k fort und gehört zu $\mathfrak{p}$.

Beweis: Wir betrachten den ganzen Abschluss $\mathcal{O}_p$. Der Ring ist ganz abgeschlossen. Mit denselben Argumenten wie im Beweis von Theorem 2.1 (der Fall des Ganzheitsrings) zeigt man, dass $\mathcal{O}_p$ endlich erzeugt über $\mathbb{Z}_p$ ist, insbesondere also noethersch. Wie im Beweis von Satz 4.10 ist $\mathcal{O}_p$ nun ein Dedekindring.

Wähle $\mathfrak{p} \subset \mathcal{O}_p$ ein Primideal ungleich 0. Dann ist $p \in \mathfrak{p}$. Der Betrag $|\cdot|_\mathfrak{p}$ setzt - bei geeigneter Normierung - den Betrag $|\cdot|_p$ fort. Nach Satz 9.12 ist diese Fortsetzung eindeutig. Wegen

$$\mathfrak{p} = \{x \in \mathcal{O}_p \mid |x|_\mathfrak{p} < 0\}$$

legt dies auch das Primideal eindeutig fest. Damit ist $\mathcal{O}_p$ ein diskreter Bewertungsring. □

Bemerkung. Insbesondere ist $\mathcal{O}_p$ ein Hauptidealring. $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ ist ein Erzeuger.

Theorem 9.15. *Sei $k/\mathbb{Q}_p$ endlich. Dann gibt es einen Zahlkörper $K/\mathbb{Q}$ mit $[K : \mathbb{Q}] = [k : \mathbb{Q}_p]$ und $K \subset k$ ist dicht, d.h. k ist Abschluss von K bezüglich eines Betrages, der $|\cdot|_p$ fortsetzt.*

Beweis: Nach Lemma 9.14 gibt es einen Betrag auf k, der $|\cdot|_p$ fortsetzt. Er ist eindeutig nach Satz 9.12. Wir schreiben $|\cdot|_p$ auch für die Fortsetzung.
Sei $k = \mathbb{Q}_p(\alpha)$ (Satz vom primitiven Element), $f = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Q}_p[X]$ das Minimalpolynom. Wähle $g = X^d + b_1X^{d-1} + \cdots + b_d \in \mathbb{Q}[T]$ mit $|a_i - b_i|_p < \varepsilon$. Es gilt

$$f = \prod(X - \alpha_i) \qquad \alpha_i \in \overline{\mathbb{Q}}_p$$
$$g = \prod(X - \beta_i) \qquad \beta_i \in \overline{\mathbb{Q}}$$

Die Differenz

$$|f(\alpha) - g(\alpha)|_p = |0 - \prod(\alpha - \beta_i)|_p = \prod|\alpha - \beta_i|$$

ist klein nach Wahl der b_i, also ist ein Faktor klein. Also wird jede Wurzel von f durch eine Wurzel von g approximiert. Weiterhin sind alle Wurzeln von f verschieden, da das Polynom separabel ist. Für genügend kleines ε sind dann auch alle Wurzeln von g verschieden, d.h. g ist irreduzibel. Sei β die Nullstelle von g, die α approximiert. Wir setzen $K = \mathbb{Q}(\beta)$.

Behauptung. $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$ *für ε klein genug.*

Beide Körper sind in k', der normalen Hülle von $\mathbb{Q}_p(\alpha, \beta)$ enthalten. $k'/\mathbb{Q}_p$ ist galois.
Wir überprüfen $\alpha \in \mathbb{Q}_p(\beta) = (k')^{\mathrm{Gal}(k'/\mathbb{Q}_p(\beta)}$ (Hauptsatz der Galoistheorie). Da $|\beta - \alpha|_p$ klein ist, gilt

$$|\beta - \alpha|_p < |\sigma(\alpha) - \alpha|_p \qquad \sigma \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta)) \text{ falls } \sigma(\alpha) \neq \alpha$$

Sei $\tau \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta))$. Dann folgt $|\tau(\gamma)|_p = |\gamma|_p$ für alle $\gamma \in k'$ nach der Bemerkung nach Satz 9.12. Es folgt

$$|\beta - \tau\alpha|_p = |\tau\beta - \tau(\alpha)|_p < |\sigma\alpha - \alpha|_p$$

Hieraus folgt

$$|\tau\alpha - \alpha| = |\tau\alpha - \beta + \beta - \alpha|_p < |\sigma(\alpha) - \alpha)|_p$$

für alle $\sigma \in \mathrm{Gal}(k'/\mathbb{Q}_p(\beta))$ mit $\sigma(\alpha) \neq \alpha$. Für $\sigma = \tau$ ist dies ein Widerspruch, also $\sigma(\alpha) = \alpha$ für alle σ. Damit haben wir $\mathbb{Q}_p(\alpha) \subset \mathbb{Q}_p(\beta)$ gezeigt. Die andere Inklusion wird genauso gezeigt.
Auf K erhalten wird durch Einschränken des Betrages auf k eine Absolutbetrag, der $|\cdot|_p$ fortsetzt. Da $d = [K : \mathbb{Q}] = [k : \mathbb{Q}_p]$ stimmt k mit der Komplettierung von K überein. □

Korollar 9.16. *k ist lokal, d.h. Komplettierung eines kanonischen Betrages auf einem Zahlkörper, genau dann, wenn $k = \mathbb{R}, \mathbb{C}$ oder endliche Erweiterung eine $\mathbb{Q}_p$.*

Beweis: Theorem 9.15 und Satz 9.13 □

Definition 9.17. *Die kanonischen Absolutbeträge auf K heißen* Stellen *von K.*

Wir schreiben $v|w$, wenn $|\cdot|_w$ den Betrag $|\cdot|_v$ fortsetzt.

Bemerkung. $\mathbb{Q}$ hat die Stellenmenge $S(\mathbb{Q}) = \{\infty, p\mathrm{prim}\}$.

Korollar 9.18. *Sei K ein Zahlkörper, v eine Stelle von K, $p|v$ eine Primzahl. Dann ist v assoziiert zu einem Primideal $\mathfrak{p}$ von $\mathcal{O}_k$, das p enthält.*

Beweis: Auf $K_v \subset \mathcal{O}_v$ ist der Betrag $|\cdot|_v$ nach Lemma 9.14 von einem Primideal $\mathfrak{p}_v$ induziert. Es gilt $\mathcal{O} \subset \mathcal{O}_v$, da die Elemente von $\mathcal{O}$ ganz über $\mathbb{Z}$, also erst recht ganz über $\mathbb{Z}_p$ sind. Das Primideal $\mathfrak{p} = \mathcal{O} \cap \mathfrak{p}_v$ induziert dann $|\cdot|_v$. □

Korollar 9.19. *Sei K ein Zahlkörper, S die Menge der Stellen von K, die Unendlich nicht teilen. Dann gilt*

$$\mathcal{O}_K = \{x \in K \mid |x|_v \leq 1 \text{ für alle } v \in S\}$$

Beweis: Sei $x = a/b$ mit $a, b \in \mathcal{O}_K$. Sei $|x|_v = |x|_\mathfrak{p}$ für ein Primideal $\mathfrak{p}$. Dann gilt

$$\left|\frac{a}{b}\right|_v \leq 1 \Leftrightarrow v_p f(a) \geq v_\mathfrak{p}(b)$$

In der Primfaktorzerlegung von a und b gilt also

$$(a) = \prod \mathfrak{p}^{v_\mathfrak{p}(a)} \subset (b) = \prod \mathfrak{p}^{v_\mathfrak{p}(b)}$$

Dies bedeutet $a = \gamma b$ für $\gamma \in \mathcal{O}_K$, also $\gamma = x \in \mathcal{O}_K$. □

Kapitel 10

Erweiterungen von lokalen Körpern

Sei L/K eine Erweiterung von lokalen Körpern. Falls $\mathbb{R} \subset K$ gibt es nur drei Möglichkeiten: $\mathbb{R}/\mathbb{R}, \mathbb{C}/\mathbb{R}, \mathbb{C}/\mathbb{C}$. Wir definieren $e(\mathbb{C}/\mathbb{R}) = 2$ (Verzweigungsindex), $f(\mathbb{C}/\mathbb{R}) = 1$ (Restklassengrad). Ab jetzt behandeln wir den Fall $\mathbb{Q}_p \subset K$ für eine feste Primzahl p. Wir nenne diese Körper p-adisch.

Definition 10.1. *Sei L/K Erweiterung von p-adischen Körpern. Sei π_L Primelemet von $\mathcal{O}_L$, π_K Primelement von $\mathcal{O}_K$. Dann heißt $\kappa(K) = \mathcal{O}_K/(\pi_K)$* Restklassenkörper *von K. $f(L/K) = [\kappa(L) : \kappa(K)]$ heißt* Restklassengrad *von L/K. Der* Verzweigungsgrad *$e(L/K)$ wir definiert durch $(\pi_K \mathcal{O}_L)(\pi_L)^{e(L/K)}$.*

Bemerkung. Sei $v : L^* \to \mathbb{R}$ eine diskrete Bewertung. Nach Definition gilt $\pi_K = u\pi_L^{e(L/K)}$ für eine Einheit $u \in \mathcal{O}_L^*$. Es folgt

$$v(\pi_K) = 0 + e(L/K)v(\pi_L) \Rightarrow e(L/K) = v(\pi_K)/v(\pi_L)$$

Satz 10.2 (Gradformel)**.** *Sei L/K Erweiterung von lokalen Körpern. Dann ist*

$$[L : K] = e(L/K)f(L/K)$$

Beweis: Siehe Beweis von Satz 7.2 (Gradformel für Zahlkörper). □

Korollar 10.3. *Sei L/K Erweiterung von Zahlkörpern, $\mathfrak{p} \mid \mathfrak{P}$ ein Primideal. Dann gilt*

$$e(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = e(\mathfrak{P}/\mathfrak{p}) \qquad f(L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

Beweis: Nach Satz 9.11 stimmen die Restklassenkörper überein, $\kappa(\mathfrak{p}) = \kappa(K_{\mathfrak{p}})$, daher auch der Restklassengrad. Die Aussage für den Verzweigungindex folgt aus der Definition der Bewertung und der obigen Bemerkung. □

Die globale Gradformel kann also umgeschrieben werden als

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

Bemerkung. Unsere Definition für $v \mid \infty$ ist so gemacht, dass diese Formel auch für $v \mid \infty$ stimmt, z.B. für $K/\mathbb{Q}$:

$$[K : \mathbb{Q}] = r_1 + 2r_2 = \sum_{v|\infty} e(K_v/\mathbb{R})$$

Viele Eigenschaften des Zahlrings, z.B. die Verzweigung, können also bestimmt werden, ohne $\mathcal{O}$ aus den Gleichungen zu bestimmen.

Galoistheorie

Lemma 10.4. *Sei L/K Galoiserweiterung p-adischer Körper. Dann operiert $\mathrm{Gal}(L/K)$ auf $\mathcal{O}_L$. Dies induziert einen surjektiven Gruppenhomomorphismus*

$$\Phi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa(L)/\kappa(K)$$

Sei $I(L/K) = \operatorname{Ker} \Phi$. Dann gilt

$$|I(L/K)| = e(L/K), |\operatorname{Gal}(\kappa(L), \kappa(K)| = f(L/K)$$

Beweis: Wie im Zahlkörperfall, nur einfacher. □

Bemerkung. Wie im Zahlkörperfall gilt: Die Teilerweiterung $L^{I(L/K)}/K$ ist unverzweigt.

Satz 10.5. *Sei L/K Galoiserweiterung von Zahlkörpern, $\mathfrak{P} \mid \mathfrak{p}$ Primideale. Es gilt*

$$D(\mathfrak{P}/\mathfrak{p}) = \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}), I(\mathfrak{P}/\mathfrak{p}) = I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

Beweis: Sei w die zu $\mathfrak{P}$ gehörende Bewertung auf L, $\sigma \in \mathrm{Gal}(L/K)$. Durch $w'(x) = w(\sigma(x))$ wird eine andere Bewertung von L definiert. Beide stimmen auf K überein und gehören dort zu $\mathfrak{p}$. Sei $\mathfrak{P}'$ das Primideal zu w'. Für $\sigma \in D(\mathfrak{P}/\mathfrak{p})$, so gilt nach Definition $\sigma(\mathfrak{P}) = \mathfrak{P}$, also $\mathfrak{P}' = \mathfrak{P}$. Wegen der Eindeutigkeit der Bewertung folgt $w = w'$. Durch stetige Fortsetzung operiert $D(\mathfrak{P}/\mathfrak{p})$ auf L_w. Auf K und damit auf K_w operiert $D(\mathfrak{P}/\mathfrak{p})$. Wir erhalten eine injektive Abbildung

$$D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L_w/K_w)$$

Da beide Gruppen ef Elemente haben, ist die Zurordnung bijektiv. Das Diagramm

$$\begin{array}{ccc} D(\mathfrak{P}/\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L_w/K_w) & \longrightarrow & \mathrm{Gal}(\kappa(L_w)/\kappa(K_w) \end{array}$$

kommutiert. Daher stimmen auch die beiden Kerne überein. □

Satz 10.6. *Seien $L_1, L_2/K$ Galoiserweiterungen, $e(L_1/K) = 1$, $L = L_1L_2$. Dann ist $e(L/K) = e(L_2/K)$. Insbesondere ist L/K unverzweigt, falls L_2/K ebenfalls unverzweigt.*

Beweis: Der Teilkörper $L_1 \cap L_2$ ist unverzweigt über K. Ohne Einschränkung ist $K = L_1 \cap L_2$. Wir betrachten den unverzweigten Fall. Wie im globalen Fall (Satz 7.15) gilt $\mathcal{O}_L = \mathcal{O}_{L_1}\mathcal{O}_{L_2}$ und die Diskriminante kann explizit berechnet werden. Sie ist in unserem Fall 1.
Allgemein sei L_2^u der unverzweigte Teilkörper von L_2/L. Dann ist $L' = L_1 L_2^u$ unverzweigt über K und

$$e(L/K) \leq [L : L'] = [L_2 : L_2^u] = e(L_2/K)$$

Andererseits ist der Verzweigungsindex multiplikativ, daher $e(L_2/K)|e(L/K)$. Es folgt Gleichheit. □

Theorem 10.7 (lokaler Satz von Kronecker-Weber)**.** *Sei $k/\mathbb{Q}_p$ abelsche Galoiserweiterung lokaler Körper. Dann gilt*

$$k \subset \mathbb{Q}_p(\zeta_N)$$

für geeignetes N.

Beweis von Theorem 8.6. Sei $K/\mathbb{Q}$ abelsche Erweiterung. Sei S die Menge der Primzahlen, die in K verzweigen. Sei K_p die Komplettierung bezüglich einer Stelle von K über $p \in S$. Dann ist $L_p/\mathbb{Q}_p$ abelsch und daher $L_p \subset \mathbb{Q}_p(\zeta_{n_p})$ für geeignetes n_p. Sei p^{e_p} die genaue p-Potenz i n_p. Wir setzen

$$N = \prod_{p \in S} p^{e_p}$$

Behauptung. $K \subset \mathbb{Q}(\zeta_N)$.

Sei $M = L(\zeta_N)$. Dies ist abelsch über $\mathbb{Q}$ und unverzweigt außerhalb S. Sei M_p die Komplettierung bezüglich einer Stelle, die die Stelle zu L_p enthält, also $\mathbb{Q}_p \subset L_p \subset M_p$. Es gilt

$$M_p = L_p(\zeta_n) = \mathbb{Q}_p(\zeta_{p^{e_p} n'}) = \mathbb{Q}_p(\zeta_{p^{e_p}})\mathbb{Q}(\zeta_{n'})$$

für $(n', p) = 1$. Hierbei ist $\mathbb{Q}_p(\zeta_{n'})/\mathbb{Q}_p$ unverzweigt und $\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p$ rein verzweigt. Da $\mathbb{Q}(\zeta_{p^{e_p}}))/\mathbb{Q}$ ebenfalls rein verzweigt ist in p, folgt

$$e_p(\mathbb{Q}(\zeta_{p^{e_p}}))/\mathbb{Q}) = e(\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p = \phi(p^{e_p})$$

Die Trägheitsgruppe $I_p = I(M_p/\mathbb{Q}_p)$ hat daher $\phi(e^{e_p})$ Elemente.
Sei nun I die Untergruppe von $\mathrm{Gal}(M/\mathbb{Q})$, die von den I_p für $p \in S$ erzeugt wird. Da die Gruppen abelsch sind, ist dies das Bild von $\prod I_p$ unter der natürlichen Abbildung. Es gilt

$$|I| \leq \prod_{p \in S} |I_p| = \prod_{p \in S} \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_N) : \mathbb{Q})]$$

Der Fixkörper M^I ist unverzweigt an Stellen, muss also nach dem Theorem von Minkowski mit $\mathbb{Q}$ übereinstimmen, d.h.

$$[M : \mathbb{Q}] = |I| \leq \phi(N)$$

Hieraus folgt $M = \mathbb{Q}(\zeta_N)$. □

Strukturtheorie lokaler Körper (Schnelldurchgang)

Sei nun $k/\mathbb{Q}_p$ lokaler Körper.

Lemma 10.8. *In k gilt: $\sum_{i=0}^{\infty} a_i$ konvergent genau dann, wenn $(a_i)_{i=0}^{\infty}$ Nullfolge.*

Beweis: Beachte: $|\sum_{i=0}^{N} a_i| \leq \max_{i=0}^{N} |a_i|$ □

Satz 10.9 (Henselsches Lemma)**.** *Sei $\mathcal{O} \subset k$ der Bewertungsring, $f \in \mathcal{O}[T]$. Sei $\alpha_0 \in \mathcal{O}$ mit*

$$|f(\alpha_0)| < |f'(\alpha_0)^2|$$

wobei f' die formale Ableitung von f ist. Dann konvergiert die Folge

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

gegen eine Wurzel α von f. Es gilt

$$|\alpha - \alpha_0| \leq \frac{|f(\alpha_0)|}{|f'(\alpha_0)^2|} \leq 1$$

Bemerkung. Dies lässt sich auch in Termen der Bewertung, also von Teilbarkeit durch das Primelement formulieren und beweisen. Ein wichtiger Spezialfall ist $\alpha_0 \in \mathcal{O}$, $f(\alpha_0) = 0$ im Restklassenkörper (d.h. $|f(\alpha_0) < 1$) und $f'(\alpha_0) \neq 0$ im Restklassenkörper (d.h. $|f'(\alpha_0)| = 1$).

Beweis: Dies ist das Newton-Verfahren für den p-adischen Betrag. Für Einzelheiten siehe: Koblitz, p-adic Numbers, p-adic Analysis and Zeta-Functions, Lang: Algebraic Number Theory.
Sei

$$c = \left| \frac{f(\alpha_0)}{f'(\alpha_0)^2} \right|_p < 1$$

Wir zeigen induktiv:

(i) $|\alpha_i| \leq 1$

(ii) $|\alpha_i - \alpha_0| \leq c$

(iii) $\left| \frac{f(\alpha_i)}{f'(\alpha_i)^2} \right|_p < c^{2^i}$

Die Bedinung (i) besagt, dass alle α_i und damit auch alle $f(\alpha_i)$, $f'(\alpha_i)$ ganz sind. Die Bedingung (iii) besagt, dass

$$|\alpha_{i+1} - \alpha_i| = \left| \frac{f(\alpha_i)}{f'(\alpha_i)} \right|_p \leq |f'(\alpha_i)|_p c^{2^i} \leq c^{2^i}$$

Also ist dies eine Nullfolge. Hieraus folgt Konvergenz der Folge α_i. Wegen der Stetigkeit des Betrages folgt aus (ii) die Abschätzung für α. Der Grenzwert erfüllt wegen Stetigkeit von f und f' die Gleichung

$$\alpha = \alpha - \frac{f(\alpha)}{f'(\alpha)}$$

Dies bedeutet $f(\alpha) = 0$.
Nun verifizieren wir die Eigenschaften (i), (ii), (iii). Für $i = 0$ ist dies jeweils die Voraussetzung. Schluss von i nach $i + 1$:

(i) Die Eigenschaft (iii) bedeutet

$$\alpha_{i+1} - \alpha_i| = \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|_p = \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right|_p |f'(\alpha_i)|_p \leq 1c^{2^i}$$

Mit (i) impliziert dies $|\alpha_{i+1} \leq 1$.

(ii) $|\alpha_{i+1} - \alpha_0| \leq \max(|\alpha_{i+1} - \alpha_i|, |\alpha_i - \alpha_0|) \leq \max(c^{2^i}, c) = c$.

(iii) Sei $g \in \mathcal{O}[T]$ ein Polynom. Seine Taylorentwicklung in einem Punkt x_0 ist

$$g(x_0 + T) = g(x_0) + g'(x_0)T + h(T)T^2$$

(Betrachte z.B. $g(T) = cT^n$) Wir setzen nun $g = f$, $x_0 = \alpha_i$, $T = -\frac{f(\alpha_i)}{f'(\alpha_i)}$. Es gilt also

$$f(\alpha_{i+1} = f(\alpha_i) - f'(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \beta\left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2$$

mit $\beta \in \mathcal{O}$. Die ersten beiden Summanden heben sich weg, also

$$|f(\alpha_{i+1})| \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2$$

Nun setzen wir $g = f'$, $x_0 = \alpha_i$ und $T = -\frac{f(\alpha_i)}{f'(\alpha_i)}$. Damit

$$f'(\alpha_{i+1}) = f'(\alpha_i) + \gamma\frac{f(\alpha_i)}{f'(\alpha_i)}$$

mit $\gamma \in \mathcal{O}$. Dies impliziert

$$|f'(\alpha_{i+1})| \geq \max\left(|f'(\alpha_i)|, \left|\gamma\frac{f(\alpha_i)}{f'(\alpha_i)}\right|\right)$$

und sogar Gleichheit, falls die Beträge unterschiedlich sind. Nach Induktionsvoraussetzung gilt

$$|f'(\alpha_i)| > \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right| \geq |\gamma\frac{f(\alpha_i)}{f'(\alpha_i)}$$

Also $|f'(\alpha_{i+1})| = |f'(\alpha_i)|$. Zusammen folgt nun

$$\left|\frac{f(\alpha_{i+1})}{f'(\alpha_{i+1})^2}\right|_p \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2 \frac{1}{|f'(\alpha_i)|} = \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right|^2 < (c^{2^i})^2$$

□

Beispiel. Sei $(N,p) = 1$, Φ_N das zyklotomische Polynom, also ein Teiler von $X^N - 1$. Sei $\alpha \in \mathcal{O}$ eine Nullstelle dieses Polynoms im Restklassenkörper, $|f(a_0)| < 1$ wobei π ein Primelement ist. Weiterhin ist $f'(\alpha) \neq 0$ im Restklassenkörper, da $(X^N - 1)' = NX^{N-1}$ ungleich Null. Dies bedeutet $|f'(\alpha_0)|^2 = 1$. Die Vorraussetzung des Henselschen Lemmas ist erfüllt. Φ_N hat eine Nullstelle in k.

Korollar 10.10. *Sei $k/\mathbb{Q}_p$ endlich. Dann gibt es einen Teilkörper $k^u \subset k$, der unverzweigt über $\mathbb{Q}_p$ ist. Es gilt $f(k/\mathbb{Q}_p) = f(k^u/\mathbb{Q}_p)$ und $e(k/k^u) = e(k/\mathbb{Q}_p)$. Der Körper k^u wird von Einheitswurzeln erzeugt, deren Ordnung prim zu p ist.*

Beweis: Sei $f = f(k/\mathbb{Q}_p)$, d.h. $\mathbb{F}_{p^f}$ ist der Restklassenkörper von k. Es gilt $\mathbb{F}_{p^f} = \mathbb{F}_p(\overline{\alpha})$, wobei $\overline{\alpha}$ eine primitive (p^f-1)-te Einheitswurzel ist. Dies bedeutet, dass das zyklotomische Polynom Φ_{p^f-1} eine Nullstelle im Restklassenkörper hat. Wie im Beispiel hat Φ_{p^f-1} eine Nullstelle α in k, die $\overline{\alpha}$ induziert. Sei nun $k^u = \mathbb{Q}_p(\alpha) \subset k$. Der Restklassenkörer von k^u enthält $\overline{\alpha}$, ist also ganz $\mathbb{F}_{p^f}$. Damit ist $f(k^u/\mathbb{Q}_p) = f$. □

Kronecker-Weber

Wir reduzieren nun den Beweis von Theorem 10.7 auf die folgenden Aussagen:

Lemma 10.11. *Sei K p-adischer Körper, $e \in \mathbb{N}$ mit $(p,e) = 1$ und $u \in \mathcal{O}_K^*$. Sei $L = K(\alpha)$, wobei $\alpha^e = u$. Dann ist L/K unverzweigt.*

Beweis: Übungsaufgabe. □

Lemma 10.12. $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$

Beweis: Übungsaufgabe. □

Beide Körper sind Galois mit derselben Ordnung und zyklischer Galoisgruppe.

Satz 10.13. *Es gibt keine Galoiserweiterung von $\mathbb{Q}_p$ mit Galoisgruppe isomorph zu $(\mathbb{Z}/p\mathbb{Z})^3$.*

Beweis: Kummertheorie, kommt noch. □

Beweis von Theorem 10.7. Sei $K/\mathbb{Q}_p$ Galoiserweiterung mit abelscher Galoisgruppe. Wir betrachten nacheinander die Fälle

(i) *unverzweigt:* $e(K/\mathbb{Q}_p) = 1$ (ok nach Korollar 10.10)

(ii) *zahm verzweigt:* $(p, e(K/\mathbb{Q}_p)) = 1$

(iii) *wild verzweigt:* $p|e(K/\mathbb{Q}_p)$.

$K/\mathbb{Q}_p$ **zahm verzweigt**: Sei e der Verzweigungsindex, π ein Primelement von K.
Sei $K^u = \mathbb{Q}_p(\zeta_n)$ der maximale unverzweigt Teilkörper von K. $K/\mathbb{Q}_p(\zeta_n)$ ist rein verweigt vom Grad e.
Es ist $\pi^e = -up$ für $u \in \mathcal{O}_K^*$. Wir gehen über von K zu $L = K(u^{1/e})$. Nach Lemma 10.11 ist L/K unverzweigt, d.h. π bleibt Primelement von L. Nach Korollar 10.10 wird L/K von einer Einheitswurzel ζ_N mit $(p, N) = 1$ erzeugt.
$\pi' = u^{-1/e}\pi$ ist ein anderes Primelement von K'. Es erfüllt $(\pi')^e = -p$, d.h. $\pi' = \sqrt[e]{-p}$. Daher ist

$$L = \mathbb{Q}_p(\zeta_n, \zeta_N, \sqrt[e]{-p}) = \mathbb{Q}_p(\zeta_n, \zeta_N)\mathbb{Q}_p(\sqrt[e]{-p})$$

Insbesondere sind L und sein Teilkörper $\mathbb{Q}_(\sqrt[e]{-p})$ abelsch. Da $\mathbb{Q}_p(\sqrt[e]{-p})/\mathbb{Q}_p$ galois ist, folgt $\zeta_e \in \mathbb{Q}_p(\sqrt[e]{-p})$. Da der Körper zahm verzeigt ist, folgt $e|p-1$. Andererseits ist $\mathbb{Q}_p(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_p)$. Damit ist dieser Fall abgeschlossen.
$K/\mathbb{Q}_p$ **wild verzweigt:** Sei nun $K/\mathbb{Q}_p$ beliebig, $G = \mathrm{Gal}(K/\mathbb{Q}_p)$. Dann ist $K = K_1K_2$ mit $[K_1 : \mathbb{Q}_p]$ teilerfremd zu p, $[K_2 : \mathbb{Q}_p]$ eine Potenz von p. Die Erweiterung K_1/K ist zahm verzweigt. Diesen Fall haben wir bereits behandelt. Es genügt also ohne Einschränkung, $K = K_2$ zu betrachten. Seine Galoisgruppe ist ein p-Gruppe der Ordnung p^d.
Wir kennen zwei solche Körper: $L_1 \subset \mathbb{Q}(\zeta_{p^{d+1}})$ der Teilkörper vom Grad p^d. Er ist rein verzweigt über $\mathbb{Q}_p$. Sei L_2 die unverweigte Erweiterung vom Grad p^d. Das Kompositum $L = L_1L_2$ ist abelsch mit Galoisgruppe $(\mathbb{Z}/p^d)^2$. Angenommen, K ist nicht in L enthalten. Dann ist KL eine Galoiserweiterung von $\mathbb{Q}_p$ mit Galoisgruppe $(\mathbb{Z}/p^d)^2 \times G'$ für eine p-Gruppe G'. Dann gibt es einen Teilkörper E von KL mit Galoisgruppe $\mathrm{Gal}(E/\mathbb{Q}_p) \cong (\mathbb{Z}/p)^3$. Dies ist unmöglich. □

Nachtrag zur Galoistheorie: Seien $L, K\mathbb{Q}_p$ wie im Beweis: $L/\mathbb{Q}_p$ galois mit Gruppe $(\mathbb{Z}/p^d\mathbb{Z})^2$, $K/\mathbb{Q}_p$ endlich abelsch mit Galoisgruppe eine p-Gruppe mit p^d Elementen, $K \cap L \neq K$. Nach Elementarteilersatz hat ein endliche abelsche p-Gruppe die Form

$$(\mathbb{Z}/p^{d_1}\mathbb{Z}) \times \ldots (\mathbb{Z}/p^{d_n}\mathbb{Z})$$

mit $d_1 \geq d_2 \geq \ldots d_n$. Dabei sind n und die d_i eindeutig.
Nach Voraussetzung hat die Galoisgruppe von $L/\mathbb{Q}_p$ zwei Elementarteiler, die von $K/\mathbb{Q}_p$ wenigstens einen. Angenommen $\mathrm{Gal}(L/L \cap K)$ hat weniger als zwei Elementarteiler. Dann geht ein Faktor $\mathbb{Z}/d\mathbb{Z}$ in der Galoisgruppe von $K \cap L/\mathbb{Q}_p$ auf. Diese hat Ordnung mindestens p^d. Wegen $[K : \mathbb{Q}_p] = p^d$ folgt $K \cap L = K$. Dies widerspricht der Vorraussetzung.
Es gilt $\mathrm{Gal}(LK/L \cap K) = \mathrm{Gal}(L/L \cap K) \times \mathrm{Gal}(K/L \cap K)$. Also hat diese Gruppe wenigstens drei Elementarteiler. Wegen $\mathrm{Gal}(LK/\mathbb{Q}_p) \supset \mathrm{Gal}(LK/L \cap K)$ folgt dies auch für $\mathrm{Gal}(LK/\mathbb{Q}_p)$. Mit etwas mehr Sorgfalt erhält man, dass der maximale Elementarteiler p^d ist. Dies wird aber für den Beweis des Satzes gar nicht benötig.

Kapitel 11

Kummer-Theorie

Etwas homologische Algebra

Definition 11.1. *Sei $[a,b] \subset \mathbb{Z}$ ein Intervall ($a = -\infty$, $b = \infty$ sind erlaubt). Ein* (kohomologischer) Komplex *ist eine Folge K^i für $i \in [a,b]$ von abelschen Gruppen zusammen mit* Randabbildungen *$d^i : K^i \to K^{i+1}$, so dass gilt $d^i \circ d^{i-1} = 0$ für $i \in [a+1, b]$.*

$$\ldots K^{i-1} \xrightarrow{d^{i-1}} K^i \xrightarrow{d^i} C^{i+1} \xrightarrow{d^{i+1}} K^{i+2} \to \ldots$$

*$Z^i = \operatorname{Ker} d^i$ heißt Gruppe der i-*Kozykel*. $B^i = \operatorname{Im} d^{i-1}$ heißt Gruppe der* Koränder*.*

$$H^i(K^*) = Z^i/B^i$$

heißt i-te Kohomologiegruppe *von K^*. Ein Komplex heißt* exakt*, wenn $H^i(K^*) = 0$ für alle i.*

Bemerkung. Wegen $d^i \circ d^{i+1} = 0$ gilt $B^i \subset Z^i$. Ein Komplex ist exakt, wenn $\operatorname{Im} d^{i-1} = \operatorname{Ker} d^i$ für alle i.

Exakte Komplexe der Form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

heißen *kurze exakte Sequenz*. Dies bedeutet, dass g surjektiv ist mit Kern A. Oder umgekehrt formuliert: f injektiv mit *Kokern* $B/f(A) \cong C$.

Definition 11.2. *Seien A^* und B^* Komplexe. Ein* Morphismus von Komplexen *$f^* : A^* \to B^*$ ist eine Folge von Homomorphismen $f^i : A^i \to B^i$, so dass die Diagramm kommutieren:*

$$\begin{array}{ccc} A^{i+1} & \xrightarrow{f^{i+1}} & B^{i+1} \\ {\scriptstyle d^i}\uparrow & & \uparrow{\scriptstyle d^i} \\ A^i & \xrightarrow{f^i} & B^i \end{array}$$

Eine kurze exakte Sequenz von Komplexen *ist ein Folge von Morphismen von Komplexn*

$$0 \to A^* \to B^* \to C^* \to 0$$

so dass alle Zeilen $0 \to A^i \to B^i \to C^i \to 0$ *kurze exakte Sequenzen von abelschen Gruppen sind.*

Der Witz ist, dass man mit Kohomologiegruppen rechen kann.

Satz 11.3. *Sei* $0 \to A^* \to B^* \to C^* \to 0$ *ein kurze exakte Sequenz von Komplexen. Dann gibt es eine natürliche lange exakte Sequenz*

$$\to H^i(A^*) \to H^i(B^*) \to H^i(C^*) \to H^{i+1}(A^*) \to \dots$$

Beweis: Vergl. z.B. S. Lang, Algebra oder Bücher zur algebraischen Topologie. Die Abbildungen $H^i(A^*) \to H^i(B)$ sind einfach, sie werden von $A^i \to B^i$ induziert. Schwierig ist der Verbindungshomomorphismus

$$\delta : H^i(C^*) \to H^{i+1}(A^*)$$

Man erhält ihn wie folgt. Sei $\overline{c} \in H^i(C)$, $c \in Z^i(C^*)$ ein Repräsentant. Wegen der Surjektivität von $B^i \to C^i$ gibt es ein Urbild $b \in B^i$. Wir bilden es mit d^i nach $b' \in B^{i+1}$ ab. Nun überprüfen wir, dass das Bild von b' in C^{i+1} verschwindet. Es stimmt nämlich mit $d^i(c)$ überein und nach Vorraussetzung liegt c im Kern von d^e. Da die Sequenz

$$0 \to A^{i+1} \to B^{i+1} \to C^{i+1} \to 0$$

exakt ist, folgt dass $b' \in A^{i+1}$. Zur Unterscheidung nennen wir es dort a. Wir zeigen, dass $d^{i+1}a = 0$. Es ist nämlich $d^{i+1}b' = d^{i+1}d^i b = 0$. Wir setzen $\delta(\overline{c})$ die Klasse von a in $H^{i+1}(A)$.
Wohldefiniertheit und Exaktheit der Sequenz rechnet man nach. □

Galoiskohomologie

Definition 11.4. *Sei* G *ein Gruppe. Ein* G-Modul *ist eine abelsche Gruppe* M *zusammen mit einer Abbildung*

$$G \times M \to M; (g, m) \mapsto gm$$

so dass gilt

(i) $(gh)m = g(hm)$ *für alle* $g, h \in G$, $m \in M$.

(ii) $em = m$ *für das neutrale Element* $e \in G$.

(iii) $g(m + n) = gm + gn$ *für alle* $g \in G$, $m, n \in M$.

Beispiel. Sei M eine abelsche Gruppe. Dann ist $gm := m$ eine Operation. M heißt dann *trivialer G-Modul*.

Ist speziell $G = \mathrm{Gal}(L/K)$ für eine Körpererweiterung, so sprechen wir auch von *Galoismoduln*.

Beispiel. Sei L/K algebraische Körpererweiterung. Dann sind L und L^* mit der natürlichen Operation $\sigma x = \sigma(x)$ Galoismoduln.

Lemma 11.5. *Sei G eine Gruppe, M ein G-Modul. Wir setzen für $i \geq 0$*

$$C^i(G, M) = \mathrm{Abb}(G^i, M)$$

(mengentheoretische Abbildungen) mit dem Differential $d^i : C^i(G, M) \to C^{i+1}(G, M)$

$$d^i(f)(g_1, \ldots, g_{n+1}) =$$

$$g_1 f(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j f(g_1, \ldots, g_{j-1}, g_j g_{j+1}, \ldots, g_{i+1}) + (-1)^{i+1} f(g_1, \ldots, g_i)$$

Dies ist ein Komplex.

Beweis: Wir machen kleine Grade explizit: $C^0(G, M) = M$. Es gilt $d^0(m)(g) = gm - m$. Für $f \in C^1(G, M)$ gilt

$$d^1 f(g, h) = gf(h) - f(gh) + f(g)$$

Es folgt also

$$\begin{aligned} d^1 d^0(m)(g, h) &= g d^0(m)(h) - d^0(m)(gh) + d^0(m)(g) \\ &= g(hm - m) - (ghm - m) + (gm - m) = 0 \end{aligned}$$

Höhere Grade werden wir nicht benötigen. Man rechnet sie genauso explizit nach. □

Definition 11.6. *Mit den Notationen aus Lemma 11.5 heißt*

$$H^i(G, M) = H^i(C^*(G, M))$$

die i-te Gruppenkohomologie *von G mit Koeffizienten in M. Ist speziell $G = \mathrm{Gal}(L/K)$, so heißt*

$$H^i(L/K, M) = H^i(G, M)$$

i-te Galoiskohomologie.

Beispiel.

$$H^0(G, M) = \mathrm{Ker}(d^0 : M \to C^1(G,)) = \{m \in M | gm = m\} = M^G$$

Insbesondere $H^0(L/K, L) = K$, $H^0(L/K, L^*) = K^*$ falls L/K Galoiserweiterung.

$$Z^1(G, M) = \mathrm{Ker}\, d^1 = \{f : G \to M | gf(h) - f(gh) + f(h) = 0\}$$

Abbildungen $f : G \to M$ mit $f(gh) = gf(h) + f(h)$ heißen auch *verschränkte Homomorphismen*. Ist M ein trivialer G-Modul, so sind dies genau die Gruppenhomomorphismen.

$$B^1(G, M) = \operatorname{Im} d^0 = \{f : G \to M | \text{es gibt } m \in M, f(g) = gm - m\}$$

Ist M trivialer G-Modul, so gilt $f(g) = m - m = 0$. Also zusammen:

$$H^1(G, M) = \operatorname{Hom}(G, M)$$

für triviale G-Modulen.

Satz 11.7. *Sei $0 \to M_1 \to M_2 \to M_3 \to 0$ ein kurze exakte Sequenz von G-Moduln. Dann erhalten wir eine natürliche exakte Sequenz*

$$0 \to H^0(G, M_1) \to H^0(G, M_2) \to H^0(G, M_3) \to H^1(G, M_1) \to \dots$$

Beweis: Für jedes i ist

$$0 \to C^i(G, M_1) \to C^i(G, M_2) \to C^i(G, M_3) \to 0$$

eine kurze exakte Sequenz. Es handelt sich um die lange exakte Kohomologiesequenz einer kurzen exakten Sequenz von Komplexen. □

Satz 11.8 (Hilbert 90)**.** *Sei L/K endliche Galoiserweiterung. Dann gilt*

$$H^1(L/K, L^*) = 1$$

Jeder Kozykel ist ein Korand.

Beweis: Sei $f : \operatorname{Gal}(L/K) \to L^*$ ein Kozykel. Zu $x \in L$ betrachten wir

$$b = \sum_{\tau \in \operatorname{Gal}(L/K)} f(\tau)\tau(x) \in L$$

Da die τ linear unabhängig sind, gibt es ein x mit $b \neq 0$. Für dieses x, b folgt

$$\begin{aligned}\sigma(b) = \sigma\left(\sum_\tau f(\tau)\tau(x)\right) &= \sum_\tau \sigma(f(\tau))\sigma\tau(x) \\ &= \sum f(\sigma\tau)f(\sigma)^{-1}\sigma\tau(x) = f(\sigma)^{-1}b\end{aligned}$$

wobei wir die Kozykelbedingung ausgenutzt haben. Es folgt $f(\sigma) = b/\sigma(b)$, also $f = d^0(b)$. □

Sei $\mu_n(L)$ die Gruppe der n-ten Einheitswurzeln in L. Dies ist ein Untergruppe von L^*. Es ist der Kern der n-Potenzierungsabbildung $x \mapsto x^n$. Wir schreiben L^{*n} für die n-ten Potenzen, also das Bild.

Korollar 11.9. *Sei L/K endliche Galoiserweiterung.*

(i) Es gilt

$$H^1(L/K, \mu_n(L)) \cong L^{*n} \cap K^*/K^{*n}$$

(ii) Enthält K alle n-ten Einheitswurzeln, so gilt

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n(L)) \cong L^{*n} \cap K^*/K^{*n}$$

Die induzierte Paarung

$$L^{*n} \cap K^*/K^{*n} \times \mathrm{Gal}(L/K) \to \mu_n(L)$$

ist gegeben durch $(a, \sigma) \mapsto \sigma(\sqrt[n]{a})/\sqrt[n]{a}$.

Bemerkung. Man beachte, dass $\sqrt[n]{a}$ in L existiert. Es unterscheidet sich von $\sigma(\sqrt[n]{a})$ um eine n-the Einheitswurzel, da beides Lösungen von $X^n - a$ sind.

Beweis: Wir betrachten die lange exakte Kohomologiesequenz zur kurzen exakten Sequenz

$$1 \to \mu_n(L) \to L^* \xrightarrow{x \mapsto x^n} L^{*n} \to 1$$

(Wir schreiben 1 statt 0, da die abelschen Gruppen multiplikativ sind). Sie lautet

$$1 \to \mu_n(K) \to K^* \to K^* \cap L^{*n} \to H^1(L/K, \mu_n(K) \to 1$$

nach Hilbert 90. Also ist die letzte Abbildung surjektiv und der Kern ist das Bild von K^* unter n-Potenzierung. Die zeigt die erste Aussage.
Ist $\mu_n(K) = \mu_n(L)$, so operiert die Galoisgruppe trivial. Die zweite Ausage folgt wegen unserer Berechnung für Gruppenkohomologie von trivialen Moduln. Die explite Formel folgt aus der Konstruktion der Randabbildung der Kohomologiesequenz. □

Theorem 11.10 (Kummererweiterung)**.** *Sei K ein Körper, n natürliche Zahl mit $(\mathrm{Char}\, K, n) = 1$. K enthalte alle n-ten Einheitswurzeln. Sei weiter L/K eine endliche Galoiserweiterung mit $\mathrm{Gal}(L/K)$ zyklisch der Ordnung n. Dann gilt $L = K(a)$ und $\mathrm{Min}(a)(X) = X^n - b$, d.h. $a = \sqrt[n]{b}$.*

Bemerkung. Umgekehrt sieht man leicht, dass $K(\sqrt[n]{b})/K$ Galois ist mit Galoisgruppe eine Untergruppe von $\mathbb{Z}/n\mathbb{Z}$, also zyklisch.

Beweis: Wegen der Vorraussetzung an die Charakteristik hat $\mu_n(K)$ genau n Elemente. Die Gruppe ist als Untergruppe eines Körpers zyklisch. Daher gilt

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \cong \mathrm{Hom}(\mathbb{Z}/n, \mathbb{Z}/n) \cong \mathbb{Z}/n$$

Nach Korollar 11.9 folgt

$$L^{*n} \cap K^*/K^{*n} \cong \mathbb{Z}/n$$

Sei b ein Erzeuger. Dies ist ein Element von K, das in L von der Form $a^n = b$ ist. Es erfüllt das Polynom $X^n - b$

Behauptung. *$X^n - b$ ist das Minimalpolynom von a.*

Sei σ Erzeuger von $\mathrm{Gal}(L/K)$. Nach Wahl von b ist unter der Kummerpaarung $(b, \sigma) = \sigma(a)/a$ eine primitive n-te Einheitswurzel. Nach dem Hauptsatz der Galoistheorie muss dann $K(a) = L$ sein. □

Theorem 11.11. *Sei K Körper der Charakteristik 0, $P \in K[X]$ ein irreduzibles Polynom, $a \in \overline{K}$ ein Nullstelle von P. Dann ist a genau dann durch Radikale ausdrückbar, wenn die Galoisgruppe des Zerfällungskörpers von P auflösbar ist.*

Beweis: Die Hinrichtung folgt aus der Analysise von Radikalerweiterungen $L(\sqrt[n]{a})/L$ und wird in der Regel in Algebra behandelt. Nun geht es um die Rückrichtung. Sei L der Zerfällungskörper von P und $G = \mathrm{Gal}(L/K)$. Nach Vorraussetzung (und Strukturtheorie von auflösbaren Gruppen) gibt es ein Kette von Untergruppen

$$\{e\} = G_0 \subset G_1 \subset \ldots G_n = G$$

so dass $G_{i-1} \subset G_i$ Normalteiler und G_i/G_{i-1} zyklisch von Ordnung n_i. Ohne Einschränkung enhält K alle n_i-ten Einheitswurzeln. Sei $K^i = L^{G_i}$. Dann ist $\mathrm{Gal}(K^{i-1}/K^i) \cong G_i/G_{i-1}$. Nach dem Hauptsatz der Kummertheorie ist dies eine Erweiterung der Form $K^i(\sqrt[n_i]{a_i})$. □

Auch wenn K nicht alle n-ten Einheitswurzeln enthält, kann die Kummerpaarung ausgenutzt werden.

Korollar 11.12. *Sei L/K endliche Galoiserweiterung mit Galoisgruppe zyklisch der Ordnung p für eine Primzahl $p \neq \mathrm{Char}\, K$. Sei $\omega : \mathrm{Gal}(K(\zeta_p)/K) \to \mathbb{F}_p^*$ definiert durch $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$. Sei $a \in L(\zeta_p)^{*p} \cap K(\zeta_p)^*$. Dann gilt gilt*

$$\sigma(a) = a^{\omega(\sigma)} \mod K(\zeta_p)^{*p}$$

Beweis: Falls $\zeta_p \in K$ ist die Aussage leer. Andernfalls ist ω ein Isomorphismus. Sei $H = \mathrm{Gal}(K(\zeta_p)/K \cong \mathbb{F}_p^*$ und $G = \mathrm{Gal}(L/K)$. Dann gilt $\mathrm{Gal}(L(\zeta_p)/K(\zeta_p) \cong G$ und $\mathrm{Gal}(L(\zeta_p)/K) \cong G \times H$. Die Kummerpaarung

$$L(\zeta_p)^{*p} \cap K(\zeta_p)^*/K(\zeta_p)^{*p} \times G \to \mu_n$$

ist verträglich mit der Operation von H. Da $L(\zeta_p)/K$ abelsch ist, operiert H trivial auf G. Sei also $a \in L(\zeta_p)^{*p} \cap K(\zeta_p)^*/K(\zeta_p)^{*p}$, $g \in G$, $\sigma \in H$. Dann gilt

$$(a^{\omega(\sigma)}, g) = (a, g)^{\omega(\sigma))} = (\sigma(a), g)$$

Da dies für alle g gilt und die Paarung nicht ausgeartet ist, folgt die Behauptung. □

Beweis von Theorem 10.7. (Vergl. Washington, Introduction to Cyclotomic Fields, GTM 83, Lemma 14.8) Wir wollen dies anwenden auf $N/\mathbb{Q}_p$ mit $G = \mathrm{Gal}(N/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^n$. Es gilt dann

$$N(\zeta_p)^{*p} \cap \mathbb{Q}_p(\zeta_p)^*/\mathbb{Q}_p(\zeta_p)^{*p} \cong \mathrm{Hom}(G, \mu_p)$$

Wir untersuchen daher die Einheiten von $\mathbb{Q}_p(\zeta_p)$. Sei $\lambda = 1-\zeta_p$ das Primelement von $\mathbb{Q}_p(\zeta_p)$. Dann lässt sich jede Einheit schreiben als $\lambda^r u$ mit $u \in \mathbb{Z}_p[\zeta_p]^*$. Es gilt $\mathbb{Z}_p[\zeta_p]/(\lambda) \cong \mathbb{Z}_p/(p)$ da die Erweiterung rein verzweigt ist. Für $a \in \mathbb{Z}/p\mathbb{Z}$ sei $[a] \in \mathbb{Z}_p$ die $p-1$-te Einheitswurzel mit Reduktion a (bzw. $[0] = 0$). Dann lässt sich u schreiben als $[a]v$ mit $v = 1 \mod \lambda$. Es gilt also

$$\mathbb{Q}_p(\zeta_p)^* \cong \pi^{\mathbb{Z}} \times \mathbb{F}_p^* \times U_1$$

wobei $U_1 = \{u | u = 1 \mod \lambda\}$ die Gruppe der *Einseinheiten* ist. Es gilt $U_1^p = \{u | u = 1 \mod \lambda^{p+1}\}$ (Henselsches Lemma oder Argument mit p-adischem Logarithmus, Übungsaufgabe), also ist die $\mathbb{F}_p$-Dimension von U_1/U_1^p größer als 1, daher müssen wir die Situation genauer analysieren.
Sei Sei v die Bewertung auf $\mathbb{Q}_p(\zeta_p)$ mit $v(\lambda) = 1$. Dann gilt

$$v(a) = v(\sigma(a)) = \omega(\sigma)v(a) \mod p$$

Für $\sigma \neq e$ ist $\omega(\sigma) \neq 1 \mod p$, also folgt $v(a) = 0 \mod p$. Wir können a modulo $\mathbb{Q}_p(\zeta_p)^{*p}$ abändern, so dass $v(a) = 0$. Die Elemente in $\mathbb{F}_p^*$ sind p-te Potenzen. Wir können also a um eine $p-1$-te Einheitswurzel abändern, so dass $a \in U_1$. Sei $a = 1 + \lambda b$. Wegen $\zeta_p = 1 + \lambda$ gilt $\zeta_p^b = 1 + b\lambda + \dots$, also $a = \zeta_p^b a_1$ mit $a_1 = 1 \mod \lambda^2$. Wieder gilt

$$\sigma(a) = a^{\omega(\sigma)} \mod U_1^p \Rightarrow \sigma(a_1) = a_1^{\omega(\sigma)} \mod U_1^p$$

Für ζ_p ist die Relation erfüllt, also gilt sie auch für a_1. Wir schreiben $a_1 = 1 + c\lambda^d + \dots$ mit $p \nmid c \in \mathbb{Z}$. Wegen $\sigma(\lambda)/\lambda = \omega(\sigma) \mod \lambda$ (nachrechnen) folgt

$$\sigma(a_1) = 1 + c\omega(\sigma)^d \lambda^d + \dots$$

Andererseits folgt aus der Relation

$$\sigma(a_1) = a_1^{\omega(\sigma)} = 1 + c\omega(\sigma)\lambda^d + \dots \mod U_1^p$$

Da $U_1^p = \{x | x = 1 \mod \lambda^{p+1}\}$ (Argument mit p-adischem Logarithmus, siehe Nachtrag) folgt also entweder $d \geq p+1$ oder $d = 1 \mod p-1$, also $d = p$.
Insgesamt haben wir gezeigt, dass $a \in < \zeta_p, 1 + \lambda^p > \subset U_1/U_1^p$. Diese Gruppe hat $\mathbb{F}_p$-Dimension 2, also $n \leq 2$. □

Nachtrag: p-te Potenzen von U_1.
Wie im Beweis betrachten wir den Ganzheitsring $\mathbb{Z}_p[\zeta_p]$ von $\mathbb{Q}_p(\zeta_p)$ mit seinem Primelement $\lambda = 1 - \zeta_p$. Wir setzen

$$U_k = \{x \in \mathbb{Z}_p[\zeta_p] \mid x = 1 \mod \lambda^n\}$$

Für $k = 1$ finden wir die Einseinheiten wieder. Es gilt $\zeta_p = 1 - \lambda \in U_1$.

Behauptung. $U_1 = < \zeta_p > \times U_2$

Das Argument haben wir oben schon benutzt: Für $x = 1 + b\lambda + \dots$ gilt

$$\zeta_p^b x = (1-\lambda)^b(1 + b\lambda + \dots) = (1 - b\lambda + \dots)(1 + b\lambda + \dots) = 1 \mod \lambda^2$$

Behauptung. *Für $k \geq 2$ gilt $U_k \cong \lambda^k \mathbb{Z}_p[\zeta_p]$ als abelsche Gruppen.*

Der Isomorphismus wird durch die Exponentialabbildung $x \mapsto \sum_{i \geq 0} \frac{x^i}{i!}$ gegeben, die Umkehrabbildung durch den Logarithmus $1 + x \mapsto \sum_{i \geq 1} \frac{(-1)^i x^i}{i}$. Zu zeigen ist Konvergenz, vergleiche Washington, Cyclotomic Fields §5.1. Normiert den p-adischen Betrag zu $|p|_p = 1/p$, so konvergiert exp für $|x|_p < p^{-1/(p-1)}$. Es gilt $|\lambda|_p = |p|_p^{1/(p-1)}$, also liegt λ^k für $k \geq 2$ im Konvergenzgebiet. Wegen $|\log(1+x)|_p = |x|_p$ im Konvergenzgebiet (loc. cit. Prop. 5.5.) ergibt sich die behauptete Bijektion.

Behauptung. $U_1^p = U_2^p = U_{p+1}$

Wegen ζ_p^p und der Zerlegung $U_1 =< \zeta_p > \times U_2$ gilt die erste Gleichheit. Auf U_2 gehen wir mit log zur additiven Situation über. Zu zeigen ist dann $p\lambda^2 \mathbb{Z}_p[\zeta_p] = \lambda^{p+1} \mathbb{Z}_p[\zeta_p]$. Dies ist erfüllt wegen $(p) = (\lambda)^{p-1}$ als Ideale von $\mathbb{Z}_p[\zeta_p]$.