Dr. Fritz Hörmann

Vorlesungsskript:
Algebraische Zahlentheorie

Universität Freiburg — SS 2018

---

1 Motivation

1.1 Literatur

[N] Neukirch, Jürgen. *Algebraische Zahlentheorie.* Springer-Verlag, Berlin, 1992.

[M] Milne, James. *Algebraic Number Theory.* `http://www.jmilne.org/math/CourseNotes/ANT.pdf`

[L] Lang, Serge. *Algebraic number theory.* Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[Lo] Lorenz, Falko. *Algebraische Zahlentheorie.* Bibliographisches Institut, Mannheim, 1993.

[HK] Huber-Klawitter, Annette. *Algebraische Zahlentheorie.* Vorlesungsskript 2014, Universität Freiburg. `https://home.mathematik.uni-freiburg.de/arithgeom/lehre/ss14/algzt/azt.pdf`

Für das letzte Kapitel:

[KKS2] Kato, Kazuya; Kurokawa, Nobushige; Saito, Takeshi. *Number theory. 2. Introduction to class field theory.* American Mathematical Society 2011.

Bitte schreiben Sie mir eventuelle Fehler und Kommentare per eMail: `fritz.hoermann@math.uni-freiburg.de`.

1.2 Einführung

Sie haben alle irgendwann einmal gelernt, dass sich jede ganze Zahl $x \in \mathbb{Z}$ schreiben lässt als

$$x = \pm p_1 \cdots p_n$$

wobei die p_i Primzahlen sind und dass diese Zerlegung (bis auf Vertauschung der Reihenfolge) eindeutig ist. Wir sagen, dass in $\mathbb{Z}$ **eindeutige Primfaktorzerlegung** gilt. Der Hauptgegenstand der Vorlesung ist motiviert durch die Frage, ob eine solche Zerlegung auch für algebraische Zahlen, also Elemente einer endlichen Körpererweiterung über $\mathbb{Q}$ gilt. Dazu ist es erst einmal nötig zu definieren und zu verstehen, was eine **ganze** algebraische Zahl überhaupt ist. Wir werden in jeder endlichen Körpererweiterung K über $\mathbb{Q}$

— im folgenden auch einfach **Zahlkörper** genannt — einen Unterring $\mathcal{O}_K$ der ganzen Zahlen in K definieren. Dieser Ring[1] spielt dieselbe Rolle wie $\mathbb{Z}$ für $\mathbb{Q}$:

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \cup & & \cup \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

In diesen Ringen kann die eindeutige Primfaktorzerlegung gelten, muss aber nicht; dies geschieht genau dann, wenn $\mathcal{O}_K$ ein Hauptidealring ist. Ansonsten werden wir die sogenannte **Klassengruppe** Cl_K definieren, die die Abweichung von der eindeutigen Zerlegung misst. Es gilt dann

$$\mathrm{Cl}_K = \{1\} \quad \Leftrightarrow \quad \text{eindeutige Primfaktorzerlegung gilt in } \mathcal{O}_K.$$

Eines der fundamentalen Resultate, das wir beweisen werden, besagt, dass die **Klassengruppe endlich** ist. Die Abweichung von der eindeutigen Primfaktorzerlegung kann also nicht zu extrem ausfallen.
Primfaktorzerlegung kann höchstens bis auf Einheiten eindeutig sein. Um die Struktur der multiplikativen Gruppe K^* des Zahlkörpers vollständig zu verstehen, müssen wir also zusätzlich die Gruppe $\mathcal{O}_K^*$ der Einheiten untersuchen. Wir werden hierzu den **Dirichletschen Einheitensatz** kennenlernen, der besagt, dass

$$\mathcal{O}_K^* \cong \mu_k \times \mathbb{Z}^r$$

ist, wobei μ_k die (endlich zyklische) Gruppe der Einheitswurzeln in K ist. Auch der Rang r lässt sich einfach bestimmen.

Warum ist dies alles interessant?

Eine der klassischen Fragestellungen der Zahlentheorie ist die Lösbarkeit von algebraischen Gleichungen durch ganze Zahlen (**diophantische Gleichungen**).

Beispiel 1.2.1 (Gauss)**.** *Sei p eine Primzahl. Gibt es ganze Zahlen a, b so dass*

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

Hier hilft der Übergang zu den algebraischen Zahlen, denn wir können die Gleichung umformen (mit $i = \sqrt{-1}$):

$$(a + ib)(a - ib) = p$$

[1] in dieser Vorlesung sind Ringe immer kommutativ mit 1

und die Frage wird: Bleibt p eine Primzahl im Ring $\mathbb{Z}[i]$ oder nicht? *Dadurch dass in* $\mathbb{Z}[i]$ *eindeutige Primfaktorzerlegung gilt, können wir die folgende überraschende Antwort geben:*

$$a^2 + b^2 = p \quad \textit{lösbar} \quad \Leftrightarrow \quad p = 2 \textit{ oder } p \equiv 1 \ (4).$$

(diese Folgerung aus der eindeutigen Primfaktorzerlegung ist nicht ganz offensichtlich und wird im nächsten Abschnitt erklärt.)

Beispiel 1.2.2 (Pellsche Gleichung)**.** *Gibt es ganze Zahlen* a, b *so dass*

$$a^2 - 7b^2 = 1 \ ?$$

Wieder können wir mithilfe algebraischer Zahlen umformen:

$$(a + b\sqrt{7})(a - b\sqrt{7}) = 1$$

und die Frage wird: Gibt es Einheiten im Ring $\mathbb{Z}[\sqrt{7}]$? *Der Dirichletsche Einheitensatz impliziert ja, und in der Tat ist*

$$8^2 - 7 \cdot 3^2 = 1.$$

Es gibt sogar unendlich viele Lösungen (die den Potenzen von $8 + 3\sqrt{7}$ *entsprechen). Siehe auch Beispiel 1.6.6 weiter unten.*

Beispiel 1.2.3 (Fermatsche Gleichung)**.** *Sei* p *eine Primzahl. Gibt es ganze Zahlen* a, b, c *(alle ungleich Null) so dass*

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

Wieder können wir mithilfe algebraischer Zahlen umformen (mit ζ *eine* p*-te Einheitswurzel):*

$$(a - c)(a - \zeta c) \cdots (a - \zeta^{p-1} c) = b^p.$$

(Überprüfen Sie dies!)
Falls nun die eindeutige Primfaktorzerlegung in $\mathbb{Z}[\zeta]$ *gelten würde, könnten wir so argumentieren: Jedes Primelement* π*, das die rechte Seite teilt, muss auch einen der Faktoren auf der linken Seite teilen. Kann es zwei der Faktoren teilen? In diesem Fall müsste es auch die Differenz*

$$(a - \zeta^k c) - (a - \zeta^l c) = c(\zeta^l - \zeta^k)$$

teilen und o.B.d.A. teilt es nicht b*. Man kann sich überlegen, dass alle Zahlen* $\zeta^l - \zeta^k$ *prim sind und bis auf Einheiten alle gleich* $1 - \zeta$*. D.h. falls* π *nicht*

das Primelement $1-\zeta$ ist, dann muss π^p schon einen der Faktoren auf der linken Seite teilen (denn sonst käme π in mindestens zweien vor). Daher bekommen wir für alle k, dass

$$a - \zeta^k c = \varepsilon(1-\zeta)^? \alpha^p,$$

wobei ε eine Einheit ist. Man kann dies mit elementaren Methoden zu einem Widerspruch führen, was allerdings nicht so einfach ist. Hingegen hat das Problem für allgemeine p, also solche, für die in $\mathbb{Z}[\zeta_p]$ keine eindeutige Primfaktorzerlegung gilt[2]*, über 300 Jahre einer Lösung widerstanden! Es wurde erst in den 90er Jahren durch die englischen Mathematiker* Andrew Wiles *und* Richard Taylor *gelöst. Dieser Beweis ist einer der kompliziertesten der Mathematikgeschichte.*

1.3 Aufwärmbeispiel: Gaussche Zahlen

In Beispiel 1.2.1 ging es um den Ring

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{Q}(i)$$

welcher, wie wir sehen werden, der Ring der ganzen Zahlen im imaginär quadratischen Körper $\mathbb{Q}(i)$ ist. Er wird auch der Ring der **gausschen Zahlen** genannt. Es ist lehrreich, sich zu Beginn etwas genauer mit ihm zu beschäftigen. Oben machten wir schon die folgende

Behauptung 1.3.1.

$$p \in \mathbb{Z}[i] \text{ reduzibel} \quad \Leftrightarrow \quad p = a^2 + b^2 \text{ lösbar.}$$

Um dies wirklich zu verstehen, führen wir eine Abbildung ein, die **Norm**

$$N : \mathbb{Z}[i] \to \mathbb{Z}.$$

Sie ist dieselbe, die Sie aus der Algebra schon kennen, und für $x = a + bi$ definiert durch

$$N(x) := x \cdot \overline{x} = (a+bi)(a-bi) = a^2 + b^2.$$

Sie besitzt die folgenden fundamentalen Eigenschaften:

1. $N(1) = 1$;

[2] Ernst Kummer hat obiges Argument (bereits im Jahre 1850!) noch gerettet, falls $p \nmid |\operatorname{Cl}_{\mathbb{Q}(\zeta_p)}|$. Primzahlen p mit dieser Eigenschaft werden regulär genannt.

2. $N(xy) = N(x)N(y)$ (**Multiplikativität**);

3. $N(x) = 1 \Leftrightarrow x$ ist eine Einheit in $\mathbb{Z}[i]$.

Beweis. 1. ist klar. 2. $N(x)N(y) = x\overline{x}y\overline{y} = xy\overline{xy} = (xy)\overline{(xy)} = N(xy)$. 3. Falls $N(x) = x\overline{x} = \pm 1$ so ist $\pm\overline{x}$, welches offensichtlich auch in $\mathbb{Z}[i]$ liegt, ein Inverses von x. Falls x umgekehrt ein Inverses y besitzt, so ist $N(xy) = N(x)N(y) = N(1) = 1$. Da $N(x)$ und $N(y)$ ganze Zahlen sind muss $N(x) = \pm 1$ sein. In diesem speziellen Ring ist aber N immer positiv. □

Damit können wir Behauptung 1.3.1 beweisen:

Beweis. Falls $p = a^2 + b^2$ so ist $p = N(x) = x\overline{x}$ für $x = a + bi$. Dies ist eine Zerlegung von p! Umgekehrt, falls $p = xy$ reduzibel (zerlegbar) ist, so folgt $p^2 = N(xy) = N(x)N(y)$. Da x und y (nach Definition von reduzibel) keine Einheiten sind, muss $N(x) = p$ sein, also falls wir $x = a+bi$ schreiben, $p = a^2 + b^2$. □

Es gab noch eine zweite Behauptung in Beispiel 1.2.1:

Behauptung 1.3.2.

$$p \in \mathbb{Z}[i] \text{ } \textit{reduzibel} \quad \Leftrightarrow \quad p = 2 \text{ } \textit{oder } p \equiv 1 \text{ } (4)$$

Wir werden im nächsten Abschnitt sehen, dass im Ring $\mathbb{Z}[i]$ die eindeutige Primfaktorzerlegung gilt. Damit können wir die Behauptung beweisen:

Beweis. Falls $p = a^2 + b^2$, so gilt natürlich auch die Kongruenz

$$p \equiv a^2 + b^2 \text{ } (4).$$

Nun gilt $a^2 \equiv 0$ (4) oder $a^2 \equiv 1$ (4) für alle ganzen Zahlen a. Daher ist

$$p \equiv 0, 1 \text{ oder } 2 \text{ } (4).$$

Nun ist $p = 2$ oder p ungerade und im letzteren Fall bleibt nur $p \equiv 1$ (4). Umgekehrt, falls $p = 2$, gilt $p = (1 + i)(1 - i)$, p ist also reduzibel. Erinnern wir uns aus der Algebra, dass die Gruppe $\mathbb{F}_p^*$ zyklisch von der Ordung $p - 1$ ist. Falls p ungerade und $p \equiv 1$ (4), dann ist diese Ordnung durch 4 teilbar. Es gibt daher ein Element x der Ordnung 4. Es muss daher $x^2 = -1$ in $\mathbb{F}_p^*$ sein. Mit anderen Worten, wir finden eine ganze Zahl x so, dass

$$x^2 + 1 \equiv 0 \text{ } (p).$$

Es ist daher in $\mathbb{Z}[i]$:

$$(x+i)(x-i) = np.$$

Da nun in $\mathbb{Z}[i]$ die eindeutige Primfaktorzerlegung gilt: Falls p irreduzibel ist, muss es prim sein, und daher entweder $x+i$ oder $x-i$ teilen. Die Zahlen $\frac{x \pm i}{p}$ liegen aber beide nicht in $\mathbb{Z}[i]$. Daher muss p reduzibel sein. □

1.4 Wiederholung zur eindeutigen Primfaktorzerlegung

Im letzten Abschnitt haben wir gesehen, dass die eindeutige Primfaktorzerlegung in Ringen wie $\mathbb{Z}[i]$ unmittelbar elementar-zahlentheorische Konsequenzen hat. Um besser zu verstehen welche Eigenschaften eines Ringes die eindeutige Primfaktorzerlegung zur Folge haben, wiederholen wir aus der Algebra die Begriffe:

irreduzibel
: Ein Element x eines Ringes, das ungleich 0 und keine Einheit ist, heisst irreduzibel, falls aus $x = yz$ folgt, dass entweder y oder z eine Einheit sind.

prim
: Ein Element p eines Ringes, das ungleich 0 und keine Einheit ist, heisst prim, falls aus $p|xy$ folgt, dass $p|x$ oder $p|y$.

faktoriell
: Ein faktorieller Ring ist ein Ring in dem jedes Element ungleich 0 eine (bis auf Reihenfolge und Multiplikation mit Einheiten) eindeutige Zerlegung in irreduzible Elemente besitzt.

Hauptidealring
: Ein nullteilerfreier Ring heisst Hauptidealring, wenn jedes Ideal von einem Element erzeugt wird.

Euklidisch
: Ein nullteilerfreier Ring heisst Euklidisch, wenn in ihm eine Division mit Rest möglich ist.

Erinnere, dass "nullteilerfrei" bedeutet, dass aus $xy = 0$ folgt, dass $x = 0$ oder $y = 0$. Alle Unterringe von Körpern, wie die Ringe der ganzen Zahlen in Zahlkörpern, die wir definieren werden, sind also nullteilerfrei.
Die präzise Definition von Euklidisch ist etwas technisch:

Definition 1.4.1. *Ein nullteilerfreier Ring R heisst Euklidisch, wenn es eine Bewertungsfunktion $\nu : R \setminus \{0\} \to \mathbb{N}_0$ gibt, so dass für je zwei Elemente $x, y \in R$ mit $y \neq 0$, Elemente q (Quotient) und r (Rest) existieren so dass*

$$x = qy + r$$

mit $\nu(r) < \nu(y)$ oder $r = 0$. Ferner muss gelten $\nu(xy) \geq \nu(y)$ für alle $x, y \neq 0$.

Zum Beispiel ist der Ring $\mathbb{Z}$ mittels der Bewertungsfunktion $\nu(x) := |x|$ Euklidisch.
Zunächst haben wir folgendes

Lemma 1.4.2. *In einem nullteilerfreien Ring R gilt immer die Implikation "prim" $\Rightarrow$ "irreduzibel".*

Beweis. Sei x prim und betrachte eine Zerlegung $x = yz$. Dann teilt x das Produkt yz also einen der Faktoren, z.B. $y = wx$. Daher $x = xwz$, und da R nullteilerfrei ist können wir kürzen: $wz = 1$ also z Einheit. □

Satz 1.4.3. *Für einen Noetherschen[3] nullteilerfreien Ring gelten die folgenden Implikationen:*

$$\boxed{\textbf{Euklidisch}} \Rightarrow \boxed{\textbf{Hauptidealring}} \Rightarrow \boxed{\begin{matrix}\textbf{irreduzibel}\\ \textbf{=prim}\end{matrix}} \Leftrightarrow \boxed{\textbf{faktoriell}}$$

Im allgemeinen gilt *keine* der anderen Umkehrungen. Für Ringe von ganzen Zahlen in Zahlkörpern wird jedoch auch die Implikation "faktoriell impliziert Hauptidealring" gelten, aber *nicht* die Umkehrung "Hauptidealring impliziert Euklidisch".
Zur Erinnerung geben wir hier den Beweis des Satzes 1.4.3:

Beweis. Euklidisch impliziert Hauptidealring: Sei R Euklidisch und $I \subseteq R$ ein Ideal. Wähle ein Element $y \in I$ ungleich 0 mit $\nu(y)$ minimal. Sei $x \in I$ ein beliebiges Element und schreibe $x = yq + r$ mit $\nu(r) < \nu(y)$ oder $r = 0$. Nun ist $r = x - yq \in I$ und daher folgt $r = 0$, da y minimale Bewertung unter den Elementen von I hat. Also ist ein beliebiges Element $x \in I$ ein Vielfaches von y, und somit ist $I = (y)$ ein Hauptideal.
Hauptidealring impliziert "irreduzibel = prim": Zunächst impliziert in nullteilerfreien Ringen "prim" immer "irreduzibel" (Lemma 1.4.2). Umgekehrt sei x irreduzibel und $x|yz$. Betrachte das von x und y erzeugte Ideal (x, y).

[3]Diese Annahme vereinfacht die Situation, da a priori *irgendeine* Zerlegung in irreduzible existiert. Ausserdem sind alle Ringe der Vorlesung Noethersch.

Da R Hauptidealring ist es von einem Element a erzeugt: $(x, y) = (a)$. Es folgt $x = ab$ und dann a Einheit (also $(x, y) = R$) oder b Einheit. Falls b eine Einheit ist, gilt $(x, y) = (x)$, also $y \in (x)$, d.h. $x|y$. Genauso bekommt man durch Vertauschen von y und z, dass entweder $(x, z) = R$ oder $x|z$. Wir müssen also nur den Fall auschliessen, dass $(x, y) = (x, z) = R$. Daraus würde aber folgen, dass $R = (x^2, xy, xz, yz) \subset (x)$, also x Einheit und nach Definition nicht irreduzibel.
"Irreduzibel = prim" impliziert faktoriell: Sei $x \in R$ nicht 0. Da R Noethersch ist, gibt es eine Zerlegung

$$x = p_1 \cdots p_n$$

in irreduzible Elemente p_i (Überlegen Sie sich dies als Übung!), welche nach Annahme auch prim sind. Angenommen, es gibt zwei solche Zerlegungen

$$q_1 \cdots q_m = x = p_1 \cdots p_n.$$

Dann folgt $q_1|p_1 \cdots p_n$ also $q_1|p_i$ für irgendein i (Primeigenschaft). Da p_i irreduzibel ist, müssen also p_i und q_1 bis auf Einheit übereinstimmen. Durch Umnummerieren können wir annehmen, dass $i = 1$. Durch kürzen von q_1 erhalten wir also

$$q_2 \cdots q_m = \varepsilon p_2 \cdots p_n$$

mit einer Einheit ε. Durch Induktion folgt die Eindeutigkeit.
Faktoriell impliziert "irreduzibel = prim": Nach Lemma 1.4.2 impliziert "prim" immer "irreduzibel". Sei also x irreduzibel und $x|yz$, also $ax = yz$ für ein a ungleich 0[4]. Durch weitere Zerlegung von a, y und z in irreduzible (R ist Noethersch) bekommen wir

$$\underbrace{a_1 \cdots a_n}_{a} \cdot x = \underbrace{y_1 \cdots y_n}_{y} \cdot \underbrace{z_1 \cdots z_n}_{z}.$$

Da diese Zerlegung nach Voraussetzung bis auf Umnummerieren und Multiplikation mit Einheiten eindeutig ist, folgt, dass x bis auf eine Einheit gleich einem der Faktoren y_i oder z_i ist. Insbesondere teilt x entweder y oder z. x ist also prim. □

Wir werden jetzt noch die Begründung nachliefern, dass der Ring der Gausschen Zahlen $\mathbb{Z}[i]$ faktoriell ist, indem wir zeigen:

Proposition 1.4.4. *Der Ring $\mathbb{Z}[i]$ der Gausschen Zahlen ist Euklidisch bzgl. der Norm als Bewertungsfunktion.*

[4]Falls $y = 0$ oder $z = 0$ ist die Implikation klar.

Beweis. Seien x und y in $\mathbb{Z}[i]$ gegeben, beide ungleich Null. Wir müssen q und r finden, so dass

$$x = qy + r$$

mit $N(r) < N(y)$, oder äquivalent $|r| < |y|$, bzw. $\left|\frac{r}{y}\right| < 1$. Teilen der Gleichung durch y und auflösen nach $\frac{r}{y}$ ergibt:

$$\frac{r}{y} = q - \frac{x}{y}.$$

Wir können also das Problem so umformulieren: Sei $\alpha \in \mathbb{Q}(i) \subset \mathbb{C}$ gegeben. Finde $q \in \mathbb{Z}[i]$ so, dass

$$|q - \alpha| < 1.$$

Man stelle sich $\mathbb{Z}[i]$ als Gitter in der komplexen Ebene vor. Sogar für jedes $\alpha \in \mathbb{C}$ findet man einen Gitterpunkt q welcher einen Abstand zu α von höchstens $\frac{\sqrt{2}}{2} < 1$ hat. (Wenn man es ganz explizit haben möchte: $q = [\mathrm{Re}(\alpha)] + [\mathrm{Im}(\alpha)]i$, wobei $[\beta] \in \mathbb{Z}$ für $\beta \in \mathbb{R}$ diejenige ganze Zahl mit geringstem Abstand zu β bezeichne.) □

1.5 Imaginär quadratische Körper

Ein **imaginär quadratischer Körper** ist eine Körpererweiterung von $\mathbb{Q}$ welche durch Adjunktion einer Quadratwurzel aus einer negativen rationalen Zahl (oder äquivalent: einer negativen ganzen Zahl) entsteht. Dies sind also die Körper $\mathbb{Q}(\sqrt{-d})$ für $d \in \mathbb{N}$ quadratfrei. Der Körper $\mathbb{Q}(i)$ des letzten Abschnittes ist der einfachste imaginär quadratische Körper.
Wir haben gesehen, dass im Ring

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

eindeutige Primfaktorzerlegung gilt. Was gilt in allgemeinen imaginär quadratischen Körpern? Wir werden sehen, dass der Ring der ganzen Zahlen in $\mathbb{Q}(\sqrt{-d})$ gleich

$$\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$$

ist ($\mathbb{Z}[i]$ ist der Spezialfall $d = 1$) falls $d \equiv 1, 2\ (4)$, aber gleich

$$\mathbb{Z}[\frac{1 + \sqrt{-d}}{2}] = \{a + b\frac{1 + \sqrt{-d}}{2} \mid a, b \in \mathbb{Z}\}$$

falls $d \equiv 3\ (4)$. Im Augenblick ist dies für uns noch nicht interessant, da wir noch nicht formal definiert haben, was der Ring der ganzen Zahlen im allgemeinen ist.

Bereits hier gibt es i.A. *keine* eindeutige Primfaktorzerlegung. Z.B. hat man im Ring $\mathbb{Z}[\sqrt{-5}]$ die beiden Faktorzerlegungen

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

Behauptung 1.5.1. *Die beiden Faktorzerlegungen in (1) sind maximal und wesentlich verschieden.*

Beweis. Zunächst wollen wir sehen, dass die einzelnen Faktoren irreduzibel sind, sich die beiden Faktorzerlegungen also nicht weiter verfeinern lassen. Nehme z.B. an, wir hätten eine weitere Faktorzerlegung $2 = \alpha \cdot \beta$. Wir wenden die Norm (genauso definiert wie in 1.3) an und erhalten

$$4 = N(2) = N(\alpha) \cdot N(\beta).$$

Es muss also $N(\alpha) = 2$ gelten, wenn α und β beide keine Einheiten sein dürfen. Schreibe $\alpha = a + b\sqrt{-5}$, dann gilt

$$N(\alpha) = a^2 + 5b^2.$$

Offensichtlich kann dieser Ausdruck für $a, b \in \mathbb{Z}$ niemals 2 werden. Überlegen Sie sich als Übung analog, dass auch die anderen Faktoren $3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ irreduzibel sind. Die Faktorzerlegungen sind aber auch wesentlich verschieden. Dann wenn sich z.B. $1+\sqrt{-5}$ von 2 nur um eine Einheit unterscheiden würde, hiesse dies, dass der Quotient $\frac{1+\sqrt{-5}}{2}$ eine Einheit, also insbesondere auch ein Element von $\mathbb{Z}[\sqrt{-5}]$ wäre. Dies ist aber offensichtlich falsch. □

Auch in $\mathbb{Z}$ gibt es natürlich wesentlich verschiedene Faktorzerlegungen, wie z.B:

$$20 = 2 \cdot 10 = 4 \cdot 5.$$

Der Unterschied ist, dass sie sich *verfeinern* lassen zu einer (im wesentlichen) eindeutigen Faktorzerlegung. Man könnte sich daher wünschen, dass es auch im Fall $\mathbb{Z}[\sqrt{-5}]$ einen erweiterten Bereich "idealer Zahlen" gäbe, in welchem eindeutige (Prim-)faktorzerlegung möglich ist, so dass wir in unserem Beispiel schreiben könnten:

$$\begin{aligned} 2 &= (\mathfrak{p}_2)^2 \\ 3 &= \mathfrak{p}_3\overline{\mathfrak{p}}_3 \\ 1+\sqrt{-5} &= \mathfrak{p}_2\mathfrak{p}_3 \\ 1-\sqrt{-5} &= \mathfrak{p}_2\overline{\mathfrak{p}}_3 \end{aligned}$$

und wir dann die folgende gemeinsame Verfeinerung von (1) hätten:

$$6 = (\mathfrak{p}_2)^2 \mathfrak{p}_3 \overline{\mathfrak{p}}_3.$$

Eine solche "ideale Zahl" $\mathfrak{p}$ sollte durch die Menge der gewöhnlichen Zahlen charakterisiert sein, die sie teilt:

$$\{x \in \mathbb{Z}[\sqrt{-5}] \mid \mathfrak{p}|x\}.$$

Aus den gewöhnlichen Rechenregeln für die Teilbarkeit folgt, dass dies ein **Ideal** des Ringes $\mathbb{Z}[\sqrt{-5}]$ ist. Man ist daher dazu übergegangen, mit den Idealen des Ringes selber zu arbeiten. Der Name "Ideal" kommt historisch von dieser hier beschriebenen Bedeutung als "ideale Zahl". Wir werden am Anfang der Vorlesung sehen, dass es in den Ringen der ganzen Zahlen in Zahlkörpern tatsächlich immer eine eindeutige Faktorzerlegung in (Prim-)ideale gibt!
Die Rechnung im Beweis der Behauptung 1.5.1 oben lässt vermuten, dass es sich bei $\mathbb{Z}[\sqrt{-5}]$ um keinen exotischen Fall handelt, sondern es dagegen eher zur Regel gehört, dass in einem imaginär quadratischen Körper *keine* eindeutige Primfaktorzerlegung herrscht.
Bereits Gauss hat durch experimentelle Untersuchungen die folgende Vermutung aufgestellt:

Vermutung 1.5.2. *Ein imaginär-quadratischer Körper $\mathbb{Q}(\sqrt{-d})$ hat eindeutige Primfaktorzerlegung (im Ring der ganzen Zahlen), genau dann wenn*

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Ein unvollständiger Beweis dieser bemerkenswerten Vermutung wurde durch Heegner gegeben, und erst im Jahre 1966 von Baker und Stark fertiggestellt.
Bemerkenswert ist vor allem, *dass* in $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ noch die eindeutige Primfaktorzerlegung gilt! Warum bekommen wir nicht z.B. wieder wesentlich verschiedene Zerlegungen der Form

$$(a + \frac{1+\sqrt{-163}}{2})(a + \frac{1-\sqrt{-163}}{2}) = a^2 + a + 41 = x \cdot y?$$

Dies spiegelt sich darin wieder, dass das Polynom $a^2 + a + 41$ für $a = 1, 2, \ldots, 39$ nur Primzahlen produziert! Eine höchst überraschende Tatsache, die schon Euler beobachtet hat. Wir werden den Beweis der Vermutung in der Vorlesung nicht behandeln können, aber wir werden Werkzeuge erlernen,

mit denen sich verifizieren lässt, dass in den obigen 9 Fällen die eindeutige Primfaktorzerlegung gilt.
Das Beipiel 1.2.1 zur Lösbarkeit der diophantischen Gleichung $x^2 + y^2 = p$ verallgemeinert sich:

Satz 1.5.3. *Die Lösbarkeit der diophantischen Gleichung*

$$a^2 + d \cdot b^2 = p$$

(falls $d \equiv 1, 2\ (4)$) oder

$$a^2 + ab + (\frac{d+1}{4})b^2 = p$$

(falls $d \equiv 3\ (4)$)) lässt sich an einer Kongruenzbedingung an p ablesen, wenn in $\mathbb{Q}(\sqrt{-d})$ eindeutige Primfaktorzerlegung (im Ring der ganzen Zahlen) gilt.

Beachte, dass beide Gleichungen von der Form "$N(x) = p$" sind, für $x \in \mathbb{Z}[\sqrt{-d}]$ bzw. $x \in \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$.
Das Lösbarkeitsverhalten der diophantischen Gleichung $N(x) = p$ im Falle, dass in $\mathbb{Q}(\sqrt{-d})$ keine eindeutige Primfaktorzerlegung gilt, ist (in den meisten Fällen) komplizierter. Die Beschreibung führt in die sogenannte Klassenkörpertheorie und in die Theorie der Modulformen, die wir beide in der Vorlesung nicht behandeln werden. Siehe aber Satz 6.2.2 ganz am Ende für eine Ausnahme.

1.6 Reell quadratische Körper und ihre Einheiten

Wir runden die motivierende Diskussion ab, in dem wir auch die Körper $\mathbb{Q}(\sqrt{d})$ mit $d > 0$ kurz im Detail studieren. Analog zu den imaginär quadratischen Körpern werden wir später beweisen, dass für $d \in \mathbb{N}$ quadratfrei und positiv, der Ring $\mathcal{O}_K$ der ganzen Zahlen in $K = \mathbb{Q}(\sqrt{d})$ gleich

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

ist, falls $d \equiv 2, 3\ (4)$, aber gleich

$$\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\}$$

falls $d \equiv 1\ (4)$. Es ist bis heute nicht bekannt, in welchen dieser Ringe eindeutige Primfaktorzerlegung gilt. Man vermutet, dass dies für unendlich viele d der Fall ist.

Wir haben schon in Beispiel 1.2.2 oben gesehen, dass es interessant ist, nach den Einheiten in diesen Ringen zu fragen. Auch hier bedienen wir uns der Norm $N : \mathcal{O}_K \to \mathbb{Z}$, welche durch

$$N(x) = x \cdot \sigma(x)$$

gegeben ist, wobei σ der nicht-trivale Körperautomorphismus von K ist, also durch

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}.$$

gegeben ist. Es handelt sich also hier, im Gegensatz zu den imaginär-quadratischen Körpern nicht um die komplexe Konjugation. Es gilt also

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

im ersten Fall und

$$N(a + b\frac{1+\sqrt{d}}{2}) = (a + b\frac{1+\sqrt{d}}{2})(a + b\frac{1-\sqrt{d}}{2}) = a^2 + ab - \frac{d-1}{4}b^2$$

im zweiten Fall. Wiederum ist N multiplikativ und es gilt

$$N(x) = \pm 1 \quad \Leftrightarrow \quad x \text{ ist Einheit.}$$

Im Unterschied zum imaginär-quadratischen Fall kann hier auch die Norm -1 vorkommen, muss aber nicht. A priori ist nicht klar, dass es überhaupt Einheiten geben muss. Wir haben bereits in Beispiel 1.2.2 erwähnt, dass der Dirichletsche Einheitensatz, den wir später beweisen wollen, impliziert, dass es immer Einheiten gibt. Im Fall der reell-quadratischen Körper gibt es aber eine interessante Theorie (und einen alternativen Beweis der Existenz von Einheiten) die sich nicht auf andere Körper verallgemeinert. Sie führt auf die Theorie der **Kettenbrüche** und die Approximation von irrationalen Zahlen durch rationale. Der Zusammenhang ist einfach zu sehen. Falls wir die Gleichung $N(x) = 1$ im ersten Fall ($d \equiv 2, 3\ (4)$) ausschreiben

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

und den Betrag nehmen, erhalten wir

$$|a + \sqrt{d}b| \cdot |a - \sqrt{d}b| = 1.$$

Man kann o.B.d.A. annehmen, dass a und b positive ganze Zahlen sind (wir dürfen beide mit -1 Multiplizieren, so dass a o.B.d.A. positiv ist, dann ist

aber mit $a+b\sqrt{d}$ auch $a-b\sqrt{d}$ eine Einheit, so dass o.B.d.A. auch b positiv ist). Teile nun die Gleichung durch b^2:

$$|\frac{a}{b}+\sqrt{d}|\cdot|\frac{a}{b}-\sqrt{d}|=\frac{1}{b^2}.$$

Da sicher $|\frac{a}{b}+\sqrt{d}|>2$, bekommen wir eine Abschätzung der Form:

$$|\frac{a}{b}-\sqrt{d}|\leq\frac{1}{2b^2}.$$

Mit anderen Worten. Falls $a+b\sqrt{d}$ eine Einheit ist (mit $a,b\in\mathbb{N}$), dann ist $\frac{a}{b}$ eine **besonders gute** rationale Approximation von $\sqrt{d}$. Mittels Kettenbrüchen bekommen wir eine alternative, konstruktive Beschreibung solcher besonders guten Approximationen.

Definition 1.6.1. *Ein endlicher* **Kettenbruch** *ist eine rationale Zahl der Form*

$$[a_0;a_1,\ldots,a_n]:=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots\cfrac{1}{a_n}}}}$$

mit $a_0\in\mathbb{Z},a_i\in\mathbb{N}$.

Für eine reelle *irrationale* Zahl $x\in\mathbb{R}$ können wir induktiv eine Folge von Kettenbrüchen definieren, die α approximieren:

$$x_0:=x\quad a_0:=\lfloor x\rfloor$$

$$x_1:=\frac{1}{x_0-a_0}\quad a_1:=\lfloor x_1\rfloor$$

$$x_2:=\frac{1}{x_1-a_1}\quad a_2:=\lfloor x_2\rfloor$$

u.s.w.
Die endlichen Kettenbrüche

$$\frac{p_n}{q_n}:=[a_0;a_1,\ldots,a_n]$$

heissen **Konvergenten** von x. Wir nehmen immer an, dass p_n und q_n teilerfremd sind und dass $q_n>0$. In diesem Fall erfüllen die p_n und q_n eine interessante Rekursionsgleichung. Im Appendix werden wir dies untersuchen und auch den folgenden Satz beweisen.

Satz 1.6.2. *1. Eine rationale Zahl ist selber ein endlicher Kettenbruch.*

2. *Falls x irrational ist, gilt*

$$x = \lim_{n\to\infty} [a_0; a_1, \ldots, a_n],$$

wobei die a_i wie oben konstruiert sind. Sie sind durch diese Gleichung eindeutig bestimmt.

3. *Unter zwei aufeinanderfolgenden Konvergenten gibt es immer eine mit der Abschätzung*

$$|x - \frac{p_n}{q_n}| < \frac{1}{2q_n^2}.$$

4. *Falls* irgendeine *rationale Zahl $\frac{p}{q}$ (mit $q > 0$ und p, q teilerfremd) die Abschätzung*

$$|x - \frac{p}{q}| < \frac{1}{2q^2}$$

erfüllt, dann ist $\frac{p}{q}$ Konvergente.

Wir erhalten die folgende überraschende Konsequenz:

Korollar 1.6.3. *Falls $a + b\sqrt{d}$ eine Einheit von $\mathbb{Z}[\sqrt{d}]$ ist (mit $a, b > 0$), dann ist $\frac{a}{b}$ Konvergente von $\sqrt{d}$.*

Dies gibt uns also ein Verfahren, um die Einheiten von $\mathbb{Z}[\sqrt{d}]$ tatsächlich zu finden. Wir wissen jedoch immer noch nicht, dass tatsächlich Einheiten existieren! Dies folgt jedoch auch als Korollar aus Satz 1.6.2:

Korollar 1.6.4. *Es gibt nicht-triviale*[5] *Einheiten in $\mathbb{Z}[\sqrt{d}]$ (und damit unendlich viele).*

Beweis. Unter den Konvergenten finden wir nach Satz 1.6.2 unendlich viele mit den Abschätzungen

$$|\frac{p_n}{q_n} - \sqrt{d}| < \frac{1}{2q_n^2} \qquad |\frac{p_n}{q_n} + \sqrt{d}| < 4\sqrt{d}.$$

(Die erste Abschätzung ist die aus dem Satz und die zweite folgt daraus auf triviale Weise). Multiplikation mit q_n ergibt:

$$|p_n - q_n\sqrt{d}| < \frac{1}{2q_n} \qquad |p_n + q_n\sqrt{d}| < 4\sqrt{d}q_n.$$

[5] d.h. nicht gleich ± 1.

und Multiplikation der Abschätzungen miteinander ergibt:

$$|p_n^2 - d \cdot q_n^2| = |N(x_n)| < 2\sqrt{d}.$$

für $x_n = p_n + q_n\sqrt{d}$. Mit anderen Worten:

> Es gibt unendlich viele $x \in \mathbb{Z}[\sqrt{d}]$ mit $-2\sqrt{d} < N(x) < 2\sqrt{d}$.

Da sich im Intervall $(-2\sqrt{d}, 2\sqrt{d})$ nur endlich viele ganze Zahlen befinden, können wir nach dem Schubfachprinzip folgern:

> Es gibt ein $m \in \mathbb{Z}$ und unendlich viele $x \in \mathbb{Z}[\sqrt{d}]$ mit $N(x) = m$.

Nun bedienen wir uns eines Tricks: Wir haben

$$\mathbb{Z}[\sqrt{d}]/(m) \cong \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}/m\mathbb{Z}\}.$$

Dieser Restklassenring hat endlich viele, nämlich m^2 Elemente. Wir können also nach nochmaligem Anwenden des Schubfachprinzips folgern:

> Es gibt ein $m \in \mathbb{Z}$ und $y \in \mathbb{Z}[\sqrt{d}]$ und unendlich viele $x \in \mathbb{Z}[\sqrt{d}]$ mit $N(x) = m$ und $x \equiv y\ (m)$.

Nun reichen eigentlich schon *zwei* dieser unendlich vielen x. Seien also x und x' so, dass

$$N(x) = N(x') = m \quad x - x' = m \cdot q$$

für irgendein $q \in \mathbb{Z}[\sqrt{d}]$. Wir bekommen

$$x - x' = x \cdot \sigma(x) \cdot q$$

also

$$x \cdot (1 - \sigma(x) \cdot q) = x'.$$

Anwenden der Norm ergibt:

$$N(x) \cdot N(1 - \sigma(x) \cdot q) = N(x').$$

Da $N(x) = N(x') = m$ folgt:

$$N(1 - \sigma(x) \cdot q) = 1.$$

Also ist $1 - \sigma(x) \cdot q$ eine Einheit, und der Fall, dass dies zufällig -1 ist, kann nur für höchstens ein gewähltes Paar auftreten. □

Später werden wir sehen, dass $\mathbb{Z}[\sqrt{d}]^* \cong \{\pm 1\} \times \mathbb{Z}$ (Dirichletscher Einheitensatz). Die gefundenen Einheiten sind also bis auf Vorzeichen alle Potenzen einer erzeugenden Grundeinheit ε.

Beispiel 1.6.5.

$$\mathbb{Z}[\sqrt{3}]$$

Berechnen wir zunächst die Kettenbruchentwicklung:

$$\begin{array}{ll} x_0 = \sqrt{3} = 1,732\ldots & a_0 = \lfloor 1,732\ldots \rfloor = 1 \\ x_1 = \frac{1}{0,732\ldots} = 1,366\ldots & a_1 = \lfloor 1,336\ldots \rfloor = 1 \\ x_2 = \frac{1}{0,336\ldots} = 2,732\ldots & a_2 = \lfloor 2,732\ldots \rfloor = 2 \\ x_3 = \frac{1}{0,732\ldots} = 1,366\ldots & a_3 = \lfloor 1,336\ldots \rfloor = 1 \\ \vdots & \vdots \end{array}$$

Überraschenderweise wird die Kettenbruchentwicklung periodisch. Wir schreiben daher auch

$$\sqrt{3} = [1; \overline{1,2}].$$

(Man kann zeigen, dass eine irrationale Zahl genau dann eine periodische Kettenbruchentwicklung hat, wenn Sie algebraisch vom Grad 2 über $\mathbb{Q}$ ist). Berechnen wir nun die Konvergenten $\frac{p_n}{q_n}$ und testen ob die Norm des korrespondierenden Elementes $p_n + q_n\sqrt{d}$ tatsächlich ± 1 ist:

$$\begin{array}{ll} [1] = 1 = \frac{1}{1} & N(1+\sqrt{3}) = -2 \\ [1;1] = 1 + \frac{1}{1} = \frac{2}{1} & N(2+\sqrt{3}) = 1 \end{array}$$

Wir wurden also schnell fündig: $2 + \sqrt{3}$ ist eine Einheit!

Beispiel 1.6.6 (cf. Beispiel 1.2.2)**.**

$$\mathbb{Z}[\sqrt{7}]$$

Wie oben können wir die Kettenbruchentwicklung bestimmen und erhalten:

$$\sqrt{7} = [2; \overline{1,1,1,4}].$$

Berechnen wir nun die Konvergenten $\frac{p_n}{q_n}$ und testen ob die Norm des korrespondierenden Elementes $p_n + q_n\sqrt{d}$ tatsächlich ± 1 ist:

$$\begin{array}{ll} [2] = 2 = \frac{2}{1} & N(2+\sqrt{7}) = -3 \\ [2;1] = 2 + \frac{1}{1} = \frac{3}{1} & N(3+\sqrt{7}) = 2 \\ [2;1,1] = 2 + \frac{1}{1+\frac{1}{1}} = \frac{5}{2} & N(5+2\sqrt{7}) = -3 \\ [2;1,1,1] = 2 + \frac{1}{1+\frac{1}{1+\frac{1}{1}}} = \frac{8}{3} & N(8+3\sqrt{7}) = 1 \end{array}$$

Wieder finden wir die Einheit $8 + 3\sqrt{7}$.

1.7 Appendix: Mehr zu Kettenbrüchen

Dieser Abschnitt wurde in der Vorlesung nicht behandelt. Für Interessierte wird hier der Satz 1.6.2 über die Kettenbruchentwicklung bewiesen.
Sei $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$. Auf dieser Menge operieren ganzzahlig-invertierbare Matrizen

$$\mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z}, ad - bc = \pm 1 \right\}$$

durch Möbiustransformationen:

$$\tau \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ \tau := \frac{a\tau + b}{c\tau + d}.$$

Dieser Ausdruck ist entsprechend der üblichen Konventionen zu verstehen, falls $c\tau + d = 0$ oder $\tau = \infty$.
Man überlegt sich leicht, dass

$$\underbrace{\begin{pmatrix} 1 & a_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix}}_{=:A_n} \circ 0 = [a_0; a_1, \ldots, a_n].$$

und wenn wir die rechte Seite als $\frac{p_n}{q_n}$ (mit $q_n > 0$ und teilerfremd) schreiben, gilt auch

$$A_n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} p_n \\ q_n \end{pmatrix}$$

(Grund: Dies gilt sicher bis auf Vielfache. Da aber p_n, q_n als Einträge einer Spalte der ganzzahlig invertierbaren Matrix A auftauchen, müssen Sie teilerfremd sein.) Ferner gilt:

$$A_n \circ \infty = [a_0; a_1, \ldots, a_{n-1}],$$

da $\frac{1}{a_n + \infty} = 0$ nach unseren Konventionen (der letzte Faktor der Matrix A_n wird also aufgefressen). Daher aus demselben Grund

$$A_n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} p_{n-1} \\ q_{n-1} \end{pmatrix}.$$

Also insgesamt:

$$A_n = \begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix}.$$

Inbesondere erhalten wir, dass

$$\begin{pmatrix} p_{n-2} & p_{n-1} \\ q_{n-2} & q_{n-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix}.$$

Dies ermöglicht, Zähler und Nenner der Konvergenten über die Rekursionsgleichungen

$$\boxed{p_n = p_{n-1}a_n + p_{n-2} \qquad q_n = q_{n-1}a_n + q_{n-2}}$$

zu berechnen.

Satz 1.7.1. *1. Die Konvergenten erfüllen die folgenden Abschätzungen*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < x < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

2. $|\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}}| = \frac{1}{q_{2n+1}q_{2n}}$.

3. $|x - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$.

Insbesondere konvergieren die Konvergenten tatsächlich gegen x.

4. Es gilt sogar eine der Abschätzungen

$$|x - \frac{p_n}{q_n}| < \frac{1}{2q_n^2} \quad \textit{oder} \quad |x - \frac{p_{n+1}}{q_{n+1}}| < \frac{1}{2q_{n+1}^2}.$$

Beweis. Nach Konstruktion gilt:

$$A_n^{-1} \circ x = x_{n+1}^{-1} < 1$$

und also

$$A_n \circ (x_{n+1})^{-1} = x, \qquad A_n \circ 0 = \frac{p_n}{q_n}.$$

Wir haben die folgenden Ungleichungen

$$0 < \frac{1}{\frac{1}{a_{n+2}} + a_{n+1}} < \frac{1}{x_{n+1}} < \frac{1}{a_{n+1}} \tag{2}$$

unter Benutzung von $a_{n+1} = \lfloor x_{n+1} \rfloor$ und $a_{n+2} = \lfloor \frac{1}{x_{n+1} - a_{n+1}} \rfloor$.
Aus Lemma 1.7.4 unten folgt: Wenn wir A_n, n gerade, auf die Zahlen (2) anwenden, bekommen wir

$$\frac{p_n}{q_n} < \frac{p_{n+2}}{q_{n+2}} < x < \frac{p_{n+1}}{q_{n+1}}$$

und falls n ungerade ist, dasselbe mit umgekehrten Relationen. Daraus folgt 1.
Berechnen wir einige genaue Abstände mit Lemma 1.7.4. Der Abstand zwischen 0 und $\frac{1}{x_{n+1}}$ wird

$$\frac{1}{q_{n-1}x_{n+1}^{-1}+q_n}\cdot\frac{1}{q_n}\cdot\left(\frac{1}{x_{n+1}}-0\right)=\boxed{\frac{1}{q_{n-1}+q_nx_{n+1}}\cdot\frac{1}{q_n}<\frac{1}{q_n^2}}$$

(Beachte: $x_{n+1}>1$.) Hieraus folgt 3.
Der Abstand zwischen 0 und $\frac{1}{a_{n+1}}$ wird

$$\frac{1}{q_{n-1}a_{n+1}^{-1}+q_n}\cdot\frac{1}{q_n}\cdot\left(\frac{1}{a_{n+1}}-0\right)=\frac{1}{q_{n-1}+q_na_{n+1}}\cdot\frac{1}{q_n}=\boxed{\frac{1}{q_{n+1}q_n}}$$

Dies ist 2.
4. Falls nun

$$x-\frac{p_{2n}}{q_{2n}}>\frac{1}{2q_{2n}^2}\quad\text{und}\quad\frac{p_{2n+1}}{q_{2n+1}}-x>\frac{1}{2q_{2n+1}^2}\tag{3}$$

dann würde folgen:

$$\frac{1}{2q_{2n+1}^2}+\frac{1}{2q_{2n}^2}<\frac{1}{q_{2n+1}q_{2n}}$$

und daraus durch leichtes Umformen: $(q_{2n+1}-q_{2n})^2\leq 0$. Dies ist aber (wegen der Rekursionsformel) unmöglich, sobald $n\geq 1$. Also gilt zumindest eine der Abschätzungen in (3), also Aussage 4. □

Die Konvergenten $\frac{p_n}{q_n}$ sind die besten Approximationen mit einem durch q_n beschränkten Nenner, die man für eine irrationale Zahl finden kann:

Lemma 1.7.2. *1. Falls*

$$|x-\frac{p}{q}|<|x-\frac{p_n}{q_n}|$$

dann ist $q>q_n$.

2. Falls sogar

$$|qx-p|<|q_nx-p_n|$$

dann ist $q\geq q_{n+1}$.

Beweis. 2. Annahme $q < q_{n+1}$. Sei

$$\begin{pmatrix} r \\ s \end{pmatrix} = A_{n+1}^{-1} \circ \begin{pmatrix} p \\ q \end{pmatrix}$$

Dann folgt $q_n r + q_{n+1} s = q$. Daraus folgt, dass r und s verschiedene Vorzeichen haben müssen. Denn wenn beide positiv wären, müsste s Null sein, denn q ist kleiner als q_{n+1}. Dann wäre aber $\frac{p}{q} = \frac{p_n}{q_n}$ was ausgeschlossen ist. Dann ist

$$|qx-p| = |(q_n r+q_{n+1}s)x+(p_n r+q_{p+1}s)| = |r(q_n x-p_n)+s(q_{n+1}x-p_{n+1})|.$$

Nun haben $q_n x - p_n$ und $q_{n+1}x - p_{n+1}$ auch unterschiedliche Vorzeichen, d.h. wir bekommen

$$= |r(q_n x - p_n)| + |s(q_{n+1}x - p_{n+1})| \geq |r(q_n x - p_n)| \geq |q_n x - p_n|.$$

($r = 0$ impliziert $\frac{p}{q} = \frac{p_{n+1}}{q_{n+1}}$ und daher $q = q_{n+1}$.) Widerspruch.
1. Falls $q \leq q_n$ und $|x - \frac{p}{q}| < |x - \frac{p_n}{q_n}|$ dann gilt auch das Produkt der Abschätzungen

$$|px - q| < |q_n x - p_n|$$

und daher $q \geq q_{n+1} > q_n$ nach 2. Widerspruch. □

Satz 1.7.3. *Falls*

$$|x - \frac{p}{q}| < \frac{1}{2q^2}$$

dann ist $\frac{p}{q}$ Konvergente.

Beweis. Wähle n so, dass $q_n \leq q < q_{n+1}$. Dann gilt nach Lemma 1.7.2, 2.:

$$|qx - p| \geq |q_n x - p_n|$$

also unter Benutzung der gegebenen Abschätzung

$$\frac{1}{2qq_n} > \frac{q}{q_n}|x - \frac{p}{q}| \geq |x - \frac{p_n}{p_n}|.$$

Daher, falls $\frac{p}{q} \neq \frac{p_n}{q_n}$

$$\frac{1}{q_n q} \leq |\frac{p}{q} - \frac{p_n}{q_n}| \leq |x - \frac{p}{q}| + |x - \frac{p_n}{q_n}| < \frac{1}{2q^2} + \frac{1}{2qq_n}.$$

Also durch Multiplikation mit $2q^2 q_n$:

$$2q < q_n + q.$$

Also $q < q_n$. Widerspruch. □

Lemma 1.7.4. *Für eine beliebige Matrix* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *in* $\mathrm{GL}_2(\mathbb{Z})$ *und* $\kappa, \tau \in \mathbb{R}$ *gilt:*

$$A \circ \tau - A \circ \kappa = \det(A) \frac{\tau - \kappa}{(c\tau + d) \cdot (c\kappa + d)},$$

insbesondere:

$$|A \circ \tau - A \circ \kappa| = \frac{|\tau - \kappa|}{|c\tau + d| \cdot |c\kappa + d|},$$

vorausgesetzt, dass nicht A *angewendet auf eine der Zahlen* τ, κ *gleich* ∞ *ist.*

Beweis. Übung. □

Satz 1.6.2, 2.–4. ergibt sich aus den in diesem Abschnitt bewiesenen Aussagen. Die Aussage 1., also dass sich jede *rationale* Zahl als Kettenbruch darstellen lässt, folgt aus der folgenden Beobachtung. Wenn wir das Verfahren für irrationale Zahlen auf einen Bruch $x = \frac{c}{d}$ anwenden, bekommen wir

$$a_0 = \lfloor \frac{c}{d} \rfloor = \lfloor \frac{qd + r}{d} \rfloor = \lfloor q + \frac{r}{d} \rfloor = q.$$

Der erste Koeffizient der Kettenbruchentwicklung ist also gerade der Quotient bei der Division mit Rest. Wir bekommen $x_1 = \frac{1}{x - a_0} = \frac{d}{r}$. Das Verfahren ist also nichts anderes als der Euklidische Algorithmus! Nach endlich vielen Schritten kommt dieser zum Ende (in jedem Schritt ist x_{n+1} ein Bruch mit kleinerem Nenner als der von x_n), d.h. irgendwann ist der auftretende Rest 0, d.h. $a_n = x_n$ und damit

$$\frac{x}{y} = [a_0; a_1, \ldots, a_n].$$

Diese Darstellung ist aber nicht eindeutig, denn

$$[a_0; a_1, \ldots, a_n] = [a_0; a_1, \ldots, a_n - 1, 1].$$

2 Grundlagen

2.1 Ganzheitsringe

Im Fall $\mathbb{Q}(i)$ haben wir mit dem Ring $\mathbb{Z}[i]$ als "Ring der ganzen Zahlen" gearbeitet. Genauso gut hätten wir auch z.B. einen der Ringe

$$\cdots \subset \mathbb{Z}[4i] \subset \mathbb{Z}[2i] \subset \mathbb{Z}[i] \subset \mathbb{Z}[\frac{1}{2}i]$$

nehmen können. Was zeichnet $\mathbb{Z}[i]$ aus? Der Ring $\mathbb{Z}[\frac{1}{2}i]$ ist kein endlich erzeugter $\mathbb{Z}$-Modul mehr, denn in ihm liegen z.B. alle Elemente $\frac{1}{2^k} \in \mathbb{Q}$. Der Ring $\mathbb{Z}[2i]$ ist — wie $\mathbb{Z}[i]$ — auch ein Gitter, also als Modul isomorph zu $\mathbb{Z}^2$. In ihm gilt aber nicht mehr die eindeutige Primfaktorzerlegung. In gewissem Sinne ist also $\mathbb{Z}[i]$ optimal. Im Fall $\mathbb{Q}(\sqrt{-3})$ haben wir gesehen, dass es besser ist, mit $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ zu arbeiten, in dem allerdings sehr wohl in dieser Darstellung ein Nenner auftritt. Trotzdem handelt es sich um ein Gitter, d.h. als Modul ist dieser Ring isomorph zu $\mathbb{Z}^2$.

Lemma 2.1.1.

$$\mathbb{Z}[i] = \{x \in \mathbb{Q}(i) \mid \operatorname{mipol}_{\mathbb{Q}}(x) \in \mathbb{Z}[t]\}.$$

Hier ist das normierte *Minimalpolynom gemeint.*

Beweis. Aus der Algebra wissen wir, dass für ein $x = a + bi \in \mathbb{Q}(i)$, welches nicht in $\mathbb{Q}$ liegt

$$\operatorname{mipol}_{\mathbb{Q}}(x) = t^2 - \operatorname{tr}(x)t + N(x) = t^2 - 2at + a^2 + b^2.$$

Die Inklusion $\subseteq$ ist also sofort klar. Umgekehrt, falls $2a \in \mathbb{Z}$ und $a^2 + b^2 \in \mathbb{Z}$ schreibe $a = \frac{\widetilde{a}}{2}$ mit $\widetilde{a} \in \mathbb{Z}$ und $b = \frac{\widetilde{b}}{2}$. Es gilt dann

$$\widetilde{a}^2 + \widetilde{b}^2 \in 4\mathbb{Z}$$

und daher auch $\widetilde{b} \in \mathbb{Z}$. Da Quadrate kongruent zu 0 oder 1 modulo 4 sind, müssen sowohl $\widetilde{a}$ als auch $\widetilde{b}$ gerade sein, also $a, b \in \mathbb{Z}$. □

Dies wird das entscheidende Kriterium sein. Es ist aber praktisch, nicht unbedingt zu fordern, dass das normierte Minimalpolynom ganzzahlige Koeffizienten hat, sondern dass x *irgendein* normiertes Polynom mit ganzzahligen Koeffizienten erfüllt. (Später werden wir sehen, dass diese Forderung äquivalent ist.)

Definition 2.1.2. *Eine algebraische Zahl x heisst* **ganz**, *falls es $a_i \in \mathbb{Z}$ gibt so, dass*

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

mit $n \geq 1$.

Beachte, dass es entscheidend ist, dass das Polynom normiert ist, denn jedes beliebige Polynom kann natürlich durch Multiplikation mit dem Hauptnenner ganzzahlig gemacht werden. Wir können deshalb definieren:

Definition 2.1.3. *Sei K ein Zahlkörper.*

$$\mathcal{O}_K := \{x \in K \mid x \text{ ist ganz }\}$$

heisst der **Ring der ganzen Zahlen** *(oder auch* **Ganzheitsring***) in K.*

Beachte, dass keineswegs klar ist, dass diese Teilmenge von K tatsächlich ein Ring ist. Dies werden wir im Laufe dieses Abschnitts beweisen.
Die Begrifflichkeit "ganz" ist auch sinnvoll für andere Grundringe als $\mathbb{Z}$:

Definition 2.1.4. *Seien $A \subset B$ Ringe. Ein Element $b \in B$ heisst* **ganz über** *A falls es $a_i \in A$ gibt so, dass*

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

mit $n \geq 1$.

Um mit dem Begriff arbeiten zu können ist es praktisch, die folgende alternative Charakterisierung zu haben:

Satz 2.1.5. *Seien $A \subset B$ Ringe. Endlich viele Elemente $b_1, \ldots, b_n \in B$ sind genau dann ganz über A, wenn der Ring*

$$A[b_1, \ldots, b_n]$$

als A-Modul endlich erzeugt ist.

Beachte, dass $A[b_1, \ldots, b_n]$ aus allen *polynomialen* Ausdrücken in den b_i besteht, in denen beliebige Exponenten vorkommen dürfen. Als A-Modul endlich erzeugt zu sein, heisst hingegen, dass es eine endliche Menge $\omega_1, \ldots, \omega_m$ gibt (ein Erzeugendensystem) so dass

$$A[b_1, \ldots, b_n] = \{\sum_i \alpha_i \omega_i \mid \alpha_i \in A\}.$$

Von den ω_i dürfen also keine Produkte oder Potenzen genommen werden. Wenn man $A[b_1, \ldots, b_n]$ als A-Modul auffasst, vergisst man die Multiplikation!

Beweis. Die Richtung "$b_1, \ldots, b_n$ ganz $\Rightarrow A[b_1, \ldots, b_n]$ als A-Modul endlich erzeugt" beweisen wir durch Induktion. Dazu ist zu zeigen: "b ganz $\Rightarrow A[b]$ als A-Modul endlich erzeugt". Sei

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

eine Ganzheitsgleichung für b. Behauptung: Die Menge $1, b, b^2, \ldots, b^{n-1}$ ist ein Erzeugendensystem von $A[b]$ als A-Modul. Sicherlich ist die unendliche Menge $1, b, \ldots, b^n, b^{n+1}, \ldots$ ein Erzeugendensystem. Wir müssen also sehen, dass von b^n an, alle diese Potenzen als Linearkombinationen der $1, \ldots, b^{n-1}$ ausdrückbar sind. Für b^n folgt dies aus der Ganzheitsgleichung, denn

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

(Hier ist entscheidend, dass der erste Koeffizient eins ist!) Für die höheren Potenzen folgt dies per Induktion: Indem wir die Ganzheitsgleichung mit einer Potenz b^k multiplizieren, können wir b^{n+k} durch kleinere Potenzen ausdrücken.
Sei nun umgekehrt $A[b_1, \ldots, b_n]$ als A-Modul endlich erzeugt und wähle ein endliches Erzeugendensystem $\omega_1, \ldots, \omega_m$. Sei $b \in A[b_1, \ldots, b_n]$ ein beliebiges Element. Wir können für jedes i das Produkt $b\omega_i$ wieder durch die Elemente des Erzeugensystems ausdrücken:

$$b\omega_i = \sum_j a_{ij}\omega_j.$$

Die Matrix $A = (a_{ij})$ ist also die (besser: eine) Matrixdarstellung der Multiplikation mit b im Erzeugendensystem $\omega_1, \ldots, \omega_m$. In Matrixschreibweise:

$$b \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_m \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_m \end{pmatrix}$$

oder suggestiver:

$$(b1 - A) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_m \end{pmatrix} = 0.$$

Nun gilt für eine beliebige Matrix X mit Koeffizienten in einem beliebigen Ring die Gleichung (Laplacescher Entwicklungssatz)

$$\boxed{X \cdot X^* = X^* \cdot X = \det(X) \cdot 1}$$

wobei X^* die adjungierte Matrix ist. In dem wir mit der Adjungierten $(b1 - A)^*$ multiplizieren, erhalten wir also:

$$\det(b1 - A) \cdot \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_m \end{pmatrix} = 0.$$

Da aber $\omega_1, \ldots, \omega_m$ ein Erzeugendensystem ist, gibt es insbesondere eine Darstellung

$$1 = \alpha_1\omega_1 + \cdots + \alpha_m\omega_m.$$

Multiplikation mit $\det(b1 - A)$ ergibt:

$$\det(b1 - A) = 0.$$

Die Formel für die Determinante ergibt:

$$b^n - \mathrm{tr}(A)b^{n-1} \pm \cdots \pm \det(A) = 0.$$

Dies ist eine normierte Gleichung mit Koeffizienten in A, das Element b ist also ganz über A. □

Insbesondere folgt aus dem Beweis, dass der Ring der ganzen Zahlen $\mathcal{O}_K$ (Definition 2.1.3) tatsächlich ein Ring ist: Falls $x, y \in \mathcal{O}_K$ so ist $\mathbb{Z}[x, y]$ als $\mathbb{Z}$-Modul endlich erzeugt und daher ist jedes Element darin ganz, insbesondere $x + y$ und xy.
Falls $A \subseteq B$ Ringe sind, sagen wir, dass B ganz über A ist, falls jedes Element $b \in B$ ganz über A ist.

Satz 2.1.6. *Seien $A \subseteq B \subseteq C$ Ringe. Falls C ganz über B und B ganz über A, dann ist C ganz über A.*

Beweis. Wir zeigen dies zunächst für den Fall, dass B und C endlich erzeugte A-Algebren sind. Dann impliziert Satz 2.1.5, dass B als A-Modul endlich erzeugt ist und dass C als B-Modul endlich erzeugt ist. Es folgt daher, dass auch C als A-Modul endlich erzeugt ist (dies zeigt man genauso wie für Körpererweiterungen). C ist also ganz über A.
Nun zum allgemeinen Fall. Sei $c \in C$. Wir müssen zeigen, dass c ganz über A ist. c ist zunächst ganz über B, d.h. erfüllt eine Gleichung

$$c^n + b_1c^{n-1} + \cdots + b_n = 0.$$

mit $b_i \in B$. D.h. insbesondere ist c ganz über $A[b_1, \ldots, b_n]$. Wenn wir den Satz also für die Ringe

$$A \subseteq A[b_1, \ldots, b_n] \subseteq A[b_1, \ldots, b_n, c]$$

kennen, dann folgt die Aussage. Mit anderen Worten, wir dürfen o.B.d.A. annehmen, dass B und C endlich erzeugte A-Algebren sind. □

Definition 2.1.7. *Seien $A \subseteq B$ Ringe.*

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

heisst **ganzer Abschluss** *von A in B.*

Zum Besipiel ist $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z}$ in K. Wie für diesen zeigt man, dass $\overline{A}$ immer ein Ring ist.

Definition 2.1.8. *Sei A ein nullteilerfreier Ring. Dann heisst der ganze Abschluss $\overline{A}$ von A in* $\mathrm{Quot}(A)$ *(beachte, da A nullteilerfrei ist $A \subseteq \mathrm{Quot}(A)$) die* **Normalisierung von** *A. Gilt $A = \overline{A}$ so heisst A* **normal** *(oder* **ganzabgeschlossen***).*

Lemma 2.1.9. *$\mathcal{O}_K$ is ganzabgeschlossen.*

Beweis. Sei $\overline{\mathcal{O}_K}$ die Normalisierung von $\mathcal{O}_K$. Wir haben

$$\mathbb{Z} \subseteq \mathcal{O}_K \subseteq \overline{\mathcal{O}_K}$$

Nach Definition ist $\mathcal{O}_K$ ganz über $\mathbb{Z}$ und $\overline{\mathcal{O}_K}$ ganz über $\mathcal{O}_K$. Daher ist nach Satz 2.1.6 auch $\overline{\mathcal{O}_K}$ ganz über $\mathbb{Z}$. Daraus folgt aber $\overline{\mathcal{O}_K} \subseteq \mathcal{O}_K$. □

Beispiel 2.1.10. *$\mathbb{Z}[2i]$ ist nicht ganzabgeschlossen. Betrachte das Element $i = \frac{2i}{2}$. Es liegt im Quotientenkörper* $\mathrm{Quot}(\mathbb{Z}[2i]) = \mathbb{Q}(i)$ *und erfüllt die normierte Gleichung $t^2 + 1 = 0$ mit Koeffizienten in $\mathbb{Z} \subset \mathbb{Z}[2i]$, d.h. es ist ganz über $\mathbb{Z}[2i]$. Aber i liegt selber nicht in $\mathbb{Z}[2i]$.*

Wir sehen also, warum es sinnvoll war, den Ring der ganzen Zahlen so zu definieren, wie wir es getan haben. Wäre der Ring zu gross, enthielte er nicht-ganze Elemente und könnte daher *auf keinen Fall* als $\mathbb{Z}$-Modul endlich erzeugt sein. (Wir werden später sehen, dass er eine endlich erzeugte $\mathbb{Z}$-Algebra ist und daher nach Satz 2.1.5 in der Tat ein endlich erzeugter $\mathbb{Z}$-Modul). Wäre der Ring zu klein, so wäre er nicht mehr ganzabgeschlossen. Das folgende Lemma zeigt, dass dies notwendig für die eindeutige Primfaktorzerlegung ist. (Später werden wir sehen, dass es auch notwendig ist, um die anvisierte Verallgemeinerung, also die eindeutige Faktorisierung in Prim*ideale* zu haben.)

Lemma 2.1.11. *"Faktoriell" impliziert "ganzabgeschlossen".*

Beweis. Sei A ein nullteilerfreier Ring und sei $\frac{x}{y} \in \mathrm{Quot}(A)$ ganz über A, d.h. es gibt $a_i \in A$ so dass

$$\left(\frac{x}{y}\right)^n + a_1 \left(\frac{x}{y}\right)^{n-1} + \cdots + a_n = 0.$$

Multiplikation mit y^n ergibt:

$$x^n + a_1 x^{n-1} y + \cdots + a_n y^n = 0.$$

D.h. aber, dass jeder Primteiler von y auch x teilt. Wenn wir annehmen, dass $\frac{x}{y}$ gekürzt ist, so folgt y Einheit, und daher $\frac{x}{y} \in A$. A ist also ganzabgeschlossen. □

Wir wollen zum Abschluss des Abschnittes noch beweisen, dass die Definition von ganzer Zahl über das Minimalpolynom (siehe auch Lemma 2.1.1) äquivalent ist:

Lemma 2.1.12. *Sei K ein Zahlkörper. Dann gilt: $x \in K$ ist ganz $\Leftrightarrow$ $\mathrm{mipol}_{\mathbb{Q}}(x) \in \mathbb{Z}[t]$.*

Beweis. "$\Leftarrow$" ist klar.
"$\Rightarrow$": Falls x ganz ist, existiert ein normiertes Polynom $p \in \mathbb{Z}[t]$ mit $p(x) = 0$. Nun teilt das Minimalpolynom jedes Polynom, welches x annulliert, also $\mathrm{mipol}_{\mathbb{Q}}(x) | p$. Daraus folgt, dass alle Nullstellen von $\mathrm{mipol}_{\mathbb{Q}}$ ganz sind, denn Sie erfüllen ja p. Daher sind auch die Koeffizienten von $\mathrm{mipol}_{\mathbb{Q}}$ ganz, denn diese sind — für ein normiertes Polynom ! — ganzzahlige algebraische Ausdrücke in den Nullstellen. Diese liegen aber auch in $\mathbb{Q}$ und da $\mathbb{Z}$ ganzabgeschlossen ist (nach dem vorigen Lemma) müssen sie in $\mathbb{Z}$ liegen. □

2.2 Norm und Spur

Wir haben bereits im ersten Kapitel gesehen, dass die Norm praktisch ist, um Fragen der Faktorzerlegung ganzer algebraischer Zahlen zu untersuchen. In diesem Abschnitt werden die Abbildungen "Norm" und "Spur" für eine beliebige Körpererweiterung (aus der Algebra) wiederholt.
Falls $L|K$ eine endliche Körpererweiterung vom Grad n ist, so bedeutet dies insbesondere, dass L ein n-dimensionaler K-Vektorraum ist. Für jedes Element $x \in L$ ist die Multiplikation mit x:

$$\begin{aligned} T_x : L &\to L \\ y &\mapsto x \cdot y \end{aligned}$$

eine K-lineare Abbildung. (Dies folgt sofort aus den Körperaxiomen.) Insbesondere hat die Abbildung T_x eine Determinante und eine Spur, sowie ein charakteristisches Polynom

$$\mathrm{charpol}(T_x) = t^n - \mathrm{tr}(T_x) t^{n-1} + \cdots + (-1)^n \det(T_x). \tag{4}$$

Beachte, dass alle Koeffizienten dieses Polynoms in K liegen.

Definition 2.2.1. *Sei $L|K$ eine Körpererweiterung und $x \in L$. Wir definieren:*

Spur

$\mathrm{tr}_{L|K}(x) := \mathrm{tr}(T_x)$.

Norm

$\mathrm{N}_{L|K} := \det(T_x)$.

Sofort aus der Definition folgt, dass $\mathrm{tr}_{L|K}(x+y) = \mathrm{tr}_{L|K}(x) + \mathrm{tr}_{L|K}(y)$ und $\mathrm{N}_{L|K}(xy) = \mathrm{N}_{L|K}(x) \cdot \mathrm{N}_{L|K}(y)$.

Beispiel 2.2.2. *Wir wollen sehen, dass wir für den Körper $\mathbb{Q}(i)$ die bereits definierten Abbildungen Norm und Spur zurückerhalten. Wenn wir $\mathbb{Q}(i)$ in der üblichen Weise als $\mathbb{Q}$-Vektorraum mit Basis $1, i$ auffassen:*

$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto a + bi,$$

so überlegt man sich leicht, dass die Multiplikation T_x mit einem Element $a + bi \in \mathbb{Q}(i)$ durch die Matrix

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

beschrieben wird. Wir erhalten also wie gehabt:

$$\begin{aligned} \mathrm{tr}_{\mathbb{Q}(i)|\mathbb{Q}}(a+bi) &= 2a \\ \mathrm{N}_{\mathbb{Q}(i)|\mathbb{Q}}(a+bi) &= a^2 + b^2. \end{aligned}$$

Auch die vorige Berechnungsvorschrift durch das Produkt (bzw. die Summe) über Konjugierte verallgemeinert sich:

Lemma 2.2.3. *Falls $L|K$ separabel ist (also z.B. immer in Charakteristik 0), dann gilt*

$$\begin{aligned} \mathrm{charpol}(T_x) &= \prod_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} (t - \sigma(x)) \\ \mathrm{tr}_{L|K}(x) &= \sum_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(x) \\ \mathrm{N}_{L|K}(x) &= \prod_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(x) \end{aligned}$$

Dabei durchlaufen die σ jeweils alle K-Einbettungen $L \hookrightarrow \overline{K}$ in einen fest gewählten algebraischen Abschluss von K. (Falls $L|K$ galoissch ist, kann man äquivalent σ über $\mathrm{Gal}(L|K)$ laufen lassen.)

Beweis. Gleichung (4) impliziert, dass die Formeln für Norm und Spur aus der Formel für das charakteristische Polynom folgen. Um diese zu erhalten, beweisen wir zunächst, dass

$$\boxed{\text{charpol}(T_x) = \text{mipol}(x)^d}$$

Dabei ist $d = [L|K(x)]$. Wir haben die Basis $1, x, x^2, \ldots, x^{n-1}$ von $K(x)$ über K. Wähle nun eine Basis $y_1, \ldots, y_d$ von L über $K(x)$. Wir bekommen die Basis

$$y_1, y_1x, y_1x^2, \ldots, y_1x^{n-1}, \ldots, y_d, y_dx, y_dx^2, \ldots, y_dx^{n-1}$$

von L über K. Die Matrix von T_x hat in dieser Basis Blockgestalt:

$$T_x = \begin{pmatrix} T_{x,K(x)} & & \\ & \ddots & \\ & & T_{x,K(x)} \end{pmatrix}$$

wobei $T_{x,K(x)}$ die Matrix der Multiplikation von x in $K(x)$ ist. Daher

$$\text{charpol}(T_x) = \text{charpol}(T_{x,K(x)})^d.$$

Es gilt aber $\text{charpol}(T_{x,K(x)}) = \text{mipol}(x)$, da beide Polynome normiert sind, x annulieren, und denselben Grad haben. (Explizit ist $T_{x,K(x)}$ offensichtlich durch

$$\begin{pmatrix} 0 & & & & -a_n \\ 1 & 0 & & & -a_{n-1} \\ & 1 & 0 & & -a_{n-2} \\ & & & \ddots & \\ & & & 1 & -a_1 \end{pmatrix}$$

gegeben, wobei die a_i die Koeffizienten des Minimalpolynoms sind.)
Es reicht also zu zeigen, dass

$$\text{charpol}(T_x) = \prod_{\sigma \in \text{Hom}_K(L,\overline{K})} (t - \sigma(x)) = \left(\prod_{\sigma \in \text{Hom}_K(K(x),\overline{K})} (t - \sigma(x)) \right)^d$$

denn $\prod_{\sigma \in \text{Hom}_K(K(x),\overline{K})}(t - \sigma(x)))$ ist das Minimalpolynom von x. (Es ist normiert vom selben Grad, annuliert x und hat wegen Galoisinvarianz Koeffizienten in K.) Nun setzt sich aber jede K-Einbettung $\sigma : K(x) \to \overline{K}$ auf genau d Weisen auf L fort (Galoistheorie!), d.h. der Faktor $(t-\sigma(x))$ kommt genau d Mal im linken Produkt vor. □

Wir benötigen später noch einige Eigenschaften von Norm und Spur

Lemma 2.2.4. *1. Falls $M|L|K$ endliche Körpererweiterungen sind, so gilt*

$$\mathrm{tr}_{L|K}(\mathrm{tr}_{M|L}(x)) = \mathrm{tr}_{M|K}(x) \qquad \mathrm{N}_{L|K}(\mathrm{N}_{M|L}(x)) = \mathrm{N}_{M|K}(x).$$

2. Falls $L|K$ eine Erweiterung von Zahlkörpern ist, so gilt: $x \in \mathcal{O}_L \Rightarrow \mathrm{tr}_{L|K}(x) \in \mathcal{O}_K$ und $\mathrm{N}_{L|K}(x) \in \mathcal{O}_K$.

3. Falls $L|K$ eine Erweiterung von Zahlkörpern ist, so gilt für $x \in \mathcal{O}_L$:

$$x \in \mathcal{O}_L^* \Leftrightarrow N_{L|K}(x) \in \mathcal{O}_K^*.$$

4. Für jede endliche separable Erweiterung $L|K$ ist die symmetrische Bilinearform des K-Vektorraum L **(Spurpaarung)***:*

$$x, y \mapsto \mathrm{tr}_{L|K}(x \cdot y)$$

nicht ausgeartet.

Beweis. 1. wird analog zur Rechnung im Beweis des letzten Lemmas durch geeignete Basiswahl von M über K bewiesen.
2. Falls x ganz ist, so sind auch alle $\sigma(x)$ ganz. (Sie erfüllen dasselbe normierte ganzzahlige Polynom!) Daher sind auch alle Produkte und Summen von diesen Konjugierten ganz, und daher auch $\mathrm{tr}_{L|K}(x)$ und $N_{L|K}(x)$.
3. Falls $x \cdot y = 1$ in $\mathcal{O}_L$ gilt, so gilt $N_{L|K}(x) \cdot N_{L|K}(y) = 1$ in $\mathcal{O}_K$, $N_{L|K}(x)$ ist also auch eine Einheit. Umgekehrt, sei

$$N_{L|K}(x) = \prod_{\sigma} \sigma(x) = \varepsilon$$

eine Einheit in $\mathcal{O}_K$. Wir können o.B.d.A. annehmen, dass $L \subset \overline{K}$ und schreiben:

$$x \cdot \underbrace{(\prod_{\sigma \neq \mathrm{id}} \sigma(x)) \cdot \varepsilon^{-1}}_{y:=} = 1.$$

Das Produkt y in dieser Gleichung ist in K (denn es ist ja einfach $\frac{1}{x}$) und ganz (da alle Faktoren ganz sind), und deshalb in $\mathcal{O}_K$. x ist also eine Einheit.
4. Die Spurpaarung ist, wie wir sehen werden, sehr praktisch, um Aussagen über Ganzheitsringe zu machen. Eine Bilinearform ist genau dann nicht ausgeartet, wenn die Determinante ihrer Matrix (in einer beliebigen Basis)

ungleich 0 ist. Hier ist es geschickt, die Basis $1, \Theta, \Theta^2, \ldots, \Theta^{n-1}$ zu wählen, wobei Θ ein primitives Element von $L|K$ ist (d.h. also $L = K(\Theta)$). Die Matrix der Spurpaarung in dieser Basis ist einfach:

$$A = (a_{ij}) \text{ mit } a_{ij} = \mathrm{tr}_{L|K}(\Theta^i \cdot \Theta^j).$$

Nun gilt aber, wenn $\sigma_1, \ldots, \sigma_n$ die K-Einbettungen von L nach $\overline{K}$ bezeichnet:

$$a_{ij} = \sum_k \sigma_k(\Theta^i \cdot \Theta^j) = \sum_k \sigma_k(\Theta)^i \cdot \sigma_k(\Theta)^j.$$

Falls wir eine Matrix $B = (b_{ij})$ mit $b_{ij} := \sigma_i(\Theta)^j$ definieren, so bedeutet dies gerade:

$$A = {}^tB \cdot B.$$

Inbesondere ist $\det(A) = \det(B)^2$. Nun gilt:

$$\det(B) = \det \begin{pmatrix} 1 & \Theta_1 & \Theta_1^2 & \ldots, \Theta_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \Theta_n & \Theta_n^2 & \ldots, \Theta_n^{n-1} \end{pmatrix}$$

für $\Theta_i := \sigma_i(\Theta)$. Dies ist die sogenannte VANDERMONDE Determinante und (Übung!) gleich

$$\prod_{i<j} (\Theta_i - \Theta_j).$$

Dies ist nicht null, da die $\Theta_i = \sigma_i(\Theta)$ alle verschieden sind. Wären etwa $\sigma_i(\Theta) = \sigma_j(\Theta)$ so würde schon $\sigma_i = \sigma_j$ folgen, da Θ die Körpererweiterung erzeugt. □

2.3 Ganzheitsbasen und Diskriminante

Wir wissen noch nicht, dass $\mathcal{O}_K$ tatsächlich ein freier $\mathbb{Z}$-Modul (von endlichem Rang) ist, also $\mathcal{O}_K \cong \mathbb{Z}^n$. Dies ist gleichbedeutend mit der Existenz einer endlichen $\mathbb{Z}$-Basis von $\mathcal{O}_K$, die in diesem Fall auch **Ganzheitsbasis** genannt wird.
Falls wir für einen Augenblick annehmen, dass $\mathcal{O}_K \cong \mathbb{Z}^n$ mit zugehöriger Ganzheitsbasis $x_1, \ldots, x_n$, so kann nur $n = [K|\mathbb{Q}]$ sein. Denn wäre $n > [K|\mathbb{Q}]$, so müssten $x_1, \ldots, x_n$ linear abhängig über $\mathbb{Q}$ sein. Multiplikation einer solchen linearen Abhängigkeit mit dem Hauptnenner der Koeffizienten ergibt jedoch eine lineare Abhängigkeit schon über $\mathbb{Z}$. Ausserdem existiert für jedes $x \in K$ ein $n \in \mathbb{Z}$ so dass $n \cdot x$ ganz ist, also in $\mathcal{O}_K$ liegt. Daher muss $x_1, \ldots, x_n$ ein Erzeugendensystem auch von K über $\mathbb{Q}$ sein. Daher kann n nicht kleiner als $[K|\mathbb{Q}]$ sein.

Definition 2.3.1. *Sei $x_1, \ldots, x_n$ eine Basis von K über $\mathbb{Q}$ mit $x_i \in \mathcal{O}_K$ (z.B. eine Ganzheitsbasis) Dann heisst die Determinante der Matrix der Spurpaarung in dieser Basis*

$$d(x_1, \ldots, x_n) = \det(\mathrm{tr}_{K|\mathbb{Q}}(x_i \cdot x_j)) \in \mathbb{Z}$$

die **Diskriminante** *von $x_1, \ldots, x_n$. Ist dies eine Ganzheitsbasis, so sprechen wir auch von der* **Diskriminante von** *K bzw. von $\mathcal{O}_K$.*

Beachte: Die Diskriminante hängt nur von dem $\mathbb{Z}$-Modul $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$ ab (und nicht von der Wahl der Basis). Insbedondere ergibt es Sinn, von *der* Diskriminante von $\mathcal{O}_K$ oder K zu sprechen. Grund: Falls zwei Basen $x_1, \ldots, x_n$ und $x_1', \ldots, x_n'$ gegeben sind und A und A' die Matrizen der Spurpaarung in diesen Basen, so gilt:

$$A' = {}^tSAS \quad \text{also} \quad \det(A') = \det(A)\det(S)^2,$$

wobei S die Basiswechselmatrix ist. Diese und ihr Inverses S^{-1} haben jedoch ganzzahlige Einträge, daher muss $\det(S) = \pm 1$ sein. Es folgt also

$$\det(A) = \det(A').$$

Lemma 2.3.2. *Sei $L|K$ ein Erweiterung von Zahlkörpern, und $x_1, \ldots, x_n$ eine Basis von $L|K$ mit $x_i \in \mathcal{O}_L$. (Solch eine existiert immer, da man mit geeigneten $n \in \mathbb{Z}$ multiplizieren darf.) Sei*

$$d = d(x_1, \ldots, x_n) = \det(\mathrm{tr}_{L|K}(x_i \cdot x_j)) \in \mathcal{O}_K$$

die $\mathcal{O}_K$-Diskriminante dieser Basis. Dann gilt:

$$d \cdot \mathcal{O}_L \subset \mathcal{O}_K x_1 + \cdots + \mathcal{O}_K x_n.$$

Hieraus folgt sofort:

Korollar 2.3.3. *Sei K ein Zahlkörper vom Grad n über $\mathbb{Q}$. Dann gilt:*

$$\mathcal{O}_K \cong \mathbb{Z}^n,$$

d.h. $\mathcal{O}_K$ besitzt eine Ganzheitsbasis.

Beweis. Aus dem Lemma folgt:

$$\mathcal{O}_L \subset \mathbb{Z}\frac{x_1}{d} + \cdots + \mathbb{Z}\frac{x_n}{d}.$$

d.h. $\mathcal{O}_L$ ist ein Untermodul eines freien $\mathbb{Z}$-Modul von endlichem Rang. Er muss daher auch frei von endlichem Rang sein (elementares Resultat aus der Algebra, siehe weiter unten die Diskussion über Moduln über Hauptidealringen), d.h. $\mathcal{O}_K \cong \mathbb{Z}^m$. Wir haben bereits gesehen, dass dann notwendigerweise $m = n$ sein muss. □

Beweis von Lemma 2.3.2. Drücke ein beliebiges $x \in \mathcal{O}_L$ in der gewählten Basis aus:

$$x = \sum_i \alpha_i x_i.$$

mit $\alpha_i \in K$. Wir müssen sehen, dass $d\alpha_i$ für alle i ganz ist. Wir wenden nun einen Trick an und multiplizieren die Gleichung mit x_j und nehmen die Spur:

$$\mathrm{tr}_{L|K}(x \cdot x_j) = \sum_i \alpha_i \,\mathrm{tr}_{L|K}(x_i \cdot x_j).$$

Beachte, dass man die α_i aus der Spur herausziehen kann, da sie in K liegen. Mit anderen Worten:

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \mathrm{tr}_{L|K}(x \cdot x_1) \\ \vdots \\ \mathrm{tr}_{L|K}(x \cdot x_n) \end{pmatrix},$$

wobei $A = (\mathrm{tr}_{L|K}(x_i \cdot x_j))$ die Matrix der Spurpaarung ist. Daraus folgt durch Multiplikation mit der adjungierten Matrix A^*:

$$d \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = A^* \begin{pmatrix} \mathrm{tr}_{L|K}(x \cdot x_1) \\ \vdots \\ \mathrm{tr}_{L|K}(x \cdot x_n) \end{pmatrix},$$

für $d = \det(A) = d(x_1, \ldots, x_n)$. Die rechte Seite dieser Gleichung ist aber eine Matrix mit ganzen Einträgen, alle $d\alpha_i$ sind also in der Tat ganz. □

Was gilt in der relativen Situation, für eine Erweiterung von Zahlkörpern $L|K$ vom Grad n?

$$\begin{array}{ccc} \mathcal{O}_L & \subset & L \\ \cup & & \cup \\ \mathcal{O}_K & \subset & K \end{array}$$

Folgt auch hier, dass $\mathcal{O}_L \cong (\mathcal{O}_K)^n$? Dies gilt genauso wie für $K = \mathbb{Q}, \mathcal{O}_K = \mathbb{Z}$, wenn $\mathcal{O}_K$ ein Hauptidealring ist. Um dies zu sehen, brauchen wir aus der Algebra einige Eigenschaften endlich erzeugter Moduln über Hauptidealringen:

Satz 2.3.4. *Sei R ein Hauptidealring.*

1. *Untermoduln endlich erzeugter R-Moduln sind endlich erzeugt (dies gilt allgemeiner für Moduln über Noetherschen Ringen).*

2. *Sei M ein endlich erzeugter R-Modul. Dann gilt:*

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_n) \oplus R^n.$$

   für gewisse $a_1, \ldots, a_n \in R \setminus \{0\}$. Die Moduln R und $R/(a_i)$ heissen (in Analogie zu Z und $\mathbb{Z}/N\mathbb{Z}$) **zyklische** *Moduln. n heisst der* **Rang** *von M und ist eindeutig bestimmt. Falls $M \cong R^n$ so heisst M* **frei**.

3. *Untermoduln freier endlich erzeugter R-Moduln sind frei.*

Mit Hilfe von Aussage 3. dieses Satzes ergibt sich aus Lemma 2.3.2 (exakt genauso wie Korollar 2.3.3):

Korollar 2.3.5. *Sei $L|K$ eine Erweiterung von Zahlkörpern vom Grad n, so dass $\mathcal{O}_K$ ein Hauptidealring ist. Dann gilt:*

$$\mathcal{O}_L \cong (\mathcal{O}_K)^n,$$

d.h. $\mathcal{O}_L$ besitzt eine $\mathcal{O}_K$-Ganzheitsbasis.

2.4 Eindeutige Faktorisierung in Primideale

Wir haben bereits gesehen, dass z.B. im Ring $\mathbb{Z}[\sqrt{-5}]$ die eindeutige Primfaktorzerlegung nicht mehr gilt:

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

sind zwei wesentlich verschiedene Zerlegungen von 6 in irreduzible Elemente. Wenn es eine Verfeinerung wie in 1.5 anvisiert als Idealzerlegung

$$(6) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_4$$

geben soll, dann muss also jedes $\mathfrak{p}_i$ zwei der irreduziblen Elemente in (5) teilen. Das heisst z.B. $2 \in \mathfrak{p}_1$ und $(1 + \sqrt{-5}) \in \mathfrak{p}_1$. Das kleinste solche Ideal ist das von diesen beiden Elementen erzeugte Ideal:

$$\mathfrak{p}_1 := (2, 1 + \sqrt{-5}).$$

Dies kann kein Hauptideal sein, denn ein Erzeuger von $\mathfrak{p}_1$ wäre ein Teiler der beiden irreduziblen Elemente 2 und $(1 + \sqrt{-5})$. Es würde folgen, dass diese bis auf Einheit übereinstimmen, was wir bereits ausgeschlossen haben. Wir

sehen erneut, wie die Nichteindeutigkeit der Zerlegung (5) mit der Existenz von Nichthauptidealen verzahnt ist. Wenn wir genauso für alle anderen Paare definieren:

$$\begin{aligned}\mathfrak{p}_2 &:= (2, 1-\sqrt{-5}) = \mathfrak{p}_1,\\ \mathfrak{p}_3 &:= (3, 1+\sqrt{-5}),\\ \mathfrak{p}_4 &:= (3, 1-\sqrt{-5}).\end{aligned}$$

so erhalten wir aus demselben Grund stets Nichthauptideale. Beachte: Hier gilt zufällig $(2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5})$, denn $1+\sqrt{-5} = 2-(1-\sqrt{-5})$. Tatsächlich löst diese recht naive Konstruktion das Problem! Denn wir haben

$$\begin{aligned}(2, 1+\sqrt{-5})^2 &= (4, 2+2\sqrt{-5}, -4+2\sqrt{-5}) = \underline{(2)}\\ (2, 1+\sqrt{-5})\cdot(3, 1+\sqrt{-5}) &= (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5})\\ &= \underline{(1+\sqrt{-5})}\\ (2, 1-\sqrt{-5})\cdot(3, 1-\sqrt{-5}) &= (6, 2-2\sqrt{-5}, 3-3\sqrt{-5}, -4-2\sqrt{-5})\\ &= \underline{(1-\sqrt{-5})}\\ (3, 1+\sqrt{-5})\cdot(3, 1-\sqrt{-5}) &= (9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6) = \underline{(3)}\end{aligned}$$

Die Uneindeutigkeit der Faktorzerleugung löst sich also in die folgende Eindeutigkeit der Idealzerlegung auf:

$$(6) = \underbrace{\mathfrak{p}_1\cdot\mathfrak{p}_2}_{(2)}\cdot\underbrace{\mathfrak{p}_3\cdot\mathfrak{p}_4}_{(3)} = \underbrace{\mathfrak{p}_1\cdot\mathfrak{p}_3}_{(1+\sqrt{-5})}\cdot\underbrace{\mathfrak{p}_2\cdot\mathfrak{p}_4}_{(1-\sqrt{-5})}.$$

Die Ideale $\mathfrak{p}_i$ sind nicht weiter als Produkt zerlegbar und auch *prim*, d.h. aus $xy \in \mathfrak{p}_i$ folgt $x \in \mathfrak{p}_i$ oder $y \in \mathfrak{p}_i$.
Wir beginnen mit dem folgenden

Lemma 2.4.1. *Sei K ein Zahlkörper vom Grad n. Dann ist jedes Ideal $\mathfrak{p} \subset \mathcal{O}_K$ ungleich (0) ebenfalls ein freier $\mathbb{Z}$-Modul vom Rang n:*

$$\mathfrak{p} \cong \mathbb{Z}^n$$

Beweis. Als Untermodul des freien Moduls $\mathcal{O}_K$ von Rang n ist zumindest $\mathfrak{p} \cong \mathbb{Z}^m$ mit $m \leq n$. Sei $x \in \mathfrak{p}$ ungleich 0. Dann haben wir

$$x\mathcal{O}_K \subseteq \mathfrak{p} \subseteq \mathcal{O}_K.$$

Der Rang kann also auch nicht kleiner sein als n. □

Im Fall eines imaginär-quadratischen Körpers K kann man diese Gitter schön visualisieren (siehe Abbildungen 5–4). Falls $\mathcal{O}_K$ ein Hauptidealring ist, sich also alle Ideale bis auf Multiplikation mit einer komplexen Zahl unterscheiden, sehen die entsprechenden Gitter alle gleich aus. Sie gehen durch eine Drehsteckung auseinander hervor! Ist $\mathcal{O}_K$ kein Hauptidealring, so gibt es unterschiedliche Formen. Wir werden später die sogenannte Idealklassengruppe einführen. Zu jeder dieser unterschiedlichen Formen gehört dann genau eine Idealklasse.

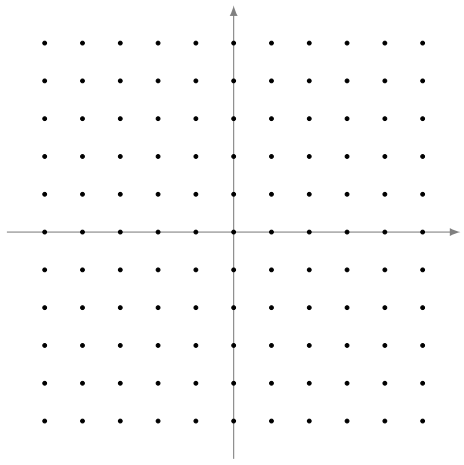


Abbildung 1: $\mathbb{Z}[i]$

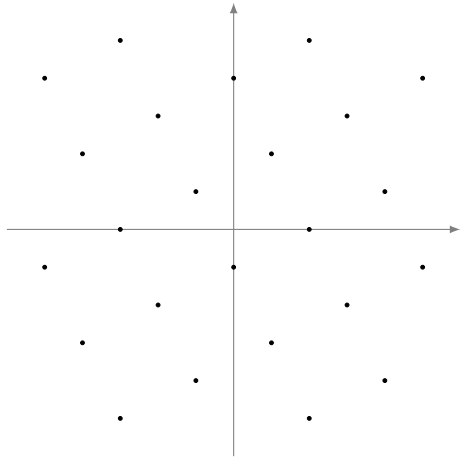


Abbildung 2: Das Ideal $(2+i) \subset \mathbb{Z}[i]$

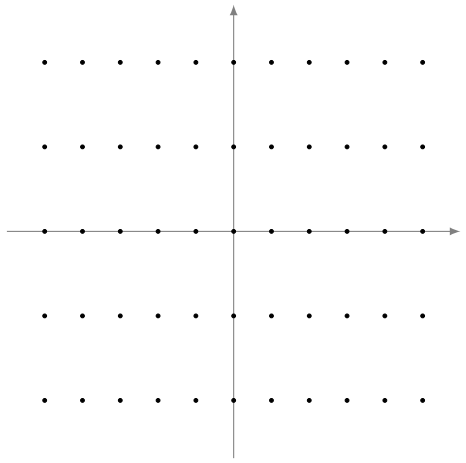


Abbildung 3: $\mathbb{Z}[\sqrt{-5}]$

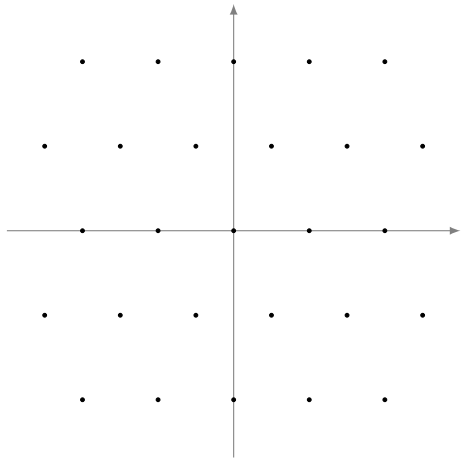


Abbildung 4: Das Ideal $(2, 1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$

Wir möchten beweisen, dass eine eindeutige Primfaktorzerlegung für Ideale in den Ringen $\mathcal{O}_K$ immer existiert. Für Hauptideale haben wir die offensichtliche Implikation

$$a|b \quad \Leftrightarrow \quad (b) \subset (a).$$

Falls wir für Ideale analog definieren: $\mathfrak{a}|\mathfrak{b}$, falls ein Ideal $\mathfrak{c}$ existiert, so dass $\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c}$, so ist nur noch

$$\mathfrak{a}|\mathfrak{b} \quad \Rightarrow \quad \mathfrak{b} \subseteq \mathfrak{a}$$

offensichtlich. Wir werden sehen, dass in unseren Ringen $\mathcal{O}_K$ auch die Umkehrung gilt. Auf jeden Fall wird ein Ideal $\mathfrak{p}$ in diesem Sinne unzerlegbar sein, falls es kein grösseres (echtes) Ideal gibt, dass $\mathfrak{p}$ umfasst. Mit anderen Worten aus $\mathfrak{p} \subseteq \mathfrak{a} \subsetneq \mathcal{O}_K$ folgt, dass $\mathfrak{p} = \mathfrak{a}$. Ideale mit dieser Eigenschaft heissen **maximal**. Auch die Eigenschaft prim zu sein hat eine einfache Entsprechung für Ideale. Ein echtes Ideal $\mathfrak{p}$ heisst **prim** wenn aus $xy \in \mathfrak{p}$ folgt, dass entweder $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. Die Definition ist so gemacht, dass ein Element x genau dann prim ist, wenn das Hauptideal (x) prim ist. Es gibt folgende einfache Implikation:

Lemma 2.4.2. *Für ein Ideal $\mathfrak{a}$ eines Ringes R gilt:*

$$\boxed{\mathfrak{a} \text{ maximal } \Rightarrow \mathfrak{a} \text{ prim.}}$$

Beweis. Ein Ideal $\mathfrak{a}$ ist genau dann prim, wenn $R/\mathfrak{a}$ nullteilerfrei ist. Es ist maximal genau dann, wenn $R/\mathfrak{a}$ ein Körper ist[6]. Da ein Körper nullteilerfrei ist, folgt die Aussage. □

Gilt auch die Umkehrung? In einem nullteilerfreien Ring R ist das Ideal (0), welches nur aus der 0 besteht, offensichtlich immer prim. Es ist genau dann maximal wenn R ein Körper ist. In unseren Ringen $\mathcal{O}_K$ kann daher die Umkehrung nicht gelten. Es zeigt sich aber, dass (0) die einzige Ausnahme ist:

Lemma 2.4.3. *Sei K ein Zahlkörper und $\mathcal{O}_K$ der Ring der ganzen Zahlen. Dann ist in $\mathcal{O}_K$ jedes Primideal ungleich* (0) *maximal.*

Beweis. Sei $\mathfrak{a}$ ein Primideal ungleich (0). Dann folgt aus Lemma 2.4.1, dass $\mathcal{O}_K/\mathfrak{a}$ ein endlicher Ring ist. Für einen endlichen Ring R gilt nun auch die Implikation: "R nullteilerfrei $\Rightarrow$ R Körper" [7]. □

Ein Primideal $\mathfrak{p}$ hat auch die folgende Eigenschaft:

$$\mathfrak{ab} \subseteq \mathfrak{p} \;\Rightarrow\; \mathfrak{a} \subseteq \mathfrak{p} \text{ oder } \mathfrak{b} \subseteq \mathfrak{p} \tag{6}$$

[6] Dies folgt zum Beispiel aus der einfachen Tatsache, dass es für jedes Ideal $\mathfrak{a}$ eine Bijektion:

$$\{ \text{ Ideale von } R/\mathfrak{a} \} \cong \{ \text{ Ideale von } R \text{ welche } \mathfrak{a} \text{ enthalten } \}$$

gibt.

[7] Beweis: Sei R nullteilerfrei und $x \in R \setminus \{0\}$. Dann ist die Multiplikation mit x als Abbildung $R \to R$ injektiv (wegen $xy = xy' \Rightarrow y = y'$ in nullteilerfreien Ringen). Da aber R endlich viele Elemente hat, ist jede injektive Selbstabbildung auch surjektiv, und daher hat x ein Inverses. R ist also ein Körper.

Falls $\mathfrak{a}$ und $\mathfrak{b}$ Hauptideale sind, übersetzt sich dies sofort in die Definition. Für allgemeine Ideale zeigt man die äquivalente Aussage:

$$\mathfrak{a} \not\subseteq \mathfrak{p} \text{ und } \mathfrak{b} \not\subseteq \mathfrak{p} \;\Rightarrow\; \mathfrak{ab} \not\subseteq \mathfrak{p}.$$

Falls $x \in \mathfrak{a}$ und $\notin \mathfrak{p}$, und $y \in \mathfrak{b}$ und $\notin \mathfrak{p}$, dann ist $x \cdot y \in \mathfrak{ab}$. Das Produkt $x \cdot y$ kann aber nicht in $\mathfrak{p}$ liegen, da x und y nicht in $\mathfrak{p}$ liegen (Primeigenschaft). Für den Beweis der eindeutigen Zerlegung in Ideale werden wir nur die folgenden Eigenschaften von $\mathcal{O}_K$ benötigen. Sie sind sehr grundlegend, deshalb definieren wir:

Definition 2.4.4. *Ein Ring R, welcher die folgenden Eigenschaften besitzt, heisst* **Dedekindring**.

1. *R ist nullteilerfrei und Noethersch,*
2. *R ist ganzabgeschlossen,*
3. *In R ist jedes Primideal ungleich (0) maximal.*

Wir haben für $\mathcal{O}_K$ diese Eigenschaften schon verifiziert, ausser die Eigenschaft Noethersch zu sein, die nicht explizit erwähnt wurde. Aber wir haben schon gesehen, dass jedes Ideal $\mathfrak{a}$ ein endlich erzeugter $\mathbb{Z}$-Modul ist. Es ist daher insbesondere als $\mathcal{O}_K$-Modul (also als Ideal) endlich erzeugt. $\mathcal{O}_K$ ist also Noethersch. Wir arbeiten ab jetzt mit einem beliebigen Dedekindring R und nennen $K := \mathrm{Quot}(R)$ den Quotientenkörper.
Ziel des Abschnittes ist der

Satz 2.4.5. *In einem Dedekindring R gibt es für jedes Ideal $\mathfrak{a}$ ungleich (0) eine bis auf Reihenfolge eindeutige Faktorzerlegung*

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

in Primideale[8]*.*

Für den Beweis benötigen wir einige Vorbereitungen. Zunächst ist es praktisch, auch Elementen in K^*, also solchen, die nicht unbedingt ganz sind, Ideale zuordnen zu können. Dazu definieren wir

Definition 2.4.6. *Ein endlich erzeugter R-Untermodul von K heisst ein* **gebrochenes Ideal**.

[8] Hier ist auch $n = 0$ zugelassen und tritt für $\mathfrak{a} = R$ auf.

Z.B. definiert jedes Element $x \in K$ ein gebrochenes Ideal $(x) := R \cdot x \subset K$. Diese heissen gebrochene Hauptideale. Jedes gewöhnliche Ideal ist insbesondere auch ein gebrochenes Ideal.
Wir beweisen nun zunächst, dass jedes Ideal ein Produkt von Primidealen enthält:

Lemma 2.4.7. *Sei R ein Dedekindring und $\mathfrak{a}$ ein Ideal ungleich (0). Dann existieren endlich viele Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ungleich (0) so, dass*

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

Beweis. Nimm an, es gibt ein Ideal, dass diese Eigenschaft nicht hat. Da R Noethersch ist, gibt es dann in der Menge aller Ideale, die *nicht* diese Eigenschaft haben, ein maximales Element $\mathfrak{a}$. $\mathfrak{a}$ kann selber nicht prim sein, also gibt es $x, y \in R$ mit $xy \in \mathfrak{a}$ aber $x \notin \mathfrak{a}$ und $y \notin \mathfrak{a}$. Die Ideale $\mathfrak{a} + (x)$ und $\mathfrak{a} + (y)$ sind also echt grösser als $\mathfrak{a}$ und haben daher nach Konstruktion die gewünschte Eigenschaft. D.h. es existieren Primideale $\mathfrak{p}_i$ mit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a} + (x) \qquad \mathfrak{p}_{n+1} \cdots \mathfrak{p}_m \subseteq \mathfrak{a} + (y)$$

Durch Multiplikation ergibt sich:

$$\mathfrak{p}_1 \cdots \mathfrak{p}_m \subseteq (\mathfrak{a} + (x)) \cdot (\mathfrak{a} + (y)) \subseteq \mathfrak{a} + (xy) = \mathfrak{a}.$$

Widerspruch. □

Wir nennen ein gebrochenes Ideal $\mathfrak{a}$ **invertierbar**, falls ein gebrochenes Ideal $\mathfrak{b}$ existiert mit

$$\mathfrak{a} \cdot \mathfrak{b} = R.$$

Notwendigerweise ist in diesem Fall $\mathfrak{b} = \mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq R\}$.

Lemma 2.4.8. *Sei R ein Dedekindring. Jedes Primideal $\mathfrak{p}$ ungleich (0) ist invertierbar.*

Beweis. Sei $\mathfrak{p}^{-1}$ so wie oben definiert. Alle Elemente im Produkt $\mathfrak{p} \cdot \mathfrak{p}^{-1}$ sind nach Definition von $\mathfrak{p}^{-1}$ ganz. Ausserdem ist $1 \in \mathfrak{p}^{-1}$, also ist $\mathfrak{p}$ im Produkt enthalten. Mit anderen Worten:

$$\mathfrak{p} \subseteq \mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq R.$$

Da $\mathfrak{p}$ maximal ist, müssen wir nur den Fall

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

ausschliessen. In diesem Fall definiert jedes $x \in \mathfrak{p}^{-1}$ aber einen Endomorphismus des endlich erzeugten R-Moduls $\mathfrak{p}$. Wie im Beweis von Satz 2.1.5 erfüllt es daher ein normiertes Polynom mit Koeffizienten in R (das charakteristische Polynom). Da R als Dedekindring ganzabgeschlossen ist, folgt $x \in R$. Wir bekommen also $\mathfrak{p}^{-1} = R$. Wir müssen zeigen, dass dies nicht der Fall sein kann. Sei $a \in \mathfrak{p} \setminus \{0\}$. Nach Lemma 2.4.7 gibt es Primideale $\mathfrak{p}_i$ so dass

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq (a) \subseteq \mathfrak{p}$$

Wir können annehmen, dass n minimal mit dieser Eigenschaft ist. Aufgrund von Eigenschaft (6) von Primidealen müsste dann $\mathfrak{p}$ eines der $\mathfrak{p}_i$ enthalten. Wegen der Maximalität von Primidealen (R ist Dedekindring) gilt also $\mathfrak{p}_i = \mathfrak{p}$, o.B.d.A. $i = 1$. Da $\mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_n \not\subset (a)$ existiert ein $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$, welches nicht in (a) liegt. Daher ist das Element $a^{-1}b$ nicht ganz. Es gilt aber

$$a^{-1}b\,\mathfrak{p} \subseteq a^{-1}\,\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq a^{-1}(a) = R,$$

also $a^{-1}b \in \mathfrak{p}^{-1}$. Widerspruch. □

Beweis von Satz 2.4.5. Wir zeigen zunächst, dass jedes Ideal eine Zerlegung in Primideale besitzt. Jedes Ideal ungleich (0) enthält nach Lemma 2.4.7 ein Produkt von Primidealen ungleich (0). Wir gehen durch Induktion nach der Anzahl dieser Primideale vor. Wenn $\mathfrak{a}$ ein leeres Produkt von Primidealen enthält, so bedeutet dies gerade $\mathfrak{a} = R$. Ansonsten sei

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}$$

und $\mathfrak{a}$ ein echtes Ideal. Es ist daher einem maximalen Ideal enthalten:

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

Wie im letzten Lemma folgt o.B.d.A. $\mathfrak{p}_1 = \mathfrak{p}$. Multiplikation mit $\mathfrak{p}^{-1}$ ergibt (da Primideale invertierbar sind):

$$\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}^{-1}\mathfrak{a} \subseteq R.$$

Nun ist für das Ideal $\mathfrak{p}^{-1}\mathfrak{a}$ ein kleineres n erreicht, d.h. nach Induktionsvoraussetzung:

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

für irgendwelche Primideale $\mathfrak{q}_i$. Dann ist aber nach Multiplikation mit $\mathfrak{p}$ (da Primideale invertierbar sind):

$$\mathfrak{a} = \mathfrak{p} \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_m.$$

Wir müssen noch die Eindeutigkeit zeigen. Seien

$$\mathfrak{p}_1 \dots \mathfrak{p}_n = \mathfrak{a} = \mathfrak{q}_1 \dots \mathfrak{q}_m$$

zwei verschiedene Faktorzerlegungen von $\mathfrak{a}$. Da die linke Seite in $\mathfrak{p}_1$ enthalten ist muss nach der Eigenschaft (6) der Primideale auch eines der $\mathfrak{q}_i$ in $\mathfrak{p}_1$ enthalten sein. Da Primideale ungleich (0) aber maximal sind (R ist Dedekindring) folgt: $\mathfrak{q}_i = \mathfrak{p}_1$. Durch Umnummerieren können wir $i = 1$ erreichen. Durch Multiplikation mit $\mathfrak{p}_1$ folgt (da Primideale invertierbar sind):

$$\mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{q}_2 \dots \mathfrak{q}_m.$$

Durch Induktion folgt die Eindeutigkeit. □

2.4.9. Noch einige Folgerungen für einen Dedekindring R:

1. Alle gebrochenen Ideale ungleich (0) sind invertierbar.
2. Es gilt tatsächlich für ganze Ideale $\mathfrak{a}, \mathfrak{b}$ die Aussage

$$\mathfrak{a} | \mathfrak{b} \ \Leftrightarrow \mathfrak{b} \subset \mathfrak{a}.$$

3. Die gebrochenen Ideale ungleich (0) bilden eine Gruppe bzgl. Multiplikation. Es ist eine freie Abelsche Gruppe mit Basis $\cong$ {Primideale von R}.

Beweis. 1. Für ganze Ideale folgt dies sofort aus der Existenz der Faktorisierung in Primideale und der Tatsache, dass Primideale invertierbar sind. Ein gebrochenes Ideal ist nach Voraussetzung endlich erzeugt, d.h. $\mathfrak{a} = (a_1, \dots, a_n)$ mit $a_i \in \mathrm{Quot}(R)$. Für jedes a_i existiert offensichtlich ein $n \in R$, so dass $n \cdot a_i \in R$. D.h. es existiert auch ein $n \in R$ so dass

$$\mathfrak{a} = n^{-1}\widetilde{\mathfrak{a}}$$

mit $\widetilde{\mathfrak{a}}$ ganz. Daher ist auch $\mathfrak{a}$ invertierbar.
2. Die Richtung $\Rightarrow$ ist klar. Falls umgekehrt $\mathfrak{b} \subseteq \mathfrak{a}$ folgt wegen 1.

$$\mathfrak{a}^{-1}\mathfrak{b} \subseteq R$$

und

$$\mathfrak{a} \cdot (\mathfrak{a}^{-1}\mathfrak{b}) = \mathfrak{b}.$$

3. Alle Gruppenaxiome ausser der Existenz des Inversen sind klar. Dies ist aber gerade Aussage 1. Dass es sich um eine freie Abelsche Gruppe mit Basis $\cong$ {Primideale von R} handelt, ist eine Umformulierung der eindeutigen Faktorzerlegung in Primideale. □

Definition 2.4.10. *Die Gruppe der gebrochenen Ideale eines Zahlkörpers K wird mit J_K bezeichnet. Die Gruppe der gebrochenen Hauptideale darin mit P_K. Die Faktorgruppe*

$$\mathrm{Cl}_K := J_K/P_K$$

heisst die **Idealklassengruppe** *des Körpers K.*

Die Idealklassengruppe ist die wichtigste Invariante der algebraischen Zahlentheorie. Unser nächstes Ziel wird sein, zu beweisen, dass sie immer endlich ist. (Dies gilt nicht für beliebige Dedekindringe.) Die Anzahl der Elemente wird die Klassenzahl des Körpers K genannt. Beachte: Die Gruppe Cl_K ist genau dann trivial (also Klassenzahl 1) wenn jedes Ideal in $\mathcal{O}_K$ ein Hauptideal ist, also eindeutige Primfaktorzerlegung für Elemente (statt nur für Ideale) gilt. Überlegen Sie sich, dass letztere in diesem Fall trivialerweise aus der Faktorzerlegung in Primideale folgt! Die Gruppe Cl_K misst also die Abweichung von der eindeutige Primfaktorzerlegung für Elemente.
Man kann dies wie folgt ausdrücken: Es gibt eine exakte Sequenz von Gruppenhomomorphismen

$$1 \to \mathcal{O}_K^* \to K^* \to J_K \to \mathrm{Cl}_K \to 1.$$

wobei der mittlere Homomorphismus nichts anderes ist, als die Abbildung, die einem Element von K das davon erzeugte gebrochene Hauptideal zuordnet:

$$\begin{array}{rcl} K^* & \to & J_K \\ x & \mapsto & (x). \end{array}$$

Erinnere aus der Algebra, dass die Aussage exakte Sequenz zu sein (hier) bedeutet, dass diese Abbildung den Kern $\mathcal{O}_K^*$ (also die Gruppe der Einheiten von $\mathcal{O}_K$) hat, und dass ihr Kokern (also die Faktorgruppe: Zielgruppe modulo Bild) isomorph zu Cl_K ist. Letzteres ist nach Definition so, und ersteres ist klar.

2.5 Primideale in Ganzheitsringen

In diesem Abschnitt werden wir explizit bestimmen, welche Primideale die Ringe der ganzen Zahlen $\mathcal{O}_K$ in Zahlkörpern besitzen. Eine Primzahl p erzeugt ein Primideal (p) von $\mathbb{Z}$. Im allgemeinen wird aber das Ideal $p\mathcal{O}_K$ nicht mehr prim sein (siehe auch Beispiel 1.2.1). Wir bekommen also wegen der eindeutigen Primfaktorzerlgung für Ideale

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k},$$

wobei wir immer annehmen, dass die Primideale $\mathfrak{P}_i$ verschieden sein. Wir werden in diesem Abschnitt

1. für alle p (bis auf endlich viele Ausnahmen) ein explizites Verfahren angeben, um die $\mathfrak{P}_i$, sowie die Exponenten n_i, zu bestimmen;

2. die Formel
$$[L|\mathbb{Q}] = \sum_i n_i \cdot f_i$$
beweisen, wobei f_i der Körpergrad von $\mathcal{O}_K/\mathfrak{P}_i$ über $\mathbb{F}_p$ ist, der sogenannte **Trägheitsgrad**. (Beachte: Aus Lemma 2.4.1 folgt, dass dies ein endlicher Körper ist, und f_i lässt sich daher auch an seiner Anzahl der Elemente, nämlich p^{f_i} ablesen.)

2.5.1. Obige Fragestellung ergibt auch Sinn, wenn wir eine Körpererweiterung $L|K$ von Zahlkörpern haben. Sei $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ und sei
$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}$$
seine Faktorzerlegung in Primideale von $\mathcal{O}_L$. Wir nennen wieder den Körpergrad $f_i := [\mathcal{O}_L/\mathfrak{P}_i|\mathcal{O}_K/\mathfrak{p}]$ den **Trägheitsgrad** von $\mathfrak{P}_i$ über $\mathfrak{p}$.

Definition 2.5.2. *Das Ideal $\mathfrak{p}$ heisst*

unverzweigt in L
falls alle $e_i = 1$;

träge in L
falls es unverzweigt ist und $k = 1$, also falls $\mathfrak{p}\mathcal{O}_L$ wieder ein Primideal ist;

vollzerlegt in L
falls $k = n$.

Das adjektiv "träge" bezieht sich also auf die Zerlegungsfreudigkeit. Es erklärt sich auch der Name Trägheitsgrad f_i. Dieser ist nach der Formel oben, die wir beweisen wollen, genau dann gleich n (und maximal möglich) wenn $\mathfrak{p}$ träge in L ist.
Zunächst eine Aussage, die Sie von den ganzen Zahlen schon kennen:

Satz 2.5.3 (Chinesischer Restsatz)**.** *Sei R ein Ring und $\mathfrak{a} = \mathfrak{b}_1 \cdots \mathfrak{b}_k$ Ideale mit $\mathfrak{b}_i + \mathfrak{b}_j = R$ für $i \neq j$. Dann gibt es einen Ringisomorphismus:*
$$R/\mathfrak{a} \cong R/\mathfrak{b}_1 \oplus \cdots \oplus R/\mathfrak{b}_k.$$

Beweis. Im folgenden sehen Sie einen modernen Beweis. Die Aussage ist aber elementar und Sie sollten sich dies als Übung genau überlegen. Es genügt sicher, die Aussage für zwei Ideale zu beweisen. Wir haben dann eine *Injektion* zwischen zwei exakten Sequenzen (von R-Moduln)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{b}_1 \cap \mathfrak{b}_2 & \longrightarrow & \mathfrak{b}_1 \oplus \mathfrak{b}_2 & \longrightarrow & \mathfrak{b}_1 + \mathfrak{b}_2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & R & \xrightarrow{\begin{pmatrix} 1 \\ -1 \end{pmatrix}} & R \oplus R & \xrightarrow{\begin{pmatrix} 1 & 1 \end{pmatrix}} & R & \longrightarrow & 0 \end{array}$$

Es folgt, dass auch der Quotient dieser exakten Sequenzen eine exakte Sequenz ist:

$$0 \longrightarrow R/(\mathfrak{b}_1 \cap \mathfrak{b}_2) \longrightarrow R/\mathfrak{b}_1 \oplus R/\mathfrak{b}_2 \longrightarrow R/(\mathfrak{b}_1 + \mathfrak{b}_2) \longrightarrow 0$$

Nun ist nach Voraussetzung $\mathfrak{b}_1 + \mathfrak{b}_2 = R$, daher bekommen wir einen Isomorphismus

$$R/(\mathfrak{b}_1 \cap \mathfrak{b}_2) \cong R/\mathfrak{b}_1 \oplus R/\mathfrak{b}_2.$$

Falls $\mathfrak{b}_1 + \mathfrak{b}_2 = R$ ist aber $\mathfrak{b}_1 \cap \mathfrak{b}_2 = \mathfrak{b}_1 \cdot \mathfrak{b}_2$ [9]. Daher folgt die Aussage. □

Dies können wir auf die Situation oben anwenden und bekommen

$$\boxed{\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathfrak{P}_1^{e_1} \oplus \cdots \oplus \mathcal{O}_L/\mathfrak{P}_k^{e_k},} \tag{7}$$

denn für zwei *verschiedene* maximale Ideale $\mathfrak{P}_i$ und $\mathfrak{P}_j$ gilt immer: $\mathfrak{P}_i + \mathfrak{P}_j = \mathcal{O}_L$ und daraus folgt durch Potenzieren $\mathfrak{P}_i^k + \mathfrak{P}_j^l \supseteq (\mathfrak{P}_i + \mathfrak{P}_j)^{k+l} = \mathcal{O}_L$.

Lemma 2.5.4. *Die $\mathfrak{P}_i$ und e_i sind durch den $\mathcal{O}_L$-Modul (7) eindeutig bestimmt. Mit anderen Worten: aus einem Isomorphismus von $\mathcal{O}_L$-Moduln*

$$\mathcal{O}_L/\mathfrak{P}_1^{e_i} \oplus \cdots \oplus \mathcal{O}_L/\mathfrak{P}_k^{e_j} \cong \mathcal{O}_L/\mathfrak{Q}_1^{e_i'} \oplus \cdots \oplus \mathcal{O}_L/\mathfrak{Q}_{k'}^{e_j'}$$

folgt bis auf Umnummerieren $\mathfrak{P}_i = \mathfrak{Q}_i$, $k = k'$ und $e_i = e_i'$.

Beweis. Dies folgt aus dem Chinesischen Restsatz und der eindeutigen Primfaktorzerlegung, da sich ein Ideal $\mathfrak{a}$ als der Kern einer beliebigen Projektion (=surjektiver Homomorphismus) $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{a}$ rekonstruieren lässt. □

[9] $\supseteq$ ist klar. $\subseteq$: Sei $b \in \mathfrak{b}_1 \cap \mathfrak{b}_2$ und $1 = b_1 + b_2$. Dann folgt: $b = b_1 b + b b_2 \in \mathfrak{b}_1 \cdot \mathfrak{b}_2$.

Satz 2.5.5. *In der Situation von (2.5.1) gilt:*

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

Beweis. Wie haben nach dem Chinesischen Restsatz

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathfrak{P}_1^{e_1} \oplus \cdots \oplus \mathcal{O}_L/\mathfrak{P}_k^{e_k}$$

Indem wir auf beiden Seiten die Dimensionen als $F := \mathcal{O}_K/\mathfrak{p}$-Vektorraum betrachten, genügt es zu zeigen, dass

$$(1)\ \dim_F \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n \qquad (2)\ \dim_F \mathcal{O}_L/\mathfrak{P}^e = e \cdot \dim_F \mathcal{O}_L/\mathfrak{P}.$$

(1) Wir haben bereits gesehen, dass $\mathcal{O}_L$ ein endlich erzeugter $\mathcal{O}_K$-Modul ist (sogar ein e.e. $\mathbb{Z}$-Modul). Daher ist $\dim_F \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L < \infty$. Sei $\overline{\omega}_1, \ldots, \overline{\omega}_m$ eine F-Basis und seien $\omega_1, \ldots, \omega_m$ Urbilder in $\mathcal{O}_L$. Angenommen $m > n$, dann hätten wir sicher

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

mit $a_i \in \mathcal{O}_K$. Es könnte sein, dass alle $a_i \in \mathfrak{p}$ liegen, es sich durch Reduktion modulo $\mathfrak{p}$ also kein direkter Widerspruch ergibt. Trick: Betrache das Ideal $\mathfrak{a} = (a_1, \ldots, a_n)$ von $\mathcal{O}_L$. Wir können ein Element $a \in \mathfrak{a}^{-1}$ wählen, so dass $a \notin \mathfrak{a}^{-1}\mathfrak{p}$. Es gilt dann $a \cdot a_i \in \mathcal{O}$ für alle i, aber nicht alle $a \cdot a_i \in \mathfrak{p}$. Die Gleichung

$$aa_1\omega_1 + \cdots + aa_m\omega_m = 0$$

ergibt also modulo $\mathfrak{p}$ einen Widerspruch.
Es bleibt zu zeigen, dass $\omega_1, \ldots, \omega_m$ ein Erzeugendensystem von $L|K$ bilden. Betrachte den $\mathcal{O}_K$-Untermodul $M = \mathcal{O}_K\omega_1 + \cdots + \mathcal{O}_K\omega_n$. Wir haben $\mathcal{O}_L = M + \mathcal{O}_L\mathfrak{p}$. Betrachte den $\mathcal{O}_K$-Modul $N := \mathcal{O}_L/M$. Er ist endlich erzeugt, da $\mathcal{O}_L$ endlich erzeugt ist. Für ihn gilt: $\mathfrak{p}N = N$. Sei $\alpha_1, \ldots, \alpha_k$ ein Erzeugendensystem. Wir finden also $\alpha_{ij} \in \mathfrak{p}$ so dass

$$\omega_i = \sum_j \alpha_{ij}\omega_j$$

oder

$$(1 - A)\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_k \end{pmatrix} = 0$$

für die Matrix A mit Einträgen α_{ij}. Sei $d = \det(1 - A)$. Wie schon vorher (Multiplikation mit der adjungierten Matrix) bekommen wir: $dN = 0$.

Ausserdem ist $d \neq 0$, denn $\det(1-A) = 1 - \mathrm{tr}(A) \pm \cdots \pm \det(A)$ und alle Summanden ausser 1 sind in $\mathfrak{p}$. Daher ist $\mathcal{O}_L \subseteq \frac{1}{d}M$ und daher ist $\omega_1, \ldots, \omega_m$ ein Erzeugendensystem.
(2) Wir beweisen die Aussage durch Induktion nach e. Für $e = 1$ ist nichts zu zeigen. Für jedes e bekommen wir eine exakte Sequenz von F-Vektorräumen

$$0 \longrightarrow \mathfrak{P}^{e-1}/\mathfrak{P}^e \longrightarrow \mathcal{O}_L/\mathfrak{P}^e \longrightarrow \mathcal{O}_L/\mathfrak{P}^{e-1} \longrightarrow 0$$

und müssen $\dim_{\mathcal{O}_L/\mathfrak{P}}(\mathfrak{P}^{e-1}/\mathfrak{P}^e) = 1$ zeigen. Daraus folgt $\dim_F \mathfrak{P}^{e-1}/\mathfrak{P}^e = f$. Die Dimension kann nicht 0 sein, denn dann wäre $\mathfrak{P}^{e-1} = \mathfrak{P}^e$ was der eindeutigen Primfaktorzerlegung widerspricht. Es gibt also ein Element $\alpha \neq 0$ in $\mathfrak{P}^{e-1}/\mathfrak{P}^e$. Die Abbildung

$$\begin{array}{rcl} \mathcal{O}_L & \to & \mathfrak{P}^{e-1}/\mathfrak{P}^e \\ x & \mapsto & \alpha x \end{array}$$

hat Kern $\mathfrak{P}$ (da $\mathfrak{P}$ maximal). Sie ist aber auch surjektiv, denn $\mathfrak{P}^e \subseteq (\alpha) + \mathfrak{P}^e \subseteq \mathfrak{P}^{e-1}$. Durch Multiplikation mit $(\mathfrak{P}^{e-1})^{-1}$ und der Maximalität von $\mathfrak{P}$ sieht man, dass entweder das linke oder rechte $\subseteq$ eine Gleichheit sein muss, und wegen $\alpha \neq 0$ kommt die erste Gleichheit nicht in Frage. □

Um die Zerlegung von $\mathfrak{p}$ explizit zu bestimmt, muss also die Struktur von $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ als $\mathcal{O}_L$-Modul bestimmt werden. Wir nehmen dazu zunächst an, dass $\mathcal{O}_L = \mathcal{O}_K[\omega]$, d.h. also, dass $1, \omega, \ldots, \omega^{n-1}$ eine Ganzheitsbasis von L über K ist. Dies ist, wie wir gesehen haben, zum Beispiel immer der Fall, wenn $K = \mathbb{Q}$ und $L|\mathbb{Q}$ quadratisch ist. In diesem Fall ist

$$\mathcal{O}_L \cong \mathcal{O}_K[X]/(q)$$

für ein Polynom $q \in \mathcal{O}_K[X]$ und daher

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

für die Reduktion $\overline{q}$ von q modulo $\mathfrak{p}$. Machen Sie sich die zweite Isomorphie klar: Sie ist der entscheidende Trick!
Bezeichne wieder $F := \mathcal{O}_K/\mathfrak{p}$. Dies ist ein endlicher Körper. Wir können nun das Polynom $\overline{q} \in F[X]$ in irreduzible Faktoren zerlegen ($F[X]$ ist ein Hauptidealring und also faktoriell):

$$\overline{q} = (\overline{q}_1)^{e_1} \cdots (\overline{q}_k)^{e_k}$$

und nach dem Chinesischen Restsatz ist

$$\boxed{\mathcal{O}_L/\mathfrak{p} \cong F[X]/\overline{q} \cong F[X]/(\overline{q}_1)^{e_1} \oplus \cdots \oplus F[X]/(\overline{q}_k)^{e_k}.} \qquad (8)$$

Satz 2.5.6. *Die Zerlegungen (7) und (8) entsprechen sich, d.h. wir haben eine Bijektion zwischen*

$$\{\overline{q}_i\} \cong \{\mathfrak{P}_i\}$$

(o.B.d.A. mit derselben Indizierung) und

$$\mathcal{O}_L/\mathfrak{P}_i \cong F[X]/\overline{q}_i \qquad \mathcal{O}_L/(\mathfrak{P}_i)^{e_i} \cong F[X]/(\overline{q}_i)^{e_i}.$$

Insbesondere ist f_i einfach der Grad des Polynoms $\overline{q}_i$.

Beweis. Die Zerlegung (8), die vom Chinesischen Restsatz herkommt, ist sogar ein Ringisomorphismus. Insbesondere ist es daher auch eine Zerlegung von $\mathcal{O}_L$-Moduln. Beachte $\mathcal{O}_L \cong \mathcal{O}_K[X]/(q)$ und ω (das Urbild von X) wirkt auf den $F[X]/(\overline{q}_i)^{e_i}$ durch Multiplikation mit X. Betrachte die resultierende Abbildung

$$\mathcal{O}_L \quad \to \quad F[X]/(\overline{q}_i)^{e_i}$$

welche $\mathcal{O}_K$ auf F reduziert und ω auf X abbildet. Das Urbild des maximalen Ideals $(\overline{q}_i)$ rechts ist ein Primideal $\mathfrak{P}_\mathfrak{i}$ von $\mathcal{O}_L$ und es folgt:

$$\mathcal{O}_L/\mathfrak{P}_i \cong F[X]/\overline{q}_i \qquad \mathcal{O}_L/(\mathfrak{P}_i)^{e_i} \cong F[X]/(\overline{q}_i)^{e_i}.$$

□

Wir können sogar aus dem Beweis entnehmen, dass explizit

$$\boxed{\mathfrak{P}_i = q_i(\omega) + \mathfrak{p}\mathcal{O}_L}$$

ist, wobei $q_i \in \mathcal{O}_K[X]$ ein Urbild von $\overline{q}_i$ ist.
Der Fall $\mathcal{O}_L \cong \mathcal{O}_K[\omega]$, den wir am Anfang der Überlegungen angenommen haben, ist selten erfüllt. Wir können aber folgendes beweisen:

Satz 2.5.7. *Sei $\omega \in \mathcal{O}_L$ und betrachte $\mathcal{O}_K[X]/(q) \cong \mathcal{O}_K[\omega] \subseteq \mathcal{O}_L$. Definiere das Ideal*[10]

$$\mathfrak{f} = \{f \in \mathcal{O}_L \mid (f) \subseteq \mathcal{O}_K[\omega]\}.$$

Falls $\mathfrak{p}$ zu $\mathfrak{f}$ teilerfremd ist (d.h. $\mathfrak{p}\mathcal{O}_L + \mathfrak{f} = \mathcal{O}_L$) dann gilt Satz 2.5.6 genauso bzgl. der Zerlegung (8) von $\overline{q}$ modulo $\mathfrak{p}$.

[10]Zeige als Übung, dass dies ein Ideal ist und immer ungleich (0). Es wird auch der **Führer** von $\mathcal{O}_K[\omega]$ genannt. Wegen der negativen Konnotation dieses Begriffs in der deutschen Sprache wurde auch schon die Bezeichnung **Schaffner** als Rückübersetzung von engl. conductor vorgeschlagen.

Beweis. Wir müssen dazu nur beweisen, dass der Ringhomomorphismus

$$\mathcal{O}_K[\omega]/\mathfrak{p}\mathcal{O}_K[\omega] \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$$

ein Isomorphismus ist. Dann geht alles genauso.
Zunächst folgt aus $\mathfrak{p}\mathcal{O}_L + \mathfrak{f} = \mathcal{O}_L$ auch, dass[11] $\mathfrak{p} + \mathfrak{f} \cap \mathcal{O}_K = \mathcal{O}_K$. Schreibe $1 = y + f$ mit $f \in \mathfrak{f} \cap \mathcal{O}_K$ und $y \in \mathfrak{p}$
Surjektivität: . Für ein beliebieges $x \in \mathcal{O}_L$ erhalten wir $x = yx + fx$. Modulo $\mathfrak{p}\mathcal{O}_L$ ist x also kongruent zu fx, was aber nach Definition von $\mathfrak{f}$ in $\mathcal{O}_K[\omega]$ liegt.
Injektivität: Sei $x \in \mathcal{O}_K[\omega] \cap \mathfrak{p}\mathcal{O}_L$ und schreibe $x = yx + fx$. Es folgt: $fx \in \mathfrak{p}\mathcal{O}_K[\omega]$ und $yx \in \mathfrak{p}\mathcal{O}_K[\omega]$. □

2.5.8. Wir möchten nun am Beispiel der quadratischen Zahlkörper die Primideale von $\mathcal{O}_K$ bestimmen. Sei dazu $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z} \setminus \{0\}$ quadratfrei ($d > 0$ oder $d < 0$ spielt für diese Fragestellung keine Rolle). Wir wissen bereits, dass der Ring der ganzen Zahlen leicht unterschiedliche Form hat, je nachdem, ob $d \equiv 1\ (4)$ oder nicht. Wir betrachten zunächst den einfacheren Fall $d \equiv 2, 3\ (4)$. In diesem Fall ist die Diskriminante $4d$ und wir haben

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}].$$

Die Aufgabe, die uns durch Satz 2.5.6 gestellt wird, ist also das Polynom $X^2 - d$ modulo der Primzahlen p in $\mathbb{Z}$ zu faktorisieren. Offenbar zerfällt dieses Polynom genau dann, wenn d modulo p ein Quadrat ist. Dazu führt man für $a \in \mathbb{Z}$ und Primzahlen $p \neq 2$ das folgende Symbol ein, genannt **Legendresymbol**:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } X^2 \equiv a\ (p) \text{ lösbar und } p \nmid a, \\ -1 & \text{falls } X^2 \equiv a\ (p) \text{ nicht lösbar}, \\ 0 & \text{falls } p \mid a. \end{cases}$$

Ausserdem führen wir noch ein[12]:

$$\left(\frac{a}{2}\right) := \begin{cases} 1 & \text{falls } a \equiv \pm 1\ (8) \\ -1 & \text{falls } a \equiv \pm 3\ (8)\ . \\ 0 & \text{falls } 2 \mid a. \end{cases}$$

Wir erhalten:

[11] Sei $y + f = 1$, dann ist auch $\sigma(y) + \sigma(f) = 1$ für alle $\sigma : L \to \overline{K}$. Multipliziere diese Ausdrücke alle zusammen.

[12] Dies wird historisch nicht Legendresymbol genannt, sondern ist ein Spezialfall vom *Kroneckersymbol*.

Satz 2.5.9. *In $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, d quadratfrei, $d \equiv 2, 3\ (4)$, mit Diskriminante $D = 4d$ gilt für eine Primzahl $p \in \mathbb{Z}$:*

$$\begin{aligned}
(p)\ \textit{prim} \qquad &\textit{(träge)} \qquad &&\textit{falls } \left(\frac{D}{p}\right) = -1,\\
(p) = \mathfrak{p} \cdot \overline{\mathfrak{p}} \quad &\textit{(voll-zerlegt)} \quad &&\textit{falls } \left(\frac{D}{p}\right) = 1,\\
(p) = \mathfrak{p}^2 \quad &\textit{(verzweigt)} \quad &&\textit{falls } \left(\frac{D}{p}\right) = 0.
\end{aligned}$$

Sei im zweiten Fall a eine Lösung von $a^2 \equiv d\ (p)$. Dann gilt:

$$\mathfrak{p} = (p, a + \sqrt{d}) \qquad \overline{\mathfrak{p}} = (p, a - \sqrt{d}).$$

Im dritten Fall ist

$$\mathfrak{p} = (p, \sqrt{d})$$

falls $p \neq 2$. Falls $p = 2$, so bekommen wir

$$\mathfrak{p} = (2, \sqrt{d}) \qquad \textit{oder } \mathfrak{p} = (2, 1 + \sqrt{d})$$

je nachdem, ob $d \equiv 0, 1\ (2)$.

Für den anderen Fall erhalten wir analog:

Satz 2.5.10. *In $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, d quadratfrei, $d \equiv 1\ (4)$, mit Diskriminante $D = d$ gilt für eine Primzahl $p \in \mathbb{Z}$:*

$$\begin{aligned}
(p)\ \textit{prim} \qquad &\textit{(träge)} \qquad &&\textit{falls } \left(\frac{D}{p}\right) = -1,\\
(p) = \mathfrak{p} \cdot \overline{\mathfrak{p}} \quad &\textit{(voll-zerlegt)} \quad &&\textit{falls } \left(\frac{D}{p}\right) = 1,\\
(p) = \mathfrak{p}^2 \quad &\textit{(verzweigt)} \quad &&\textit{falls } \left(\frac{D}{p}\right) = 0.
\end{aligned}$$

Für $p \neq 2$ bekommen wir (wie vorher) im zweiten Fall: Falls a eine Lösung von $a^2 \equiv d\ (p)$ ist, dann gilt:

$$\mathfrak{p} = (p, a + \sqrt{d}) \qquad \overline{\mathfrak{p}} = (p, a - \sqrt{d})$$

und im dritten Fall (d.h. $p \mid d$):

$$\mathfrak{p} = (p, \sqrt{d}).$$

Falls $p = 2$ ist p in diesem Fall unverzweigt und im 2. Fall (d.h. $d \equiv 1\ (8)$) ist

$$\mathfrak{p} = (2, \frac{1+\sqrt{d}}{2}) \qquad \overline{\mathfrak{p}} = (2, \frac{1-\sqrt{d}}{2})$$

Beachte, dass in jedem Fall (für beliebige d) eine Primzahl p genau dann verzweigt ist, wenn $p|D$. Eine Tatsache, die sich auf andere Zahlkörper verallgemeinert.

Beweis von Satz 2.5.10. Zunächst können wir wegen Satz 2.5.7 für $p \neq 2$ auch mit $\mathbb{Z}[\sqrt{d}]$ arbeiten, da das Ideal $\mathfrak{f}$ in diesem Fall ein Teiler von (2) ist. Dazu ist nur zu sehen, dass $2 \cdot \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subset \mathbb{Z}[\sqrt{d}]$, was offensichtlich ist. Den Fall $p = 2$ lassen wir als Übung. □

Zum Abschluss beweisen wir noch das folgende Lemma über die Zerlegung in Primideale:

Lemma 2.5.11. *Sei $L|K$ eine Galoiserweiterung von Zahlkörpern, sei $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ und sei*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}$$

die Zerlegung in Primideale von $\mathcal{O}_L$. Dann sind alle e_i gleich und $\mathrm{Gal}(L|K)$ operiert transitiv auf den $\mathfrak{P}_i$.

Beweis. Es genügt zu zeigen: Falls $\mathfrak{P}$ und $\mathfrak{P}'$ zwei Primideale von $\mathcal{O}_L$ sind, mit $\mathfrak{p} \subseteq \mathfrak{P}$ und $\mathfrak{p} \subseteq \mathfrak{P}'$, dann gibt es ein $\sigma \in \mathrm{Gal}(L|K)$ mit $\mathfrak{P}' = \sigma\mathfrak{P}$. (Die Gleichheit der zugehörigen e_i folgt dann durch Anwenden von σ aus der Eindeutigkeit der Primfaktorzerlegung). Wir beweisen dies durch Widerspruch und nehmen an, dass $\mathfrak{P}' \neq \sigma\mathfrak{P}$ für alle $\sigma \in \mathrm{Gal}(L|K)$. Nach dem Chinesischen Restsatz gibt es dann ein $x \in \mathcal{O}_L$ mit

$$x \equiv 0\ (\mathfrak{P}') \qquad x \equiv 1\ (\sigma\mathfrak{P}) \text{ für alle } \sigma$$

Betrachte nun die Norm

$$N_{L|K}(x) = \prod_{\sigma} \sigma(x).$$

Sie liegt nicht in $\mathfrak{P}$, da alle $\sigma(x) \equiv 1\ (\mathfrak{P})$. Andererseits liegt $x \in \mathfrak{P}'$, daher auch die Norm. Da $\mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$ ist also $N_{L|K}(x) \in \mathfrak{p} \subset \mathfrak{P}$. Widerspruch. □

2.6 Zyklotomische Körper

In diesem Abschnitt wollen wir den Ring der ganzen Zahlen und deren Primideale in den zyklotomischen Körpern $\mathbb{Q}(\zeta_{p^l})$ bestimmen, wobei ζ_{p^l} eine primitive p^l-te Einheitswurzel ist. Hier ist p eine Primzahl. Das ganze kann man auf beliebige $\mathbb{Q}(\zeta_n)$ verallgemeinern. Wir werden das allerdings nicht diskutieren.

Satz 2.6.1. *Der Ring der ganzen Zahlen in $K = \mathbb{Q}(\zeta_{p^l})$ ist*

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^l}].$$

Ganze Zahlen in $\mathbb{Q}(\zeta_{p^l})$ bestehen also einfach aus Polynomen in einer p^l-ten Einheitswurzel mit ganzen Koeffizienten.

Wir benötigen einige Vorüberlegungen und schreiben ab jetzt einfach ζ für ζ_{p^l}.

Lemma 2.6.2. *1. Für i und j teilerfremd zu p sind die Elemente $\frac{1-\zeta^i}{1-\zeta^j}$ Einheiten im Ring $\mathcal{O}_K$.*

2. Es gilt die Idealgleichung

$$(p) = (1-\zeta)^{\varphi(p^l)}$$

dabei ist $\varphi(p^l) = p^{l-1}(p-1)$ die Eulersche φ-Funktion.

3. Die Diskriminante von $\mathbb{Z}[\zeta_{p^l}]$ ist eine Potenz von p.

Beweis. 1. Es genügt sicher, dies für $j = 1$ zu zeigen, denn alle anderen Ausdrücke sind Quotienten derjenigen für $j = 1$. Wegen

$$\frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{i-1}$$

ist das Element ganz. Nun gilt aber $\zeta = (\zeta^i)^j$ für ein Element j mit $i \cdot j \equiv 1\ (p^l)$. Daher ist auch der Kehrwert ganz.
2. Wir wissen aus der Algebra, dass ζ Nullstelle des p^l-ten zyklotomischen Polynoms ist, also

$$\frac{X^{p^l}-1}{X^{p^{l-1}}-1} = X^{p^{l-1}(p-1)} + \cdots + X^{p^{l-1}} + 1 = \prod_{i \in (\mathbb{Z}/p^l\mathbb{Z})^*} (X - \zeta^i).$$

Indem wir in diesem Ausdruck $X = 1$ setzen, ergibt sich

$$p = \prod_{i \in (\mathbb{Z}/p^l\mathbb{Z})^*} (1 - \zeta^i).$$

Da sich nun die Elemente $1 - \zeta^i$ nach 1. nur bis auf Einheiten voneinander unterscheiden folgt die Idealgleichung:

$$(p) = (1 - \zeta)^{\varphi(p^l)}.$$

3. Wir wissen nach dem Beweis von Lemma 2.2.4, dass

$$d(1, \zeta, \ldots, \zeta^{\varphi(p^l)-1}) = \prod_{\substack{i,j \in (\mathbb{Z}/p^l\mathbb{Z})^* \\ i \neq j}} (\zeta^j - \zeta^i).$$

Nun sind aber die p^l-ten Einheitswurzeln modulo jeder Primzahl $q \neq p$ verschieden, da $q^k - 1$ irgendwann einmal durch p^l teilbar wird (q hat endliche Ordnung modulo p^l). Daher kann dieser Ausdruck höchstens 0 werden modulo p aber nicht modulo anderen Primzahlen. □

Beweis von Satz 2.6.1. Wegen der in Lemma 2.6.2, 2. bewiesenen Gleichung

$$(p) = (1 - \zeta)^{\varphi(p^l)}$$

gibt es in der folgenden Formel nur einen Summanden:

$$n = \sum_i e_i f_i = \varphi(p^l) \cdot f.$$

Da aber sicherlich $n \leq \varphi(p^l)$ (da $\varphi(p^l)$ der Grad des zyklotomischen Polynoms ist) gilt

$$(1 - \zeta) \text{ prim} \quad \text{und} \quad n = \varphi(p^l) \quad \text{und} \quad f = 1.$$

Der Grad der Körpererweiterung ist also tatsächlich gleich $\varphi(p^l)$. (Dies ergibt einen alternativen Beweis, dass das p^l-te zyklotomische Polynom irreduzibel ist.) $f = 1$ bedeutet, dass $\mathcal{O}_K/(1-\zeta) = \mathbb{Z}/p\mathbb{Z}$ ist, also insbesondere $\mathbb{Z} + (1 - \zeta) = \mathcal{O}_K$ und also auch:

$$\mathbb{Z}[\zeta] + (1 - \zeta) = \mathcal{O}_K.$$

Durch Multiplikation mit $1 - \zeta$ ergibt sich $(1 - \zeta) = (1 - \zeta)\mathbb{Z}[\zeta] + (1 - \zeta)^2$. Wenn wir dies einsetzen:

$$\mathbb{Z}[\zeta] + (1 - \zeta)^2 = \mathcal{O}_K.$$

und schliesslich per Induktion unter Verwendung von $(1-\zeta)^{\varphi(p^l)} = (p)$, dass

$$\mathbb{Z}[\zeta] + (p^s) = \mathcal{O}_K.$$

für beliebiges s. Nun haben wir in Lemma 2.3.2 gelernt, dass $d\mathcal{O}_K \subset \mathbb{Z}[\zeta]$ für die Diskriminante d von $\mathbb{Z}[\zeta]$ welche nach Lemma 2.6.2, 3. eine Potenz von p ist, also:

$$(p^s) \subset \mathbb{Z}[\zeta].$$

Wir erhalten

$$\mathbb{Z}[\zeta] = \mathcal{O}_K.$$

□

Wir möchten nun die Primideale in $\mathbb{Z}[\zeta]$ bestimmen und schauen uns dazu wiederum an, wie ein Hauptideal (q), wobei q eine gewöhnliche Primzahl ist, in $\mathbb{Z}[\zeta]$ in Primideale zerfällt. Für $q = p$ wissen wir schon, dass $(p) = (1-\zeta)^{\varphi(p^l)}$ die Zerlegung ist, d.h. $(1-\zeta)$ ist in diesem Fall das einzige Primideal über p. Ansonsten könnten wir Satz 2.5.6 anwenden und erhalten dass die Zerlegung

$$(q) = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_k^{e_k}$$

der Faktorisierung des zyklotomischen Polynoms

$$\frac{X^{p^l}-1}{X^{p^{l-1}}-1} = X^{p^{l-1}(p-1)} + \cdots + X^{p^{l-1}} + 1 = \prod_{i \in (\mathbb{Z}/p^l\mathbb{Z})^*} (X - \zeta^i).$$

modulo (q) entspricht. Wir können allerdings anders argumentieren. Zunächst sind modulo q alle Nullstellen verschieden, wie wir schon im Beweis des Lemmas oben benutzt haben. Deshalb können keine Potenzen auftreten. Jeder Faktor $\mathcal{O}_L/\mathfrak{q}_i$ wird nun über $\mathbb{F}_q$ von einer p^l-ten Einheitswurzel erzeugt. Es handelt sich also um die kleinste Erweiterung von $\mathbb{F}_q$ welche eine solche enthält, d.h.

$$\#\mathcal{O}_L/\mathfrak{q}_i = q^f$$

und f ist die kleinste natürliche Zahl so dass $p^l | (q^f - 1)$. Wir haben bewiesen:

Satz 2.6.3. *Sei $L = \mathbb{Q}(\zeta_{p^l})$, sei $q \neq p$ eine Primzahl und f die Ordnung von q modulo p^l. Dann gilt in $\mathcal{O}_L$*

$$(q) = \mathfrak{q}_1 \cdots \mathfrak{q}_k$$

und alle Trägheitsgrade $[\mathcal{O}_L/\mathfrak{q}_i : \mathbb{F}_q]$ sind gleich f und also $k = \frac{\varphi(p^l)}{f}$.

2.7 Das quadratische Reziprozitätsgesetz

Seien $p \neq q$ zwei Primzahlen kongruent 1 modulo 4. Das quadratische Reziprozitätsgesetz ist die erstaunliche Aussage

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

für das Legendresymbol (siehe 2.5.8). Falls p und q beliebige Primzahlen sind, gilt

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

wobei $p^* = -p$ für $p \equiv 3\ (4)$ und $2^* = 2$ gesetzt wird.
Es ergibt sich hier einfach aus dem Vergleich der Erkenntnisse, die wir über die zyklotomischen und die quadratischen Zahlkörper gewonnen haben. Zunächst haben wir:

Lemma 2.7.1. *Für ungerade p enthält $\mathbb{Q}(\zeta_{p^l})$ $l \geq 1$ genau einen quadratischen Zahlkörper und zwar $\mathbb{Q}(\sqrt{p^*})$.*
$\mathbb{Q}(\zeta_{2^l})$ $l \geq 3$ enthält genau die quadratischen Zahlkörper $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{-2})$.

Beweis. Sei p ungerade. Wir wissen, dass $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^l})|\mathbb{Q}) \cong (\mathbb{Z}/p^l\mathbb{Z})^*$. Diese Gruppe ist zyklisch von gerader Ordnung (wir werden das hier nicht beweisen, da es eher der elementaren Zahlentheorie angehört). Diese hat daher genau eine Untergruppe vom Index 2. Daher gibt es nach Galoistheorie genau einen quadratischen Zwischenkörper K:

$$L := \mathbb{Q}(\zeta_{p^l}) \mid K = \mathbb{Q}(\sqrt{d}) \mid \mathbb{Q}.$$

Behauptung: In K ist auch höchstens die Primzahl p verzweigt. Falls wir nämlich eine Gleichung

$$q\mathcal{O}_K = \mathfrak{q}^2$$

hätten, und $\mathfrak{q}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_n$, dann ist auch

$$q\mathcal{O}_L = (\mathfrak{q}_1 \cdots \mathfrak{q}_n)^2$$

und daher q verzweigt in $\mathcal{O}_L$. Wir haben gesehen, dass dann $q = p$ sein muss. In unserer Bestimmung der quadratischen Körper haben wir gesehen, dass ein quadratischer Körper genau an den Primzahlen verzweigt, die die Diskriminante d bzw. $4d$ teilen. Der Fall $4d$ darf also nicht vorkommen, denn sonst wäre 2 verzweigt. Daher muss $d \equiv 1\ (4)$ sein und ausserdem

muss $d = \pm p$ sein, denn sonst wäre eine andere Primzahl $q \neq p$ verzweigt. Es bleibt nur $d = p$, falls $p \equiv 1\ (4)$ und $d = -p$, falls $p \equiv 3\ (4)$.
Sei p nun gerade. Wir wissen, dass $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^l})|\mathbb{Q}) \cong (\mathbb{Z}/2^l\mathbb{Z})^* \cong \mathbb{Z}/2^{l-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Auch die zweite Isomorphie wollen wir hier nicht beweisen. Für $l \geq 3$ gibt es darin genau 3 Untergruppen vom Index 2. Die zugehörigen quadratischen Zahlkörper dürfen höchstens an der Primzahl 2 verzweigt sein. D.h. es kommen nur $d \in \{-2, -1, 2\}$ in Frage. Alle anderen d sind durch eine andere Primzahl teilbar. □

Das Lemma sagt uns insbesondere, dass die Wurzel $\sqrt{p^*}$ als ganzzahliges Polynom in einer primitiven Einheitswurzel ζ_p ausdrückbar ist. In der Tat kann man für ungerade p zeigen, dass

$$\sqrt{p^*} = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right) \zeta_p^a.$$

Z.B. ist $\sqrt{-3} = \zeta_3 - \zeta_3^2 = 2\zeta_3 - 1$. In diesem Fall ist sogar $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Genauso ist

$$\sqrt{2} = \sum_{a \in (\mathbb{Z}/8\mathbb{Z})^*} \left(\frac{a}{2}\right) \zeta_8^a$$

oder auch

$$\zeta_8 = \frac{1+i}{\sqrt{2}}.$$

D.h. $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$ und $\mathbb{Q}(\zeta_8)$ ist das Kompositum von $\mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-1})$, und $\mathbb{Q}(\sqrt{2})$.
Wir zeigen nun

Satz 2.7.2. *Sei $K = \mathbb{Q}(\sqrt{p^*})$ und q eine Primzahl ungleich p. Dann ist q voll-zerlegt in K genau dann wenn*

$$\left(\frac{q}{p}\right) = 1.$$

Nun hatten wir aber bereits gesehen, dass in $\mathbb{Q}(\sqrt{d})$ eine Primzahl q genau dann voll-zerlegt ist, wenn $\left(\frac{D}{q}\right) = 1$, also hier für $D = d = p^*$, wenn $\left(\frac{p^*}{q}\right) = 1$. Es folgt:

Korollar 2.7.3 (Quadratisches Reziprozitätsgesetz)**.** *Für zwei Primzahlen p und q gilt:*

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

Beweis von Satz 2.7.2. Wir nehmen zunächst an, dass p ungerade ist. O.B.d.A. ist $q \neq p$.
Sei f die Ordnung von q modulo p. Da $\mathbb{F}_p^*$ zyklisch ist, kann man dann schreiben

$$q = \xi^{\frac{p-1}{f}}$$

wobei ξ ein Erzeuger der multiplikativen Gruppe ist. q hat also eine Quadratwurzel genau dann wenn $\frac{p-1}{f}$ gerade ist:

$$\left(\frac{q}{p}\right) = 1 \;\Leftrightarrow\; \frac{p-1}{f} \text{ gerade.}$$

Nun zerfällt (q) in $\mathbb{Q}(\zeta_p)$ nach Satz 2.6.3 in $k = \frac{p-1}{f}$ Primideale. Wir haben also

$$\left(\frac{q}{p}\right) = 1 \;\Leftrightarrow\; \begin{array}{c}(q) \text{ zerfällt in } \mathbb{Q}(\zeta_p) \text{ in} \\ \text{eine gerade Anzahl von Primidealen.}\end{array}$$

Daher genügt es zu zeigen

$$\begin{array}{c}(q) \text{ zerfällt in } \mathbb{Q}(\zeta_p) \text{ in} \\ \text{eine gerade Anzahl von Primidealen}\end{array} \Leftrightarrow (q) \text{ voll-zerlegt in } \mathbb{Q}(\sqrt{p^*}).$$

Wir wissen, dass $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$. Bezeichne die Körper wie folgt:

$$L = \mathbb{Q}(\zeta_p) \mid K = \mathbb{Q}(\sqrt{p^*}) \mid \mathbb{Q}.$$

Wir haben in K entweder

$$q\mathcal{O}_K = \mathfrak{q}\overline{\mathfrak{q}} \quad \text{oder} \quad q\mathcal{O}_K \text{ prim}$$

und daher in L

$$q\mathcal{O}_L = \underbrace{\mathfrak{Q}_1 \cdots \mathfrak{Q}_k}_{\mathfrak{q}\mathcal{O}_L} \cdot \underbrace{\overline{\mathfrak{Q}}_1 \cdots \overline{\mathfrak{Q}}_k}_{\overline{\mathfrak{q}}\mathcal{O}_L} \quad \text{oder} \quad q\mathcal{O}_L = \mathfrak{Q}_1 \cdots \mathfrak{Q}_{k'}.$$

Nach Lemma 2.5.11 operiert die Galoisgruppe $\mathrm{Gal}(L|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ transitiv auf dieser Zerlegung. Wir sehen, dass der 1. Fall, d.h. (q) voll-zerlegt in K genau dann auftritt, wenn die Galoisgruppe $\mathrm{Gal}(L|K)$ *nicht* transitiv operiert. Wir haben im Beweis von Lemma 2.7.1 gesehen, dass die Galoisgruppe $\mathrm{Gal}(L|K)$ die eindeutig bestimmte Untergruppe von $\mathrm{Gal}(L|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ vom Index 2 ist. Die Aussage folgt daher aus Lemma 2.7.4 unten.
Falls $p = 2$, dann ist q ungerade, und die Aussage des quadratischen Reziprozitätsgesetzes (welche äquivalent zu der zu beweisenden Aussage ist) folgt durch Vertauschen von p und q unter Beachtung von $2^* = 2$ (nach Definition) und $\left(\frac{q^*}{2}\right) = \left(\frac{q}{2}\right)$ (ebenfalls nach Definition). □

Lemma 2.7.4. *Sei G eine endliche zyklische Gruppe gerader Ordnung welche auf einer Menge X transitiv operiert, und $H \subset G$ die (eindeutig bestimmte) Untergruppe vom Index 2. Dann gilt*

$$\#X \text{ gerade } \Leftrightarrow H \text{ operiert nicht transitiv auf } X$$

Beweis. Übung. Wir haben $X \cong G/H'$ wobei H' der Stabilisator eines (und daher aller) Elemente aus X ist. H operiert also genau dann transitiv, wenn $H \cdot H' = G$ ist. Nun überlege man sich:

$$\#X \text{ gerade } \Leftrightarrow 2 \mid [G : H'] \Leftrightarrow H' \subset H \Leftrightarrow H \cdot H' \neq G.$$

□

3 Minkowski-Theorie

3.1 Der additive Minkowski-Raum

Wir haben in 2.3.3 gesehen, dass der Ring der ganzen Zahlen $\mathcal{O}_K$ in einem Zahlkörper K eine Ganzheitsbasis besitzt, also ein freier $\mathbb{Z}$-Modul ist:

$$\mathcal{O}_K \cong \mathbb{Z}^n.$$

Für den Fall der imaginär-quadratischen Körper ergab sich eine natürliche Einbettung $\mathcal{O}_K \subset \mathbb{C}$. Der Ring der ganzen Zahlen, und auch jedes Ideal darin, wird so zu einem *Gitter* in $\mathbb{C}$. Wir möchten gerne diese Situation für einen beliebigen Zahlkörper herstellen. Aus einem freien $\mathbb{Z}$-Modul M vom Rang n kann man immer einen $\mathbb{R}$-Vektorraum von der Dimension n machen, in den M als Gitter eingebettet ist, nämlich das Tensorprodukt

$$M \otimes_{\mathbb{Z}} \mathbb{R}.$$

Wir werden die Eigenschaften der Tensorprodukte hier nicht im Detail studieren, da sie eher der (elementaren) Algebra angehören. Wichtig ist für uns nur: Falls $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von M ist, so ist $x_1 \otimes 1, \ldots, x_n \otimes 1$ eine Basis von $M \otimes_{\mathbb{Z}} \mathbb{R}$ als $\mathbb{R}$-Vektorraum. Hier passiert also etwas sehr einfaches. Wenn einmal die Basis von M festgehalten wird, besteht M aus Vektoren aus n ganzen Zahlen. $M \otimes_{\mathbb{Z}} \mathbb{R}$ besteht aus Vektoren aus n reellen Zahlen und die Einbettung $M \hookrightarrow M \otimes_{\mathbb{Z}} \mathbb{R}$ fasst einfach einen ganzzahligen Vektor als Vektor mit reellen Einträgen auf. Es ist klar, dass M in $M \otimes_{\mathbb{Z}} \mathbb{R}$ ein Gitter bildet. Der Vorteil des Tensorproduktes ist, dass die Definition basisunabhängig ist.

Wir betachten also den reellen Vektorraum

$$K_{\mathbb{R}} := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{R} \cong K \otimes_{\mathbb{Q}} \mathbb{R}.$$

Lemma 3.1.1. *Es gibt einen* kanonischen *(also von allen etwaigen Wahlen unabhängigen) Isomorphismus von $\mathbb{R}$-Vektorräumen (oder sogar $\mathbb{R}$-Algebren)*

$$K_{\mathbb{R}} \cong \bigoplus_{\tau: K \hookrightarrow \mathbb{R}} \mathbb{R} \oplus \bigoplus_{\substack{\sigma, \overline{\sigma}: K \hookrightarrow \mathbb{C} \\ \text{Paar konjugiert} \\ \text{komplexer Einbettungen}}} \mathbb{C} = \mathbb{R}^t \oplus \mathbb{C}^s.$$

Hier ist t die Anzahl der reellen Einbettungen und s die Anzahl der Paare *komplex konjugierter Einbettungen. Insbesondere gilt: $r + 2s = n$.*

Beweis. Wir betrachten zunächst $K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C}$. Es gibt eine kanonische $\mathbb{C}$-lineare Abbildung

$$\begin{aligned} K \otimes_{\mathbb{Q}} \mathbb{C} &\to \bigoplus_{\sigma: K \hookrightarrow \mathbb{C}} \mathbb{C} \\ k \otimes \alpha &\mapsto (\alpha \cdot \sigma(k))_\sigma. \end{aligned} \tag{9}$$

Beachte, dass das Tensorprodukt durch die formalen Symbole $k \otimes \alpha$ für $k \in K$ und $\alpha \in \mathbb{C}$ erzeugt wird. Dafür, dass die Abbildung wohldefiniert ist, ist notwendig und hinreichend, dass die Formel bilinear in α und k ist. Dies kann man direkt ablesen. Wir wollen zeigen, dass sie invertierbar ist. Dazu wähle ein primitives Element ω von K. K hat also die Basis $1, \omega, \ldots, \omega^{n-1}$ als $\mathbb{Q}$-Vektorraum. Die Matrix[13] der Abbildung (9) ist offenbar durch

$$\begin{pmatrix} 1 & \sigma_1(\omega) & \cdots & \sigma_1(\omega)^{n-1} \\ \vdots & & \ddots & \vdots \\ 1 & \sigma_n(\omega) & \cdots & \sigma_n(\omega)^{n-1} \end{pmatrix}$$

gegeben. Dies ist eine VANDERMONDE Determinante und ungleich 0, da alle $\sigma_i(\omega)$ verschieden sind. Die Abbildung ist also ein Isomorphismus. An der Formel (9) liesst man sofort ab, dass dies sogar ein Isomorphismus von $\mathbb{C}$-Algebren ist.
Auf $K \otimes_{\mathbb{Q}} \mathbb{C}$ gibt es einen $\mathbb{R}$-linearen Automorphismus F (aber nicht $\mathbb{C}$-linear!), der von der komplexen Konjugation herkommt, und den wir auch "komplexe Konjugation" nennen wollen. Es ist durch $F(k \otimes \alpha) = k \otimes \overline{\alpha}$

[13] bzgl. der Basis $1 \otimes 1, \omega \otimes 1, \ldots, \omega^{n-1} \otimes 1$ links und der offensichtlichen (durch die Einbettungen indizierten) rechts.

gegeben. $K \otimes_{\mathbb{Q}} \mathbb{R}$ ist also die Menge der Invarianten unter F. Wie sieht F auf der rechten Seite von (9) aus? Dies ist *nicht* einfach die komplexe Konjugation in jedem Eintrag a_σ (dieses wäre nicht mit der Abbildung (9) verträglich), sondern wird durch

$$F : a_\sigma \mapsto (\overline{a_{\overline{\sigma}}})_\sigma$$

gegeben. Falls $\sigma = \overline{\sigma}$, also falls σ eine reelle Einbettung ist, dann konjugiert F einfach den entsprechenden Eintrag. Ansonsten werden die Einträge für σ und $\overline{\sigma}$ vertauscht und dabei komplex kongugiert. Falls wir die Einbettungen durchnummerieren: $\tau_1, \ldots, \tau_r$ für die reellen Einbettungen, und $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s$ für die Paare von komplex konjugierten Einbettungen, so wird F also gegeben durch

$$F : \left(\begin{array}{c} a_{\tau_1} \\ \vdots \\ a_{\tau_r} \\ \hline a_{\sigma_1} \\ a_{\overline{\sigma}_1} \\ \vdots \\ a_{\sigma_s} \\ a_{\overline{\sigma}_s} \end{array}\right) \mapsto \left(\begin{array}{c} \overline{a_{\tau_1}} \\ \vdots \\ \overline{a_{\tau_r}} \\ \hline \overline{a_{\overline{\sigma}_1}} \\ \overline{a_{\sigma_1}} \\ \vdots \\ \overline{a_{\overline{\sigma}_s}} \\ \overline{a_{\sigma_s}} \end{array}\right)$$

Die Invarianten unter F sind daher von der Form

$$\left(\begin{array}{c} a_{\tau_1} \\ \vdots \\ a_{\tau_r} \\ \hline a_{\sigma_1} \\ \overline{a_{\sigma_1}} \\ \vdots \\ a_{\sigma_s} \\ \overline{a_{\sigma_s}} \end{array}\right)$$

mit $a_{\tau_i} \in \mathbb{R}, i = 1, \ldots, t$ und $a_{\sigma_i} \in \mathbb{C}, i = 1, \ldots, s$. □

3.2 Gitter

Der Schlüssel, um die Endlichkeit der Klassenzahl zu beweisen, liegt darin, in den Idealen von $\mathcal{O}_K$ Elemente zu finden, deren Norm möglichst klein

ist. Die MINKOWSKI-Theorie, die wir in diesem Kapitel entwickeln werden, gibt Werkzeuge, um dieses "möglichst klein" quantitativ zu messen. Wir beginnen mit der präzisen Definition des Begriffs "Gitter".

Definition 3.2.1. *Sei V ein $\mathbb{R}$-Vektorraum der Dimension n. Ein* **Gitter** *in V ist ein (freier) $\mathbb{Z}$-Untermodul von V*

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

so dass $v_1, \ldots, v_m$ $\mathbb{R}$-linear unabhängig sind. $v_1, \ldots, v_m$ heisst **Basis** *des Gitters. Die Menge*

$$\Phi := \{x_1v_1 + \cdots + x_nv_n \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\}$$

heisst **Grundmasche** *des Gitters.*

Beachte, dass die Forderung, dass $v_1, \ldots, v_m$ $\mathbb{R}$-linear unabhängig sind, nicht automatisch ist. Z.B. ist $\mathbb{Z} + \sqrt{2}\mathbb{Z} \subset \mathbb{R}$ ein freier $\mathbb{Z}$-Untermodul vom Rang 2, aber 1 und $\sqrt{2}$ sind natürlich nicht $\mathbb{R}$-linear unabhängig.

Definition 3.2.2. *Ein Gitter $\Gamma \subset V$ heisst vollständig, wenn $m = n$ ist, also falls $v_1, \ldots, v_m$ eine $\mathbb{R}$-Basis von V bilden.*

Äquivalente Definitionen sind:

1. $V = \bigcup_{\gamma \in \Gamma} \Phi + \gamma$.
2. Die natürliche Abbildung $\Gamma \otimes_{\mathbb{Z}} \mathbb{R} \to V$ ist ein Isomorphismus.
3. V/Γ ist kompakt.

Wir lassen den Beweis als Übung.
Erinnere, dass eine Teilmenge $\Gamma \subset V$ in einem topologischen Raum **diskret** heisst, wenn zu jedem $\gamma \in \Gamma$ eine offene Umgebung $U \ni \gamma$ existiert so, dass $U \cap \Gamma = \{\gamma\}$. Wir haben folgende Charakterisierung:

Lemma 3.2.3. *Eine Untergruppe Γ des endlich dimensionalen reellen Vektorraums V ist genau dann ein Gitter, wenn sie diskret ist.*

Beweis. Wir können o.B.d.A. annehmen, dass $\mathbb{R}\Gamma = V$ ist, dass also V von den Vektoren in Γ erzeugt wird.
Es ist dann klar, dass ein Gitter diskret ist, denn $\gamma + \Phi^\circ - \frac{1}{2}(v_1 + \cdots + v_n)$ ist offen und erfüllt offenbar die Bedingung $\Gamma \cap (\gamma + \Phi^\circ - \frac{1}{2}(v_1 + \cdots + v_n)) = \{\gamma\}$. Hier ist Φ° das Innere der Grundmasche.

Wähle umgekehrt eine Basis $v_1, \ldots, v_n$ von V mit $v_i \in \Gamma$. Bezeichne $\Gamma_0 = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$. Es genügt zu zeigen, dass der Index

$$[\Gamma : \Gamma_0]$$

endlich ist. Γ/Γ_0 bettet nun in die kompakte Gruppe V/Γ_0 ein. Es ist also diskret in einer kompakten Menge, daher endlich. □

3.3 Volumen

Wir möchten gerne das Volumen eines Gitters Γ durch

$$\mathrm{vol}(\Gamma) := \mathrm{vol}(\Phi)$$

definieren, wobei Φ die Fundamentalmasche ist. Im $\mathbb{R}^n$ ist klar, was mit dem Volumen gemeint ist. In einem beliebigen $\mathbb{R}$-Vektorraum V hängt dies erstmal von der Basiswahl ab. Wir wollen uns zunächst überlegen, dass es genügt, ein *Skalarprodukt* auf V zu fixieren (also eine symmetrische, positiv definite Bilinearform). Dieses induziert immer ein Volumen, so dass für eine Orthonormalbasis $v_1, \ldots, v_n$

$$\mathrm{vol}(\{x_1v_1 + \cdots + x_nv_n \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\}) = 1$$

ist. Dazu müssen wir uns nur überlegen, dass für zwei verschiedene Orthonormalbasen $v_1, \ldots, v_n$ und $v_1', \ldots, v_n'$ und ein beliebiges Volumen auf V gilt:

$$\mathrm{vol}(\{x_1v_1+\cdots+x_nv_n \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\}) = \mathrm{vol}(\{x_1v_1'+\cdots+x_nv_n' \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\})$$

In der Tat unterscheiden sich die beiden nach der Integraltransformationsformel um den Betrag der Basiswechselabbildung. Die Determinante einer orthogonalen Abbildung ist aber immer gleich ± 1.

Lemma 3.3.1. *Sei V ein reeller Vektorraum der Dimension n mit Skalarprodukt $\langle \cdot, \cdot \rangle$ und zugehörigem Volumen. Für ein Gitter $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ gilt:*

$$\mathrm{vol}(\Gamma) = \sqrt{\det(\langle v_i, v_j \rangle)_{i,j}}.$$

Beweis. Sei $v_1', \ldots, v_n'$ eine Orthonormalbasis und M die Basiswechselmatrix welche $v_1, \ldots, v_n$ in dieser Basis ausdrückt. Wir haben

$$\mathrm{vol}(\Gamma) = |\det(M)|.$$

Andererseits ist

$$(\langle v_i, v_j \rangle)_{ij} = {}^tM \cdot M.$$

Daraus folgt die Behauptung. □

3.3.2. Auf einem Zahlkörper K haben wir stets die nicht-ausgeartete Bilinearform

$$\langle x, y\rangle = \mathrm{tr}_{K|\mathbb{Q}}(x \cdot y)$$

betrachtet. Sie setzt sich linear auf $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ fort, und zwar einfach durch

$$\langle x \otimes \alpha, y \otimes \beta\rangle = \alpha\beta \,\mathrm{tr}_{K|\mathbb{Q}}(x \cdot y).$$

Diese Bilinearform ist jedoch nicht positiv-definit und deshalb nicht geeignet, um ein Volumen zu definieren. Wir konstruieren deshalb eine andere auf $K \otimes_{\mathbb{Q}} \mathbb{R}$, indem wir das hermitesche Standardskalarprodukt (bzgl. der kanonischen Basis, die durch die Einbettungen gegeben ist) auf

$$K \otimes_{\mathbb{Q}} \mathbb{C} \cong \bigoplus_{\sigma: K \hookrightarrow \mathbb{C}} \mathbb{C}$$

auf $K \otimes_{\mathbb{Q}} \mathbb{R}$ einschränken. Dazu beobachte, dass

$$\langle Fa_\sigma, Fb_\sigma\rangle = \sum_\sigma \overline{a_{\overline{\sigma}}} b_{\overline{\sigma}} = \overline{\sum_\sigma a_\sigma \overline{b_\sigma}} = \overline{\langle a_\sigma, b_\sigma\rangle}.$$

Daraus folgt, dass auf dem Raum der F-Invarianten (welcher gerade $K \otimes_{\mathbb{Q}} \mathbb{R}$ ist) das hermitesche Standardskalarprodukt reelle Werte annimmt und deshalb ein Skalarprodukt ist. Explizit wird es durch:

$$\left\langle \begin{pmatrix} a_{\tau_1} \\ \vdots \\ a_{\tau_r} \\ \hline a_{\sigma_1} \\ \vdots \\ a_{\sigma_s} \end{pmatrix}, \begin{pmatrix} b_{\tau_1} \\ \vdots \\ b_{\tau_r} \\ \hline b_{\sigma_1} \\ \vdots \\ b_{\sigma_s} \end{pmatrix} \right\rangle = \sum_{i=1}^{r} a_{\tau_i} b_{\tau_i} + 2\sum_{i=1}^{s} (\Re(a_{\sigma_i})\Re(b_{\sigma_i}) + \Im(a_{\sigma_i})\Im(b_{\sigma_i}))$$

gegeben. Es ist also, bis auf einen Faktor 2 in den komplexen Variablen, gleich dem Standardskalarprodukt (wenn man $\mathbb{C}$ mit $\mathbb{R}^2$ identifiziert). Wir wählen auf $K_{\mathbb{R}}$ nun das zu diesem Skalarprodukt assoziierte Volumen. Es unterscheidet sich von dem gewöhnlichen Volumen also durch den Faktor 2^s.

3.4 Der Minkowskische Gitterpunktsatz

Der Minkowskische Gitterpunktsatz ist das Hauptwerkzeug, um die Endlichkeit der Klassenzahl und den Dirichletschen Einheitensatz zu beweisen. Er ist recht elementar und besagt folgendes:

Satz 3.4.1. *Sei $\Gamma \subset V$ ein vollständiges Gitter in einem $\mathbb{R}$-Vektorraum der Dimension n. Falls $X \subset V$ irgendeine Menge ist, welche*

1. **zentralsymmetrisch** *ist (also $x \in X \Rightarrow -x \in X$);*
2. **konvex** *ist (also mit $x, x' \in X$ liegt auch die Verbindungsstrecke von x nach x' in X);*
3. *und so dass* $\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\Gamma)$,

dann gibt es einen von Null verschiedenen Gitterpunkt $\gamma \in X \cap \Gamma$.

Überlegen Sie sich, dass die drei Bedingungen alle notwendig sind.

Beweis. Es genügt zu zeigen, dass $\gamma_1 \neq \gamma_2 \in \Gamma$ existieren, mit

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

Falls nämlich $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$ mit $x_1, x_2 \in X$, dann ist

$$\gamma := \gamma_1 - \gamma_2 = \frac{1}{2}(x_1 - x_2) \in X$$

da $\frac{1}{2}(x_1 - x_2)$ der Mittelpunkt der Verbindungsgerade zwischen x_1 und $-x_2$ ist.
Nehmen wir nun umgekehrt an, dass $\frac{1}{2}X + \gamma$ alle disjunkt sind. Dann gilt

$$\begin{aligned}\mathrm{vol}(\Phi) &\geq \sum_{\gamma \in \Gamma} \mathrm{vol}(\Phi \cap (\frac{1}{2}X + \gamma)) \\ &= \sum_{\gamma \in \Gamma} \mathrm{vol}((\Phi - \gamma) \cap \frac{1}{2}X) \\ &= \mathrm{vol}(\frac{1}{2}X) = 2^{-n} \,\mathrm{vol}(X).\end{aligned}$$

Dies widerspricht Bedingung 3. □

3.5 Die Endlichkeit der Klassenzahl

Die grobe Beweisidee der Endlichkeit der Klassenzahl ist:

1. Zeige, dass jedes gebrochene Ideal $\mathfrak{a}$ ein Element x enthält, so dass $N_{K|\mathbb{Q}}(x)$ "klein" ist. Daher ist das Ideal $(x)\mathfrak{a}^{-1}$ ganz und auch "klein".

2. Es gibt nur endlich viele "kleine" ganze Ideale.

Es folgt, dass sich jedes gebrochene Ideal durch ein Hauptideal von einem "kleinen" ganzen Ideal unterscheidet. Es kann also nur endlich viele Idealklassen geben.
Die "Grösse" eines Ideales wird wie folgt gemessen:

Definition 3.5.1. *Sei $\mathfrak{a} \subseteq \mathcal{O}_K$ ein Ideal. Wir definieren die* **Norm** *von $\mathfrak{a}$ durch:*

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

Lemma 3.5.2. *Es gilt:*

1. $N(\mathcal{O}_K) = 1$;
2. $N(\mathfrak{a}) \cdot N(\mathfrak{b}) = N(\mathfrak{ab})$;
3. $N((x)) = |N_{K|\mathbb{Q}}(x)|$.

Insbesondere setzt sich die Norm auf die Gruppe J_K der gebrochenen Ideale fort.

Beweis. 1. folgt aus der Definition.
2. Falls $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind, so folgt die Aussage sofort aus dem Chinesischen Restsatz. Es genügt also unter Verwendung der eindeutigen Primfaktorzerlegung

$$N(\mathfrak{p}^n) = N(\mathfrak{p})^n$$

zu zeigen. Wir haben bereits im Beweis von Satz 2.5.5 gesehen, dass in der exakten Sequenz

$$0 \longrightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1} \longrightarrow \mathcal{O}_K/\mathfrak{p}^{n+1} \longrightarrow \mathcal{O}_K/\mathfrak{p}^n \longrightarrow 0$$

der Modul $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ ein eindimensionaler $\mathcal{O}_K/\mathfrak{p}$-Vektorraum ist. Es gilt also

$$\#\mathcal{O}_K/\mathfrak{p}^{n+1} = \underbrace{\#\mathcal{O}_K/\mathfrak{p}}_{N(\mathfrak{p})} \cdot \#\mathcal{O}_K/\mathfrak{p}^n.$$

Durch Induktion folgt die Aussage.
3. Sei $\Gamma \subset \mathcal{O}_K$ irgendein freier $\mathbb{Z}$-Modul vom selben Rang n wie $\mathcal{O}_K$. Seien $x_1', \ldots, x_n'$ und $x_1, \ldots, x_n$ Basen von Γ bzw. $\mathcal{O}_K$ und sei M die (ganzzahlige) Basiswechselabbildung die $x_1', \ldots, x_n'$ in der Basis $x_1, \ldots, x_n$ ausdrückt. Dann gilt

$$[\mathcal{O}_K : \Gamma] = |\det(M)|.$$

(Dies ist ein Satz aus der elementaren Algebra. Z.B. kann man o.B.d.A. annehmen, dass M Smith-Normalform hat. Die Aussage ist dann offensichtlich.) Nun geht aber das Hauptideal (x) aus $\mathcal{O}_K$ durch Multiplikation mit x hervor. Die Determinante der Matrix der Multiplikation mit x ist aber per Definition gleich $N_{K|\mathbb{Q}}(x)$. □

Das Lemma sagt uns insbesondere, dass sich *der Betrag der Normabbildung* von K^* auf J_K fortsetzt:

$$\begin{array}{ccc} K^* & \longrightarrow & J_K \\ & \searrow^{|N_{K|\mathbb{Q}}|} & \downarrow N \\ & & \mathbb{Q}^*_{>0}. \end{array}$$

Wir möchten den Minkowskischen Gitterpunktsatz 4.1.3 auf das Gitter $\mathcal{O}_K$ (oder auch andere Ideale $\mathfrak{a} \subset \mathcal{O}_K$) in $K_\mathbb{R}$ anwenden. Dabei wählen wir auf $K_\mathbb{R}$ das in 3.3.2 konstruierte Volumen.

Lemma 3.5.3. *Sei $\mathfrak{a} \subset K$ ein gebrochenes Ideal. Dann gilt*

$$\mathrm{vol}(\mathfrak{a}) = \sqrt{|D|} \cdot N(\mathfrak{a})$$

wobei D die Diskriminante *von $\mathcal{O}_K$ ist.*

Beweis. Sei zunächst $\mathfrak{a} \subset \mathcal{O}_K$ ein ganzes Ideal. Zunächst gilt

$$\mathrm{vol}(\mathfrak{a}) = |\det(M)| \,\mathrm{vol}(\mathcal{O}_K)$$

wobei M eine Basiswechselabbildung von einer $\mathbb{Z}$-Basis von $\mathcal{O}_K$ in eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ ist. Wie wir schon im Beweis von Lemma 3.5.2 gesehen haben, gilt auch

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

Dies führt uns zurück auf den Fall $\mathfrak{a} = \mathcal{O}_K$. Sei $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$. Dann ist nach Lemma 3.3.1

$$\mathrm{vol}(\mathcal{O}_K) = \sqrt{\det(\langle x_i, x_j \rangle)_{ij}}$$

und es gilt

$$\langle x_i, x_j \rangle = \sum_j \sigma_j(x_i)\overline{\sigma_j(x_i)}$$

nach Definition des Skalarproduktes. Ähnlich wie im Beweis von Lemma 2.2.4, 4. können wir daher schreiben

$$(\langle x_i, x_j \rangle)_{ij} = {}^tA \cdot \overline{A}$$

wobei $A = (\sigma_j(x_i))_{ij}$ ist. Andererseits ist auch (siehe wiederum Beweis von Lemma 2.2.4, 4.)

$$(\mathrm{tr}_{K|Q}(x_i \cdot x_j))_{ij} = {}^tA \cdot A$$

und nach Definition ist die Diskriminante D die Determinante dieser Matrix. Es gilt also

$$\mathrm{vol}(\mathcal{O}_K) = \sqrt{\det({}^tA \cdot \overline{A})} = \sqrt{\det(A) \cdot \overline{\det(A)}} = \sqrt{|\det(A)|^2} = \sqrt{|D|}.$$

Den Fall, dass $\mathfrak{a}$ ein gebrochenes Ideal ist, lassen wir als Übung (wende das Lemma auf $m\mathfrak{a}$ an, für $m \in \mathbb{N}$ genügend gross). □

Damit können wir nun den Minkowskischen Gitterpunktsatz 4.1.3 anwenden und erhalten

Satz 3.5.4. *Jedes gebrochene Ideal $\mathfrak{a} \subseteq K$ enthält ein Element $x \neq 0$ mit*

$$|N_{K|\mathbb{Q}}(x)| \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|} \cdot N(\mathfrak{a})$$

wobei D die Diskriminante von $\mathcal{O}_K$ ist.

Beweis. Wir definieren die Menge

$$X := \{a \in K_{\mathbb{R}} \mid |a_\sigma| < C \ \forall \sigma\}$$

(dabei durchläuft $\sigma : K \to \mathbb{C}$ alle Einbettungen). Diese Menge hat das Volumen $2^r(2\pi)^s C^n$ (Übung). Falls dies grösser als $2^n \,\mathrm{vol}(\mathfrak{a})$ ist, so finden wir nach dem Minkowskischen Gitterpunktsatz 4.1.3 ein $x \in \mathfrak{a}$ mit $x \in X$. Berechne die Norm:

$$|N_{K|\mathbb{Q}}(x)| = \prod_\sigma |\sigma(x)| \leq C^n.$$

Wir können C so wählen, dass dies gerade (für beliebig kleines $\varepsilon > 0$)

$$\leq 2^{-r}(2\pi)^{-s} \cdot 2^n \,\mathrm{vol}(\mathfrak{a}) + \varepsilon,$$

ist. Da Normen ganze Zahlen sind, können wir das ε auch weglassen, und erhalten (unter Verwendung von $n = r + 2s$ und Lemma 3.5.3)

$$|N_{K|\mathbb{Q}}(x)| \leq \left(\frac{2}{\pi}\right)^s \cdot \mathrm{vol}(\mathfrak{a}) = \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|} \cdot N(\mathfrak{a}).$$

□

Aus diesem Satz können wir die Endlichkeit der Klassenzahl folgern, benötigen aber noch die Aussage, dass es nur endlich viele Ideale mit beschränkter Norm gibt:

Lemma 3.5.5. *Sei $C > 0$ eine Konstante. In $\mathcal{O}_K$ gibt es nur endlich viele (ganze) Ideale $\mathfrak{a}$ mit*

$$N(\mathfrak{a}) \leq C.$$

Beweis. Wegen der eindeutigen Primfaktorzerlegung gilt

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

und die $n_\mathfrak{p}$ sind nicht-negativ und durch $\mathfrak{a}$ eindeutig bestimmt. Nach Lemma 3.5.2 ist

$$N(\mathfrak{a}) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{n_\mathfrak{p}}.$$

Nun ist $N(\mathfrak{p})$ immer eine Potenz einer Primzahl (es ist definiert als die Anzahl der Elemente im endlichen Körper $\mathcal{O}_K/\mathfrak{p}$). Jede Primzahl p kommt aber nur für endlich viele $\mathfrak{p}$ vor (nämlich für genau diejenigen $\mathfrak{p}$, die in der Faktorisierung des Hauptideals (p) vorkommen). Es folgt, dass der Exponent $n_\mathfrak{p}$ nur für eine feste endliche Menge von Primidealen $\mathfrak{p}$ ungleich Null sein kann, und dass diese $n_\mathfrak{p}$ beschränkt sind. Es gibt also nur endlich viele Wahlen. □

Satz 3.5.6. *In $\mathcal{O}_K$ enthält jede Idealklasse ein ganzes Ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ mit Norm*

$$N(\mathfrak{b}) \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|}.$$

Beweis. Sei $\mathfrak{a}$ ein Vertreter der Idealklasse. Nach Satz 3.5.4 enthält $\mathfrak{a}^{-1}$ ein Element $x \neq 0$ mit

$$|N_{K|\mathbb{Q}}(x)| \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|} \cdot N(\mathfrak{a}^{-1}).$$

Das Ideal $\mathfrak{xb} := (x)\mathfrak{a}$ ist dann ganz (da $x \in \mathfrak{a}^{-1}$) und hat Norm

$$N((x)\mathfrak{a}) = |N_{K|\mathbb{Q}}(x)| \cdot N(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|}.$$

Ausserdem liegen natürlich $\mathfrak{a}$ und $(x)\mathfrak{a}$ in derselben Klasse. □

Korollar 3.5.7 (Kronecker)**.** *Die Klassenzahl eines Zahlkörpers ist endlich.*

Beweis. Dies folgt sofort aus Satz 3.5.6 und Lemma 3.5.5. □

Die Zahl $\left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|}$ aus dem Satz wird auch **Minkowski-Schranke**[14] genannt.
Der Beweis liefert sogar ein effektives Verfahren, um die Klassenzahl (und sogar die Klassengruppe Cl_K) eines Zahlkörpers zu bestimmen. Man muss dazu nur die endlich vielen Ideale mit $N(\mathfrak{b}) \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|}$ untersuchen. Wegen der Faktorzerlegung in Primideale gilt sogar noch stärker: Die Klassengruppe wird durch die Klassen $[\mathfrak{p}]$ erzeugt, wobei $\mathfrak{p}$ die Primideale mit $N(\mathfrak{p}) \leq \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|}$ durchläuft. Wir wollen dies an einigen Beispielen illustrieren:

Beispiel 3.5.8. *$K = \mathbb{Q}(\sqrt{2})$. Die Diskriminante ist $D = 8$. Die Minkowski-Schranke beträgt:*

$$\left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|} = \sqrt{8} \sim 2.8.$$

Also wird Cl_K durch Primideale mit Norm ≤ 2 erzeugt. Ein solches muss ein Teiler von 2 sein. Es gilt aber

$$(2) = (\sqrt{2})^2$$

Es gibt also nur ein Primideal mit Norm 2, das Hauptideal $(\sqrt{2})$. Es folgt, dass $\mathrm{Cl}_K = \{1\}$.

Beispiel 3.5.9. *$K = \mathbb{Q}(\sqrt{-14})$. Die Diskriminante ist $D = -56$. Also sind genau 2 und 7 verzweigt. Die Minkowski-Schranke beträgt:*

$$\left(\frac{2}{\pi}\right)^s \cdot \sqrt{|D|} = \frac{2}{\pi}\sqrt{56} \sim 4.764.$$

Also wird Cl_K durch Primideale mit Norm ≤ 3 erzeugt. Wir haben

$$(2) = (\sqrt{-14}, 2)^2 = \mathfrak{p}^2.$$

-14 ist ein Quadrat modulo 3, daher (siehe Satz 2.5.9):

$$(3) = (1 + \sqrt{-14}, 3)(1 - \sqrt{-14}, 3) = \mathfrak{q}\overline{\mathfrak{q}}.$$

Keines der drei Ideale kann ein Hauptideal sein, denn $N(a + b\sqrt{-14}) = a^2 + 14b^2$ kann sicher nicht 2 oder 3 werden.

[14] Man kann diese Schranke durch eine verfeinerte Analyse auf $\frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|D|}$ verbessern (siehe auch Abschnitt 4.1). Meist wird in der Literatur diese bessere Schranke als Minkowski-Schranke bezeichnet.

Um Relationen zwischen diesen Idealen zu finden, versuchen wir Elemente mit kleiner Norm zu finden, die nur durch 2 oder 3 teilbar ist.
Z.B. ist

$$N(2+\sqrt{-14}) = 4 + 14 = 18 = 9 \cdot 2$$

Da $2+\sqrt{-14}$ *offensichtlich nicht durch 3 teilbar ist, kommt nur die Faktorisierung*

$$(2+\sqrt{-14}) = (1 \pm \sqrt{-14}, 3)^2(\sqrt{-14}, 2)$$

in Frage. Es gilt also $[\mathfrak{q}]^2 = [\mathfrak{p}]$ *oder* $[\overline{\mathfrak{q}}]^2 = [\mathfrak{p}]$ *in* Cl_K *und damit beide (da die Gleichungen in* Cl_K *invers zueinander sind).*
Wir bekommen also einen surjektiven Homomorphismus,

$$\begin{array}{rcl} \mathbb{Z}/4\mathbb{Z} & \to & \mathrm{Cl}_K \\ 1 & \mapsto & [\mathfrak{q}] \end{array}$$

welcher 2 *auf* $[\mathfrak{p}]$ *und* 3 *auf* $[\overline{\mathfrak{q}}]$ *abbildet. Da keine dieser drei Idealklassen trivial ist, handelt es sich um einen Isomorphismus.*

3.6 Der multiplikative Minkowski-Raum und der Dirichletsche Einheitensatz

Unser nächstes Ziel ist es, den Dirichletschen Einheitensatz zu beweisen. Als Aufwärmbeispiel und um die Beweisstrategie zu illustrieren, wenden wir uns erneut dem Beispiel der reell quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$, $d > 0$ zu. Wir wollen mit dem Minkowskischen Gitterpunktsatz 4.1.3 erneut beweisen, dass unendlich viele Einheiten existieren. Wir haben auf Seite 16 gesehen, dass es genügt, unendlich viele Elemente $x \in \mathcal{O}_K$ zu finden, so dass $|N_{K|\mathbb{Q}}(x)| \leq C$ (für irgeneine feste Zahl $C \in \mathbb{R}$). Wir betrachten wiederum $\mathcal{O}_K$ eingebettet als Gitter in $K_{\mathbb{R}}$. Letzterer ist in diesem Fall isomorph zu $\mathbb{R}^2$ und die Einbettung sieht wie folgt aus

$$\begin{array}{rcl} \mathcal{O}_K & \hookrightarrow & \mathbb{R}^2, \\ x & \mapsto & \begin{pmatrix} \sigma_1(x) \\ \sigma_2(x) \end{pmatrix}. \end{array}$$

Dabei ist σ_1 die reelle Einbettung, welche durch $\sqrt{d} \mapsto \sqrt{d}$ gegeben ist und σ_2 die Einbettung, welche durch $\sqrt{d} \mapsto -\sqrt{d}$ gegeben ist. Schreibe $C = C_1 \cdot C_2$ für irgendwelche Zahlen C_1 und C_2 und betrachte das Rechteck:

$$X := \{\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \in \mathbb{R}^2 \mid |a_1| \leq C_1 \ |a_2| \leq C_2\}.$$

Dieses hat Volumen $4C$. Falls $4C > 4\sqrt{|D|} = 4\,\mathrm{vol}(\mathcal{O}_K)$, finden wir also nach dem Minkowskischen Gitterpunktsatz 4.1.3 ein $x \in \mathcal{O}_K \cap X$, welches nicht Null ist. Es ergibt sich

$$|N_{K|\mathbb{Q}}(x)| = |\sigma_1(x)| \cdot |\sigma_2(x)| \leq C_1 \cdot C_2 = C.$$

Wir haben also *ein* Element mit Norm $\leq C$ gefunden. Es ist dafür $|\sigma_1(x)| \leq C_1$. Wähle nun $0 < C_1' < |\sigma_1(x)|$ und $C_2' := C/C_1'$. Wiederum finden wir ein Element $x' \neq 0$ mit Norm $\leq C$, welches wegen $|\sigma_1(x')| \leq C_1' < |\sigma_1(x)|$ ungleich x ist. Induktiv finden wir so die gewünschte unendliche Menge von Elementen $x \in \mathcal{O}_K$ mit $|N_{K|\mathbb{Q}}(x)| \leq C$.
Der Dirichletsche Einheitensatz besagt allerdings nicht nur, dass unendlich viele Einheiten existieren, sondern gibt darüberhinaus Auskunft über den genauen Rang von $\mathcal{O}_K^*$ als $\mathbb{Z}$-Modul. Sein Beweis ist im Prinzip analog, erfordert aber eine etwas genauere Analyse der Situation.

Satz 3.6.1 (Dirichletscher Einheitensatz)**.** *Sei K ein Zahlkörper, r die Anzahl der reellen Einbettungen und s die Anzahl der Paare komplex konjugierter Einbettungen nach $\mathbb{C}$. Dann gilt*

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

wobei μ_K die (endlich zyklische) Gruppe der Einheitswurzeln in K ist.

Für reell quadratische Körper ist $r = 2$ und $s = 0$. Es ergibt sich also

$$\mathcal{O}_K^* \cong \{\pm 1\} \times \mathbb{Z}.$$

Mit anderen Worten finden wir eine Einheit $\varepsilon \in \mathcal{O}_K^*$ (die sogenannte **Grundeinheit**) so dass jede Einheit von der Form

$$\pm\varepsilon^n$$

für ein $n \in \mathbb{Z}$ ist.
Die Beweisstrategie für den Dirichletschen Einheitensatz besteht darin, zu zeigen, dass $\mathcal{O}_K^*/\mu_K$ (als *multiplikative* Gruppe!) ein vollständiges Gitter in einem Vektorraum der Dimension $r + s - 1$ ist.
Um von der additiven Gruppe in $K_\mathbb{R}$ auf eine multiplikative überzugehen, betrachten wir die Abbildung

$$\begin{array}{rcl} l : K_{\mathbb{R}}^* & \to & \mathbb{R}^{r+s} \\ \begin{pmatrix} a_{\tau_1} \\ \cdots \\ a_{\tau_r} \\ \hline a_{\sigma_1} \\ \cdots \\ a_{\sigma_s} \end{pmatrix} & \mapsto & \begin{pmatrix} \log|a_{\tau_1}| \\ \cdots \\ \log|a_{\tau_r}| \\ \hline \log|a_{\sigma_1}|^2 \\ \cdots \\ \log|a_{\sigma_s}|^2 \end{pmatrix} \end{array}$$

Dabei ist $K_{\mathbb{R}}^*$ die Teilmenge von $K_{\mathbb{R}}$, in der alle Koordinaten ungleich 0 sind. Sie trägt eine Gruppenstruktur, in der einfach die Einträge multipliziert werden. Die Abbildung l ist ein Gruppenhomomorphismus.
Da $\mathcal{O}_K^* \subset K_{\mathbb{R}}^*$, bekommen wir auch einen Gruppenhomomorphismus

$$l : \mathcal{O}_K^* \to \mathbb{R}^{r+s}.$$

Wir überlegen uns zunächst

1. Der Kern von l (eingeschränkt auf $\mathcal{O}_K^*$) besteht gerade aus der Gruppe μ_K der Einheitswurzeln in K.

2. $l(\mathcal{O}_K^*)$ ist enthalten im Unterraum

$$H := \{v \in \mathbb{R}^{r+s} \mid \sum v_{\tau_i} + \sum v_{\sigma_i} = 0\}.$$

   Dieser Raum hat offensichtlich die Dimension $r + s - 1$.

Beweis. 1. Sei $x \in \mathcal{O}_K^*$ so, dass $l(x) = 0$. D.h. $\log|\sigma| = 0$ für alle Einbettungen σ (reelle und komplexe!), oder äquivalent $|\sigma(x)| = 1$ für alle Einbettungen σ. Betrachte die Potenzen $1, x, x^2, \ldots$. Sie erfüllen alle $|\sigma(x^n)| = 1$ für alle Einbettungen. Dies bedeutet aber, dass $1, x, x^2, \ldots$ alle im kompakten Bereich

$$X = \{ \begin{pmatrix} a_{\tau_1} \\ \cdots \\ a_{\tau_r} \\ \hline a_{\sigma_1} \\ \cdots \\ a_{\sigma_s} \end{pmatrix} \in K_{\mathbb{R}} \mid |a_{\tau_i}| \leq 1 \ |a_{\sigma_i}| \leq 1 \ \}$$

von $K_{\mathbb{R}}$ liegen. Hierin können sich sich nur endlich viele Elemente von $\mathcal{O}_K$ befinden, da $\mathcal{O}_K$ darin ein Gitter bildet, x muss also eine Einheitswurzel

sein. Umgekehrt ist es klar, dass eine Einheitswurzel $|\sigma(x)| = 1$ für alle Einbettungen erfüllt.
2. Wir haben gesehen, dass für Einheiten $x \in \mathcal{O}_K^*$ gilt: $N_{K|\mathbb{Q}}(x) = \pm 1$. Es gilt also

$$\prod_{i=1}^{r} |\tau_i(x)| \cdot \prod_{i=1}^{s} |\sigma_i(x)|^2 = 1.$$

Anwenden des Logarithmus ergibt:

$$\sum_{i=1}^{r} \log |\tau_i(x)| + \sum_{i=1}^{s} \log |\sigma_i(x)|^2 = 0.$$

$l(x)$ liegt also in H. □

Satz 3.6.2. *$l(\mathcal{O}_K^*)$ bildet ein vollständiges Gitter in H.*

Wir wollen uns zunächst überlegen, dass hieraus der Dirichletsche Einheitensatz folgt:

Beweis von Satz 3.6.1. Wir haben gesehen, dass l den Kern μ_K hat. Wenn das Bild von l ein vollständiges Gitter in H bildet, heisst dies, dass $l(\mathcal{O}_K^*) \cong \mathbb{Z}^{r+s-1}$ ($r+s-1$ ist die Dimension von H). Wir bekommen also eine exakte Sequenz

$$1 \longrightarrow \mu_K \longrightarrow \mathcal{O}_K^* \xrightarrow{l} \mathbb{Z}^{r+s-1} \longrightarrow 0$$

Daraus folgt aber sofort (Übung) $\mathcal{O}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$, da $\mathbb{Z}^{r+s-1}$ eine *freie* Abelsche Gruppe ist. □

Wir benötigen noch ein Lemma, das analog ist zu den Überlegungen auf Seite 16 für reell quadratische Körper, für das wir allerdings jetzt einen verständlicheren Beweis zur Verfügung haben:

Lemma 3.6.3. *Sei $C > 0$ eine Konstante. Bis auf Multiplikation mit Einheiten gibt es nur endlich viele Elemente $x \in \mathcal{O}_K$ mit beschränkter Norm $|N_{K|\mathbb{Q}}(x)| \leq C$.*

Beweis. x und x' stimmen genau dann bis auf Multiplikation mit einer Einheit überein, wenn $(x) = (x')$. Wir haben aber in Lemma 3.5.5 gesehen, dass nur endlich viele Ideale mit beschränkter Norm existieren. □

Wir benötigen zum Beweis von Satz 3.6.2 eine Vorbereitung.

3.6.4. Wähle eine reelle Konstante $C > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$. Nach den Lemma gibt es eine endliche Menge $\{x_1, \ldots, x_k\} \subset \mathcal{O}_K \setminus \{0\}$ so dass gilt:
Für $x \in \mathcal{O}_K \setminus \{0\}$ mit $|N_{K|\mathbb{Q}}(x)| < C$ gibt es eine Einheit ε und i so dass

$$x = \varepsilon \cdot x_i.$$

3.6.5. Wir betrachten Tupel positiver reeller positiver Zahlen

$$c = (c_{\tau_1}, \ldots, c_{\tau_r}, c_{\sigma_1}, \ldots, c_{\sigma_s})$$

mit

$$\prod c_{\tau_i} \cdot \prod c_{\sigma_i}^2 = C$$

und betrachten die Menge (ganz analog zu dem Quadrat, dass wir im Fall der reell quadratischen Körper betrachtet haben):

$$X_c := \{ \left(\begin{array}{c} a_{\tau_1} \\ \cdots \\ a_{\tau_r} \\ \hline a_{\sigma_1} \\ \cdots \\ a_{\sigma_s} \end{array}\right) \in K_{\mathbb{R}} \mid \ |a_{\tau_i}| < c_{\tau_i},\ |a_{\sigma_i}| < c_{\sigma_i} \ \}.$$

Diese hat Volumen $\mathrm{vol}(X_c) = 2^r(2\pi)^s C$. Da $C > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$ gilt: $\mathrm{vol}(X_c) = 2^r(2\pi)^s C > 2^n \sqrt{|D|} = 2^n \,\mathrm{vol}(\mathcal{O}_K)$. Nach dem Minkowskischen Gitterpunktsatz 4.1.3 gibt es also ein Element $x \in \mathcal{O}_K \cap X_c$ ungleich Null und nach Konstruktion von X_c gilt $|N_{K|\mathbb{Q}}(x)| \leq C$. Es gibt daher, wie wir uns überlegt haben, eine Einheit ε und i so, dass $x = \varepsilon \cdot x_i$.

Beweis von Satz 3.6.2. Um zu zeigen, dass $l(\mathcal{O}_K^*)$ ein Gitter ist, reicht es zu begründen, dass es diskret ist. Es genügt hierzu eine offene Umgebung von $0 \in \mathbb{R}^{r+s}$ anzugeben, so dass $l(\mathcal{O}_K^*) \cap Y = \{0\}$. Betrachte ein $c > 0$ und die offene Menge

$$Y := \{v \in \mathbb{R}^{r+s} \mid |v_{\tau_i}| < c,\ |v_{\sigma_i}| < c\}.$$

Das Urbild von Y in $K_{\mathbb{R}}^*$ unter l ist die Menge

$$l^{-1}(Y) = \{ \left(\begin{array}{c} a_{\tau_1} \\ \cdots \\ a_{\tau_r} \\ \hline a_{\sigma_1} \\ \cdots \\ a_{\sigma_s} \end{array}\right) \in K_{\mathbb{R}} \mid e^{-c} < \ |a_{\tau_i}| < e^c,\ e^{-c} < |a_{\sigma_i}|^2 < e^c \ \}.$$

Dies ist ebenfalls eine beschränkte Menge, in der deshalb nur endlich viele Elemente des Gitters $\mathcal{O}_K$ liegen, und daher erst recht nur endlich viele Einheiten. Daher enthält auch der Schnitt $l(\mathcal{O}_K^*) \cap X$ nur endlich viele Elemente. Wir können daher c so klein wählen, dass nur noch 0 in $X \cap l(\mathcal{O}_K^*)$ liegt. $l(\mathcal{O}_K^*)$ ist also in der Tat ein Gitter.
$l(\mathcal{O}_K^*)$ ist genau dann vollständig, wenn wir eine *beschränkte* Menge $Y \subset H$ finden können, so dass

$$H = \bigcup_{\varepsilon \in \mathcal{O}_K^*} l(\varepsilon) + Y. \tag{10}$$

Betrachte die Menge

$$Y := \bigcup_{i=1}^{k} (l(X_c) - l(x_i)) \cap H$$

wobei die x_i in 3.6.4 gewählt wurden.
Behauptung: 1. Y ist beschränkt und 2. Y erfüllt (10). Daraus folgt, wie wir gesehen haben, der Satz.
Beweis der Behauptung:
1. Es gilt offensichtlich:

$$l(X_c) - l(x_i) \subset \{y \in \mathbb{R}^{r+s} \mid y_j < R \ \forall j\}.$$

für ein $R \in \mathbb{R}$. Die Einträge y_j können hier zwar beliebig negativ werden, aber unter der Bedingung $y \in H$ folgt auch, dass $y_j > -(r+s)R$ für alle j. Die Menge $(l(X_c) - l(x_i)) \cap H$ ist also beschränkt und damit auch Y.
2. Sei nun $v \in H$ beliebig und e^v ein Urbild in $K_{\mathbb{R}}^*$ unter l. Es gilt nun

$$X_c = e^v \cdot X_{c'}$$

für $c'_{\tau_i} = e^{-v_{\tau_i}} c_{\tau_i}$ und $c'_{\sigma_i} = e^{-\frac{1}{2} v_{\sigma_i}} c_{\sigma_i}$ und wegen $v \in H$ gilt dann immer noch

$$\prod c'_{\tau_i} \cdot \prod (c'_{\sigma_i})^2 = C.$$

Nach den Überlegungen in 3.6.5 finden wir also ein $x \in \mathcal{O}_K \cap X_{c'}$ mit $x = \varepsilon \cdot x_i$ für eine Einheit ε, also:

$$\varepsilon \cdot x_i \in (e^v)^{-1} \cdot X_c.$$

Anwenden von l ergibt:

$$l(\varepsilon) + l(x_i) \in -v + l(X_c)$$

oder

$$v \in l(\varepsilon^{-1}) + l(X_c) - l(x_i).$$

und da $v \in H$ und $l(\varepsilon^{-1}) \in H$ auch:

$$v \in l(\varepsilon^{-1}) + Y.$$

Y erfüllt also in der Tat (10). □

4 Mehr über Verzweigung und Zerlegung

4.1 Die Sätze von Hermite und Minkowski

Wir haben bereits im Fall der quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ diskutiert, dass die Verzweigung (also die Information darüber, welche Primzahlen p in $\mathcal{O}_K$ verzweigt sind) einiges über K aussagt. Z.B. ist, wie wir gesehen haben, jeder quadratische Zahlkörper mindestens an einer Primzahl verzweigt und $\mathbb{Q}(\sqrt{d})$ lässt sich *fast* aus dieser Information rekonstruieren. Wir haben für quadratische Zahlkörper auch gesehen, dass eine Primzahl genau dann verzweigt, wenn sie die Diskriminante teilt. Dies soll hier auf beliebige Zahlköper verallgemeinert werden:

Satz 4.1.1. *Eine Primzahl p ist genau dann in $\mathcal{O}_K$ verzweigt, wenn $p|D$.*

Ausserdem werden wir die folgenden wichtigen Sätze beweisen.

Satz 4.1.2 (Hermite)**.** *Sei $C > 0$ gegeben. Dann gibt es nur endlich viele Zahlkörper K mit*

$$|D_K| < C.$$

Satz 4.1.3 (Minkowski)**.** *Es gibt keine Zahlkörper, für die alle Primzahlen unverzweigt sind.*

Der Satz von Minkowski verallgemeinert sich *nicht* auf Körpererweiterungen $L|K$ zwischen Zahlkörpern. Es gibt sehr wohl solche Erweiterungen in denen alle Primideale $\mathfrak{p}$ von $\mathcal{O}_K$ in $\mathcal{O}_L$ unverweigt sind. Allerdings kann man zeigen (dies ist Teil der Klassenkörpertheorie), dass es nur endlich viele solche Erweiterungen gibt, die *Abelsch* sind. In der Tat gibt es eine maximale solche, den sogenannten Hilbertschen Klassenkörper $H|K$, für dessen Galoisgruppe überraschenderweise

$$\mathrm{Gal}(H|K) \cong \mathrm{Cl}_K$$

gilt. Inbesondere gibt es, wie für $K = \mathbb{Q}$, keine *Abelschen* überall unverzweigten Erweiterungen, wenn K Klassenzahl eins hat. Allerdings kann es auch in diesen Fällen nicht Abelsche überall unverzweigte Erweiterungen geben. Im Hilbertschen Klassenkörper H ist ein Primideal $\mathfrak{p}$ von K genau dann voll-zerlegt, wenn es ein Hauptideal ist.

Beweis von Satz 4.1.1. Der Beweis ist einfacher, wenn wir $\mathcal{O}_K = \mathbb{Z}[\omega]$ annehmen, es also eine Ganzheitsbasis der Form $1, \omega, \omega^2, \ldots, \omega^{n-1}$ gibt. Dann haben wir im Beweis von Lemma 2.2.4, 4. die Gleichung

$$D = \prod_{i \neq j} (\sigma_i(\Omega) - \sigma_j(\Omega))$$

bewiesen, wobei die σ_i alle Einbettungen von K in einen fest gewählten algebraischen Abschluss von $\mathbb{Q}$ durchlaufen (davon gibt es genau n). Es reicht, die Einbettungen in die Galoissche Hülle L von K darin zu betrachten. Auf der anderen Seite wissen wir (Satz 2.5.6) dass die Zerlegung von p

$$(p) = \prod_i \mathfrak{p}_i^{e_i}$$

der Zerlegung modulo p des normierten Minimalpolynoms $q \in \mathbb{Z}[x]$ von ω entspricht:

$$q \equiv \prod_i q_i^{e_i} \pmod{p}.$$

Wähle nun ein Primideal $\mathfrak{P}$ über p in $\mathcal{O}_L$. (L war die Galoissche Hülle von K). Das Polynom q zerfällt dann modulo $\mathfrak{P}$ in Linearfaktoren und die Nullstellen sind gerade die Reduktionen der $\sigma_i(\Omega)$ modulo $\mathfrak{P}$. Die Diskriminante ist also genau dann 0 modulo $\mathfrak{P}$, wenn in q modulo $\mathfrak{P}$ keine mehrfachen Nullstellen vorkommen. Da endliche Körper separabel sind, ist dies gleichbedeutend damit, dass in q modulo p keine mehrfachen Faktoren vorkommen. Da die Diskriminante in $\mathbb{Z}$ liegt, ist sie darüberhinaus 0 modulo $\mathfrak{P}$ genau dann, wenn sie 0 modulo (p) ist, da $\mathfrak{P} \cap \mathbb{Z} = (p)$. □

Wir geben nun einen zweiten Beweis, für den wir die Annahme $\mathcal{O}_K = \mathbb{Z}[\omega]$ nicht benötigen, der aber etwas technischer ist. Wir brauchen einige Vorbereitungen:

4.1.4. Sei R ein Ring und S eine R-Algebra, welche frei von endlichem Rang als R-Modul ist. Dann können wir auf S immer eine Spurpaarung nach R definieren durch

$$\langle x, y \rangle_{S|R} := \mathrm{tr}_{S|R}(x \cdot y)$$

wobei die Spur $\mathrm{tr}_{S|R}(\alpha)$ als die Spur der Matrix der Multiplikation mit α bedeutet. Beachte, dass dies sinnvoll ist, da S ein freier R-Modul ist und wir daher jede R-lineare Abbildung in eine Matrix entwickeln können. Ferner ist die Spur nicht von der Basiswahl abhängig.

4.1.5. Betrachte nun $\mathcal{O}_K$ als freien $\mathbb{Z}$-Modul. Wir haben dann

$$\langle x, y\rangle_{\mathcal{O}_K|\mathbb{Z}} \equiv \langle \overline{x}, \overline{y}\rangle_{\mathcal{O}_K/(p)|\mathbb{F}_p} \pmod{p}.$$

Wir lassen die Verifikation als Übung. Beachte, dass $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul vom Rang n ist und ebenso $\mathcal{O}_K/(p)$ ein freier $\mathbb{F}_p$-Modul (=$\mathbb{F}_p$-Vektorraum) vom Rang n. Man kann sogar als Basis für letzteren die Reduktion einer Basis von $\mathcal{O}_K$ als $\mathbb{Z}$-Modul nehmen.

4.1.6. Falls $S = S_1 \times \cdots \times S_n$ ein endliches Produkt von $\mathbb{F}_p$-Algebren ist, und S ein endlicher $\mathbb{F}_p$-VR ist, dann gilt:

$$\langle x, y\rangle_{S|\mathbb{F}_p} = \sum_i \langle x_i, y_i\rangle_{S_i|\mathbb{F}_p}.$$

Insbesondere ist $\langle -, -\rangle_{S|\mathbb{F}_p}$ genau dann nicht ausgeartet, wenn alle $\langle -, -\rangle_{S_i|\mathbb{F}_p}$ nicht ausgeartet sind.

Zweiter Beweis von Satz 4.1.1. Nach 4.1.5 gilt

$$p|D \;\Leftrightarrow\; \langle -, -\rangle_{\mathcal{O}_K/(p)|\mathbb{F}_p} \text{ nicht ausgeartet.}$$

Sei

$$(p) = \prod_i \mathfrak{p}_i^{e_i}$$

die Faktorzerlegung von (p) in Primideale. Nach dem Chinesischen Restsatz gilt dann

$$\mathcal{O}_K/(p) = \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_k^{e_k}.$$

Und nach 4.1.6 ist $\langle -, -\rangle_{\mathcal{O}_K/(p)|\mathbb{F}_p}$ nicht ausgeartet, genau dann wenn alle $\langle -, -\rangle_{\mathcal{O}_K/\mathfrak{p}_i^{e_i}|\mathbb{F}_p}$ nicht ausgeartet sind. Die Aussage des Satzes folgt also aus den beiden folgenden Behauptungen:

1. $\langle -, -\rangle_{\mathcal{O}_K/\mathfrak{p}_i|\mathbb{F}_p}$ nicht ausgeartet,
2. $\langle -, -\rangle_{\mathcal{O}_K/\mathfrak{p}_i^{e_i}|\mathbb{F}_p}$ ausgeartet, falls $e_i > 1$.

1. folgt aus Lemma 2.2.4, 4., da ein endlicher Körper separabel ist. 2. Falls $e_i > 1$ gibt es in $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ (mindestens) ein nilpotentes Element x. Dann ist auch $x \cdot y$ nilpotent für alle y. Ebenso ist jede Matrix, die die Multiplikation mit $x \cdot y$ darstellt, nilpotent. Die Spur einer nilpotenten Matrix ist 0. D.h. das Element x erfüllt

$$\langle x, y\rangle_{\mathcal{O}_K/\mathfrak{p}_i^{e_i}|\mathbb{F}_p} = 0 \qquad \text{für alle } y.$$

Die Form ist also ausgeartet. □

Um die Sätze von Hermite und Minkowski beweisen zu können, benötigen wir eine Verschärfung von Satz 3.5.6:

Satz 4.1.7. *In $\mathcal{O}_K$ enthält jede Idealklasse ein ganzes Ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ mit Norm*

$$N(\mathfrak{b}) \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|D|}.$$

Beweis. Wenn wir uns anschauen, wie Satz 3.5.6 bewiesen wurde, reicht es zu zeigen, dass jedes (gebrochene) Ideal $\mathfrak{a}$ ein Element mit Norm

$$|N_{K|\mathbb{Q}}(x)| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|D|} \cdot N(\mathfrak{a})$$

enthält. Bisher hatten wir in $K_\mathbb{R}$ die Menge

$$X := \{a \in K_\mathbb{R} \mid |a_\sigma| < C \ \forall \sigma\}$$

mit Volumen $2^r(2\pi)^s C^n$ betrachtet. Wir betrachten nun stattdessen die Menge

$$X' := \{a \in K_\mathbb{R} \mid \sum_\sigma |a_\sigma| < C\}.$$

Wir lassen als (nicht ganz einfache) Übung zu verifizieren, dass diese das Volumen $2^r \pi^s \frac{C^n}{n!}$ hat. Um den Minkowskischen Gitterpunktsatz anwenden zu können, muss

$$\mathrm{vol}(X') = 2^r \cdot \pi^s \cdot \frac{C^n}{n!} > 2^n \cdot \mathrm{vol}(\mathfrak{a}) = 2^n \cdot \sqrt{|D|} \cdot N(\mathfrak{a})$$

sein, also

$$C^n > n! \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|D|} \cdot N(\mathfrak{a}).$$

Wähle C so, dass

$$C^n = n! \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|D|} \cdot N(\mathfrak{a}) + \varepsilon.$$

Unter dieser Bedingung finden wir ein Element $x \in \mathfrak{a}$ ungleich 0, welches in X' liegt. Um die Norm von x abzuschätzen, bedienen wir uns der Ungleichung zwischen arithmetischem und geometrischem Mittel:

$$\sqrt[n]{|N_{K|\mathbb{Q}}(x)|} = \sqrt[n]{\prod_\sigma |\sigma(x)|} \leq \frac{1}{n} \sum_\sigma |\sigma(x)|$$

Da $\sum_\sigma |\sigma(x)| < C$, nach Definition von X', gilt:

$$|N_{K|\mathbb{Q}}(x)| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|D|} \cdot N(\mathfrak{a}) + \varepsilon$$

Da Normen von Elementen von $\mathfrak{a}$ diskrete Werte annehmen, können wir wiederum das ε auch weglassen. □

Wir können damit den Satz von Minkowski folgern:

Beweis von Satz 4.1.3. Da die Norm eines Ideals immer grösser gleich 1 ist, folgt aus Satz 4.1.7, dass

$$\frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{n/2} \cdot \sqrt{|D|} \geq 1,$$

(wobei noch $n \geq 2s$ benutzt wurde) also

$$\sqrt{|D|} \geq \frac{n^n}{n!} \cdot \left(\frac{\pi}{4}\right)^{n/2}.$$

Behauptung: Die rechte Seite ist stets > 1, falls $n > 1$.
Daraus folgt dass es keine Zahlkörper mit Diskriminante ± 1 geben kann und daher nach Satz 4.1.1 keine an allen Primzahlen unverzweigten Erweiterungen von $\mathbb{Q}$.
Beweis der Behauptung: Bezeichne die rechte Seite mit a_n. Es gilt

$$a_2 = \frac{\pi}{2} > 1.$$

Ausserdem ist für $n > 1$

$$\frac{a_{n+1}}{a_n} = \frac{\frac{(n+1)^{n+1}}{(n+1)n!}}{\frac{n^n}{n!}} \cdot \sqrt{\frac{\pi}{4}} = \left(1 + \frac{1}{n}\right)^n \sqrt{\frac{\pi}{4}} > 1$$

da $\left(1 + \frac{1}{n}\right)^n$ monoton steigend ist und für $n = 2$ gleich $\frac{9}{4} > 2$. □

Aus dem Beweis können wir entnehmen, dass die Diskriminante mit dem Körpergrad gegen unendlich geht. Dass heisst umgekehrt für einen Körper mit beschränkter Diskriminante muss auch der Grad beschränkt sein. Dies benutzen wir, um den Satz von Hermite zu beweisen:

Beweis von Satz 4.1.2. Es genügt also zu beweisen, dass es nur endlich viele Zahlkörper K mit gegebenem Grad n und gegebener Diskriminante D gibt. Dazu machen wir eine Fallunterscheidung:
Fall I: K hat eine reelle Einbettung τ_1: Betrachte dann in $K_\mathbb{R}$ die Menge

$$X := \{ \left(\begin{array}{c} a_{\tau_1} \\ \cdots \\ a_{\tau_r} \\ \hline a_{\sigma_1} \\ \cdots \\ a_{\sigma_s} \end{array}\right) \in K_\mathbb{R} \mid \ |a_{\tau_1}| < C, \ |a_\kappa| < 1 \ \forall \kappa \neq \tau_1 \ \}.$$

Dabei ist C irgendeine fest gewählte Konstante, κ durchläuft die restlichen Einbettungen ungleich τ_1. Falls $\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\mathcal{O}_K) = 2^n \sqrt{|D|}$ ist, gibt es also einen Gitterpunkt $x \in \mathcal{O}_K$ mit $x \in X$. Beachte: Dazu müssen wir nur C gross genug machen, relativ zu n und D, also *unabhängig* von K!
Dann gilt $|\tau_1(x)| \geq 1$, denn aus $|\kappa(x)| < 1$ für alle Einbettungen κ würde $|N_{K|\mathbb{Q}}(x)| < 1$ folgen, was Unsinn ist. Daher muss x ein primitives Element sein, d.h. $K = \mathbb{Q}(x)$. Ansonsten gäbe es eine andere Fortsetzung κ von $\tau_1|_{\mathbb{Q}(x)}$ mit $\kappa(x) = \tau_1(x)$ im Widerspruch zu $|\kappa(\alpha)| < 1$. Das Minimalpolynom $q \in \mathbb{Z}[X]$ von x bestimmt also K (da $K = \mathbb{Q}(x)$), hat Grad n und aus $x \in X$ folgt, dass die Koeffizienten von q nur in Abhängigkeit von C beschränkt sind. Da sie darüberhinaus ganze Zahlen sind (x ist ganz) gibt es nur endlich viele Möglichkeiten für q.
Fall II: K hat nur komplexe Einbettungen: Betrachte dann in $K_\mathbb{R}$ die Menge

$$X := \{ \begin{pmatrix} a_{\sigma_1} \\ \cdots \\ a_{\sigma_s} \end{pmatrix} \in K_\mathbb{R} \mid \ |\Im a_{\sigma_1}| < C, \ |\Re a_{\sigma_1}| < 1, \ \ |a_\kappa| < 1 \ \forall \kappa \neq \sigma_1 \ \}.$$

Der Beweis funktioniert dann genauso wie für Fall I. Beachte, dass für $x \in X \cap \mathcal{O}_K$ gelten muss: $\Im\sigma_1(x) \neq 0$, also sind auch $\sigma_1(x)$ und $\overline{\sigma_1}(x)$ verschieden. □

4.2 Hilbertsche Verzweigungstheorie

Sie $L|K$ eine Galoiserweiterung und $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Schon im Beweis des quadratischen Reziprozitätsgesetzes wurde verwendet, dass die Galoisgruppe $G := \mathrm{Gal}(L|K)$ transitiv auf den Primidealen $\mathfrak{P}_i$ operiert (siehe Lemma 2.5.11), welche in der Faktorzerlegung in Primideale von $\mathcal{O}_L$

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}$$

vorkommen. (Beachte: dies sind genau die Primideale $\mathfrak{P}$ von $\mathcal{O}_L$, welche "über $\mathfrak{p}$ liegen", d.h. für die $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ gilt.) Daraus folgt sofort, dass alle e_i übereinstimmen müssen $e := e_1 = \cdots = e_k$ und dass wir einen Isomorphismus

$$\begin{array}{rcl} G_{\mathfrak{P}_i} \backslash G & \cong & \{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\} \\ G_{\mathfrak{P}_i} \cdot \sigma & \mapsto & \sigma(\mathfrak{P}_i) \end{array}$$

haben (für alle i). Dabei ist $G_{\mathfrak{P}_i}$ der Stabilisator von $\mathfrak{P}_i$, also die Menge der K-Automorphismen von L, die $\mathfrak{P}_i$ als Menge festhalten:

$$G_{\mathfrak{P}_i} := \{\sigma \in G \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}.$$

Aus der Transitivität folgt sofort, dass für zwei Primideale $\mathfrak{P}_i$ und $\mathfrak{P}_j$, welche über $\mathfrak{p}$ liegen, ein $\sigma \in G$ existiert, so dass

$$G_{\mathfrak{P}_i} = \sigma^{-1} \cdot G_{\mathfrak{P}_j} \cdot \sigma.$$

Alle $G_{\mathfrak{P}_i}$ sind also zueinander konjugierte Untergruppen von G. Falls G sogar Abelsch ist, sind sie daher alle gleich.
Nicht nur die Verzweigungsindizes, sondern auch die Trägheitsgrade der $\mathfrak{P}_i$ stimmen überein, $f := f_1 = \cdots = f_k$, denn für ein σ mit $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$ definiert

$$\begin{array}{rcl} \mathcal{O}_L/\mathfrak{P}_i & \to & \mathcal{O}_L/\mathfrak{P}_j \\ x & \mapsto & \sigma(x) \end{array} \tag{11}$$

einen Isomorphismus von endlichen Körpern. (Erinnere, f_i wurde definiert als der Körpergrad $[\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.) Die wichtige Formel aus Satz 2.5.5 reduziert sich also im Galoisfall zu

$$n = e \cdot f \cdot k$$

und daher ist $\#G_{\mathfrak{P}} = \frac{n}{k} = e \cdot f$.
Nach Galoistheorie entsprechen nun die Untergruppen von G gerade den Zwischenkörpern von $L|K$.

Definition 4.2.1. *Die Untergruppe $G_{\mathfrak{P}}$ heisst die* **Zerlegungsgruppe** *von $\mathfrak{P}$ und der Fixkörper $Z_{\mathfrak{P}}$ heisst der* **Zerlegungskörper** *von $\mathfrak{P}$.*

Es folgt:

$$\begin{array}{rcccl} G_{\mathfrak{P}} = \{1\} & \Leftrightarrow & Z_{\mathfrak{P}} = L & \Leftrightarrow & \mathfrak{p} \text{ voll-zerlegt} \\ G_{\mathfrak{P}} = G & \Leftrightarrow & Z_{\mathfrak{P}} = K & \Leftrightarrow & \mathfrak{p} \text{ unzerlegt (d.h. } k = 1) \end{array}$$

Für jedes $\mathfrak{P}$ über $\mathfrak{p}$ bekommen wir einen Homomorphismus

$$G_{\mathfrak{P}} \quad \to \quad \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p}) \tag{12}$$

wobei das Bild eines σ wie in (11) definiert wird.

Lemma 4.2.2. *Der Homomorphismus (12) ist surjektiv.*

Beweis. Sei ω ein primitives Element von $L|K$, welches wir o.B.d.A. als ganz annehmen können. Das Minimalpolynom q von ω faktorisiert in L in Linearfaktoren:

$$q = \prod_{i=1}^{n}(X - \omega_i)$$

mit $\omega_1 = \omega$ und mit $\omega_i \in \mathcal{O}_L$. Betrachte nun die Reduktion dieser Gleichung modulo $\mathfrak{P}$:

$$\overline{q} \equiv \prod_{i=1}^{n}(X - \overline{\omega_i}) \qquad (\mathrm{mod}\ \mathfrak{P})$$

Die Erweiterung $\mathcal{O}_L/\mathfrak{P}$ wird über $\mathcal{O}_K/\mathfrak{p}$ durch $\overline{\omega}$ erzeugt. Das Minimalpolynom von $\overline{\omega}$ ist ein Teiler von $\overline{q}$. Jeder Galoisautomorphismus $\overline{\sigma}$ der Erweiterung $\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p}$ muss $\overline{\omega}$ offensichtlich auf eine andere Nullstelle dieses Minimalpolynoms abbilden (und ist dadurch eindeutig festgelegt). Diese Nullstellen sind aber auch Nullstellen von $\overline{q}$ und daher ist $\overline{\sigma}(\overline{\omega}) = \overline{\omega_i}$ für ein i. Nun gibt es aber auch einen Galoisautomorphismus σ von $L|K$, welcher ω auf ω_i abbildet. Es ist klar, dass die Reduktion von diesem σ gleich $\overline{\sigma}$ ist. □

Definition 4.2.3. *Der Kern des Homomorphismus (12) wird mit $I_{\mathfrak{P}}$ bezeichnet und* **Trägheitsgruppe** *von $\mathfrak{P}$ genannt.*
Der Fixkörper $T_{\mathfrak{P}}$ heisst der **Trägheitskörper** *von $\mathfrak{P}$.*

Wir haben also das folgendende Diagramm von Untergruppen mit zugehörigen Fixkörpern und Graden

$$\begin{array}{cc} L & \{1\} \\ {\scriptstyle e}\big| & \big| \\ T_{\mathfrak{P}} & I_{\mathfrak{P}} \\ {\scriptstyle f}\big| & \big| \\ Z_{\mathfrak{P}} & G_{\mathfrak{P}} \\ {\scriptstyle k}\big| & \big| \\ K & G \end{array}$$

und nach dem Lemma gilt, dass $Z_{\mathfrak{P}}|T_{\mathfrak{P}}$ ebenfalls Galoissch (sogar zyklisch) ist mit

$$\mathrm{Gal}(Z_{\mathfrak{P}}|T_{\mathfrak{P}}) \cong G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p}).$$

Die Gleichheit $[L|T_{\mathfrak{P}}] = \#I_{\mathfrak{P}} = e$ folgt aus der Gleichung $n = efk$ und der Multiplikativität der Körpergrade. Insbesondere gilt:

$$I_{\mathfrak{P}} = \{1\} \quad \Leftrightarrow \quad T_{\mathfrak{P}} = L \quad \Leftrightarrow \quad \mathfrak{p} \text{ unverzweigt } .$$

Damit spiegelt sich das Zerlegungsverhalten von $\mathfrak{p}$ vollständig in der Gruppenstruktur der Galoisgruppe bzw. in der Zwischenkörperstruktur wieder. Z.B. folgt auch: $\mathfrak{p}$ träge $\Rightarrow L|K$ zyklisch, da in diesem Fall $\mathrm{Gal}(L|K) \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p})$ ist.
Es ist noch interessant, sich zu überlegen, was mit $\mathfrak{p}$ passiert, wenn wir es nach und nach in den Ringen der ganzen Zahlen in $Z_{\mathfrak{P}}$ und $T_{\mathfrak{P}}$ faktorisieren.

Satz 4.2.4. *1. $\mathfrak{P}_Z := \mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}}$ hat Trägheitsgrad 1 und Verzweigungsindex 1 über $\mathfrak{p}$.*

Falls $L|K$ Abelsch ist, ist $\mathfrak{p}$ also voll-zerlegt in $Z_{\mathfrak{P}}$;

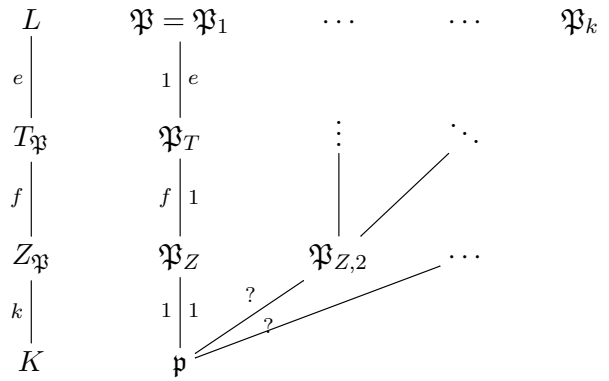
2. $\mathfrak{P}_Z$ ist träge in $T_{\mathfrak{P}}$ (daher der Name Trägheitskörper);

3. $\mathfrak{P}_T := \mathfrak{P}_Z\mathcal{O}_{T_{\mathfrak{P}}}$ ist rein verzweigt in $\mathcal{O}_L$, d.h.

$$\mathfrak{P}_T\mathcal{O}_L = \mathfrak{P}^e$$

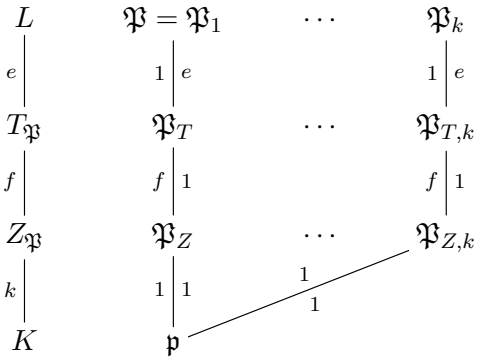
und $\mathfrak{P}$ hat Trägheitsgrad 1 über $\mathfrak{P}_T$.

Zusammenfassung:



Hier haben wir an den Primideale die jeweils übereinanderliegen links den Trägheitsgrad und rechts den Verzweigungsindex notiert. Wie und wann die

restlichen Primideale $\mathfrak{P}_{Z,2} = \mathfrak{P}_2 \cap \mathcal{O}_{Z_\mathfrak{P}}$ u.s.w. sich zerlegen, ist nicht klar. Beachte, dass z.B. für die Zerlegung der Ideale unter $\mathfrak{P}_2$ stattdessen die Gruppe $G_{\mathfrak{P}_2}$ mit Zwischenkörpern $Z_{\mathfrak{P}_2}$ und $T_{\mathfrak{P}_2}$ betrachtet werden sollte! Im Abelschen Fall sind alle Gruppen $G_{\mathfrak{P}_i}$ gleich und die Situation wird viel übersichtlicher:



Beweis. 1. L ist auch Galois über $Z_\mathfrak{P}$ und falls wir

$$\mathfrak{P}_Z \mathcal{O}_L = (\prod_{j=1}^{k'} \mathfrak{P}_{i_j})^{e'}$$

schreiben, so muss $k' = 1$ sein, denn die Galoisgruppe $G_\mathfrak{P}$ operiert immer noch transitiv auf diesen $\mathfrak{P}_{i_j}$ aber gleichzeitig lässt sie — nach Definition — $\mathfrak{P}$ fest. Der Körpergrad von L über $Z_\mathfrak{P}$ ist gleich $e \cdot f$, wegen $\#G_\mathfrak{P} = \frac{n}{k} = e \cdot f$. Da $G_\mathfrak{P}/I_\mathfrak{P}$ zur Galoisgruppe der Restklassenkörperweiterung isomorph ist, muss der Trägheitsgrad von $\mathfrak{P}$ über $Z_\mathfrak{P}$ ebenfalls f sein. Da $\mathfrak{P}$ das einzige Ideal ist, welches über $\mathfrak{P}_Z$ liegt, also $k = 1$ ist für die Erweiterung $L|Z_\mathcal{P}$, folgt, dass auch der Verzweigungsgrad von $\mathfrak{P}_Z$ in L gleich e sein muss. Es ist eine einfache Übung zu sehen, dass Trägheitsgrad und Verzweigungsindex multiplikativ sind, daher müssen beide eins sein für $\mathfrak{P}_Z$ über $\mathfrak{p}$.
Für den Beweis von 2. und 3. können wir annehmen, dass $K = Z_\mathfrak{P}$, dass also $\mathfrak{P}$ das einzige über $\mathfrak{p}$ gelegene Primideal von $\mathcal{O}_L$ ist. In diesem Fall ist $\mathfrak{p}$ träge genau dann, wenn $\mathrm{Gal}(L|K) \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p})$ ist. Dies gilt nach Definition von $I_\mathfrak{P}$ für die Erweiterung $T_\mathfrak{P}|K$. Der Rest folgt dann wiederum aus der Multiplikativität von Trägheitsgrad und Verzweigungsindex. □

4.3 Čebotarevscher Dichtigkeitssatz

Man kann sich umgekehrt fragen, ob eine gegebene Untergruppe von G immer als Zerlegungsgruppe oder Trägheitsgruppe vorkommt. Diese Frage wird

— neben anderen wichtigen Konsequenzen — durch den Satz von Čebotarev beantwortet, den wir kurz diskutieren wollen, aber nicht beweisen. Sein Beweis erfordert Resultate der analytischen Zahlentheorie.

Definition 4.3.1. *Sei $L|K$ eine Galoiserweiterung von Zahlkörpern. Sei $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ und $\mathfrak{P}$ ein Primideal von $\mathcal{O}_L$ über $\mathfrak{p}$. Sei p^k die Ordnung des Restklassenkörpers $\mathcal{O}_K/\mathfrak{p}$. Ein Urbild des Frobenius-Automorphismus*

$$F_{\mathfrak{P}} : x \mapsto x^{p^k}$$

welcher die zyklische Galoisgruppe der endlichen Körpererweiterung $\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p}$ erzeugt, unter dem Homomorphismus

$$G_{\mathfrak{P}} \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P}|\mathcal{O}_K/\mathfrak{p})$$

heisst **Frobeniuselement** $\sigma_{\mathfrak{P}}$.

Aus den Überlegungen am Anfang des Abschnittes folgt sofort:

Lemma 4.3.2. *Falls $\mathfrak{p}$ in $\mathcal{O}_L$ unverzweigt ist, so ist $\sigma_{\mathfrak{P}}$ eindeutig bestimmt. Die Konjugationsklasse von $\sigma_{\mathfrak{P}}$ ist dann sogar durch $\mathfrak{p}$ bestimmt, denn es gilt $\tau^{-1} \cdot \sigma_{\mathfrak{P}} \cdot \tau = \sigma_{\tau(\mathfrak{P})}$.*

Falls $\mathfrak{p}$ unverzweigt ist, ist also $\sigma_{\mathfrak{P}}$ eindeutig bestimmt durch

$$\begin{aligned} \sigma_{\mathfrak{P}}(\mathfrak{P}) &= \mathfrak{P} \\ \sigma_{\mathfrak{P}}(x) &\equiv x^{p^k} \pmod{\mathfrak{P}} \qquad \forall x \in \mathcal{O}_L. \end{aligned}$$

Die Lage der Frobeniuselemente in $\mathrm{Gal}(L|K)$ gibt Auskunft über die Zerlegung von $\mathfrak{p}$ in $\mathcal{O}_L$: Man überlege sich, dass für unverzweigte $\mathfrak{p}$ (also $e = 1$ gilt):

$$\mathrm{ord}(\sigma_{\mathfrak{P}}) = \frac{n}{k} = f.$$

Der Satz von Čebotarev gibt Auskunft darüber, für "wieviele" (unverzweigte) $\mathfrak{p}$ eine gegebene Konjugationsklasse ein Frobeniuselement $\sigma_{\mathfrak{P}}$ für ein Primideal $\mathfrak{P}$ über $\mathfrak{p}$ enthählt. Insbesondere besagt er, dass dies immer für unendlich viele $\mathfrak{p}$ der Fall ist. Um aber den *Anteil* an allen Primidealen $\mathfrak{p}$ von $\mathcal{O}_K$ zu messen, definiert man

Definition 4.3.3. *Sei X eine Menge von Primidealen von $\mathcal{O}_K$. Der Limes*

$$\delta(X) := \lim_{C \to \infty} \frac{\#\{\mathfrak{p} \in X \mid N(\mathfrak{p}) \leq C\}}{\#\{\mathfrak{p} \mid N(\mathfrak{p}) \leq C\}}$$

heisst die **natürliche Dichtigkeit** *von X, falls er existiert.*

Beachte, dass für eine *endliche* Menge X von Primidealen offensichtlich stets $\delta(X) = 0$ gilt. Falls allgemeiner für eine Menge X die natürliche Dichtigkeit $\delta(X)$ existiert und ungleich Null ist (oder nicht existiert), dann muss X aus unendlich vielen Primidealen bestehen. $\delta(X)$ hängt dann von X nur "bis auf endlich viele Primideale" ab. Das heisst, wenn wir endliche viele Primideale zu X hinzufügen oder entfernen, ändert sich $\delta(X)$ nicht.

Satz 4.3.4 (Čebotarevscher Dichtigkeitssatz)**.** *Sei $\sigma \in \mathrm{Gal}(L|K)$ ein Element. Die Menge*

$$X(\sigma) = \{\mathfrak{p} \mid \mathfrak{p} \text{ unverzweigt und } \sigma = \sigma_{\mathfrak{P}} \text{ für ein } \mathfrak{P} \text{ über } \mathfrak{p} \}$$

hat die natürliche Dichtigkeit

$$\delta(X(\sigma)) = \frac{\#\langle\sigma\rangle}{\#G}.$$

Beweis. siehe z.B. [N, §13][15]. □

Dabei ist $\langle\sigma\rangle$ die Konjugationsklasse von σ. Beachte, dass auch $X(\sigma)$ nur von der Konjugationsklasse von σ abhängt. Insbesondere besagt der Satz, dass jede Konjugationsklasse aus Frobeniuselementen für Primideale über *unendlich vielen* $\mathfrak{p}$ besteht.
Zusammen mit dem explizit bestimmten Zerlegungsverhalten der Primideale in quadratischen oder zyklotomischen Körpern erhalten wir interessante arithmetische Konsequenzen. Zunächst folgt, dass alle Ordnungen der Elemente von $G(L|K)$ tatsächlich als Trägheitsgrade von Primidealen auftreten. Man kann aber noch feinere Informationen gewinnen. Z.B. folgt durch Anwendung auf zyklotomische Körper $\mathbb{Q}(\zeta_n)$ über $\mathbb{Q}$:

Satz 4.3.5 (Dirichletscher Primzahlsatz)**.** *Seien $n \in \mathbb{N}$ und $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Die Primzahlen p mit*

$$p \equiv a \pmod{n}$$

bilden eine Menge der natürlichen Dichtigkeit $\frac{1}{\varphi(n)}$.

Beweis. Für $\mathbb{Q}(\zeta_n)$ haben wir einen Isomorphismus

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \cong & \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \\ a & \mapsto & \tau_a \end{array}$$

[15] Neukirch verwendet die sogenannte Dirichlet-Dichtigkeit, die einfacher zu handhaben ist. Für einen Beweis, dass der Satz auch bzgl. der natürlichen Dichtigkeit gilt, siehe: Lenstra, H. W.; Stevenhagen, P. (1996), "Čebotarev and his density theorem"

welcher durch

$$\tau_a(\zeta_n) = (\zeta_n)^a$$

festgelegt ist. Sei $p \nmid n$ eine Primzahl. p ist dann unverzweigt[16]. Die Frobeniuselemente $\sigma_{\mathfrak{P}}$ für alle $\mathfrak{P}$, die über $p\mathbb{Z}$ liegen, sind a priori alle gleich, da $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ abelsch ist. Sei $\mathfrak{P}$ eines von den Primidealen die über $p\mathbb{Z}$ liegen. Aus der Definition folgt sofort, dass

$$\sigma_{\mathfrak{P}}(\zeta_n) \equiv \tau_p(\zeta_n) \pmod{\mathfrak{P}}$$

sein muss. Es folgt $\sigma_{\mathfrak{P}} = \tau_p$, da die Reduktion $G_{\mathfrak{P}} \to \mathrm{Gal}(\mathcal{O}_{\mathbb{Q}(\zeta_n)}/\mathfrak{P}|\mathbb{F}_p)$ injektiv ist. Daher folgt die Aussage des Satzes aus dem Čebotarevschen Dichtigkeitssatz angewendet auf τ_a. □

5 Lokale Körper

5.1 Beträge

In der Analysis lernt man, dass die reellen Zahlen aus den rationalen durch Vervollständigung bzgl. des gewöhnlichen Absolutbetrages $|\cdot|_\infty$ gewonnen werden können. Das heisst genauer, dass sich die reellen Zahlen als die Menge der Cauchy-Folgen rationaler Zahlen modulo Nullfolgen definieren lassen. Überraschenderweise gibt es auf den rationalen Zahlen — und allgemeiner auf Zahlkörpern — weitere Beträge, welche dieselben Axiome wie der gewöhnliche Absolutbetrag für $\mathbb{Q}$ erfüllen. Sie sind zahlentheoretischer Natur. Während für den gewöhnlichen Absolutbetrag die Folge der natürlichen Zahlen $\{1, 2, 3, \dots\}$ unbeschränkt ist (wir nennen einen solchen Betrag "Archimedisch") ist diese Menge für die anderen Beträge beschränkt (wir nennen sie deshalb "nicht-Archimedisch"). Für jede Primzahl p gibt es einen solchen nicht-Archimedischen Betrag $|\cdot|_p$ auf $\mathbb{Q}$. Er hat die Eigenschaft, dass ganze Zahlen a und b umso näher beieinanderliegen, je öfter ihre Differenz durch p teilbar ist. Die Vervollständigung von $\mathbb{Q}$ bzgl. dieses Betrages ist der Körper der **p-adischen Zahlen** $\mathbb{Q}_p$.

Definition 5.1.1. *Sei K ein Körper. Ein* **Betrag** *(oder auch eine multiplikative Bewertung) von K ist eine Funktion $|\cdot| : K \to \mathbb{R}$ mit*

1. *(Positivität) $|0| = 0$ und $|x| > 0$ für alle $x \neq 0$;*
2. *(Multiplikativität) $|xy| = |x| \cdot |y|$;*

[16] Für $n = l^n$ für eine Primzahl l folgt dies aus den Überlegungen in Abschnitt 2.6. Für den allgemeinen Fall, siehe z.B. [N, I, §10]

3. (Dreiecksungleichung) $|x+y| \leq |x| + |y|$.

Beispiel 5.1.2. *Der gewöhnliche Absolutbetrag* $|\cdot|_\infty$ *auf* $\mathbb{Q}$, $\mathbb{R}$ *oder* $\mathbb{C}$. *Die Eigenschaften 1.–3. sind hier wohlbekannt. Für einen Zahlkörper* K *und eine Einbettung* $\sigma : K \to \mathbb{C}$ *definiert*

$$|x|_\sigma := |\sigma(x)|_\infty$$

einen Betrag auf K.

Beispiel 5.1.3. *Für jeden Körper* K *gibt es den* **trivialen Betrag**, *der durch* $|0| := 0$ *und* $|x| := 1$ *für* $x \neq 0$ *definiert ist. Dieser Betrag ist offensichtlich uninteressant. Überlegen Sie sich als Übung, dass alle Beträge eines endlichen Körpers trivial sind.*

Beispiel 5.1.4. *Der* p**-adische Betrag** *auf* $\mathbb{Q}$. *Schreibe für eine ganze Zahl* x *die Primfaktorzerlegung als*

$$x = \prod_p p^{\nu_p(x)}.$$

Definiere dann für eine rationale Zahl ungleich Null

$$\left|\frac{a}{b}\right|_p := p^{\nu_p(b)-\nu_p(a)}.$$

Es ist klar, dass dies unabhängig von der Darstellung als Bruch ist.

Wir wollen uns überlegen, dass $|\cdot|_p$ wirklich ein Betrag ist. Die Positivität ist klar. Die Multiplikativität folgt, da die Funktion $\nu_p(\cdot) : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ die Relation $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ erfüllt. Die Dreiecksungleichung hat sogar eine **verschärfte Form**:

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}. \tag{13}$$

Beweis der verschärften Dreiecksungleichung für $|\cdot|_p$. Seien $x, y \in \mathbb{Q}$ gegeben. Sei b der Hauptnenner. Wegen

$$|b| \cdot |x+y| = |bx+by| \quad |b\cdot x| + |b\cdot y| = |b|\cdot|x| + |b|\cdot|y|$$

genügt es, den Fall $x, y \in \mathbb{Z}$ zu betrachten und

$$\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}.$$

zu beweisen. Falls x und y beide durch p teilbar sind können wir die Multiplikativität erneut ausnutzen und daher sogar annehmen, dass o.B.d.A. x nicht durch p teilbar ist, also $\nu_p(x) = 0$. Es ist dann

$$\nu_p(x + y) \geq \min\{0, \nu_p(y)\} = 0.$$

zu zeigen, was aber nach Definition so ist. □

Lemma 5.1.5. *Ein Betrag $|\cdot|$ erfüllt genau dann die verschärfte Dreiecksungleichung (13), wenn die Menge $\{|n| \mid n \in \mathbb{N}\}$ beschränkt ist.*

Wie schon zu Beginn erwähnt, nennen wir einen solchen Betrag **nicht-Archimedisch**.

Beweis. Falls $|\cdot|$ die verschärfte Dreiecksungleichung (13) erfüllt, so gilt:

$$|n| = |1 + \cdots + 1| \leq |1| = 1.$$

Umgekehrt, sei $|n| \leq C$ für alle $n \in \mathbb{N}$. Dann gilt:

$$|x + y|^n = |\sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}| \leq \sum_{r=0}^{n} |\binom{n}{r}| \cdot |x|^r \cdot |y|^{n-r}.$$

Nun gilt: $|x|^r \cdot |y|^{n-r} \leq \max\{|x|, |y|\}^n$. Da $\binom{n}{r} \in \mathbb{N}$ ist also der Betrag durch C beschränkt, daher:

$$|x + y|^n \leq C(n + 1) \max\{|x|, |y|\}^n.$$

Nach ziehen der n-ten Wurzel ergibt sich:

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

und eine einfache Übung zeigt, dass im Limes $n \to \infty$ folgt:

$$|x + y| \leq \max\{|x|, |y|\}.$$

□

Definition/Lemma 5.1.6. *In jedem Körper K mit* nicht-Archimedischen *Betrag $|\cdot|$ ist*[17]

$$\mathcal{O}_K := \{x \in K \mid |x| \leq 1\}$$

[17] Wir verwenden dieselbe Bezeichnung, wie für den Ring der ganzen Zahlen in einem Zahlkörper. Es gibt eine Verbindung zwischen beiden, wie wir später sehen werden.

ein Unterring von K und

$$\mathfrak{m}_K := \{x \in K \mid |x| < 1\}$$

ist das einzige maximale Ideal von $\mathcal{O}_K$. Der Quotient heisst der Restklassenkörper von $(K, |\cdot|)$.
Der Betrag heisst **diskret**, *falls*

$$|K^*|$$

eine diskrete Untergruppe von $\mathbb{R}^*_{>0}$ ist.

5.1.7. Wenn ein Betrag diskret ist, ist $\log|K^*|$ eine diskrete additive Untergruppe von $\mathbb{R}$, also ein Gitter (Lemma 3.2.3). Falls der Betrag nicht der triviale Betrag ist, so folgt $|K^*| \cong \mathbb{Z}$. Daher:

1. Es gibt ein $\pi \in \mathcal{O}_K$ mit
$$|\pi|$$
maximal unter den Beträgen < 1. Es wird auch **uniformisierendes Element** genannt.

2. $$\mathfrak{m}_K = \pi \cdot \mathcal{O}_K.$$

3. Jedes $x \in K^*$ hat eine eindeutige Darstellung
$$x = \varepsilon \cdot \pi^n$$
mit $\varepsilon \in \mathcal{O}_K^*$ (d.h. $|\varepsilon| = 1$) und $n \in \mathbb{Z}$.

Man nennt das Paar $(\mathcal{O}_K, \mathfrak{m}_K)$ mit den Eigenschaften 2. und 3. auch einen **diskreten Bewertungsring**.

Überlegen Sie sich, dass der p-adische Betrag auf $\mathbb{Q}$ diskret ist und was diese Aussagen in diesem Fall genau bedeuten.

5.2 Vervollständigung, p-adische Zahlen

Wir wollen uns nun überlegen, dass auch für den p-adischen Betrag eine Vervollständigung von $\mathbb{Q}$ existiert. Fixiere einen beliebigen Körper K mit Betrag $|\cdot|$. Erinnere, dass eine Folge $(a_n)_{n\in\mathbb{N}}$ **Cauchy-Folge** heisst, falls für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$ existiert mit

$$|a_n - a_m| \leq \varepsilon \quad \text{für alle } m, n > N.$$

Definition 5.2.1. *Wir nennen $(K, |\cdot|)$* **vollständig**, *falls jede Cauchy-Folge in K konvergiert.*

Satz 5.2.2. *Für jeden Körper K mit Betrag $|\cdot|$ gibt es einen vollständigen Körper $\widehat{K}$ mit Betrag $|\cdot|$, eine Einbettung $\iota : K \hookrightarrow \widehat{K}$ welche mit dem Betrag kompatibel ist und mit folgender universeller Eigenschaft: Für jeden Homomorphismus $\sigma : K \to L$ in einen vollständigen Körper $(L, |\cdot|)$, welcher mit den Beträgen kompatibel ist, existiert ein eindeutiger Homomorphismus $\widetilde{\sigma} : \widehat{K} \to L$ so, dass $\sigma = \widetilde{\sigma} \circ \iota$.*

Aus der universellen Eigenschaft folgt, dass der Körper $\widehat{K}$ mit seinem Betrag $|\cdot|$ eindeutig bestimmt ist (bis auf Isomorphie). Wir nennen ihn die **Komplettierung** von K bzgl. $|\cdot|$.

Beweisskizze. Der Beweis ist im wesentlichen der gleiche wie in der Analysis. Man definiert $\widehat{K}$ als die Menge der Cauchy-Folgen in K bzgl. $|\cdot|$, modulo der Menge der Nullfolgen. Die Cauchyfolgen bilden einen Ring bzgl. der folgengliedweisen Addition und Multiplikation. Man zeigt, dass das Ideal der Nullfolgen maximal ist, und daher der Quotient $\widehat{K}$ ein Körper. Anschliessend überzeugt man sich, dass der Quotient tatsächlich vollständig ist. (Es ist a priori nur klar, dass Cauchy-Folgen mit Einträgen in K in $\widehat{K}$ konvergieren, aber nicht unbedingt solche mit Einträgen in $\widehat{K}$!) Die Einbettung $\iota : K \hookrightarrow \widehat{K}$ bildet ein Element $x \in K$ auf die konstante Folge x ab. □

Es ist leicht zu sehen, dass K in $\widehat{K}$ dicht liegt, und ein *diskreter* Betrag auf K seinen Wertebereich nicht ändert, also insbesondere diskret bleibt.

Definition 5.2.3. *Sei p eine Primzahl. Dann heisst die Komplettierung von $\mathbb{Q}$ bzgl. des p-adischen Betrages (5.1.4) der Körper der* **p-adischen Zahlen** $\mathbb{Q}_p$.

Satz 5.2.4. *Jedes $x \in \mathbb{Q}_p^*$ lässt sich in* eindeutiger *Weise darstellen als unendliche konvergente Summe:*

$$x = \sum_{n=N}^{\infty} a_n p^n$$

mit $a_n \in \{0, \ldots, p-1\}$, $N \in \mathbb{Z}$ und $a_N \neq 0$.
Es gilt $|x|_p = p^{-N}$, die Elemente in $\mathbb{Z}_p := \mathcal{O}_{\mathbb{Q}_p}$ sind genau diejenigen, bei denen $N \geq 0$ ist. Ferner ist $\mathfrak{m}_{\mathbb{Q}_p} = p\mathbb{Z}_p$ und der Restklassenkörper $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Wir möchten später Analoga der p-adischen Beträge und p-adischen Zahlen auch für Zahlkörper definieren und formulieren daher den Satz etwas allgemeiner.

Satz 5.2.5. *Sei $(K, |\cdot|)$ ein vollständiger Körper mit* diskretem *nicht-Archimedischem Betrag. Wähle eine Menge $S \subset \mathcal{O}_K$ von Repräsentanten des Restklassenkörpers*

$$k = \mathcal{O}_K/\mathfrak{m}_K$$

und ein uniformisierendes Element $\pi \in K$. Dann hat jedes $x \in K$ eine eindeutige *Darstellung als unendliche konvergente Summe:*

$$x = \sum_{n=N}^{\infty} a_n \pi^n$$

mit $a_n \in S$ und $a_N \neq 0$.

Wir wollen zunächst uns überlegen, dass Satz 5.2.4 aus diesem Satz folgt. Wir müssen uns dazu überlegen:

1. p ist ein uniformisierendes Element.
2. Der Restklassenkörper von $\mathbb{Q}_p$ ist $\mathbb{F}_p$ (denn dann ist $S := \{0, \ldots, p-1\}$ ein Repräsentatensystem.)

1. folgt, da

$$|\mathbb{Q}_p^*| = |\mathbb{Q}^*| = p^{\mathbb{Z}}$$

(eine diskreter Betrag ändert unter Vervollständigung nicht seinen Wertebereich). p hat daher auch in $\mathbb{Q}_p$ unter den Elementen mit Betrag < 1 den maximalen, nämlich p^{-1}.
2. Der Restklassenkörper von $\mathbb{Q}$ bzgl. dem p-adischen Betrag ist gleich $\mathbb{F}_p$ (Übung). Auch er ändert sich nicht unter Vervollständigung, denn K liegt dicht in $\widehat{K}$: das heisst insbesondere, dass zu jedem $x \in \mathcal{O}_{\widehat{K}}$ ein $x' \in \mathcal{O}_K$ existiert mit

$$|x - x'| < 1$$

und daher $x \equiv x' \pmod{\mathfrak{m}_{\widehat{K}}}$.

Beweis von Satz 5.2.5. In einem vollständigen Körper mit nicht-Archimedischem Betrag gilt:

$$\sum_{n=0}^{\infty} a_n \text{ konvergiert } \Leftrightarrow \lim_{n\to\infty} |a_n| = 0.$$

Wir lassen den Beweis als Übung. Da $|a_n\pi^n| \leq |\pi|^n$ und $|\pi| < 1$, konvergiert also die Summe.
Um die Umkehrung zu beweisen, reicht es zu zeigen, dass für jedes $x \in K$ *genau eine* Summe der Form

$$x_M = \sum_{n=N}^{M-1} a_n \pi^n$$

mit $a_n \in S$, $a_N \neq 0$ existiert, so dass

$$|x - x_M| \leq |\pi|^M.$$

Wir beweisen das durch Induktion nach M.
Induktionsanfang: Wir haben schon in 5.1.7 gesehen, dass sich jedes Element von K eindeutig als

$$x = \varepsilon \cdot \pi^N$$

mit $|\varepsilon| = 1$. schreiben lässt. Es gibt nun ein eindeutiges $a_N \in S$ mit $a_N \equiv \varepsilon \pmod{\mathfrak{m}_K}$. Es gilt dann

$$|x - a_N \pi^N| \leq |\pi|^{N+1}$$

und $x_{N+1} := s\pi^N$ ist eindeutig bestimmt.
Induktionsschritt: Wir haben

$$|x - x_M| \leq |\pi|^M$$

und x_M ist eindeutig bestimmt. Nach dem selben Argument wie im Induktionsanfang finden wir ein $a_M \in S$ so dass

$$|x - x_M - a_M \pi^M| \leq |\pi|^{M+1}$$

und a_M ist eindeutig bestimmt. Setze dann $x_{M+1} := x_M + a_M \pi^M$. □

Beispiel 5.2.6. *Jede* natürliche *Zahl* $x \in \mathbb{N}$ *lässt sich als eine eindeutige* endliche *Summe*

$$x = \sum_{n=0}^{N} a_n p^n$$

mit $a_n \in \{0, \ldots, p-1\}$ *schreiben.*
Es gilt in $\mathbb{Q}_p$ *(Teleskopsumme!):*

$$-1 = \sum_{n=0}^{\infty} (p-1) p^n.$$

Es gilt in $\mathbb{Q}_p$ (Formel für die geometrische Reihe):

$$\frac{1}{p-1} = \sum_{n=0}^{\infty} p^n.$$

Allgemeiner lässt sich jede rationale Zahl als (schliesslich) periodische *p-adische Zahl darstellen.*

5.3 Äquivalenz von Beträgen

Ein Betrag eines Körpers K definiert eine **Topologie** auf K in der die offenen Mengen $X \subseteq K$ diejenigen sind, so dass für alle $x \in X$ ein $\varepsilon > 0$ existiert mit $\{y \in K \mid |y - x| < \varepsilon\} \subseteq X$. Der Begriff der Cauchy-Folge und damit die Komplettierung hängen nur von der Topologie ab[18]. Wir wollen daher untersuchen, wann zwei Beträge dieselbe Topologie definieren.
Mit jedem nicht-Archimedischen Betrag $|\cdot|$ ist auch $|\cdot|^s$ für alle $s \in \mathbb{R}_{>0}$ ein Betrag: Die Positivität und Multiplikativität sind klar. Ausserdem ist

$$|x+y|^s \leq (\max\{|x|, |y|\})^s = \max\{|x|^s, |y|^s\}.$$

(Für einen Archimedischen Betrag bleibt die Dreiecksungleichung im Allgemeinen nur für $s \leq 1$ erhalten.) Offensichtlich definieren $|\cdot|$ und $|\cdot|^s$ dieselbe Topologie auf K. Die Umkehrung gilt auch:

Satz 5.3.1. *Sei K ein Körper mit Beträgen $|\cdot|_1$ und $|\cdot|_2$. Dann sind äquivalent:*

1. *$|\cdot|_1$ und $|\cdot|_2$ definieren dieselbe Topologie auf K;*
2. *$|x|_1 < 1 \Leftrightarrow |x|_2 < 1$;*
3. *$|\cdot|_1 = |\cdot|_2^s$ für ein $s \in \mathbb{R}_{>0}$.*

Sind diese Bedingungen erfüllt, nennen wir $|\cdot|_1$ und $|\cdot|_2$ **äquivalent**.

Beweis. Wir nehmen an, dass die Beträge $|\cdot|_1$ und $|\cdot|_2$ beide nicht trivial sind (ansonsten sind die Aussagen klar).
3. $\Rightarrow$ 1. ist klar und wurde schon erwähnt.
1. $\Rightarrow$ 2.: $|x| < 1$ ist gleichbedeutend zu $\lim_{x\to\infty} x^n = 0$. Dies hängt nur von der Topologie ab.

[18] Eine Folge (a_n) ist Cauchy-Folge, genau dann wenn zu jeder offenen Umgebung $0 \in U \subset X$ ein $N \in \mathbb{N}$ existiert, so dass $a_m - a_n \in U$ für alle $m, n > N$.

2. $\Rightarrow$ 3.: Seien x und y zwei Elemente des Körpers mit $|y|_1 > 1$ und daher auch $|y|_2 > 1$. Es genügt zu zeigen, dass

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2},$$

denn dann ist $|x|_1 = |x|_2^s$, wobei s dieser Quotient ist welcher von x unabhängig ist.
Genauso gut können wir

$$\frac{\log|x|_1}{\log|y|_1} = \frac{\log|x|_2}{\log|y|_2}$$

zeigen. Sei $\alpha := \frac{\log|x|_1}{\log|y|_1}$, d.h. $|x|_1 = |y|_1^\alpha$.

1. Wähle eine Folge rationaler Zahlen $\frac{p_n}{q_n}$ welche *von oben* gegen α konvergiert. Es gilt dann $|x|_1 < |y|_1^{\frac{p_n}{q_n}}$ für alle n, also $|\frac{x^{p_n}}{y^{q_n}}|_1 < 1$. Daher $|\frac{x^{p_n}}{y^{q_n}}|_2 < 1$ für alle n, also $|x|_2 < |y|_2^{\frac{p_n}{q_n}}$ für alle n, also $|x|_2 \leq |y|_2^\alpha$.
2. Wähle eine Folge rationaler Zahlen $\frac{p_n}{q_n}$ welche *von unten* gegen α konvergiert. Es gilt dann $|x|_1 > |y|_1^{\frac{p_n}{q_n}}$ für alle n, also $|\frac{y^{q_n}}{x^{p_n}}|_1 < 1$. Daher $|\frac{y^{q_n}}{x^{p_n}}|_2 < 1$ für alle n, also $|x|_2 > |y|_2^{\frac{p_n}{q_n}}$ für alle n, also $|x|_2 \geq |y|_2^\alpha$.

Zusammen folgt: $|x|_2 = |y|_2^\alpha$. □

5.4 Die Sätze von Ostrowski

Für $K = \mathbb{Q}$ kennen wir den gewöhnlichen Absolutbetrag und für jede Primzahl p den p-adischen Betrag. Der erste Satz von Ostrowski, der in diesem Abschnitt bewiesen werden soll, besagt, dass es bis auf Äquivalenz keine anderen (nicht-trivialen) Beträge auf $\mathbb{Q}$ gibt.

Satz 5.4.1 (Ostrowski)**.** *Jeder nicht-triviale Betrag auf $\mathbb{Q}$ ist entweder zu $|\cdot|_\infty$ oder einem $|\cdot|_p$ äquivalent.*

Beweis. 1. Sei $|\cdot|$ ein nicht-Archimedischer Betrag auf $\mathbb{Q}$. Es gilt dann für $n \in \mathbb{N}$

$$|n| = |1 + \cdots + 1| \leq 1$$

wegen der verschärften Dreiecksungleichung. Es gibt dann eine Primzahl mit $|p| < 1$, weil sonst aus der eindeutigen Primfaktorzerlegung $|x| = 1$ für alle $x \in \mathbb{Q}^*$ folgt. Die Menge

$$\mathfrak{m} = \{x \in \mathbb{Z} \mid |x| < 1\} \subsetneq \mathbb{Z}$$

ist ein Ideal und wegen $(p) \subseteq \mathfrak{m} \subsetneq \mathbb{Z}$ gilt $(p) = \mathfrak{m}$ da (p) maximal ist. Insbesondere gilt $|q| = 1$ für alle Primzahlen $q \neq p$. Es folgt aus der eindeutigen Primfaktorzerlegung

$$|\frac{r}{s}| = |p|^{\nu_p(r)-\nu_p(s)}.$$

Der Betrag ist also offensichtlich äquivalent zum p-adischen Betrag.

2. Sei $|\cdot|$ ein Archimedischer Betrag auf $\mathbb{Q}$.

   Wir überlegen uns zunächst einige Folgerungen aus den Betragsaxiomen:

   (a) Seien $m, n \in \mathbb{N}$ und schreibe m in der n-adischen Entwicklung:

   $$m = a_0 + a_1 n + \cdots + a_n n^r$$

   für $a_i \in \{0, \ldots, n-1\}$ und $a_n \neq 0$. Dann gilt $m \leq n^r$ und daher

   $$r \leq \frac{\log m}{\log n}$$

   (b) Sei $n \in \mathbb{N}$. $|n| = |1 + \cdots + 1| \leq |1| + \cdots + |1| = n$.

   (c) Aus (a) und (b) folgt, wegen $|a_n| \leq a_n < n$:

   $$|m| \leq (r+1)n(\max\{1, |n|\})^r \leq (\frac{\log m}{\log n} + 1)n(\max\{1, |n|\})^{\frac{\log m}{\log n}}.$$

   Beachte, dass wir noch nicht wissen, dass $|n| \geq 1$.

   (d) Ersetze nun in (c) m durch m^t und ziehe t-te Wurzeln:

   $$|m| \leq (\frac{t \log m}{\log n} + 1)^{\frac{1}{t}} n^{\frac{1}{t}} (\max\{1, |n|\})^{\frac{\log m}{\log n}}.$$

   (e) Im Limes $t \to \infty$ ergibt sich:

   $$|m| \leq (\max\{1, |n|\})^{\frac{\log m}{\log n}}.$$

Falls nun $|n| \leq 1$ für ein $n > 1$ folgt aus (e), dass $|m| \leq 1$ für alle m, $|\cdot|$ wäre also nicht-Archimedisch. Daher ist $|n| > 1$ für alle $n > 1$ und daher

$$|m| \leq |n|^{\frac{\log m}{\log n}}$$

also

$$\frac{\log |m|}{\log m} \leq \frac{\log |n|}{\log n}$$

für alle $m, n > 1$. Durch Vertauschen von m und n folgt

$$\frac{\log |m|}{\log m} = \frac{\log |n|}{\log n}$$

für alle $m, n > 1$. Sei s dieser gemeinsame Wert. Dann gilt:

$$|n| = n^s = |n|_\infty^s.$$

Da jede positive rationale Zahl ein Quotient natürlicher Zahlen ist, folgt die Aussage.

□

Es gibt noch einen zweiten Satz von Ostrowski:

Satz 5.4.2 (Ostrowski)**.** *Jeder bzgl. eines Archimedischen Betrages $|\cdot|$ vollständige Körper K ist entweder isomorph zu $\mathbb{R}$ oder $\mathbb{C}$ und der Betrag ist zum gewöhnlichen äquivalent.*

Beweis. K muss Charakteristik Null haben, denn ansonsten wäre (das Bild von) $\mathbb{N}$ in K endlich und somit beschränkt. Daher ist $\mathbb{Q} \subset K$ und die Einschränkung von $|\cdot|$ auf $\mathbb{Q}$ ist äquivalent zum gewöhnlichen Absolutbetrag (nach Satz 5.4.1). Wegen der universellen Eigenschaft der Komplettierung erhalten wir eine Einbettung $\mathbb{R} \hookrightarrow K$ so dass die Einschränkung von $|\cdot|$ auf $\mathbb{R}$ gleich $|\cdot|_\infty^s$ ist.
Wir müssen daher nur zeigen, dass jedes $\xi \in K$ eine quadratische Gleichung über $\mathbb{R}$ erfüllt. Denn dann ist $K \cong \mathbb{R}$ oder $K \cong \mathbb{C}$ und im zweiten Fall, wie wir gesehen haben, $|\cdot|$ gleich der eindeutigen Fortsetzung von $|\cdot|_\infty^s$, also gleich dem komplexen Absolutbetrag (hoch s). Für ein $z \in \mathbb{C}$ betrachte das *reelle* Polynom

$$p_z(x) = (x - z)(x - \overline{z}) = x^2 - (z - \overline{z})x + z\overline{z}$$

mit $p_z(z) = 0$. Betrachte die Abbildung

$$\begin{array}{rcl} f : \mathbb{C} & \to & \mathbb{R} \\ z & \mapsto & |p_z(\xi)|. \end{array}$$

Diese Abbildung ist stetig, da $|\cdot|$ stetig auf K und $z - \overline{z}$ und $z\overline{z}$ stetige Abbildungen $\mathbb{C} \to \mathbb{R} \subseteq K$ sind. Es gilt $\lim_{z\to\infty} f(z) = \infty$ und daher muss f ein Minimum m annehmen. Die Menge

$$S = \{z \in \mathbb{C} \mid f(z) = m\}$$

ist nicht-leer, beschränkt und abgeschlossen. Es gibt daher ein $z_0 \in S$ mit $|z_0|_\infty \geq |z|_\infty$ für alle $z \in S$. Falls $m = 0$ gibt es ein z mit $|p_z(\xi)| = 0$ also $p_z(\xi) = 0$, d.h. ξ erfüllt eine quadratische Gleichung.
Wir beweisen $m = 0$ durch Widerspruch. Annahme $m > 0$. Wähle ein $0 < \varepsilon^s < m$ und sei z_1 eine komplexe Zahl mit $p_{z_0}(z_1) = -\varepsilon$. Es gilt dann $z_1\overline{z}_1 = z_0\overline{z}_0 + \varepsilon$, daher $|z_1|_\infty > |z_0|_\infty$. Wegen der Wahl von z_0 muss daher

$$f(z_1) > m$$

sein. Betrachte nun das Polynom

$$G(x) = p_{z_0}(x)^n - (-\varepsilon)^n.$$

Es hat Nullstelle z_1 und noch $2n-1$ weitere: $z_2, \ldots, z_{2n}$. Es gilt die Abschätzung:

$$|G(\xi)| \leq |p_{z_0}(\xi)|^n + |-\varepsilon|^n = f(z_0)^n + \varepsilon^{sn} = m^n + \varepsilon^{sn}.$$

Es gilt nach einer leichten Rechnung:

$$G(x)^2 = \prod_{i=1}^{2n} p_{z_i}(x).$$

Wir haben daher

$$|G(\xi)|^2 = \prod_{i=1}^{2n} f(z_i) \geq f(z_1)m^{2n-1}.$$

Es folgt

$$f(z_1)m^{2n-1} \leq (m^n + \varepsilon^{sn})^2,$$

also

$$\frac{f(z_1)}{m} \leq \left(1 + \left(\frac{\varepsilon^s}{m}\right)^n\right)^2.$$

Im Limes $n \to \infty$ ergibt sich

$$f(z_1) \leq m.$$

Widerspruch. □

5.5 $\mathfrak{p}$-adische Körper

Sei K ein Zahlkörper. Jedes Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ definiert analog zu den p-adischen Beträgen auf $\mathbb{Q}$ einen **$\mathfrak{p}$-adischen** Betrag $|\cdot|_\mathfrak{p}$ auf K. Die Definition benutzt die eindeutige Faktorzerlegung in Primideale. Sei $x \in K^*$ und schreibe

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

Erinnere: Die Exponenten $\nu_\mathfrak{p}(x)$ sind ganze Zahlen und durch x eindeutig bestimmt. Definiere dann

$$\boxed{|x|_\mathfrak{p} := p^{-\frac{\nu_\mathfrak{p}(x)}{e}}}$$

wobei e der Verzweigungsindex von $\mathfrak{p}$ über p ist, wobei p diejenige Primzahl ist mit $p \in \mathfrak{p}$.
Für $\mathbb{Q}$ und (p) ergibt sich genau der p-adische Betrag, wie vorher definiert. Ausserdem ist die Einschränkung von $|\cdot|_\mathfrak{p}$ auf $\mathbb{Q}$ gleich $|\cdot|_p$. Für diesen Zweck haben wir das $\frac{1}{e}$ eingefügt.
Für zwei verschiedene Primideale $\mathfrak{p}$ und $\mathfrak{q}$ definieren $|\cdot|_\mathfrak{p}$ und $|\cdot|_\mathfrak{q}$ inäquivalente Beträge, denn sei $x \in \mathfrak{p}$ aber $x \notin \mathfrak{q}$. Dann gilt $|x|_\mathfrak{p} < 1$ aber $|x|_\mathfrak{q} = 1$. Die Beträge können also nach Satz 5.3.1 nicht äquivalent sein. Insbesondere hat der p-adische Betrag $|\cdot|_p$ auf $\mathbb{Q}$ in der Regel mehrere verschiedene Fortsetzungen auf einen Zahlkörper K (für jedes Primideal über p eine). Dies kann für vollständige Körper nicht passieren:

Lemma 5.5.1. *Sei K ein vollständiger Körper mit Betrag $|\cdot|_K$ und $L|K$ eine endliche Körpererweiterung. Dann gibt es genau einen Betrag $|\cdot|_L$ auf L, welcher $|\cdot|_K$ fortsetzt.*

Beweis. Eindeutigkeit der Fortsetzung: Sie haben in der Analysis gelernt, dass alle Normen auf endlich-dimensionalen $\mathbb{R}$-Vektorräumen äquivalent sind, also dieselbe Topologie definieren und dass der Vektorraum für diese Topologie wieder vollständig ist.
Derselbe Beweis funktioniert für einen beliebigen vollständigen Körper. Und ein Betrag auf L ist insbesondere eine K-Norm bzgl. $|\cdot|_K$. Daher sind alle Beträge auf L, welche $|\cdot|_K$ fortsetzen, äquivalent. Da sie aber auf K übereinstimmen, müssen sie nach Satz 5.3.1 gleich sein.
Existenz der Fortsetzung: Falls $|\cdot|_K$ Archimedisch ist, haben wir gesehen, dass $K \cong \mathbb{R}$ oder $\mathbb{C}$ so dass $|\cdot|_K$ zum gewöhnlichen Betrag äquivalent ist, und falls $K \cong \mathbb{R}$ und $L \cong \mathbb{C}$ ist es klar, dass eine Fortsetzung existiert.

Falls $|\cdot|_K$ nicht-Archimedisch ist, beweisen wir dies zunächst für den Fall, dass die Bewertung *diskret* ist. Dann folgt sie aus dem, was wir zu Anfang der Vorlesung gelernt haben. $\mathcal{O}_K$ ist als diskreter Bewertungsring offensichtlich ein Dedekindring. Wir definieren (provisorisch, denn wir wissen noch nicht, dass ein Betrag auf L existiert) $\mathcal{O}_L$ als ganzen Abschluss von $\mathcal{O}_K$ in L. Das folgende Lemma zeigt, dass dann $\mathcal{O}_L$ wieder ein Dedekindring ist. (Wir haben das bisher nur für Zahlkörper gesehen.) Dann gilt die eindeutige Faktorzerlegung in Primideale und jedes Primideal $\mathfrak{M}$, welches über $\mathfrak{m}_K$ liegt, definiert daher einen $\mathfrak{M}$-adischen Betrag $|\cdot|_{\mathfrak{M}}$ welcher $|\cdot|_K$ fortsetzt[19]. Wegen der Eindeutigkeit hängt dieser Betrag nicht von der Wahl von $\mathfrak{M}$ ab. □

Wir können daraus die folgenden wichtigen Konsequenzen ziehen:

Satz 5.5.2. *Sei K vollständig bzgl. des (diskreten) nicht-Archimedischen Betrages $|\cdot|_K$ und sei $L|K$ eine endliche Körpererweiterung. Sei $|\cdot|_L$ die eindeutige Fortsetzung von $|\cdot|_K$.*

1. $\mathcal{O}_L = \{x \in L \mid |x|_L \leq 1\}$ *ist der ganze Abschluss von $\mathcal{O}_K$ in L.*
2. $\mathfrak{m}_L = \{x \in L \mid |x|_L < 1\}$ *ist das einzige Primideal von $\mathcal{O}_L$, welches über $\mathfrak{m}_K$ liegt.*
3. $$\boxed{|x|_L = \sqrt[n]{|N_{L|K}(x)|_K}}$$

Beweis. 1. Der ganze Abschluss $\mathcal{O}_L$ besteht (wie für Zahlkörper) aus denjenigen Elementen, in deren Primfaktorzerlegung alle Exponenten nicht-negativ sind, d.h. aus denjenigen Elementen für die alle $\mathfrak{M}$-adischen Beträge für die Ideale $\mathfrak{M}$ über $\mathfrak{m}_K$ kleiner gleich 1 sind. Wenn K und damit L vollständig sind, wenn also alle Beträge, die $|\cdot|_K$ fortsetzen übereinstimmen, heisst dies, dass die Definition von $\mathcal{O}_L$ als ganzer Abschluss mit der bisherigen (als Menge der Elemente mit Betrag kleiner gleich 1) übereinstimmt.
2. In $\mathcal{O}_L$ gibt es nur ein maximales Ideal $\mathfrak{m}_L$. Die $\mathfrak{M}$'s über $\mathfrak{m}_K$ sind daher alle gleich $\mathfrak{m}_L$.
3. Wir beweisen die Formel für den Fall, dass L Charakteristik Null hat, da wir hauptsächlich an diesem Fall interessiert sind. Es genügt diese Formel für die Galoissche Hülle von L zu beweisen. Wir können daher o.B.d.A.

[19] $|\cdot|_{\mathfrak{M}}$ wird genauso definiert, wie zu Beginn des Abschnittes für Zahlkörper definiert: Falls $x\mathcal{O}_L = \prod_{i=1}^{k} \mathfrak{M}_i^{n_i}$ setze dann $|x|_{\mathfrak{M}_i} := (|\pi|_K)^{\frac{n_i}{e_i}}$, wobei e_i der Verzweigungsindex von $\mathfrak{M}_i$ über $\mathfrak{m}_K$ ist.

annehmen, dass L Galoissch ist. Sei $(x) = \mathfrak{m}_L^k$ und $\mathfrak{m}_K \mathcal{O}_L = \pi_K \mathcal{O}_L = \mathfrak{m}_L^e$. Es gilt daher (nach Konstruktion der Fortsetzung)

$$|x|_L = |\pi_K|^{\frac{k}{e}}.$$

Es gilt aber auch $(N_{L|K}(x)) = \prod_\sigma \sigma(\mathfrak{m}_L)^k = (\mathfrak{m}_L)^{kn} = (\mathfrak{m}_K)^{\frac{kn}{e}}$ also

$$|N_{L|K}(x)|_K = |\pi_K|^{\frac{kn}{e}}.$$

□

Wir haben die wichtige Formel 3. hier mithilfe der Theorie der Dedekindringe bewiesen. Man kann einen direkten bewertungstheoretischen Beweis geben, der für beliebige nicht-Archimedische Beträge funktioniert, also auch für nicht notwendigerweise diskrete. Er benutzt das wichtige *Henselsche Lemma*, das wir am Ende des Abschnittes für den diskreten Fall aus dem bereits bewiesenen herleiten wollen. Anschliessend geben wir einen rein bewertungstheoretischen, konstruktiven Beweis. Er funktioniert ebenfalls für beliebige nicht-Archimedische Beträge.
Oben wurde benutzt:

Lemma 5.5.3. *Sei $\mathcal{O}_K$ ein Dedekindring mit Quotientenkörper K und L eine endliche Körpererweiterung von K. Dann ist auch $\mathcal{O}_L$, der ganze Abschluss von $\mathcal{O}_K$ in L, wieder ein Dedekindring.*

Beweis. Siehe [N, I, Satz 8.1]. □

Satz 5.5.4. *Sei K ein Zahlkörper und p eine Primzahl, und sei $p\mathcal{O}_K = \prod_{i=1}^k \mathfrak{p}_i^{e_i}$ die Faktorzerlegung in Primideale. Bezeichne, wie gehabt, mit f_i die Trägheitsgrade.*

1. *Es gibt Bijektionen*

$$\{\textit{Konjugationsklassen von Einbettungen } \sigma : K \hookrightarrow \overline{\mathbb{Q}_p}\} \cong \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$$

$$\cong \{\textit{Beträge } |\cdot| \textit{ von } K \textit{ welche } |\cdot|_p \textit{ fortsetzen}\}$$

Falls K Galois ist, sind diese mit den offensichtlichen Operationen der Galoisgruppe verträglich[20].

[20] Ein $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ operiert auf den Mengen wie folgt. Eine Einbettung $\tau : K \to \overline{\mathbb{Q}_p}$ wird auf $\tau \circ \sigma$ abgebildet, ein Betrag $|\cdot|$ auf $|\sigma(\cdot)|$, und ein Primideal $\mathfrak{p}$ auf $\sigma(\mathfrak{p})$

2. *Die Vervollständigung $K_{\mathfrak{p}_i}$ von K (wir schreiben manchmal auch $\widehat{K}_{\mathfrak{p}_i}$) bzgl. des $\mathfrak{p}_i$-adischen Betrag ist eine Erweiterung vom Grad $e_i \cdot f_i$ von $\mathbb{Q}_p$. Falls K Galoissch ist, ist $K_{\mathfrak{p}_i}$ Galoissch über $\mathbb{Q}_p$ und es gibt einen kanonischen Isomorphismus*

$$G_{\mathfrak{p}_i} \cong \mathrm{Gal}(K_{\mathfrak{p}_i}|\mathbb{Q}_p)$$

wobei $G_{\mathfrak{p}_i}$ die Zerlegungsgruppe von $\mathfrak{p}_i$ in $\mathrm{Gal}(K|\mathbb{Q})$ ist.

3. *Es gilt:*

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \bigoplus_{i=1}^{k} K_{\mathfrak{p}_i}.$$

Beweis. 1. Jedes Primideal $\mathfrak{p}_i$ über (p) definiert eine Betragsfortsetzung $|\cdot|_{\mathfrak{p}_i}$ von $|\cdot|_p$ wie wir uns oben überlegt haben. Es bleibt zu sehen, dass jeder Betrag $|\cdot|$ auf K welcher $|\cdot|_p$ fortsetzt zu einem Primideal auf $\mathcal{O}_K$ gehört. Definiere das Ideal

$$\mathfrak{p} := \{x \in \mathcal{O}_K \mid |x| < 1\}.$$

Falls $x \in \mathcal{O}_K$ so folgt, dass[21] $|x| \leq 1$. Daraus folgt, dass $\mathfrak{p}$ ein Primideal ist, denn wenn $|xy| = |x| \cdot |y| < 1$ und $x, y \in \mathcal{O}_K$, dann muss einer der Beträge $|x|$ oder $|y|$ kleiner eins sein. Ausserdem ist $p \in \mathfrak{p}$, $\mathfrak{p}$ ist also ein Primideal über (p). Man überlegt sich, dass diese Zuordnungen in der Tat invers zueinander sind.
Wir beweisen zunächst, dass es eine Einbettung

$$K_{\mathfrak{p}_i} \hookrightarrow \overline{\mathbb{Q}_p} \tag{14}$$

gibt (mit anderen Worten: $K_{\mathfrak{p}_i}$ ist algebraisch über $\mathbb{Q}_p$). Es genügt dies für K Galoissch zu zeigen. Es gibt sicher eine Einbettung $K \hookrightarrow \overline{\mathbb{Q}_p}$. Die Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$ operiert nun auf den Beträgen transitiv (wegen der Bijektion Primideale über (p) mit Fortsetzungen). Daher können wir die Einbettung mit einem $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ komponieren und erhalten eine, so dass der Rückzug des eindeutig bestimmten Betrages auf $\overline{\mathbb{Q}_p}$ der Betrag $|\cdot|_{\mathfrak{p}_i}$ auf K ist. Die Einbettung (14) existiert dann aufgrund der universellen Eigenschaft der Komplettierung[22]. Alle solchen $\mathbb{Q}_p$-Einbettungen sind nach

[21] Sei $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ mit $a_i \in \mathbb{Z}$. Dann gilt: $|a_n| \leq \max\{|x|^n, |a_1| \cdot |x|^{n-1}, \ldots, |a_{n-1}| \cdot |x|\}$. Da alle $|a_i| \leq 1$ folgt aus $|x| > 1$, dass dieses Maximum gleich $|x|^n > 1$ ist. Ausserdem ist $|x|^n$ echt grösser als alle anderen Beträge der Summanden, es gilt daher (Übung) sogar Gleichheit: $|a_n| = |x|^n$. Widerspruch.

[22] Es ist von vorherein klar, dass K in eine endliche Erweiterung von $\mathbb{Q}_p$ einbettet. Diese ist vollständig.

Galoistheorie unter $\mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p)$ konjugiert, die Konjugationsklasse ist somit eindeutig bestimmt. Da $K \subset K_{\mathfrak{p}_i}$ liefert dies auch eine Konjugationsklasse von Einbettungen $K \hookrightarrow \overline{\mathbb{Q}_p}$.
Eine Einbettung $K \hookrightarrow \overline{\mathbb{Q}_p}$ liefert umgekehrt einen Betrag auf K, nämlich die Einschränkung des eindeutig bestimmten Betrages[23] auf $\overline{\mathbb{Q}_p}$.
2. Wir beweisen dies nur für den Fall, dass K Galoissch ist. Der allgemeine Fall folgt daraus mit etwas Galoistheorie. Fixiere eine Einbettung $K \hookrightarrow K_{\mathfrak{p}} \subset \overline{\mathbb{Q}_p}$. Zu jedem $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p)$ ist dann die Einschränkung auf K ein Element von $\mathrm{Gal}(K|\mathbb{Q})$. Offensichtlich ist diese Einschränkung in $G_{\mathfrak{p}}$, denn sonst würde sie $\mathfrak{p}$ und damit den Betrag verändern. Dies liefert einen Homomorphismus

$$\mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p) \to G_{\mathfrak{p}}.$$

Der Kern: Sei σ im Kern dieses Homomorphismus und sei K^σ der Fixkörper. $K^\sigma \cap K_{\mathfrak{p}}$ enthält $\mathbb{Q}_p$, und K bettet bereits ein (mit dem Betrag kompatibel). Wegen der universellen Eigenschaft von $K_{\mathfrak{p}}$ ist also $K^\sigma \cap K_{\mathfrak{p}} = K_{\mathfrak{p}}$. Der Kern ist also gleich $\mathrm{Gal}(\overline{\mathbb{Q}_p}|K_{\mathfrak{p}})$ und daher ist $K_{\mathfrak{p}}$ Galoissch (Kerne sind Normalteiler) und wir können die Abbildung als

$$\mathrm{Gal}(K_{\mathfrak{p}}|\mathbb{Q}_p) \to G_{\mathfrak{p}}$$

schreiben.
Surjektivität: Fixiere eine Einbettung $\tau : K \subset K_{\mathfrak{p}} \hookrightarrow \overline{\mathbb{Q}_p}$. Ein $\sigma \in G_{\mathfrak{p}}$ definiert eine Einbettung $\tau \circ \sigma : K \hookrightarrow \overline{\mathbb{Q}_p}$. Da σ das Primideal $\mathfrak{p}$ festhält muss sie, nachdem was wir uns oben überlegt haben, auch die Konjugationsklasse $K \hookrightarrow K_{\mathfrak{p}}$ festhalten. Es gibt daher ein $\overline{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p)$ mit $\tau \circ \sigma = \overline{\sigma} \circ \tau$. Die Einschränkung von $\overline{\sigma}$ auf $K_{\mathfrak{p}}$ (via der fixierten Einbettung) ist dann ein Urbild von σ in $\mathrm{Gal}(K_{\mathfrak{p}}|\mathbb{Q}_p)$.
Da $G_{\mathfrak{p}}$ die Ordnung $e \cdot f$ hat, ist also der Grad von $K_{\mathfrak{p}}|\mathbb{Q}_p$ gleich $e \cdot f$.
3. Dies geht Wort für Wort genauso wie in Lemma 3.1.1. Zunächst ist

$$K \otimes \overline{\mathbb{Q}_p} = \sum_{\sigma : K \hookrightarrow \overline{\mathbb{Q}_p}} \overline{\mathbb{Q}_p}$$

nach demselben Argument wie in Lemma 3.1.1. Man untersucht dann die Galoisinvarianten unter der Operation von $\mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p)$. □

Dieser Satz hat eine offensichtliche relative Version für eine Erweiterung $L|K$ von Zahlkörpern, die Sie selber ausformulieren sollten.

[23] Beachte, das $\overline{\mathbb{Q}_p}$ eine Vereinigung von endlichen Erweiterungen ist auf die der Betrag eindeutig fortsetzt.

Beachte, dass der Satz im wesentlichen auch für die Archimedischen Beträge von K gilt: Es gibt eine Bijektion

$$\{\text{Konjugationsklassen von Einbettungen } \sigma : K \hookrightarrow \mathbb{C}\}$$

$$\cong \{\text{Beträge } |\cdot| \text{ von } K \text{ welche } |\cdot|_\infty \text{ fortsetzen}\}$$

und es gilt (Lemma 3.1.1)

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \sum_{[\sigma]} K_\sigma.$$

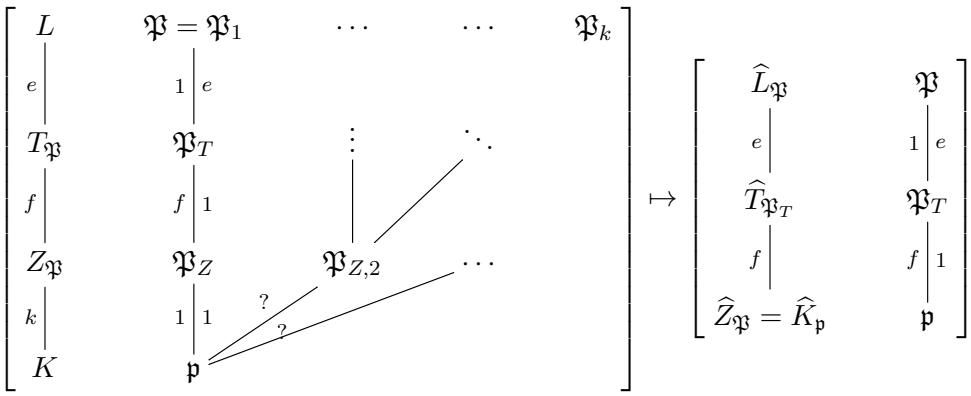
Dabei ist K_σ die Vervollständigung bzgl. $|x| = |\sigma(x)|_\infty$ und gleich $\mathbb{R}$, wenn σ reell ist und gleich $\mathbb{C}$, wenn σ komplex ist. Man kann sogar im Galoisfall für einen Archimedischen Betrag eine Zerlegungsgruppe $G_{|\cdot|} = \{\sigma \in \mathrm{Gal}(K|\mathbb{Q}) \text{ mod } |\sigma(\cdot)| = |\cdot|\}$ definieren und erhält: $G_{|\cdot|} \cong \mathrm{Gal}(\mathbb{C}|\mathbb{R})$ falls $\widehat{K}$ komplex ist und trivial sonst.
Man bezeichnet in dieser Analogie die Konjugationsklassen von Einbettungen $\sigma : K \hookrightarrow \mathbb{C}$ (also reelle Einbettungen oder Paare komplex konjugierter Einbettungen) auch als die **unendlichen Primstellen** $\mathfrak{p}$ des Körpers K und schreibt $\mathfrak{p} \mid \infty$. Die Primideale $\mathfrak{p}$ heissen die **endlichen Primstellen** und man schreibt $\mathfrak{p} \nmid \infty$.

Beispiel 5.5.5. *Aus dem Satz folgt insbesondere, dass in den $\mathbb{Q}_p$ viele (über $\mathbb{Q}$) algebraische Zahlen liegen. Behauptung: $\sqrt{-1} \in \mathbb{Q}_5$. Beweis: Im Körper $\mathbb{Q}(i)$ gilt $(5) = (2+i)(2-i)$. Die Vervollständigung von $\mathbb{Q}(i)$ am $(2+i)$-adischen Betrag (oder auch am $(2-i)$-adischen Betrag) ist daher isomorph zu $\mathbb{Q}_5$ (da jeweils $e = f = 1$). Insbesondere gibt es zwei Einbettungen $\mathbb{Q}(i) \hookrightarrow \mathbb{Q}_5$.*
Folgern Sie als Übung auf dieselbe Weise aus Satz 2.6.3 dass allgemeiner $\mathbb{Q}_p$ die $(p-1)$-ten Einheitswurzeln enthält. Es gibt also ein Linksinsverses l der Reduktionsabbildung

$$\mathbb{Z}_p^* \xleftarrow{\ l\ } \twoheadrightarrow \mathbb{F}_p^*$$

welches ein Homomorphismus ist (der sogenannte **Teichmüllerlift***).*

Wenn wir die hier bewiesenen Aussagen in Verbindung bringen mit der Hilbertschen Verzweigungstheorie aus Abschnitt 4.2 erhalten wir folgendes Bild:



Alle Zerfällungskörper $Z_{\mathfrak{P}}$ für die Primideale $\mathfrak{P}$ über $\mathfrak{p}$ liegen also bereits in $\widehat{K}_{\mathfrak{p}}$. Dies ist ja auch die einzige mögliche Konsequenz aus dem "Zerfällungsverbot" für Primidealen in den Komplettierungen die, wie wir gesehen haben, aus der eindeutigen Normfortsetzung folgt. Die Verzweigung und Trägheit bleibt hingegen vollständig in den Komplettierungen sichtbar. Es gibt dort aber eine Besonderheit: Der Trägheitskörper $\widehat{T}_{\mathfrak{P}_T}$ hängt nur von f ab! Mit anderen Worten:

Satz 5.5.6. *Für eine endliche Erweiterung von K von $\mathbb{Q}_p$, gibt es (bis auf Isomorphie) genau eine unverzweigte Körpererweiterung von Grad f.*

Beweis. Es reicht zu zeigen, dass es in jeder endlichen Galoiserweiterung L von K alle unverzweigten Körpererweiterungen in einer maximalen zyklischen enthalten sind. Für jede endliche Galoiserweiterung L von K gibt es einen Homomorphismus

$$\mathrm{Gal}(L|K) \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{m}_L|\mathcal{O}_K/\mathfrak{m}_K)$$

wie in (12) definiert. Sei I der Kern (Trägheitsgruppe). Der Fixkörper von I ist eine Erweiterung K_f von K mit Isomorphismus

$$\mathrm{Gal}(K_f|K) \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{m}_L|\mathcal{O}_K/\mathfrak{m}_K).$$

Falls nun K' irgendeine unverzweigte Erweiterung von K ist so gilt $f_{K'} = [K' : K]$. Für die Galoissche Hülle $K'' \subset L$ ist die Abbildung

$$\mathrm{Gal}(K''|K) \to \mathrm{Gal}(\mathcal{O}_{K'}/\mathfrak{m}_{K'}|\mathcal{O}_K/\mathfrak{m}_K).$$

surjektiv. Die Gruppe $\mathrm{Gal}(K''|K')$ liegt offensichtlich im Kern. Daher muss sie aus Anzahlgründen gleich dem Kern sein. Also ist K' Galoissch und daher gleich K''. Da $\mathrm{Gal}(L|K_f) \subseteq \mathrm{Gal}(L|K')$ gilt $K' \subseteq K_f$. □

Sei K ein Körper mit diskretem Betrag. Wir haben in Satz 2.5.6 gesehen, das die Zerfällung eines Primideals $\mathfrak{p}$ in einer Körpererweiterung $L|K$ der Faktorzerlegung eines Polynoms in einem endlichen Körper entspricht (zumindest, falls $\mathcal{O}_L \cong \mathcal{O}_K[\omega]$, dann ist das Polynom einfach die Reduktion des Minimalpolynoms von ω.) Der gleiche Sachverhalt bleibt natürlich über den Vervollständigungen richtig. Nur gibt es dort, wie wir jetzt wissen, immer nur ein Primideal. Deshalb muss ein irreduzibles Polynom (welches als Minimalpolynom eines ω wie oben auftritt) in K modulo $\mathfrak{m}_K$ (bis auf eine Konstante) eine Potenz eines irreduziblen Polynom sein.
Dieselbe Folgerung gilt aber auch für ein beliebiges irreduzibles Polynom $f \in \mathcal{O}_K[X]$:

Lemma 5.5.7. *Let K ein vollständiger Körper mit diskretem Betrag $|\cdot|$ und Restklassenkörper $k = \mathcal{O}_K/\mathfrak{m}_K$. Sei $f \in \mathcal{O}_K[X]$ ein irreduzibles Polynom, dann ist entweder $\overline{f} = c$ mit $c \in k$, oder $\deg(f) = \deg(\overline{f})$ und $\overline{f} = c \cdot g^e$, wobei $g \in k[X]$ irreduzibel ist und $c \in k^*$.*

Beweis. Sei $f = a_n X^n + \cdots + a_0$. Wir unterscheiden drei Fälle:

1. $|a_n| < 1$ und $|a_0| < 1$. Dann ist $\frac{1}{a_n} \cdot f$ normiert. Falls dann $|\frac{a_0}{a_n}| \leq 1$ so folgt $|\frac{a_i}{a_n}| \leq 1$ für alle i, denn falls α eine Nullstelle von $\frac{1}{a_n} \cdot f$ ist, so ist α genau dann ganz, wenn $a_0 = N_{K(\alpha)|K}(\alpha)$ ganz ist (Satz 5.5.2). In diesem Fall ist also $\overline{f} = 0$. Ansonsten betrachte

   $$\widetilde{f} = a_n + a_{n-1}X + \cdots + a_0 X^n.$$

   Dies ist natürlich auch irreduzibel. Dann folgt aus derselben Argumentation entweder $\widetilde{\overline{f}} = 0$ also $\overline{f} = 0$ oder $|\frac{a_n}{a_0}| > 1$. Daher folgt $\overline{f} = 0$ in jedem Fall.

2. $|a_n| = 1$. Dann ist $\deg(f) = \deg(\overline{f})$. Die Galoisgruppe permutiert die Nullstellen von f. Da die Galoisgruppe (wegen der Eindeutigkeit des maximalen Ideals) auch auf $\mathcal{O}_L/\mathfrak{m}_L$ operiert, permutiert die Galoisgruppe der endlichen Körpererweiterung $\mathcal{O}_L/\mathfrak{m}_L|k$ auch die Nullstellen von $\overline{f}$. Daraus folgt aber, dass $\overline{f} = c \cdot g^e$ wobei $g \in k[X]$ irreduzibel ist.

3. $|a_0| = 1$. Dann hat $\widetilde{f}$ die Darstellung aus Fall 2. Dann folgt dies auch für f, es sei denn, für den konstanten Koeffizienten a_n von $\widetilde{f}$ gilt $|a_n| < 1$. Dann muss der konstante Koeffizient von g Null sein. Da g irreduzibel ist, folgt also $g = X$. Daher gilt $\widetilde{\overline{f}} = c \cdot X^n$, also $\overline{f} = c$.

□

Beachte, dass e hier *nicht* unbedingt der Verzweigungindex von $\mathfrak{m}_K$ in $L = K(\alpha)$ sein muss. Gegenbeispiel: $f = X^2 + 3$ über $\mathbb{Q}_2$ ist irreduzibel, und es gilt $\overline{f} = (X+1)^2$, aber die Erweiterung $\mathbb{Q}_2(\sqrt{-3})|\mathbb{Q}_2$ ist unverzweigt!
Aus dem Lemma folgt

Satz 5.5.8 (Henselsches Lemma)**.** *Sei K ein vollständiger Körper mit (diskretem) Betrag und Restklassenkörper k. Sei f ein Polynom in $\mathcal{O}_K[X]$ so dass $\overline{f} \neq 0$ und*

$$\overline{f} = \overline{h}_1 \cdot \overline{h}_2$$

in $k[X]$ mit $\overline{h}_1$ und $\overline{h}_2$ teilerfremd. Dann gibt es Lifts h_1 und h_2 nach $\mathcal{O}_K[X]$ so dass

$$f = h_1 \cdot h_2$$

und mit $\deg(h_1) = \deg(\overline{h}_1)$.

Beweis. Sei $f = f_1 \cdots f_n$ eine Zerlegung in irreduzible Faktoren (mehrfache Faktoren möglich). Wir können sicher annehmen, dass alle $f_i \in \mathcal{O}_K[X]$ liegen. Dann gilt

$$\overline{f} = \overline{f}_1 \cdots \overline{f}_n$$

und nach Lemma 5.5.7 gilt: $\overline{f}_i = c_i \cdot (g_i)^{e_i}$ für g_i irreduzibel oder $\overline{f}_i$ konstant. Falls nun

$$\overline{f} = \overline{h}_1 \cdot \overline{h}_2$$

eine Zerlegung in *teilerfremde* Faktoren ist, so teilt jedes $(g_i)^{e_i}$ genau einen der Faktoren. Daher können wir h_1 und h_2 als eine geeignete Konstante mal dem entsprechenden Produkt der f_i setzen. Die f_i mit konstanter Reduktion können wir als Faktoren von h_2 hinzufügen, so dass $\deg(h_1) = \deg(\overline{h}_1)$ erfüllt ist. □

Bemerkung 5.5.9. *Überlegen Sie sich als Übung, dass die Formulierung des Henselschen Lemma in Satz 5.5.8 sogar äquivalent ist zu der Aussage in Lemma 5.5.7.*

5.6 Newton Verfahren und Henselsches Lemma konstruktiv

Das Henselsche Lemma gilt in beliebigen vollstängigen Körpern mit nicht-Archimedischem Betrag. Wir geben in diesem Abschnitt einen konstruktiven Beweis für den Spezialfall, dass $\overline{g}_1$ eine Potenz eines Linearfaktors ist, also m.a.W. f modulo $\mathfrak{m}_K$ eine Nullstelle hat. Dann ist der konstruktive Beweis im wesentlichen das aus der Analysis bekannte Newton-Verfahren. Für einen Beweis des allgemeinen Falles siehe z.B. [N, II, 4.6].

Satz 5.6.1. *Sei K vollständing bzgl. eines nicht-Archimedischen Betrages $|\cdot|$. Sei $f \in \mathcal{O}_K[X]$ und $\alpha_0 \in \mathcal{O}_K$ mit*

$$|f(\alpha_0)| < |f'(\alpha_0)|^2$$

wobei f' die (formale) Ableitung von f ist. Dann konvergiert die Folge (α_n) mit

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

gegen ein $\alpha \in K$ mit $f(\alpha) = 0$ und $|\alpha - \alpha_0| \leq 1$.

Beispiel 5.6.2. *Das Henselsche Lemma für $\overline{h}_1$ linear folgt hieraus: Sei $\overline{\alpha} \in k$ eine* einfache *Nullstelle von $\overline{f}$. Sei $\alpha_0 \in \mathcal{O}_K$ ein Element mit $\alpha_0 \equiv \overline{\alpha}$ $(\mathfrak{m}_K)$. Dann ist $f(\alpha_0) \equiv f(\overline{\alpha}) \equiv 0$ $(\mathfrak{m}_K)$, also $|f(\alpha_0)| < 1$. Ausserdem ist $f'(\alpha_0) \equiv f'(\overline{\alpha}) \not\equiv 0$ $(\mathfrak{m}_K)$ (da $\overline{\alpha}$ eine einfache Nullstelle ist). Es folgt also $|f'(\alpha_0)| = 1$ und daher trivialerweise $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Es gibt also ein $\alpha \in \mathcal{O}_K$ mit $f(\alpha) = 0$ und $\alpha \equiv \overline{\alpha}$ $(\mathfrak{m}_K)$.*

Beweis von Satz 5.6.1. Setze

$$d := |f'(\alpha_0)| \leq 1 \quad c := \frac{|f(\alpha_0)|}{d^2} < 1$$

Wir zeigen die folgenden Aussagen per Induktion nach n:

1. $|\alpha_n| \leq 1$
2. $|\alpha_n - \alpha_0| \leq c$
3. $|f'(\alpha_n)| = d$.
4. $\frac{|f(\alpha_n)|}{|f'(\alpha_n)|^2} \leq c^{2^n}$.

1. Es gilt

$$|\alpha_{n+1}| \leq \max\{|\alpha_n|, \left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|\} \overset{\text{I.V.}}{\leq} \max\{1, cd\} = 1.$$

2. Es gilt

$$|\alpha_{n+1} - \alpha_0| = |\alpha_{n+1} - \alpha_n + \alpha_n - \alpha_0| \leq \max\{\left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|, |\alpha_n - \alpha_0|\} \overset{\text{I.V.}}{\leq} \max\{c^{2^n} d, c\} = c.$$

3. Nach der Taylorformel für f' gilt:

$$f'(\alpha_{n+1}) = f'(\alpha_n) + \xi \cdot \underbrace{(\alpha_{n+1} - \alpha_n)}_{\frac{f(\alpha_n)}{f'(\alpha_n)}}$$

mit $|\xi| \leq 1$, also

$$|f'(\alpha_{n+1})| \leq \max\{|f'(\alpha_n)|, |\xi| \cdot |\frac{f(\alpha_n)}{f'(\alpha_n)}|\} \overset{\text{I.V.}}{=} d.$$

Ausserdem gilt: $|\xi| \cdot |\frac{f(\alpha_n)}{f'(\alpha_n)}| \leq cd < d = |f'(\alpha_n)|$, also gilt sogar das Gleichheitszeichen.
4. Nach der Taylorformel für f gilt:

$$f(\alpha_{n+1}) = f(\alpha_n) + f'(\alpha_n) \cdot \underbrace{(\alpha_{n+1} - \alpha_n)}_{-\frac{f(\alpha_n)}{f'(\alpha_n)}} + \xi \cdot (\alpha_{n+1} - \alpha_n)^2$$

mit $|\xi| \leq 1$, also

$$|f(\alpha_{n+1})| \leq \left| \frac{f(\alpha_n)}{f'(\alpha_n)} \right|^2.$$

Dividieren durch $|f'(\alpha_{n+1})|^2 = |f'(\alpha_n)|^2$ ergibt:

$$\frac{|f(\alpha_{n+1})|}{|f'(\alpha_{n+1})|^2} \leq \left(\frac{|f(\alpha_n)|}{|f'(\alpha_n)|^2} \right)^2 \leq (c^{2^n})^2 = c^{2^{n+1}}.$$

Aus 3. und 4. folgt:

$$|\alpha_{n+1} - \alpha_n| = \frac{|f(\alpha_n)|}{|f'(\alpha_n)|} \leq d \cdot c^{2^n}.$$

Daher ist (α_n) eine Cauchy-Folge. Sei α der Grenzwert. Es gilt:

$$|f(\alpha_n)| \leq d^2 c^{2^n} \to 0.$$

Da f stetig ist, folgt $f(\alpha) = 0$. □

Wir haben die Aussage des Henselschen Lemmas hergeleitet aus der eindeutigen Normfortsetzung. Wir wollen nun umgekehrt zeigen, dass aus dem Henselschen Lemma (in der äquivalenten Form 5.5.7) die eindeutige Normfortsetzung folgt. Dazu zeigen wir zunächst:

Lemma 5.6.3. *Sei K ein Körper mit nicht-archimedischem Betrag $|\cdot|$ für den das Henselsche Lemma in der Form 5.5.7 gilt, und sei $L|K$ eine endliche Erweiterung. Sei $\mathcal{O}_L$ der ganze Abschluss des Ringes $\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ in L. Dann gilt:*

$$\mathcal{O}_L = \{x \in L \mid |N_{L|K}(x)| \leq 1\}.$$

Beweis. Wir wissen bereits, dass aus x ganz $N_{L|K}(x) \in \mathcal{O}_K$ folgt[24]. Sei umgekehrt $x \in L$ mit $|N_{L|K}(x)| \leq 1$ und

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

das Minimalpolynom von x. Es genügt, den Fall $L = K(x)$ zu betrachten. Dann gilt $a_0 = N_{L|K}(x)$. Wir können das Minimalpolynom mit einer Konstanten a_n mit $|a_n| \leq 1$ so multiplizieren, dass $a_n f \in \mathcal{O}_K[X]$ und so dass $\overline{a_n f} \neq 0$. Da $a_n f$ auch irreduzibel ist, folgt aus dem Henselschen Lemma, dass entweder $\overline{a_n f} = c$ oder, dass $\deg(\overline{a_n f}) = n$. Im ersten Fall kann c nicht 0 sein (dann hätten wir a_n zu klein gewählt), also ist $|a_n a_0| = 1$ und $|a_n| < 1$. Daher ist $|a_0| > 1$ im Widerspruch zur Annahme. Im zweiten Fall folgt $|a_n| = 1$, also $f \in \mathcal{O}_K[X]$, d.h. x ist ganz. □

Damit erhalten wir:

Satz 5.6.4. *Sei K ein Körper mit nicht-archimedischem Betrag $|\cdot|_K$ für den das Henselsche Lemma in der Form 5.5.7 gilt, und sei $L|K$ eine endliche Erweiterung. Dann definiert*

$$|x|_L := \sqrt[n]{|N_{L|K}(x)|_K}$$

die einzig mögliche Betragsfortsetzung von $|\cdot|_K$.

Beweis. Wir zeigen zunächst, dass $|\cdot|_L$ eine Betragsfortsetzung ist.

$$|x|_L = |x|_K$$

für $x \in K$ ist klar. Ausserdem folgen die Positivität und Multiplikativität auch sofort aus den elementaren Eigenschaften der Norm. Wir müssen also die verschärfte Dreiecksungleichung zeigen. Diese ist wegen der Multiplikativität äquivalent zu

$$|1 + \alpha| \leq \max\{1, |\alpha|\} = 1$$

für $|\alpha| \leq 1$. Wegen Lemma 5.6.3 sind wir also auf $x \in \mathcal{O}_L \Rightarrow x + 1 \in \mathcal{O}_L$ zurückgeführt, wobei $\mathcal{O}_L$ der ganze Abschluss von $\mathcal{O}_K$ in L ist. Dies gilt, da $\mathcal{O}_L$ ein Ring ist.
Wir müssen noch zeigen, dass die Fortsetzung die einzig mögliche ist. Sei $|\cdot|'$ eine andere Fortsetzung. Es genügt zu zeigen, dass für x mit $|N_{L|K}(x)|_K < 1$

[24]Dies bedarf vielleicht einer kleinen zusätzlichen Überlegung, falls $|\cdot|$ nicht diskret ist, denn dann ist $\mathcal{O}_K$ kein Dedekindring (da nicht Noethersch). Er ist aber immer noch ganzabgeschlossen, und dies reicht aus.

(also $|x|_L < 1$) gilt: $|x|' < 1$, denn dann sind $|\cdot|_L$ und $|\cdot|'$ äquivalent und also gleich, da sie auf K übereinstimmen. Sei also $x \in K$ mit $|N_{L|K}(x)|_K < 1$. O.B.d.A. ist $L = K(x)$. Sei f das Minimalpolynom von x:

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

mit $n > 1$, $|a_i| \leq 1$ und $|a_0| = |N_{L|K}(x)| < 1$. Dann folgt aus dem Henselschen Lemma, dass die Reduktion von f gleich X^n ist. Daher gilt $|a_i|_K = |a_i|' < 1$ für alle Koeffizienten. Aus

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

folgt dann auch $|x|' < 1$. □

Beachte, dass wir an keiner Stelle gefordert haben, dass K vollständig ist. Es reicht für die eindeutige Betragsfortsetzung und alles, was wir im letzten Abschnitt daraus gefolgert haben, dass das Henselsche Lemma für K gilt. Man kann daher z.B. für Zahlkörper die Komplettierung $K_\mathfrak{p}$ auch durch eine (unendliche) *algebraische* Erweiterung ersetzen, in der gerade soviele algebraische Elemente adjungiert wurden, dass das Henselsche Lemma gilt[25]. Diese Erweiterung heisst die **Henselisierung** von K bzgl. $|\cdot|_\mathfrak{p}$.

5.7 Struktur lokaler Körper

Wir haben im Abschnitt 5.2 gesehen, dass sich jede p-adische Zahl $x \neq 0$ eindeutig schreiben lässt als unendliche konvergente Summe

$$x = \sum_{i=N}^{\infty} a_i \cdot p^i$$

mit $a_i \in \{0, \ldots, p-1\}$ und $a_N \neq 0$. Es ist in dieser Darstellung nicht so einfach zu sehen, wie p-adische Zahlen addiert und multipliziert werden. Sicherlich gelten die Regeln für die Addition und Multiplikation von Potenzreihen auch für p-adische Zahlen. Nach Anwendung wird allerdings die Bedingung $a_i \in \{0, \ldots, p-1\}$ i.A. verletzt sein. Man kann diese Bedingung nun anschliessend mit Hilfe von Überträgen wiederherstellen, ganz ähnlich zu den Schulalgorithmen zur Addition von Zahlen in Basis 10.
Es gibt jedoch eine andere Repräsentation des Ringes der (ganzen) p-adischen Zahlen als *projektiver Limes* der endlichen Ringe $\mathbb{Z}/p^n\mathbb{Z}$. In dieser Repräsentation

[25] Für Details dieser Konstruktion siehe [N, II, §9, Aufgabe 4]. Im wesentlichen muss man im algebraischen Abschluss die Vereinigung aller Zerlegungskörper betrachten.

wird die Addition und Multiplikation sehr einfach. Beachte, dass die endlichen Ringe $\mathbb{Z}/p^n\mathbb{Z}$ mit Projektionsabbildungen

$$\cdots \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/p^3\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z}$$

ausgestattet sind, welche einfach dadurch gegeben sind, dass eine Restklasse modulo p^n als eine Restklasse modulo p^{n-1} aufgefasst wird. Der **projektive Limes** ist per Definition diejenige Teilmenge des (unendlichen) Produktes

$$\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z},$$

welche aus unendlichen Tupeln (a_n) mit $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ besteht, welche mit den Projektionen verträglich sind:

$$\lim_n \mathbb{Z}/p^n\mathbb{Z} := \{(a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z} \mid \pi(a_i) = a_{i-1}\ \forall i\}.$$

Beachte, dass $\prod \mathbb{Z}/p^n\mathbb{Z}$ einen Ring bzgl. komponentenweiser Addition und Multiplikation bildet. Überlegen Sie sich, dass der projektive Limes ein Unterring ist. $\prod \mathbb{Z}/p^n\mathbb{Z}$ ist auch ein topologischer Raum. Er ist mit der Produkttopologie der trivialen (diskreten) topologischen Räume $\mathbb{Z}/p^n\mathbb{Z}$ ausgestattet. Dies bedeutet, dass die offenen Mengen U genau diejenigen sind, so dass zu jedem Tupel $(a_n) \in U$ ein $N \in \mathbb{N}$ existiert, so dass auch $(a'_n) \in U$ falls $a_n = a'_n$ für alle $n < N$ (also insbesondere stimmen nur endlich viele überein).

Lemma 5.7.1.

$$\mathbb{Z}_p \cong \lim_n \mathbb{Z}/p^n\mathbb{Z}$$

als topologische Ringe.

Beweis. Wir haben gesehen, dass

$$\mathbb{Z}_p/p^n\mathbb{Z}_p = \mathbb{Z}/p^n\mathbb{Z}$$

ist. Die Abbildung ist also einfach durch die Projektionen $\mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ gegeben. Es ist deshalb auch klar, dass es ein Ringhomomorphismus ist.
Die Abbildung ist in obiger Darstellung konkret durch

$$\sum_{i=0}^{\infty} a_i p^i \mapsto \left(\overline{\sum_{i=0}^{n-1} a_i p^{n-1}}\right)_n$$

gegeben. Es ist also klar, dass es ein Isomorphismus ist (der Eintrag in $\mathbb{Z}/p^n\mathbb{Z}$ bestimmt bereits die a_i mit $i < n$ eindeutig). Den Beweis, dass die Abbildung ein Homöomorphismus ist, lassen wir als Übung. □

Bemerkung 5.7.2. *Überlegen Sie sich genauso, dass es für einen vollständigen Körper K mit diskretem Betrag $|\cdot|_K$ immer einen kanonischen Isomorphismus topologischer Ringe*

$$\mathcal{O}_K \cong \lim_n \mathcal{O}_K/\mathfrak{m}_K^n\mathcal{O}_K$$

gibt.

Bemerkung 5.7.3. *Aus der Beschreibung als projektivem Limes kann man auf sehr elementare Weise das folgende schliessen:*

- *Ein Polynom $f \in \mathbb{Z}[X_1, \ldots, X_m]$ hat genau dann eine Nullstelle in $\mathbb{Z}_p$ wenn die Kongruenzen*

$$f(x_1, \ldots, x_m) \equiv 0 \pmod{p^n}$$

  für alle n eine Lösung besitzen.

Das Henselsche Lemma impliziert, dass sogar eine einzige Kongruenz (für genügend grosses n) ausreicht.

Um sich den projektiven Limes und seine Topologie besser vorzustellen, hilft die folgende Beobachtung. Erinnere, dass die **Cantor-Menge** C in $\mathbb{R}$ definiert wird als der Durchschnitt der folgenden Sequenz (C_n) von Teilmengen. C_0 ist das abgeschlossene Intervall $[0,1] \subset \mathbb{R}$. Die Teilmenge C_1 ist $C_0 \setminus (\frac{1}{3}, \frac{2}{3})$. Es wird also das Intervall $[0,1]$ in drei Intervalle geteilt und das mittlere (offene) Intervall herausgenommen. C_n wird nun induktiv dadurch gebildet, dass in C_{n-1} alle Intervalle in drei Intervalle geteilt und das mittlere (offene) Intervall herausgenommen wird. Schliesslich ist

$$C := \bigcap_n C_n.$$

Überlegen Sie sich, dass C abgeschlossen (und somit kompakt) ist und genau aus denjenigen Zahlen in $[0,1]$ besteht, die eine (gewöhnliche!) 3-adische Entwicklung besitzen, in der die 1 nicht vorkommt.
Betrachte nun die Abbildung

$$\begin{array}{rcl} \mathbb{Z}_2 & \to & C \\ \sum a_i \cdot 2^i & \mapsto & \sum 2 \cdot a_i \cdot 3^{-i-1}. \end{array}$$

Überlegen Sie sich als Übung, dass dies ein Homöomorphismus ist.

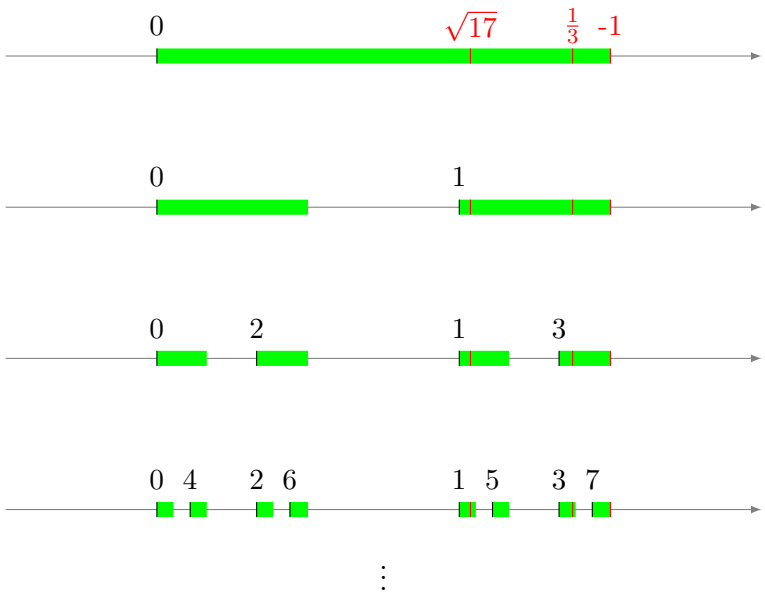


Abbildung 5: Die Mengen C_i mit den Bildern einiger natürlicher Zahlen unter dem Homöomorphismus $\mathbb{Z}_2 \cong C$. Beobachte die 2-adische Topologie: Zahlen liegen um so näher beieinander, je öfter ihre Differenz durch 2 teilbar ist. Zur Illustration wurden in rot einige 2-adische Zahlen $\notin \mathbb{N}$ eingefügt. Das maximale Ideal $2\mathbb{Z}_2$ besteht gerade aus der "linken Hälfte".

5.7.4. Im letzten Teil des Abschnittes wollen wir die Struktur der multiplikativen Gruppe einer endlichen Erweiterung K von $\mathbb{Q}_p$ untersuchen. Für die Komplettierungen eines Zahlkörpers bzgl. der Archimedischen Beträge, welche immer isomorph zu $\mathbb{R}$ oder $\mathbb{C}$ sind, erhalten wir mittels Exponentialabbildung und Logarithmus:

$$\begin{aligned} \mathbb{R}^* &\cong \mu_2 \times \mathbb{R}, \\ \mathbb{C}^* &\cong \mathbb{C}/2\pi i\mathbb{Z} \cong S^1 \times \mathbb{R}. \end{aligned}$$

Für eine endliche Erweiterung K von $\mathbb{Q}_p$ haben wir zunächst eine spaltende exakte Sequenz

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \underset{1\mapsto\pi_K}{\overset{x\mapsto\frac{\log|x|}{\log|\pi_K|}}{\rightleftarrows}} \mathbb{Z} \longrightarrow 1$$

Die Abbildung $\log|\cdot|$ haben wir geeignet skaliert, damit das Bild genau mit $\mathbb{Z}$ übereinstimmt. Daraus folgt:

$$\boxed{K^* \cong \mathbb{Z} \times \mathcal{O}_K^*}$$

algebraisch und topologisch (wobei $\mathbb{Z}$ die diskrete Topologie trägt).
Für die Gruppe $\mathcal{O}_K^*$ haben wir exakte Sequenzen

$$1 \longrightarrow U^{(n)} \longrightarrow \mathcal{O}_K^* \longrightarrow (\mathcal{O}_K/\mathfrak{m}_K^n)^* \longrightarrow 1$$

Hierbei ist $U^{(n)}$ gerade als der Kern der rechten Abbildung definiert. Die Surjektivität folgt aus der Tatsache, dass jedes Element $x \in \mathcal{O}_K$ mit $1-x \in \mathfrak{m}_K$ (d.h. also $|x|=1$) in $\mathcal{O}_K$ invertierbar ist. Es folgt auch

$$U^{(n)} = 1 + \mathfrak{m}_K^n.$$

Man kann sich überlegen, dass ähnlich wie im Fall $\mathcal{O}_K$ gilt:

$$\mathcal{O}_K^* \cong \lim_n \mathcal{O}_K^*/U^{(n)}.$$

Wir wollen aber anders vorgehen, und bemerken, dass obige exakte Sequenz für $n=1$ spaltet:

$$1 \longrightarrow U^{(1)} \longrightarrow \mathcal{O}_K^* \underset{l}{\overset{}{\rightleftarrows}} (\mathcal{O}_K/\mathfrak{m}_K)^* \longrightarrow 1$$

Dies folgt aus der Existenz des Teichmüllerliftes l (5.5.5). Wir erhalten:

$$\boxed{K^* \cong U(1) \times \mu_{q-1}}$$

wobei μ_{q-1} die Gruppe der $q-1$-ten Einheitswurzeln ist (das Bild von l). Hierbei ist $q = p^f$ die Anzahl der Elemente im Körper $\mathcal{O}_K/\mathfrak{m}_K$.
Die Struktur von $U^{(1)}$ lässt sich, wiederum mit Exponential- und Logarithmusreihe mit der additiven Gruppe von $\mathcal{O}_K$ in Verbindung bringen. Dazu benutzen wir den

Satz 5.7.5. *Sei e der Verzweigungsindex von $K|\mathbb{Q}_p$ (d.h. $|\pi_K| = p^{-\frac{1}{e}}$). Für $n > \frac{e}{p-1}$ definieren die gewöhnlichen Reihen für die Exponentialfunktion und den Logarithmus Isomorphismen topologischer Gruppen*

$$U^{(n)} \cong (1+\mathfrak{m}_K^n) \underset{\exp}{\overset{\log}{\underset{\longleftarrow}{\overset{\sim}{\longrightarrow}}}} \mathfrak{m}_K^n.$$

Beweisskizze. Die formalen Potenzreihen

$$\log(1+x) = \sum_n \frac{(-1)^{n+1}}{n} x^n$$

$$\exp(x) = \sum_n \frac{1}{n!} x^n$$

erfüllen die Identitäten

$$\exp(\log(1+x)) = 1+x \qquad \log(\exp(x)) = x$$

$$\exp(x+y) = \exp(x)\exp(y) \qquad \log((1+x)(1+y)) = \log(1+x) + \log(1+y)$$

Es genügt daher, zu zeigen, dass die Reihen exp und log auf den angegebenen Teilmengen von K konvergieren. Im nicht-Archimedischen gilt dies genau dann, wenn

$$|\frac{1}{n}| \cdot |x|^n \to 0 \quad \text{bzw.} \quad |\frac{1}{n!}| \cdot |x|^n \to 0.$$

Die erste Aussage gilt sogar, falls $|x| < 1$. Für die zweite muss man genau untersuchen, wie oft $n!$ durch p teilbar ist. Für Details siehe [N, II, §5]. Es zeigt sich $|x| < p^{-\frac{1}{p-1}}$ hinreichend ist. □

Damit ist $U^{(n)}$ für $n > \frac{e}{p-1}$ ein topologischer $\mathcal{O}_K$ und damit ein topologischer $\mathbb{Z}_p$-Modul. Es gilt sogar (algebraisch und topologisch)

$$\boxed{U^{(n)} \cong \mathfrak{m}_K^n = \pi_K^n \mathcal{O}_K \cong \mathcal{O}_K.}$$

Als $\mathbb{Z}_p$-Modul gilt (Existenz einer Ganzheitsbasis über Hauptidealringen)

$$\mathcal{O}_K \cong \mathbb{Z}_p^n,$$

wobei n der Grad von K über $\mathbb{Q}_p$ ist.
Behauptung: Auch $U^{(1)}$ ist ein $\mathbb{Z}_p$-Modul. Dazu muss man zeigen, dass

$$(1+x)^{p^m} = 1 \quad \text{in} \quad U^{(1)}/U^{(n)}$$

für $x \in \mathfrak{m}_K$ und genügend grosses m. M.a.W. $U^{(1)}/U^{(n)}$ hat p-Potenzordnung. Wir lassen dies als Übung. Dann gilt, da $U^{(n)}$ ein topologischer $\mathbb{Z}_p$-Modul ist,

$$(1+x)^{p^n} \to 0$$

auch in $U^{(1)}$ für $n \to \infty$.
Da $\mathbb{Z}_p$ ein Hauptidealring ist, und sowohl $U^{(1)}$, als auch $U^{(1)}/U^{(n)}$ (als endlicher Modul), als $\mathbb{Z}_p$-Moduln endlich erzeugt sind, gilt nach dem Hauptsatz für endlich erzeugte Moduln über Hauptidealringen

$$U^{(1)} \cong \mathbb{Z}_p/p^{a_1}\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p/p^{a_k}\mathbb{Z}_p \oplus \mathbb{Z}_p^{n'}.$$

Da aber endliche Untergruppen der multiplikativen Gruppe eines Körpers zyklisch sind, muss $k = 1$ sein. Da $U^{(1)}/U^{(n)}$ eine endliche Gruppe ist muss auch $n = n'$ sein, d.h.

$$\boxed{U^{(1)} \cong \mu_{p^a} \times \mathbb{Z}_p^n.}$$

Insgesamt haben wir bewiesen:

Satz 5.7.6. *Es gibt einen Isomorphismus topologischer Gruppen*

$$\boxed{K^* \cong \mathbb{Z} \times \mu_{p^f-1} \times \mu_{p^a} \times \mathbb{Z}_p^n.}$$

Dieser hängt nur von der Wahl eines uniformisierenden Elementes und der Wahl einer $\mathbb{Z}_p$-Ganzheitsbasis von $\mathcal{O}_K$ ab.

6 Klassenkörpertheorie (Überblick)

Im letzten Kapitel möchte ich die Klassenkörpertheorie kurz umreissen. Ich hoffe, dieses Kapitel zeigt Ihnen, dass die algebraische Zahlentheorie noch viel zu bieten hat, was über den Stoff der Vorlesung hinausgeht. Die Beweise der Klassenkörpertheorie sind nicht ganz einfach und z.B. im Buch von Neukirch [N] dargestellt. Um die Klassenkörpertheorie aber zu verstehen und anschaulich dargestellt zu bekommen sei das Buch [KKS2] empfohlen.

6.1 Klassenkörpertheorie über $\mathbb{Q}$

Den ersten Teil der Klassenkörpertheorie über $\mathbb{Q}$ haben wir schon kennengelernt. Es handelt sich um die Aussage

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

zusammen mit der Beobachtung dass ein Frobeniuselement $F_{\mathfrak{p}}$ (siehe 4.3.1) für ein Primideal $\mathfrak{p}$ über p (welches n nicht teilt) unter dieser Abbildung auf p abgebildet wird:

$$F_p \leftrightarrow p.$$

Wir haben hier F_p statt $F_{\mathfrak{p}}$ geschrieben. Dies ergibt Sinn, da die $F_{\mathfrak{p}}$ für die Primideale $\mathfrak{p}$ über p alle konjugiert sind. Die Galoisgruppe ist jedoch kommutativ. Daher sind sie alle gleich. Es gibt also eine Körperfamilie $\mathbb{Q}(\zeta_n)$ von Abelschen Erweiterungen von $\mathbb{Q}$ deren Galoisgruppe arithmetische Information über $\mathbb{Q}$ kodiert und dessen Frobeniuselemente einfach zu verstehen sind. Insbesondere folgt daraus, dass das Zerlegungsverhalten der Primzahlen in diesen Körpern nur durch eine Kongruenzbedingung an p bestimmt wird, denn die Frobeniuselemente bestimmen dieses. Der zweite Teil der Klassenkörpertheorie über $\mathbb{Q}$ liegt tiefer und wird durch den Satz von Kronecker und Weber beschrieben:

Satz 6.1.1 (Kronecker, Weber)**.** *Für jede endliche Abelsche Erweiterung K von $\mathbb{Q}$ existiert ein $n \in \mathbb{N}$, so dass*

$$K \subseteq \mathbb{Q}(\zeta_n).$$

Für eine Galoiserweiterung K von $\mathbb{Q}$ ist also für die Tatsache in einem Einheitswurzelkörper enthalten zu sein (und damit alle oben diskutierten Vorzüge zu geniessen) hinreichend, dass die Galoisgruppe Abelsch ist. Dies ist auf den ersten Blick äusserst überraschend und nicht leicht zu beweisen.

6.2 Klassenkörpertheorie über Zahlkörpern

Wie verallgemeinert sich diese Theorie auf Zahlkörper? Als Analogon der Gruppen $(\mathbb{Z}/n\mathbb{Z})^*$ kommen uns natürlich zunächst die Gruppen

$$(\mathcal{O}_K/n\mathcal{O}_K)^*$$

in den Sinn. Allerdings sind diese nicht (ganz) die korrekte Verallgemeinerung. Überraschenderweise spielt die Klassengruppe Cl_K eine Rolle, welche natürlich für $\mathbb{Q}$ trivial gewesen ist, und deshalb nicht aufgetaucht ist. Um die Darstellung etwas zu vereinfachen, nehmen wir für den Rest des Abschnittes an, dass K *nur komplexe Einbettungen hat.*
Für jedes n gibt es dann eine exakte Sequenz

$$1 \longrightarrow (\mathcal{O}_K/n\mathcal{O}_K)^*/\mathcal{O}_K^* \longrightarrow \mathrm{Cl}_K(n) \longrightarrow \mathrm{Cl}_K \longrightarrow 1$$

worin Cl_K die Klassengruppe ist und $\mathcal{O}_K^*$ die Gruppe der Einheiten. Die präzise Definition von $\mathrm{Cl}_K(n)$ werden wir nicht geben.
Zu jedem n gibt es wieder eine Abelsche Erweiterung K_n von K, den sogenannten n-ten **Strahlklassenkörper**, für den es einen kanonischen Isomorphismus

$$\mathrm{Gal}(K_n|\mathbb{Q}) \cong \mathrm{Cl}_K(n)$$

gibt. K_n ist allerdings nicht mehr so einfach explizit zu beschreiben. Jedes Primideal $\mathfrak{p}$ definiert wiederum ein eindeutiges Frobeniuselement $F_\mathfrak{p}$ (siehe 4.3.1) falls $\mathfrak{p} \nmid n$ und

$$F_\mathfrak{p} \leftrightarrow [\mathfrak{p}]$$

unter obigem Isomorphismus. (Jedes Primideal $\mathfrak{p} \nmid n$ hat eine Klasse in $\mathrm{Cl}_K(n)$, welche die gewöhnliche Klasse $[\mathfrak{p}]$ in der Klassengruppe Cl_K verallgemeinert[26].)
Dies impliziert (dies ist der Fall $n = 1$) insbesondere ein neues Phänomen: Es gibt eine Abelsche Erweiterung K_1 von K, für die es einen kanonischen Isomorphismus

$$\mathrm{Gal}(K_1|\mathbb{Q}) \cong \mathrm{Cl}_K$$

gibt. Dieser Körper K_1 heisst der **Hilbertsche Klassenkörper**. Er ist überall unverzweigt über K. Beachte, dass dies für $\mathbb{Q}$ nach dem Satz von Minkowski (4.1.3) a priori nicht passieren kann.
Der Satz von Kronecker und Weber verallgemeinert sich wie folgt:

[26] Sie ist genau dann trivial, wenn $\mathfrak{p} = (\alpha)$ ein Hauptideal ist, aber so dass $\alpha \equiv 1 \pmod{n}$.

Satz 6.2.1 (Hauptsatz der Klassenkörpertheorie)**.** *Für jede endliche Abelsche Erweiterung L von K existiert ein $n \in \mathbb{N}$, so dass*

$$L \subseteq K_n.$$

Falls L überall unverzweigt ist gilt sogar $L \subseteq K_1$. Der Hilbertsche Klassenkörper ist also die *maximale* Abelsche überall unverzweigte Erweiterung von K.
Die Strahlklassenkörper K_n (insbesondere bereits der Hilbertsche Klassenkörper) haben die Eigenschaft, dass *die Primideale von $\mathcal{O}_K$ zu Hauptidealen werden.* Die Primideale $\mathfrak{p} \subset \mathcal{O}_K$ sind darüberhinaus genau dann *voll zerlegt* in K_n, wenn $\mathfrak{p} = (\alpha)$ mit $\alpha \equiv 1 \pmod{n}$. Überlegen Sie sich, dass dies bereits aus der oben angesprochenen Entsprechung der Frobeniuselemente $F_\mathfrak{p}$ und der Klassen $[\mathfrak{p}]$ folgt, denn ein Primideal ist (in einer Galoiserweiterung) genau dann voll zerlegt, wenn $F_\mathfrak{p} = 1$.
Die Klassenkörpertheorie hat viele ganz konkrete arithmetische Konsequenzen, die mit den bisherigen Methoden der Vorlesung nicht zugänglich waren. Als Beispiel wollen wir folgenden Satz beweisen, der die Beobachtungen, die wir für einen imaginär quadratischen Zahlkörper mit Klassenzahl eins gemacht haben, ergänzt.

Satz 6.2.2. *Eine Primzahl $p \neq 2, 5$ ist genau dann von der Form $x^2 + 5y^2$ wenn $p \equiv 1$ oder 9 modulo 20.*

Beweis.

$$p \equiv 1, 9 \pmod{20}$$

ist gleichbedeutend zu

$$p \equiv \pm 1 \pmod{5} \quad \text{und} \quad p \equiv 1 \pmod{4}.$$

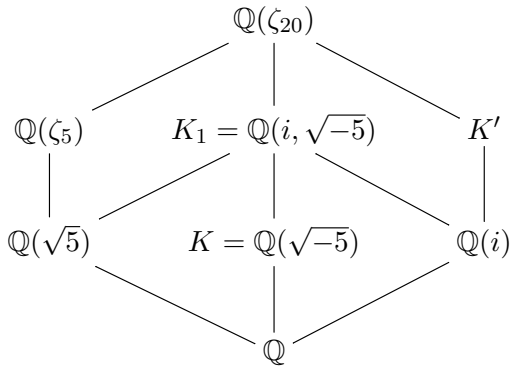
Falls $p = x^2 + 5y^2$ dann ist $p \equiv x^2 \pmod{5}$ und daher $p \equiv \pm 1 \pmod{5}$. Ebenso folgt aus $p \equiv x^2 + 5y^2 \equiv x^2 + y^2 \pmod{4}$ sofort $p \equiv 1 \pmod{4}$.
Umgekehrt folgt aus $p \equiv \pm 1 \pmod{5}$, dass $\left(\frac{-20}{p}\right) = \left(\frac{-5}{p}\right) = \left(\frac{p}{5}\right) = 1$, also ist p im Körper $K = \mathbb{Q}(\sqrt{-5})$ (mit Diskriminante -20) zerlegt. D.h. $(p) = \mathfrak{p} \cdot \overline{\mathfrak{p}}$ in $\mathcal{O}_K$. Falls $\mathfrak{p} = (x + y\sqrt{-5})$ ein Hauptideal wäre, so würde $p = x^2 + 5y^2$ folgen. $\mathcal{O}_K$ ist allerdings kein Hauptidealring! Dies war gerade unser Standardgegenbeispiel am Anfang der Vorlesung.
Wir müssen also zeigen (unter der Annahme dass $(p) = \mathfrak{p} \cdot \overline{\mathfrak{p}}$ in $\mathcal{O}_K$):

$$p \equiv 1 \pmod{4} \Rightarrow \mathfrak{p} \text{ Hauptideal.}$$

Hier kommt die Klassenkörpertheorie ins Spiel. Sie besagt, dass

$$\mathfrak{p} \text{ voll-zerlegt in } K_1 \Leftrightarrow \mathfrak{p} \text{ Hauptideal},$$

wobei K_1 der Hilbertsche Klassenkörper über K ist. Er hat Grad zwei über K, da die Klassengruppe von K gleich $\mathbb{Z}/2\mathbb{Z}$ ist.
Um K_1 zu finden, reicht es daher, eine quadratische Erweiterung von K zu finden, die überall unverzweigt ist.
Behauptung 1: $K(i)$ ist eine solche Erweiterung.
Wir stellen den Beweis der Behauptung für den Moment zurück. Aus der Behauptung folgt $K_1 = K(i)$. Dies ist (durch Zufall) sogar eine Abelsche Erweiterung von $\mathbb{Q}$. D.h. sie ist bereits in einem Einheitswurzelkörper enthalten. Da auch $K_1 = \mathbb{Q}(\sqrt{5}, i)$ und i eine vierte Einheitswurzel ist und $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ (wie wir wissen), tun es offensichtlich die zwanzigsten Einheitswurzeln. Wir haben folgendes Körperdiagramm:



welches den Untergruppen von

$$(\mathbb{Z}/20\mathbb{Z})^* = (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

entspricht.
Behauptung 2: p ist genau dann voll-zerlegt in $K_1 = \mathbb{Q}(i, \sqrt{-5})$ wenn p in $K = \mathbb{Q}(\sqrt{-5})$ und $\mathbb{Q}(i)$ zerlegt ist.
Aus dieser Behauptung folgt die Aussage, denn $p \equiv \pm 1 \pmod 5$ impliziert p (voll-)zerlegt in $\mathbb{Q}(\sqrt{-5})$ und $p \equiv 1 \pmod 4$ impliziert p (voll-)zerlegt in $\mathbb{Q}(i)$. Zusammen ist also p voll-zerlegt in K_1, d.h. insbesondere, dass $\mathfrak{p}$ (voll-)zerlegt ist in K_1, also $\mathfrak{p}$ ein Hauptideal ist.
Beweis Behauptung 1. Man kann zeigen, dass $\mathcal{O}_{K(i)} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}, i]$ ist. Für $p \neq 5$ ist p in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ unverzweigt. Sei $\mathfrak{p}$ ein Primideal von $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ über p. Um die weitere Zerlegung/Verzweigung von $\mathfrak{p}$ zu bestimmen, müssen

wir das Polynom X^2+1 in $\mathbb{F}_p$ bzw. in $\mathbb{F}_{p^2}$ faktorisieren, da $\mathbb{Z}[\frac{1+\sqrt{5}}{2}, i] = \mathbb{Z}[\frac{1+\sqrt{5}}{2}][X]/(X^2+1)$. Es folgt, dass unter diesen Primzahlen nur $p=2$ verzweigt und zwar mit Verzweigungsindex 2. Über 5 liegt in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ das Primideal $(\sqrt{5})$ mit Verzweigungsindex 2. Darüber findet ebenfalls keine weitere Verzweigung statt. Es folgt: Nur 2 und 5 sind in K_1 verzweigt, und zwar jeweils mit Verzweigungsindex 2. Nun sind die Verzweigungsindizes in einem Körperturm $K_1|K|\mathbb{Q}$ multiplikativ. In K sind ebenfalls genau 2 und 5 verzweigt, und auch (trivialerweise) mit Verzweigungsindex 2. Es folgt, dass die Erweiterung $K_1|K$ überall unverzweigt sein muss.
Beweis Behauptung 2. Für unverzweigte Primzahlen p ist p genau dann voll-zelegt in $K_1 = \mathbb{Q}(i, \sqrt{-5})$ bzw. in $K = \mathbb{Q}(\sqrt{-5})$ bzw. in $\mathbb{Q}(i)$, wenn das Frobeniuselement F_p in der jeweiligen Galoisgruppe trivial ist. Nun ist der Homomorphismus (durch die Einschränkungen gegeben)

$$\mathrm{Gal}(K_1|\mathbb{Q}) \to \mathrm{Gal}(K|\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)|\mathbb{Q})$$

bijektiv. D.h. das Frobeniuselement F_p ist genau dann trivial in $\mathrm{Gal}(K_1|\mathbb{Q})$ wenn die Einschränkungen auf $\mathbb{Q}(i)$ und K beide trivial sind. Diese Einschränkungen sind aber (wie man sich leicht überlegt) gerade die Frobeniuselemente F_p in $\mathbb{Q}(i)$ und in K. □

Die Tatsache, dass der Hilbertsche Klassenkörper von $\mathbb{Q}(\sqrt{-5})$ nicht nur Abelsch über $\mathbb{Q}(\sqrt{-5})$ sondern sogar Abelsch über $\mathbb{Q}$ ist, ist ein Zufall. Der obige Beweis bricht zusammen wenn dies nicht mehr der Fall ist. Z.B. kann der Umstand, ob p von der Form x^2+29y^2 ist, nicht mehr an einer Kongruenzbedingung an p abgelesen werden.

Inhaltsverzeichnis