ETH ZÜRICH

–

SEMINAR IN ALGEBRAISCHER ZAHLENTHEORIE

–

FRÜHJAHRSSEMESTER 2021

Seminar Leiter: Dr. Raphael Sebastian Steiner, *raphael.steiner@math.ethz.ch*
Hilfsassistent: Lauro Silini, *lauro.silini@math.ethz.ch*

Inhaltsverzeichnis

1. Gauss'sche Zahlen $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$

Jöran Schlömer, *joerans@student.ethz.ch*

Auf den folgenden Seiten untersuchen wir die grundlegenden Eigenschaften der gauss'schen Zahlen $\mathbb{Z}[i]$, sowie des Ringes $\mathbb{Z}\left[\sqrt{3}\right]$. Insbesondere werden wir zeigen, dass beide Ringe euklidisch sind, ihre Einheiten bestimmen sowie in beiden Fällen die Primelemente bis auf Assoziiertheit bestimmen.

1.1. **Definitionen.** Wir beginnen mit den notwendigen Definitionen, die wir im weiteren Verlauf benötigen. Zuerst gilt es unsere beiden Ringe zu definieren.

Definition 1.1. *Wir bezeichnen mit $\mathbb{Z}[i]$ die Menge*

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

Für $(a + bi), (c + di) \in \mathbb{Z}[i]$ definieren wir die Operationen

$$(a + bi) + (c + di) = (a + c) + (c + d)i,$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Mit diesen Operationen ist $\mathbb{Z}[i]$ ein Ring, welchen wir Gauss'sche Zahlen nennen. Für ein Element $x = (a + bi)$ definieren wir das konjugierte Element $\bar{x} = (a - bi)$.

Analog dazu definieren wir auch den zweiten Ring, den wir untersuchen werden:

Definition 1.2. *Wir bezeichnen mit $\mathbb{Z}\left[\sqrt{3}\right]$ die Menge*

$$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}.$$

Für $(a + b\sqrt{3}), (c + d\sqrt{3}) \in \mathbb{Z}\left[\sqrt{3}\right]$ definieren wir die Operationen

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (c + d)\sqrt{3},$$
$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

Mit diesen Operationen ist auch $\mathbb{Z}\left[\sqrt{3}\right]$ ein Ring. Für ein Element $x = (a + b\sqrt{3})$ definieren wir das konjugierte Element $\bar{x} = (a - b\sqrt{3})$.

Wir benötigen für unsere weiteren Untersuchungen einige Begrifflichkeiten aus der Teilbarkeitstheorie, welche wir nun kurz wiederholen. Dabei folgen wir den Definition in A. Schmidts Buch über algebraische Zahlentheorie [5]. Im Folgenden sind alle Ringe kommutativ mit 1-Element.

Definition 1.3. *In einem Ring R nennen wir zwei Elemente $a, b \in R$ assoziiert, wenn die beiden Elemente sich gegenseitig teilen, in Symbolen ausgedrückt $a \mid b$ und $b \mid a$. Für assoziierte Elemente schreiben wir $a \sim b$.*

Für uns von besonderem Interesse in Ringen sind irreduzible Elemente und Primelemente.

Definition 1.4. *In einem Ring R wird ein Element $\pi \in R$ irreduzibel genannt, wenn es von Null verschieden sowie keine Einheit ist und gilt*

$$\pi = ab \implies a \text{ oder } b \text{ ist eine Einheit.}$$

Ein Element $\pi \in R$ ist ein Primelement, wenn es von Null verschieden ist und keine Einheit ist, sowie gilt

$$\pi \mid ab \implies \pi \mid a \text{ oder } \pi \mid b.$$

Definition 1.5. *Ein Ring heisst Integritätsring, wenn*

$$ab = 0 \implies a = 0 \text{ oder } b = 0.$$

Lemma 1.6. *In einem Integritätsring R gilt $a \sim b$ genau dann wenn eine Einheit $u \in R$ existiert, so dass $a = bu$.*

Beweis. Wenn $a = bu$ für eine Einheit $u \in R$, dann gilt auch $b = au'$ für eine Einheit u'. Es folgt, dass $a \mid b$ und $b \mid a$. Für die Gegenrichtung gilt, wenn $a = 0$, so gilt auch $b = 0$. Wenn $a \neq 0$, so folgt nach Annahme, dass es $u, u' \in R$ gibt, so dass $a = bu$ und $b = au'$. Es folgt $a = auu'$, weshalb also $a(1 - uu') = 0$ folgt. In einem Integritätsring folgt dann aber wegen $a \neq 0$, dass $(1 - uu') = 0$, so dass u und u' Einheiten sind. Die Behauptung folgt. □

Darüber hinaus werden uns zwei Typen von Ringen besonders interessieren. Auf der einen Seite sind das die sogenannten faktoriellen Ringe.

Definition 1.7. *Ein Integritätsring R heißt faktoriell wenn jede von Null verschiedene Nicht-Einheit $a \in R$ eine bis auf Einheiten und Reihenfolge eindeutige Zerlegung als Produkt irreduzibeler Elemente hat.*

Darüber hinaus möchten wir zeigen, dass $\mathbb{Z}[i]$ und $\mathbb{Z}\left[\sqrt{3}\right]$ sogenannte euklidische Ringe sind.

Definition 1.8. *Ein Integritätsring R heißt euklidisch, wenn es eine Abbildung $N : R\backslash\{0\} \to \mathbb{N}$ gibt, so dass es für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren, die*

$$a = qb + r \text{ und } N(r) < N(b) \text{ oder } r = 0$$

erfüllen. Wir nennen eine solche Abbildung (euklidische) Normfunktion.

Euklidische Ringe sind von Bedeutung, da es in ihnen möglich ist eine verallgemeinerte Version der euklidischen Division zu definieren mit Hilfe derer beispielsweise die Bestimmung eines größten gemeinsamen Teilers für beliebige Element des Ringes möglich ist.

Bemerkung 1.9. Auf einem Ring kann es mehrere euklidische Normfunktionen geben.

Nachdem wir nun alle notwendigen Definitionen gegeben haben, zeigen wir zunächst einige Eigenschaften euklidischer Ringe, bevor wir uns den Ringen $\mathbb{Z}[i]$ und $\mathbb{Z}\left[\sqrt{3}\right]$ zuwenden.

1.2. **Euklidische Ringe.** In diesem Abschnitt beweisen wir einige Eigenschaften euklidischer Ringe, die im weiteren Verlauf nützlich sein werden. Wir orientieren uns weiterhin stark an [5].

Proposition 1.10. *Für einen euklidischen Ring R gibt es eine euklidische Normfunktion N mit*

$$N(a) \leqslant N(ab) \tag{1}$$

für alle von Null verschiedenen Elemente $a, b \in R$.

Beweis. Sei N' eine beliebige euklidische Normfunktion auf R. Wir definieren nun eine weitere Abbildung

$$N : R\backslash\{0\} \to N, a \mapsto \min_{a' \sim a'} N'(a').$$

Um zu sehen, dass es sich bei N um eine euklidische Normfunktion handelt, wählen wir $a, b \in R$ mit $b \neq 0$. Sei nun b' das zu b assozierte Element in R welches $N(b) = N'(b')$ erfüllt. Da R euklidisch ist können wir $q, r \in R$ wählen, so dass $a = qb' + r$ und $r = 0$ oder $N(r') < N(b')$ gilt. Wir können $b' = be$ für eine Einheit $e \in R$ schreiben und erhalten $a = qeb + r$ mit $r = 0$ oder $N(r) \leqslant N'(r) \leqslant N'(b') = N(b)$ wegen der Minimalität von b', weshalb N eine euklidische Normfunktion ist. Wir zeigen, per Widerspruch, dass die euklidische Normfunktion N die gewünschte Eigenschaft erfüllt. Sei $a \in R$ ein beliebiges von Null verschiedenes Element und sei $b \in R$ ein weiteres von Null verschiedenes Element, für welches $N(ab)$ minimal ist. Angenommen es wäre $N(a) > N(ab)$. Per Definition nimmt N auf assozierten Elementen den selben Wert an, weshalb b keine Einheit sein kann. Da R euklidisch ist existieren $q, r \in R$ so dass $a = q(ab) - r$ und entweder $r = 0$ oder $N(r) < N(ab)$. Da aber b keine Einheit ist folgt mit $a \neq 0$ aus $a(1 - qb) = r$, dass $r \neq 0$ gilt. Dann ist $N(r) = N(a(1 - qb)) < N(ab)$, was der Minimalität von b widerspricht. Also erfüllt N die gewünschte Eigenschaft. □

Bemerkung 1.11. Sei N eine euklidische Normfunktion wie in Prop 1.10. Dann folgt aus $a \mid b$, dass $N(a) \leqslant N(b)$.

Die im weiteren Verlauf wichtigste Eigenschaft zeigt das folgende Lemma:

Lemma 1.12. *Euklidische Ringe sind faktoriell.*

Beweis. Sei R ein euklidischer Ring mit Normfunktion N. Wir zeigen, dass R ein Hauptidealring ist. Sei I ein Ideal in R. Wenn $I = 0$, dann gilt $I = (0)$. Wenn $I \neq 0$, dann wähle ein von nullverschiedenes Element $a \in I$ so dass für alle $b \in I$ gilt $N(a) \leqslant N(b)$. Da R ein euklidischer Ring ist, existieren zu einem beliebigen $b \in I$ $q, r \in R$ so dass $a = qb + r$, wobei $N(r) < N(a)$ gilt. Da aber I ein Ideal ist, also $r = a - qb \in I$, und da a minimal gewählt wurde, folgt $r = 0$. Also gilt $a = bq$ und deshalb $I = (a)$. Die Behauptung folgt nun, da Hauptidealringe faktorielle Ringe sind. □

Ein grundlegender Fakt aus der Algebra ist das folgende Lemma, welches wir ohne Beweis angeben:

Lemma 1.13. *In einem faktoriellen Ring sind ist jedes irreduzibeles Element ein Primelement.*

Da wir die Einheiten der beiden Ringe $\mathbb{Z}[i]$ und $\mathbb{Z}\left[\sqrt{3}\right]$ bestimmen möchten, beweisen wir als letztes Lemma in diesem Abschnitt, den folgenden Fakt:

Proposition 1.14. *Sei R ein nicht-leerer euklidischer Ring. Für eine euklidische Normfunktion welche die Ungleichung (1) erfüllt ist ein Element $e \in R$ eine Einheit dann und nur dann, wenn $N(e) = N(1)$ gilt.*

Beweis. Sei $e \in R$ eine Einheit. Dann existiert ein $a \in R$ so dass $ea = 1$. Sei N eine Normfunktion wie in Proposition 1.10. Es gilt $e \mid 1$, woraus folgt, dass $N(e) \leqslant N(1)$. Gleichzeitig gilt aber offensichtlich $1 \mid a$ für jedes $a \in R$, weshalb $N(u) = N(1)$ folgt.
Sei nun $e \in R$ so dass $N(e) = N(1)$. Da unser Ring euklidisch ist existieren $q, r \in R$ mit $1 = qe + r$ wobei entweder $r = 0$ oder $N(r) < N(e)$. Angenommen $r \neq 0$, dann folgt mit $N(r) < N(u) = N(1)$ ein Widerspruch, da $N(1)$ wie oben beschrieben immer minimal ist. Also gilt $qe = 1$ und es folgt, dass e eine Einheit ist. □

1.3. **Die Ringe $\mathbb{Z}[i]$ und $\mathbb{Z}\left[\sqrt{3}\right]$.** In diesem Abschnitt befassen wir uns mit den Eigenschaften von $\mathbb{Z}[i]$ und $\mathbb{Z}\left[\sqrt{3}\right]$. Wir beginnen damit zu zeigen, dass es sich bei beiden Ringen tatsächlich um euklidische Ringe handelt. Zuerst befassen wir uns mit den Gauss'schen Zahlen.

Proposition 1.15. *Die Abbildung $N : \mathbb{Z}[i]\backslash\{0\} \to \mathbb{N}$ definiert durch*

$$(a + bi) \mapsto a^2 + b^2$$

ist eine euklidische Normfunktion für $\mathbb{Z}[i]$. Insbesondere macht N $\mathbb{Z}[i]$ zu einem euklidischer Ring.

Bemerkung 1.16. Die Normfunktion N ist die Restriktion des Quadrats des komplexen Absolutbetrags auf die Teilmenge $\mathbb{Z}[i] \subset \mathbb{C}$. Es gilt also $N(a) = a\bar{a}$.

Bevor wir Proposition 1.15 beweisen zeigen wir

Lemma 1.17. *Die Abbildung N aus Proposition 1.15 ist multiplikativ, das heisst für alle $a, b \in R$ gilt*

$$N(ab) = N(a)N(b).$$

Beweis. Seien $a = a_1 + a_2 i$ und $b = b_1 + b_2 i$ zwei Elemente in $\mathbb{Z}[i]$. Dann gilt

$$\begin{aligned} N(ab) &= (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2 \\ &= (a_1b_1)^2 - 2a_1b_1a_2b_2 + (a_2b_2)^2 + (a_1b_2)^2 + 2a_1b_1a_2b_2 + (a_2b_1)^2 \\ &= (a_1b_1)^2 + (a_1b_2)^2 + (a_2b_1)^2 + (a_2b_2)^2 \\ &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) \\ &= N(a)N(b) \end{aligned}$$

□

Nun widmen wir uns dem Beweis von Proposition 1.15.

Beweis. Es ist offensichtlich, dass die Abbildung N wohldefiniert ist. Seien nun $a, b \in \mathbb{Z}[i]$, wobei $b \neq 0$. Wir müssen nun die Existenz von zwei Gauss'schen Zahlen $q, r \in \mathbb{Z}[i]$ zeigen, die $a = qb + r$ sowie $r = 0$ oder $N(r) < N(b)$ erfüllen. Die Zahl $\frac{a}{b}$ ist eine komplexe Zahl. Geometrisch bilden die Gauss'schen Zahlen ein Gitter in der komplexen Ebene (siehe Fig. 1), dessen Kanten zwischen Knoten immer Länge 1 haben. Da $\frac{a}{b}$ innerhalb einer Masche dieses Gitters liegen muss, hat $\frac{a}{b}$ zum

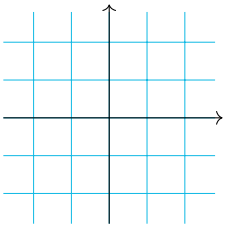


ABBILDUNG 1. Visualisierung von $\mathbb{Z}[i]$ als Gitter in der komplexen Ebene. Die Elemente von $\mathbb{Z}[i]$ entsprechen den Knotenpunkten

nächsten Gitterpunkt einen Abstand der kleiner gleich $\frac{\sqrt{2}}{2}$ ist. Deshalb existiert ein $q \in \mathbb{Z}[i]$, so dass $|a/b - q| < 1$. Wir setzen nun $r = a - bq \in \mathbb{Z}[i]$ und beobachten, dass

$$N(r) = N(a - bq) = |b(\frac{a}{b} - q)|^2 = |b|^2|\frac{a}{b} - q|^2 < |b|^2 = N(b),$$

wie gewünscht. Die Behauptung folgt. □

Wir bestimmen nun als nächstes die Einheiten in $\mathbb{Z}[i]$.

Lemma 1.18. *Die Einheiten in $\mathbb{Z}[i]$ sind die Elemente $\{1, -1, i, -i\}$.*

Beweis. Durch Proposition 1.14 wissen wir, dass eine Einheit $e \in \mathbb{Z}[i]$ $N(e) = N(1)$ erfüllen muss. Da gilt $N(1) = 1^2 = 1$ folgt, dass die Einheiten genau jene Elemente sind die $N(e) = 1$ erfüllen. Schreiben wir $e = a + bi$ so folgt mit $N(a + bi) = a^2 + b^2$ die Behauptung. □

Bemerkung 1.19. Wir halten fest, dass eine Einheit in $\mathbb{Z}[i]$ unter N auf 1 abgebildet wird.

Bevor wir mit der Bestimmung der Primelemente beginnen, widmen wir uns zwischenzeitlich dem Ring $\mathbb{Z}\ [\sqrt{3}]$. Wie für $\mathbb{Z}[i]$ beginnen wir damit zu zeigen, dass es sich bei $\mathbb{Z}\ [\sqrt{3}]$ ebenfalls um einen euklidischen Ring handelt.

Proposition 1.20. *Die Abbildung $N_{\sqrt{3}} : \mathbb{Q}[\sqrt{3}]\backslash\{0\} \to \mathbb{Q}_{>0}$ definiert durch*

$$(a + b\sqrt{3}) \mapsto |a^2 - 3b^2|$$

eingeschränkt auf $\mathbb{Z}[\sqrt{3}]$ ist eine euklidische Normfunktion auf $\mathbb{Z}[\sqrt{3}]$.

Der Beweis ist analog zu dem Beweis von Proposition 1.15, wobei wir dem Beweis aus [5] folgen. Wieder zeigen wir zuerst

Lemma 1.21. *Die Abbildung $N_{\sqrt{3}}$ ist multiplikativ.*

Beweis. Seien $a = a_1 + a_2\sqrt{3}$ und $b = b_1 + b_2\sqrt{3}$ Elemente von $\mathbb{Q}[\sqrt{3}]$. Dann gilt:

$$\begin{aligned}
N_{\sqrt{3}}(ab) &= N_{\sqrt{3}}((a_1 + a_2\sqrt{3}])(b_1 + b_2\sqrt{3})) \\
&= N_{\sqrt{3}}((a_1b_1 + 3a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{3}) \\
&= |(a_1b_1 + 3a_2b_2)^2 - 3(a_1b_2 + a_2b_1)^2| \\
&= |(a_1b_1)^2 + (3a_2b_2)^2 - 3((a_1b_2)^2 - (a_2b_1)^2)| \\
&= |a_1^2 - 3a_2^2||b_1^2 - 3b_2^2| \\
&= N_{\sqrt{3}}((a_1 + a_2\sqrt{3}]))N_{\sqrt{3}}((b_1 + b_2\sqrt{3})) \\
&= N_{\sqrt{3}}(a)N_{\sqrt{3}}(b)
\end{aligned}$$

□

Nun beweisen wir Proposition 1.20

Beweis. Die Wohldefiniertheit der Abbildung ist klar. Wir bemerken, dass für rationale $p, q \in \mathbb{Q}$ mit $|p| \leqslant \frac{1}{2}$ und $|q| \leqslant \frac{1}{2}$ gilt

$$|p^2 - 3q^2| \leqslant \frac{3}{4} < 1.$$

Seien nun $x = u + v\sqrt{3}$ sowie $y = u' + v'\sqrt{3}$ für $u, v, u', v' \in \mathbb{Q}$, dann haben $x + y, xy$ und x/y die selbe Form. Seien nun $a, b \in \mathbb{Z}[\sqrt{3}]$ mit $b \neq 0$, dann ist $\frac{a}{b} = u + v\sqrt{3}$ für $u, v \in \mathbb{Q}$. Wir wählen nun ganze Zahlen $m, n \in \mathbb{Z}$ so dass $|u - m| \leqslant \frac{1}{2}$ und $|v - n| \leqslant \frac{1}{2}$. Mit $q = m + n\sqrt{3}$ gilt dann

$$N_{\sqrt{3}}(\frac{a}{b} - q) = |(u - m)^2 - 3(v - n)^2| < 1.$$

Deshalb ist für $r = a - bq \in \mathbb{Z}[\sqrt{3}]$

$$N_{\sqrt{3}}(r) = N_{\sqrt{3}}(a - bq) = N_{\sqrt{3}}(b)N_{\sqrt{3}}(\frac{a}{b} - q) < N_{\sqrt{3}}(b),$$

und die Behauptung folgt. □

Wir können nun auch die Einheiten in $\mathbb{Z}\ [\sqrt{3}]$ bestimmen.

Bemerkung 1.22. Es gilt $N_{\sqrt{3}}(1) = 1$. Desweiteren ist $N_{\sqrt{3}}(a) = |a\bar{a}|$.

Es gilt das

Lemma 1.23. *Die Einheiten in* $\mathbb{Z}\ [\sqrt{3}]$ *sind alle Zahlen* $a + b\sqrt{3}$*, welche* $a^2 - 3b^2 = \pm 1$ *erfüllen.*

Beweis. Sei $x = a + b\sqrt{3}$ mit $a^2 - 3b^2 = \pm 1$. Dann gilt offensichtlich $N_{\sqrt{3}}(x) = 1$, woraus mit Bemerkung 1.22 und Proposition 1.14 folgt, dass x eine Einheit ist. Sei umgekehrt $x = a + b\sqrt{3}$ eine Einheit, dann gilt wieder wegen Bemerkung 1.22 und Proposition 1.14 $N_{\sqrt{3}}(x) = 1$ weshalb $a + b\sqrt{3} = \pm 1$ sein muss. Die Behauptung folgt. □

1.4. **Primelemente in $\mathbb{Z}[i]$ und $\mathbb{Z}\ [\sqrt{3}]$.** In diesem Abschnitt bestimmen wir nun die Primelemente in $\mathbb{Z}[i]$ und $\mathbb{Z}\ [\sqrt{3}]$ bis auf Assoziiertheit.

Bemerkung 1.24. Wenn wir im folgenden von Primzahlen in $\mathbb{Z}$ sprechen, so meinen wir die Primelemente von $\mathbb{Z}$, weshalb auch Zahlen mit negativem Vorzeichen Primzahlen sind.

Um uns zu vergewissern, dass diese Klassifizierung nicht trivial ist, betrachten wir die folgenden zwei Beispiele

Beispiel 1.25. *In* $\mathbb{Z}[i]$ *können wir die Primzahl* $2 \in \mathbb{Z}$ *schreiben als* $(1 - i)(1 + i)$*. Deshalb ist* 2 *kein Primelement in* $\mathbb{Z}[i]$ *.*

Ähnlich finden wir auch in $\mathbb{Z}[\sqrt{3}]$, dass nicht alle Primzahlen aus $\mathbb{Z}$ zu Primelementen in $\mathbb{Z}\ [\sqrt{3}]$ werden.

Beispiel 1.26. *Wir können die Primzahl 13 in* $\mathbb{Z}\ [\sqrt{3}]$ *als* $(4 + \sqrt{3})(4 - \sqrt{3})$ *zerlegen.*

Bevor wir uns der Klassifizierung der Primelemente widmen, beweisen wir zwei nützliche Hilfslemmas. Wir beginnen mit dem

Lemma 1.27. *Ist* $\pi \in \mathbb{Z}[i]$ *(resp.* $\mathbb{Z}\ [\sqrt{3}]$ *) ein Element mit* $N(\pi) = p$ *(resp.* $N_{\sqrt{3}}(\pi) = p$*) für eine Primzahl* $p \in \mathbb{Z}$*, so ist* π *ein Primelement in* $\mathbb{Z}[i]$ *(resp.* $\mathbb{Z}\ [\sqrt{3}]$ *).*

Beweis. Der Beweis verwendet nur die Multiplikativität der jeweiligen euklidischen Norm, sowie Proposition 1.14 zusammen mit Bemerkung 1.19 bzw. Bemerkung 1.22. Deswegen können wir o.B.d.A. nur den Fall $\mathbb{Z}[i]$ betrachten. Sei π wie in der Annahme. Angenommen $\pi = ab$ für $a, b \in \mathbb{Z}[i]$, so folgt aus der Multiplikativität von N

$$p = N(\pi) = N(ab) = N(a)N(b),$$

weshalb mit p prim folgt, dass entweder $N(a) = 1$ oder $N(b) = 1$ gilt, so dass eines der Elemente eine Einheit sein muss. Es folgt, dass π ein irreduzibeles Element ist. Mit Lemma 1.13 folgt, dass π ein Primelement ist. □

Desweiteren gilt auch das folgende

Lemma 1.28. *Ist* $\pi \in \mathbb{Z}[i]$ *ein Primelement, so folgt* $N(\pi) \in \{p, p^2\}$ *für eine Primzahl* $p \in \mathbb{N}$.

Beweis. Sei $\pi \in \mathbb{Z}[i]$ ein Primelement. Dann folgt mit $N(\pi) = \pi\bar{\pi}$, dass $\pi \mid N(\pi) \in \mathbb{N}$ teilt. Wir können eine Primzerlegung für $N(\pi)$ finden und schreiben $N(\pi) = p_1 \dots p_n$ für Primzahlen $p_i \in \mathbb{N}$. Da π ein Primelement ist teilt π eine der Primzahlen, sagen wir p_k. Dann gilt $p_k = \pi b$ für ein $b \in \mathbb{Z}[i]$. Mit der Multiplikativität der Normfunktion folgt

$$p^2 = N(p_k) = N(\pi b) = N(\pi)N(b),$$

weshalb $N(\pi) = p$ oder $N(\pi) = p^2$ gelten muss. □

Gleichermassen gilt

Lemma 1.29. *Ist $\pi \in \mathbb{Z}[\sqrt{3}]$ ein Primelement, so folgt $N_{\sqrt{3}}(\pi) \in \{p, p^2\}$ für eine Primzahl $p \in \mathbb{N}$.*

Der Beweis ist sehr ähnlich zu dem Beweis von Lemma 1.28.

Beweis. Sei $\pi \in \mathbb{Z}[\sqrt{3}]$ ein Primelement. Aus $N_{\sqrt{3}}(\pi) = |\pi\bar{\pi}|$ folgt mit $N_{\sqrt{3}}(\pi) = p_1 \dots p_n$ und dem Wissen, dass π ein Primelement ist, dass $\pi \mid p_k$ für ein p_k aus obigem Produkt. Mit $p_k = \pi b$ folgt mittels Multiplikativität

$$p^2 = N_{\sqrt{3}}(p_k) = N_{\sqrt{3}}(\pi b) = N_{\sqrt{3}}(\pi)N_{\sqrt{3}}(b),$$

weshalb $N_{\sqrt{3}}(\pi) = p$ oder $N_{\sqrt{3}}(a) = p^2$, wie gewünscht. □

Bemerkung 1.30. Ist π ein Primelement in $\mathbb{Z}[i]$ oder $\mathbb{Z}\left[\sqrt{3}\right]$, dann folgt aus den obigen Lemmas für den Fall, dass $N(\pi) = p^2$ bzw. $N_{\sqrt{3}}(\pi) = p^2$ mit Lemma 1.6, dass π assoziiert zu p ist. Ausserdem gilt, dass $\pi \mid p$.

Abschliessend bestimmen wir nun die Primelemente von $\mathbb{Z}[i]$ und $\mathbb{Z}\left[\sqrt{3}\right]$ bis auf Assoziiertheit. Wir beginnen mit $\mathbb{Z}[i]$ und beweisen hierfür noch ein weiteres Hilfslemma:

Wir reporduzieren dabei die Argumentation in Neukirchs *Algebraische Zahlentheorie* [4]:

Proposition 1.31. *Für Primzahlen $p \neq 2$ gilt*

$$p = a^2 + b^2 \ (a, b \in \mathbb{Z}) \iff p \equiv 1 \ \textit{mod}\ 4.$$

Beweis. Angenommen p ist eine ungerade Primzahl der Form $p = a^2 + b^2$ $(a, b \in \mathbb{Z})$. Dann folgt $p \equiv 1 \bmod 4$, da für Quadratzahlen gilt, dass sie

$$a^2 \equiv 1 \bmod 4 \text{ oder } a^2 \equiv 0 \bmod 4$$

erfüllen und weil p ungerade ist. Für die andere Richtung genügt es zu zeigen, dass eine Primzahl mit $p \equiv 1 \bmod 4$ kein Primelement in $\mathbb{Z}[i]$ ist. In diesem Fall gibt es eine Zerlegung $p = ab$ in zwei Nicht-Einheiten $a, b \in \mathbb{Z}[i]$. Mit Lemma 1.17 können erhalten wir, dass

$$p^2 = N(p) = N(ab) = N(a)N(b)$$

gilt, woraus mit Bemerkung 1.19 $N(a) = N(b) = p$ folgt. Also gilt dann mit $a = a_1 + a_2 i$, dass $a_1^2 + a_2^2 = p$, wie gewünscht. Um zu sehen, dass eine Primzahl wie in der Annahmen kein Primelement in $\mathbb{Z}[i]$ bleibt verwenden wir, dass nach dem Satz von Wilson für Primzahlen p gilt

$$(p-1)! \equiv_p -1 \bmod p.$$

Sei nun $p = 4k + 1$, so gilt mit

$$\begin{aligned} -1 \equiv_p (p-1)! &= (1 \dots 2k)(p-1 \dots p-2k) \\ &\equiv_p (2k)!((-1)^{2k}2k)! \\ &= ((2k)!)^2, \end{aligned}$$

dass für $x = (2k)!$ gilt $p \mid x^2 + 1 = (x+i)(x-i)$. Es gilt aber offensichtlich $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, so dass p keinen der Faktoren teilt und deshalb kein Primelement in $\mathbb{Z}[i]$ ist. □

Wir beweisen nun

Theorem 1.32. *Die Primzahlen in $\mathbb{Z}[i]$ bis auf Assoziiertheit sind:*

- $1 + i$
- $a + bi$ *wobei* $a^2 + b^2 = p \in \mathbb{Z}\backslash\{2\}$ *eine Primzahl* $\equiv 1 \bmod 4$ *ist*
- p, *wobei* $p \equiv 3 \bmod 4$ *eine Primzahl in* $\mathbb{Z}$ *ist.*

Auch in diesem Fall folgen wir der Argumentation in [4].

Beweis. Mit Hilfe von Lemma 1.27 ist es in den ersten zwei Fällen klar, dass es sich bei den Elemente um Primelemente handelt. Sei nun $p \in \mathbb{Z}[i]$ mit $p \equiv 3 \bmod 4$. Wenn p kein Primelement ist, dann ist es wegen Lemma 1.13 auch nicht irreduzibel und wir können $p = ab$ für Nicht-Einheiten $a, b \in \mathbb{Z}[i]$ schreiben. In diesem Fall folgt mit $p^2 = N(p) = N(a)N(b)$, dass $N(a) = p$ gilt, weshalb mit $a = a_1 + a_2 i$ der Widerspruch $p = a_1^2 + a_2^2 \iff p \cong 1 \bmod 4$ ensteht. Nun bleibt nur zu zeigen, dass alle Primelemente assoziiert zu einem dieser drei Elemente ist. Sei π ein beliebiges Primelement in $\mathbb{Z}[i]$. Wegen Lemma 1.28 gilt dann $N(\pi) \in \{p, p^2\}$, wobei $p \in \mathbb{N}$ eine Primzahl ist. Angenommen es gilt $N(\pi) = p$. Schreiben wir $\pi = a + bi$, so folgt $a^2 + b^2 = p$. Im Fall $p = 2$ müssen dann sowohl a als auch b Absolutbetrag 1 haben, weshalb nur vier Elemente in Frage kommen. Durch Betrachtung der Einheiten sehen wir sofort, dass alle diese vier Elemente zu $1 + i$ assoziiert sind. Für $p \neq 2$ folgt wegen Proposition 1.31 in diesem Fall $p \cong 1 \bmod 4$, so dass π einem Primelement aus unserer obigen Liste entspricht. Ist dagegen $N(\pi) = p^2$, so folgt mit Bemerkung 1.30, dass π assoziiert zu p ist. Desweiteren gilt $p \cong 3 \bmod 4$, da sonst entweder $p = 2$, woraus dann $2 = (1 + i)(1 - i)$ folgt, oder aber es ist $p \cong 1 \bmod 4$ womit dann nach Proposition 1.31 $a^2 + b^2 = p$ gelten muss und somit $p = (a + bi)(a - bi)$ wäre. In beiden Fällen teilt p kein Element auf der rechten Seite, woraus folgt, dass p kein Primelement ist. Da Assoziierte von Primelementen auch Primelemente sind, impliziert dies, dass auch π kein Primelement ist. Ein Widerspruch zur Annahme. Das Theorem folgt. □

Als letztes Theorem klassifizieren wir nun die Primelemente von $\mathbb{Z}\left[\sqrt{3}\right]$ bis auf Assoziiertheit.

Theorem 1.33. *Die Primzahlen in* $\mathbb{Z}\left[\sqrt{3}\right]$ *sind bis auf Assoziiertheit:*

- $-1 + \sqrt{3}$
- $\sqrt{3}$
- $a + b\sqrt{3}$ *wobei* $a^2 - 3b^2 = \pm p \in \mathbb{Z}\backslash\{2, 3\}$ *eine Primzahl ist sodass* 3 *ein Quadrat in* $\mathbb{Z}/p\mathbb{Z}$ *ist* ($\iff p \cong \pm 1 \bmod 12$)
- p*, wobei* p *eine Primzahl ist sodass* 3 *kein Quadrat in* $\mathbb{Z}/p\mathbb{Z}$ *ist* ($\iff p \cong \pm 5 \bmod 12$)

Im Beweis von Theorem 1.33 werden wir das folgende Lemma verwenden.

Lemma 1.34. *Für eine Primzahl* $p \in Z$ *gilt* $\pm p = a^2 - 3b^2 \implies 3$ *ist ein Quadrat in* $\mathbb{Z}/p\mathbb{Z}$.

Beweis. Sei p prim mit $\pm p = a^2 - 3b^2$. Angenommen $b \equiv_p 0 \bmod p$, dann folgt auch $a \equiv_p 0 \bmod p$, was aber wegen $\pm p = a^2 - 3b^2$ nicht eintreten kann. Es ist also $b \not\equiv_p 0 \bmod p$. Dann gilt

$$\begin{aligned} & a^2 - 3b^2 && = \pm p \\ \iff & a^2 - 3b^2 && \equiv_p 0 \\ \iff & a^2 && \equiv_p 3b^2 \\ \iff & a^2(b^{-1})^2 && \equiv_p 3 \\ \iff & (ab^{-1})^2 && \equiv_p 3 \end{aligned}$$

und die Behauptung folgt. □

Bemerkung 1.35. Allgemein gilt für eine Primzahl p, wenn $a^2 - 3b^2 \equiv_p 0$, dass entweder $a \equiv_p b \equiv_p 0$ oder 3 ist ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$.

Der Beweis ist ähnlich zu dem Beweis von Theorem 1.32.

Beweis. Mit Hilfe von Lemma 1.27 ist es auch hier klar, dass es sich bei den ersten drei Elementen der Liste jeweils um Primzahlen handelt. Sei nun $p \in \mathbb{Z}$ ein Primelement, sodass 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist. Angenommen p ist kein Primelement in $\mathbb{Z}[\sqrt{(3)}]$, dann können wir für zwei Nicht-Einheiten $a, b \in \mathbb{Z}[\sqrt{3}]$ schreiben $p = ab$. Mit $p^2 = N_{\sqrt{3}}(p) = N_{\sqrt{3}}(ab) = N_{\sqrt{3}}(a)N_{\sqrt{3}}(b)$ folgt dann $N(a) = p$, weshalb nach Lemma 1.34 3 ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist, ein Widerspruch.

Nachdem wir nun gezeigt haben, dass die vier Elemente prim sind, sei $\pi \in \mathbb{Z}[\sqrt{3}]$ ein beliebiges Primelement. Nach Lemma 1.29 gilt dann $N_{\sqrt{3}}(\pi) \in \{p, p^2\}$. Im Fall $N_{\sqrt{3}}(\pi) = p$ unterscheiden wir zwischen den Fällen $p = 2$, $p = 3$, sowie $p \in \mathbb{Z}\backslash\{2, 3\}$. Angenommen $p = 2$. Wir können schreiben $2 = (2 + \sqrt{3})(-1 + \sqrt{3})^2$. Mit Bemerkung 1.30 folgt $\pi \mid 2$ weshalb $\pi\beta = 2$. Mit der Eindeutigkeit

der Primfaktorisierung folgt nun $\pi \sim (-1+\sqrt{3})$. Ähnlich verfahren wir für $p=3$. In diesem Fall faktorisieren wir $3=\sqrt{3}^2$ und argumentieren wie oben. Also $\pi \mid 3$, weshalb aus $\pi\beta = 3 = \sqrt{3}^2$ wegen der Eindeutigkeit der Primzerlegung Assoziiertheit folgt. Sei nun $N(\pi)=p \in \mathbb{Z}\backslash\{2,3\}$. Dann gilt $a^2-3b^2=\pm p$ und mit Lemma 1.34 folgt ausserdem, dass 3 ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist. Sei nun $N_{\sqrt{3}}(\pi)=p^2$. Mit Bemerkung 1.30 folgt direkt dass $\pi \sim p$. Es verbleibt zu zeigen, dass 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist. Wir nehmen dafür an, dass $3 \equiv c^2 \bmod p$ gilt und führen dies zu einem Widerspruch. Wir haben $N_{\sqrt{3}}(c+\sqrt{3}) = \pm c^2 - 3 \equiv 0 \bmod p$. Wir können nun o.B.d.A $c \in [-\frac{p-1}{2}, \frac{p-1}{2}]$ wählen. In diesem Fall erhalten wir $p^2 \nmid c^2-3$ während aber gleichzeitig per Annahme gilt, dass $p \mid (c+\sqrt{3})(c-\sqrt{3}) = c^2-3$. Da p prim ist, gilt $p \mid (c+\sqrt{3})$ oder $p \mid (c-\sqrt{3})$. Deshalb folgt $ggT(p, c+\sqrt{3}) \neq \pm 1$ oder $ggT(p, c-\sqrt{3}) \neq \pm 1$. Sei β einer der ggT ungleich ± 1. Unter Verwendung der Multiplikativität der Normfunktion folgt $N_{\sqrt{3}}(\beta) \mid N_{\sqrt{3}}(p) = p^2$ und $N_{\sqrt{3}}(\beta) \mid c^2-3 = (c+\sqrt{3})(c-\sqrt{3})$. Es folgt $N_{\sqrt{3}}(\beta) \in \{p, p^2\}$. Da wir aber bereits wissen, dass $p^2 \nmid c^2-3$ muss $N_{\sqrt{3}}(\beta)=p$ gelten. Deshalb ist β nach Lemma 1.27 ein Primelement und es gilt

$$\pi\bar{\pi} = \pm p^2 = \beta\beta\bar{\beta}\bar{\beta}.$$

Weil β prim ist, ist dies ein Widerspruch zur Eindeutigkeit der Primzerlegung im euklidischen Ring $\mathbb{Z}[\sqrt{3}]$, weshalb 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ sein kann.

Das Theorem folgt.

□

Wir haben nun sowohl die Einheiten, als auch die Primelemente bis auf Assoziiertheit in den beiden euklidischen Ringen $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$ bestimmt.

2. Legendresymbol & Lucas-Lehmer-Test

Gabriel Dettling, *gabriede@student.ethz.ch*

Lemma 2.1. *Endliche Körper haben zyklische Einheitengruppen.*

Beweis. Sei K ein endlicher Körper. Nach dem Klassifikationssatz für endlich erzeugte abelsche Gruppen ist

$$K^\times \cong \mathbb{Z}/e_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/e_r\mathbb{Z}$$

mit $e_1 \mid e_2 \mid \ldots \mid e_r$. Daraus folgt, dass jedes Element von $K^\times$ eine Nullstelle von $X^{e_r}-1$ ist. Ein Polynom in $K[X]$ vom Grad e_r hat jedoch höchstens e_r verschiedene Nullstellen in K. Es gilt also

$$\prod_{i=1}^{r} e_i = |K^\times| \leqslant e_r$$

und somit $r=1$. □

Definition 2.2. *Sei $a \in \mathbb{Z}$. Das **Legendresymbol** $\left(\frac{a}{p}\right)$ ist*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } a \equiv 0 \bmod p \\ +1 & \text{falls } a \equiv b^2 \bmod p \text{ für ein } b \in \mathbb{Z} \\ -1 & \text{sonst} \end{cases}$$

*Man sagt auch a ist ein **quadratischer Rest modulo** p falls $\left(\frac{a}{p}\right)=1$. Da dies nur von der Restklasse von a modulo p abhängt schreiben wir auch $\left(\frac{a}{p}\right)$ für $a \in \mathbb{Z}/p\mathbb{Z}$.*

Lemma 2.3. *Sei p eine Primzahl und g eine Primitivwurzel modulo p, d.h. ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$. Dann sind die quadratischen Reste in $\mathbb{Z}/p\mathbb{Z}$ genau $\{g^{2k} \mid k \in \mathbb{Z}\}$, und für p ungerade ist*

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) = 0$$

Beweis. Es ist klar, dass jedes solche Element ein quadratischer Rest ist. Ist umgekehrt $a=b^2$ für $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$, so ist $b=g^k$ für ein $k \in \mathbb{Z}$ und somit $a=g^{2k}$.

Für p ungerade ist $|(\mathbb{Z}/p\mathbb{Z})^\times|$ gerade, und somit sind für ein $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ die k mit $g^k = a$ alle gerade oder alle ungerade. Also ist $\left(\frac{g^{2k+1}}{p}\right) = -1$ für alle $k \in \mathbb{Z}$. Die obige Gleichung folgt also aus $\mathbb{Z}/p\mathbb{Z} = \{0, g, g^2, ..., g^{p-2}, g^{p-1}\}$. □

Theorem 2.4. *(Eulersches Kriterium) Ist p eine ungerade Primzahl, so gilt*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

für alle $a \in \mathbb{Z}$

Beweis. Für $a \equiv 0 \bmod p$ sind beide Seiten 0. Sei also ab jetzt $a \not\equiv 0 \bmod p$. Dann gilt

$$\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \bmod p$$

$\Rightarrow$ Ist $a \equiv b^2 \bmod p$, so ist $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p$

$\Leftarrow$ Sei g eine Primitivwurzel modulo p, und schreibe $a \equiv g^k$ für $k \in \{1, ...p-1\}$. Aus

$$g^{k\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1$$

folgt $(p-1) \mid k\frac{p-1}{2}$. Somit ist k gerade und nach Lemma 2.3 ist $\left(\frac{a}{p}\right) = 1$

Da wegen $(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1$ beide Seiten Werte in $\{\pm 1\}$ haben, beweist dies die Aussage des Satzes. □

Korollar 2.5. *Für alle $a, b \in \mathbb{Z}$, p prim gilt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Beweis. Mit dem Eulerschen Kriterium (2.4), bzw. für $p = 2$ mit $\left(\frac{a}{p}\right) \equiv a \bmod 2$, folgt dass die beiden Seiten Kongruent modulo p sind. Da zudem beide Seiten Werte in $\{\pm 1, 0\}$ bzw. für $p = 2$ in $\{0, 1\}$ haben impliziert die Kongruenz eine Gleichheit. □

Proposition 2.6. *Ist p eine ungerade Primzahl, so gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Beweis. Wir bemerken zunächst, dass $(-1)^{\frac{p^2-1}{8}}$ nur von p modulo 8 abhängt:

$$(-1)^{\frac{(p+8k)^2-1}{8}} = (-1)^{\frac{p^2-1}{8}+2k+8k^2} = (-1)^{\frac{p^2-1}{8}}$$

Dasselbe gilt für $\left(\frac{2}{p}\right)$: nach dem Eulerschen Kriterium 2.4 ist

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \bmod p$$

Mit $2 = (-i)(1+i)^2$ gilt in $\mathbb{Z}[i]$:

$$2^{\frac{p-1}{2}} = (-i)^{\frac{p-1}{2}}(1+i)^{(p-1)} = \frac{(-i)^{\frac{p-1}{2}}}{1+i}(1+i)^p \equiv \frac{(-i)^{\frac{p-1}{2}}}{(1+i)}(1+i^p) \bmod p$$

Wegen $i^4 = 1$ ist der rechte Term auch nur abhängig von p modulo 8. Da p ungerade ist, genügt es die Gleichheit für $p \equiv \pm 1, \pm 3 \bmod 8$ zu prüfen. Sowohl im obigen Ausdruck als auch in $(-1)^{\frac{p^2-1}{8}}$ erhalten wir 1 für $p \equiv \pm 1 \bmod 8$ und -1 für $p \equiv \pm 3 \bmod 8$. □

Definition 2.7. *Sei p prim, $\xi = e^{\frac{2\pi i}{p}}$. Die **Gaussumme** von $a \in \mathbb{Z}$ ist*

$$g_a = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\xi^{ai}.$$

Lemma 2.8. *Seien p, q verschiedene ungerade Primzahlen und $a \in \mathbb{Z}$, $a \not\equiv 0 \bmod p$. Dann gilt*

(1) $g_a = \left(\frac{a}{p}\right)g_1$
(2) $g_1^2 = \left(\frac{-1}{p}\right)p$
(3) $g_1^q \equiv g_q \bmod q$

Beweis. (1) Da alle Summanden nur von der Restklasse von i modulo p abhängen, können wir die Indexverschiebung $i \mapsto ai$ anwenden:

$$\left(\frac{a}{p}\right) g_1 = \left(\frac{a}{p}\right) \sum_{i=1}^{p-1} \left(\frac{ai}{p}\right) \xi^{ai} = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi^{ai} = g_a$$

Die zweite Gleichheit verwendet die Multiplikativität des Legendresymbols und $\left(\frac{a^2}{p}\right) = 1$.

(2) Wie in (1) verwenden wir die Indexverschiebung $j \mapsto ij$, und erhalten

$$g_1^2 = \sum_{i,j=1}^{p-1} \left(\frac{ij}{p}\right) \xi^{i+j} = \sum_{i,j=1}^{p-1} \left(\frac{i^2 j}{p}\right) \xi^{i(j+1)} = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \sum_{i=1}^{p-1} \xi^{i(j+1)}$$

Für $j = p-1$ ist $\xi^{i(j+1)} = (\xi^p)^i = 1$. Für $j+1 \not\equiv 0 \bmod p$ ist

$$\sum_{i=1}^{p-1} \xi^{i(j+1)} = \sum_{i=1}^{p-1} \xi^i = \frac{\xi^p - 1}{\xi - 1} - 1 = -1$$

Also erhalten wir

$$g_1^2 = (p-1)\left(\frac{p-1}{p}\right) - \sum_{i=1}^{p-2} \left(\frac{i}{p}\right)$$

Aber nach Lemma 2.3 ist $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$. Somit folgt (2):

$$g_1^2 = p\left(\frac{p-1}{p}\right) = p\left(\frac{-1}{p}\right)$$

(3) Da q prim und ungerade ist, gilt

$$g_1^q = \left(\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi^i\right)^q \equiv \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^q \xi^{iq} = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi^{iq} = g_q \bmod q$$

□

Theorem 2.9. *(quadratische Reziprozität) Sind p, q ungerade verschiedene Primzahlen, so gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Beweis. Nach Lemma 2.8, Teil (2) und (3) ist

$$g_q \equiv g_1^q = g_1 (g_1^2)^{\frac{q-1}{2}} = g_1 \left(\left(\frac{-1}{p}\right) p\right)^{\frac{q-1}{2}} \bmod q$$

Nach Teil (1) ist

$$g_q = g_1 \left(\frac{q}{p}\right)$$

Da aus Lemma 2.8, Teil (2) $g_1 \not\equiv 0 \bmod q$ folgt, ist

$$\left(\frac{q}{p}\right) \equiv \left(\left(\frac{-1}{p}\right) p\right)^{\frac{q-1}{2}} \bmod q$$

Mit dem Eulerschen Kriterium 2.4 und der Multiplikativität erhalten wir

$$\left(\frac{q}{p}\right) \equiv \left(\frac{\left(\frac{-1}{p}\right) p}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \bmod q$$

Analog zum Beweis der Multiplikativität sind hier beide Seiten in $\{\pm 1\}$, und deshalb sind sie nicht nur kongruent sondern sogar gleich. □

Theorem 2.10. *(Lucas-Lehmer-Test) Sei $(S_k)_{k \geqslant 1}$ die Folge definiert durch $S_1 = 4$ und $S_{k+1} = S_k^2 - 2$. Ist p eine ungerade Primzahl, und $n = 2^p - 1$ so gilt:*

$$n \text{ ist prim} \iff n \mid S_{p-1}$$

Beweis. Seien $\omega = 2 + \sqrt{3}, \bar{\omega} = 2 - \sqrt{3}$. Mit einem Induktionsargument folgt $S_{k+1} = \omega^{2^k} + \bar{\omega}^{2^k}$ für alle $k \geqslant 1$.

$\Rightarrow$ Angenommen n sei Prim: Aus dem eulerschen Kriterium folgt

$$2^{\frac{n-1}{2}} \equiv \left(\frac{2}{n}\right) = \left(\frac{2+2n}{n}\right) = 1 \bmod n$$

Mit $\omega = \frac{1}{2}(1+\sqrt{3})^2$ und $2^{p-1} = \frac{n+1}{2}$ rechnen wir nun

$$\omega^{2^{p-1}} \equiv 2^{\frac{n-1}{2}}\omega^{\frac{n+1}{2}} = \frac{1}{2}(1+\sqrt{3})^{n+1} \equiv \frac{1}{2}(1+\sqrt{3}^n)(1+\sqrt{3}) = \frac{1}{2}(1+3^{\frac{n-1}{2}}\sqrt{3})(1+\sqrt{3}) \bmod n$$

Aus dem quadratischen Reziprozitätsgesetz, sowie $n \equiv (-1)^p - 1 \equiv -2 \equiv 1 \bmod 3$ erhalten wir

$$3^{\frac{n-1}{2}} \equiv \left(\frac{3}{n}\right) = -\left(\frac{n}{3}\right) = -\left(\frac{1}{3}\right) = -1 \bmod n$$

Insgesamt folgt also

$$\omega^{2^{p-1}} \equiv \frac{1}{2}(1-\sqrt{3})(1+\sqrt{3}) = -1 \bmod n$$

$$S_{p-1} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = \bar{\omega}^{2^{p-2}}(\omega^{2^{p-1}}+1) \equiv 0 \bmod n$$

$\Leftarrow$ Sei umgekehrt $S_{p-1} = an$ für $a \in \mathbb{N}$. Falls ein Primfaktor $q \in [3, \sqrt{n}]$ von n existiert, so ist

$$\omega^{2^{p-1}} = S_{p-1}\omega^{2^{p-2}} - 1 \equiv -1 \bmod q$$

Somit ist ω eine Einheit der Ordnung 2^p in $\mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}]$:

Wegen $\omega^{2^p} = 1$ ist ω eine Einheit, und die Ordnung von ω teilt 2^p.

Wegen $\omega^{2^{p-1}} = -1$ und $-1 \neq 1$ da $q \neq 2$, kann die Ordnung von ω kein Teiler von 2^{p-1} sein. Also bleibt nur 2^p.

Aber $\mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}]$ hat nur q^2-1 von 0 verschiedene Elemente, und

$$2^p \leqslant q^2 - 1 \leqslant n - 1 = 2^p - 2$$

geht nicht. Also ist n eine Primzahl.

□

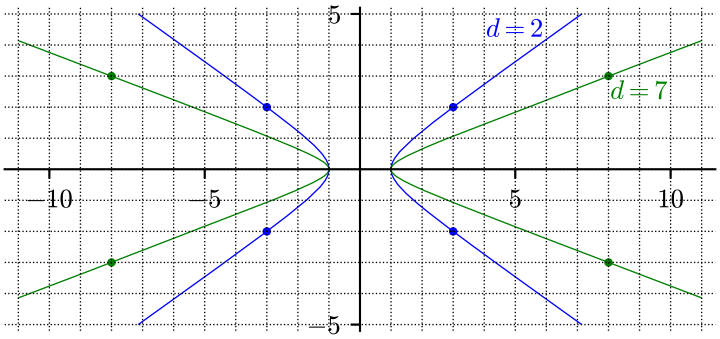
3. Pell Gleichung und Einheiten in quadratischen Zahlkörpern

Johann Birnick, *jbirnick@student.ethz.ch*

3.1. **Die Pell Gleichung.** Die Gleichung

$$x^2 - dy^2 = 1,$$

wobei $d > 0$ ganzzahlig, heißt *Pell Gleichung*. Die Lösungen $(x, y) \in \mathbb{R}^2$ bilden eine Hyperbel:



Wir suchen die ganzzahligen Lösungen $(x, y) \in \mathbb{Z}^2$. Wie wir bald sehen werden, stehen diese in Zusammenhang mit der Struktur von Einheiten in bestimmten Ringen. Dem liegt die Identität $x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$ zu Grunde, die uns bereits in diesem Kapitel helfen wird.

Wir haben immer die trivialen Lösungen $(x, y) = (\pm 1, 0)$. Falls $d = n^2$ eine Quadratzahl ist, so erfüllt jede Lösung $(x + ny)(x - ny) = 1$, also $x + ny = x - ny$ $(= \pm 1)$, also $y = 0$, und wir haben nur die trivialen Lösungen. Für dieses Kapitel fixieren wir also ein d, dass keine Quadratzahl ist.

Es gibt verschiedenste Methoden, die Pell Gleichung zu lösen. Eine wichtige Beobachtung ist, dass große Lösungen (x, y) gute rationale Approximationen von $\sqrt{d}$ liefern, denn $x/y \approx \sqrt{d}$. Tatsächlich kann man $\sqrt{d}$ in Kettenbrüche entwickeln, und alle (positiven) Lösungen der Pellgleichung treten als solcher Kettenbruch auf. Wir verfolgen eine etwas andere Methode, die aber auch auf rationalen Approximationen beruht:

Satz 3.1 (Dirichlet Lemma)**.** *Sei $x \in \mathbb{R}$ und $N \in \mathbb{N}^+$. Dann gibt es $p, q \in \mathbb{Z}$ teilerfremd mit*

$$\left| x - \frac{p}{q} \right| \leqslant \frac{1}{q(N+1)} \quad \text{und} \quad 1 \leqslant q \leqslant N.$$

Beweis. Wir schreiben $[\xi]$ für $\xi - \lfloor \xi \rfloor$ und betrachten die $N+1$ Zahlen $0, [x], [2x], ..., [Nx] \in [0, 1)$. Wir teilen $[0, 1)$ in die $N+1$ disjunkten Intervalle $[\frac{j}{N+1}, \frac{j+1}{N+1})$, $j = 0, ..., N$, auf.

Wenn im letzten Intervall eine Zahl liegt, gibt es also $1 \leqslant q \leqslant N$ ganz mit $\frac{N}{N+1} \leqslant [qx] < 1$. Mit $p \coloneqq \lfloor qx \rfloor$ folgt $|qx - p| \leqslant \frac{1}{N+1}$, also die Behauptung.

Sonst gibt es nach dem Schubfachprinzip ein Intervall, in dem zwei Zahlen liegen. Also $0 \leqslant r < s \leqslant N$ ganz mit $|[rx] - [sx]| < \frac{1}{N+1}$. Mit $q \coloneqq s - r$ und $p \coloneqq \lfloor sx \rfloor - \lfloor rx \rfloor$ folgt $|qx - p| = |sx - rx - \lfloor sx \rfloor + \lfloor rx \rfloor| = |[sx] - [rx]| < \frac{1}{N+1}$.

Für p, q teilerfremd, teile einfach durch $\mathrm{ggT}(p, q)$; unsere Abschätzung wird nur strikter. □

Korollar 3.2. *Sei $x \in \mathbb{R} \backslash \mathbb{Q}$. Dann gibt es unendlich viele $p, q \in \mathbb{Z}$ teilerfremd mit $|qx - p| < \frac{1}{q}$.*

Beweis. Das Dirichlet Lemma mit N beliebig liefert ein solches Paar, da $|qx - p| \leqslant \frac{1}{N+1} < \frac{1}{q}$. Wenn es nur endlich viele solcher Paare (p_i, q_i) gibt, ist $\varepsilon \coloneqq \min_i |q_i x - p_i| > 0$ da $x \notin \mathbb{Q}$. Anwendung des Lemmas mit $N \geqslant 1/\varepsilon$ liefert dann wegen $|qx - p| < 1/N \leqslant \varepsilon$ aber ein verschiedenes Paar. ↯ □

Theorem 3.3. *Die Pell Gleichung $x^2 - dy^2 = 1$, $0 < d \neq n^2$, hat eine nichttriviale Lösung $(x, y) \in \mathbb{Z}^2$.*

Beweis. Nach Korollar 3.2 gibt es unendlich viele $x, y \in \mathbb{N}$ teilerfremd mit $|x - y\sqrt{d}| \leqslant \frac{1}{y} \leqslant 1$. ($\mathbb{N}$ statt $\mathbb{Z}$ da $\sqrt{d} > 1$) Insbesondere gilt für diese auch $x \leqslant 1 + y\sqrt{d}$, und somit

$$|x^2 - dy^2| = |x + y\sqrt{d}||x - y\sqrt{d}| \leqslant \frac{x + y\sqrt{d}}{y} \leqslant \frac{1 + 2y\sqrt{d}}{y} \leqslant 1 + 2\sqrt{d}.$$

Da $|x^2 - dy^2|$ ganz ist, gibt es nach dem Schubfachprinzip ein $M \in [-1 - 2\sqrt{d}, 1 + 2\sqrt{d}]$ ganzzahlig, sodass die Gleichung $x^2 - dy^2 = M$ unendlich viele Lösungen $(x, y) \in \mathbb{N}^2$ mit x, y teilerfremd hat.

$M \neq 0$ da $\sqrt{d} \notin \mathbb{Q}$. Da $(\mathbb{Z}/M\mathbb{Z})^2$ endlich ist, gibt es nach dem Schubfachprinzip zwei verschiedene Lösungen (x_1, y_1), $(x_2, y_2) \in \mathbb{N}^2$ mit $x_1 \equiv x_2 \bmod M$ und $y_1 \equiv y_2 \bmod M$. Wir definieren nun

$$\begin{aligned} A &\coloneqq x_1 x_2 - d y_1 y_2 \\ B &\coloneqq x_2 y_1 - x_1 y_2 \end{aligned} \quad \text{, sodass} \quad (x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = A + B\sqrt{d}.$$

Es folgt $A \equiv x_1^2 - dy_1^2 \equiv 0 \bmod M$ und $B \equiv 0 \bmod M$, also $A = M\widetilde{A}$, $B = M\widetilde{B}$. Außerdem

$$A^2 - dB^2 = (A + B\sqrt{d})(A - B\sqrt{d}) = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = M^2,$$

also $\widetilde{A}^2 - d\widetilde{B}^2 = 1$. Die Lösung ist nicht trivial, da $\widetilde{B} = 0 \implies x_2 y_1 = x_1 y_2 \implies \frac{x_1}{y_1} = \frac{x_2}{y_2}$ ↯. □

Um die Einheiten in besagten Ringen zu klassifizieren, genügt uns dieses Resultat bereits. Nichtsdestoweniger möchten wir noch zeigen, dass es sogar unendlich viele Lösungen der Pell Gleichung gibt! Wir rechnen hier explizit aus, was wir gleich implizit machen werden, indem wir Elemente in Ringen potenzieren.

Korollar 3.4. *Die Pell Gleichung $x^2 - dy^2 = 1$, $0 < d \neq n^2$, hat unendlich viele Lösungen $(x, y) \in \mathbb{Z}^2$.*

Beweis. Sei (x, y) eine nichttriviale Lösung. Für $n \in \mathbb{N}^+$ definiere:

$$x_n \coloneqq \frac{(x + y\sqrt{d})^n + (x - y\sqrt{d})^n}{2} \qquad y_n \coloneqq \frac{(x + y\sqrt{d})^n - (x - y\sqrt{d})^n}{2\sqrt{d}}$$

Anhand der Binomialentwicklung sieht man, dass $x_n, y_n \in \mathbb{Z}$ ganzzahlig sind. Es gilt

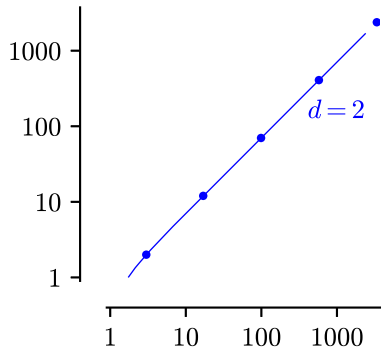
$$x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n \quad \text{und} \quad x_n - y_n\sqrt{d} = (x - y\sqrt{d})^n,$$

also folgt $x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = (x^2 - dy^2)^n = 1$.

Die Lösungen sind alle verschieden, da $|x_n + y_n\sqrt{d}| = |x + y\sqrt{d}|^n$ und $|x + y\sqrt{d}| \neq 1$ da sonst wegen $1 = (x + y\sqrt{d})(x - y\sqrt{d})$ folgt $x + y\sqrt{d} = x - y\sqrt{d}$ $(= \pm 1)$, also $y = 0$ ↯. □

Tatsächlich sind sogar alle Lösungen von solcher Form, in dem Sinne, dass es eine *Fundamentallösung* $(x, y) \in \mathbb{Z}^2$ gibt, und jede andere Lösung ist von der Form $(\pm x_n, \pm y_n)$ mit x_n, y_n wie im letzten Beweis. Wir werden das im nächsten Kapitel sehen. (Streng genommen nur für spezielle d, aber der Beweis funktioniert genauso für alle d, die wir hier betrachten.)

Die Lösungen von $x^2 - 2y^2 = 1$ sind generiert von $(\pm 3, \pm 2)$, und lauten weiter $(\pm 17, \pm 12)$, $(\pm 99, \pm 70)$, $(\pm 577, \pm 408)$, $(\pm 3363, \pm 2378)$, ... Nachfolgend sind sie auf einem log-log Plot dargestellt. Warum sind die Abstände (nahezu) linear?



3.2. **Quadratische Zahlkörper und Zahlringe.** Als *Zahlkörper* bezeichnen wir alle endlichen Körpererweiterungen von $\mathbb{Q}$. Für $\xi \in \mathbb{C}$ bezeichnet $\mathbb{Q}(\xi)$ den kleinsten Unterkörper von $\mathbb{C}$, der sowohl $\mathbb{Q}$ als auch ξ enthält. Im Folgenden möchten wir die *quadratischen Zahlkörper* $\mathbb{Q}(\sqrt{d})$ betrachten, wobei $d \in \mathbb{Z}$ eine ganze Zahl ist.

Die Fälle $d \in \{0, 1\}$ sind schnell abgehandelt. Und wenn $n^2 | d$ für ein $n \in \mathbb{N}$, so ist $\sqrt{d} = n\sqrt{d/n^2}$, also $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d/n^2})$. Deshalb können wir voraussetzen, dass $d \notin \{0, 1\}$ und d *quadratfrei*, das heißt d besitzt nur einfache Primfaktoren. Wir fixieren ab nun ein solches $d \in \mathbb{Z}$.

$\sqrt{d}$ ist (per Definition) Nullstelle des Polynoms $X^2 - d \in \mathbb{Q}[X]$, also algebraisch über $\mathbb{Q}$. Da d quadratfrei ist, ist auch $\sqrt{d} \notin \mathbb{Q}$, also ist dies das Minimalpolynom und es folgt:

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q} + \mathbb{Q}\sqrt{d} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

Dem Leser ist sicher bereits aufgefallen, dass in unserer bisher einheitlichen Betrachtung sich doch zwei durchaus verschiedene Fälle ergeben. Ist nämlich $d < 0$, so ist $\sqrt{d}$ rein imaginär und wir erhalten bildlich gesehen ein gleichmäßiges Gitter in $\mathbb{C}$. In diesem Fall heißt der Körper *imaginär-quadratisch*. Wenn hingegen $d > 0$, so ist $\mathbb{Q}(d)$ ein Unterkörper von $\mathbb{R}$, und er heißt *reell-quadratisch*. Trotzdem möchten wir eine – zu der im komplexen Fall bereits bekannten analoge – allgemeine Konjugation definieren:

$$\begin{aligned} \overline{\square}: \quad & \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d}) \\ & z = a + b\sqrt{d} \mapsto \overline{z} \coloneqq a - b\sqrt{d} \end{aligned}$$

Dies ist ein Körperautomorphismus. So sieht man auch, dass die Konjugation gleichermaßen für den Fall $d > 0$ Sinn ergibt und wichtig ist, denn $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \overline{\square}\}$.

Dass $\mathbb{Q}(\sqrt{d})$ ein endlichdimensionaler $\mathbb{Q}$-Vektorraum ist, kann man noch anderweitig nutzen. Die Multiplikation $L_{a+b\sqrt{d}}$ mit $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ ist wegen dem Distributiv- und Assoziativgesetz nämlich eine lineare Abbildung auf $\mathbb{Q}(\sqrt{d})$. Wählen wir zum Beispiel die Basis $(1, \sqrt{d})$, besitzt sie die Matrixdarstellung

$$L_{a+b\sqrt{d}} \simeq \begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Über Determinante und Spur – beides unabhängig von der Wahl der Basis – können wir also $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ weitere Eigenschaften zuordnen, die *Norm* und die *Spur*:

$$N: \quad \mathbb{Q}(\sqrt{d}) \to \mathbb{Q} \qquad\qquad \mathrm{tr}: \quad \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$$
$$z = a + b\sqrt{d} \mapsto a^2 - db^2 = z \cdot \overline{z} \qquad\qquad z = a + b\sqrt{d} \mapsto 2a = z + \overline{z}$$

Man verifiziert, unter Verwendung der Multiplikativität der Determinante, dass:

$$N(z \cdot w) = N(z) \cdot N(w) \qquad\qquad \mathrm{tr}(z + w) = \mathrm{tr}(z) + \mathrm{tr}(w)$$

Analog zu den ganzen Zahlen $\mathbb{Z}$ in den rationalen, möchten wir nun einen Unterring $\mathcal{O}_d \subseteq \mathbb{Q}(\sqrt{d})$ von $\mathbb{Q}(\sqrt{d})$ als die "ganzen" Zahlen identifizieren. Eine sinnvolle Forderung scheint $\mathcal{O}_d \cap \mathbb{Q} = \mathbb{Z}$. Die erste Idee ist $\mathbb{Z} + \mathbb{Z}\sqrt{d}$. Doch wir wollen stattdessden das normierte Minimalpolynom von $z \in \mathbb{Q}(\sqrt{d})$ betrachten, $(X - z)(X - \overline{z}) = X^2 - \mathrm{tr}(z)X + N(z) \in \mathbb{Q}[X]$ bzw. $X - z$, und fordern, dass es ganzzahlige Koeffizienten hat.

Definition 3.5. $\mathcal{O}_d \coloneqq \{z \in \mathbb{Q}(\sqrt{d}) \mid \mathrm{tr}(z) \in \mathbb{Z}, N(z) \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{d})$ *heißt* quadratischer Zahlring.

Bemerkung 3.6. Auch für einen beliebigen Zahlkörper K betrachtet man die ganzen Zahlen $\mathcal{O}_K \subseteq K$ als die Elemente in K, deren normiertes Minimalpolynom in $\mathbb{Z}[X]$ liegt. Man nennt sie auch *ganz-algebraische* Zahlen. Eine Zahl ist im Übrigen ganz-algebraisch genau dann, wenn sie Nullstelle *irgendeines* normierten Polynoms in $\mathbb{Z}[X]$ ist. Das beweist man mit Hilfe des Gauss-Lemmas.

Lemma 3.7. *$\mathcal{O}_d$ ist tatsächlich ein Unterring, und es gilt:*

- $\mathcal{O}_d = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ *falls* $d \equiv 2, 3 \bmod 4$
- $\mathcal{O}_d = \{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z} \text{ und } a \equiv b \bmod 2\} = \mathbb{Z} + \mathbb{Z}\omega$ *mit* $\omega = \frac{1+\sqrt{d}}{2}$ *falls* $d \equiv 1 \bmod 4$

Bemerkung 3.8. $(1, \sqrt{d})$ beziehungsweise $(1, \frac{1+\sqrt{d}}{2})$ nennt man auch *Ganzheitsbasis* von $\mathcal{O}_d$.

Beweis. Durch Berechnen von Norm und Spur prüft man nach, dass die beschriebenen Mengen tatsächlich in $\mathcal{O}_d$ liegen. Sei nun $\frac{A+B\sqrt{d}}{2} \in \mathcal{O}_d$ mit $A, B \in \mathbb{Q}$. Also $A \in \mathbb{Z}$ und $\frac{A^2-dB^2}{4} \in \mathbb{Z}$. Insbesondere $A^2 - dB^2 \in \mathbb{Z}$, also wegen $A^2 \in \mathbb{Z}$ auch $dB^2 \in \mathbb{Z}$. Da d quadratfrei, folgt somit $B \in \mathbb{Z}$.

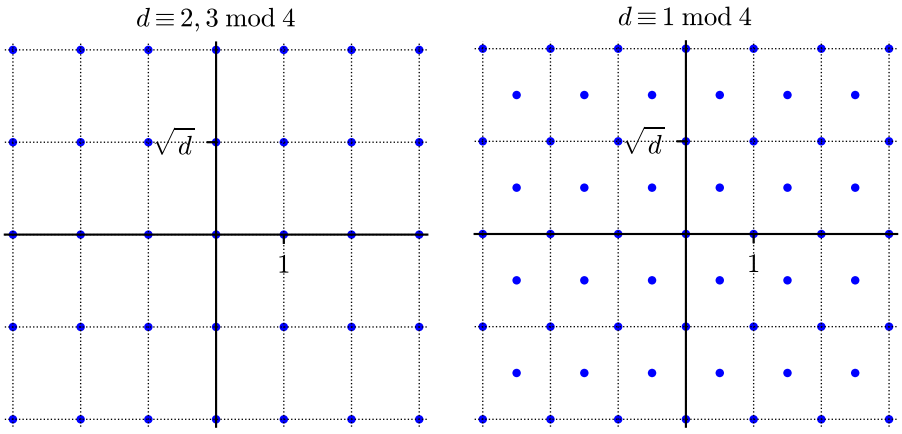
Wir haben also $A, B \in \mathbb{Z}$ und $A^2 \equiv dB^2 \bmod 4$. Die einzigen Quadrate in $\mathbb{Z}/4\mathbb{Z}$ sind 0 und 1.

$\rightsquigarrow$ $d \equiv 2, 3 \bmod 4 \implies A^2 \equiv B^2 \equiv 0 \bmod 4 \implies A \equiv B \equiv 0 \bmod 2$.

$\rightsquigarrow$ $d \equiv 1 \bmod 4 \implies A^2 \equiv B^2 \bmod 2 \implies A \equiv B \bmod 2$.

Also folgen die behaupteten Gleichungen. Dass diese Mengen tatsächlich einen Unterring bilden, prüft man durch eine kurze Rechnung nach. □

Nachfolgend sind die Elemente von $\mathcal{O}_d$ als Vektoren bezüglich der Basis $(1, \sqrt{d})$ dargestellt. Man beachte, dass das nur im Fall $d < 0$ auch der komplexen Zahlenebene entspricht!



3.3. **Einheiten in quadratischen Zahlringen.** Welche Elemente in $\mathcal{O}_d$ sind invertierbar? Über die Norm finden wir dafür ein klares Kriterium. Und durch die Darstellung in Lemma 3.7 können wir dieses in diophantische Gleichungen umwandeln.

Lemma 3.9. *Für $z \in \mathcal{O}_d$ ist* $z \in \mathcal{O}_d^\times \iff N(z) = \pm 1$.

Beweis. $\boxed{\Rightarrow}$ $zw = 1 \implies 1 = N(1) = N(z)N(w) \implies N(z) = \pm 1$
$\boxed{\Leftarrow}$ $\pm 1 = N(z) = z\overline{z} \implies z$ hat Inverses $\pm\overline{z}$ □

Korollar 3.10. *Für $a, b \in \mathbb{Z}$ gilt:*

- $a + b\sqrt{d} \in \mathcal{O}_d^\times \iff a^2 - db^2 = \pm 1$ *falls* $d \equiv 2, 3 \bmod 4$
- $\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_d^\times \iff a^2 - db^2 = \pm 4$ *falls* $d \equiv 1 \bmod 4$

Beweis. Im Fall $d \equiv 2, 3 \bmod 4$ ist das genau Lemma 3.9. Für $d \equiv 1 \bmod 4$ haben wir auch $\pm 1 = N(\frac{a+b\sqrt{d}}{2}) = \left(\frac{a}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 \iff \pm 4 = a^2 - db^2$, aber wir müssen zeigen, dass für jede Lösung der rechten Gleichung auch $a \equiv b \bmod 2$ gilt. Wir haben aber $d \equiv 1 \bmod 2$, also folgt wegen $a^2 - db^2 \equiv 0 \bmod 2$, dass $a^2 \equiv b^2 \bmod 2$, also $a \equiv b \bmod 2$. □

Im Fall $d > 0$ entspricht die Norm dem Absolutbetrag. Dann sieht man schnell an obigem Bildchen, dass wir nur endlich viele Einheiten haben können.

Satz 3.11. *Im imaginär-quadratischen Fall $d < 0$ sind alle Einheiten Einheitswurzeln. Konkret:*

$$\mathcal{O}_{-1}^\times = \langle \xi_4 \rangle \qquad \mathcal{O}_{-3}^\times = \langle \xi_6 \rangle \qquad \mathcal{O}_d^\times = \langle \xi_2 \rangle = \pm 1 \quad \text{für } d \leqslant -5 \text{ oder } d = -2$$

Beweis. Sei $e \in \mathcal{O}_d$. Da $d < 0$ entspricht die Norm dem komplexen Absolutbetrag. Insbesondere ist $N(e) > 0$, also mit Lemma 3.9 $N(e) = 1$. $\mathcal{O}_d^\times$ kann aber nur endlich viele Elemente auf dem Einheitskreis haben. Für $e \in \mathcal{O}_d^\times$ folgt also $e^k = e^l$ mit $k > l \in \mathbb{N}$, also $e^{k-l} = 1$.

Die behaupteten Gleichungen scheinen grafisch plausibel. Man kann sie mit Hilfe konkreter Rechnungen und einer Abschätzung für $d \leqslant -5$ nachprüfen. (Es gibt nur endlich viele Elemente mit Norm $\leqslant 1$, z.B. da die quadratische Form $a^2 - db^2$ ist positiv definit ist. Für $d \leqslant -5$ gibt es eben gar keine.) □

Der Fall $d > 0$ ist nicht ganz so einfach. Wichtig zu beobachten ist, dass wir wieder im ersten Kapitel angekommen sind: Wir müssen die Gleichungen $x^2 - dy^2 = \pm 1, \pm 4$ mit $d \in \mathbb{N}^+$ lösen! Wir haben zwar nur die Gleichung ... = 1 gelöst, aber damit erhalten wir auch eine Lösung für ... = 4, also in jedem Fall eine nichttriviale Einheit. Aus dieser konstruieren wir dann alle:

Lemma 3.12. *Im reellquadratischen Fall $d > 0$ ist $\mathcal{O}_d^\times \cap (1, M)$ endlich für alle $M > 1$.*

Beweis. Für $e \in \mathcal{O}_d^\times \cap (1, M)$ folgt wegen $e\overline{e} = N(e) = \pm 1$, dass $\overline{e} \in (-1, 1)$. Also $\operatorname{tr}(e) = e + \overline{e} \in (0, M + 1)$. Es gibt also nur endlich viele Möglichkeiten für $N(e)$ und $\operatorname{tr}(e)$.

Da e Nullstelle von $(X - e)(X - \overline{e}) = X^2 - \operatorname{tr}(e)X + N(e)$ ist, ist e also eine der $4M$ Nullstellen von $\{X^2 - aX + b\}_{a \in \{1,\dots,M\}, b = \pm 1}$. □

Satz 3.13. *Im reellquadratischen Fall $d > 0$ gibt es $\varepsilon \in \mathcal{O}_d^\times, \varepsilon \neq \pm 1$, sodass $\mathcal{O}_d^\times = \{\pm\varepsilon^k \mid k \in \mathbb{Z}\}$.*

Beweis. Wir zeigen zunächst, dass es eine nichttriviale Einheit gibt. Wegen Korollar 3.10 genügt es, eine nichttriviale Lösung der entsprechenden Gleichung zu finden. Diese existiert nach Theorem 3.3 aus dem ersten Kapitel, wobei wir im Fall $d \equiv 1 \bmod 4$ die Lösung der einfachen Pell Gleichung mit 2 multiplizieren.

Da mit $e \in \mathcal{O}_d^\times$ auch $-e, e^{-1}, -e^{-1} \in \mathcal{O}_d^\times$, gibt es also $e \in \mathcal{O}_d^\times$ mit $e > 1$. Nach Lemma 3.12 gibt es dann eine kleinste Einheit $\varepsilon > 1$. $\{\pm\varepsilon^k\}_{k \in \mathbb{Z}} \subseteq \mathcal{O}_d^\times$ ist klar. Angenommen es gibt $e \in \mathcal{O}_d^\times, e \neq \varepsilon^k$. O.b.d.A. $e > 0$. Also $\varepsilon^k < e < \varepsilon^{k+1}$ mit $k \in \mathbb{Z}$. Dann ist aber $1 < e\varepsilon^{-k} < \varepsilon$ und $e\varepsilon^{-k} \in \mathcal{O}_d^\times$ ↯. □

Die Einheit ε in Satz 3.13 und ihre nahen Verwandten $-\varepsilon, \pm\varepsilon^{-1}$ heißen *Fundamentaleinheit*.

Insgesamt haben wir also folgendes Endresultat bewiesen:

Theorem 3.14. *Sei $d \in \mathbb{Z}\backslash\{0, 1\}$ quadratfrei und $U \subseteq \mathcal{O}_d$ die multiplikative Gruppe der Einheitswurzeln im Ganzzahlring $\mathcal{O}_d$ des Körpers $\mathbb{Q}(\sqrt{d})$. Dann gilt:*

$$\mathcal{O}_d^\times \cong \begin{cases} U & d < 0 \\ U \times \mathbb{Z} & d > 0 \end{cases}$$

4. Faktorisieren in quadratischen Zahlkörpern

Sabrina Galfetti, *sabringa@student.ethz.ch*

4.1. **Erinnerung.** Wir beginnen mit eine kürze Erinnerung von den notwendigen Konzepte, die wir in dieser Kapitel benötigen.

Definition 4.1. *$\mathcal{O}_K$ ist der Ring der ganzen Zahlen von K, die ganz-algebraisch sind. Diese ist ein Ring und es gilt*

$$\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

Definition 4.2. *Ein quadratischer Zahlkörper ist ein Körper der Form $\mathbb{Q}(\sqrt{d})$. Er entsteht aus den rationalen Zahlen durch Hinzunahme eine Quadratwurzel.*

4.2. **Rechnen mit Idealen.** In diesem Abschnitt wollen wir zeigen, dass nicht alle Ringe der ganzen algebraischen Zahlen in (quadratische) Zahlkörpern faktorielle Ring sind. Das bedeutet dass, die Primfaktorzerlegung nicht eindeutig ist.

Beispiel 4.3. *$\mathbb{Q}(\sqrt{-5})$ hat keine eindeutige Zerlegung:*

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

Um das zu sagen sollten wir natürlich überprüfen dass, 2, 3, $1 \pm \sqrt{-5}$ alle verschieden sind (trivial) und dass alle irreduzibel in $\mathcal{O}_K$ sind. Das geht ziemlich einfach mit dem Norm. Wir machen als Beispiel das erste Fall, für die andere geht es völlig analog.

Beispiel 4.4. *Wäre nämlich $2 = x \cdot y$ mit x, y nicht Einheiten, so wurde aus der Norm an beide Seiten dann folgen $4 = N(x) \cdot N(y)$. x hat die folgende Form: $x = a + \sqrt{-5}b$ und dann ist $N(x) = a^2 + 5b^2$. Die Norm von x hat folgende mögliche Werten: $0, 1, 4, 5$ undsoweiter. Aber wenn wir die obige Gleichungen mit Normen schauen, sehen wir dass, eine Norm soll 4 sein und die andere 1. Norm 1 ist eine Einheit, entsprechend folgt dass, x oder y eine Einheit ist und insbesondere ist dann 2 irreduzibel.*

Es liegen also zwei verschiedene Primzerlegungen der Zahl 6 vor. Historisch hat Kummer die Idee gehabt, dass es ïdealer Zahlen"gibt wo man wieder eindeutig faktorisieren kann. Um diese Problem zu lösen ist eine Idee gekommen, indem wir in einen grösseren Bereich finden können, wobei die Eindeutikeit der Primfaktorzerlegung wieder gültig ist. Aus diesem Grund führen wir das Konzept von Ideal ein.

Definition 4.5. *Ein Ideal von $\mathcal{O}_K$ ist eine Teilmenge $\mathfrak{a} \subset \mathcal{O}_K$, die die folgende Bedingung erfüllt:*

(1) $\mathfrak{a} \neq \varnothing$.
(2) $\forall a, b \in \mathfrak{a} : a + b \in \mathfrak{a}$.
(3) $\forall x \in \mathcal{O}_K, \forall a \in \mathfrak{a} : xa \in \mathfrak{a}$.

Diese Eigenschaften zeigen wie ein Ideal eine additive Untergruppe von $\mathcal{O}_K$ ist.

Definition 4.6. *Für jedes Element $a \in \mathcal{O}_K$ ist die Menge*

$$a\mathcal{O}_K = \{ax | x \in \mathcal{O}_K\}$$

ein Ideal von $\mathcal{O}_K$, genannt das von a erzeugt Hauptideal.

Bemerkung 4.7. Ein Ideal $\mathfrak{a} \subset \mathcal{O}_K$ heisst Hauptideal wenn es ein $a \in \mathcal{O}_K$ mit $\mathfrak{a} = (a)$ gibt.

Beweis. Wir sollten zeigen, dass ein Hauptideal ein Ideal ist. Wir prüfen einfach die Eigenschaften:

(1) $a \in (a) \neq \varnothing$.
(2) Gegeben $xa, ya \in (a)$ folgt $xa + ya = (x + y)a \in (a)$
(3) Gegeben $t \in \mathcal{O}_K, xa \in (a)$ folgt $t \cdot (xa) = (tx)a \in (a)$

□

Beispiel 4.8. *Ein Beispiel von Idealen sind das Nullideal $(0) = \{0\}$ und das Einsideal $(1) = \mathcal{O}_K$. Diese sind beide Hauptidealen.*

Natürlich Hauptideale sind nicht eindeutig bestimmt, mit dem folgende Lemma sehen wir genauer warum.

Lemma 4.9. *Zwei Hauptideale (a) und (b) von Elementen $a, b \in \mathcal{O}_K$ sind genau dann gleich, wenn a und b assoziiert sind, d.h.*

$$(a) = (b) \Leftrightarrow a \sim b$$

Beweis. Aus $a \in (b)$ folgt, dass ein $x \in \mathcal{O}_K$ mit $a = xb$ existiert. Also gilt $b|a$. Analog schliesst man $a|b$, also $a \sim b$. Die Rückrichtung ist offensichtlich. □

Definition 4.10. *Seien $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ Ideale. Ihre Summe und ihr Produkt sind in folgender Weise definiert:*

$$\mathfrak{a} + \mathfrak{b} = \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}, \qquad \mathfrak{ab} = \{ \sum_{endl.} a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

Es ist leicht zu verifizieren, dass $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{ab}$ wieder Ideale sind. Wir bezeichnen die Summe von Hauptidealen $(a_1) + \ldots + (a_n)$ mit $(a_1, \ldots, a_n)$.

Wir benötigen für unsere weiteren Untersuchungen einige Begrifflichkeiten aus der Faktorringstheorie, welche wir nun kurz wiederholen. Diese sind grundlegender Fakten aus der Algebra, welches wir ohne Beweis angeben.

4.3. **Faktorringe.**

Definition 4.11. *Sei $\mathfrak{a} \subset \mathcal{O}_K$ ein Ideal. Für jedes $x \in \mathcal{O}_K$ heisst die Teilmenge*

$$x + \mathfrak{a} := \{x + a | a \in \mathfrak{a}\} \subset \mathcal{O}_K$$

eine Nebenklasse von $\mathfrak{a}$. Wir bezeichnen die Menge aller Nebenklassen wie folgt:

$$\mathcal{O}_K/\mathfrak{a} := \{x + \mathfrak{a} | x \in \mathcal{O}_K\}.$$

Satz 4.12. *Die Menge $\mathcal{O}_K/\mathfrak{a}$ besitzt eine eindeutige Ringstruktur, so dass gilt:*

(1) $\forall x, x' \in \mathcal{O}_K : (x + \mathfrak{a}) + (x' + \mathfrak{a}) = (x + x') + \mathfrak{a}$.
(2) $\forall x, x' \in \mathcal{O}_K : (x + \mathfrak{a}) \cdot (x' + \mathfrak{a}) = xx' + \mathfrak{a}$.

Für diese gilt weiter:

(1) Das Nullelement von $\mathcal{O}_K/\mathfrak{a}$ ist $0 + \mathfrak{a} = \mathfrak{a}$.
(2) Das Einselement von $\mathcal{O}_K/\mathfrak{a}$ ist $1 + \mathfrak{a}$.
(3) $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}, x \mapsto x + \mathfrak{a}$ ist ein surjektiver Ringhomomorphismus mit Kern $\mathfrak{a}$.

Definition 4.13. *Der Ring $\mathcal{O}_K/\mathfrak{a}$ heisst Faktorring von $\mathcal{O}_K$ nach $\mathfrak{a}$.*

Für uns von besonderem Interesse in Ringe sind Ideale und vor allem Primideale.

4.4. **Primideale.**

Definition 4.14. *Ein Primideal von $\mathcal{O}_K$ ist ein echtes Ideal $\mathfrak{p} \subsetneq \mathcal{O}_K$ mit der Eigenschaft:*

$$\forall a, b \in \mathcal{O}_K : ab \in \mathfrak{p} \to (a \in \mathfrak{p} \vee b \in \mathfrak{p}).$$

Satz 4.15. *Ein Ideal $\mathfrak{p}$ von $\mathcal{O}_K$ ist ein Primideal genau dann, wenn der Faktorring $\mathcal{O}_K/\mathfrak{p}$ ein Integritätsring ist.*

Wir machen das Beweis nicht, es geht einfach mit Eigenschaften von Ideale und Primideale.

Definition 4.16. *Ein Ideal $\mathfrak{m} \subsetneq \mathcal{O}_K$ heisst Maximalideal, wenn es kein Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq \mathcal{O}_K$ gibt.*

Satz 4.17. *Ein Ideal $\mathfrak{m} \subsetneq \mathcal{O}_K$ ist maximal genau dann, wenn der Faktorring $\mathcal{O}_K/\mathfrak{m}$ ein Körper ist.*

Beweis. Wir überprüfen zuerst die Nichtrivialität: $\mathfrak{m} \neq \mathcal{O}_K \Leftrightarrow \mathcal{O}_K/\mathfrak{m} \neq 0$.
Ist $\mathfrak{m}$ maximal, sei $x + \mathfrak{m} \in (\mathcal{O}_K/\mathfrak{m})\backslash\{0\}$, dies bedeutet $x \notin \mathfrak{m}$. Dann ist $\mathfrak{m} \subsetneq \mathfrak{m} + (x) \subseteq \mathcal{O}_K$. Die Maximalität impliziert dann, dass das letzte Symbol der obige Gleichung eine Gleichheit ist. Somit ist $1 \in \mathfrak{m} + (x)$. So folgt, dass $\exists n \in \mathfrak{m}, b \in \mathcal{O}_K : n + bx = 1$, das impliziert $bx + \mathfrak{m} = 1 + \mathfrak{m}$. Somit ist $x + \mathfrak{m}$ in $\mathcal{O}_K/\mathfrak{m}$ invertierbar. Somit ist $\mathcal{O}_K/\mathfrak{m}$ ein Körper.
Umgekehrt ist $\mathcal{O}_K/\mathfrak{m}$ ein Körper, betrachten wir $\mathfrak{m} \subsetneq \mathfrak{a} \subseteq \mathcal{O}_K$. Wie sollten prüfen, dass $\mathfrak{a} = \mathcal{O}_K$. Wähle $x \in \mathfrak{a}\backslash\mathfrak{m}$, dann folgt $0 \neq x + \mathfrak{m} \in \mathcal{O}_K/\mathfrak{m}$. Dann existiert $b \in \mathcal{O}_K : (b + \mathfrak{m})(x + \mathfrak{m}) = 1 + \mathfrak{m}$. Dann ist $1 \in bx + \mathfrak{m} \subseteq \mathfrak{a}$. Dies impliziert $1 \in \mathfrak{a}$, das Äquivalent ist zu sagen $\mathfrak{a} = \mathcal{O}_K$. □

Korollar 4.18. *Jedes maximales Ideal ist ein Primideal.*

Beweis. Sei $\mathfrak{m}$ maximal. Dann ist $\mathcal{O}_K/\mathfrak{m}$ ein Körper, und ausserdem ein Integritätsring. Deswegen ist $\mathfrak{m}$ ein Primideal. □

4.5. **Beispiel.** Jetzt gehen wir weiter mit der vorherige Beispiel, wir wollen diesesmal eine eindeutige Primfaktorisierung mit Ideale finden. Um das zu machen brauchen wir das folgende Theorem.

Theorem 4.19. *Jedes von* (0) *und* (1) *verschiedene Ideal* $\mathfrak{a} \subset \mathcal{O}_K$ *hat eine bis auf Reihenfolge der Faktoren eindeutige Zerlegung in ein Produkt von Primidealen*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

Das Beweis dieses Theorem kommt später im Seminar.
Somit können wir jedes ganze Ideal $\mathfrak{a} \neq (0)$ eindeutig in der Form

$$\mathfrak{a} = \prod_{\mathfrak{p}\ Primideal} \mathfrak{p}^{e_\mathfrak{p}}$$

schreiben. Die Exponenten $e_\mathfrak{p}$ sind nicht negative ganze Zahlen und es gilt $e_\mathfrak{p} = 0$ für alle bis auf endliche viele $\mathfrak{p}$.

Das Ideal (2) ist nicht ein Primideal. Wir können diese Ideal mit Hilfe des vorheriges Theorem in Primideale faktorisieren. Wir erhalten:

$$(2) = (2, 1 + \sqrt{-5}) \cdot (2, 1 + \sqrt{-5}).$$

Wir setzen $\mathfrak{p} := (2, 1 + \sqrt{-5})$. Um zu zeigen, dass $\mathfrak{p}$ Primideal ist, benutzen wir die vorherige Sektion über Faktorringe. Wir zeigen, dass $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}$ ein Körper ist.
Wir haben die folgende Isomorphismus:

$$\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[X]/(X^2 + 5)$$

das heisst isomorph zur Polynomring $\mathbb{Z}[X]$ modulo das Ideal $(X^2 + 5)$. Aus selben Grunden gilt das folgende Isomorphismus:

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \cong \mathbb{Z}[X]/(X^2 + 5, 2, 1 + X) \cong \mathbb{Z}/2\mathbb{Z}.$$

Das letzte ist ein klarerweise ein Körper mit genau zwei Elementen. Somit haben wir bewiesen dass $\mathfrak{p}$ ein Primideal ist (mit der Hilfe der obigen Sätze). Ähnlicher zeigen wir, dass $(3, 1 \pm \sqrt{-5})$ Primideale sind.

Wir machen dasselbe Prozess auch für die andere Fälle und wie erhalten das folgende:

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

Somit erhalten wir

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

wobei wir haben die folgende Eigenschaft benutzt: $(2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$.
Wir haben somit eine eindeutige Zerlegung in Primidealen erhalten.

4.6. **Das Zerlegungsgesetz.** In diesen Kapitel brauchen wir die folgende Unterschied, wir bezeichnen mit $n\mathbb{Z}$ das von n erzeugte Hauptideal in $\mathbb{Z}$, und mit $n\mathcal{O}_K$ das von n in $\mathcal{O}_K$ erzeugte Hauptideal.

Lemma 4.20. *Für* $n \in \mathbb{Z}$ *gilt*

$$n\mathcal{O}_K \cap \mathbb{Z} = n\mathbb{Z}.$$

Insbesondere gilt für $n, m \in \mathbb{Z}$: $n\mathcal{O}_K = m\mathcal{O}_K \Leftrightarrow n\mathbb{Z} = m\mathbb{Z}$.

Um das Lemma zu beweisen brauchen wir eine vorherige Satz, die wir ohne Beweis geben.

Satz 4.21. *Eine rationale Zahl ist genau dann ganz-algebraisch, wenn sie in* $\mathbb{Z}$ *liegt.*

Beweis. Für $n = 0$ ist die aussage trivial. Sei $n \neq 0$. Die Inklusion $n\mathbb{Z} \subset n\mathcal{O}_K \cap \mathbb{Z}$ ist offensichtlich. Für ein beliebig gewähltes Element $a \in n\mathcal{O}_K \cap \mathbb{Z}$ existiert nach Definition ein $x \in \mathcal{O}_K$ mit $a = nx$. Nun liegt $x = a/n$ in $\mathbb{Q}$. Somit ist x eine ganz algebraische rationale Zahl, und daher folgt $x \in \mathbb{Z}$, und daher gilt $a \in n\mathbb{Z}$. □

Definition 4.22. *Eine Primzahl p heisst in K*

- *träge, wenn $p\mathcal{O}_K$ ein Primideal ist,*
- *zerlegt, wenn $p\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ mit Primidealen $\mathfrak{p}_1 \neq \mathfrak{p}_2$ in $\mathcal{O}_K$,*
- *verzweigt, wenn $p\mathcal{O}_K = \mathfrak{p}^2$ für ein Primideal $\mathfrak{p}$ in $\mathcal{O}_K$.*

Wir erinnern dass $(1, w)$ Ganzheitsbasis des Ringes $\mathcal{O}_K$. Das heisst $w = \sqrt{d}$ wenn $d \not\equiv 1 \, mod \, 4$, und $w = (1 + \sqrt{d})/2$ wenn $d \equiv 1 \, mod \, 4$ ist.

Sei nun f_w das Minimalpolynom von w, das heisst

$$f_w(X) = \begin{cases} X^2 - d, & wenn \, d \not\equiv 1 \, mod \, 4, \\ X^2 - X - \frac{d-1}{4}, & wenn \, d \equiv 1 \, mod \, 4. \end{cases}$$

Satz 4.23. *Eine Primzahl p heisst in K*

- *träge, wenn f_w irreduzibel modulo p ist,*
- *zerlegt, wenn f_w modulo p in zwei verschiedene Linearfaktoren zerfällt,*
- *verzweigt, wenn f_w modulo p eine doppelte Nullstelle hat.*

Beweis. Sei $f \in \mathbb{Z}[X]$ so dass $\bar{f}$ ein Primteiler von $\bar{f}_w$ in $\mathbb{Z}/p\mathbb{Z}[X]$ ist. Wir betrachten das ganze Ideal $\mathfrak{p} = p\mathcal{O}_K + f(w)\mathcal{O}_K$.
Behaupthung: $\mathfrak{p} \neq \mathcal{O}_K$.
Beweis: Anderenfalls wäre $1 \in p\mathcal{O}_K + f(w)\mathcal{O}_K$, d.h es gäbe $x, y \in \mathcal{O}_K$ mit $xp + yf(w) = 1$. Sei $g \in \mathbb{Z}[X]$ ein lineares Polynom mit $x = g(w)$ und sei $h \in \mathbb{Z}[X]$ ein lineares Polynom mit $y = h(w)$. Die Polynome g und h existieren, weil $(1, w)$ eine Ganzbasis ist. Dann gilt

$$g(w)p + h(w)f(w) - 1 = 0.$$

Daher gilt

$$f_w | (gp + hf - 1),$$

und modulo p betrachtet erhalten wir: $\bar{f}|\bar{f}_w|(\bar{h}\bar{f} - \bar{1})$. Also gilt $\bar{f}|\bar{1}$ in $\mathbb{Z}/p\mathbb{Z}[X]$, im Widerspruch dazu, dass $\bar{f}$ ein Primpolynom ist. Also ist p ein echtes Ideal.
Behauptung: $\mathfrak{p}$ ist ein Primideal.
Beweis: Seien $x, y \in \mathcal{O}_K$ mit $xy \in \mathfrak{p}$. Es existieren (lineare) Polynome $F, G \in \mathbb{Z}[X]$ mit $x = F(w), y = G(w)$. Wäre $(\bar{f}, \bar{F}\bar{G}) = 1 \in \mathbb{Z}/p\mathbb{Z}[X]$, so gäbe es Polynome $h, g \in \mathbb{Z}[X]$ mit $\bar{h}\bar{f} + \bar{g}\bar{F}\bar{G} = 1$. Hieraus folgt

$$1 \equiv h(w)f(w) + g(w)F(w)G(w) \;\; mod \, p\mathcal{O}_K.$$

Wegen $p\mathcal{O}_K \subset \mathfrak{p}, f(w) \in \mathfrak{p}$ und $F(w)G(w) = xy \in \mathfrak{p}$ erhalten wir den Widerspruch $1 \in \mathfrak{p}$. Damit wird $\bar{f}$ von einem der beiden Primpolynome $\bar{F}$ oder $\bar{G}$ geteilt. Je nachdem folgt $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. Also ist $\mathfrak{p}$ ein Primideal.
Nehmen wir nun an, dass f_w modulo p irreduzibel ist. Dann können wir $f = f_w$ setzen und es gilt $0 = f(w)$, folglich $\mathfrak{p} = p\mathcal{O}_K$.
Zerfällt f_w modulo p in die Linearfaktoren $\bar{f}_1$ und $\bar{f}_2$, dann gilt

$$0 = f_w(w) \equiv f_1(w)f_2(w) \, mod \, p\mathcal{O}_K.$$

Bilden wir die Primideale $\mathfrak{p}_1, \mathfrak{p}_2$ wie oben, so folgt, dass

$$\mathfrak{p}_1\mathfrak{p}_2 = p^2\mathcal{O}_K + pf_1(w)\mathcal{O}_K + pf_2(w)\mathcal{O}_K + f_1(w)f_2(w)\mathcal{O}_K \subset p\mathcal{O}_K.$$

Daher gilt $p\mathcal{O}_K | \mathfrak{p}_1\mathfrak{p}_2$ und es verbleiben die Möglichkeiten $p\mathcal{O}_K = \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_2$.
Wäre $p\mathcal{O}_K = \mathfrak{p}_1$, so wäre $f_1(w) \in p\mathcal{O}_K$. Also existiert ein Polynom $g \in \mathbb{Z}[X]$ mit $f_1(w) = pg(w)$. Es folgt $f_w|(f_1 - pg)$ und modulo p erhalten wir den Widerspruch $\bar{f}_w|\bar{f}_1$. Analog schließen wir die Möglichkeit $p\mathcal{O}_K = \mathfrak{p}_2$ aus und erhalten

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2.$$

Hat f_w modulo p eine Doppelnullstelle, so könnenn wir $f_1 = f_2$ wählen und erhalten $\mathfrak{p}_1 = \mathfrak{p}_2$. Es bleibt zu zeigen, dass $\bar{f}_1 \neq \bar{f}_2$ auch $\mathfrak{p}_1 \neq \mathfrak{p}_2$ impliziert. Dies folgt aus der linearen Kombinierbarkeit des grössten gemeinsamen Teilers. Wir wählen Polynome $g, h \in \mathbb{Z}[X]$ mit $\bar{f}_1\bar{g} + \bar{f}_2\bar{h} = 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Dann gibt es ein Polynom $F \in \mathbb{Z}[X]$ mit $f_1g + f_2h - pF = 1$. Einsetzen von w ergibt

$$f_1(w)g(w) + f_2(w)h(w) - pF(w) = 1.$$

Wäre nun $\mathfrak{p}_1 = \mathfrak{p}_2$, so wäre der Ausdruck auf der linken Seite in $\mathfrak{p}_1$ und wir erhalten einen Widerspruch. □

Definition 4.24. *Die Zahl*

$$\Delta_K = \left|\begin{pmatrix} 1 & w \\ 1 & \sigma(w) \end{pmatrix}\right|^2 = \begin{cases} 4d, & wenn\ d \not\equiv 1 \bmod 4, \\ d, & wenn\ d \equiv 1 \bmod 4. \end{cases}$$

Heisst die Diskriminante des quadratisches Zahlkörpers K.

Satz 4.25. *Eine Primzahl p ist genau dann in K verzweigt, wenn sie die Diskriminante Δ_K von K teilt.*

Beweis. Angenommen, die Primzahl p ist verzweigt in $\mathcal{O}_K$, das heisst $p\mathcal{O}_K = \mathfrak{p}^2$. Dann gilt $\sigma(\mathfrak{p})^2 = \sigma(p)\mathcal{O}_K = p\mathcal{O}_K = \mathfrak{p}^2$. Wegen der Eindeutigkeit der Primidealzerlegung folgt $\mathfrak{p} = \sigma(\mathfrak{p})$. Angenommen, für jedes $a + bw \in \mathfrak{p}$, wäre $b \in p\mathbb{Z}$. Dann wäre jedes auftretende $a \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Hieraus würde $\mathfrak{p} = p\mathcal{O}_K$ folgen. Also findet man $a, b \in \mathbb{Z}, 0 < b < p$ mit $a + bw \in \mathfrak{p}$. Wegen $\mathfrak{p} = \sigma(\mathfrak{p})$ ist auch $a + b\sigma(w) \in \mathfrak{p}$. Wir schliessen $b(w - \sigma(w)) \in \mathfrak{p}$ und $b^2\Delta_K \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Wegen $0 < b < p$ folgt $p|\Delta_K$.
Sei umgekehrt Δ_K durch p teilbar. Wir betrachten zunächst den Fall $d \not\equiv 1 \bmod 4$. Dann gilt $f_w = X^2 - d$. Für ungerades p folgt aus $p|\Delta_K$ auch $p|d$ und f_w hat modulo p eine doppelte Nullstelle. Modulo 2 hat $X^2 - d$ für ungerades d die Doppelnullstelle 1 und für geardes d die Doppelnullstelle 0. Nun betrachten wir den Fall $d \equiv 1 \bmod 4$. Dann gilt $\Delta_K = d$ und $f_w = X^2 - X - \frac{d-1}{4}$. Ein Diskriminantenteiler p ist notwendig ungerade und modulo p gilt $f_w = (X - 1/2)^2$. □

Korollar 4.26. *Mindestens eine und höchstens endlich viele Primzahlen verzweigen in K.*

Beweis. Folgt direkt von obige Satz und daraus dass der Betrag von Δ_K stets grösser als 1 ist. □

Theorem 4.27. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper mit Diskriminante Δ_K. Dann gilt:*

(1) Eine ungerade Primzahl p heisst in K
träge, wenn $(\frac{\Delta_K}{p}) = -1$,
zerlegt, wenn $(\frac{\Delta_K}{p}) = +1$,
verzweigt, wenn $(\frac{\Delta_K}{p}) = 0$.

(2) Die Primzahl 2 ist in K
träge, wenn $\Delta_K \equiv 5 \bmod 8$,
zerlegt, wenn $\Delta_K \equiv 1 \bmod 8$,
verzweigt, wenn $\Delta_K \equiv 0 \bmod 2$.

Beweis. Sei p ungerade. Ist $d \not\equiv 1 \bmod 4$, so ist das Minimalpolynom $f_w = X^2 - d$ genau dann, irreduzibel modulo p, wenn d kein quadratischer Rest modulo p ist. Wenn $d \equiv 1 \bmod 4$ ist, so gilt $f_w = X^2 - X - \frac{d-1}{4}$. Die Substitution $f_w(X + 1/2) = X^2 - d/4$ zeigt dann das gleiche Ergebnis. Nun betrachten wir den Fall $p = 2$. Ist $d \not\equiv 1 \bmod 4$, so ist $\Delta_K = 4d$ gerade und 2 ist verzweigt. Sei $\Delta_K = d \equiv 1 \bmod 4$. Dann ist f_w genau dann irreduzibel modulo 2, wenn $(d - 1)/4$ ungerade ist. □

5. Lokalisation und diskrete Evualationsringe

Fabian Roshardt, *fabiaros@student.ethz.ch*

5.1. **Lokalisation.** Wir folgen hier den Referenzen [4] und [1].
Im gesamten Kapitel sei A ein Integritätsbereich.
Sei $S \subseteq A\backslash\{0\}$ so, dass:
(1) $1 \in S$
(2) $\forall x, y \in S : xy \in S$

Wir definieren nun eine Relation $\equiv$ auf $A \times S$ folgendermassen: $(a, s) \equiv (b, t) \iff at - bs = 0$

Proposition 5.1. *$\equiv$ ist eine Äquivalenzrelation*

Beweis. Reflexivität und Symmetrie sind klar.

Transitivität: Sei $(a, s) \equiv (b, t) \wedge (b, t) \equiv (c, u) \implies at - bs = bu - ct = 0 \implies \begin{cases} aut = bsu \\ cst = bsu \end{cases}$

$\implies (au - cs)t = 0, t \in S \implies (a, s) \equiv (c, u)$ □

Wir bezeichnen nun mit $\frac{a}{s}$ die Äquivalenzklasse (a, s) und mit $S^{-1}A$ die Menge aller Äquivalenzklassen. Wir führen eine Ringstruktur auf $S^{-1}A$ folgendermassen ein:
$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$
$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$
Das Nullelement ist $\frac{0}{1}$, das Einselement $\frac{1}{1}$
Dies erinnert an die Konstruktion des Quotientenkörpers über einem Integritätsbereich. Der Beweis, dass die oben definierte Struktur tatsächlich ein Ring ist, ist analog zum Beweis beim Quotientenkörper. Ausserdem existiert wie beim Quotientenkörper ein Ringhomomorphismus, $f : A \to S^{-1}A, x \mapsto \frac{x}{1}$
In der Tat ist der Quotientenkörper ein Spezialfall der obigen Konstruktion, wähle $S = A\backslash\{0\}$

Beispiel 5.2. *$f \in A\backslash\{0\}, S = \{f^n\}_{n\in\mathbb{N}}$, schreibe $S^{-1}A = A_f$*

Beispiel 5.3. *Sei $\mathfrak{p}$ ein Primideal von A. Setze $S = A\backslash\mathfrak{p}$. Schreibe $A_\mathfrak{p}$ für $S^{-1}A$. Bemerke, dass der Quotientenkörper ein Spezialfall dieses Beispiels ist, denn falls A ein Integritätsbereich ist, so ist $\{0\}$ ein Primideal.*

Diese Ringe $A_\mathfrak{p}$ sind der wahrscheinlich wichtigste Fall und wir werden sie im Folgenden noch genauer untersuchen.

Beispiel 5.4. *Sei $A = \mathbb{Z}, \mathfrak{p} = (p), \mathbb{Z}_{(p)} = \{\frac{g}{h} | g, h \in \mathbb{Z}, p \nmid h\}$*

Ausserdem können wir die obige Konstruktion auf A-Module M erweitern. Sei wieder S wie oben. Definiere $\equiv$ auf $M \times S : (m, s) \equiv (m', s') \iff \exists t \in S : t(sm' - s'm) = 0$. Bezeichne mit $\frac{m}{s}$ eine Äquivalenzklasse und mit $S^{-1}M$ die Menge aller Äquivalenzklassen, $S^{-1}M$ ist wieder ein A-Modul. Die Addition ist wieder die gleiche wie oben, Multiplikation mit einem Ringelement ist gegeben durch:
$a \cdot \frac{m}{s} = \frac{am}{s}$
und falls $S = A\backslash\mathfrak{p}$ schreiben wir $M_\mathfrak{p}$ für $S^{-1}M$. Nun beweisen wir noch folgenden Satz:

Satz 5.5. *Die Primideale $\mathfrak{Q}$ von $S^{-1}A$ stehen in $1-1$ Korrespondenz mit den Primidealen $\mathfrak{q}$ von A, welche S nicht schneiden: $\mathfrak{q} \mapsto S^{-1}\mathfrak{q} = \{\frac{q}{s} | q \in \mathfrak{q}, s \in S\}, \mathfrak{Q} \mapsto \mathfrak{Q} \cap A$*

Beweis. Zuerst beweisen wir: $\mathfrak{Q} = S^{-1}q$ ist ein Primideal von $S^{-1}A$. Sei $\frac{a}{s} \cdot \frac{b}{t} = \frac{q}{u} \in \mathfrak{Q} \implies abu - stq = 0 \implies abu \in \mathfrak{q}$, aber $u \in S$, also nicht in $\mathfrak{q}$, also $(a \in \mathfrak{q} \vee b \in \mathfrak{q}) \implies (\frac{a}{s} \in \mathfrak{Q} \vee \frac{b}{t} \in \mathfrak{Q})$. Also $\mathfrak{Q}$ prim. Ausserdem gilt: $\mathfrak{q} = \mathfrak{Q} \cap A$. Denn: $\frac{q}{s} = a \implies q = sa$ aber wieder ist $s \notin \mathfrak{q}$, also $a \in \mathfrak{q}$
Sei nun $\mathfrak{Q}$ ein beliebiges Primideal von $S^{-1}A$. $\mathfrak{q} = \mathfrak{Q} \cap A$ ist ein Primideal von A, da es das Urbild eines Primideals unter einem Ringhomomorphismus ist. Ausserdem gilt: $\mathfrak{q}$ schneidet S nicht, denn sonst: Sei $s \in \mathfrak{q} \cap S \implies s \cdot \frac{1}{s} = 1 \in \mathfrak{Q}$, Widerspruch. Ausserdem gilt: $\mathfrak{Q} = S^{-1}\mathfrak{q}$, denn: $\frac{a}{s} \in \mathfrak{Q} \implies a = s\frac{a}{s} \in \mathfrak{Q} \cap A = \mathfrak{q} \implies \frac{a}{s} \in S^{-1}\mathfrak{q}$. Also sind die oben gegebenen Abbildungen zueinander invers und wir sind fertig. □

Definition 5.6. *Ein Ring, welcher genau ein maximales Ideal besitzt, heisst **lokaler Ring**.*

Korollar 5.7. *Sei $\mathfrak{p}$ ein Primideal, dann ist $A_\mathfrak{p}$ ein lokaler Ring*

Beweis. Die Primideale von $A_\mathfrak{p}$ entsprechen den Primidealen, welche nicht $S = A\backslash\mathfrak{p}$ schneiden, also in $\mathfrak{p}$ enthalten sind. Also ist das Primideal in $A_\mathfrak{p}$, welches mit $\mathfrak{p}$ korrespondiert, das einzig maximale. □

5.2. **Diskrete Evaluationsringe.**

Definition 5.8. *Ein **diskreter Bewertungsring**, auch **diskreter Evaluationsring** genannt, ist ein Hauptidealring $\mathfrak{o}$ mit einem einzigen maximalen Ideal $\mathfrak{p} \neq 0$*

Beispiel 5.9. *Der Ring der formalen Potenzreihen, $k[[X]]$, in einer Variable. Das einzige maximale Ideal ist (X).*

Beispiel 5.10. *Der Ring $\mathbb{Z}_p$ der ganzen p-adischen Zahlen. Für weitere Information siehe [2]*

Definition 5.11. *Eine Primidealkette der Länge n ist eine Kette von Primidealen*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \mathfrak{p}_n \tag{5.1}$$

*Die **Krull-Dimension** eines Ringes A ist das Supremum aller Längen solcher Ketten in A.*

Proposition 5.12. *Ein Hauptidealring hat Krull-Dimension 0 oder 1.*

Beweis. Nehme per Widerspruch an $\exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$, da wir einen Hauptidealring haben sei $\mathfrak{p}_1 = (a), a \neq 0, \mathfrak{p}_2 = (b)$. Dann haben wir: $a \in \mathfrak{p}_2$, also $b \cdot k = a$, aber $\mathfrak{p}_1$ ist ein Primideal, also folgt $k \in (a)$, also $k = c \cdot a$. Aber dann folgt $a = k\dot{b} = a \cdot c \cdot b$, also wäre b eine Einheit, Widerspruch. □

Bemerkung 5.13. Ein Integritätsbereich hat Krull-Dimension 0 genau dann wenn er ein Körper ist.

Korollar 5.14. *Ein diskreter Evaluationsring besitzt genau 2 Primideale.*

Wir schauen uns nun ein paar weitere Eigenschaften eines diskreten Evaluationsrings an. Sei das maximale Ideal $\mathfrak{p}$ durch ein Primelement π erzeugt, d.h. $(\pi) = \mathfrak{p}$. Da in einem beliebigen Ring jedes Element, welches in keinem maximalen Ideal enthalten ist, eine Einheit ist, bedeutet dies insbesondere hier: Jedes Element, welches nicht in $\mathfrak{p}$ liegt, ist eine Einheit. Nach Korollar 5.14 ist $\mathfrak{p}$ das einzige Primideal abgesehen von $\{0\}$, also ist π bis auf Assoziiertheit das einzige Primelement. Daher folgt: $\forall a \in \mathfrak{o} - \{0\} : \exists \epsilon \in \mathfrak{o}^* : a = \epsilon\pi^n, n \geqslant 0$. Allgemeiner: Im Quotientenkörper K gilt:

$$\forall a \in K^* : \exists \epsilon \in \mathfrak{o}^* : a = \epsilon\pi^n, n \in \mathbb{Z} \tag{5.2}$$

Bemerkung 5.15. Es gilt insbesondere, $\forall a \in K^* : a \in \mathfrak{o}$ oder $a^{-1} \in \mathfrak{o}$

Definition 5.16. *Der Exponent n in 5.2 heisst die* ***Bewertung*** *von a.*

Wir können die Bewertung als eine Funktion: $v : K^* \to \mathbb{Z}$ interpretieren. Wie können sie auf ganz K erweitern, indem wir $v(0) = \infty$ setzen. Es gilt: $(a) = \mathfrak{p}^{v(a)}$. Ausserdem gelten folgende Gleichungen:

$$(ii) \quad v(ab) = v(a) + v(b), \quad (iii) \quad v(a+b) \geqslant \min\{v(a), v(b)\} \tag{5.3}$$

Definition 5.17. *Ein Ring heisst* ***noethersch****, wenn jede aufsteigende Folge von Idealen*

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_i \ldots \tag{5.4}$$

stationär wird, d.h. $\exists n_0$ so, dass $\forall n \geqslant n_0 : \mathfrak{a}_n = \mathfrak{a}_{n_0}$

Satz 5.18. *Jeder Hauptidealring ist noethersch*

Beweis. Sei $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \ldots$ eine aufsteigende Folge von Idealen. Wir nehmen $\bigcup_{i=1}^{\infty} \mathfrak{a}_i$, dies ist wieder ein Ideal. Da wir in einem Hauptidealring sind, ist es durch ein Element erzeugt, sagen wir $\bigcup_{i=1}^{\infty} \mathfrak{a}_i = (b)$, nun $\exists n_0$ so, dass $b \in \mathfrak{a}_{n_0}$ und wir sind fertig. □

Wir möchten nun eine äquivalente Charakterisierung eines diskreten Evaluationsrings sehen, dafür müssen wir noch gewisse Definitionen einführen.

Definition 5.19. *Seien $A \subseteq B$ Ringe, wir sagen $x \in B$ ist* ***ganz*** *über A, falls x eine Nullstelle eines monischen Polynoms mit Koeffizienten in A ist, d.h.*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_i \in A, n \geqslant 1 \tag{5.5}$$

Definition 5.20. *Die Menge $C = \{x \in B | x$ ist ganz über $A\}$ heisst der* ***ganze Abschluss*** *von A in B.*
Falls $C = A$ heisst A ***ganz abgeschlossen*** *in B.*
Falls $C = B$ heisst B ***ganz*** *über A.*

Definition 5.21. *Ein Integritätsbereich A, welcher in seinem Quotientenkörper ganz abgeschlossen ist, heisst* ***normal****.*

Beispiel 5.22. *Die Ringe $\mathbb{Z}$ und $\mathbb{Z}[i]$ sind beide normal.*

Beispiel 5.23. *Die Ringe $\mathbb{Z}[di], d > 1$ sind nicht normal, denn i liegt im Quotientenkörper und nicht in $\mathbb{Z}[di]$, ist aber ganz über $\mathbb{Z}[di]$*

Wir beweisen nun einen Teil des folgende Satzes:

Satz 5.24. *Sei A ein Integritätsbereich. Folgende Aussagen sind äquivalent:*

(i) A ist ein diskreter Evaluationsring
(ii) A ist ein normaler noetherscher lokaler Ring mit Krull-Dimension 1.

Beweis. $(i) \implies (ii)$ Laut 5.18 und 5.12 zusammen mit 5.13 reicht es zu zeigen: A ist normal. Sei also K der Quotientenkörper von A. Sei $x \in K\backslash\{0\}$ so, dass $x^n + a_1x^{n-1} \dots a_n = 0$, Laut 5.15 gilt $x \in A$ oder $x^{-1} \in A$. Im ersten Fall sind wir fertig, im zweiten gilt: $x = -(a_1 + a_2x^{-1} + \dots + a_nx^{1-n})$, also ebenfalls $x \in A$

Die andere Richtung werden wir hier nicht beweisen, denn hierzu bräuchten wir noch etwas mehr Theorie zur Ganzheit. Der Beweis findet sich in [1]. □

Wir können auch umgekehrt mit einer sogenannten Exponentialbewertung auf einem Körper starten und davon ausgehend einen diskreten Evaluationsring als Unterring dieses Körpers finden.

Definition 5.25. *Eine surjektive Funktion $v : K \to \mathbb{Z} \cup \{\infty\}$ auf einem Körper K mit den Eigenschaften (ii) und (iii) aus 5.3 zusammen mit:*

(i) $v(x) = \infty \iff x = 0$

*heisst eine **Exponentialbewertung, diskrete Bewertung** oder **nicht-archimedische Bewertung**.*

Bemerkung 5.26. $v(1) = v(-1) = 0, \forall x \in K^* : v(x^{-1}) = -v(x)$

Es folgt aus den Bedingungen direkt folgender Satz:

Satz 5.27. *Sei v eine Exponentialbewertung, K ein Körper. Es ist*

$\mathfrak{o} = \{x \in K | v(x) \geqslant 0\}$

ein Ring mit der Einheitengruppe

$\mathfrak{o}^* = \{x \in K | v(x) = 0\}$

die einzigen Ideale von $\mathfrak{o}$ sind von der Form

$\mathfrak{a} = \{x \in K | v(x) \geqslant d, d \in \mathbb{N} \cup \{\infty\}\}$

und das einzige maximale Ideal ist

$\mathfrak{p} = \{x \in K | v(x) > 0\}$

Beispiel 5.28. *Sei $K = \mathbb{Q}$, sei p eine Primzahl. Jedes $x \in Q^*$ kann eindeutig geschrieben werden als: $x = p^n \cdot \frac{a}{b}$ so, dass $ggt(a, b) = 1, p \nmid a, b$. Dann ist: $v : \mathbb{Q}^* \to \mathbb{Z}, p^n \frac{a}{b} \mapsto n$ eine Exponentialbewertung, wenn wir $v(0) = \infty$ setzen, und es gilt: $\mathfrak{o} = \{x \in K | v(x) \geqslant 0\} = \mathbb{Z}_{(p)}$*

Wir geben nun eine letzte Konstruktion von diskreten Evaluationsringen an; Falls wir einen sogenannten Dedekindring (siehe später in der Vorlesung) an einem Primideal $\mathfrak{p} \neq \{0\}$ lokalisieren, ist der enstehende Ring ein diskreter Evaluationsring.

Beispiel 5.29. $\mathbb{Z}_{(p)}$

6. Dedekind Ringe und Klassengruppen, Teil I

Benjamin Reinhard, *breinhar@student.ethz.ch*

In den folgenden Seiten wollen wir die Dedekindringe einführen, welche eine Grundlage für die Faktorisierung von Idealen bilden. Bis dahin müssen wir erstmals unsere Kenntnisse über die Ganzheit ausbauen und dafür werden Module nützlich sein, welche in Kommutativer Algebra sehr genau behandelt werden.

Unsere wichtigste Anwendung dieser Theorie ist beim Ring der ganzen Zahlen eines algebraischen Zahlkörpers. Wir wollen letztendlich zeigen, dass dieser ein Dedekindring ist und dafür müssen wir die bisher bekannten Werkzeuge Spur und Diskriminante auf allgemeine algebraische Zahlkörper erweitern.

6.1. Module.

In diesem Abschnitt führen wir Module ein. Sie stellen eine Verallgemeinerung der Vektorräume dar und die meisten Eigenschaften lassen sich auch übertragen. Die Aussagen werden wir aber nicht beweisen, man findet sie ganz einfach in Textbüchern auf dem Internet.

Sei A ein Ring. Man sollte sich $\mathbb{Z}$ als zentrales Beispiel vorstellen.

Definition 6.1. *Ein Tupel $(M, +, \cdot, 0)$ mit $0 \in M$ und Abbildungen*

$$+ : M \times M \to M$$

$$\cdot : A \times M \to M$$

nennen wir ein A-Modul, falls für alle $m, m_1, m_2 \in M$ und $a, a_1, a_2 \in A$ gilt

- $(M, +, 0)$ *ist eine abelsche Gruppe.*
- $(a_1 a_2) \cdot m = a_1 \cdot (a_2 \cdot m)$
- $(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m$
- $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$
- $1 \cdot m = m$

Beispiel 6.2.

(1) Jeder K-Vektorraum ist ein K-Modul.
(2) Seien $A \subseteq B$ Ringe, so ist B ein A-Modul via $\cdot : A \times B \to B, (a, b) \mapsto ab$.

Sei M ein A-Modul.

Definition 6.3. *Sei I eine Indexmenge, so sagen wir $\{m_i \in M : i \in I\}$ erzeugt M, falls*

$$M = \left\{ \sum_{j \in J} a_j m_j : J \subseteq I \text{ endlich}, \ a_i \in A \right\}$$

und nennen die Menge A-linear unabhängig, falls

$$\sum_{j \in J} a_j m_j = 0 \text{ und } a_j \in A, \ J \subseteq I \text{ endlich} \Rightarrow a_j = 0.$$

Letztendlich nennen wir die Menge eine A-Basis, falls sie M erzeugen und A-linear unabhängig sind. M nennt man frei, falls es eine A-Basis besitzt.

Proposition-Definition 6.4. *Besitzt M zwei A-Basen, so ist ihre Anzahl gleich. Also ist*

$$\mathrm{Rang}(M) = \text{ Anzahl Elemente einer Basis}$$

wohldefiniert und heisst der Rang von B.

Lemma 6.5. *Ist A ein Hauptidealring und M frei, so ist jeder A-Untermodul $N \subseteq M$ frei und es gilt*

$$\mathrm{Rang}(N) \leqslant \mathrm{Rang}(M).$$

6.2. **Ganzheit.** Seien von nun an durchgehend $A \subseteq B$ Ringe.

Lemma 6.6. *Folgende Aussagen sind äquivalent:*

(1) $A[b_1, ..., b_n]$ ist ganz über A.
(2) $b_1, ..., b_n \in B$ sind ganz über A.
(3) $A[b_1, ..., b_n]$ ist ein endlich erzeugter A-Modul.

Beweis. (1) $\Rightarrow$ (2) ist klar, da $b_1, ..., b_n \in A[b_1, ..., b_n]$. Die Implikation (2) $\Rightarrow$ (3) überlasse ich dem/der Leser/in als Aufgabe. Ansonsten findet man die Lösung im Buch von Neukirch [4, Satz I.2.2]. Wir zeigen nun (3) $\Rightarrow$ (1). Sei $A[b_1, ..., b_n]$ endlich erzeugt, das heisst

$$A[b_1, ..., b_n] = A\omega_1 + ... + \omega_m \text{ für geeignete } \omega_i \in A[b_1, ..., b_n]$$

Sei nun $c \in A[b_1, ..., b_n]$ beliebig, wir zeigen, dass es ganz über A ist. Seien $a_{ij} \in A$, sodass $c\omega_i = \sum_{j=1}^m a_{ij}\omega_i$, $M(x)$ die Matrix mit Einträgen $x\delta_{ij} - a_{ij} \in A[x]$ und $f(x) = \det(M(x)) \in A[x]$ ein nicht-konstantes normiertes Polynom.

Eine Folgerung der Cramerschen Regel liefert uns eine Matrix $N(x) \in \mathrm{Mat}_{m \times m}(A)$ mit

$$N(x)M(x) = \det(M(x))I_m$$

und für $\omega = (\omega_1, ..., \omega_m)^T$ kann man nachrechnen, dass $M(c)\omega = 0$ gilt, also ist mit der obigen Gleichung

$$\omega_i \det(M(c)) = 0 \text{ für alle } i.$$

Da schliesslich $1 \in A[b_1 ... b_n]$ gilt, existieren $d_i \in A$, sodass $1 = \sum_{j=1}^m d_i\omega_i$ und daraus folgt $f(c) = 1 \cdot \det(M(c)) = \sum_{j=1}^m d_i\omega_i \det(M(c)) = 0$. Also ist c ganz über A. □

Lemma 6.7. *Seien $A \subseteq B \subseteq C$ Ringe, C ganz über B und B ganz über A, so ist C ganz über A.*

Beweis. Sei $c \in C$ so existiert ein $f \in B[x]$ mit $f(c) = c^n + b_{n-1}c^{n-1} ... + b_0 = 0$ und somit ist c ganz über $R = A[b_{n-1}, ..., b_0]$. Da nun $b_{n-1}, ..., b_0$ ganz über A sind, ist wegen Lemma 6.6 R ein endlich erzeugter A-Modul und auch $R[c]$ ein endlich erzeugter R-Modul. Daraus kann man einfach schliessen, dass $R[c] = A[b_{n-1}, ..., b_0, c]$ ein endlich erzeugter A-Modul ist und somit wieder wegen Lemma 6.6 c ganz über A ist. □

Satz 6.8. *Der ganze Abschluss $\bar{A}$ von A in B ist ein Ring.*

Beweis. Es ist klar, dass $0, 1 \in \bar{A}$ gilt. Seien nun $b_1, b_2 \in \bar{A}$, so ist laut Lemma 6.6 $A[b_1, b_2]$ ganz über A und da $b_1 + b_2, -b_1, b_1 b_2 \in A[b_1, b_2]$, so sind $b_1 + b_2, -b_1, b_1 b_2$ ganz über A, also liegen sie in $\bar{A}$. Alle restlichen Ringeigenschaften folgen aus $\bar{A} \subseteq B$. □

Wir betrachten kurz unser zentrales Beispiel. Sei von nun an $K/\mathbb{Q}$ ein algebraischer Zahlkörper.

Definition 6.9. *Wir definieren den Ring der ganzen Zahlen von K als*

$$\mathcal{O}_K := \mathbb{Z}_K := \{b \in K : b \text{ ganz über } \mathbb{Z}\}.$$

Bemerkung 6.10. Die bisher definierten quadratischen Zahlringe sind die ganzen Zahlen von $\mathbb{Q}(\sqrt{d})$

$$\mathcal{O}_d = \{b \in \mathbb{Q}(\sqrt{d}) : \mathrm{tr}(b) \in \mathbb{Z}, \mathrm{N}(b) \in \mathbb{Z}\} = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

Sei $b \in \mathcal{O}_d$, so ist b die Nullstelle des Polynoms $x^2 - \mathrm{tr}(b)x + \mathrm{N}(b)$, wobei die Koeffizienten per Voraussetzung in $\mathbb{Z}$ liegen. Also liegt b in $\mathcal{O}_{\mathbb{Q}(\sqrt{b})}$.

Umgekehrt ist $b = x + \sqrt{d}y \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, so existiert ein nicht-konstantes, normiertes Polynom $f \in \mathbb{Z}[x]$ mit $f(b) = 0$. Es gilt $f(x - \sqrt{d}y) = f(\bar{b}) = \overline{f(b)} = 0$, also ist $\bar{b}$ auch in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ und da $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ein Ring ist, ist $\mathrm{tr}(b) = b + \bar{b} = 2x, \mathrm{N}(b) = b\bar{b} = x^2 + y^2$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Also sind $\mathrm{tr}(b), \mathrm{N}(b)$ ganz über $\mathbb{Z}$ und liegen offensichtlich in $\mathbb{Q}$. Es ist nun dem/der Leser/in überlassen zu zeigen, dass $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \cap \mathbb{Q} = \mathbb{Z}$ gilt. Daraus schliessen wir, dass $\mathrm{tr}(b)$ und $\mathrm{N}(b)$ tatsächlich in $\mathbb{Z}$ liegen und somit b in $\mathcal{O}_d$.

6.3. **Spur und Diskriminante.** Da $\mathbb{Z} \subseteq \mathcal{O}_K$ gilt, können wir $\mathcal{O}_K$ als $\mathbb{Z}$-Modul auffassen. Genauso können wir K als $\mathbb{Q}$-Vektorraum auffassen und da er per Definition endlich ist, besitzt er eine endliche $\mathbb{Q}$-Basis. Unser nächstes grosses Ziel ist es zu zeigen, dass $\mathcal{O}_K$ eine endliche $\mathbb{Z}$-Basis besitzt.

Proposition-Definition 6.11. *Sei $v \in K$, so ist $T_v : K \to K, x \mapsto vx$ $\mathbb{Q}$-linear. Die Abbildung*

$$\mathrm{Tr}_{K/\mathbb{Q}} : K \to \mathbb{Q}, \ v \mapsto \mathrm{trace}(T_v)$$

nennen wir Spur und sie ist auch $\mathbb{Q}$-linear.

Der Beweis ist nicht schwierig und ist dem/der Leser/in überlassen.

Bemerkung 6.12. Die bisher definierte Spur für quadratische Zahlkörper

$$\mathrm{tr} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, a + b\sqrt{d} \mapsto 2a$$

stimmt mit der oben definierten Spur überein.

Proposition 6.13. *Folgende Abbildung ist eine nicht-ausgeartete $\mathbb{Q}$-Bilinearform*

$$\beta : K \times K \to \mathbb{Q}, (v, w) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(vw)$$

Dies ist ebenfalls nicht schwierig zu beweisen.

Definition 6.14. *Sei $v_1, ..., v_n \in K$ eine $\mathbb{Q}$-Basis von K, so definieren wir*

$$d(v_1, ..., v_n) := \det\left((\beta(v_i, v_j))_{ij}\right)$$

als die Diskriminante der Basis.

Bemerkung 6.15. Man kann zeigen, dass $K = (\mathbb{Z}\backslash\{0\})^{-1}\mathcal{O}_K$ gilt, also jedes Element von K dargestellt werden kann als $\frac{b}{a}$, wobei $b \in \mathcal{O}_K$ und $a \in \mathbb{Z}\backslash\{0\}$ liegt. Ist also $v_1 = \frac{b_1}{a_1}, ..., v_n = \frac{b_n}{a_n}$ eine $\mathbb{Q}$-Basis von K, so ist es leicht zu sehen, dass $b_1, ..., b_n$ auch eine $\mathbb{Q}$-Basis von K.

Lemma 6.16. *Sei $b_1, ..., b_n$ eine in $\mathcal{O}_K$ gelegene $\mathbb{Q}$-Basis von K und d die Diskriminante, so gilt*

$$d\mathcal{O}_K \subseteq \mathbb{Z}b_1 + ... + \mathbb{Z}b_n.$$

Beweis. Sei $b \in \mathcal{O}_K$ mit $b = \sum_{i=1}^n \lambda_i b_i$ für $\lambda_i \in \mathbb{Q}$, so gilt $\beta(b_i, b) = \sum_{j=1}^n \beta(b_i, b_j)\lambda_j$ und somit

$$(\beta(b_1, b), ..., \beta(b_n, b))^T = M(\lambda_1, ..., \lambda_n)^T$$

wobei $M = (\beta(b_i, b_j))_{ij}$ ist. Im Buch von Neukirch [4] auf Seite 12 wird erklärt, dass wenn b ganz über $\mathbb{Z}$ ist, so ist $\mathrm{Tr}_{K/\mathbb{Q}}(b)$ in $\mathbb{Z}$ und daraus folgt, dass e und M Einträge in $\mathbb{Z}$ haben. Neukirch

erklärt auch in [4, Satz I.2.8], dass $\det(M) = d \neq 0$ und somit können wir die Cramersche Regel anwenden, um geeignete $a_i \in \mathbb{Z}$ mit $\lambda_i = \frac{a_i}{d}$ zu erhalten, also $d\lambda_i = a_i$. Dies ergibt

$$db = \sum_{i=1}^{n} d\lambda_i b_i = \sum_{i=1}^{n} a_i b_i \in \mathbb{Z}b_1 + ... + \mathbb{Z}b_n.$$

□

Satz 6.17. *$\mathcal{O}_K$ besitzt eine endliche $\mathbb{Z}$-Basis mit* $\mathrm{Rang}(\mathcal{O}_K) = [K : \mathbb{Q}]$.

Beweis. Seien $b_1, ..., b_n$ und d wie im Lemma 6.16, so kann man einfach überprüfen, dass $M := \mathbb{Z}b_1 + ... + \mathbb{Z}b_n$ ein freier $\mathbb{Z}$-Modul ist mit $\mathrm{Rang}(M) = n$. Nun ist $d\mathcal{O}_K$ auch ein $\mathbb{Z}$-Modul mit $d\mathcal{O}_K \subseteq M$ und $\mathbb{Z}$ ein Hauptidealring, so erhalten wir aus Lemma 6.5, dass $d\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul ist mit $m = \mathrm{Rang}(d\mathcal{O}_K) \leqslant n$.

Sei $de_1, ..., de_m \in d\mathcal{O}_K$ eine $\mathbb{Z}$-Basis von $d\mathcal{O}_K$, so ist offensichtlich $e_1, ..., e_n \in \mathcal{O}_K$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$.

Letztendlich haben wir $N := \mathbb{Z}b_1 + ... + \mathbb{Z}b_n \subseteq \mathcal{O}_K$ und N ist offensichtlich auch ein freier $\mathbb{Z}$-Modul mit $\mathrm{Rang}(N) = n$, also folgt wieder aus Lemma 6.5

$$n = \mathrm{Rang}(N) \leqslant \mathrm{Rang}(\mathcal{O}_K) = m \leqslant \mathrm{Rang}(M) = n$$

und somit $\mathrm{Rang}(\mathcal{O}_K) = m = n = [K : \mathbb{Q}]$. □

Korollar 6.18. *Ist $b_1, ..., b_n \in \mathcal{O}_K$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$, so ist $b_1, ..., b_n$ eine $\mathbb{Q}$-Basis von K.*

Beweis. Wir zeigen zuerst, dass $b_1..., b_n$ $\mathbb{Q}$-linear unabhängig sind. Sei also $\sum_{i=1}^{n} \frac{p_i}{q_i} b_i = 0$, so erhält man durch Umformen $c\sum_{i=1}^{n} c_i p_i b_i = 0$, wobei $c = \prod_{j=1}^{n} q_j$ und $c_i = \prod_{j \neq i} q_j$ ist. Da c nicht Null ist, muss $\sum_{i=1}^{n} c_i p_i b_i = 0$ sein und somit $c_i p_i = 0$ für alle i, da $b_1, ..., b_n$ $\mathbb{Z}$-linear unabhängig sind. Nun wegen $c_i \neq 0$ für alle i erhält man $p_i = 0$ und somit sind alle $\frac{p_i}{q_i}$ Null.

Also sind $b_1, ..., b_n$ $\mathbb{Q}$-linear unabhängig mit $n = [K : \mathbb{Q}]$. Aus der linearen Algebra wissen wir, dass $b_1..., b_n$ deswegen erzeugend sind und somit eine $\mathbb{Q}$-Basis bilden. □

6.4. **Noethersch.** Wir wollen kurz zeigen, dass $\mathcal{O}_K$ noethersch ist.

Lemma 6.19. *Ist B/I endlich für jedes Ideal $I \neq 0$, so ist B noehtersch.*

Beweis. Sei $B_0 \subseteq B_1 \subseteq ...$ eine aufsteigende Folge von Idealen in B, so ist auch $B_0/B_0 \subseteq B_1/B_0 \subseteq ...$ eine aufsteigende Folge in B/B_0 und da B/B_0 endlich ist, muss es ein n geben mit $B_i/B_0 = B_n/B_0$ für alle $i \geqslant n$ und somit auch $B_i = B_n$. □

Satz 6.20. *$\mathcal{O}_K$ ist noehtersch.*

Beweis. Sei $I \subseteq \mathcal{O}_K$ ein Ideal ungleich Null. Wir zeigen zuerst, dass $I \cap \mathbb{Z} \supsetneq 0$ gilt. Da I nicht Null ist, haben wir $0 \neq b \in I \subseteq \mathcal{O}_K$ und somit ist b ganz über $\mathbb{Z}$, also existiert ein $f \in \mathbb{Z}[x]$ mit $f(b) = b^n + ... + a_0 = 0$. Falls a_0 nicht Null ist, sieht man anhand der Gliechung, dass es in I liegen muss. Ansonsten ist es einfach zu folgern, dass ein anderes a_i in I liegen muss.

Sei nun $a \in I \cap \mathbb{Z}$, so gilt $a\mathcal{O}_K \subseteq I$ und somit $\mathcal{O}_K/I \subseteq \mathcal{O}_K/a\mathcal{O}_K$. Nun wir wissen, dass $\mathcal{O}_K$ eine $\mathbb{Z}$-Basis besitzt, also gilt $\mathcal{O}_K \simeq \mathbb{Z}^n$ als abelsche Gruppen, sowie auch $a\mathcal{O}_K \simeq a\mathbb{Z}^n$. Wir erhalten

$$\mathbb{Z}^n/a\mathbb{Z}^n \simeq \mathbb{Z}/a\mathbb{Z} \oplus ... \oplus \mathbb{Z}/a\mathbb{Z}$$

und daraus folgt, dass $\mathbb{Z}^n/a\mathbb{Z}^n$ endlich ist und somit auch $\mathcal{O}_K/I$. Wegen Lemma 6.19 folgt der Satz. □

6.5. **Dedekindringe.** Wir sind jetzt soweit, die Dedekindringe einzuführen.

Definition 6.21. *Ein noetherscher, normaler Integritätsbereich, bei dem jedes von Null verschiedene Primideal ein Maximalideal ist, nennen wir Dedekindring.*

Lemma 6.22. *Ist B ganz über A, so ist B ein Körper genau dann, wenn A ein Körper ist.*

Beweis. Sei B ein Körper, so reicht es zu zeigen, dass jedes Element in A ein multiplikatives Inverses in A besitzt. Sei also $a \in A$, so ist $a^{-1} \in B$. Da B ganz über A ist, existiert ein normiertes Polynom $f \in A[x]$ mit $f(a^{-1}) = (a^{-1})^n + ... + a_0 = 0$. Durch Umformen erhält man

$$a(-a_0 a^{n-1} - ... - a_{n-1}) = 1.$$

Also gilt $a^{-1} = (-a_0 a^{n-1} - ... - a_{n-1}) \in A$. Umgekehrt sei A ein Körper. Es reicht zu zeigen, dass jedes Element in B ein multiplikatives Inverses besitzt. Sei also $b \in B$, so existiert ein normiertes Polynom $f \in A[x]$ mit $f(b) = b^n + ... + a_0 = 0$. Durch Umformen erhält man

$$b(b^{n-1} + ... + a_1)(-a_0^{-1}) = 1.$$

Man bemerke, dass a_0^{-1} existiert, da A ein Körper ist. Also gilt $b^{-1} = (b^{n-1} + ... + a_1)(-a_0^{-1})$. □

Satz 6.23. *$\mathcal{O}_K$ ist ein Dedekindring.*

Beweis. Noethersch wurde in Satz 6.20 gezeigt. Wir zeigen Nomralität. Sei $E \subseteq K$ der Quotientenkörper von $\mathcal{O}_K$ und C der ganze Abschluss von $\mathcal{O}_K$ in E, so ist offensichtlich C ganz über $\mathcal{O}_K$ und per Definition $\mathcal{O}_K$ ganz über $\mathbb{Z}$. Also folgt aus Lemma 6.7, dass C ganz über $\mathbb{Z}$ ist und somit $C \subseteq \mathcal{O}_K$. Die andere Inklusion ist klar.

Nun sei $\mathfrak{p} \subseteq \mathcal{O}_K$ ein von Null verschiedenes Ideal. Wir zeigen, dass $\mathcal{O}_K/\mathfrak{p}$ ein Körper ist, woraus folgt, dass $\mathfrak{p}$ maximal ist. $\mathfrak{p} \cap \mathbb{Z}$ ist ein Primideal in $\mathbb{Z}$ und deswegen von der Form $\mathbb{Z}/p\mathbb{Z}$ für ein Primelement $p \in \mathbb{Z}$. Wir können $\mathbb{Z}/p\mathbb{Z}$ ganz einfach in $\mathcal{O}_K/\mathfrak{p}$ einbetten mit folgender Abbildung

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p},\ z + p\mathbb{Z} \mapsto z + \mathfrak{p}$$

und es ist auch nicht schwierig zu zeigen, dass $\mathcal{O}_K/\mathfrak{p}$ ganz über $\mathbb{Z}/p\mathbb{Z}$ ist. Da nun $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, folgt nach Lemma 6.22, dass $\mathcal{O}_K/\mathfrak{p}$ ein Körper ist. □

7. Dedekind Ringe und Klassengruppen, Teil II

Ana Marija Vego, *avego@student.ethz.ch*

7.1. **Gebrochene Ideale.** Im folgenden Abschnitt bezeichnet $\mathcal{O}$ einen beliebigen Dedekindring, und K seinen Quotientenkörper.

Lemma 7.1. *Zu jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}$, existiert ein $r \in \mathbb{N}$ und von Null verschiedene Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ mit*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r$$

Beweis: Sei M die Menge aller Ideale $\mathfrak{a}$ s.d. keine Primideale mit der obigen Eigenschaft existieren. Angenommen M sei nicht leer. Da $\mathcal{O}$ noethersch ist, bricht jede aufsteigende Idealkette ab. M ist daher hinsichtlich der Inklusion induktiv geordnet und besitzt somit nach dem Zornschen Lemma ein maximales Element $\mathfrak{a}$. Dieses kann kein Primideal sein, d.h. es gibt Elemente $b_1, b_2 \in \mathcal{O}$ mit $b_1 b_2 \in \mathfrak{a}$, aber $b_1, b_2 \notin \mathfrak{a}$. Setzen wir $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$, $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$, so ist $\mathfrak{a} \subsetneq \mathfrak{a}_1$, $\mathfrak{a} \subsetneq \mathfrak{a}_2$ und $\mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a}$. Wegen der Maximalität enthalten $\mathfrak{a}_1$ und $\mathfrak{a}_2$ Primidealprodukte, deren Produkt in $\mathfrak{a}$ liegt, Widerspruch. □

Lemma 7.2. *Ist $\mathfrak{p}$ ein Primideal von $\mathcal{O}$ und*

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\}$$

so ist $\mathfrak{a}\mathfrak{p}^{-1} := \left\{\sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\right\} \neq \mathfrak{a}$ für jedes Ideal $\mathfrak{a} \neq 0$.

Beweis: Sei $a \in \mathfrak{p}, a \neq 0$, und $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ mit minimalem r, wobei $\mathfrak{p}_1$, ..., $\mathfrak{p}_r$ Primideale wie in Lemma 1.1 sind. Dann ist eines der $\mathfrak{p}_i$, o.B.d.A. $\mathfrak{p}_1$, in $\mathfrak{p}$ enthalten, also $\mathfrak{p}_1 = \mathfrak{p}$ wegen der Maximalität von $\mathfrak{p}_1$. Denn sonst gäbe es für jedes i ein $a_i \in \mathfrak{p}_i \backslash \mathfrak{p}$ mit $a_1 \ldots a_r \in \mathfrak{p}$. Wegen $\mathfrak{p}_2 \ldots \mathfrak{p}_r \subsetneq (a)$ gibt es ein $b \in \mathfrak{p}_2 \ldots \mathfrak{p}_r$ mit $b \notin a\mathcal{O}$ also $a^{-1}b \notin \mathcal{O}$. Andererseits ist aber $b\mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$, und somit $a^{-1}b \in \mathfrak{p}^{-1}$. Damit ist $\mathfrak{p}^{-1} \neq \mathcal{O}$. Sei nun $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}$ und $\alpha_1, \ldots, \alpha_n$ ein Erzeugendensystem. Nehmen wir an, das $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Dann ist für jedes $x \in \mathfrak{p}^{-1}$

$$x\alpha_i = \sum_j a_{ij}\alpha_j, \quad a_{ij} \in \mathcal{O}$$

Ist A die Matrix $(x\delta_{ij} - a_{ij})$, so ist also $A(\alpha_1, \ldots, \alpha_n)^t = \underline{0}$. Für die Determinante $d := det(A)$ folgt $d\alpha_1 = \ldots = d\alpha_n = 0$ und somit $d = 0$. Daher ist x als Nullstelle des normierten Polynoms $f(x) = det(X\delta_{ij} - a_{ij}) \in \mathcal{O}[X]$ ganz über $\mathcal{O}$, d.h. $x \in \mathcal{O}$. Es ergibt sich somit $\mathfrak{p}^{-1} = \mathcal{O}$, Wiederspruch. □

Theorem 7.3. *Jedes von* (0) *und* (1) *verschiedene Ideal* $\mathfrak{a}$ *von* $\mathcal{O}$ *besitzt eine, bis auf Vertauschung, eindeutige Zerlegung*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

in Primideale $\mathfrak{p}_i$ *von* $\mathcal{O}$.

Beweis:
I. Existenz der Primzerlegung.
Sei $\mathfrak{M}$ *die Menge aller von (0) und (1) verschiedenen Ideale, die keine Primzerlegung besitzen. Ist* $\mathfrak{M}$ *nicht leer, so schließen wir wie bei (1.1), dass es ein maximales Element, sage* $\mathfrak{a}$, *in* $\mathfrak{M}$ *gibt. Es liegt in einem maximalen Ideal* $\mathfrak{p}$, *und wir erhalten wegen* $\mathcal{O} \subseteq \mathfrak{p}^{-1}$*:*

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$$

Nach Lemma 1.2 ist $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ *und* $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. *Da* $\mathfrak{p}$ *ein maximales Ideal ist, so folgt* $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. *Wegen der Maximalität von* $\mathfrak{a}$ *in* $\mathfrak{M}$ *und wegen* $\mathfrak{a} \neq \mathfrak{p}$, *also* $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$, *besitzt* $\mathfrak{a}\mathfrak{p}^{-1}$ *eine Primzerlegung* $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ *also auch* $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p}$, *Widerspruch.*
II. Eindeutigkeit der Primzerlegung.
Für ein Primideal $\mathfrak{p}$ *gilt nach Definition:* $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ *oder* $\mathfrak{b} \subseteq \mathfrak{p}$, *d.h.* $\mathfrak{p}|\mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p}|\mathfrak{a}$ *oder* $\mathfrak{p}|\mathfrak{b}$. *Seien nun*

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s$$

zwei Primzerlegungen von $\mathfrak{a}$. *Dann teilt* $\mathfrak{p}_1$ *einen Faktor* $\mathfrak{q}_i$, *etwa* $\mathfrak{q}_1$, *und ist wegen der Maximalität* $= \mathfrak{q}_1$. *Wir multiplizieren mit* $\mathfrak{p}_1^{-1}$ *und erhalten wegen* $\mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s$$

So fortfahrend erhalten wir $r = s$ *und nach eventueller Umordnung* $\mathfrak{p}_i = \mathfrak{q}_i, i = 1, \dots, r$. □

Definition 7.4 (gebrochenes Ideal)**.** *Sei* $\mathcal{O}$ *ein Dedekind Ring und* K *sein Quotientenkörper. Ein* ***gebrochenes Ideal*** *von* K *ist ein endlich erzeugter* $\mathcal{O}$*-Untermodul* $\mathfrak{a} \neq 0$ *von* K. *Ein* ***ganzes Ideal*** *von* K *ist ein Ideal von* $\mathcal{O}$.

Die Definition vom ganzen Ideal ist jetzt nötig um unterscheiden zu können von gebrochenen Idealen.

Theorem 7.5. *Die gebrochenen Ideale bilden eine abelsche Gruppe, die Idealgruppe* J_K *von* K. *Das Einselement* $(1) = \mathcal{O}$, *und das Inverse zu* $\mathfrak{a}$ *ist*

$$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathcal{O}\}$$

Beweis: Assoziativität, Kommutativität und $\mathfrak{a}(1) = \mathfrak{a}$ *sind klar. Für ein Primideal* $\mathfrak{p}$ *ist nach Lemma (1.1)* $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$ *, also* $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ *wegen der Maximalität von* $\mathfrak{p}$. *Ist* $\mathfrak{a} = \mathfrak{p}_1 ... \mathfrak{p}_r$ *ein ganzes Ideal, so ist* $\mathfrak{b} = \mathfrak{p}_1^{-1} ... \mathfrak{p}_r^{-1}$ *ein Inverses. Wegen* $\mathfrak{b}\mathfrak{a} = \mathcal{O}$ *ist* $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. *Ist umgekehrt* $x\mathfrak{a} \subseteq \mathcal{O}$, *so ist* $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, *also* $x \in \mathfrak{b}$ *wegen* $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. *Daher ist* $\mathfrak{b} = \mathfrak{a}^{-1}$. *Ist* $\mathfrak{a}$ *ein gebrochenes Ideal und* $\mathfrak{c} \in \mathcal{O}$, $\mathfrak{c} \neq 0$, *mit* $\mathfrak{c}\mathfrak{a} \subseteq \mathcal{O}$, *so ist* $(\mathfrak{c}\mathfrak{a})^{-1} = \mathfrak{c}^{-1}\mathfrak{a}^{-1}$ *das Inverse von* $\mathfrak{c}\mathfrak{a}$, *also* $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

Bemerkung: Da $\mathcal{O}$ noeterisch ist, ist ein $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von $K = \mathrm{Quot}(\mathcal{O})$ ein gebrochenes Ideal g.d.w. ein $0 \neq c \in \mathcal{O}$ existiert mit $c\mathfrak{a} \subseteq \mathcal{O}$. Die gebrochene Ideale multipliziert man genauso wie Ideale von $\mathcal{O}$.

Korollar 7.6. *Jedes gebrochene Ideal* $\mathfrak{a}$ *besitzt eine eindeutige Produktdarstellung*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$$

mit $\nu_\mathfrak{p} \in \mathbb{Z}$ *und* $\nu_\mathfrak{p} = 0$ *für fast alle* $\mathfrak{p}$. *Mit anderen Worten:* J_K *ist die durch die Primideale* $\mathfrak{p} \neq 0$ *erzeugte freie abelsche Gruppe.*

Beweis: Jedes gebrochene Ideal $\mathfrak{a}$ *ist Quotient* $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ *zweier ganzer Ideale* $\mathfrak{b}$ *und* $\mathfrak{c}$, *die nach (1.3) eine Primfaktorzerlegung besitzen. Daher besitzt* $\mathfrak{a}$ *eine Primzerlegung im Sinne des Korollars. Sie ist nach (1.3) eindeutig, wenn* $\mathfrak{a}$ *ganz ist, und damit auch im allgemeinen Fall.* □

Das Korollar 1.4.1 gibt einen Zusammenhang zu den lokalen Bewertungen. Nach dem Satz (11.5) in [MP11] [2] erhalten wir dass zu jedem Primideal $\mathfrak{p} \neq 0$ in $\mathcal{O}$ ein zugehöriger diskreter Bewertungsring $\mathcal{O}_\mathfrak{p}$ mit der entsprechenden Bewertung des Quotientenkörpers:

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

existiert. Diese Bewertung hat eine beziehung zur Primzerlegung. Ist $x \in K^\times$ und

$$(x) = \prod_\mathfrak{p} \mathfrak{p}^{\nu_p}$$

die Primzerlegung des Hauptideals (x), so ist

$$\nu_\mathfrak{p} = v_\mathfrak{p}(x)$$

für alle $\mathfrak{p}$. Denn für ein festes Primideal $\mathfrak{q} \neq 0$ von $\mathcal{O}$ folgt (wegen $\mathfrak{p}\mathcal{O}_\mathfrak{q} = \mathcal{O}_\mathfrak{q}$ für $\mathfrak{p} \neq \mathfrak{q}$) aus der ersten Gleichung

$$x\mathcal{O}_\mathfrak{q} = (\prod_\mathfrak{p} \mathfrak{p}^{\nu_p})\mathcal{O}_\mathfrak{q} = \mathfrak{q}^{\nu_\mathfrak{q}}\mathcal{O}_\mathfrak{q} = {\mathfrak{m}_\mathfrak{q}}^{\nu_\mathfrak{q}}$$

also in der Tat $v_\mathfrak{q}(x) = \nu_\mathfrak{q}$.

7.2. **Die Klassengruppe.**

Definition 7.7. ***Die Klassengruppe*** *ist definiert als die Faktorgruppe*

$$Cl_K = J_K/P_K.$$

wobei P_K aus den gebrochenen Hauptidealen $(a) = a\mathcal{O}$, $a \in K^\times$ besteht.
Bemerkung: P_K ist eine Untergruppe der Idealgruppe J_K.

Generell rechnet man in der Gruppe der gebrochenen Ideale mit der entsprechenden Äquivalenzrelation lieber als in der Klassengruppe von K. Man setzt hierbei für zwei gebrochene Ideale $\mathcal{I}, \mathcal{J}$:

$$\begin{aligned} \mathcal{I} \sim \mathcal{J} &\iff \mathcal{I}P_K = \mathcal{J}P_K \\ &\iff \exists x \in K^\times : \mathcal{I} = (x)\mathcal{J} \\ &\iff \exists x \in K^\times : \mathcal{I} = x\mathcal{J} \end{aligned} \tag{7.1}$$

Bemerkung: Ein Dedekindring ist ein Hauptidealring wenn die Klassengruppe trivial ist.

Beispiel: Sei $K := \mathbb{Q}(\sqrt{d})$, für $d \in \mathbb{Z}$ quadratfrei. Die negativen quadratfreien Zahlen $d < 0$ für die die Klassengruppe von K trivial ist, sind:

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

8. Ganze Algebraische Zahlen und Idealfaktorisierung

Antonio Casetta, *acasetta@student.ethz.ch*

In diesem Abschnitt möchten wir zeigen, wie man die Faktorisierung von Idealen berechnen kann und diverse damit zusammenhängende Begriffe.

8.1. **Erinnerung.**

Definition 8.1. *Sei $\mathcal{o} \subseteq \mathcal{o}'$ eine Ringerweiterung, d.h. ein injektiver Ringhomomorphismus. Ein Element $x \in \mathcal{o}'$ heißt* ganz *(oder* ganz-algebraisch*) über $\mathcal{o}$, wenn x einer normierten Gleichung genügt, d.h. wenn es $a_1, \ldots, a_n \in \mathcal{o}$ gibt mit $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Die Menge $\mathcal{O} = \{x \in \mathcal{o}' \mid \exists a_1, \ldots, a_n \in \mathcal{o}\colon x^n + a_1x^{n-1} + \cdots + a_n = 0\}$ heißt* ganzer Abschluss *von $\mathcal{o}$ in $\mathcal{o}'$.*

Satz 8.2. *Eine rationale Zahl ist genau dann ganz-algebraisch, wenn sie in $\mathbb{Z}$ liegt.*

Definition 8.3. *Wir definieren den Ring der ganzen Zahlen von einem Körper K als*

$$\mathcal{O}_K \coloneqq \mathbb{Z}_K \coloneqq \{b \in K : b \text{ ganz über } \mathbb{Z}\}$$

Satz 8.4. *$\mathcal{O}_K$ ist ein Dedekind-Ring, i.e. ein noetherscher Integritätsbereich.*

Definition 8.5. *Sei $\mathcal{O}$ ein Dedekind-Ring und K sein Quotientenkörper. Ein* gebrochenes Ideal *von K ist ein endlich erzeugter $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von K.*

Satz 8.6. *Sei $\mathcal{O}$ ein Dedekind-Ring. Dann sind die folgenden Aussagen äquivalent:*

(i) $\mathcal{O}$ ist ein Dedekind-Ring.

(ii) Jedes von 0 verschiedene Ideal $\mathfrak{a}$ kann eindeutig als Produkt von Primidealen geschrieben werden:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}, \qquad \nu_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z} \text{ fast alle gleich null}$$

(iii) Jedes von 0 verschiedene Ideal kann als Produkt von Primidealen geschrieben werden.

(iv) Die Menge der gebrochenen Ideale von K ungleich 0 ist eine Gruppe.

Korollar 8.7 (Chinesischer Restsatz)**.** *Sei $\mathcal{O}$ ein Dedekind-Ring, $\mathfrak{a} \subseteq \mathcal{O}$ ein Ideal. Dann ist*

$$\mathcal{O}/\mathfrak{a} \cong \prod_{\mathfrak{p}} \mathcal{O}/\mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$$

Definition 8.8. *Sei $\mathcal{O}$ ein Integritätsbereich mit Quotientenkörper K. Dann definieren wir:*

(1) Für zwei gebrochene Ideale $\mathfrak{a}, \mathfrak{b}$ in $\mathcal{O}$ ist $\mathfrak{a}|\mathfrak{b}$ genau dann, wenn ein ganzes Ideal $\mathfrak{c}$ gibt, sodass $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$. Dies is äquivalent zu $\nu_{\mathfrak{p}}(\mathfrak{b}) \geqslant \nu_{\mathfrak{p}}(\mathfrak{a})$ für alle Primideale $\mathfrak{p}$. Desweiteren ist es auch äquivalent zu $\mathfrak{b} \subseteq \mathfrak{a}$.

(2) Ein gebrochenes Ideal $\mathfrak{a} \subseteq \mathcal{O}$ heißt invertierbar*, falls es ein gebrochenes Ideal $\mathfrak{a}'$ gibt, so dass $\mathfrak{a} \cdot \mathfrak{a}' = \mathcal{O}$. Also für ein ganzes Ideal $\mathfrak{a} \subseteq \mathcal{O}$ definieren wir $\mathfrak{a}^{-1} \coloneqq \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$.*

Lemma 8.9. *Seien $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Q}$-Basis eines Körpers K mit alle α_i ganz über K. Falls $d = \operatorname{disk}(\bigoplus_i \alpha_i\mathbb{Z}) = \det(\operatorname{tr}(\alpha_i\alpha_j)_{i,j=1,\ldots,n})$ dann gilt $\bigoplus_i \alpha_i\mathbb{Z} \subseteq \mathbb{Z}_K \subseteq \frac{1}{d}\bigoplus_i \alpha_i\mathbb{Z}$.*

8.2. **Primidealfaktorisierung.** Jedes Primideal $\mathfrak{p} \neq 0$ von $\mathcal{O}_K$ enthält eine rationale Primzahl p und ist ein Teiler des Ideals $p\mathcal{O}_K$. Also fragen wir uns, wie eine Primzahl p in Primidealen des Rings $\mathcal{O}_K$ zerfällt. Wir betrachten dies Problem in einem allgemeinen Kontext, und beginnen mit einem beliebigen Dedekind-Ring o anstatt von $\mathbb{Z}$. Dann, anstatt von $\mathcal{O}_K$, wählen wir den ganzen Abschluss $\mathcal{O}$ von o in einer endlichen Erweiterung von seinem Quotientenkörper.

Für ein Primideal $\mathfrak{p}$ in o hat man immer $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$. In der Tat, sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ so, dass $\pi o = \mathfrak{p}\mathfrak{a}$ mit $\mathfrak{p} \nmid \mathfrak{a}$, also $\mathfrak{p} + \mathfrak{a} = o$. Betrachtet $1 = b + s$, mit $b \in \mathfrak{p}$ und $s \in \mathfrak{a}$, finden wir $s \notin \mathfrak{p}$ und $s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi o$. Falls man $\mathfrak{p}\mathcal{O} = \mathcal{O}$ hätte, dann würde es folgen, dass $s\mathcal{O} = s\mathfrak{p}\mathcal{O} \subseteq \pi\mathcal{O}$, also, dass $s = \pi x$ für eine $x \in \mathcal{O} \cap K = o$, i.e. $s \in \mathfrak{p}$, Widerspruch.

Ein Primideal $\mathfrak{p} \neq 0$ in dem Ring o zerfällt in $\mathcal{O}$ in einem eindeutigen Weg in einem Produkt von Primidealen

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

Die Primideale $\mathfrak{P}_i$ in der Faktorisierung sind genau die Primideale $\mathfrak{P}$ in $\mathcal{O}$, die über $\mathfrak{p}$ liegen, i.e. man hat die Relation $\mathfrak{p} = \mathfrak{P} \cap o$. Dies bezeichnen wir als $\mathfrak{P}|\mathfrak{p}$, und wir nennen $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$. Wir bemerken auch, dass $(\mathcal{O}/\mathfrak{P}_i)/(o/\mathfrak{p})$ eine Körpererweiterung ist, weil die Abbildung $o \to \mathcal{O} \to \mathcal{O}/\mathfrak{P}$ Kern $\mathfrak{P} \cap o = \mathfrak{p}$ hat. Also ist die Abbildung $o/\mathfrak{p} \hookrightarrow \mathcal{O}/\mathfrak{P}$ injektiv.

Definition 8.10. *(1) Das Exponent e_i heißt* ***Verzweigungsindex****.*

(2) Der Grad von der Körpererweiterung $f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$ wird ***Trägheitsgrad*** *von $\mathfrak{P}_i$ über $\mathfrak{p}$ genannt.*

(3) $\mathfrak{P}_i$ heißt ***unverzweigt*** *über $\mathfrak{p}$, wenn $e_i = 1$ und wenn die Körpererweiterung $(\mathcal{O}/\mathfrak{P}_i)/(o/\mathfrak{p})$ separabel ist.*

(4) $\mathfrak{p}$ heißt unverzweigt in L/K, wenn für alle $i = 1, \ldots, r : \mathfrak{P}_i/\mathfrak{p}$ unverzweigt über $\mathfrak{p}$ sind.

(5) $\mathfrak{p}$ heißt ***unzerlegt*** *in L/K, wenn $r = 1$, d.h., wenn es nur ein Primideal $\mathfrak{P}$ über $\mathfrak{p}$ gibt, und* ***träge****, wenn zusätzlich $p\mathcal{O}_K$ prim ist.*

(6) $\mathfrak{p}$ heißt ***total zerlegt*** *in L/K, wenn für alle $i = 1, \ldots, r : f_i = 1$ und $e_i = 1$.*

Satz 8.11. *Sei o ein Dedekind-Ring mit Quotientenkörper K und ganzem Abschluss $\mathcal{O}$ in einem Körper L, sodass L/K eine separable Körpererweiterung mit Grad $n = [L : K]$ ist. Für jede Primideal $\mathfrak{p} \neq 0$ in o, schreiben wir die Faktorisierung von $\mathfrak{p}$ als*

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

mit Trägheitsgrade $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}]$. *Dann gilt*

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

Beweis. Der Beweis basiert auf dem Chinesichen Restsatz in der folgenden Variante:

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}$$

$\mathcal{O}/\mathfrak{p}\mathcal{O}$ und $\mathcal{O}/\mathfrak{P}_i^{e_i}$ sind Vektorräume über dem Körper $\kappa = \mathcal{o}/\mathfrak{p}$, und es ist genug zu zeigen

$$\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n \quad \text{und} \quad \dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i f_i$$

Um die erste Identität zu beweisen, seien $\omega_1, \dots, \omega_m \in \mathcal{O}$ Repräsentanten für eine Basis $\bar{\omega}_1, \dots, \bar{\omega}_m$ von $\mathcal{O}/\mathfrak{p}\mathcal{O}$ über κ. Es ist genug zu zeigen, dass $\omega_1, \dots, \omega_m$ eine Basis von L/K bilden. Wir nehmen an, dass $\omega_1, \dots, \omega_m$ linear abhängig über K sind, und also über $\mathcal{o}$ auch. Dann gibt es Elemente $a_1, \dots, a_m \in \mathcal{o}$ nicht alle gleich Null, sodass $a_1\omega_1 + \cdots + a_m\omega_m = 0$. Definiere das Ideal $\mathfrak{a} = (a_1, \dots, a_m)$ von $\mathcal{o}$ und finde ein $a \in \mathfrak{a}^{-1}$ so, dass $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, also $a\mathfrak{a} \nsubseteq \mathfrak{p}$. Dann liegen die Elemente $aa_1, \dots, aa_m$ in $\mathcal{o}$, aber nicht alle gehören zu $\mathfrak{p}$. Der Ausdruck $aa_1\omega_1 + \cdots + aa_m\omega_m \equiv 0 \bmod \mathfrak{p}$ impliziert also die lineare Abhängigkeit zwischen die $\bar{\omega}_1, \dots, \bar{\omega}_m$ über κ, Widerspruch. Die $\omega_1, \dots, \omega_m$ sind also linear unabhängig über K. Um zu zeigen, dass alle ω_i eine Basis von L/K bilden, betrachten wir die $\mathcal{o}$-Module $M = \mathcal{o}\omega_1 + \cdots + \mathcal{o}\omega_m$ und $N = \mathcal{O}/M$. Seit $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, haben wir $\mathfrak{p}N = N$. Seit L/K separabel ist, sind $\mathcal{O}$ und N endlich erzeugte $\mathcal{o}$-Module. Mit $\alpha_1, \dots, \alpha_s$ als System von Erzeugenden von N, dann

$$\alpha_i = \sum_j a_{ij}\alpha_j \quad \text{für } a_{ij} \in \mathfrak{p}$$

Sei A die Matrix $(a_{ij}) - I$, wo I ist die unitäre Matrix mit Rank s, und sei B die adjunkte Matrix von A, deren Elementen die Unterdeterminanten von Rank $(s-1)$ von A sind. Dann haben wir $A(\alpha_1, \dots, \alpha_s)^T = 0$ und $BA = dI$, mit $d = \det(A)$. Also

$$0 = BA(\alpha_1, \dots, \alpha_s)^T = (d\alpha_1, \dots, d\alpha_s)^T$$

und also $dN = 0$, i.e. $d\mathcal{O} \subseteq M = \mathcal{o}\omega_1 + \cdots + \mathcal{o}\omega_m$. Wir haben $d \neq 0$, weil wir mit $d = \det((a_{ij}) - I)$ finden, dass $d \equiv (-1)^s \bmod \mathfrak{p}$, weil $a_{ij} \in \mathfrak{p}$. Es folgt, dass $L = dL = K\omega_1 + \cdots + K\omega_m$. $\omega_1, \dots, \omega_m$ ist also eine Basis von L/K.

Um die zweite Identität zu zeigen, betrachten wir die absteigende Kette

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)$$

von κ-Vektorräumen. Die sukzessive Quotienten $\mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}$ in dieser Kette sind isomorph zu $\mathcal{O}/\mathfrak{P}_i$, für $\alpha \in \mathfrak{P}_i^\nu \backslash \mathfrak{P}_i^{\nu+1}$, dann hat der Homomorphismus

$$\mathcal{O} \longrightarrow \mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}, \quad a \mapsto a\alpha$$

Kern $\mathfrak{P}_i$ und ist surjektiv, weil $\mathfrak{P}_i^\nu$ der ggT von $\mathfrak{P}_i^{\nu+1}$ und $(\alpha) = \alpha\mathcal{O}$ ist, also $\mathfrak{P}_i^\nu = \alpha\mathcal{O} + \mathfrak{P}_i^{\nu+1}$. Seit $f_i = [\mathcal{O}/\mathfrak{P}_i : \kappa]$, haben wir $\dim_\kappa(\mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}) = f_i$ und also

$$\dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{\nu=0}^{e_i-1} \dim_\kappa(\mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}) = e_i f_i$$

□

Falls $p \in \mathbb{Z}$ eine Primzahl ist, so lässt sich das Ideal $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ faktorisieren. Nun ist $\mathfrak{P}_i \cap \mathbb{Z} = p\mathbb{Z}$. Entsprechend hat man eine Körpererweiterung von endlichen Körpern: $\mathcal{O}_K/\mathfrak{P}_i$ über $\mathbb{Z}/p\mathbb{Z}$. Sagen wir jene ist vom Grad f_i. Nun hat man $[K : \mathbb{Q}] = \sum_{i=1}^r e_i f_i$.
Im nächsten Satz Wählen wir $K = \mathbb{Q}(\theta)$ für eine ganz-algebraische Zahl θ mit Minimalpolynom $Q(X)$. Für die meisten Primzahlen p ist die Faktorisation $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ im Zusammenhang mit der Faktorisierung in $\mathbb{Z}/p\mathbb{Z}[X]$ von der Projektion von $Q(X)$ zu $(\mathbb{Z}/p\mathbb{Z})[X]$.

Satz 8.12. *Sei $\theta \in \mathbb{Z}_K$ eine ganze primitive Zahl von einem Zahlkörper $K = \mathbb{Q}(\theta)$ vom Grad n über $\mathbb{Q}$ und $d = \operatorname{disk}(1, \theta, \dots, \theta^{n-1})$. Sei nun $p \in \mathbb{Z}$ eine Primzahl, welche zu d teilerfremd ist. Sei*

$Q(X) \in \mathbb{Z}[X]$ das Minimalpolynom von θ und nehme an, dass die Reduktion $\overline{Q}(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ sich wie folgt

$$\overline{Q}(X) = \overline{Q}_1(X)^{e_1} \cdots \overline{Q}_r(X)^{e_r}$$

in irreduzible, paarweise teilerfemde Polynome $\overline{Q}_i(X)$ zerlegt. Seien ferner $Q_i(X) \in \mathbb{Z}[X]$ Polynome, welche sich auf $\overline{Q}_i$ reduzieren, dann sind

$$\mathfrak{P}_i = p\mathbb{Z}_K + Q_i(\theta)\mathbb{Z}_K$$

die verschiedenen über (p) liegenden Primideale von $\mathbb{Z}_K$. Ferner ist der Trägheitsgrad von $\mathfrak{P}_i$ über (p) gleich dem Grad von $\overline{Q}_i(X)$ und es gilt

$$p\mathbb{Z}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

Beweis. Wir zeigen die Isomorphismen

$$\mathbb{Z}_K/p\mathbb{Z}_K \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X))$$

Wir anfangen mit dem ersten. $1, \theta, \ldots, \theta^{n-1}$ bildet eine $\mathbb{Z}$-Basis von $\mathbb{Z}[\theta]$. $d = \mathrm{disk}(1, \theta, \ldots, \theta^{n-1}) = \det(\mathrm{tr}(\theta^{i+j})_{i,j=0,\ldots,n-1})$, also gilt $\mathbb{Z}[\theta] \subseteq \mathbb{Z}_K \subseteq \frac{1}{d}\mathbb{Z}[\theta]$. Falls nun $(d,p) = 1$, dann ist d invertierbar in $\mathbb{Z}/p\mathbb{Z}$, daraus folgt dann, dass die Abbildung $\mathbb{Z}[\theta] \to \mathbb{Z}_K \to \mathbb{Z}_K/p\mathbb{Z}_K$ surjektiv ist mit Kern $p\mathbb{Z}[\theta]$ und somit $\mathbb{Z}_K/p\mathbb{Z}_K \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \mathbb{Z}[X]/(p, Q(X))$.

Der zweite Isomorphismus ist aus dem surjektiven Homomorphismus

$$\mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X))$$

ableitbar. Sein Kern ist das Ideal erzeugt von p und $Q(X)$, und aus $\mathbb{Z}[\theta] = \mathbb{Z}[X]/(Q(X))$, haben wir $\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X))$.

Seit $\overline{Q}(X) = \prod_{i=1}^r \overline{Q}_i(X)^{e_i}$, der Chinesiche Restsatz besagt endlich, dass

$$(\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X)) \cong \bigoplus_{i=1}^r (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}_i(X))^{e_i}$$

Dies zeigt, dass die Primideale des Rings $R = (\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X))$ die Hauptideale $(\overline{Q}_i)$ sind, die erzeugt von den $\overline{Q}_i(X) \bmod \overline{Q}(X)$, für $i = 1, \ldots, r$, sind. Dies zeigt auch, dass der Grad $[R/(\overline{Q}_i) : \mathbb{Z}/p\mathbb{Z}]$ gleich der Grad von $\overline{Q}_i(X)$ ist, und

$$(0) = (\overline{Q}) = \bigcap_{i=1}^r (\overline{Q}_i)^{e_i}$$

Aus dem Isomorphismus $(\mathbb{Z}/p\mathbb{Z})[X]/(\overline{Q}(X)) \cong \mathbb{Z}_K/p\mathbb{Z}_K$, $f(X) \mapsto f(\theta)$, gilt das gleiche für $\mathbb{Z}_K/p\mathbb{Z}_K$. Also sind die Primideale $\overline{\mathfrak{P}}_i$ von $\mathbb{Z}_K/p\mathbb{Z}_K$ die Primideale $(\overline{Q}_i)$, und sie sind die Primideale erzeugt von den $Q_i(\theta) \bmod p\mathbb{Z}_K$. Der Grad $[(\mathbb{Z}_K/p\mathbb{Z}_K)/\overline{\mathfrak{P}}_i : \mathbb{Z}/p\mathbb{Z}]$ ist der Grad des Polynoms $\overline{Q}_i(X)$, und wir haben $(0) = \bigcap_{i=1}^r \overline{\mathfrak{P}}_i^{e_i}$. Jetzt sei $\mathfrak{P}_i = p\mathbb{Z}_K + Q_i(\theta)\mathbb{Z}_K$ das Vorbild von $\overline{\mathfrak{P}}_i$ bezüglich dem Homomorphismus

$$\mathbb{Z}_K \longrightarrow \mathbb{Z}_K/p\mathbb{Z}_K$$

Dann, für $i = 1, \ldots, r$, variiert $\mathfrak{P}_i$ über den Primidealen von $\mathbb{Z}_K$ über p. $f_i = [\mathbb{Z}_K/\mathfrak{P}_i : \mathbb{Z}/p\mathbb{Z}]$ ist der Grad des Polynoms $\overline{Q}_i(X)$. Ausserdem ist $\mathfrak{P}_i^{e_i}$ das Vorbild von $\overline{\mathfrak{P}}_i^{e_i}$ (weil $e_i = \#\{\overline{\mathfrak{P}}^\nu \mid \nu \in \mathbb{N}\}$), und $p\mathbb{Z}_K \supseteq \bigcap_{i=1}^r \mathfrak{P}_i^{e_i}$ so, dass $p\mathbb{Z}_K \mid \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ und folglich $p\mathbb{Z}_K = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$, weil $\sum_i e_i f_i = n$. □

Bemerkung 8.13. Desweiteren kann man auch zeigen, dass $d = (-1)^{n(n-1)/2}\mathrm{disk}(Q(X)) = \mathrm{Res}(Q(X), \frac{d}{dX}Q(X))$ gilt. Da nun $(p,d) = 1$ gilt, folgt, dass $\overline{Q}(X) \in \mathbb{Z}/p\mathbb{Z}$ keine mehrfache Nullstelle hat, insbesondere folgt sogar, dass alle $e_i = 1$ und somit p ist unverzweigt.

Beispiel 8.14. *$\theta = \sqrt[3]{2}$ hat Minimalpolynom $Q(X) = X^3 - 2 \in \mathbb{Z}[X]$.*
Wir bemerken, dass $X^3 - 2 \equiv (X+2)(X^2+3X+4) \bmod (5)$ wobei beide Faktoren irreduzibel in $\mathbb{Z}/5\mathbb{Z}[X]$ sind. Ferner sind 5 und die Diskriminante $d = -108$ von $Q(X)$ teilerfremd. Daraus folgt

$$5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} = \mathfrak{P}_1\mathfrak{P}_2 = \left(5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} + (\sqrt[3]{2}+2)\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})}\right)\left(5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} + (\sqrt[3]{4}+3\sqrt[3]{2}+4)\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})}\right)$$

mit Trägheitsgraden $f_1 = 1$ und $f_2 = 2$.

9. Kreisteilungskörper

Quirin Reding, *quirin.reding@math.ethz.ch*

In diesem Abschnitt befassen wir uns mit dem n-ten Kreisteilungskörper $\mathbb{Q}(\zeta)$. Dabei bezeichnet ζ eine primitive n-te Einheitswurzel, das heisst $\zeta^n = 1$ und $\zeta^k \neq 1$ für alle $1 \leqslant k < n$. Die Körpererweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ ist galoissch von Grad $\varphi(n)$, wobei wir mit φ die Eulersche Phi-Funktion bezeichnen.

9.1. **Ganze Zahlen.** Die ganzen Zahlen in $\mathbb{Q}(\zeta)$ sind $\mathbb{Z}[\zeta]$. Um das zu zeigen, beweisen wir den folgende Satz.

Satz 9.1. *$1, \zeta, \dots, \zeta^{d-1}$ mit $d = \varphi(n)$ ist eine Ganzheitsbasis für den Ring $\mathcal{O}$ der ganzen Zahlen von $\mathbb{Q}(\zeta)$, d.h.*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{d-1} = \mathbb{Z}[\zeta]$$

Für den Beweis benötigen wir das folgende Lemma.

Lemma 9.2. *Sei $n = q^\nu$ eine Primzahlpotenz und $\lambda = 1 - \zeta$. Dann ist das Hauptideal $(\lambda) \subseteq \mathcal{O}$ ein Primideal vom Grad 1 und für $d = \varphi(n)$ ist*

$$q\mathcal{O} = (\lambda)^d.$$

Ferner hat die Basis $1, \zeta, \dots, \zeta^{d-1}$ von $\mathbb{Q}(\zeta)|\mathbb{Q}$ die Diskriminante

$$d(1, \zeta, \dots, \zeta^{d-1}) = \pm q^s,$$

mit $s = q^{\nu-1}(\nu q - \nu - 1)$.

Beweis. Das Minimalpolynom von ζ ist das n-te Kreisteilungspolynom

$$\phi_n(X) = \prod_{\substack{1 \leqslant k \leqslant n \\ (k,n)=1}} (X - \zeta^k) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^k) = (X^{q^\nu} - 1)/(X^{q^{\nu-1}} - 1)$$

$$= X^{q^{\nu-1}(q-1)} + \cdots + X^{q^{\nu-1}} + 1.$$

Also ist ζ ganz in $\mathbb{Q}(\zeta)$ und so auch

$$\varepsilon_k \coloneqq 1 + \zeta + \cdots + \zeta^{k-1} = \frac{1 - \zeta^k}{1 - \zeta}.$$

Mit $X = 1$ erhalten wir aus den obigen Gleichungen

$$q = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (1 - \zeta^k) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \varepsilon_k (1 - \zeta). \tag{9.1}$$

Da $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ invertierbar ist, gibt es ein $k' \in \mathbb{Z}$, so dass $k'k \equiv 1 \bmod n$. Somit ist

$$\frac{1 - \zeta}{1 - \zeta^k} = \frac{1 - (\zeta^k)^{k'}}{1 - \zeta^k} = 1 + \zeta^k + \cdots + (\zeta^k)^{k'-1} \in \mathcal{O}.$$

Das heisst ε_k ist eine Einheit in $\mathcal{O}$, also auch $\varepsilon \coloneqq \prod_k \varepsilon_k$. Es folgt, dass $q = \varepsilon(1 - \zeta)^d$ und somit auch $q\mathcal{O} = (\lambda)^d$. Wegen der fundamentalen Gleichung $\sum_i e_i f_i = d$ der Primidealzerlegung muss (λ) ein Primideal vom Grad 1 sein.

Für die Bestimmung der Diskriminanten verwenden wir, dass

$$\pm d(1, \zeta, \dots, \zeta^{d-1}) = \prod_{i \neq j} (\zeta_i - \zeta_j) = \prod_{i=1}^{d} \phi_n'(\zeta_i),$$

wobei $\zeta_1, \dots, \zeta_d$ die Konjugierten von ζ unter der Wirkung der Galois-Gruppe bezeichnen.

Nach [4, Satz 2.6] ist ferner

$$\prod_{i=1}^{d} \phi_n'(\zeta_i) = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\phi_n'(\zeta)).$$

Aus der Identität $(X^{q^{\nu-1}}-1)\phi_n(X) = (X^{q^\nu}-1)$ für das n-te Kreisteilungspolynom ϕ_n erhalten wir durch differenzieren nach X und Auswertung bei $X=\zeta$, dass

$$q^{\nu-1}X^{q^{\nu-1}-1}\phi_n(X) + (X^{q^{\nu-1}}-1)\phi_n'(X) = q^\nu X^{q^\nu-1}$$
$$0 + (\zeta^{q^{\nu-1}}-1)\phi_n'(\zeta) = q^\nu\zeta^{q^\nu-1} = q^\nu\zeta^{-1}.$$

Mit der primitiven q-ten Einheitswurzel $\xi \coloneqq \zeta^{q^{\nu-1}}$ haben wir also

$$(\xi-1)\phi_n'(\zeta) = q^\nu\zeta^{-1}.$$

Da q prim ist folgt nach [4, Satz 2.6], dass

$$N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1) = \prod_{1\leqslant k<q}(\xi^k-1) = \pm\phi_q(1) = \pm q.$$

Es ist also

$$N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\xi-1) = N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi-1)^{q^{\nu-1}} = \pm q^{q^{\nu-1}}.$$

Wir folgern mit der Kenntnis, dass ζ^{-1} Norm ±1 und $q^\nu = n$ Norm $n^{\varphi(n)}$ hat,

$$\pm d(1,\zeta,\dots,\zeta^{d-1}) = \pm(q^\nu)^{q^{\nu-1}(q-1)}q^{-q^{\nu-1}} = \pm q^s$$

mit $s = q^{\nu-1}(\nu q-\nu-1)$. □

Nun können wir Satz 9.1 beweisen.

Beweis von Satz 9.1. Wir nehmen zuerst an $n=q^\nu$ sei eine Primzahlpotenz. Wie in einem Lemma im Abschnitt über Dedeking Ringe gesehen gilt für die Diskriminante $d(1,\zeta,\dots,\zeta^{d-1}) = \pm q^s$

$$q^s\mathcal{O} \subseteq \mathbb{Z}+\zeta\mathbb{Z}+\cdots+\zeta^{d-1}\mathbb{Z} = \mathbb{Z}[\zeta] \subseteq \mathcal{O}, \tag{9.2}$$

wobei wir verwendet haben, dass das Minimalpolynom ϕ_n von ζ Grad d hat und $\zeta\in\mathcal{O}$.

Da λ wegen Lemma 9.2 ein Primideal von Grad 1 mit $q\mathcal{O} = (\lambda)^d$ ist, gilt $\mathcal{O}/\lambda\mathcal{O} \cong \mathbb{Z}/q\mathbb{Z}$. Somit ist $\mathcal{O} = \mathbb{Z}/q\mathbb{Z} + \lambda\mathcal{O}$ und wegen $\mathbb{Z}/q\mathbb{Z}\subseteq\mathbb{Z}[\zeta]\subseteq\mathcal{O}$, ist auch $\mathcal{O} = \mathbb{Z}[\zeta]+\lambda\mathcal{O}$. Mulitplikation mit λ und einsetzen in die ursprüngliche Gleichung liefert $\mathcal{O} = \mathbb{Z}[\zeta]+\lambda\mathbb{Z}[\zeta]+\lambda^2\mathcal{O} = \mathbb{Z}[\zeta]+\lambda^2\mathcal{O}$. Induktiv erhalten wir also $\forall t\geqslant 1$:

$$\mathcal{O} = \mathbb{Z}[\zeta]+\lambda^t\mathcal{O}.$$

Also erhalten wir unter Verwendung von 9.2 und $(\lambda)^d = q\mathcal{O}$ aus Lemma 9.2

$$\mathcal{O} = \mathbb{Z}[\zeta]+\lambda^{ds}\mathcal{O} = \mathbb{Z}[\zeta]+(q\mathcal{O})^s\mathcal{O} = \mathbb{Z}[\zeta]+q^s\mathcal{O} = \mathbb{Z}[\zeta].$$

Im allgemeinen Fall sei $n = q_1^{\nu_1}\cdots q_r^{\nu_r}$ die Primfaktorzerlegung von n in $\mathbb{Z}$. Dann haben wir die Zerlegung

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1)\cdots\mathbb{Q}(\zeta_r),$$

mit den primitiven $q_i^{\nu_i}$-ten Einheitswurzeln $\zeta_i \coloneqq \zeta^{n/q_i^{\nu_i}}$. Sei $d_i \coloneqq \varphi(q_i^{\nu_i})$, dann ist nach vorheriger Betrachtung jeweils $1,\zeta_i,\dots,\zeta_i^{d_i-1}$ eine Ganzheitsbasis von $\mathbb{Q}(\zeta_i)|\mathbb{Q}$ mit Diskriminante $q_i^{s_i}$. Da diese Diskriminanten zueinander paarweise teilerfremd sind und $\mathbb{Q}(\zeta_1)\cdots\mathbb{Q}(\zeta_{i-1})\cap\mathbb{Q}(\zeta_i) = \mathbb{Q}$ für alle $1<i\leqslant r$ gilt, ist nach [4, Satz 2.11] die Menge $\{\zeta_1^{j_1}\cdots\zeta_r^{j_r} : 0\leqslant j_i\leqslant d_i-1\}$ eine Ganzheitsbasis von $\mathbb{Q}(\zeta)|\mathbb{Q}$. Da diese Basiselemente alle Potenzen von ζ sind, gibt es für jedes $\alpha\in\mathcal{O}$ ein Polynom $f\in\mathbb{Z}[X]$, so dass $f(\zeta)=\alpha$. Mithilfe von $\zeta^d=1$ können wir f vom Grad $\leqslant d-1$ wählen und erhalten somit eine Darstellung der Form $\alpha = a_0+a_1\zeta+\cdots+a_{d-1}\zeta^{d-1}$, womit $1,\zeta,\dots,\zeta^{d-1}$ auch eine Ganzheitsbasis ist. □

9.2. **Primidealzerlegung.** Im Kreisteilungskörper $\mathbb{Q}(\zeta)$ können wir die Zerlegung in Primideale explizit angeben.

Satz 9.3. *Sei $n = \prod_p p^{\nu_p}$ die Primzerlegung von n und ζ eine primitive n-te Einheitswurzel. Ferner sei $f_p\in\mathbb{Z}$ für jede Primzahl p die kleinste postive ganze Zahl mit $p^{f_p}\equiv 1 \bmod n/p^{\nu_p}$.*

Dann zerlegt sich p über $\mathbb{Q}(\zeta)$ in

$$p = (\mathfrak{p}_1\cdots\mathfrak{p}_r)^{\varphi(p^{\nu_p})},$$

wobei die $\mathfrak{p}_i$ verschiedene Primideale vom Grad f_p sind.

Beweis. Der Führer von $\mathbb{Z}[\zeta]$ ist 1, da $\mathbb{Z}[\zeta]$ der Ring der ganzen Zahlen von $\mathbb{Q}(\zeta)$ ist. Also können wir für p prim Satz 8.3 aus [4] anwenden. Folglich zerfällt p in $\mathbb{Q}(\zeta)$ auf gleiche Weise in Primideale wie das Minimalpolynom $\phi_n(X)$ von ζ in irreduzible Faktoren mod p. Es genügt also zu zeigen, dass

$$\phi_n(X) \equiv \big(p_1(X)\cdots p_r(X)\big)^{\varphi(p^{\nu_p})} \bmod p$$

mit verschiedenen irreduziblen Polynomen $p_1(X),\dots,p_r(X)$ über $\mathbb{Z}/p\mathbb{Z}$ vom Grad f_p.

Wir schreiben $m \coloneqq n/p^{\nu_p}$ und definieren ξ_i und η_j als die primitiven m-ten bzw. p^{ν_p}-ten Einheitswurzeln. Entsprechend sind die Produkte $\xi_i\eta_j$ genau die primitiven n-ten Einheitswurzeln. Also ist

$$\phi_n(X) = \prod_{i,j}(X - \xi_i\eta_j),$$

wobei die Indizes i und j über die entsprechenden Einheitengruppen $(\mathbb{Z}/m\mathbb{Z})^\times$ bzw. $(\mathbb{Z}/p^{\nu_p}\mathbb{Z})^\times$ laufen. Nun ist für jedes Primideal $\mathfrak{p} \supseteq (p)$ jedoch $\eta_j \equiv 1 \bmod \mathfrak{p}$, da $X^{p^{\nu_p}} - 1 \equiv (X-1)^{p^{\nu_p}} \bmod p$. Folglich haben wir

$$\phi_n(X) \equiv \prod_i (X-\xi_i)^{\varphi(p^{\nu_p})} = \phi_m(X)^{\varphi(p^{\nu_p})} \bmod \mathfrak{p}.$$

Da die Kreisteilungspolynome $\phi_n(X)$ und $\phi_m(X)$ Koeffizienten in $\mathbb{Z}$ haben, folgt auch, dass

$$\phi_n(X) \equiv \phi_m(X)^{\varphi(p^{\nu_p})} \bmod p.$$

Ferner ist $\mathbb{Z}[\zeta]/\mathfrak{p}$ eine endliche Körpererweiterung von $\mathbb{F}_p$, also von der Form $\mathbb{F}_{p^f}$ für ein $f \geqslant 1$. Nun haben wegen $(m,p)=1$ die Polynome X^m-1 und mX^{m-1} keine gemeinsamen Nullstellen mod $\mathfrak{p}$. Deshalb haben sowohl X^m-1 als auch $\phi_m(X)$ keine mehrfachen Nullstellen mod $\mathfrak{p}$. Folglich ist das Bild $\bar\zeta_m$ der primitiven m-ten Einheitswurzel ζ_m unter der Abbildung $\mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/\mathfrak{p}$ wiederum eine primitive m-te Einheitswurzel. Deshalb teilt die Ordung m vom $\bar\zeta_m$ die Kardinalität der Einheitengruppe $\mathbb{F}_{p^f}^\times = \mathbb{F}_{p^f} - \{0\}$. Das heisst $p^f \equiv 1 \bmod m$. Also ist $f \geqslant f_p$.

Da nun aber auch die Bilder $\bar\zeta_m^i \in \mathbb{Z}[\zeta]/\mathfrak{p}$ primitive m-te Einheitswurzeln sind für alle $1 \leqslant i < m$ mit $(i,m)=1$, zerfällt das Bild $\bar\phi_m(X)$ des Kreisteilungspolynoms $\phi_m(X)$ in $\mathbb{Z}[\zeta]/\mathfrak{p} = \mathbb{F}_{p^{f_p}}$ in Linearfaktoren. Seien nun $P_i(X)$ die irreduziblen Faktoren von $\phi_m(X)$ mod p. Dann hat jedes $P_i(X)$ mindestens Grad f mit $p^f \equiv 1 \bmod m$ und maximal Grad f_p, da $\bar\phi_m(X)$ in $\mathbb{F}_{p^{f_p}}$ in Linearfaktoren zerfällt. Somit ist $f = f_p$. □

9.3. **Grosser Fermatscher Satz für reguläre Primzahlen.** Als Anwendung der Kreisteilungskörper betrachten wir den grossen Fermatschen Satz:

Satz 9.4. *Die Gleichung $x^n + y^n = z^n$ hat für jede natürliche Zahl $n > 2$ keine positiven ganzzahligen Lösungen $(x,y,z) \in \mathbb{Z}^3_{>0}$.*

Und zwar betrachten wir den Fall, dass $n = p \geqslant 5$ eine Primzahl ist. Wir argumentieren per Widerspruch, sei also (x,y,z) eine positive ganzzahlige Lösung. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass x,y,z paarweise teilerfremd sind. Wir nehmen zudem an dass p keine der Zahlen x,y,z teilt. (Der andere Fall, nämlich dass p genau eine der Zahlen x,y,z teilt, ist etwas aufwendiger.)

Wir faktorisieren nun die Summe $x^p + y^p$ in $\mathbb{Q}(\zeta)$ mit ζ einer primitiven p-ten Einheitswurzel. Es gilt

$$t^p - 1 = \prod_{0\leqslant k<p}(t - \zeta^k)$$

und somit

$$(-x/y)^p - 1 = \prod_{0\leqslant k<p}(-x/y - \zeta^k)$$

$$x^p + y^p = \prod_{0\leqslant k<p}(x + y\zeta^k).$$

Die Gleichung $x^p + y^p = z^p$ führt also zur folgenden Hauptidealgleichung in $\mathbb{Z}[\zeta]$

$$(x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}) = (z)^p. \tag{9.3}$$

Wir zeigen nun mithilfe der Primidealzerlegung in $\mathbb{Z}[\zeta]$, dass das Hauptideal $(x+y\zeta)$ keine gemeinsamen Primidealfaktoren mit den den anderen Hauptidealen auf der linken Seite von Gleichung

9.3 hat. Angenommen dies sei nicht der Fall. Dann gibt es ein Primideal π mit $\pi \supseteq (x+y\zeta)$ und $\pi \supseteq (x+y\zeta^k)$ für ein $k \not\equiv 1 \bmod p$. Folglich

$$\begin{aligned}\pi &\supseteq (x+y\zeta^k) - (x+y\zeta)\\ \pi &\supseteq \big(y\zeta(\zeta^{k-1}-1) = \big(y(\zeta^{k-1}-1)\big),\end{aligned}$$

wobei wir im letzten Schritt verwendet haben, dass ζ eine Einheit in $\mathbb{Z}[\zeta]$ ist. Analog zu Gleichung 9.1 erhalten wir die Hauptidealgleichung $(p) = (1-\zeta)\cdots(1-\zeta^{p-1})$. Somit folgt, dass $\pi \supseteq (yp)$. Zudem folgt direkt aus Gleichung 9.3, dass $\pi \supseteq (z)^p$ und da π prim ist, muss folglich auch $\pi \supseteq (z)$ gelten. Da aber p, y und z paarweise teilerfremd sind, ist $\pi \supseteq (z) + (yp) = \mathbb{Z}[\zeta]$ im Widerspruch zur Annahme, dass π prim ist. Dies zeigt die Behauptung.

Somit ist der Verzweigungsindex jedes Primidealfaktors von $(x+y\zeta)$ durch p teilbar. Folglich ist $(x+y\zeta) = I^p$ die p-te Potenz eines Ideals I. Wir nehmen nun im folgenden an p sei eine reguläre Primzahl um zu zeigen, dass I ein Hauptideal ist.

Definition 9.5. *Eine Primzahl $p \in \mathbb{Z}$ heisst* regulär *falls p die Kardinalität der Klassengruppe von $\mathbb{Q}(\zeta)$ nicht teilt. (ζ ist eine primitive p-te Einheitswurzel)*

Wenn also p regulär ist, so gibt es keine Elemente der Ordnung p in der Klassengruppe von $\mathbb{Q}(\zeta)$. Sei C die Klasse in der das Ideal I liegt. Dann ist wegen $I^p \in C^p$ die Klasse C^p das triviale Element der Klassengruppe, da $I^p = (x+y\zeta)$ ein Hauptideal ist. Somit ist die Ordnung von C ein Teiler von p und folglich 1. Somit ist C bereits trivial in der Klassengruppe, d.h. I ist ein Hauptideal.

Wir können also schreiben $x + y\zeta = u\alpha^p$ für ein $\alpha \in \mathbb{Z}[\zeta]$. Unter Verwendung von $(\beta+\gamma)^p \equiv \beta^p + \gamma^p \bmod p$ für alle $\beta, \gamma \in \mathbb{Z}[\zeta]$ ist

$$\alpha^p = \Big(\sum_{i=0}^{p-1} a_i \zeta^i\Big)^p \equiv \sum_{i=0}^{p-1} a_i^p \zeta^{ip} \in \mathbb{Z}.$$

Nun verwenden wir, dass für jede Einheit $u \in \mathbb{Z}[\zeta]$ der Quotient $u/\bar{u}$ eine p-te Einheitswurzel ist. Es ist folglich

$$x + y\zeta = u\alpha^p \equiv (u/\bar{u})\overline{u\alpha^p} = \zeta^k(x + y\zeta^{-1}).$$

Wir behaupten, dass $k \equiv 1 \bmod p$. Denn andernfalls folgt aus

$$\begin{aligned}p \mid \zeta^k(x+y\zeta^{-1}) - (x+y\zeta)\\ p \mid x(\zeta^k - 1) + y(\zeta^{k-1} - \zeta)\\ p \mid -x - y\zeta + x\zeta^k + y\zeta^{k-1},\end{aligned}$$

dass p auch x oder y teilt, (da $1, \zeta, \ldots, \zeta^{p-2}$ eine Ganzheitsbasis ist) im Widerspruch zur ursprünglichen Annahme.

Für $k \equiv 1$ erhalten wir nun $x + y\zeta \equiv x\zeta + y$, also $x \equiv y \bmod p$. Wegen p ungerade gilt aber auch $x^p + (-z)^p = (-y)^p$ und folglich $x \equiv -z \bmod p$. Zusammen erhalten wir

$$\begin{aligned}2x^p \equiv x^p + y^p = z^p \equiv -x^p\\ \Rightarrow p \mid 3x^p\\ \Rightarrow p \mid x,\end{aligned}$$

im Widerspruch zur ursprünglichen Annahme. Somit haben wir gezeigt, dass es keine positiv ganzzahligen Lösungen zur Gleichung $x^p + y^p = z^p$ gibt für $p \geqslant 5$ eine reguläre Primzahl mit $p \nmid xyz$.

9.4. **Eine weitere Anwendung.** Zu guter Letzt beweisen wir noch folgende Aussage über quadratische Zahlkörper.

Satz 9.6. *Für jede ungerade Primzahl p mit $p^\star = (-1)^{\frac{p-1}{2}} p$ ist $\mathbb{Q}(\sqrt{p^\star}) \subseteq \mathbb{Q}(\zeta)$. Wobei ζ eine primitive p-te Einheitswurzel bezeichnet.*

Beweis. Nach dem Eulerschen Kriterium ist $p^\star = \left(\frac{-1}{p}\right)p$. Sei ferner

$$\tau \coloneqq \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\zeta^a.$$

Wir zeigen nun, dass $p^\star = \tau^2$. Wir berechnen wie folgt, wobei die Summierungsindizes a, b, c jeweils über die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ laufen.

$$\begin{aligned}\left(\frac{-1}{p}\right)\tau^2 &= \left(\frac{-1}{p}\right)\left(\sum_a \left(\frac{a}{p}\right)\zeta^a\right)\left(\sum_b \left(\frac{b}{p}\right)\zeta^b\right)\\ &= \sum_{a,b}\left(\frac{a}{p}\right)\left(\frac{-b}{p}\right)\zeta^{a+b} = \sum_{a,b'}\left(\frac{a}{p}\right)\left(\frac{b'}{p}\right)\zeta^{a-b'}\end{aligned}$$

Wobei wir im letzten Schritt $b' \coloneqq -b$ substituiert haben. Weiter gilt $\left(\frac{b}{q}\right) = \left(\frac{b^{-1}}{q}\right)$ nach dem Eulerschen Kriterium. Somit ist

$$\begin{aligned}\left(\frac{-1}{p}\right)\tau^2 &= \sum_{a,b}\left(\frac{a}{p}\right)\left(\frac{b^{-1}}{p}\right)\zeta^{a-b} = \sum_{a,b}\left(\frac{ab^{-1}}{p}\right)\zeta^{a-b}\\ &= \sum_{b,c}\left(\frac{c}{p}\right)\zeta^{bc-b}, \text{ mit } c \coloneqq ab^{-1}\\ &= \sum_c \left(\frac{c}{p}\right)\sum_b \zeta^{b(c-1)}\\ &= \sum_{c\neq 1}\left(\frac{c}{p}\right)\sum_b \xi^b + \left(\frac{1}{p}\right)\sum_b 1, \text{ mit } \xi \coloneqq \zeta^{c-1}\\ &= \sum_{c\neq 1}\left(\frac{c}{p}\right)(-1) + p - 1.\end{aligned}$$

Ferner ist $\sum_c \left(\frac{c}{p}\right) = 0$, da für $\left(\frac{x}{p}\right) = -1$

$$-\sum_c \left(\frac{c}{p}\right) = \left(\frac{x}{p}\right)\sum_c \left(\frac{c}{p}\right) = \sum_c \left(\frac{xc}{p}\right) = \sum_{c'}\left(\frac{c'}{p}\right),$$

mit der Substitution $c' \coloneqq xc$ in der Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$.

Somit haben wir

$$\left(\frac{-1}{p}\right)\tau^2 = -\left(\frac{1}{p}\right)(-1) + p - 1 = p.$$

Es folgt, dass

$$\tau^2 = \left(\frac{-1}{p}\right)\left(\frac{-1}{p}\right)\tau^2 = \left(\frac{-1}{p}\right)p = p^\star.$$

□

10. Lokaler Frobenius und quadratische Reziprozität

Kevin Zhang, *kezhang@ethz.ch*

10.1. **Hilbertsche Verzweigungstheorie.** Sei $\mathcal{o}$ wieder ein beliebiger Dedekindring mit Quotientenkörper K. Wir betrachten hier den Fall einer endlichen galoisschen Körpererweiterung $L|K$ mit Galoisgruppe $G = G(L|K)$ vom Grad n. Wir nennen den ganzen Abschluss von $\mathcal{o}$ in L wieder $\mathcal{O}$.

Lemma 10.1. *Sei $\sigma \in G$, dann ist $\mathcal{O}$ σ-invariant. Ist zusätzlich $\mathfrak{p}$ ein Primideal in $\mathcal{o}$ und $\mathfrak{P}$ ein Primideal von $\mathcal{O}$ über $\mathfrak{p}$, so ist $\sigma\mathfrak{P}$ wieder ein Primideal von $\mathcal{O}$ über $\mathfrak{p}$.*

Beweis. Sei $a \in \mathcal{O}$. Dann existiert ein normiertes $P \in \mathcal{o}[X]$, sodass $P(a) = 0$. Da die Koeffizienten von P in K liegen, ist $P(\sigma a) = \sigma P(a) = 0$, folglich $\sigma a \in \mathcal{O}$. Ist $\mathfrak{P}$ ein Primideal von $\mathcal{O}$ über $\mathfrak{p}$, ist hiermit $\sigma\mathfrak{P}$ wieder ein Primideal von $\mathcal{O}$. Zudem ist $\sigma\mathfrak{P} \cap \mathcal{o} = \sigma(\mathfrak{P} \cap \mathcal{o}) = \sigma\mathfrak{p} = \mathfrak{p}$, folglich ist $\sigma\mathfrak{P}$ ebenfalls ein Primideal über $\mathfrak{p}$. □

Bemerkung 10.2. G operiert folglich auf der Menge der Primideale über $\mathfrak{p}$. Die $\sigma\mathfrak{P}$ werden auch die zu $\mathfrak{P}$ konjugierten Primideale genannt.

Satz 10.3. *G operiert transitiv auf der Menge der Primideale über $\mathfrak{p}$.*

Beweis. Angenommen es gibt zwei Primideale $\mathfrak{P}$ und $\mathfrak{P}'$ über $\mathfrak{p}$, sodass für alle $\sigma \in G$ gilt, dass $\sigma\mathfrak{P} \neq \mathfrak{P}'$. Wir erinnern uns, dass $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, wobei das Produkt die Primideale über $\mathfrak{p}$ durchläuft. Mit dem chinesischen Restsatz ist $\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}$, was die Exitenz eines $x \in \mathcal{O}$ impliziert, sodass $x \equiv 0 \bmod \mathfrak{P}'$ und $x \equiv 1 \bmod \sigma\mathfrak{P}$ für alle $\sigma \in G$.
Sei $N = \prod_{\sigma\in G} \sigma x$, so ist für $\sigma \in G$ beliebig $\sigma N = N$, folglich $N \in K$ und somit $N \in \mathcal{o}$. Nach Konstruktion ist somit $N \in \mathfrak{P}' \cap \mathcal{o} = \mathfrak{p}$. Es ist aber ebenfalls $\sigma x \notin \mathfrak{P}$ für alle $\sigma \in G$, folglich $N \notin \mathfrak{p}$, was ein Widerspruch ergibt. Somit folgt $\sigma\mathfrak{P} = \mathfrak{P}'$ für ein $\sigma \in G$. □

Definition 10.4. *Für ein Primideal $\mathfrak{P}$ von O sei die Zerlegungsgruppe von $\mathfrak{P}$ über K definiert als die Untergruppe $G_{\mathfrak{P}} := \{\sigma \in G | \sigma\mathfrak{P} = \mathfrak{P}\}$ und der Zerlegungskörper von $\mathfrak{P}$ über K als den Fixkörper $Z_{\mathfrak{P}} := \{x \in L | \forall \sigma \in G_{\mathfrak{P}} : \sigma x = x\}$.*

Bemerkung 10.5. Es existiert insbesondere eine wohldefinierte Bijektion zwischen den Nebenklassen $G/G_{\mathfrak{P}}$ und der Menge der konjugierten Primideale von $\mathfrak{P}$, gegeben durch $\sigma G_{\mathfrak{P}} \mapsto \sigma\mathfrak{P}$. Insbesondere ist die Anzahl der konjungierten Primidealen gegeben durch $[G : G_{\mathfrak{P}}]$. Insbesondere ist $\mathfrak{p}$ voll zerlegt genau dann, wenn $G_{\mathfrak{P}} = 1$ und unzerlegt, genau dann, wenn $G_{\mathfrak{P}} = G$.

Satz 10.6. *Für die Zerlegung $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ mit Trägheitsgraden $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}]$ gilt $f_1 = \ldots = f_r =: f$ und $e_1 = \ldots = e_r =: e$. Für ein entsprechendes Repräsentantensystem von $G/G_{\mathfrak{P}}$ erhalten wir somit die Zerlegung $\mathfrak{p}\mathcal{O} = (\prod_{\sigma} \sigma\mathfrak{P})^e$.*

Beweis. Setze $\mathfrak{P} = \mathfrak{P}_1$. Aus Satz 3 folgt, dass $\sigma_i \in G$ existieren, sodass $\mathfrak{P}_i = \sigma_i\mathfrak{P}$. Für alle i induziert σ_i einen Isomorphismus zwischen $\mathcal{O}/\mathfrak{P}$ und $\mathcal{O}/\sigma_i\mathfrak{P}$, gegeben durch $x\mathfrak{P} \mapsto \sigma_i x\,(\sigma_i\mathfrak{P})$, folglich ist $f_i = [\mathcal{O}/\sigma_i\mathfrak{P} : \mathcal{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}] = f_1 =: f$.
Da $\mathcal{O}$ G-invariant ist, folgt für alle i $\sigma_i(\mathfrak{p}\mathcal{O}) \subseteq \mathfrak{p}\mathcal{O}$. Da σ_i invertierbar ist, folgt $\sigma_i(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$, folglich $\mathfrak{P}^\nu | \mathfrak{p}\mathcal{O} \Leftrightarrow \sigma_i(\mathfrak{P}^\nu) | \sigma_i(\mathfrak{p}\mathcal{O}) \Leftrightarrow (\sigma_i\mathfrak{P})^\nu | \mathfrak{p}\mathcal{O}$ und damit $e_i = e_1 =: e$. □

Satz 10.7. *Man betrachte die Körpererweiterung $Z_{\mathfrak{P}}|K$, sei $\mathcal{O}_Z$ der ganze Abschluss von $\mathcal{o}$ in $Z_{\mathfrak{P}}$. Sei $\mathfrak{P}_Z := \mathfrak{P} \cap \mathcal{O}_Z$ das Primideal von $Z_{\mathfrak{P}}$ unter $\mathfrak{P}$. So ist:*

(i) *$\mathfrak{P}_Z$ ist unzerlegt in L.*
(ii) *$\mathfrak{P}$ hat über $Z_{\mathfrak{P}}$ den Verzweigungsgrad e und Trägheitsgrad f.*
(iii) *$\mathfrak{P}_Z$ hat über K den Verzweigungsgrad 1 und Trägheitsgrad 1.*

Beweis. Aus dem Hauptsatz der Galoistheorie folgt $G(L|Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$. Somit folgt auf Bemerkung 5, dass $\mathfrak{P}_Z$ unzerlegt ist.
Man erinnere sich, an die fundamentalste Gleichung $\sum_{i=1}^{r} e_i f_i = n$, im galoisschen Fall ergibt sich entsprechend $ref = n$. Da r die Anzahl der Primideale über $\mathfrak{p}$ ist, ist $r = [G : G_{\mathfrak{P}}]$. Da $Z_{\mathfrak{P}}$ der Fixkörper von $G_{\mathfrak{P}}$ ist, folgt hiermit $[L : Z_{\mathfrak{P}}] = |G_{\mathfrak{P}}| = ef$. Wir bezeichnen die Verzweigungsindezes und Trägheitsgrade von $\mathfrak{P}$ über $Z_{\mathfrak{P}}$ bzw. $\mathfrak{P}_z$ über K mit e' und f' bzw. e'' und f''. Es ist nach (i) $\mathfrak{P}_Z\mathcal{O} = \mathfrak{P}^{e'}$. Zudem erhalten wir in $Z_{\mathfrak{P}}|K$ die Zerlegung $\mathfrak{p}\mathcal{O}_Z = \mathfrak{P}_Z^{e''} * (\ldots)$ für weitere über $\mathfrak{p}$ liegenden Primideale. Da $\mathfrak{P}$ das eindeutige über $\mathfrak{P}_Z$ liegende Primideal ist, erhalten wir die Zerlegung $\mathfrak{p}\mathcal{O} = \mathfrak{P}^{e'e''} * (\ldots)$. Insbesondere folgt $e = e'e''$.
Mithilfe der Inklusionen $\mathcal{o}/\mathfrak{p} \hookrightarrow \mathcal{O}_Z/\mathcal{P}_Z \hookrightarrow \mathcal{O}/\mathfrak{P}$ folgt genauso
$f = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{O}_Z/\mathcal{P}_Z]\,[\mathcal{O}_Z/\mathcal{P}_Z : \mathcal{o}/\mathfrak{p}] = f'f''$.
Für die Zerlegung $\mathfrak{P}_Z\mathcal{O} = \mathfrak{P}^{e'}$ erhält man zudem aus der fundamentalsten Gleichung
$e'e''f'f'' = ef = [L : Z_{\mathfrak{P}}] = e'f'$. Da $e' \leqslant e$ und $f' \leqslant f''$, folgt also $e' = e$, $f' = f'$, $e'' = 1$ und $f'' = 1$. □

Satz 10.8. *$(\mathcal{O}/\mathfrak{P}) \,|\, (\mathcal{o}/\mathfrak{p})$ ist normal.*

Beweis. Man betrachte ein beliebiges Element $\theta\mathfrak{P} \in \mathcal{O}/\mathcal{P}$. Seien $f \in K[x]$ und $\bar{g} \in (\mathcal{o}/\mathfrak{p})[X]$ die Minimalpolynome von θ und $\theta\mathfrak{P}$. Sei $\bar{f}$ das Bild unter dem Reduktionshomomorphismus $K[X] \to (\mathcal{o}/\mathfrak{p})[X]$, so folgt $\bar{f}(\theta\mathfrak{P}) = 0$, was $\bar{g}|\bar{f}$ impliziert. Da $L|K$ normal ist, zerfällt f in $K[X]$ in Linearfaktoren, unter dem Reduktionshomomorphismus zerfällt $\bar{f}$ in $(\mathcal{o}/\mathfrak{p})[X]$ somit auch in Linearfaktoren, und damit ebenfalls $\bar{g}$. Somit ist $(\mathcal{O}/\mathfrak{P}) \,|\, (\mathcal{o}/\mathfrak{p})$ normal. □

Satz 10.9. *$\Phi : G_{\mathfrak{P}} \twoheadrightarrow \mathrm{Aut}_{(\mathcal{o}/\mathfrak{p})}(\mathcal{O}/\mathfrak{P}), \sigma \mapsto (a\mathfrak{P} \mapsto \sigma a\mathfrak{P})$ definiert einen surjektiven Homomorphismus.*

Beweis. Da $\sigma\mathcal{O} = \mathcal{O}$ und $\sigma\mathfrak{P} = \mathfrak{P}$ ist Φ ein wohldefinierter Homomorphismus.
Aus Satz 7 wissen wir $[\mathcal{O}_\mathcal{Z}/\mathcal{P}_\mathcal{Z} : \mathfrak{o}/\mathfrak{p}] = 1$, die Inklusion $\mathfrak{o}/\mathfrak{p} \hookrightarrow \mathcal{O}_\mathcal{Z}/\mathcal{P}_\mathcal{Z}$ ist folglich ein Isomorphismus, demnach genügt es O.B.d.A. den Fall $\mathfrak{p} = \mathcal{P}_\mathcal{Z}$ und $K = Z_\mathfrak{P}$ zu betrachten. Daraus ergibt sich entsprechend $\mathfrak{o} = \mathcal{O}_\mathcal{Z}$ und $G = G_\mathfrak{P}$. Sei nun $\tilde{K}$ der eindeutige Zwischenkörper von $(\mathcal{O}/\mathfrak{P})\,|\,(\mathfrak{o}/\mathfrak{p})$, sodass $\tilde{K}|\,(\mathfrak{o}/\mathfrak{p})$ seperabel und $(\mathcal{O}/\mathfrak{P})\,|\tilde{K}$ rein inseperabel ist, das heißt
$\tilde{K} = \{a \in \mathcal{O}/\mathfrak{P} | a \text{ ist seperabel über } \mathfrak{o}/\mathfrak{p}\}$. Dann ist $\tilde{K}|\,(\mathfrak{o}/\mathfrak{p})$ eine endliche galoissche Körpererweiterung mit Galoisgruppe $\tilde{G}$. Da $(\mathcal{O}/\mathfrak{P})\,|\tilde{K}$ rein inseperabel ist, ist $\mathrm{Aut}_{\tilde{K}}\,(\mathcal{O}/\mathfrak{P}) = \left\{\mathrm{id}_{\mathcal{O}/\mathfrak{P}}\right\}$, folglich ist die Einschränkung auf $\tilde{K}$ ein Isomorphismus zwischen $\mathrm{Aut}_{(\mathfrak{o}/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})$ und $\tilde{G}$, wir können folglich $\mathrm{Aut}_{(\mathfrak{o}/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})$ durch $\tilde{G}$ identifizieren.
Nach dem Satz des primitiven Elements kann man ein $\tilde{a}$ wählen, sodass $\tilde{K} = (\mathfrak{o}/\mathfrak{p})\,(\tilde{a})$. Sei $a \in L$, sodass $a\mathfrak{P} = \tilde{a}$. Seien nun $f \in K[x]$ und $\bar{g} \in (\mathfrak{o}/\mathfrak{p})\,[X]$ die Minimalpolynome von a und $\tilde{a}$ und $\bar{f}$ das Bild von f in $\mathfrak{o}/\mathfrak{p}$. Sei $\tilde{\sigma} \in \tilde{G}$ beliebig, dann ist $\bar{g}(\tilde{\sigma}\tilde{a}) = \bar{f}(\tilde{\sigma}\tilde{a}) = 0$. Da f in Linearfaktoren zerfällt, existiert $a' \in L$, sodass $a'\mathfrak{P} = \tilde{\sigma}\tilde{a}$ und $f(a') = 0$. Insbesondere existiert also $\sigma \in G$, sodass $\sigma a = a'$. Da durch das Bild des primitiven Elementes ein Automorphismus eindeutig definiert ist, ist mit $\Phi(\sigma)(\tilde{a}) = \sigma a\mathfrak{P} = a'\mathfrak{P} = \tilde{\sigma}\tilde{a}$ folglich $\Phi(\sigma) = \tilde{\sigma}$, also ist Φ surjektiv. □

Definition 10.10. *Wir nennen den Kern von Φ auch die Trägheitsgruppe von $\mathfrak{P}$ über K und bezeichnen ihn mit $I_\mathfrak{P}$. Der Trägheitskörper $T_\mathfrak{P}$ ist dann entsprechend definiert als der Fixkörper von $I_\mathfrak{P}$ in L.*

Korollar 10.11. *Die Erweiterung $T_\mathfrak{P}|Z_\mathfrak{P}$ ist wieder galoissch, und es ist $G(T_\mathfrak{P}|Z_\mathfrak{P}) \cong \mathrm{Aut}_{(\mathfrak{o}/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})$ und $G(L|T_\mathfrak{P}) = I_\mathfrak{P}$.*

Beweis. Als Kern eines Homomorphismus ist $I_\mathfrak{P}$ ein Normalteiler von $G_\mathfrak{P}$, insbesondere folgt aus dem Hauptsatz der Galoistheorie, dass $T_\mathfrak{P}|Z_\mathfrak{P}$ normal ist. $G(T_\mathfrak{P}|Z_\mathfrak{P}) \cong \mathrm{Aut}_{(\mathfrak{o}/\mathfrak{p})}\,(\mathcal{O}/\mathfrak{P})$ folgt dann entsprechend aus dem Isomorphiesatz, $G(L|T_\mathfrak{P}) = I_\mathfrak{P}$ folgt aus der Definition von $T_\mathfrak{P}$. □

Satz 10.12. *Wir nehmen zudem an, dass $(\mathcal{O}/\mathfrak{P})\,|\,(\mathfrak{o}/\mathfrak{p})$ ebenfalls galoissch ist, so gilt $|I_\mathfrak{P}| = e$ und $[G_\mathfrak{P} : I_\mathfrak{P}] = f$.*
Betrachte man den Körperturm $K|Z_\mathfrak{P}|T_\mathfrak{P}|L$, und sei dann wieder mit $\mathfrak{P}_T$ das unter $\mathfrak{P}$ liegende Primideal von $T_\mathfrak{P}$ bezeichnet, so hat $\mathfrak{P}$ über $\mathfrak{P}_T$ den Verzweigungsindex e und Trägheitsgrad 1, $\mathfrak{P}_T$ hat über $\mathfrak{P}_Z$ den Verzweigungsindex 1 und Trägheitsgrad f.

Beweis. Falls $(\mathcal{O}/\mathfrak{P})\,|\,(\mathfrak{o}/\mathfrak{p})$ galoissch ist, ist die Körpererweiterung insbesondere seperabel, so ist insbesondere $[G_\mathfrak{P} : I_\mathfrak{P}] = |G(T_\mathfrak{P}|Z_\mathfrak{P})| = |G(\mathcal{O}/\mathfrak{P}|\mathfrak{o}/\mathfrak{p})| = [\mathcal{O}/\mathfrak{P} : \mathfrak{o}/\mathfrak{p}] = f$. Da $|G_\mathfrak{P}| = ef$, folgt $|I_\mathfrak{P}| = e$.
Sei $\mathcal{O}_T$ der ganzer Abschluss von $\mathfrak{o}$ in $T_\mathfrak{P}$. Per Definition wird $I_\mathfrak{P}$ durch Φ auf das neutrale Element abgebildet, was insbesondere auch für den entsprechenden Homomorphismus
$I_\mathfrak{P} \to \mathrm{Aut}_{(\mathcal{O}_\mathcal{T}/\mathcal{P}_\mathcal{T})}\,(\mathcal{O}/\mathfrak{P})$ gilt. Nach Satz 9 ist dieser Homomorphismus surjektiv, folglich ist $[\mathcal{O}/\mathfrak{P} : \mathcal{O}_\mathcal{T}/\mathcal{P}_\mathcal{T}] = 1$. Da $I_\mathfrak{P}$ eine Untergruppe von $G_\mathfrak{P}$ ist, lässt $I_\mathfrak{P}$ ebenfalls $\mathfrak{P}$ invariant, somit ist $\mathfrak{P}_T$ unzerlegt in L, somit folgt aus der fundamentalsten Gleichung, dass der Verzweigungsindex e ist.
Da $f = [\mathcal{O}/\mathfrak{P} : \mathfrak{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{O}_\mathcal{T}/\mathcal{P}_\mathcal{T}]\,[\mathcal{O}_\mathcal{T}/\mathcal{P}_\mathcal{T} : \mathcal{O}_\mathcal{Z}/\mathcal{P}_\mathcal{Z}]$, folgt dass $\mathfrak{P}_T$ über $\mathfrak{P}_Z$ Trägheitsgrad f hat. Entsprechend folgt wieder aus Unzerlegtheit, dass der Verzweigungsindex 1 ist. □

10.2. **Der Lokale Frobenius.**

Beispiel 10.13. *Wir betrachten den Fall $\mathfrak{o} = \mathbb{Z}$, folglich $K = \mathbb{Q}$ und zusätzlich eine endliche Galois Erweiterung $L|\mathbb{Q}$. Sei $\mathfrak{P}$ ein unverzweigtes Primideal in $\mathbb{Z}_L$ über ein Primideal (p). Dann existiert genau ein $\sigma \in G(L|\mathbb{Q})$, sodass für alle $a \in \mathbb{Z}_L$ gilt, dass $\sigma(a) \equiv a^p \bmod \mathfrak{P}$. Dieser Automorphismus wird auch der lokale Frobenius zum Primideal $\mathfrak{P}$ über (p) genannt.*

Beweis. Man bemerke, dass $\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p)$ eine endliche Körpererweiterung der Charakteristik p ist. Insbesondere ist die Erweiterung zyklisch mit $G(\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p)) = \langle F\rangle$, wobei
$F : \mathbb{Z}_L/\mathfrak{P} \to \mathbb{Z}_L/\mathfrak{P}, x \mapsto x^p$ der Frobeniusendomorphismus ist.
Da insbesondere $\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p)$ galoissch ist, und da $\mathfrak{P}$ unverzweigt ist, folgt aus Satz 12, dass $I_\mathfrak{P} = 1$, somit ist der Homomorphismus $\Phi : G_\mathfrak{P} \to G(\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p))$ aus Satz 9 ein Isomorphismus. Folglich gibt es genau ein $\sigma := \Phi^{-1}(F) \in G_\mathfrak{P}$, sodass für alle $a \in \mathbb{Z}_L$ gilt, dass $\sigma a \equiv a^p \bmod \mathfrak{P}$.
Da jedes Element aus $G(L|\mathbb{Q})$, welches diese Eigenschaft hat insbesondere $\mathfrak{P}$ invariant lässt, liegt dieses ebenfalls in $G_\mathfrak{P}$, folglich ist dieses σ in ganz $G(L|\mathbb{Q})$ eindeutig. □

Bemerkung 10.14. Falls $G(L|\mathbb{Q})$ abelsch ist, so ist dieser Automorphismus unabhängig von der Wahl von $\mathfrak{P}$. Dann schreibe man für den lokalen Frobenius auch $\left(\frac{L/\mathbb{Q}}{p}\right)$.

Beweis. Seien $\mathfrak{P}$ und $\mathfrak{P}'$ zwei verschiedene Primideale über (p), und seien entsprechend σ und σ' ihre lokalen Frobeniusabbildungen. Nach Satz 3 können wir ein $\tau \in G(L|\mathbb{Q})$ wählen, sodass $\tau\mathfrak{P} = \mathfrak{P}'$. Sei $a \in \mathbb{Z}_L$ beliebig, dann ist $\left(\tau \circ \sigma \circ \tau^{-1}\right)(a\mathfrak{P}') = \tau\left(\sigma\left(\tau^{-1}(a)\,\mathfrak{P}\right)\right) = \tau\left(\left(\tau^{-1}(a)\right)^p \mathfrak{P}\right) = a^p\mathfrak{P}'$, aus der Eindeutigkeit folgt somit $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. Im Fall einer abelschen Erweiterung folgt schließlich $\sigma = \sigma'$. □

Lemma 10.15. *Sei das Primideal $\mathfrak{P}$ in L über (p) unverzweigt. Dann ist der lokale Frobenius der triviale Automorphismus genau dann, wenn (p) total zerlegt ist.*

Beweis. Aus der Konstruktion des lokalen Frobenius folgt, dass dieser nur dann trivial sein kann, falls F in $G(\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}/(p)) = \langle F\rangle$ trivial ist, was gleichbedeutend ist mit $f = 1$, das heißt (p) ist total zerlegt, ist. □

Lemma 10.16. *Für quadratfreies a und einer ungeraden zur a teilerfremden Primzahl p ist $\left(\frac{a}{p}\right) = 1$ genau dann, wenn (p) total zerlegt in $\mathbb{Q}(\sqrt{a})$ ist.*

Beweis. Es ist $\left(\frac{a}{p}\right) = 1$ per Definition genau dann, wenn ein $\alpha \in \mathbb{Z}$ existiert, sodass für die Polynome gilt $x^2 - a \equiv (x-\alpha)(x+\alpha) \bmod (p)$. Jetzt ist $x^2 - a$ das Minimalpolynom von $\sqrt{a}$, und da q und a teilerfremd sind, zerfällt dieses also in unterschiedliche Linearfaktoren, nach dem Zerlegungsgesetz aus Vorlesung 4 folgt demnach, dass (p) totalzerlegt in $\mathbb{Q}(\sqrt{a})$ ist.
Ist hingegen $\left(\frac{a}{p}\right) = -1$, so ist $x^2 - a$ irreduzibel mod$p$, insbesondere erhielte man $f = 2$, (p) wäre dann nicht total zerlegt in $\mathbb{Q}(\sqrt{a})$. □

Beispiel 10.17. *Hiermit erhalten wir einen alternativen Beweis für das quadratische Reziprozitätsgesetz $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ für zwei verschiedene ungerade Primzahlen p und q.*

Beweis. Sei $q^\star := (-1)^{\frac{q-1}{2}} q$. Nach der 2. Vorlesung folgt aus der Multiplikativität $\left(\frac{q^\star}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$. Es genügt folglich $\left(\frac{q^\star}{p}\right) = \left(\frac{p}{q}\right)$ zu zeigen.
Man betrachte hierfür den Körperturm $\mathbb{Q}(\zeta_q)|\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q}$ für eine $q$te primitive Einheitswurzel. Da $G(\mathbb{Q}(\zeta_q)|\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$, ist die Erweiterung abelsch, zudem ist, da p und q verschiedene Primzahlen sind, p unverzweigt in $\mathbb{Q}(\zeta_q)$, folglich auch in $\mathbb{Q}(\sqrt{q^\star})$.
Seien $\mathfrak{P}$ und $\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Q}(\sqrt{q^\star})$ Primideale von $\mathbb{Q}(\zeta_q)$ bzw. $\mathbb{Q}(\sqrt{q^\star})$ über (p). Man bemerke, dass $\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q}$ normal ist. Da zudem für alle $a \in \mathbb{Z}_{\mathbb{Q}(\sqrt{q^\star})}$ gilt, dass $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)|_{\mathbb{Q}(\sqrt{q^\star})}(a) - a^p \in \mathfrak{P} \cap \mathbb{Q}(\sqrt{q^\star}) = \mathfrak{P}'$, ist $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)|_{\mathbb{Q}(\sqrt{q^\star})} = \left(\frac{\mathbb{Q}(\sqrt{q^\star})/\mathbb{Q}}{p}\right)$.
Da $\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q}$ normal ist, erhält man nach dem Hauptsatz der Galoistheorie durch die Einschränkung einen Isomorphismus $G(\mathbb{Q}(\zeta_q)|\mathbb{Q})/G(\mathbb{Q}(\zeta_q)|\mathbb{Q}(\sqrt{q^\star})) \to G(\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q})$, beziehungsweise somit einen surjektiven Homomorphismus $G(\mathbb{Q}(\zeta_q)|\mathbb{Q}) \twoheadrightarrow G(\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q}), \sigma \mapsto \sigma_{\mathbb{Q}(\sqrt{q^\star})}$. Da $G(\mathbb{Q}(\zeta_q)|\mathbb{Q})$ und $G(\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q})$ zyklisch sind, ist solch ein Homomorphismus eindeutig. Wir identifizieren $G(\mathbb{Q}(\zeta_q)|\mathbb{Q})$ durch $(\mathbb{Z}/q\mathbb{Z})^\times$ und $G(\mathbb{Q}(\sqrt{q^\star})|\mathbb{Q})$ durch $\{1,-1\}$. Aus Vorlesung 2 folgt, dass dieser Homomorphismus dann eindeutigerweise durch $a \mapsto \left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}} \bmod q$ definiert ist.
Sei $\sigma \in G(\mathbb{Q}(\zeta_q)|\mathbb{Q})$ definiert durch $\zeta_q \mapsto \zeta_q^p$. Da $p \in \mathfrak{P}$, folgt für alle $a \in \mathbb{Z}_{\mathbb{Q}(\zeta_q)}$ somit $\sigma(a) \equiv a^p \bmod \mathfrak{P}$, folglich aus Eindeutigkeit $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right) = \sigma$. Unter der obigen Identifikation ist die Einschränkung auf $\mathbb{Q}(\sqrt{q^\star})$ gegeben als $\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right)|_{\mathbb{Q}(\sqrt{q^\star})} = \left(\frac{\mathbb{Q}(\sqrt{q^\star})/\mathbb{Q}}{p}\right) = \left(\frac{p}{q}\right)$.
Aus Lemma 15 und 16 folgt entsprechend $\left(\frac{\mathbb{Q}(\sqrt{q^\star})/\mathbb{Q}}{p}\right) = \left(\frac{q^\star}{p}\right)$, folglich haben wir $\left(\frac{q^\star}{p}\right) = \left(\frac{p}{q}\right)$ gezeigt. □

11. Geometrie der Zahlen und Endlichkeit der Klassenzahl

Marcel Pirron, *pirronm@student.ethz.ch*

In diesem Abschnitt zeigen wir, dass die definierte Klassengruppe Cl_K für einen Zahlkörper K stets endlich ist und skizzieren den Dirichletschen Einheitensatz, um die Einheiten von $\mathcal{O}_K$ näher zu bestimmen. Unsere Untersuchungen werden uns über die *Geometrie der Zahlen* führen, eine auf Hermann Minkowski zurückgehende Theorie, in der die Elemente der Zahlkörper als

Punkte in einem Vektorraum angesehen werden. Diese Betrachtungsweise haben wir bereits bei den Gaussschen Zahlen gesehen, wobei wir die Inklusion $\mathbb{Z}[i] \subseteq \mathbb{C}$ ausnutzten und $\mathbb{Z}[i]$ als Gitter in der komplexen Ebene interpretiert haben.

11.1. **Gitter.** Die Protagonisten dieses Abschnittes werden die Gitter sein. Sie stellen eine Verallgemeinerung der eben angesprochenen Idee dar.

Definition 11.1. *Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und seien $v_1, \dots, v_m \in V$ linear unabhängig. Das **Gitter** in V zur **Basis** $(v_1, \dots, v_m)$ ist die Menge*

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m.$$

Ferner nennen wir die Menge

$$\Phi = \left\{ \sum_{i=1}^{m} x_i v_i \mid x_i \in \mathbb{R} \cap [0,1) \right\}$$

*eine **Grundmasche** des Gitters. Ein Gitter heisst **vollständig**, wenn $m = n$ ist.*

Bemerkung 11.2. In einem vollständigen Gitter überdecken die Verschiebungen $\Phi + \gamma, \gamma \in \Gamma$ den gesamten Raum V.

Diese Definition liefert eine klare geometrische Charakterisierung der Gitter. Es ist klar, dass beispielsweise $\mathbb{Z}[i]$ ein Gitter ist. Jeder Untervektorraum enthält generell eine Vielzahl von Gittern. Man erhält diese, wenn man eine Basis wählt und nur Linearkombinationen mit ganzzahligen Koeffizienten betrachtet. Diese erste Definition bezieht sich also noch auf die Wahl linear unabhängiger Vektoren. Wir erstreben nun eine äquivalente Definition, die frei von einer solchen Wahl ist. Dazu bemerken wir zunächst, dass ein Gitter eine endlich erzeugte Untergruppe von V ist. Mit der endlich erzeugten Untergruppe $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{R}$ ist aber auch schnell ein Beispiel gefunden, welches zeigt, dass diese Eigenschaft die Gitter noch nicht eindeutig charakterisieren kann. Die Hinzunahme einer weiteren Eigenschaft stellt sich jedoch als ausreichend heraus.

Satz 11.3. *Eine Untergruppe $\Gamma \subseteq V$ ist genau dann ein Gitter, wenn sie diskret ist.*

Beweis. Es ist klar, dass ein Gitter eine diskrete Untergruppe ist. Sei also nun Γ eine diskrete Untergruppe von V und $V_0 := \langle \Gamma \rangle$ der von Γ erzeugte Unterraum. Dann können wir eine Basis von V_0 aus Vektoren $u_1, \dots, u_m \in \Gamma$ bilden und das vollständige Gitter

$$\Gamma_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subseteq \Gamma$$

von V_0 betrachten. Falls der Index $q := [\Gamma : \Gamma_0]$ endlich ist, so ist $q\Gamma \subseteq \Gamma_0$ und

$$\Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z}\left(\frac{1}{q}u_1\right) + \cdots + \mathbb{Z}\left(\frac{1}{q}u_m\right).$$

Aus dem Hauptsatz über endlich erzeugte abelsche Gruppen folgt nun unmittelbar, dass Vektoren $v_1, \dots, v_r$ mit $r \leqslant m$ existieren, so dass $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r$. Da $v_1, \dots, v_r$ den m-dimensionalen Vektorraum V_0 aufspannen, sind diese linear unabhängig und es folgt, dass Γ ein Gitter ist.

Es verbleibt $q < \infty$ zu zeigen. Hierzu wählen wir einen Repräsentanten $\gamma_i \in \Gamma$ zu jeder Nebenklasse in Γ/Γ_0. Da Γ_0 vollständig in V_0 ist, überdecken die Verschiebungen der Grundmasche Φ_0 den ganzen Raum V_0. Für jedes γ_i finden wir also ein $\mu_i \in \Phi_0$ und $\gamma_{0i} \in \Gamma_0$, so dass $\gamma_i = \mu_i + \gamma_{0i}$. Die $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$ bilden eine diskrete Teilmenge der Gruppe Γ und liegen in der beschränkten Menge Φ_0, womit ihre Anzahl endlich sein muss. Damit ist auch die Anzahl der Nebenklassen begrenzt. □

Bemerkung 11.4. Nebenbei haben wir auch gezeigt, dass die 0 ein Häufungspunkt von $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ ist. Dies folgt auch aus dem Dirichlet Lemma, welches bei der Pell Gleichung besprochen wurde.

Uns geht es nun darum, den Minkowskischen Gitterpunktsatz zu beweisen. Dieser wird für unsere Anwendungen in der Zahlentheorie von grosser Bedeutung sein. Dafür setzen wir von hier an vorraus, dass V ein euklidischer Vektorraum ist. Insbesondere soll $\dim(V) := n < \infty$ sein und es soll ein Skalarprodukt auf V geben. So können wir auf V einen Volumenbegriff wie folgt

definieren: Ist Q ein Würfel, der von einer Orthonormalbasis $e_1, \dots, e_n$ aufgespannt wird, so setzen wir $\mathrm{vol}(Q) := 1$. Für n linear unabhängige Vektoren $v_1, \dots, v_n$ erhält das Parallelpiped

$$\Phi = \left\{ \sum_{i=1}^{n} x_i v_i \mid x_i \in \mathbb{R} \cap [0,1) \right\}$$

im Anschluss das Volumen $\mathrm{vol}(\Phi) := |\det(A)|$, wobei A die Übergangsmatrix von der Basis $e_1, \dots, e_n$ zu $v_1, \dots, v_n$ ist. Φ ist auch als Grundmasche des Gitters Γ zur Basis $v_1, \dots, v_n$ anzusehen und wir definieren

$$\mathrm{vol}(\Gamma) := \mathrm{vol}(\Phi).$$

Bemerkung 11.5. Das Gittervolumen ist basisunabhängig, da die Basiswechselmatrix zwischen zwei Gitterbasen ganzzahlige Koeffizenten hat und invertierbar ist. Somit hat sie Determinante ± 1 und lässt das Volumen unverändert.

Wir errinern letzlich noch an zwei Definitionen, ehe wir endlich den Gitterpunktsatz formulieren können. Eine Teilmenge $X \subseteq V$ heisst *zentralsymmetrisch*, falls für alle $x \in X$ auch $-x \in X$ ist und sie heisst *konvex*, wenn sie für alle Punkte $x, y \in X$ auch die Strecke $\{ty + (1-t)x \mid 0 \leqslant t \leqslant 1\}$ enthält.

Satz 11.6. *Sei Γ ein vollständiges Gitter in V und X eine zentralsymmetrische und konvexe Teilmenge von V. Falls*

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma),$$

so enthält X mindestens einen von Null verschiedenen Gitterpunkt.

Beweis. Es ist ausreichend zu zeigen, dass zwei verschiedene Gitterpunkte $\gamma_1, \gamma_2 \in \Gamma$ existieren, so dass

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

Dann lässt sich nämlich ein Punkt aus diesem Durchschnitt wählen

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2, \quad x_1, x_2 \in X,$$

so dass der Gitterpunkt

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

nun gleichzeitig der Mittelpunkt der Strecke von x_2 nach $-x_1$ und somit in $X \cap \Gamma$ ist.

Wären nun die Mengen $\frac{1}{2}X + \gamma, \gamma \in \Gamma$ paarweise disjunkt, so wären auch die Durchschnitte mit einer Grundmasche $\Phi \cap \left(\frac{1}{2}X + \gamma\right)$ disjunkt und es wäre

$$\mathrm{vol}(\Phi) \geqslant \sum_{\gamma \in \Gamma} \mathrm{vol}\left(\Phi \cap \left(\frac{1}{2}X + \gamma\right)\right).$$

Durch Translation mit $-\gamma$ erhalten wir aus $\Phi \cap \left(\frac{1}{2}X + \gamma\right)$ die Menge $(\Phi - \gamma) \cap \frac{1}{2}X$ von gleichem Volumen. Da die $\Phi - \gamma, \gamma \in \Gamma$ den ganzen Raum V, und insbesondere auch $\frac{1}{2}X$ überdecken, würden wir im Gegensatz zur Vorraussetzung

$$\mathrm{vol}(\Phi) \geqslant \sum_{\gamma \in \Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\mathrm{vol}(X)$$

erhalten. □

11.2. **Geometrie der Zahlen.** Um den Bezug zur Zahlentheorie herzustellen, wollen wir in diesem Abschnitt einem algebraischem Zahlkörper ein Gitter in einem geeigneten euklidischem Raum zuweisen. Wir betrachten also einen algebraischen Zahlkörper K vom Grad n und setzen $T := \mathrm{Hom}(K, \mathbb{C})$ für die Menge der **Einbettungen** von K in $\mathbb{C}$. Ferner definieren wir noch die Abbildung

$$j : K \to K_{\mathbb{C}} := \prod_{\tau \in T} \mathbb{C}, \quad a \mapsto (\tau a)_{\tau \in T}.$$

Es gibt insgesammt n Einbettungen, wovon r bereits reell sind $\rho_1, \dots, \rho_r : K \to \mathbb{R}$. Die anderen nicht-reelen gruppieren sich zu s Paaren $\sigma_1, \overline{\sigma}_1, \dots, \sigma_s, \overline{\sigma}_s : K \to \mathbb{C}$, so dass $n = r + 2s$.

Die komplexe Konjugation lässt sich nicht nur auf die Koordinaten von $\prod_{\tau \in T} \mathbb{C}$ anwenden, sondern liefert für jedes τ auch eine konjugierte Abbildung durch $\overline{\tau} z = \overline{\tau z}$. Zusammengenommen ergibt sich die Involution

$$F : K_{\mathbb{C}} \to K_{\mathbb{C}}, \quad z = (z_\tau)_{\tau \in T} \mapsto (\overline{z}_{\overline{\tau}})_{\tau \in T}.$$

Bemerkung 11.7. Für das Skalarprodukt auf $K_{\mathbb{C}}$ gilt $\langle Fx, Fy \rangle = \overline{\langle x, y \rangle}$.

Die unter F invarianten Punkte von $K_{\mathbb{C}}$ bezeichnen wir mit $K_{\mathbb{R}}$. Dies sind genau die Punkte (z_τ) mit $z_\tau = \overline{z}_{\overline{\tau}}$ beziehungsweise $\overline{z}_\tau = z_{\overline{\tau}}$. Aus $\overline{\tau} a = \overline{\tau a}$ mit $a \in K$ folgt somit $F(ja) = ja$ und wir können j als eine Abbildung $j : K \to K_{\mathbb{R}}$ ansehen. Zudem ergibt die Einschränkung des Standardskalarprodukts von $K_{\mathbb{C}}$ auf den $\mathbb{R}$-Vektorraum $K_{\mathbb{R}}$ ein reelles Skalarprodukt. Denn für $x, y \in K_{\mathbb{R}}$ ist $\langle x, y \rangle \in \mathbb{R}$, was aus Bemerkung 11.7 folgt, ausserdem folgen $\langle x, y \rangle = \overline{\langle x, y \rangle} = \langle y, x \rangle$ und $\langle x, x \rangle > 0$ aus den Eigenschaften des komplexen Skalarprodukts.

Eine konkrete Beschreibung von $K_{\mathbb{R}}$ liefert nun der folgende

Satz 11.8. *Wir erhalten einen Isomorphismus*

$$f : K_{\mathbb{R}} \to \prod_{\tau \in T} \mathbb{R} = \mathbb{R}^{r+2s}$$

durch die Zuordnung $(z_\tau) \mapsto (x_\tau)$ *mit*

$$x_\rho = z_\rho, \quad x_\sigma = \mathrm{Re}(z_\sigma), \quad x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma).$$

Das eingeschränkte Standardskalarprodukt wird hierdurch in das folgende Skalarprodukt überführt

$$(x, y) = \sum_{\tau \in T} \alpha_\tau x_\tau y_\tau,$$

wobei α_τ *gleich* 1 *ist, falls* τ *reell und gleich* 2 *ist, falls* τ *komplex ist.*

Beweis. Aus der vorangegangenen Diskussion ergibt sich die explizite Beschreibung von

$$K_{\mathbb{R}} = \{(z_\tau)_{\tau \in T} \in \prod_{\tau \in T} \mathbb{C} \mid z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z}_\sigma\},$$

woraus unmittelbar die gewünschte Isomorphie folgt. Seien nun $z = (z_\tau)_{\tau \in T} = (x_\tau + i y_\tau), z' = (z'_\tau)_{\tau \in T} = (x'_\tau + i y'_\tau) \in K_{\mathbb{R}}$. Dann ist $z_\rho \overline{z}'_\rho = x_\rho x'_\rho$ und

$$z_\sigma \overline{z}'_\sigma + z_{\overline{\sigma}} \overline{z}'_{\overline{\sigma}} = z_\sigma \overline{z}'_\sigma + \overline{z}_\sigma z'_\sigma = 2\mathrm{Re}(z_\sigma \overline{z}'_\sigma) = 2(x_\sigma x'_\sigma + x_{\overline{\sigma}} x'_{\overline{\sigma}}).$$

Die Anwendung des Isomorphismus' liefert die Behauptung über Skalarprodukte. □

Bemerkung 11.9. Das kanonische Volumen wird durch das Skalarprodukt von $K_{\mathbb{R}}$ auf $\mathbb{R}^{r+2s}$ übertragen. Mit dem üblichen Lebesgue-Mass steht es in folgendem Zusammenhang

$$\mathrm{vol}_{\mathrm{kanonisch}}(X) = 2^s \mathrm{vol}_{\mathrm{Lebesgue}}(f(X)).$$

Wir können nun die Verbindung zu den Idealen schlagen.

Satz 11.10. *Ist* $\mathfrak{a} \neq 0$ *ein Ideal von* $\mathcal{O}_K$*, so ist* $\Gamma = j\mathfrak{a}$ *ein vollständiges Gitter in* $K_{\mathbb{R}}$ *mit dem Grundmaschenvolumen*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}]$$

Da der Satz auf weiteren nicht behandelten Resultaten aufbaut, geben wir hierzu keinen Beweis an. Dieser findet sich aber in [4, 1.5]. Zusammen mit dem Minkowskischen Gitterpunktsatz ergibt sich nun dennoch das folgende wichtige Resultat.

Theorem 11.11. *Sei* $\mathfrak{a} \neq 0$ *ein ganzes Ideal von* K*, und seien* $c_\tau > 0$ *für alle* $\tau \in T$ *reelle Zahlen mit* $c_\tau = c_{\overline{\tau}}$ *und*

$$\prod_{\tau \in T} c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}].$$

Dann existiert ein $a \in \mathfrak{a}, a \neq 0$ *mit*

$$|\tau a| < c_\tau$$

für alle $\tau \in T$*.*

Beweis. Die Menge $X = \{(z_\tau)_{\tau\in T} \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$ ist zentralsymmetrisch und konvex. Ihr kanonisches Volumen ist das 2^s-fache des Inhalts von

$$f(X) = \{(x_\tau)_{\tau\in T} \in \prod_{\tau\in T} \mathbb{R} \mid |x_\rho| < c_\rho, x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2\}.$$

Also

$$\mathrm{vol}(X) = 2^s \mathrm{vol}_{\mathrm{Lebesgue}}(f(X)) = 2^s \prod_\rho (2c_\rho) \prod_\sigma (\pi c_\sigma^2) = 2^{r+s}\pi^s \prod_{\tau\in T} c_\tau.$$

Nach Vorraussetzung und mit dem vorrangegangenem Satz erhalten wir

$$\mathrm{vol}(X) > 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}] = 2^n \mathrm{vol}(\Gamma).$$

Es sind somit die Vorraussetzungen des Minkowskischen Gitterpunktsatz' erfüllt. X enthält also mindestens einen Gitterpunkt ja mit $a \neq 0, a \in \mathfrak{a}$. Die Aussage folgt nun aus der Definition von X. □

11.3. **Endlichkeit der Klassenzahl.** Wir sind nun in der Lage zu zeigen, dass die Idealklassengruppe $Cl_K = J_K/P_K$ für algebraische Zahlkörper K endlich ist. Wir nennen diese Ordnung im übrigen die **Klassenzahl** $h_K := [J_K : P_K]$. Auch $[\mathcal{O}_K : \mathfrak{a}]$ ist für Ideale $\mathfrak{a} \neq 0$ endlich und somit können wir die **Absolutnorm** von $\mathfrak{a}$

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

definieren.

Bemerkung 11.12. Ein Hauptideal (α) von $\mathcal{O}_K$ hat Absolutnorm $\mathfrak{N}((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$. Hiervon leitet sich auch der Name der Absolutnorm ab.

Es ergibt sich der folgende

Satz 11.13. *Ist $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ die Primzerlegung des Ideals $\mathfrak{a} \neq 0$, so gilt*

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

Beweis. Nach dem chinesischen Restsatz ist

$$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r}.$$

Es reicht also aus, Primidealpotenzen $\mathfrak{p}^\nu$ zu betrachten. In

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^\nu$$

ist $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ wegen der Eindeutigkeit der Primzerlegung und jeder Quotient $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ist ein $\mathcal{O}_K/\mathfrak{p}$ Vektorraum der Dimension 1. Es ist also $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K\ \mathfrak{p}$ und somit

$$\mathfrak{N}(\mathfrak{p}^\nu) = [\mathcal{O}_K : \mathfrak{p}^\nu] = [\mathcal{O}_K : \mathfrak{p}] \cdot [\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu] = \mathfrak{N}(\mathfrak{p})^\nu$$

□

Wir erhalten dadruch die Multiplikativität der Absolutnorm

$$\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}).$$

Diese lässt sich daher zu einem Homomorphismus auf allen gebrochenen Idealen $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$ fortsetzen

$$\mathfrak{N} : J_K \to \mathbb{R}_{>0}$$

Um die Endlichkeit der Klassenzahl zu beweisen, benötigen wir letztlich noch das folgende Lemma. Im Anschluss gehen wir direkt zum Beweis über die Klassenzahl über.

Lemma 11.14. *In jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}_K$ gibt es ein $a \in \mathfrak{a}, a \neq 0$ mit*

$$|N_{K|\mathbb{Q}}(a)| \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

Beweis. Für $\varepsilon > 0$ wählen wir reelle Zahlen $c_\tau > 0$ für alle $\tau \in T$, so dass $c_\tau = c_{\overline{\tau}}$ und

$$\prod_{\tau \in T} c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

Aus Theorem 11.11 ergibt sich die Existenz eines Elements $a \in \mathfrak{a}, a \neq 0$ mit $|\tau a| < c_\tau$, also

$$|N_{K|\mathbb{Q}}(a)| = \prod_{\tau \in T} |\tau a| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

Die linke Seite ist stets eine natürliche Zahl, woraus sich nun auch die Existenz eines $a \in \mathfrak{a}, a \neq 0$ mit

$$|N_{K|\mathbb{Q}}(a)| \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a})$$

ergibt. □

Theorem 11.15. *Die Klassenzahl eines algebraischen Zahlkörpers ist endlich.*

Beweis. Sei $\mathfrak{p} \neq 0$ ein Primideal von $\mathcal{O}_K$ und $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, so ist $\mathcal{O}_K/\mathfrak{p}$ eine endliche Erweiterung von $\mathbb{Z}/p\mathbb{Z}$ von Grad $f \geqslant 1$ und es ist

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

Für ein ausgewähltes p gibt es nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ wegen $\mathfrak{p}|(p)$. Daher gibt es nur endlich viele Primideale $\mathfrak{p}$ mit Absolutnorm kleiner einer gegebenen Schranke. Da jedes ganze Ideal $\mathfrak{a}$ eindeutig in Primideale zerlegt werden kann und die Absolutnorm multiplikativ ist, gibt es überhaupt nur endlich viele Ideale $\mathfrak{a}$ mit beschränkter Absolutnorm $\mathfrak{N}(\mathfrak{a}) \leqslant M$.

Es reicht daher aus, für jede Klasse $[a] \in Cl_K$ ein ganzes Ideal $\mathfrak{a}_1$ mit

$$\mathfrak{N}(\mathfrak{a}_1) \leqslant M := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

zu finden. Sei dazu $\mathfrak{a} \in [a]$ beliebig und $\gamma \in \mathcal{O}_K, \gamma \neq 0$ mit $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Mit Lemma 11.14 erhalten wir ein $\alpha \in \mathfrak{b}, \alpha \neq 0$ mit

$$|N_{K|\mathbb{Q}}(\alpha)| \cdot \mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}((\alpha)\mathfrak{b}^{-1}) = \mathfrak{N}(\alpha\mathfrak{b}^{-1}) \leqslant M.$$

Demnach hat das Ideal $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [a]$ die gewünschte Eigenschaft. □

11.4. **Der Dirichletsche Einheitensatz.** Zuletzt stellen wir noch eine weitere Anwendung der Gitter vor - den Dirichletschen Einheitensatz. Dieser erlaubt es, die Gruppe $\mathcal{O}_K^\times$ näher zu bestimmen. Wir werden seinen Beweis allerdings nur skizzenhaft besprechen können. Eine vollständige Behandlung findet sich in [4, 1.7].

Theorem 11.16. *Die Einheitengruppe $\mathcal{O}_K^\times$ von $\mathcal{O}_K$ ist das direkte Produkt der endlichen zyklischen Untergruppe der Einheitswurzeln $\mu(K)$ von K und einer freien abelschen Gruppe vom Rang $r + s - 1$.*

Es gibt also **Grundeinheiten** $\varepsilon_1, \ldots, \varepsilon_t, t = r + s - 1$, so dass sich jede weitere Einheit ε als ein Produkt

$$\varepsilon = \zeta\varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$$

mit einer Einheitswurzel ζ schreiben lässt. Wir werden im folgenden den Beweis der Aussage skizzieren.

Beweis. Wir nummerieren die Einbettungen, wobei wir diesmal aus jedem Paar komplexer Einbettungen genau eine auswählen $\tau_1, \ldots, \tau_{r+s} : K \to \mathbb{C}$. Zum Beweis studiert man die Abbildung

$$\lambda : \mathcal{O}^\times \to \mathbb{R}^{r+s}, \quad \varepsilon \mapsto (\log|\tau_j\varepsilon|^{\alpha_j})_{1 \leqslant j \leqslant r+s},$$

wobei α_j wieder gleich 1 oder 2 ist, je nachdem, ob τ_j reell oder komplex ist.

Nun zeigt man, dass für den Gruppenhomomorphismus λ gilt $\mathrm{Kern}(\lambda) = \mu(K)$. Da $\zeta \in \mu_K$ endliche Ordnung hat, wird ζ durch jede Einbettung auf eine Zahl vom Betrag 1 abgebildet und liegt somit im Kern von λ. Falls andererseits $\varepsilon \in \mathcal{O}_K^\times$ liegt, so ist $|\tau_j\varepsilon| = 1$ für alle Einbettungen. Der Kern von λ bildet also einen beschränkten Bereich in $K_\mathbb{R}$. Gleichzeitig ist $j\varepsilon$ ein Punkt des

Gitters $j\mathcal{O}_K$. Daraus folgt, dass Kern(λ) eine endliche Untergruppe von $K^\times$ ist und daher aus lauter Einheitswurzeln besteht.

Als nächstes betrachtet man den $t = r + s - 1$-dimensionalen Unterraum $H = \{x \in \mathbb{R}^{r+s} \mid \sum_{j=1}^{r+s} x_j = 0\}$ und zeigt, dass $\Gamma = \lambda(\mathcal{O}_K^\times)$ ein vollständiges Gitter in H, also isomorph zu $\mathbb{Z}^{r+s-1}$ ist. Man wählt dann eine $\mathbb{Z}$-Basis $v_1, \dots, v_t$ der freien abelschen Gruppe Γ. Seien $\varepsilon_1, \dots, \varepsilon_t \in \mathcal{O}_K^\times$ Urbilder der jeweiligen v_i. Dann wird die durch die ε_i erzeugte Untergruppe A durch λ isomorph auf Γ abgebildet. Es gilt somit $\mu(K) \cap A = \{1\}$ und daher $\mathcal{O}_K^\times = \mu(K) \times A$. □

12. Dirichlet L-Funktionen und Dichtigkeitssätze

Lara Imhof, *imhofl@student.ethz.ch*

In diesem Abschnitt betrachten wir die Riemannsche und Dedekindsche Zetafunktion anhand einiger Beispiele. Dann führen wir die Begriffe des Dirichletschen-Charakter und der Dirichletschen L-Funktion ein. Wir stellen fest, dass sich unter gewissen Voraussetzungen die Dedekindsche Zetafunktion zu einem Produkt aus Dirichletschen L-Funktionen und der Riemannschen Zetafunktion faktorisieren lässt. Danach überprüfen wir die Dirichletschte Klassenzahlformel anhand zweier Beispiele. Abschliessend führen wir zwei Dichtigkeitsbegriffe ein, welche wir für den Dirichletschen Primzahlsatz und den Chebotarev's Dichtigkeitssatz benötigen. Dieses Kapitel gibt einen Überblick über die oben genannten Themen. Diese werden in Anwendungen demonstriert, weswegen die meisten Behauptungen in diesem Kapitel nicht bewiesen werden. Für jeden Beweis ist jeweils eine Referenz angegeben, falls der Leser den Beweis nachschlagen möchte.
Wir folgen *Algebraische Zahlentheorie* von J. Neukirch [4] und *Einführung in die algebraische Zahlentheorie* von A. Schmidt [5].

12.1. **Die Riemannsche und Dedekindsche Zetafunktion.** In diesem Unterkapitel führen wir die Begriffe der Riemannschen Zetafunktion und der Dedekindschen Zetafunktion ein. Die Zetafunktion eines Zahlkörpers ist eine analytische Funktion, in welcher viele der arithmetischen Eigenschaften des Zahlkörpers enthalten sind. Die Zetafunktion ist auch von zentraler Bedeutung im Beweis des Dirichletschen Primzahlsatzes 12.31, welcher besagt, dass eine arithmetische Folge unendlich viele Primzahlen besitzt.

Wir beginnen mit dem Beweis der Konvergenz der Reihe (12.1).

Lemma 12.1. *Falls $s > 1$ reell, so konvergiert die Reihe*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \quad \textit{absolut.} \tag{12.1}$$

Für den Beweis von Lemma 12.1 und Theorem 12.2 folgen wir der Argumentation in [5].

Beweis. Aus der Analysis wissen wir, dass

$$0 \;<\; \int_1^\infty \frac{1}{x^s}\,\mathrm{d}x \;<\; \sum_{n=1}^{\infty} \frac{1}{n^s} \;<\; 1 + \int_1^\infty \frac{1}{x^s}\,\mathrm{d}x. \tag{12.2}$$

Aus dem Integralkriterium für Reihen folgt, dass die Reihe konvergiert genau dann, wenn das Integral auf der rechten Seite existiert, beziehungsweise einen endlichen Wert besitzt. Da $s > 1$ gilt für $N \geqslant 2$,

$$\int_1^N \frac{1}{x^s}\,\mathrm{d}x = \frac{N^{1-s} - 1}{1 - s}. \tag{12.3}$$

Für $N \to \infty$ strebt $N^{1-s} \to 0$, da $s > 1$. Daher gilt,

$$\sum_{n=1}^{\infty} \left|\frac{1}{n^s}\right| = \sum_{n=1}^{\infty} \frac{1}{n^s} < \lim_{N\to\infty} \int_1^N \frac{1}{x^s}\,\mathrm{d}x = 1 + \frac{1}{s-1} < \infty \tag{12.4}$$

und die Behauptung folgt. □

Aus dem obigen Lemma folgt folgendes Theorem über die Riemannsche Zetafunktion.

Theorem 12.2. *Sei $s \in \mathbb{C}$. Falls $\mathrm{Re}(s) > 1$, so konvergiert die Reihe*

$$\zeta(s) \;=\; \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{12.5}$$

*absolut. Des Weiteren ist die Abbildung $s \mapsto \zeta(s)$ auf $\left\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\right\}$ holomorph. Diese Abbildung wird **Riemannsche Zetafunktion** genannt, benannt nach dem deutschen Mathematiker BERNHARD RIEMANN.*

Beweis. Sei $\delta > 0$ Für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) \geqslant 1 + \delta$ gilt

$$|n^s| = |\exp(s\ \log(n))| = \exp(\mathrm{Re}(s)\ \log(n)) = n^{\mathrm{Re}(s)}. \tag{12.6}$$

Somit können wir die Summe folgendermassen umschreiben

$$\sum_{n=1}^{\infty} \left|\frac{1}{n^s}\right| \;=\; \sum_{n=1}^{\infty} \frac{1}{n^{\mathrm{Re}(s)}} \;\leqslant\; \sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}}. \tag{12.7}$$

Da $1 + \delta > 1$ reell können wir Lemma 12.1 anwenden:

$$\sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}} \;<\; \infty. \tag{12.8}$$

Mittels Majorantenkriterium folgt die absolute Konvergenz von (12.5).

Sei α sodass $\mathrm{Re}(s) > \alpha > 1$ beliebig. Definiere $D_\alpha = s \in \mathbb{C} | \,\mathrm{Re}(s) > \alpha$. Sei $N \in \mathbb{N}$, dann gilt

$$\sup_{s \in D_\alpha} \left| \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{N} \frac{1}{n^s} \right| = \sup_{s \in D_\alpha} \left| \sum_{n=N+1}^{\infty} \frac{1}{n^s} \right| \leqslant \sup_{s \in D_\alpha} \sum_{n=N+1}^{\infty} \frac{1}{n^\alpha} = \sum_{n=N+1}^{\infty} \frac{1}{n^\alpha} \to 0 \tag{12.9}$$

falls $N \to \infty$. Dies ergibt lokal gleichmässige Konvergenz. Mittels Weierstrasschem Konvergenzsatz folgt, dass die Abbildung $s \mapsto \zeta(s)$ auf $\left\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\right\}$ holomorph ist. □

Bemerkung 12.3. Für $s = 2$ beschreibt die Riemannsche Zetafunktion das Basler Problem, benannt nach den Basler Mathematikern LEONHARD EULER, den Brüdern JAKOB I und JOHANN I BERNOULLI. Ferner gilt

$$\zeta(2) \;=\; \sum_{n=1}^{\infty} \frac{1}{n^2} \;=\; \frac{\pi^2}{6}. \tag{12.10}$$

Wir können die Riemannsche Zetafunktion zu einer meromorphen Funktion auf einen grösseren Definitionsbereich ausdehnen.

Theorem 12.4. *Die Riemannsche Zetafunktion ist eindeutig zu einer holomorphen Funktion auf $\mathbb{C}\backslash\{1\}$ fortsetzbar, und sie besitzt einen einfachen Pol bei $s = 1$ mit Residuum 1.*

Für einen Beweis siehe *Algebraische Zahlentheorie* Kapitel VII.1.

Zusätzlich können wir die Riemannsche Zetafunktion als unendliches Produkt darstellen.

Theorem 12.5. (Euler-Identität). Für $\mathrm{Re}(s) > 1$ gilt

$$\zeta(s) = \prod_{\text{p ist Primzahl}} \frac{1}{1 - p^{-s}}. \tag{12.11}$$

Für einen Beweis der Euler-Identität siehe Kapitel VII.1 in *Algebraische Zahlentheorie* [4].

Aus der Produktdarstellung (12.11) folgt, dass die Riemannsche Zetafunktion keine Nullstellen für $\mathrm{Re}(s) > 1$ besitzt. Wir nennen die Nullstellen von der Form $-2n$ für $n \in \mathbb{N}$ die trivialen Nullstellen der Riemannschen Zetafunktion. Da die trivialen Nullstellen negative Realteil haben, folgt, dass die nicht trivialen Nullstellen sich im kritischen Streifen $0 \leqslant \mathrm{Re}(s) \leqslant 1$ befinden. Die **Riemannsche Vermutung** besagt, dass alle nichttrivialen Nullstellen von der Zetafunktion Realteil $\frac{1}{2}$ besitzen. Die Riemannsche Vermutung ist für die Kryptologie von Bedeutung, beispielsweise im

RSA-Verfahren. Die Vermutung wurde bis heute noch nicht bewiesen und ist eines der Millenium-Probleme.

Als nächstes definieren wir die Dedekindsche Zetafunktion, welche eine Verallgemeinerung der Riemannschen Zetafunktion ist, da wir sie auf jedem Zahlkörper K definieren können. Gilt $K = \mathbb{Q}$, so erhalten wir die Riemannsche Zetafunktion.

Sei nun K ein Zahlkörper und s eine komplexe Zahl. Falls $\mathrm{Re}(s) > 1$, so konvergiert die Reihe

$$\zeta_K(s) \;=\; \sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} \tag{12.12}$$

absolut, wobei $\mathfrak{a} \neq 0$ ein ganzes Ideal von $\mathcal{O}_K$ ist. Hier ist $\mathfrak{N}$ die Absolutnorm, welche definiert ist als

$$\mathfrak{N}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] \tag{12.13}$$

für Ideale $\mathfrak{a} \neq 0$. Wir nennen die Abbildung $s \mapsto \zeta_K(s)$ die **Dedekindsche Zetafunktion**, benannt nach dem deutschen Mathematiker RICHARD DEDEKIND. Des Weiteren folgt aus der eindeutigen Zerlegung in Primideale, Satz 13 vom Vortrag über die Geometrie der Zahlen, dass die Dedekindsche Zetafunktion folgende Produktdarstellung besitzt:

$$\zeta_K(s) \;=\; \prod_{\mathfrak{p}\subset\mathcal{O}_K} \frac{1}{1-\mathfrak{N}(\mathfrak{p})^{-s}}, \tag{12.14}$$

wobei das Produkt über alle Primideale $\mathfrak{p}$ von $\mathcal{O}_K$ geht.

Analog zur Riemannsche Zetafunktion können die Dedekindsche Zetafunktion zu einer meromorphen Funktion auf einen grösseren Definitionsbereich ausdehnen.

Theorem 12.6. *Die Dedekindsche Zetafunktion ist eindeutig zu einer holomorphen Funktion auf* $\mathbb{C}\backslash\{1\}$ *fortsetzbar, und sie besitzt einen einfachen Pol bei* $s = 1$.

Für die Dedekindsche Zetafunktion besagt die **verallgemeinerte Riemannsche Vermutung**, dass alle Nullstesllen von $\zeta_K(s)$, die im kritischen Streifen $0 < \mathrm{Re}(s) < 1$ liegen, Realteil $\frac{1}{2}$ haben.

Für ein Beispiel einer Dedekindschen Zetafunktion siehe Beispiel 12.25. Um dieses Beispiel zu verstehen, müssen wir zuerst noch zwei Begriffe einführen: den Dirichlet-Charakter und die Dirichletsche L-Funktion.

12.2. **Dirichlet-Charaktere.** In diesem Unterkapitel führen wir den Dirichlet-Charakter ein. Ferner betrachten wir primitive Charaktere und den Führer eines Dirichlet-Charakters modulo n anhand einiger Beispiele.

Wir beginnen mit einer kurzen Repetition des Begriffes des Gruppenhomomorphismus.

Definition 12.7. *Seien* $(G,\ \circ_G)$*, und* $(H,\ \circ_H)$ *eine Gruppe. Dann nennen wir die Abbildung* $f : G \mapsto H$ *einen* ***Gruppenhomomorphismus****, falls*

$$f(g_1\ \circ_G\ g_2) \;=\; f(g_1)\ \circ_H\ f(g_2),\ \forall g_1, g_2 \in G. \tag{12.15}$$

Wir beginnen mit den notwendigen Definitionen, die wir in den darauffolgenden Kapiteln brauchen werden.

Definition 12.8. *Sei* $n \in \mathbb{N}$*. Ein* ***Dirichlet-Charakter modulo*** **n** *ist ein Gruppenhomomorphismus*

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}. \tag{12.16}$$

Der Dirichlet-Charakter ist benannt nach dem deutschen Mathematiker PETER GUSTAV LEJEUNE DIRICHLET, welcher dem Gebiet der Zahlentheorie und der Analysis sehr viel beigetragen hat, wie zum Beispiel das bekannte Schubfachprinzip.

Wir bezeichnen mit dem trivialen Dirichlet-Charakter χ_0 modulo n, den Charakter, der konstant eins ist. Der triviale Charakter modulo 1 wird auch Hauptcharakter genannt.

Definition 12.9. *Wir sagen, dass ein Dirichlet-Charakter χ modulo n von einem Dirichlet-Charaktern χ' modulo m induziert wird, falls m ein Teiler von n ist und wir χ als Komposition aus χ' wie folgt schreiben können*

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{S}^1. \tag{12.17}$$

*Wir nennen einen Dirichlet-Charakter χ modulo n **primitiv**, falls kein $m \in \mathbb{N}$ echter Teiler von n existiert, sodass χ von einem Dirichlet-Charkater modulo m induziert wird.*

Definition 12.10. *Sei χ ein Dirichlet-Charakter modulo n. Wir nennen den kleinsten Teiler f von n den **Führer** von χ, falls χ von einem Dirichlet-Charakter modulo f induziert wird.*

Wir können also jeden Dirichlet-Charakter χ modulo n durch einen primitiven Charakter χ' modulo f wie folgt induzieren:

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/f\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{S}^1. \tag{12.18}$$

Des weiteren, gilt, falls $f = n$, dann ist χ primitiv.

Als nächstes geben wir einige Beispiele, um diese abstrakte Begriffe fassbarer zu machen und zu festigen.

Beispiel 12.11. *(1) Sei $\chi_3(\bar{1}) = 1$ und $\chi_3(\bar{2}) = -1$. Dann definiert χ ein Dirichlet-Charakter modulo 3. Da 3 keine echte Teiler hat, folgt, dass dieser Dirichlet-Charakter primitv ist, und Führer $f = 3$ besitzt.*

(2) Sei $\chi_4(\bar{1}) = 1$ und $\chi_4(\bar{3}) = -1$. Dann definiert χ_4 ein Dirichlet-Charakter modulo 4. Der Führer von χ_4 ist 4, daher ist χ_4 primitiv. Des Weiteren gilt $\chi_4^2 = \chi_0$.

(3) Sei $\chi_6(\bar{1}) = 1$ und $\chi_6(\bar{5}) = -1$. Dann definiert χ_6 ein Dirichlet-Charakter modulo 6. Der Führer von χ_6 ist 3, daher ist χ nicht primitiv.

(4) Sei p eine ungerade Primzahl. Dann definiert $\chi(\bar{a}) = \left(\frac{\bar{a}}{p}\right)$ ein Dirichlet-Charakter modulo p, wobei

$$\left(\frac{a}{p}\right) \;=\; \begin{cases} 0 & \text{falls } a \equiv 0 \mod p \\ +1 & \text{falls } a \equiv b^2 \mod p, \text{ wobei } b \in \mathbb{Z} \\ -1 & \text{sonst} \end{cases} \tag{12.19}$$

das Legendre-Symbol, welches im zweiten Vortrag definiert wurde. Aus der Definition des Legendre-Symbols folgt, dass χ die Werte 0 und ± 1 annimmt, daher folgt, dass $\chi(\bar{a}) \in \mathbb{S}^1$ für alle $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Aus dem Korollar 2.5 zum Eulerschen Kriterium folgt, dass χ ein Gruppenhomomorphismus ist, da für alle $\bar{a}, \bar{b} \in (\mathbb{Z}/p\mathbb{Z})^\times$

$$\chi(\bar{a} \cdot \bar{b}) \;=\; \left(\frac{\bar{a} \cdot \bar{b}}{p}\right) \;=\; \left(\frac{\bar{a}}{p}\right) \cdot \left(\frac{\bar{b}}{p}\right) \;=\; \chi(\bar{a}) \cdot \chi(\bar{b}). \tag{12.20}$$

Da p eine Primzahl, gilt $f = p$ und der Dirichlet-Charakter ist daher primitiv.

(5) Es gilt: Ein Dirichlet-Charakter besitzt Führer 1 genau dann wenn es der triviale Charakter ist.

Wir definieren die Multiplikation

$$\chi\psi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{S}^1, \; (\chi\psi)(\bar{m}) = \chi(\bar{m})\psi(\bar{m}) \tag{12.21}$$

auf der Menge der Dirichlet-Charakter modulo n. Mit dieser Multiplikation und dem trivialen Charakter χ_0 als neutrales Element bildet die Menge der Dirichlet-Charaktere modulo n eine abelsche Gruppe.

Wir können eine Dirichlet-Charakter χ modulo n zu einer Funktion auf ganz $\mathbb{Z}$ ausweiten. Wir definieren $\chi : \mathbb{Z} \to \mathbb{C}$ durch

$$\chi(m) = \begin{cases} \chi(m \mod n) & \text{ggT}(n,\ m) = 1 \\ 0 & \text{ggT}(n,\ m) \neq 1. \end{cases} \tag{12.22}$$

Eine weitere Variante wäre χ zunächst als Funktion auf $(\mathbb{Z}/f\mathbb{Z})^\times$ aufzufassen und $\chi(m) = 0$ zu setzen für jedes $m \in \mathbb{Z}$ für das gilt $\mathrm{ggT}(m,\ f) \neq 1$.

Den Dirichlet-Charakter, den wir in Beispiel 12.11 *(4)* gesehen haben, werden wir nun wie oben beschrieben auf ganz $\mathbb{Z}$ ausweiten.

Beispiel 12.12. *Sei p eine ungerade Primzahl. Dann definiert $\chi(\bar{a}) = \left(\frac{\bar{a}}{p}\right)$ ein Dirichlet-Charakter modulo p. Diesen können wir wie oben beschrieben zu $\chi : \mathbb{Z} \to \mathbb{C}$ erweitern*

$$\chi(a) = \begin{cases} \chi(a \mod p) & \mathrm{ggT}(p,\ a) = 1 \\ 0 & \mathrm{ggT}(p,\ a) \neq 1 \end{cases} = \left(\frac{a}{p}\right) \tag{12.23}$$

Das Legendre-Symbol definiert also einen Dirichlet-Charakter auf ganz $\mathbb{Z}$.

Wir können das Legendre-Symbol mittels Dirichlet-Charakter modulo n für $n \in \mathbb{N}$ ungerade zum Jacobi-Symbol wie folgt verallgemeinern:

$$\left(\frac{a}{n}\right) = \begin{cases} \chi(a \mod n) & \mathrm{ggT}(n,\ a) = 1 \\ 0 & \mathrm{ggT}(n,\ a) \neq 1. \end{cases} \tag{12.24}$$

Dies können wir noch weiter für $n \in \mathbb{Z}$ gerade verallgemeinern, indem wir

$$\left(\frac{a}{2}\right) = \begin{cases} -1 & \text{falls } a \equiv 3, 5 \bmod 8 \\ 0 & \text{falls } a \equiv 1, 7 \bmod 8 \\ 1 & \text{falls } a \equiv 0 \bmod 2, \end{cases} \tag{12.25}$$

$$\left(\frac{a}{-1}\right) = \begin{cases} -1 & \text{falls } a < 0 \\ 1 & \text{falls } a \geqslant 0 \end{cases} \tag{12.26}$$

und

$$\left(\frac{a}{0}\right) = \begin{cases} 1 & \text{falls } a = \pm 1 \\ 0 & \textit{sonst} \end{cases} \tag{12.27}$$

setzen. Alle anderen Werte ergeben sich durch folgende Rechenregel:

$$\left(\frac{a \cdot b}{c \cdot d}\right) = \left(\frac{a}{c}\right) \cdot \left(\frac{b}{c}\right) \cdot \left(\frac{a}{d}\right) \cdot \left(\frac{b}{d}\right). \tag{12.28}$$

Wir nennen dies das Kronecker-Symbol.

Sei a eine quadratfreie Zahl in $\mathbb{Z}\backslash\{0, 1\}$. Quadratfrei bedeutet, dass in der Primfaktorzerlegung von a jede Primzahl höchstens einmal auftritt. Für einen quadratischen Zahlkörper $\mathbb{Q}(\sqrt{a})$ ist der Dirichlet-Charakter von der Form $\left(\frac{d}{\cdot}\right)$, wobei d die Diskriminante ist. Die Diskriminante ist gegeben durch

$$d = \begin{cases} a & \text{falls } a \equiv 1 \bmod 4 \\ 4a & \text{falls } a \equiv 2 \text{ oder } 3 \bmod 4. \end{cases} \tag{12.29}$$

Beispiel 12.13. *Sei $a = -1$ und $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(i)$ ein quadratischer Zahlkörper. Da $a \equiv 3 \bmod 4$ ist die Diskriminante $d = 4a = -4$. Es gilt: $\chi_4(n) = \left(\frac{-4}{n}\right)$.*

12.3. **Dirichlet L-Funktionen.** In diesem Unterkapitel wird die Dirichletsche L-Reihe und die Dirichletsche L-Funktion eingeführt. Die Begriffe werden mittels einiger Beispiele erläutert. Des Weiteren finden wir die Darstellung der Dedekindschen Zetafunktion für den Körper $K = \mathbb{Q}(\xi_n)$, wobei ξ_n die n-te Einheitzwurzel ist, in Abhängigkeit der L-Funktionen. Zudem wird in diesem Abschnitt eine Darstellung der Dedekindschen Zetafunktion eines quadratischen Zahlkörpers in Abhängigkeit der Dirichletschen L-Funktion präsentiert. Wir werden die Korrektheit dieser Darstellung anhand des Beispiels $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{-3})$ zeigen. Anschliessend überprüfen wir die Dirichletschte Klassenzahlformel für $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{-3})$.

Wir können für einen Dirichlet-Charakter auf den ganzen Zahlen folgende Reihe bilden.

Definition 12.14. *Die* ***Dirichletsche L-Reihe*** *ist definiert durch*

$$L(s,\ \chi) \ = \ \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \tag{12.30}$$

wobei $\chi : \mathbb{Z} \to \mathbb{C}$ *ein Dirichlet-Charakter. Falls* $\mathrm{Re}(s) > 1$ *konvergiert die Dirichletsche L-Reihe absolut, da* $|\chi(n)| \leqslant 1$*. Wir nennen diese holomorphe Funktion die* ***Dirichletsche L-Funktion*** *zu* χ*.*

Bemerkung 12.15. Für den Hauptcharakter gilt

$$L(s,\ \epsilon) = \sum_{n=1}^{\infty} \frac{\epsilon(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s), \tag{12.31}$$

wobei ζ die Riemannsche Zetafunktion.

Wie die Zetafunktion können wir die Dirichletsche L-Reihe als unendliches Produkt darstellen.

Theorem 12.16. (Euler-Identität) Sei $\chi : \mathbb{Z} \to \mathbb{C}$ ein Dirichlet-Charakter. Sei $s \in \mathbb{C}$ und $\delta > 0$. Falls $\mathrm{Re}(s) \geqslant 1+\delta$, so konvergiert die Reihe $L(s,\ \chi)$ absolut und gleichmässig. Des Weiteren ist die Abbildung $s \mapsto L(s,\ \chi)$ auf $\left\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\right\}$ holomorph. Es gilt folgende Produktdarstellung:

$$L(s,\ \chi) = \prod_{\text{p ist Primzahl}} \frac{1}{1-\chi(p)p^{-s}}. \tag{12.32}$$

Bemerkung 12.17. Für den Hauptcharakter erhalten wir diesselbe Produktdarstellung wie für die Riemannsche Zetafunktion in Theorem 12.5:

$$L(s,\ \epsilon) = \prod_{\text{p ist Primzahl}} \frac{1}{1-\epsilon(p)p^{-s}} = \prod_{\text{p ist Primzahl}} \frac{1}{1-1\cdot p^{-s}} = \prod_{\text{p ist Primzahl}} \frac{1}{1-p^{-s}} = \zeta(s). \tag{12.33}$$

Als nächstes betrachten wir drei Beispiele von Dirichlet L-Reihen.

Beispiel 12.18. *(1) Für den trivialen Charakter* χ_0 *modulo* n *gilt*

$$\begin{aligned} L(s,\ \chi_0) &= \prod_{p\ ist\ Primzahl} \frac{1}{1-\chi_0(p)p^{-s}} = \prod_{\substack{\mathrm{ggT}(p,n)=1 \\ p\ ist\ Primzahl}} \frac{1}{1-p^{-s}} \\ &= \prod_{\substack{p|n \\ p\ ist\ Primzahl}} (1-p^{-s}) \cdot \prod_{p\ ist\ Primzahl} \frac{1}{1-p^{-s}} \\ &= \prod_{\substack{p|n \\ p\ ist\ Primzahl}} (1-p^{-s})\ \zeta(s). \end{aligned} \tag{12.34}$$

(2) Wähle $s = 1$*. Der einzige nichttriviale Charakter modulo* 4 *ist der Charakter* $\chi_4 = \left(\frac{-4}{n}\right)$*. Wir erhalten folgende Dirichletsche L-Reihe*

$$L(1,\ \chi_4) = \sum_{n=1}^{\infty} \frac{\chi_4(n)}{n^1} = \sum_{n=1}^{\infty} \frac{\left(\frac{-4}{n}\right)}{n} = \sum_{n\equiv 1 \bmod 2} \frac{(-1)^{\frac{n-1}{2}}}{n} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \dots\ . \tag{12.35}$$

Der Arkustangens hat folgende Reihendarstellung für ein x *mit* $|x| \leqslant 1$ *und* $x \neq \pm i$*:*

$$\arctan(x) = \sum_{k=1}^{\infty} (-1)^k \frac{x^{2k+1}}{2k+1} = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} \pm \dots\ . \tag{12.36}$$

Setze $x = 1$*, dann gilt*

$$L(1,\ \chi_4) = \arctan(1) = \frac{\pi}{4}. \tag{12.37}$$

(3) Wähle $s = 1$*. Der einzige nichttriviale Charakter modulo* 6 *ist der Charakter* χ_6 *aus Beispiel 12.11. Wir erhalten folgende Dirichletsche L-Reihe*

$$L(1,\ \chi_6) = \sum_{n=1}^{\infty} \frac{\chi_6(n)}{n^1} = 1 + \sum_{n=1}^{\infty} \left(\frac{-1}{6n-1} + \frac{1}{6n+1}\right) = 1 + \frac{1}{6}\sum_{n=1}^{\infty} \left(\frac{1}{\frac{1}{6}-n} + \frac{1}{\frac{1}{6}+n}\right). \tag{12.38}$$

Der Kotangens hat folgende Partialbruchzerlegung für ein $x \in \mathbb{C}\backslash\mathbb{Z}$:

$$\pi \cot(\pi x) = \frac{1}{x} + \sum_{k=1}^{\infty} \left(\frac{1}{x+k} + \frac{1}{x-k} \right) \tag{12.39}$$

Setze $x = \frac{1}{6}$, dann gilt

$$L(1,\ \chi_6) = 1 + \frac{1}{6} \left(\pi \cot\left(\frac{\pi}{6}\right) - 6 \right) = \frac{\pi\sqrt{3}}{6}, \tag{12.40}$$

wobei wir ausgenutzt haben, dass $\cot\left(\frac{\pi}{6}\right) = \sqrt{3}$.

Das nächste Theorem besagt, wie wir die Dedekindsche Zetafunktion des Körpers $K = \mathbb{Q}(\xi_n)$, wobei ξ_n eine n-te Einheitswurzel ist, faktorisieren können.

Theorem 12.19. *Sei ξ_n eine n-te Einheitswurzel. Sei $K = \mathbb{Q}(\xi_n)$, dann gilt für $s \in \mathbb{C}$*

$$\zeta_K(s) = G(s) \prod_{\chi} L(s,\ \chi), \tag{12.41}$$

wobei das Produkt über alle Dirichlet-Charaktere χ modulo n geht und $G(s)$ gegeben ist durch

$$G(s) = \prod_{\substack{p|n \\ p \text{ ist Primzahl}}} \frac{1}{1 - \mathfrak{N}(p)^{-s}}. \tag{12.42}$$

Für einen Beweis von Theorem 12.19 siehe Kapitel VII.5 in *Algebraische Zahlentheorie* [4].

Bemerkung 12.20. Für den trivialen Charakter χ_0 modulo n gilt wegen dem Beispiel 12.18 *(1)*, dass $L(s,\ \chi_0) = \prod_{\substack{p|n \\ \text{p ist Primzahl}}} (1 - p^{-s})\ \zeta(s)$. Mittels obigem Satz folgt, dass

$$\begin{aligned} \zeta_K(s) &= G(s) \prod_{\chi} L(s,\ \chi) = G(s)\ L(s,\ \chi_0) \prod_{\chi \neq \chi_0} L(s,\ \chi) \\ &= G(s) \prod_{\substack{p|n \\ \text{p ist Primzahl}}} (1 - p^{-s})\ \zeta(s) \prod_{\chi \neq \chi_0} L(s,\ \chi), \end{aligned} \tag{12.43}$$

wobei das Produkt über alle Dirichlet-Charaktere χ modulo n geht, welche nicht der triviale Charakter sind.

Auch für einen quadratischen Zahlkörper können wir die Dedekindsche Zetafunktion wie im folgenden Theorem in Abhängigkeit der Dirichletschen L-Funktionen faktorisieren.

Theorem 12.21. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper, dann ist die Dedekindsche Zetafunktion von der Form*

$$\zeta_K(s) = \zeta(s) L(s, \chi), \tag{12.44}$$

wobei der Dirichlet-Character χ von der Form $\chi(n) = \left(\frac{d}{n}\right)$ ist.

Als nächstes präsentieren wir die Klassenzahlformel, welche, wie der Name bereits sagt, benutzt werden kann, um die Klassenzahl eines Zahlkörpers K zu berechnen. Die Formel verwendet die Tatsache, dass die Dedekindsche Zetafunktion einen einfachen Pol bei Eins hat und wir somit an dieser Stelle das Residuum berechnen können.

Theorem 12.22. (Klassenzahlformel) Die Dedekindsche Zetafunktion hat einen einfachen Pol bei $s = 1$ mit Residuum

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^r (2\pi)^s}{w\sqrt{|d|}} hR, \tag{12.45}$$

wobei h die Klassenzahl, d die Diskriminante, w die Anzahl Einheitswurzeln, R der Dirichletsche Regulator, r und $2s$ die Anzahl der reellen und komplexen Einbettungen des Zahlkörpers K.

Das nächste Theorem ist ein Spezialfall der Klassenzahlformel für quadratische Körper.

Theorem 12.23. (Dirichletsche Klassenzahlformel) Sei $K = \mathbb{Q}(\sqrt{d})$ eine quadratische Zahlkörper, dann gilt

$$h = \begin{cases} \frac{w\sqrt{|d|}}{2\pi} L(1,\ \chi) & \text{falls } d < 0 \\ \frac{\sqrt{d}}{\ln \epsilon} L(1,\ \chi) & \text{falls } d > 0, \end{cases} \tag{12.46}$$

wobei h die Klasenzahl, w die Anzahl Einheitswurzeln und ϵ gegeben ist durch

$$\epsilon = \frac{1}{2}(t + u\sqrt{d}). \tag{12.47}$$

Hier sind t, u die Fundamentaleinheit der Pell Gleichung.

Bemerkung 12.24. Der Körper K hat Klassenzahl $h = 1$ genau dann, wenn $\mathcal{O}_K$ ein Haupitdeal ist. Des Weiteren existieren nur neun imaginär-quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ die Klassenzahl $h = 1$ besitzen. Diese neun Werte sind:

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163. \tag{12.48}$$

Es wird vermutet, dass unendlich viele reell-quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ die Klassenzahl $h = 1$ besitzen.

Wir betrachten nun zwei Beispiele einer Dedekindschen Zetafunktion und überprüfen damit die Korrektheit der Dirichletschen Klassenzahlformel.

Beispiel 12.25. *(1) Sei $K = \mathbb{Q}(i)$. Dann gilt, $\mathcal{O}_K = \mathbb{Z}[i]$ und die Dedekindsche Zetafunktion sieht folgendermassen aus:*

$$\zeta_{\mathbb{Q}(i)}(s) \ = \ \sum_{\mathfrak{a} \subset \mathbb{Z}[i]} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} \ = \ \prod_{\mathfrak{p} \subset \mathbb{Z}[i]} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}}. \tag{12.49}$$

Vom Theorem 1.32 *aus dem ersten Vortrag wissen wir, dass wir bis auf Assoziiertheit folgende Primideale in $\mathbb{Z}[i]$ haben:*

- *$1 + i$, wobei $\mathfrak{N}(1 + i) = 1^2 + 1^2 = 2$.*
- *$a + ib$, wobei $a > |b| > 0$, $a^2 + b^2 = p \in \mathbb{Z}$ eine Primzahl mit $p \equiv 1 \bmod 4$, und $\mathfrak{N}(a + ib) = a^2 + b^2 = p$.*
- *p, wobei $p \in \mathbb{Z}$ Primzahl mit $p \equiv 3 \bmod 4$ und $\mathfrak{N}(p) = p^2$.*

Somit gilt

$$\begin{aligned} \zeta_{\mathbb{Q}(i)}(s) \ &= \ \left(1 - 2^{-s}\right)^{-1} \cdot \prod_{\substack{p \in \mathbb{Z}\ Primzahl \\ p \equiv 3 \bmod 4}} \left(1 - (p^2)^{-s}\right)^{-1} \cdot \prod_{\substack{p \in \mathbb{Z}\ Primzahl \\ p \equiv 1 \bmod 4}} \left(1 - p^{-s}\right)^{-2} \\ &= \ \left(1 - 2^{-s}\right)^{-1} \cdot \prod_{\substack{p \in \mathbb{Z}\ Primzahl \\ p \equiv 3 \bmod 4}} \left(1 - p^{-s}\right)^{-1} \cdot \prod_{\substack{p \in \mathbb{Z}\ Primzahl \\ p \equiv 1 \bmod 4}} \left(1 - p^{-s}\right)^{-1} \\ &\quad \cdot \prod_{\substack{p \in \mathbb{Z}\ Primzahl \\ p \equiv 3 \bmod 4}} \left(1 + p^{-s}\right)^{-1} \cdot \prod_{\substack{p \in \mathbb{Z}\ Primzahl \\ p \equiv 1 \bmod 4}} \left(1 - p^{-s}\right)^{-1} \\ &= \zeta(s) \cdot \prod_{p\ ist\ Primzahl} \left(1 - \chi_4(p) p^{-s}\right)^{-1} \\ &= \zeta(s) \cdot L(s,\ \chi_4), \end{aligned} \tag{12.50}$$

wobei wir im vorletzten Schritt die Definition der Riemannschen Zetafunktion und im letzten Schritt die Produktdarstellung 12.16 der L-Funktion benutzen. Wir haben somit Theorem 12.21 überprüft.

Als nächstes wollen wir die Dirichletsche Klassenzahlformel überprüfen. Aufgrund der Bemerkung 12.24 und da $\mathbb{Z}[i]$ ein Hauptidealring ist, folgt, dass $\mathbb{Q}(i)$ Klassenzahl 1 hat.

Für $\mathbb{Q}(i)$ ist die Diskriminante $d = -4$, die Anzahl Einheiten $w = 4$ und aus Beispiel 12.18 (2) wissen wir, dass $L(1,\ \chi_4) = \frac{\pi}{4}$. Es gilt, da $d < 0$, dass

$$h = \frac{w\sqrt{|d|}}{2\pi} L(1,\ \chi_4) = \frac{4\sqrt{|-4|}}{2\pi}\frac{\pi}{4} = 1. \tag{12.51}$$

(2) Sei $K = \mathbb{Q}(\sqrt{-3})$. Dann erhält man analog zu (1)

$$\zeta_{\mathbb{Q}(\sqrt{-3})}(s) \ = \ \zeta(s) \cdot L(s,\ \chi_3). \tag{12.52}$$

Da der Führer von χ_6 3 ist, können wir χ_6 schreiben als $\chi_6 = \chi_3 \circ \psi$, wobei

$$\begin{aligned} (\mathbb{Z}/6\mathbb{Z})^\times &\to (\mathbb{Z}/3\mathbb{Z})^\times \\ \bar{1} &\mapsto \bar{1}, \\ \bar{5} &\mapsto \bar{2}. \end{aligned} \tag{12.53}$$

Daher gilt,

$$L(s,\ \chi_3) = \left(1 + \frac{1}{2^s}\right)^{-1} L(s, \chi_6). \tag{12.54}$$

Wegen (12.40) gilt, dass

$$L(1,\ \chi_3) = \left(1 + \frac{1}{2}\right)^{-1} L(1, \chi_6) = \frac{2}{3}\frac{\pi\sqrt{3}}{6} = \frac{\pi\sqrt{3}}{9}. \tag{12.55}$$

Wir können nun wieder den Dirichletschen Primzahlsatz überprüfen. Da $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ ein Hauptideal ist, gilt wieder aufgrund der Bemerkung 12.24, dass $\mathbb{Q}(\sqrt{-3})$ Klassenzahl 1 besitzt.

Für $\mathbb{Q}(\sqrt{-3})$ ist die Diskriminante $d = -12$ und die Anzahl Einheiten $w = 3$. Es gilt, da $d < 0$, dass

$$h = \frac{w\sqrt{|d|}}{2\pi} L(1,\ \chi_6) = \frac{3\sqrt{|-12|}}{2\pi}\frac{\pi\sqrt{3}}{9} = 1. \tag{12.56}$$

12.4. **Dichtigkeitssätze.** Zunächst führen wir zwei Definitionen ein, die die Dichte einer Menge beschreiben. Diese benötigen wir dann um zwei wichtige Dichtigkeitssätze zu erklären.

Definition 12.26. *Sei K ein Zahlkörper und M eine Menge von Primidealen von K. Dann heisst*

$$d(M) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in M} \mathfrak{N}(p)^{-s}}{\sum_{\mathfrak{p}} \mathfrak{N}(p)^{-s}} \tag{12.57}$$

*die **Dirichlet-Dichtigkeit** von M, falls der Limes existiert.*

Bemerkung 12.27. Die Dirichlet-Dichtigkeit nimmt einen Wert zwischen Null und Eins an, somit $0 \leqslant d(M) \leqslant 1$. Ausserdem beträgt die Dirichlet-Dichtigkeit von der Menge aller Primzahlen Eins. Jedoch ist diese nicht für jede Teilmenge der Primzahlen definiert. Eine endliche Menge an Primzahlen hat Dirichlet-Dichtigkeit Null. Falls sich zwei Mengen von Primzahlen nur um endlich viele Zahlen unterscheiden, so besitzen sie diesselbe Dirichlet-Dichtigkeit.

Wir können die Dichtigkeit einer Menge aber auch anders beschreiben.

Definition 12.28. *Sei K ein Zahlkörper und M eine Menge von Primidealen von K. Dann heisst*

$$\delta(M) = \lim_{x \to \infty} \frac{\left|\{\mathfrak{p} \in M \mid \mathfrak{N}(\mathfrak{p}) \leqslant x\}\right|}{\left|\{\mathfrak{p} \mid \mathfrak{N}(\mathfrak{p}) \leqslant x\}\right|} \tag{12.58}$$

*die **natürliche Dichtigkeit** von M, falls der Limes existiert.*

Bemerkung 12.29. Der Begriff *natürliche Dichtigkeit* kommt daher, dass die Dichte natürlich", beziehungsweise intuitiv definiert ist. Zum Beispiel ist die natürliche Dichtigkeit der geraden Zahlen $\frac{1}{2}$.

Falls $\delta(M)$ exisitiert, so existiert auch $d(M)$ und es gilt, dass $\delta(M) = d(M)$. Dahingegen impliziert die Existenz von $d(M)$ nicht die Existenz von $\delta(M)$.

Wir benutzen die Dirichletsche L-Reihe und die oben definierten Dichtigkeiten für zwei wichtige Dichtigkeitssätze. Der erste Satz, den wir erläutern werden, ist Chebotarev's Dichtigkeitssatz, benannt nach dem sowjetischen Mathematiker NIKOLAI GRIGORIEVICH CHEBOTAREV. Der Satz ist von Bedeutung, da er besagt, dass die Dichte der Menge aller unverzweigten Primideale endlich ist und existiert, und da aus ihm folgt, dass eine galloissche Erweiterung durch die Menge aller unverzweigten Primideale endeutig bestimmt ist.

Theorem 12.30. (Chebotarev's Dichtigkeitssatz). Sei L eine endliche galoissche Erweiterung über dem Körper K mit der Gruppe G. Sei $\mathfrak{p}$ ein unverzwigtes Primideal von L. Sei $C \subset G$ Konjugationsinvariant. Des Weiteren sei die Menge aller unverzweigten Primideale von K gegeben durch

$$A_C = \left\{\mathfrak{p} \subset \mathcal{O}_K \;\middle|\; \mathfrak{p} \text{ unverzweigt in } L \text{ und } \left(\frac{L/K}{\mathfrak{P}}\right) \in C \text{ für ein Primideal über } \mathfrak{p}\right\}, \tag{12.59}$$

wobei $\left(\frac{L/K}{\mathfrak{P}}\right)$ der Frobeniusautomotphismus von $\mathfrak{P}$ über K. Dann hat die Menge A_C die natürliche Dichtigkeit

$$\delta(A_C) = \lim_{x\to\infty} \frac{\left|\left\{\mathfrak{p} \in A_C \mid \mathfrak{N}(\mathfrak{p}) \leqslant x\right\}\right|}{\left|\left\{\mathfrak{p} \subset \mathcal{O}_K \mid \mathfrak{N}(\mathfrak{p}) \leqslant x\right\}\right|} = \frac{|C|}{|G|}. \tag{12.60}$$

Für den Beweis von Theorem 12.30 siehe Kapitel VII.13 in *Algebraische Zahlentheorie* [4].

Als nächstes formulieren wir den Chebotarev's Dichtigkeitssatz für eine Körpererweiterung über $\mathbb{Q}$. Sei also L eine endliche Galoissche Erweiterung über dem Körper $K = \mathbb{Q}$. Sei $G = L/\mathbb{Q}$ die dazugehörende Galoisgruppe. Sei $C \subset G$ Konjugationsinvariant. Des Weiteren sei die Menge aller unverzweigten Primideale von $\mathbb{Q}$ gegeben durch

$$A_C = \left\{(p) \subset \mathbb{Z} \;\middle|\; (p) \text{ unverzweigt in } L \text{ und } \left(\frac{L/\mathbb{Q}}{\mathfrak{P}}\right) \in C \text{ für ein Primideal über } (p)\right\}, \tag{12.61}$$

wobei $\left(\frac{L/\mathbb{Q}}{\mathfrak{P}}\right)$ der Frobeniusautomotphismus von $\mathfrak{P}$ über $\mathbb{Q}$. Dann hat die Menge A_C die natürliche Dichtigkeit

$$\delta(A_C) = \lim_{x\to\infty} \frac{\left|\left\{(p) \in A_C \mid \mathfrak{N}(p) \leqslant x\right\}\right|}{\left|\left\{(p) \subset \mathbb{Z} \mid \mathfrak{N}(p) \leqslant x\right\}\right|} = \frac{|C|}{|G|}. \tag{12.62}$$

Der zweite Dichtigkeitssatz ist der Dirichletsche Primzahlsatz. Dieser besagt, dass eine arithmetische Folge

$$a, a+n, a+2n, a+3n, ... \tag{12.63}$$

immer unendlich viele Primzahlen enthält, das heisst, dass unendlich viele Primzahlen kongruent zu a modulo n existieren.

Theorem 12.31. (Dirichletscher Primzahlsatz). Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ teilerfremd. Dann existieren unendlich viele Primzahlen die kongurent zu a modulo n sind. Die Menge der Primzahlen, die kongurent zu a modulo n sind, besitzen die natürliche Dichte $\delta(\{p \text{ ist Primzahl} \mid p \equiv a \bmod n\}) = \frac{1}{\varphi(n)}$, wobei $\varphi(n) = |\{b \in \mathbb{N} \mid 1 \leqslant b \leqslant n \text{ und } \mathrm{ggT}(b,n) = 1\}|$ die Eulersche Phi-Funktion ist.

Da Chebotarev's Dichtigkeitssatz eine Verallgemeinerung des Dirichletschen Primzahlsatzes ist, werden wir ihn verwenden, um den Primzahlsatz zu beweisen.

Beweis. Sei $n \in \mathbb{N}$ und $L = \mathbb{Q}(\xi_n)$ eine endliche galoissche Erweiterung über dem Körper $K = \mathbb{Q}$, wobei ξ_n eine primitive n-te Einheitswurzel ist. Die Galoisgruppe $G = L/K$ ist isomorph zu den invertierbaren Elementen von $\mathbb{Z}/n\mathbb{Z}$, da

$$\begin{aligned} G &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ (\xi_n \mapsto \xi_n^a) &\mapsto (a \bmod n). \end{aligned} \tag{12.64}$$

Da die Menge der verzweigten Primideale endlich ist und diese somit nicht zu der Dichte beitragen, betrachten wir nur unverzweigte Primideale.

Sei also $\mathfrak{P}$ ein unverzweigtes Primideal über einem Primideal (p), wobei $p \nmid n$. Aus der Vorlesung über den lokalen Frobenius, wissen wir, dass dieser gegeben ist durch

$$\left(\frac{L/\mathbb{Q}}{\mathfrak{P}}\right)\xi_n \;=\; \xi_n^p. \tag{12.65}$$

Wegen dem Isomorphismus (12.64) folgt, dass

$$\left(\frac{L/\mathbb{Q}}{\mathfrak{P}}\right) \;\equiv\; p \bmod n. \tag{12.66}$$

Da G abelsch ist, hat jede Konjugationsklasse genau ein Element. Sei also $C = \{a\}$ die Konjugationsklasse von a, dann gilt $|C| = 1$. Sei die Menge aller unverzweigten Primideale von $\mathbb{Q}$ gegeben durch

$$\begin{aligned} A_C \;&= \left\{(p) \subset \mathbb{Z} \;\middle|\; (p) \text{ unverzweigt in } L \text{ und } \left(\frac{L/\mathbb{Q}}{\mathfrak{P}}\right) \in C \text{ für ein Primideal über } (p)\right\} \\ &= \{p \equiv a \bmod n\}, \end{aligned} \tag{12.67}$$

wobei die letzte Äquivalenz aus (12.66) folgt.

Wir wenden nun den Chebotarev's Dichtigkeitssatz in der Form (12.62) an.

$$\lim_{x\to\infty} \frac{|\{p \equiv a \bmod n \mid p \leqslant x\}|}{|\{p \leqslant x\}|} \;=\; \lim_{x\to\infty} \frac{\left|\left\{(p) \in A_C \mid \mathfrak{N}(p) \leqslant x\right\}\right|}{\left|\left\{(p) \subset \mathbb{Z} \mid \mathfrak{N}(p) \leqslant x\right\}\right|} = \frac{|C|}{|G|} \;=\; \frac{1}{|(\mathbb{Z}/n\mathbb{Z})^\times|} = \frac{1}{\varphi(n)} \tag{12.68}$$

Im vorletzten Schritt haben wir ausgenutzt, dass es in jeder Konjugationsklasse genau ein Element hat und, dass G isomorph zu $(\mathbb{Z}/n\mathbb{Z})^\times$ ist.

Definiere nun folgende Äquivalenzrelation:

$$f(x) \sim g(x) \iff \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1. \tag{12.69}$$

Aus (12.68) folgt nun, dass

$$\lim_{x\to\infty} \frac{|\{p \equiv a \bmod n \mid p \leqslant x\}|}{|\{p \leqslant x\}| \cdot \frac{1}{\varphi(n)}} \;=\; 1. \tag{12.70}$$

Folglich gilt, dass $|\{p \equiv a \bmod n \mid p \leqslant x\}| \sim |\{p \leqslant x\}| \cdot \frac{1}{\varphi(n)}$. Da unendlich viele Primzahlen existieren, konvergiert die rechte Seite gegen unendlich, somit auch die Linke. Wir erhalten also, dass unendlich viele Primzahlen existieren, welche kongurent zu $a \bmod n$ sind. □

Für einen alternativen Beweis siehe Kapitel 8.6 in *Einführung in die algebraische Zahlentheorie* [5]. Der Beweis verwendet die Tatsache, dass der Wert der Dirichletsche L-Funktion eines Dirichlet-Charakters modulo n an der Stelle $s = 1$ nicht Null ist.

Literatur

[1] M. F. Atiyah und I. G. Macdonald, Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 196
[2] Gouvêa F.Q. p-adic Numbers. Universitext. Springer, Cham, 2020
[3] S. Müller–Stach und J. Piontkowski, *Elementare und algebraische Zahlentheorie*. Second edition. Vieweg + Teubner, Wiesbaden, 2011
[4] J. Neukirch, *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992
[5] A. Schmidt, *Einführung in die algebraische Zahlentheorie*. Springer, Berlin, 2007
[6] U. Zannier, *Lecture notes on Diophantine analysis*. Edizioni della Normale, Pisa, 2009