Einführung in die algebraische Zahlentheorie

Wintersemester 2004/05

Christoph Schweigert
Universität Hamburg
Fachbereich Mathematik
Schwerpunkt Algebra und Zahlentheorie

(Stand: 06.02.2022)

Inhaltsverzeichnis

Literatur:

Literatur, die ich bei der Vorbereitung häufig herangezogen habe:

- Pierre Samuel: Algebraic theory of numbers, Hermann, 1970.
- Jürgen Neukirch: Algebraische Zahlentheorie, Springer, 1995.

Die aktuelle Version dieses Skriptes finden Sie unter
http://www.math.uni-hamburg.de/home/schweigert/skripten/zskript.pdf
als pdf-Datei. Verweise der Form Algebra 1, Satz n.n oder Algebra 2, Satz n.n beziehen sich auf meine Skripten zu den Vorlesungen Algebra 1 und Algebra 2. Sie sind unter
http://www.math.uni-hamburg.de/home/schweigert/skripten/a1skript.pdf
http://www.math.uni-hamburg.de/home/schweigert/skripten/a2skript.pdf
erhältlich.

Bitte schicken Sie Korrekturen und Bemerkungen an christoph.schweigert@uni-hamburg.de!

Bei Frau N. Potylitsina-Kube möchte ich mich für Ihre große Hilfe bei der Erstellung dieses Skriptes und bei Herrn Hartmann, Frau Kring und Herrn Dr. Mohrdieck für zahlreiche Hinweise bedanken.

1 Einleitung

Es gilt

$$2 = 1 + 1 \qquad 5 = 1 + 4 \quad 13 = 4 + 9 \quad 17 = 1 + 16$$
$$29 = 4 + 25 \qquad 37 = 1 + 36$$

Dies sind die ersten Primzahlen, die Summe zweier Quadrate sind. Für $3, 7, 11$ gilt das nicht.

Lemma 1.1.
Eine Quadratzahl lässt modulo 4 den Rest eins oder null.

Beweis.
n ist entweder gerade oder ungerade. Gilt $n = 2n'$, so ist $n^2 = 4(n')^2 = 0 \mod 4$ gilt $n = 2n'+1$, so gilt $n^2 = 4(n')^2 + 4n' + 1 = 1 \mod 4$. □
Unter den ungeraden Primzahlen p lassen sich also bestenfalls diejenigen als Summe von Quadraten schreiben, für die

$$p = 1 \mod 4$$

gilt. Wir wollen folgenden Satz verstehen:

Satz 1.2.
Für Primzahlen $p \neq 2$ gilt:

$$p = a^2 + b^2 \text{ mit } a, b \in \mathbb{Z} \Leftrightarrow p = 1 \mod 4.$$

Wir formulieren das Problem um, indem wir den Ring $\mathbb{Z}$ der ganzen Zahlen verlassen.

Definition 1.3

i) Ein Ring ist eine Menge mit zwei assoziativen Verknüpfungen $(R, +, \cdot)$ derart, dass

- *$(R, +)$ ist abelsche Gruppe, $(R, \cdot)$ ist eine assoziative Verknüpfung.*
- *Es gelten zwei Distributivgesetze*

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc$$

Man beachte, dass wir nicht gefordert haben, dass die Multiplikation kommutativ ist. Ist dies der Fall, so heißt der Ring kommutativ. Wir werden nur mit kommutativen Ringen zu tun haben.

ii) Ein Ring mit Eins oder unitaler Ring ist ein Ring mit einem Element $1 \in R$, so dass $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.
Ein wichtiges Beispiel für einen unitalen Ring ist der Ring der Polynome $K[X]$ mit Koeffizienten in einem Körper K. Tatsächlich können wir auch den Ring $R[X]$ der Polynome mit Koeffizienten in einem Ring R betrachten. Auch die ganzen Zahlen bilden einen Ring.

iii) Ein Ringhomomorphismus $\varphi : R \to S$ ist eine Abbildung, für die gilt

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b).$$

Für einen unitalen Ringhomomorphismus fordert man zusätzlich

$$\varphi(1) = 1.$$

iv) Ein kommutativer Ring R heißt nullteilerfrei oder integer, wenn für alle $a, b \in R$ aus $ab = 0$ folgt, dass $a = 0$ oder $b = 0$.

Beispiele 1.4.

i) Die ganzen Zahlen und die Polynomringe $\mathbb{R}[X]$ und $\mathbb{C}[X]$ sind integre Ringe.

ii) Der Ring $\mathbb{Z}_6 \cong \mathbb{Z}/6\mathbb{Z}$ ist nicht integer, da

$$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0} \mod 6.$$

iii) Der Ring der Gaußschen Zahlen

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} | a, b \in \mathbb{Z}\}$$
$$\mathrm{i} = \sqrt{-1} \quad \text{ist integer.}$$

Im Ring der Gaußschen Zahlen läßt sich die Gleichung

$$p = x^2 + y^2$$

als Produktzerlegung

$$p = (x + \mathrm{i}y)(x - \mathrm{i}y)$$

umschreiben.
Die Frage ist also, ob man die Primzahl p in größeren Ring $\mathbb{Z}[\mathrm{i}]$ zerlegen kann. Dafür brauchen wir das Analogon von Primzahlen in integren Ringen. Schon in $\mathbb{Z}$ ist ein Primzahlzerlegung eigentlich nicht eindeutig:

$$15 = 3 \cdot 5 = (-3)(-5).$$

Definition 1.5
Eine Einheit in einem Ring R ist ein Element $a \in R$, das ein multiplikatives Inverses besitzt: es gibt ein $b \in R$, so dass $ab = 1 \in R$ gilt. Die Menge $R^\times$ aller Einheiten bildet eine multiplikative Gruppe, die Einheitengruppe.

Beispiele 1.6.

i) Für $R = \mathbb{Z}$ ist $R^\times = \{\pm 1\}$

ii) Für $R = \mathbb{Q}$ ist $R^\times = \mathbb{Q} \setminus \{0\}$. Analoges gilt für alle Körper.

iii) Für $R[X]$ mit R integer gilt $R[X]^\times = R^\times$

iv) Für $\mathbb{Z}[\mathrm{i}]$ sind die Elemente $\{\pm 1, \pm \mathrm{i}\}$ Einheiten.

Definition 1.7

i) Ein Element eines Rings R heißt irreduzibel oder unzerlegbar, wenn $\pi \notin R^\times$ und aus $\pi = ab$ folgt, dass $a \in R^\times$ oder $b \in R^\times$.

ii) Ein Element $\pi \in R$ heißt Primelement, falls $\pi \neq 0$ und aus π teilt ab (d.h. $\exists c \in R$ und $\pi c = ab$) folgt, dass $\pi | a$ oder $\Pi | b$ für alle $a, b \in R$.

Lemma 1.8.
Sei R integer. Dann ist jedes Primelement von R auch irreduzibel. Beweis kommt als Übung.

Definition 1.9

i) Ein Element $a \in R$ besitzt eine Zerlegung in irreduzible Elemente, wenn a eine Darstellung

$$a = \varepsilon\pi_1\pi_2 \dots \pi_r$$

mit $\varepsilon \in R^\times$ und $\pi_i \in R$ irreduzibel hat. $r = 0$ ist dabei zugelassen.

ii) Ein integer Ring heißt faktoriell oder ZPE Ring, falls jedes Element $a \in R$, $a \neq 0$ eine eindeutige Zerlegung in irreduzible Faktoren besitzt. Ausführlicher heißt dies: gilt

$$a = \varepsilon\pi_1 \dots \pi_r = \varepsilon'\pi_1' \dots \pi_r' \,,$$

so folgt $r = r'$ und nach Umnummerierung

$$\pi_i = \varepsilon_i\pi_i'$$

mit $\varepsilon_i \in R^\times$.

Satz 1.10.
Sei R ein integrer Ring. R ist genau dann faktoriell, wenn jedes $a \in R \setminus \{0\}$ eine Zerlegung in irreduzible Faktoren besitzt und jedes irreduzible Element Primelement ist.

Beweis.
Siehe Satz 3.2.7 von Algebra 1. □
Im Beweis, dass der Ring $\mathbb{Z}$[i] der Gaußschen Zahlen faktoriell ist, verwenden wir:

Definition 1.11
Ein Integritätsring heißt euklidischer Ring, wenn es eine "Division mit Rest" gibt. Das heißt, dass es eine euklidische Normfunktion

$$N : R \to \mathbb{N}_0 = \mathbb{N} \cup \{0\}$$

gibt, mit $N(0) = 0$, und zu je zwei Elementen $a, b \in R$ mit $a \neq 0$ gibt es Elemente $q, r \in R$, so dass

$$b = qa + r$$

mit $N(r) < N(a)$. Man kann zeigen:

Satz 1.12.
Euklidische Ringe sind faktoriell.

Bemerkungen 1.13.

i) $\mathbb{Z}$ ist euklidisch mit Normfunktion

$$N(a) = |a|$$

ii) Der Polynomring $K[X]$ über einem Körper K ist euklidisch. Der Wert der Normfunktion eines Polynoms ist sein Grad plus Eins.

Satz 1.14.
Der Ring $\mathbb{Z}[\mathrm{i}]$ ist euklidisch, also insbesondere faktoriell.

Beweis.
Als Normfunktion verwenden wir

$$\begin{aligned} N : \mathbb{Z} &\to \mathbb{N}_0 \\ \alpha &\mapsto |\alpha|^2 \end{aligned}$$

Für $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ mit $\beta \neq 0$ suchen wir Gaußsche Zahlen γ, g mit

$$\alpha = \gamma\beta + \rho \ \text{ mit } \quad |\rho|^2 < |\beta|^2.$$

Dazu reicht es aus, ein $\gamma \in \mathbb{Z}[\mathrm{i}]$ zu finden mit

$$\Big|\frac{\alpha}{\beta} - \gamma\Big| < 1 \qquad ,$$

denn setze $\frac{\rho}{\beta} = \frac{\alpha}{\beta} - \gamma$. Aber $\mathbb{Z}[\mathrm{i}]$ bildet ein *Gitter* in der komplexen Zahlenebene.
Die Zahl $\frac{\alpha}{\beta}$ liegt von nächsten Gitterpunkt γ nicht weiter weg als $\frac{\sqrt{2}}{2} < 1$. □
Für den Beweis von Satz 1.2 brauchen wir noch

Lemma 1.15. *Satz von Wilson*
Sei p prim. Dann gilt

$$-1 = (p-1)! \mod p$$

Beweis.
kommt als Übung. □
Beweis.
von Satz 1.2. Sei p prim und von der Form $p = 1 + 4n$.

- Setze $x = 2n!$ und finde mit Lemma 1.15

$$\begin{aligned} -1 = (p-1)! &= [1 \cdot 2 \ldots (2n)][(p-1)(p-2)\ldots(p-2n)] \\ &= [(2n)!][(-1)^{2n}(2n)!] = x^2 \mod p \end{aligned}$$

  Also teilt p die Zahl $x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i})$. Aber p teilt weder $x + \mathrm{i}$ noch $x - \mathrm{i}$, da

$$\frac{x}{p} \pm \frac{\mathrm{i}}{p} \notin \mathbb{Z}[\mathrm{i}].$$

  Also ist p nicht prim. Da der Ring $\mathbb{Z}[\mathrm{i}]$ faktoriell ist, ist p auch nicht irreduzibel.

- Im faktoriellen Ring $\mathbb{Z}[\mathrm{i}]$ hat aber p eine Zerlegung in irreduzible Elemente. Daher gibt es $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ mit $p = \alpha\beta$, wobei weder α noch β Einheiten sind.

- In einer Übung werden Sie zeigen, dass für $\alpha \in \mathbb{Z}[\mathrm{i}]$ gilt: die Norm ist genau dann Eins, $N(\alpha) = 1$, wenn α Einheit ist (siehe auch Bemerkung 5.8 (iv) unten). Wegen

$$p^2 = N(p) = N(\alpha)N(\beta)$$

  heißt dies, dass

$$N(\alpha) = p$$

  gelten muss. Schreibt man $\alpha = a + \mathrm{i}b$ mit $a, b \in \mathbb{Z}$ folgt

$$a^2 + b^2 = p,$$

  also die gewünschte Zerlegerung.

□

Wir sehen, dass zahlentheoretische Fragen auf Ringe wie $\mathbb{Z}[\mathrm{i}]$ führen. Zentrale Fragen für solche Ringe sind die nach der Einheitengruppe und den Primelementen (bis auf Assoziierte, das heißt, dass Primelemente, die sich um eine Einheit unterscheiden, identifiziert werden.) Für unseren Fall ist die Einheitengruppe $\mathbb{Z}[\mathrm{i}]^\times = \{\pm 1, \pm \mathrm{i}\} \cong \mathbb{Z}_4$.

Definition 1.16
Zwei Elemente a, b eines Ring R heißen assoziiert, wenn sie sich um ein Element der Einheitengruppe unterscheiden,

$$a = \varepsilon b \text{ mit } \varepsilon \in R^\times.$$

Dies ist eine Äquivalenzrelation auf R.

Lemma 1.17.

i) Mit einem Element $a \in R$ sind auch alle seine assoziierten Elemente irreduzibel.

ii) Mit einem Element $a \in R$ sind auch alle seine assoziierten Elemente prim.

Beweis.

i) Sei a irreduzibel und b assoziiert zu a,

$$b = \varepsilon a \qquad \text{mit } \varepsilon \in R^\times$$

Sei $b = xy$ mit $x, y \in R$. Dann gilt $a = (\varepsilon)^{-1}xy$. Da a irreduzibel, folgt $y \in R^\times$ oder $\varepsilon^{-1}x \in R^\times$. $R^\times$ ist eine Gruppe, also gilt dann auch $x \in R^\times$.

ii) Wir überlegen uns zunächst, dass mit mit a auch jedes zu a assoziierte Element ein gegebenes Ringelement teilt. Denn sei b assoziiert zu a, also $b = \varepsilon a$. Gelte $a|c$, also $c = ad$ mit $d \in R$, so folgt $c = (\varepsilon a)(\varepsilon^{-1}d)$, also $b|c$.

Sei a nun prim und b assoziiert zu a. Aus $b|xy$ folgt, dass auch a das Produkt xy teilt. Da a prim sein soll, teilt a entweder x oder y, das gleiche gilt für b.

□

Satz 1.18.
Die Primelemente π von $\mathbb{Z}[\mathrm{i}]$ sind bis auf Assoziierte wie folgt gegeben: $\pi = 1 + \mathrm{i}$, $\pi = a + b\mathrm{i}$ mit $a^2 + b^2 = p$, wobei $p = 1 \bmod 4$ eine Primzahl ist und $a > |b| > 0$ gelten soll, sowie $\pi = p$ mit $p = 3 \bmod 4$ prim.

Beweis.

- Die Elemente $1 + \mathrm{i}$ und $\pi = a + b\mathrm{i}$ wie oben sind prim, weil aus einer Zerlegung

$$\pi = \alpha\beta \qquad \text{in } \mathbb{Z}[\mathrm{i}]$$

die Gleichung

$$p = N(\pi) = N(\alpha)N(\beta)$$

mit einer Primzahl p folgt, also $N(\alpha) = 1$ oder $N(\beta)) = 1$. Dann ist aber entweder α oder β eine Einheit. π ist also irreduzibel und im faktoriellen Ring $\mathbb{Z}[\mathrm{i}]$ daher prim.

- Die Zahlen $\pi = p$, $p = 3 \mod 4$ sind prim in $\mathbb{Z}[\mathrm{i}]$. Denn aus einer Zerlegung $p = \alpha\beta$ in Nichteinheiten α, β würde folgen

  $$p = N(\alpha) = a^2 + b^2,$$

  in Widerspruch zu Satz 1.2.

- Wir müssen noch zeigen, dass wir alle Primzahlen von $\mathbb{Z}[\mathrm{i}]$ erhalten haben.
  Sei $\pi = a + \mathrm{i}b$ prim. Dann kann man in $\mathbb{Z}$ zerlegen

  $$N(\pi) = \pi\overline{\pi} = p_1 \dots p_r.$$

  Da π in $\mathbb{Z}[\mathrm{i}]$ prim ist, teilt π eine Primzahl p. Deshalb teilt

  $$N(\pi) \big| N(p) = p^2.$$

  Also gilt $N(\pi) = p$ oder $N(\pi) = p^2$. Aus $N(\pi) = p$ folgt $p = a^2 + b^2$. Für $p \neq 2$ folgt $p = 1 \mod 4$. Für $p = 2$ ist π assoziiert zu $1 + \mathrm{i}$. Gilt $N(\pi) = p^2$, so ist π in $\mathbb{Z}[\mathrm{i}]$ assoziiert zu p. Es muss $p = 3 \mod 4$ gelten, da andernfalls π zerlegbar wäre.

□

Damit ist auch die Frage gelöst, wie sich Primelemente von $\mathbb{Z}$ beim Übergang zu $\mathbb{Z}[\mathrm{i}]$ verhalten:

- $p = 2$ ist wegen $2 = (1 + \mathrm{i})(1 - \mathrm{i}) = (-\mathrm{i})(1 + \mathrm{i})^2$ assoziiert zu dem Quadrat des Primelementes $(1 + \mathrm{i})$.
- Primzahlen $p = 3 \mod 4$ bleiben prim.
- Primzahlen $p = 1 \mod 4$ zerfallen in zwei konjugierte Faktoren

  $$p = (a + b\mathrm{i})(a - b\mathrm{i}).$$

Die Gaußschen Zahlen spielen im Körper

$$\mathbb{Q}(\mathrm{i}) = \{a + b\mathrm{i} | a, b \in \mathbb{Q}\}$$

die gleiche Rolle wie $\mathbb{Z}$ in $\mathbb{Q}$. Wir haben aber Ganzheit unbefriedigend definiert, nämlich durch Bezug auf die Koordinaten eines Elementes von $\mathbb{Q}(\mathrm{i})$ in der $\mathbb{Q}$–Basis $\{1, \mathrm{i}\}$. Besser ist die folgende Charakterisierung

Satz 1.19.
$\mathbb{Z}[\mathrm{i}]$ *besteht genau aus denjenigen Elementen von* $\mathbb{Q}(\mathrm{i})$*, die einer* normierten *Gleichung*

$$X^2 + aX + b = 0$$

mit Koeffizienten $a, b \in \mathbb{Z}$ *genügen.*

Beweis.
Das Element $\alpha = c + \mathrm{i}d \in \mathbb{Q}(\mathrm{i})$ ist Nullstelle des Polynoms $X^2 + aX + b \in \mathbb{Q}[X]$ mit

$$a = -2c$$
$$b = c^2 + d^2.$$

Sind c und d ganz, so auch a und b. Also sind die Elemente von $\mathbb{Z}[\mathrm{i}]$ Nullstellen ganzer normierter Gleichungen.

Sind umgekehrt a und b ganz, so ist $2c$ ganz und für die rationale Zahl

$$d = \frac{p}{q} \quad \text{mit} \quad p, q \quad \text{teilerfremd}$$

gilt

$$4b = (2c)^2 + \big(\frac{2p}{q}\big)^2.$$

Also ist

$$\frac{4p^2}{q^2}$$

ganz. Somit muss $q^2|4$ gelten, auch $2d$ ist ganz. Die Gleichung

$$4b = (2c)^2 + (2d)^2 = 0 \mod 4$$

kann aber nur für c, d eine ganze Lösung haben, wegen Lemma 1.1. □

Damit sind die großen Fragen elementarer algebraischer Zahlentheorie angerissen: wir werden Ringe ganzer Elemente betrachten. Darin werden wir die Einheitengruppe und die Primelemente beschreiben wollen. Dies wird uns auf zwei zentrale Fragen führen: die nach der Eindeutigkeit von Primzerlegungen und das Verhalten von Primelementen unter Ringerwieterungen.

2 Hilfsmittel aus der Algebra: Ringe und Ideale

Ganz so einfach wie bei den Gaußschen Zahlen können Lösungen auf solche Fragen im allgemeinen nicht sein.

Beispiele 2.1.
Man kann zeigen, dass im Ring $\mathbb{Z}[\sqrt{-5}]$ *gilt*

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

mit irreduziblen Faktoren. Um die Irreduzibilität der Faktoren einzusehen, betrachtet man die Normfunktion

$$N(a + b\sqrt{-5}) = a^2 + 5b^2,$$

merkt (vgl. 5.8 (iv) für die allgemeine Formulierung dieses Sachverhalts)

$$\alpha \in \mathbb{Z}[\sqrt{-5}]^\times \Leftrightarrow N(\alpha) = 1$$

und rechnet etwa: aus

$$3 = \alpha\beta$$

mit Nicht-Einheiten folgt $N(\alpha) = 3$, *aber*

$$3 = a^2 + 5b^2$$

hat keine ganzen Lösungen. Da

$$\frac{1 \pm 2\sqrt{-5}}{3} \qquad \frac{1 \pm 2\sqrt{-5}}{7}$$

nicht in $\mathbb{Z}[\sqrt{-5}]$ *liegen, sind die Elemente nicht assoziiert. Also hat 21 zwei verschiedene Zerlegungen in irreduzibel Element! Kummer postulierte daher die Existenz "idealer Zahlen"* $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ *und* $\mathfrak{p}_4$, *mit der Eigenschaft, dass*

$$3 = \mathfrak{p}_1\mathfrak{p}_2 \qquad 7 = \mathfrak{p}_3\mathfrak{p}_4 \qquad 1 + 2\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3 \quad 1 - 2\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4\,.$$

Damit löst sich die mehrdeutige Zerlegung von 21 wunderbar auf:

$$21 = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4).$$

Dedekinds Idee war dann die folgende: was auch immer "ideale Zahlen" seien mögen, man soll durch sie teilen können mit den folgenden Regeln:
Wenn $\mathfrak{p}$ die Zahlen a und b teilt, so soll $\mathfrak{p}$ auch Summe und Differenz $a \pm b$ teilen.
Wenn $\mathfrak{p}$ die Zahlen a teilt, so soll $\mathfrak{p}$ auch jedes Vielfache λa von a teilen.

Die Idee ist nun, eine ideale Zahl einfach durch die Menge all der Zahlen zu ersetzen, die durch sie teilbar sein sollen. Dies motiviert, die folgenden Untermengen eines Rings zu betrachten:

Definition 2.2
Sei R ein beliebiger kommutativer Ring mit Eins. Eine nicht–leere Teilmenge I von R heißt Ideal von R, wenn

$$\begin{array}{ll} (i) & a, b \in I \qquad\qquad \Rightarrow a + b \in I \\ (ii) & a \in I \text{ und } x \in R \Rightarrow ax \in I \end{array}$$

Ideale sind also insbesondere Unterringe und additive Untergruppen. R und (0) sind Ideale, die trivialen Ideale.

Bemerkungen 2.3.

i) Ist $\varphi : R \to R'$ ein Ringhomomorphismus, so ist

$$\text{Ker } \varphi = \{x \in R | \varphi(x) = 0\}$$

ein Ideal.

ii) Sei R ein Ring mit Eins und I ein Ideal von R. Betrachte die Äquivalenzrelation

$$a \sim b \quad \Leftrightarrow \quad a - b \in I.$$

Wir schreiben $a = b \mod I$ für $a \sim b$. Die Menge der Äquivalenzklassen

$$R/I = \{\overline{a} = \{a \in R | a \sim \overline{a}\}\}$$

ist ein Ring durch

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a + b} \\ \overline{a}\,\overline{b} &= \overline{ab} \end{aligned}$$

$\overline{R} := R/I$ heißt der Restklassenring modulo dem Ideal I. Die Abbildung

$$\begin{aligned} can : \qquad R &\to R/I \\ a &\mapsto \overline{a} \end{aligned}$$

heißt Restklassenabbildung oder kanonische Abbildung von R auf R/I. Es ist Ker *$can = I$. Es tritt also jedes Ideal als Kern eines Ringhomomorphismus auf.*

iii) Es gibt einen Isomorphiesatz für Ringe: ein Ringhomomorphismus

$$\varphi : R \to R'$$

induziert einen Isomorphismus von Ringen

$$\widetilde{\varphi} : R/\operatorname{Ker}\ \varphi \xrightarrow{\sim} Im\,\varphi.$$

Das heißt insbesondere: jeder Ringhomomorphismus ist als Komposition einer Surjektion mit einer Injektion darstellbar.

$$R \xrightarrow{can} R/\operatorname{Ker}\ \varphi \xrightarrow{\widetilde{\varphi}} R'$$

iv) Sei R kommutativer Ring mit Eins. Setze für jedes $a \in R$

$$(a) = Ra = \{ca|\ c \in R\}.$$

Dies ist ein Ideal, das von a erzeugte Hauptideal. Wir schreiben auch vereinfachend $x = y \bmod a$ für $x = y \mod (a)$ und R/a an Stelle von $R/(a)$.

Definition 2.4
Ein integrer Ring, in dem jedes Ideal ein Hauptideal ist, heißt Hauptidealring oder prinzipaler Ring

Bemerkungen 2.5.
Ein euklidischer Ring ist ein Hauptidealring.

Beweis.
Sei $\mathfrak{a} \subset R$ ein nicht–triviales Ideal. Sei $a \in \mathfrak{a}$ ein Element mit minimalem nicht–verschwindenden Wert der Normfunktion N. Die Inklusion $(a) \subseteq \mathfrak{a}$ ist klar. Sei $b \in \mathfrak{a}$ beliebig; schreibe im euklidischer Ring R

$$b = qa + r \text{ mit } N(r) < N(a).$$

Da aber $N(a)$ minimal ist, muss $N(r) = 0$ gelten, also $r = 0$. □

Es gibt aber Hauptidealringe, die nicht nicht euklidisch sind. In den Übungen werden wir dazu ein Beispiel kennen lernen. Wir formulieren als nächstes Teilbarkeit idealtheoretisch.

Lemma 2.6.
Sei R ein kommutativer Ring mit Eins.

i) $a|b \Leftrightarrow (b) \subseteq (a)$ für $a, b \in R$. Insbesondere $(a) = (b)$ genau, wenn a und b assoziiert sind.

ii) Mit $\mathfrak{a}_1$ und $\mathfrak{a}_2$ sind auch $\mathfrak{a}_1 \cap \mathfrak{a}_2$ und

$$\mathfrak{a}_1 + \mathfrak{a}_2 = \{a_1 + a_2 | a_i \in \mathfrak{a}_i\}$$

Ideale von R.

iii) $v \in R$ ist Vielfaches von a und b, wobei $a, b \in R \Leftrightarrow (v) \subseteq (a) \cap (b)$

iv) $d \in R$ ist Teiler von a und b, wobei $a, b \in R \Leftrightarrow (a) + (b) \subseteq (d)$

Beweis.

i) $a|b \Leftrightarrow b = xa$ mit $x \in R \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$

ii) Übung

iii) Die Aussage folgt aus (i).

iv) Übung.

□

Definition 2.7
Sei R ein kommutativer Ring, $a_1, \ldots, a_n \in R$. Wir definieren kgV und ggT durch die folgenden zwei Eigenschaften:

i) $ggT(a_1, \ldots, a_n)|a_i$ bzw. $a_i|kgV(a_1, \ldots, a_n)$ für alle $i = 1 \ldots n$.

ii) Aus $t|a_i$ bzw. $a_i|t$ für alle i folgt $t|ggT(a_1, \ldots, a_n)$ bzw. $kgV(a_1, \ldots, a_n)|t$.

Wenn ggT bzw. kgV existieren, so sind sie offenbar eindeutig bis auf Assoziiertheit.

Satz 2.8.

i) In Hauptidealringen existieren ggT und kgV. Wir haben

$$(kgV(a, b)) = (a) \cap (b)$$
$$(ggT(a, b)) = (a) + (b)$$

ii) Insbesondere existiert in Hauptidealringen zu beliebig vorgegebenen $a_1, \ldots, a_n \in R$ ein größter gemeinsamer Teiler d mit Darstellung

$$d = x_1a_1 + x_2a_2 + \ldots + x_na_n, \text{ mit } x_i \in R.$$

Beweis.

- Das Ideal $(a) \cap (b)$ ist im Hauptidealring R von der Form

  $$(v) = (a) \cap (b).$$

  Wegen Lemma 2.6 (iii) ist v dann Vielfaches von (a) und (b). Ist v' ein weiteres Vielfaches von (a) und (b), so folgt aus 2.6 (iii), dass

  $$(v') \subseteq (a) \cap (b) = (v)$$

  Also gilt $v|v'$. Damit ist v ein kgV und das kgV existiert.

- Finde im Hauptidealring R ein Element d, so dass

  $$(a_1) + \ldots + (a_n) = (d).$$

  Damit ist $(a_i) \subseteq (d)$, also teilt $d|a_i$. Sei d' ein weiterer Teiler aller a_i . Dann gilt $(a_i) \subseteq (d')$, also

  $$(d) = (a_1) + \ldots + (a_n) \subseteq (d')$$

  Also teilt d' auch d. d ist ein ggT. Die Darstellung von d folgt unmittelbar.

□

Satz 2.9.
Hauptidealringe sind faktoriell.

Beweis.
Man kann zeigen (Satz 3.2.9 von Algebra 1): Ein Ring R ist genau dann faktoriell, wenn

1. jede Kette $(a_1) \subseteq (a_2) \subseteq \ldots$ von Hauptidealen stationär wird, also wenn es ein n gibt, so dass
$$(a_m) = (a_n) \text{ für alle } m \geq n.$$
und
2. Jedes irreduzible Element prim ist.

Damit schließen wir:
Sei $(a_1) \subseteq \ldots$ eine Kette von Hauptidealen in einem Hauptidealring. Die Vereinigung
$$I := \bigcup_i (a_i)$$
ist ein Ideal und daher Hauptideal, $I = (a)$. Aus $a \in I$ folgt $a \in (a_n)$ für n groß genug. Somit gilt für alle $m \geq n$
$$(a_m) \subseteq I = (a) \subseteq (a_n) \subseteq (a_m)$$
Somit $(a_m) = (a_n)$ für alle $m \geq n$, jede Kette von Hauptidealen wird also stationär.
Sei π irreduzibel. Um zu zeigen, dass π auch prim ist, betrachte man $a, b \in R$ mit der Eigenschaft $\pi | ab$. Wir nehmen an, π teile nicht a. Da π irreduzibel ist, ist $ggT(\pi, a) = 1$. (Der ggT existiert nach Satz 2.8.) Aus Satz 2.8(ii) folgt die Darstellung
$$1 = x\pi + ya \qquad \text{mit } x, y \in R.$$
Also $b = bx\pi + yab$. Da π ja ab teilt, teilt π das Element b. Also ist π prim. □

Bemerkungen 2.10.

(i) Wir haben also die folgenden Inklusionen für Ringe
$$\textit{euklidisch} \Rightarrow \textit{prinzipal} \Rightarrow \textit{faktoriell}$$

(ii) Aus der Eindeutigkeit der Primzahlzerlegung in faktoriellen Ringen kann man, wie in $\mathbb{Z}$, die Existenz von kgV und ggT folgen.

Wir wollen nun auch die Teilerfremdheit von Idealen einführen:

Definition 2.11
Seien $\mathfrak{a}, \mathfrak{b}$ Ideale in einem Ring R mit Eins.

i) $\mathfrak{a}$ und $\mathfrak{b}$ heißen <u>teilerfremd</u>, falls $\mathfrak{a} + \mathfrak{b} = R$ ist.

ii) Die Menge
$$\mathfrak{ab} = \Big\{ \sum_{endlich} a_i b_i | a_i \in \mathfrak{a} \text{ und } b_i \in \mathfrak{b} \Big\}$$
heißt <u>Produkt</u> der Ideale $\mathfrak{a}$ und $\mathfrak{b}$. Sie ist ein Ideal von R mit
$$\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}.$$

Lemma 2.12.

i) Seien $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale. Dann ist

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}\,.$$

ii) Ist $\mathfrak{b}$ teilerfremd zu $\mathfrak{a}_i$, $i = 1 \ldots n$, so ist $\mathfrak{b}$ auch teilerfremd zum Produkt

$$\mathfrak{a}_1 \ldots \mathfrak{a}_n.$$

Beweis.

i) Da die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind, gibt es $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ mit $a + b = 1$. Daher gilt für $c \in \mathfrak{a} \cap \mathfrak{b}$

$$c = ac + cb \qquad \in \mathfrak{a}\mathfrak{b}$$

ii) Finde Darstellungen

$$1 = a_i + b_i \text{ mit } a_i \in \mathfrak{a}_i \text{ und } b_i \in \mathfrak{b}$$

Die Multiplikation dieser Identitäten liefert

$$\begin{aligned} 1 = \prod (b_i + a_i) &= b_1 \ldots b_n + \ldots + a_1 \ldots a_n \\ &\in \mathfrak{b} + \mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n, \end{aligned}$$

woraus aber $R = \mathfrak{b} + \mathfrak{a}_1 \ldots \mathfrak{a}_n$ folgt.

□

Satz 2.13. *(Chinesischer Restsatz)*
Seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ paarweise teilerfremde Ideale von R. Dann ist der natürliche Homomorphismus

$$\begin{aligned} R/\mathfrak{a}_1 \ldots \mathfrak{a}_n &\to R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n \\ x \mod \mathfrak{a}_1 \ldots \mathfrak{a}_n &\mapsto (x \mod \mathfrak{a}_1, \ldots, x \mod \mathfrak{a}_n) \end{aligned}$$

ein Isomorphismus von Ringen.
Das heißt insbesondere: gegeben $x_1, \ldots, x_n \in R$, so gibt es ein $x \in R$ mit $x = x_i \mod \mathfrak{a}_i$. x ist modulo dem Ideal $\mathfrak{a}_1 \ldots \mathfrak{a}_n$ eindeutig bestimmt.

Beweis.
Wegen Lemma 2.12 reicht es, den Fall $n = 2$ zu betrachten. Wir zeigen, dass der Ringhomomorphismus

$$\begin{aligned} \varphi : R &\to R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \\ x &\mapsto (x \bmod \mathfrak{a}_1, x \bmod \mathfrak{a}_2) \end{aligned}$$

surjektiv ist. Da $\mathfrak{a}_1$ und $\mathfrak{a}_2$ teilerfremd, finde $a_i \in \mathfrak{a}_i$ mit $1 = a_1 + a_2$. Für vorgegebene $x_1, x_2 \in R$ betrachte

$$x := x_2 a_1 + x_1 a_2$$

Es gilt

$$\begin{aligned} x &= x_2 a_1 + x_1(1 - a_1) = x_1 \qquad \mod \mathfrak{a}_1 \\ x &= x_2(1 - a_2) + x_1 a_2 = x_2 \qquad \mod \mathfrak{a}_2. \end{aligned}$$

Also ist φ surjektiv. Der Kern ist

$$\text{Ker } \varphi = \mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$$

wegen Lemma 2.12(i). □

Korollar 2.14.
Für teilerfremde natürliche Zahlen m, n gilt:

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Beweis.
Setze $R = \mathbb{Z}$, $\mathfrak{a}_1 = (m)$ und $\mathfrak{a}_2 = (n)$. □
Wir wollen abschließend noch zwei besondere Typen von Idealen definieren.

Definition 2.15
Sei R ein kommutativer Ring mit Eins.

i) Ein Ideal $\mathfrak{p} \in R$ heißt Primideal, falls $\mathfrak{p} \neq R$ und $R/\mathfrak{p}$ Integritätsring ist.

ii) Ein Ideal $\mathfrak{m} \in R$ heißt maximales Ideal, wenn $\mathfrak{m} \neq R$ ist und $R/\mathfrak{m}$ ein Körper ist.

Bemerkungen 2.16.

i) Jedes maximale Ideal ist Primideal, denn Körper sind nullteilerfrei. Die Umkehrung gilt nicht: ist R integer, aber kein Körper, so ist (0) ein Primideal, aber kein maximales Ideal.

ii) Wir stellen auch noch äquivalente Charakterisierungen vor:

- *Ein Ideal $\mathfrak{p}$ ist genau dann ein Primideal, wenn gilt*

$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p}.$$

- *Ein Ideal $\mathfrak{m}$ ist genau dann ein maximales Ideal, wenn für jedes Ideal $\mathfrak{a}$ mit $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$ gilt:*

$$\mathfrak{m} = \mathfrak{a} \text{ oder } \mathfrak{a} = R.$$

Der Beweis dieser Aussagen kommt als Übung.

iii) Jedes von R verschiedene Ideal eines Rings ist in einem maximalen Ideal enthalten. (Ohne Beweis, der das Zornsche Lemma benutzt.)

iv) Ein Element π eines Rings ist genau dann prim, wenn das zugehörige Hauptideal Primideal ist.

Denn nach (ii) gilt: (π) ist genau dann prim, wenn aus $xy \in (\pi)$ folgt $x \in (\pi)$ oder $y \in (\pi)$. Dies ist aber genau dann der Fall, wenn aus $\pi | xy$ folgt $\pi | x$ oder $\pi | y$.

3 Hilfsmittel aus der Algebra: Moduln

Körper sind spezielle Ringe. Wir müssen nun noch den Begriff des Vektorraums über einem Körper verallgemeinern.

Definition 3.1
Sei R ein kommutativer Ring mit Eins. Eine abelsche Gruppe – die wir in der Folge additiv schreiben – heißt R–Modul, falls es eine Skalarmultiplikation

$$\begin{aligned} R \times M &\to M \\ (\alpha, x) &\mapsto \alpha x \end{aligned}$$

gibt mit den folgenden Eigenschaften für alle $x, y \in M$ und $\alpha, \beta \in R$:

i) Assoziativität $\quad (\alpha\beta)x = \alpha(\beta x)$

ii) Distributivität $\quad (\alpha + \beta)x = \alpha x + \beta x$
$\qquad\qquad\qquad\quad \alpha(x + y) = \alpha x + \alpha y$

iii) Unitalität $\quad 1 \cdot x = x$

Bemerkungen 3.2.

i) Ist R ein Körper, so ist jeder R–Modul ein R-Vektorraum

ii) Wir vereinbaren die Regel "Punkt vor Strich".

iii) Wie bei Vektorräumen zeigt man

$$O_R m = O_M \qquad \text{für alle } m \in M$$

und schließt $\quad -m = (-1)m.$

iv) Jeder Ring ist Modul über sich selbst mit Skalarmultiplikation

$$\begin{aligned} R \times R &\to R \\ (\alpha, \beta) &\mapsto \alpha \cdot \beta \quad . \end{aligned}$$

v) Die Gaußschen Zahlen sind ein $\mathbb{Z}$–Modul.

Definition 3.3

i) Eine Abbildung $f : M \to N$ von einem R–Modul M in einen R–Modul N heißt <u>R–linear</u> oder <u>R–Modulmorphismus</u>, wenn gilt

$$\begin{aligned} f(m + m') &= f(m) + f(m') \\ f(rm) &= rf(m) \quad \text{für } m, m' \in M \text{ und } r \in R \quad . \end{aligned}$$

$Hom_R(M, N)$ bezeichne die Menge der R–Modulmorphismen.

ii) Ein bijektiver Homomorphismus von Moduln heißt <u>Isomorphismus</u>.

iii) Sei M ein R–Modul. Eine Untergruppe $U \subseteq M$ heißt Untermodul, falls $rm \in U$ gilt für alle $r \in R$ und $m \in U$.

Bemerkungen 3.4.

i) Die Untermoduln des Ringes R, aufgefasst als Modul über sich selbst, sind gerade die Ideale von R.

ii) Bild und Kern eines Modulhomomorphismus sind Untermoduln.

iii) Ist U ein Untermodul von M, so wird die Faktorgruppe M/U zu einem R–Modul, dem Faktormodul oder Quotientenmodul von M nach U durch die folgende Skalarmultiplikation

$$\begin{array}{rcl} R \times M/U & \to & M/U \\ (\alpha, x+U) & \mapsto & \alpha x + U \end{array} \tag{1}$$

Es gelten Homomorphiesätze, etwa:

- *für einen Modulhomomorphismus $f : M \to N$ gibt es einen kanonischen Isomorphismus*

$$\begin{array}{rcl} M/\operatorname{Ker} f & \tilde{\to} & f(M) \\ x + \operatorname{Ker} f & \mapsto & f(x) \end{array} \tag{2}$$

- *Für Untermoduln U, V eines R-Moduls M gilt*

$$(U+V)/V \cong U/(U \cap V)\,.$$

Zum Beweis betrachte man die Abbildung $\overline{u+v} \mapsto \overline{u}$.

- *Für Untermoduln U, V eines Moduls M mit $U \subseteq V \subseteq M$ gilt*

$$(M/U)\,/\,(V/U) \cong M/V\,.$$

Zum Beweis betrachte man die Abbildung $m + U \mapsto m + V$.

Definition 3.5

i) $A \subseteq M$ Teilmenge eines R–Moduls M. Dann bezeichnet

$$\langle A \rangle = \Big\{ \sum_{endl.} r_i m_i | r_i \in R \text{ und } m_i \in A \Big\}$$

den von A erzeugten Untermodul von M. Dies ist der kleinste Untermodul von M, der die Menge A enthält.

ii) Gilt $\langle A \rangle = M$, so heißt die Menge A Erzeugendensystem von M. M heißt endlich erzeugt, falls es ein endliches Erzeugendensystem gibt.

iii) Eine Familie $(m_\lambda)_{\lambda \in \Lambda}$ von Elementen eines Moduls heißt linear unabhängig oder frei, wenn aus

$$\sum_{\lambda \in \Lambda} r_\lambda m_\lambda = 0$$

mit $r_\lambda \in R$, nur endlich viele r_λ von Null verschieden, folgt $r_\lambda = 0$ für alle $\lambda \in \Lambda$.

iv) Eine Untermenge $S \subset M$ heißt Basis des Moduls M, falls S linear unabhängig ist und S ein Erzeugendensystem von M ist, $\langle S \rangle = M$.

v) Ein Modul heißt frei, wenn er eine Basis besitzt.

Bemerkungen 3.6.

(i) Ist R Körper und damit ein Modul M ein Vektorraum, so ist M freier Modul.

(ii) Beispiel eines Moduls, der nicht frei ist: $R = \mathbb{Z}$ und $M = \mathbb{Z}_2$ mit Skalarmultiplikation

$$r\bar{s} = \overline{rs} \quad .$$

Wegen $n\bar{0} = \bar{0}$ erzeugt $\{\bar{0}\}$ nicht, wegen $2 \cdot \bar{1} = \bar{0}$ ist $\{\bar{1}\}$ nicht linear unabhängig.

(iii) Ein R–Modul M ist genau dann frei, wenn

$$M \cong \bigoplus_{s \in S} R_s \quad .$$

Die direkte Summe von Moduln ist wie bei Vektorräumen definiert. Man kann zeigen: Je zwei Basen eines freien R–Moduls haben gleiche Mächtigkeit; diese heißt Rang von M. Es gilt $rang_R M = n$ dann und nur dann, wenn $M \cong R^n$ ist.

Wir brauchen eine spezielle Klasse von Moduln.

Satz 3.7.
Sei R kommutativer Ring mit Eins. Für einen R–Modul M sind die folgenden Bedingungen äquivalent:

i) Jede aufsteigende Kette $N_1 \subseteq N_2 \subseteq \ldots$ von Untermoduln wird stationär, d.h. es gibt einen Index k, so dass $N_i = N_k$ für alle $i \geq k$.

ii) Jede nicht–leere Menge von Untermoduln von M besitzt bezüglich Inklusion ein maximales Element.

iii) Jeder Untermodul von M ist endlich erzeugt.

Definition 3.8

(i) Ein R–Modul, der eine der Bedingungen aus Satz 3.7 erfüllt, heißt noetherscher Modul

(ii) Ein Ring heißt noethersch, wenn er als Modul über sich selbst noethersch ist.

Beweis.
[(von Satz 3.7)]

$(i) \Rightarrow (ii)$ Jede nicht–leere bezüglich Inklusion total geordnete Menge von Untermoduln von M besitzt eine obere Schranke: ist $N_1 \subseteq \ldots \subseteq N_k \subseteq \ldots$ eine Kette, so ist

$$\bigcup_i N_i = N_k$$

nach (i) eine obere Schranke. Nach dem Zornschen Lemma existiert ein maximales Element.

$(ii) \Rightarrow (iii)$ Sei $N \subseteq M$ Untermodul. Betrachte die Menge

$$X = \{N' | N' \subseteq N \text{ mit } N' \text{ endlich erzeugender Untermodul } \}$$

X enthält den Nullmodul, ist also nicht leer. Sei N_0 ein maximales Element. Gäbe es $x \in N \setminus N_0$, so wäre $N_0 \subsetneqq \langle N_0, x \rangle \in X$, im Widerspruch zur Maximalität von N_0. □

$(iii) \Rightarrow (i)$ Sei $N_1 \subseteq N_2 \subseteq \ldots$ eine Kette von Untermoduln. Die Vereinigung

$$N' = \bigcup_i N_i$$

ist Untermodul und nach (iii) endlich erzeugt:

$$N' = < x_1, \ldots, x_r >$$

Daher gibt es $k \in \mathbb{N}$, so dass $x_i \in N_k$ für alle $i = 1, \ldots, r$. Es folgt $N' \subseteq N_k$, die Kette wird daher stationär.

Bemerkungen 3.9.

i) Der folgende Ring ist nicht *noethersch:*

$$\begin{aligned} R &= \{f(x) \in \mathbb{Q}[X] | f(0) \in \mathbb{Z}\} \\ &= \{f = m + Xg \ mit \ m \in \mathbb{Z}, g \in \mathbb{Q}[X]\} \end{aligned}$$

Einer Untergruppe G von $(\mathbb{Q}, +)$ ordnen wir das Ideal

$$A_G = GX + X^2\mathbb{Q}[X]$$

von R zu. Insbesondere bekommen wir für die Untergruppen

$$G_i = \{\frac{m}{i} | m \in \mathbb{Z}\} \ , i \in \mathbb{N} \, ,$$

eine unendliche aufsteigende Kette von Idealen

$$A_{G_2} \subset A_{G_4} \subset \ldots \subset A_{G_{2^n}} \subset \ldots$$

ii) Man kann zeigen:
Untermoduln und epimorphe Bilder noetherscher Moduln sind noethersch.
Sind ein Untermodul U eines Moduls M und der zugehörige Faktormodul M/U noethersch, so ist auch M noethersch. Direkte Summen noetherscher Moduln sind noethersch.

Satz 3.10.
Sei R ein kommutativer noetherscher Ring und M ein R–Modul. M ist genau dann noethersch, wenn M endlich erzeugt ist.

Beweis.
Jeder noetherscher Modul ist als Untermodul seiner selbst endlich erzeugt. Sei umgekehrt $M = \langle a_1, \ldots, a_n \rangle$. Wegen der Surjektion

$$R^n \twoheadrightarrow M$$
$$(\alpha_1, \ldots, \alpha_n) \mapsto \sum_{i=1}^{n} \alpha_i a_i$$

ist M epimorphes Bild des freien Moduls R^n und als solches nach Bemerkung 3.9(ii) noethersch. □

Korollar 3.11.

i) Hauptidealringe sind noethersch. (Insbesondere ist der Ring der Gaußschen Zahlen noethersch.)

ii) Endlich erzeugte Moduln über Hauptidealringen sind noethersch.

Beweis.

i) Die Untermoduln sind gerade die Ideale, die in einem Hauptidealring sogar von nur einem Element erzeugt werden. Wegen Satz 3.7(iii) sind Hauptideale noethersch.

ii) folgt aus Satz 3.10.

□

4 Ganzheit

Definition 4.1

i) Ein algebraischer Zahlkörper ist eine endliche Körperweiterung K von $\mathbb{Q}$, d.h. $K \supseteq \mathbb{Q}$ und $\dim_{\mathbb{Q}} K < \infty$. Die Elemente von K heißen algebraische Zahlen.

ii) Eine algebraische Zahl heißt ganz, wenn sie Nullstelle eines normierten Polynoms $f \in \mathbb{Z}[X]$ ist.

Generalvereinbarung für den Rest der Vorlesung:
Im Folgenden seien alle Ringe kommutativ mit Eins.
Wir wollen Ganzheit allgemeiner fassen.

Definition 4.2
Sei $A \subset B$ eine Ringerweiterung. Ein Element $b \in B$ heißt ganz über A, wenn es einer normierten Gleichung

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0, \qquad n \geq 1$$

mit Koeffizienten $a_i \in A$ genügt.
Der Ring B heißt ganz über A, wenn alle Elemente $b \in B$ ganz über A sind.

Mit dieser Definition von Ganzheit ist nicht klar, ob Summen und Produkte ganzer Zahlen wieder ganz sind. Dafür brauchen wir die folgende Umformulierung:

Satz 4.3.
Endlich viele Elemente $b_1, \ldots, b_n \in B$ sind genau dann sämtlich ganz über A, wenn der Ring $A[b_1, \ldots, b_n]$, aufgefasst als A–Modul, endlich erzeugt ist.

Zum Beweis brauchen wir aus der linearen Algebra

Satz 4.4. *(Laplacescher Entwicklungssatz)*
Sei $A = (a_{ij})$ eine $r \times r$ Matrix über einem beliebigen Ring und $A^* = (a^*_{ij})$ die adjungierte Matrix, d.h.

$$a^*_{ij} = (-1)^{i+j} \det(A_{ij}) \quad ,$$

wobei die Matrix A_{ij} aus A durch Streichen der i–ten Spalte und j–Zeile entstellt. Dann gilt

$$AA^* = A^*A = \det(A)E \quad ,$$

wobei E die Einheitsmatrix ist. Für einen Vektor $x = (x_1, \ldots, x_r)$ folgt die Implikation

$$Ax = 0 \quad \Rightarrow \quad (\det A)x = 0$$

Beweis.
[(von 4.3)]

- Sei b ganz über A und $f(X) \in A[X]$ normiert von Grad $n \geq 1$ mit $f(b) = 0$. Da f normiert sein soll, können wir ein beliebiges Polynom $g \in A[X]$ in der Form

  $$g(X) = q(X)f(X) + r(X)$$

  schreiben, mit $q(X),\ r(X) \in A[X]$ und grad $r(x) < n$. Es gilt also

  $$g(b) = r(b) = a_0 + a_1 b + \ldots + a_{n-1}b^{n-1}$$

  mit $a_i \in A$. Daher wird $A[b]$ als A–Modul durch $1, b, \ldots, b^{n-1}$ erzeugt.

  Sind $\{b_1, \ldots, b_n\}$ ganz über A, wende vollständige Induktion nach n an: b_n ist ganz über $R := A[b_1, \ldots, b_{n-1}]$, also ist $R[b_n]$ endlich erzeugt über R, also über A, da nach Induktionsannahme R über A endlich erzeugt ist.

- Sei umgekehrt der A–Modul $A[b_1, \ldots, b_n]$ endlich erzeugt und $\omega_1, \ldots, \omega_r$ ein Erzeugendensystem. Für jedes $b \in A[b_1, \ldots, b_r]$ gilt dann

  $$b\omega_i = \sum_{j=1}^{r} a_{ij}\omega_j \qquad \text{mit } a_{ij} \in A \ .$$

  Es folgt mit Satz 4.4

  $$\det(bE - (a_{ij}))\omega_j = 0 \tag{3}$$

  für alle $i = 1 \ldots r$. Ferner finden wir eine Darstellung der Eins

  $$1 = c_1\omega_1 + \ldots + c_r\omega_r \qquad \text{mit } c_i \in A \ ,$$

  erhalten also durch entsprechendes Aufsummieren der Gleichungen (3)

  $$\det(bE - (a_{ij})) = 0 \ ,$$

  also eine nominierte Gleichung für b mit Koeffizienten in A. Also ist b ganz über A.

□

Korollar 4.5.
Sind b_1 und b_2 ganz über A, so sind auch $b_1 + b_2$ und $b_1 b_2$ ganz über A. Die ganzen Elemente bilden also einen Ring. Gegeben eine Ringerweiterung $A \subseteq B$, so heißt der Unterring von B

$$\bar{A} = \{b \in B | b \text{ ganz über } A\}$$

der ganze Abschluss von A in B. A heißt ganz abgeschlossen in B, wenn $A = \bar{A}$ gibt.

Beweis.
Nach Satz 4.3 ist jedes Element von $A[b_1, b_2]$ ganz, insbesondere also $b_1 + b_2$ und $b_1 b_2$. □

Satz 4.6.
Seien $A \subseteq B \subseteq C$ Ringerweiterungen. Ist C ganz über B und B ganz über A, so ist C ganz über A.

Beweis.
Sei $c \in C$, dann gibt es $b_i \in B$, so dass

$$c^n + b_{n-1} c^{n-1} + \ldots + b_0 = 0 \quad .$$

Da $b_1, \ldots b_n$ ganz über A sind, ist $R := A[b_1, \ldots, b_n]$ endlich erzeugter A–Modul, $R[c]$ ist endlich erzeugter R–Modul, also auch endlich erzeugter A–Modul. □

Körper sind ein wichtiges Hilfsmittel beim Studium von Ringen. Wir müssen also genug Inverse einführen können. Die folgende Konstruktion verallgemeinert die Konstruktion des Körpers der rationalen Zahlen $\mathbb{Q}$ aus dem Ring $\mathbb{Z}$ der ganzen Zahlen.

Definition 4.7

i) Eine Teilmenge S eines kommutativen Rings R mit Eins heißt multiplikativ, falls gilt

$$1 \in S \quad \text{und} \quad x, y \in S \Rightarrow xy \in S \quad .$$

ii) Betrachte auf der Menge $R \times S$ die Äquivalenzrelation

$$(r, s) \sim (r', s') \Leftrightarrow \exists s_1 \in S\,, \quad \text{so dass} \quad s_1(rs' - r's) = 0$$

Wir definieren die Lokalisierung von R nach S als die Menge der Äquivalenzklassen und schreiben

$$S^{-1}R = (R \times S)/\sim \quad .$$

Die Elemente von $S^{-1}R$ schreiben wir als Bruch, d.h. $\frac{r}{s}$ mit $r \in R$ und $s \in S$ für die Klasse von (r, s). Die üblichen Regeln der Bruchrechnung definieren eine Ringstruktur auf $S^{-1}R$:

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}$$
$$\frac{r}{s}\frac{r'}{s'} = \frac{rr'}{ss'}$$

mit $0 = \frac{0}{1}$ und $1 = \frac{1}{1}$.

$S^{-1}R$ heißt daher auch Quotientenring von R bezüglich S. (Die Terminologie ist etwas unglücklich, da man so auch an den Quotienten nach einem Ideal von R denken könnte.)

Bemerkungen 4.8.

i) Die kanonische Abbildung
$$\varphi_S : \ R \to S^{-1}R, \quad r \mapsto \frac{r}{1}$$
ist ein nicht–notwendigerweise injektiver Ringhomomorphismus. Die Elemente aus $\varphi_S(S)$ sind in $S^{-1}R$ invertierbar:
$$\left(\frac{s}{1}\right)^{-1} = \frac{1}{s} \qquad \text{für } s \in S \ .$$

ii) Sei R integer und $S = R \setminus \{0\}$. Dann ist S multiplikativ und $S^{-1}R$ ein Körper, der Quotientenkörper $\mathrm{Quot}(R)$ von R. Die kanonische Abbildung
$$\varphi_S : \ R \to S^{-1}R = \mathrm{Quot}(R)$$
ist dann sogar injektiv, so dass wir R als Unterring von $\mathrm{Quot}(R)$ auffassen dürfen.

Beispiel.

- $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$
- *Sei K ein Körper und $K[X] = R$ der Polynomring über K.*
$$K(X) = \mathrm{Quot}\left(K[X]\right) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in K[X], g \neq 0 \right\}$$
heißt rationaler Funktionenkörper über K in einer Variablen.

iii) Sei $\mathfrak{p} \subseteq R$ ein Primideal. Die Teilmenge
$$S_{\mathfrak{p}} := R \setminus \mathfrak{p}$$
ist multiplikativ: $1 \notin \mathfrak{p}$, also $1 \in S_{\mathfrak{p}}$. Die Negation von
$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \quad \textit{oder} \quad y \in \mathfrak{p}$$
ist
$$x \notin \mathfrak{p} \quad \textit{und} \quad y \notin \mathfrak{p} \Rightarrow xy \notin \mathfrak{p} \quad ,$$
daher ist $S_{\mathfrak{p}}$ multiplikativ.
Die Lokalisierung $R_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}R$ ist ein sogenannter lokaler Ring, das heißt, dieser Ring hat genau ein maximales Ideal:
$$\mathfrak{m} = \left\{ \frac{r}{s} \mid s \notin \mathfrak{p}, r \in \mathfrak{p} \right\} \quad .$$
Dies folgt mit Hilfe einer Aufgabe von Blatt 2, da genau die Elemente des Komplements
$$R \setminus \mathfrak{m} = \left\{ \frac{r}{s} \mid s \notin \mathfrak{p}, r \notin \mathfrak{p} \right\}$$
invertiert werden können.

iv) Wir wollen noch eine Erklärung des Namens lokal geben. Sei $X \subseteq \mathbb{R}^n$ offen, $x \in X$ ein Punkt und $\mathcal{O}$ der Ring von Keimen differenzierbarer Funktionen. Dieser Ring ist lokal: einziges maximales Ideal ist $\mathfrak{m}_x$, das Ideal der Funktionen, die in x verschwinden. Lokal – d.h. in einer hinreichend kleinen Umgebung von x – kann man jede Funktion f mit $f(x) \neq 0$ invertieren, d.h. $f^{-1}(y)$ existiert.

Definition 4.9

i) Ist A integer und $B = \mathrm{Quot}(A)$, so heißt der ganze Abschluß $\bar{A}$ von A in B die Normalisierung von A.

ii) A heißt ganz abgeschlossen schlechthin, falls $A = \bar{A}$.

Bemerkungen 4.10.

i) Jeder faktorielle Ring A ist ganz abgeschlossen. Sei $K = \mathrm{Quot}(A)$, $\frac{a}{b} \in K$ sei ganz über A:

$$(\frac{a}{b})^n + a_{n-1}(\frac{a}{b})^{n-1} + \ldots + a_0 = 0$$

für gewisse $a_i \in A$. Daher

$$a^n + a_{n-1}a^{n-1}b + \ldots + a_0 b^n = 0 \; .$$

Sei $\pi \in A$ prim und gelte $\pi \mid b$, so folgt $\pi \mid a$. Ist $\frac{a}{b}$ gekürzt geschrieben, so folgt $b \in A^\times$, also $\frac{a}{b} \in A$.

ii) Sei $A \subset B$ Ringerweiterung, $\bar{A}$ der ganze Abschluss von A in B. Dann ist $\bar{A}$ ganz abgeschlossen in B: sei $\bar{\bar{A}}$ der ganze Abschluss von $\bar{A}$, so ist

$$A \subseteq \bar{A} \subseteq \bar{\bar{A}} \subset B \quad .$$

Da $\bar{A}/A$ und $\bar{\bar{A}}/\bar{A}$ ganz, ist nach Satz 4.6 auch $\bar{\bar{A}}/A$ ganz, also $\bar{\bar{A}} \subseteq \bar{A}$.

Wir müssen uns etwas mehr mit Körpern beschäftigen.

Bemerkungen 4.11.

i) Sei R ein Ring, K ein Unterkörper von R. Ein Element $x \in R$ heißt algebraisch über K, wenn es Nullstelle eines Polynoms in $K[X]$ ist. Andernfalls heißt es transzendent. Offensichtlich fallen über einem Körper K die Begriffe "algebraisch" und "ganz" zusammen. Insbesondere folgt aus $[K(x) : K]$ endlich, dass x algebraisch ist. Die algebraischen Elemente von R bilden einen Unterring.

ii) Der Ring R heißt algebraisch, wenn alle Elemente algebraisch über K sind.

iii) Sei $L \supseteq K$ eine Körpererweiterung. Wir nennen $\dim_K L =: [L : K]$ den Körpergrad von L über K. Aus $[L : K] < \infty$ folgt wieder, dass L/K algebraisch ist. In einem Körperturm $K \subseteq K' \subseteq K''$ gilt die Gradformel:

$$[K'' : K] = [K'' : K'] \cdot [K' : K] \, .$$

iv) Sei wieder R ein Ring und $K \subseteq R$ ein Körper. Für jedes $\alpha \in R$ gibt es einen eindeutigen Ringhomomorphismus

$$\varphi_\alpha : \quad K[X] \to R$$

mit $\varphi_\alpha(a) = a$ für $a \in K$ und $\varphi_\alpha(X) = \alpha$, den Einsetzungshomomorphismus. Das Element α ist genau dann algebraisch über K, wenn der Kern des Einsetzungshomomorphismus nicht trivial ist, $\mathrm{Ker}\,(\varphi_\alpha) \neq (0)$. *Da der Polynomring $K[X]$ ein Hauptidealring ist, wird der Kern von einem Element erzeugt,*

$$\mathrm{Ker}\ \varphi_\alpha = \big(\min_K(\alpha)\big)\,,$$

mit einem Polynom $\min_K(\alpha)$, das wir als normiert voraussetzen dürfen: das Minimalpolynom von α über K. Offenbar gilt: Sei $g \in K[X]$. Dann folgt aus $g(\alpha) = 0$, dass das Minimalplynom $\min_K(\alpha)$ das Polynom g teilt. Es ist

$$K[X]/\big(\min_K(\alpha)\big) = K(\alpha)\,.$$

Dies ist ein Körper, wenn $\min_K(\alpha)$ prim ist.

v) Sei K ein Körper und $f \in K[X]$ nicht konstant. Dann gibt es eine Körpererweiterung K'/K endlichen Grades, so dass f in $K'[X]$ in Linearfaktoren zerfällt.

Beweis.
Durch Induktion nach Grad f. Klar für $\mathrm{grad} f = 1$. *Sei p ein Primteiler von f. Setze*

$$K'' = K[X]/(p) \quad .$$

In K'' hat p eine Nullstelle y, also auch f. Setze

$$f = (X - y)p'(X) \quad \text{in } K''[X] \text{ und}$$

wende die Induktionsannahme an. □

vi) Allgemeiner sagt man, ein Körper K sei algebraisch abgeschlossen, wenn jedes nicht konstante Polynom in $K[X]$ in Linearfaktoren zerfällt.
Zum Beispiel ist der Körper der komplexen Zahlen algebraisch abgeschlossen. Mit transfiniten Methoden zeigt man, dass jeder Körper K Unterkörper eines algebraisch abgeschlossenen Körper C ist.
Fordert man zusätzlich, dass C/K algebraisch ist, so ist C eindeutig bis auf Isomorphie und heißt algebraischer Abschluss.

Definition 4.12

i) Seien zwei Körper L und L' gegeben, die einen gemeinsamen Unterkörper K enthalten mögen. Dann heißt einen Ringhomomorphismus von L nach L'

$$\varphi : L \to L' \quad ,$$

der K elementweise festlässt, $\varphi(a) = a$ für alle $a \in K$, ein K–Homomorphismus. Ein solcher K-Homomorphismus φ ist notwendigerweise injektiv. Ist φ überdies surjektiv, so heißen die beiden Körper L und L' konjugiert über K.

ii) Zwei Elemente $\alpha \in L$ und $\alpha' \in L$ heißen konjugiert, wenn es einen K–Isomorphismus

$$\varphi : K(\alpha) \to K(\alpha')$$

gibt mit $\varphi(\alpha) = \alpha'$. Dieser ist eindeutig. Insbesondere sind α und α' entweder beide algebraisch oder beide transzendent. Im ersten Fall haben sie das gleiche Minimalpolynom.

Wir geben noch einige Resultate ohne Beweis an:

Resultate 4.13.

i) Sei $\operatorname{char}(K) = 0$ *oder K endlich, $f \in K[X]$ irreduzibel und*

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i)$$

seine Zerlegung in Linearfaktoren in einer Körpererweiterung K' von K. Dann sind die Nullstellen α_i paarweise verschieden.

ii) Sei $\operatorname{char}(K) = 0$ *oder $|K| < \infty$, K' eine endliche Körpererweiterung von K:*

$$[K' : K] = n \quad .$$

Dann gibt es genau n verschiedene K–Morphismen von K' in den algebraischen Abschluss C von K'.

iii) In der gleichen Situation existiert ein Element $\alpha \in K'$, so dass $K(\alpha) = K'$. Das Element α heißt primitives Element.

Es ist Zeit für ein ausführliches

Beispiel 4.14.

- *Ein quadratischer Körper ist eine Erweiterung von $\mathbb{Q}$ von Grad 2. Jedes $x \in K \setminus \mathbb{Q}$ ist primitiv, da $\mathbb{Q}(x) \neq \mathbb{Q}$; sein Minimalpolynom ist von der Form*

$$x^2 + bx + c \quad mit \quad b, c \in \mathbb{Q}$$

mit Nullstellen $2x = -b \pm \sqrt{b^2 - 4c}$. Daher

$$\mathbb{Q}(x) = \mathbb{Q}(\sqrt{b^2 - 4c}) \quad .$$

Mit $b^2 - 4c = \frac{u}{v}$, wobei $u, v \in \mathbb{Z}$ als teilerfremd vorausgesetzt werden können, folgt

$$\mathbb{Q}(x) = \mathbb{Q}\big(\sqrt{\frac{u}{v}}\big) = \mathbb{Q}\big(\sqrt{\frac{uv}{v^2}}\big) = \mathbb{Q}(\sqrt{u \cdot v}) \; .$$

Also lässt sich jeder quadratischer Körper K als $\mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ quadratfrei schreiben. $\sqrt{d}$ ist Nullstelle von $X^2 - d$, daher in K konjugiert zu $-\sqrt{d}$. Ein $\mathbb{Q}$–Automorphismus von K ist:

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

- *Wir wollen den Ring A der Elemente von K bestimmen, die ganz über $\mathbb{Z}$ sind: sei $x = a + b\sqrt{d}$ ganz. Mit x ist auch $\sigma(x)$ ganz, also sind auch*

$$x + \sigma(x) = 2a \in \mathbb{Q}$$
$$x\sigma(x) = a^2 - db^2 \in \mathbb{Q}$$

Aber $\mathbb{Z}$ ist faktoriell, also nach Bemerkung 4.10(i) ganz abgeschlossen. Daher gilt

$$2a \in \mathbb{Z} \quad a^2 - db^2 \in \mathbb{Z} \quad . \tag{4}$$

Umgekehrt folgt aus (4) auch, dass $x = a + b\sqrt{d}$ ganz über $\mathbb{Z}$ ist, denn x ist Nullstelle des normierten Polynoms

$$X^2 - 2aX + a^2 - db^2 \in \mathbb{Z}[X]\,.$$

Aus (4) folgt $(2a)^2 - d(2b)^2 \in \mathbb{Z}$, also $d(2b)^2 \in \mathbb{Z}$. Da d quadratfrei ist, folgt $2b \in \mathbb{Z}$. Schreibe also $a = \frac{u}{2}$ und $b = \frac{v}{2}$ mit $u, v \in \mathbb{Z}$. Es folgt

$$u^2 - dv^2 \in 4\mathbb{Z}$$

Ist u gerade, so auch v. Ist v ungerade, so $v^2 = 1 \bmod 4$. Aber $u^2 = 0$ oder $1 \bmod 4$. d ist quadratfrei, also $d \neq 0 \bmod 4$. Es folgt $u^2 = 1 \mod 4$ und $d = 1 \mod 4$. Daher gilt:
Sei $K = \mathbb{Q}(\sqrt{d})$ mit d quadratfrei quadratischer Körper. Der Ring der ganzen Zahlen ist

(a) für $d = 2, 3 \mod 4$ $\qquad A = \{a + b\sqrt{d},\ \text{mit } a, b \in \mathbb{Z}\}$

(b) für $d = 1 \mod 4$ $\qquad A = \left\{\frac{1}{2}(a + b\sqrt{d}),\ \text{mit } a, b \in \mathbb{Z},\ a = b \mod 2\right\}$

$\mathbb{Z}$–Basen von A sind zum Beispiel

(a) $\{1, \sqrt{d}\}$

(b) $\left\{1, \frac{1}{2}(1 + \sqrt{d})\right\}$

In der Tat gilt:

$$\frac{1}{2}(u + v\sqrt{d}) = (\frac{u}{2} - \frac{v}{2})1 + v\frac{1}{2}(1 + \sqrt{d})$$

Wir führen noch ein wenig Terminologie ein: für $d > 0$ heißt der Körper $\mathbb{Q}(\sqrt{d})$ reell-quadratischer Körper, für $d < 0$ imaginär-quadratischer Körper.

5 Spur, Norm, Diskriminante

Betrachtung 5.1.
Sei A ein Ring, E ein freier *A–Modul von endlichem Rang n und*

$$u: \quad E \to E$$

ein Endomorphismus. Sei $\{e_i\}_{1 \leq i \leq n}$ eine Basis von E, und (a_{ij}) die Matrix von u in dieser Basis, so heißt

$$\mathrm{tr}u = \sum_{i=1}^{n} a_{ii} \qquad \textit{Spur}$$
$$\det u = \det(a_{ij}) \qquad \textit{Determinante}$$
$$f_u(X) = \det(X1_E - u) \qquad \textit{charakteristisches Polynom}$$

von u. Alle Größen sind von der Wahl der Basis unabhängig. Es gilt

$$\begin{array}{lcll} \mathrm{tr}(u+u') & = & \mathrm{tr}(u)+\mathrm{tr}(u') & \mathrm{tr}(\lambda u)=\lambda\,\mathrm{tr}u \\ \det(uu') & = & \det(u)\det(u') & \det(\lambda u)=\lambda^n\,\det(u) \\ \det(X1_E-u) & = & X^n-\mathrm{tr}(u)X^{n-1}+\ldots+(-1)^n\det(u)\;. & \end{array}$$

Definition 5.2
Sei $A\subseteq B$ eine Ringerweiterung, so dass B ein freier A–Modul von endlichem Rang n ist. Für jedes $x\in B$ ist

$$\begin{array}{rl} \mathbf{m}_x: & B\to B \\ & y\mapsto xy \end{array}$$

ein Endomorphismus des A–Moduls B. Spur und Norm eines Elements eines Elements $x\in B$ sind definiert als Spur und Determinante von $\mathbf{m}_x$:

$$\mathrm{tr}_{B/A}(x):=\mathrm{tr}(\mathbf{m}_x)\qquad N_{B/A}(x)=\det(\mathbf{m}_x)\quad .$$

Es folgt sofort, dass Gruppenhomomorphismen vorliegen: im Falle der Spur für die additiven Gruppen, im Falle der Norm für die multiplikativen Gruppen.

$$\begin{array}{rl} \mathrm{tr}_{B/A}: & B\to A \\ N_{B/A}: & B^*\to A^* \end{array}$$

Satz 5.3.
Sei L/K eine endliche Körpererweiterung, $\mathrm{char}\,(K)=0$ *oder $|K|<\infty$. Durchläuft*

$$\sigma:\quad L\to\bar{K}$$

die K–Homomorphismen von L in den algebraischen Abschluss $\bar{K}$ von K, so gilt

$$\begin{aligned} f_u(X)&=\prod_\sigma(X-\sigma u) \\ \mathrm{tr}_{L/K}(u)&=\sum_\sigma\sigma u \\ N_{L/K}(u)&=\prod_\sigma\sigma u\quad . \end{aligned}$$

Beweis.

- Sei $\min_K(u)$ das Minimalpolynom von u, das vom Grade m sei. Dann ist $\{1,u,\ldots,u^{m-1}\}$ eine K–Basis von $K(u)$, also
$$m=[K(u):K]\quad .$$
Sei $d:=[L:K(u)]$ und $\{\alpha_i\}_{i=1,\ldots,d}$ eine $K(u)$–Basis von L. Dann ist $\{\alpha_iu^j\}_{\substack{i=1\ldots d\\ j=0,\ldots,m-1}}$ eine K–Basis von L.
In dieser Basis ist der Multiplikationsoperator m_u offenbar blockdiagonal mit identischen Blocks. Es folgt
$$f_u(X)=\big(\min_K(u)\big)^d\quad .$$

- Die Menge $Hom_K(L, \bar{K})$ versehen wir mit der Äquivalenzrelation

$$\sigma \sim \tau \Leftrightarrow \sigma u = \tau u \quad .$$

Es gibt wegen 4.13 genau m Klassen, die den Nullstellen von $\min_K(u)$ entsprechen. Sie haben alle die gleiche Mächtigkeit, nämlich d. Sei $\{\sigma_i\}$ ein Repräsentantensystem, dann ist

$$\min_K(x) = \prod_{i=1}^{m}(X - \sigma_i u) \quad .$$

Daher

$$f_u(X) = (\min_K(u))^d = \prod_{\sigma}(X - \sigma u) \quad .$$

Die anderen Behauptungen folgen sofort aus dieser Formel.

□

Korollar 5.4. *Schachtelungsformeln*
Für einen Körperturm $K \subseteq L \subseteq M$ endlicher Erweiterungen gilt

$$\begin{aligned} \mathrm{tr}_{L/K} \circ \mathrm{tr}_{M/L} &= \mathrm{tr}_{M/K} \\ N_{L/K} \circ N_{M/L} &= N_{M/K} \quad , \end{aligned}$$

wenn $\mathrm{char}\, K = 0$ *oder* $|K| < \infty$.

Beweis.
$Hom_K(M, \bar{K})$ zerfällt unter der Äquivalenzrelation

$$\sigma \sim \tau \Leftrightarrow \sigma_{|L} = \tau_{|L}$$

in $m := [L/K]$ Äquivalenzklassen. Sei $\{\sigma_i\}$ ein Repräsentantensystem für diese Äquivalenzklassen, so ist

$$Hom_K(L, \bar{K}) = \{(\sigma_i)_{|L}\} \quad .$$

Es folgt für $x \in M$:

$$\begin{aligned} \mathrm{tr}_{M/K}(x) &= \sum_{i=1}^{m} \sum_{\sigma \sim \sigma_i} \sigma x = \sum_{i=1}^{m} \mathrm{tr}_{\sigma_i M/\sigma_i L}(\sigma_i x) \\ &= \sum_{i=1}^{m} \sigma_i \mathrm{tr}_{M/L}(x) = \mathrm{tr}_{L/K}(\mathrm{tr}_{M/L}(x)) \end{aligned}$$

Der Beweis für die Norm verläuft analog. □

Wir kommen jetzt zu einem ganz zentralen Begriff der Vorlesung, dessen Bedeutung sich allerdings erst im Laufe der Zeit erhellen wird.

Definition 5.5
Sei $\mathrm{char}\, K = 0$ *oder* $|K| < \infty$. *Die Diskriminante einer Basis* $\{\alpha_1, \ldots, \alpha_n\}$ *einer endlichen Körpererweiterung* L/K *ist definiert als:*

$$d(\alpha_1, \ldots, \alpha_n) = \det\Big((\sigma_i \alpha_j)\Big)^2 \quad ,$$

wobei σ_i, $i = 1 \ldots n$ *die verschiedenen* K*–Einbettungen* $L \to \bar{K}$ *durchläuft.*

Bemerkungen 5.6.

i) Wegen

$$\mathrm{tr}_{L/K}(\alpha_i\alpha_j) = \sum_k (\sigma_k\alpha_i)(\sigma_k\alpha_j)$$

ist die Matrix $(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))$ *das Produkt der Matrizen* $(\sigma_k\alpha_i)^t$ *und* $(\sigma_k\alpha_j)$*. Daher gilt*

$$d(\alpha_1,\ldots,\alpha_n) = \det\Big(\mathrm{tr}_{L/K}(\alpha_i\alpha_j)\Big)$$

ii) Sei θ *primitives Element der Körpererweiterung* L/K*. Dann ist* $\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ *eine Basis von* L/K*. Wir setzen* $\theta_i = \sigma_i\theta$ *und erhalten die Matrix:*

$$(\sigma_i\theta^j) = \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix}$$

Nach Vandermonde gilt $\det(\sigma_i\alpha_j) = \prod_{i<j}(\theta_j - \theta_i)$*, also*

$$d(1,\theta,\ldots,\theta^{n-1}) = \prod_{i<j}(\theta_j-\theta_i)^2 \quad .$$

Satz 5.7.
Ist $\mathrm{char}\, K = 0$ *oder* $|K| < \infty$ *und* $\{\alpha_i\}_{1\le i\le n}$ *eine Basis von* L/K*, so ist die Diskriminante ungleich Null,*

$$d(\alpha_1,\ldots,\alpha_n) \neq 0$$

und es ist $(x,y) = \mathrm{tr}_{L/K}(xy)$ *eine nicht ausgeartete Bilinearform auf dem* K*–Vektorraum* L*.*

Beweis.
Sei θ ein primitives Element, $\{1,\theta,\ldots,\theta^{n-1}\}$ ist dann eine Basis von L/K. In dieser Basis ist

$$d(1,\theta,\ldots) = \prod_{i<j}(\theta_i-\theta_j)^2 \neq 0$$

Die Bilinearform ist in dieser Basis durch die Matrix $M = \mathrm{tr}_{L/K}(\theta^{i-1}\theta^{j-1})$ gegeben, deren Determinante gerade $d \neq 0$ ist. Somit ist die Bilinearform nicht ausgeartet. Bezüglich jeder anderen Basis $\{\alpha_1,\ldots,\alpha_n\}$ ist sie dann durch die Matrix

$$M = \Big(\mathrm{tr}_{L/K}(\alpha_i\alpha_j)\Big)$$

gegeben, deren Determinante ebenfalls nicht verschwinden kann:

$$d(\alpha_1,\ldots,\alpha_n) = \det(M) \neq 0 \quad .$$

□

Die im ersten Kapitel durchgeführten Betrachtungen für die Gaußschen Zahlen führen uns dazu, die folgende Situation zu betrachten:

- Gegeben sei ein ganzabgeschlossener Integritätsring A. Mit ihm kommt sein Quotientenkörper $K = \mathrm{Quot}(A)$. Wir werden immer annehmen, dass $\mathrm{char}\, K = 0$ oder $|K| < \infty$ gilt.
- Dann betrachten wir zusätzlich eine endliche Körpererweiterung L von K. Dies liefert uns einen weiteren Ring B, nämlich den ganzen Abschluss von A in L.

Bemerkungen 5.8.

i) *Jedes Element $\beta \in L$ hat die Gestalt*

$$\beta = \frac{b}{a} \text{ mit } b \in B \text{ und } a \in A$$

Denn da L/K endlich ist, ist β algebraisch über K: es gibt also $\tilde{a}_i \in K$, so dass

$$\beta^n + \ldots + \tilde{a_1}\beta + \tilde{a_0} = 0$$

gilt. Wir multiplizieren diese Gleichung mit dem Hauptnenner der Koeffizienten und erhalten eine Gleichung:

$$a_n\beta^n + \ldots + a_1\beta + a_0 = 0 \quad \text{mit } a_i \in A \text{ und } a_n \neq 0 \quad .$$

Diese Gleichung wiederum multiplizieren wir mit $(a_n)^{n-1}$ und erhalten

$$(a_n\beta)^n + \ldots + a_1'(a_n\beta) + a_0' = 0 \quad \text{mit } a_i' \in A \quad .$$

Also ist $a_n\beta$ ganz über A. Da aber B als ganzer Abschluss ganz abgeschlossen ist, folgt $b = a_n\beta \in B$. Insbesondere sehen wir, dass L der Quotientenkörper von B ist.

ii) *Sei $\beta \in L$. Dann ist β genau dann ganz über A wenn das Minimalpolynom in $A[X]$ liegt, $\min_K(\beta) \in A[X]$.*
"$\Leftarrow$" ist klar.
"$\Rightarrow$" Sei β Nullstelle eines normierten Polynoms $g \in A[X]$. Dann teilt $\min_K(\beta)$ das Polynom g in $K[X]$. Die Nullstellen von $\min_K(\beta)$ sind also auch Nullstellen von g und daher ganz. Damit sind aber auch die Koeffizienten von $\min_K(\beta)$ ganz. Da A ganzabgeschlossen ist, liegen sie in A.

iii) *Mit $\beta \in B$ sind auch alle Konjugierten von B ganz, denn sie haben das gleiche Minimalpolynom, das nach (ii) in $A[X]$ liegt. Daher sind $\mathrm{tr}_{L/K}(\beta)$ und $N_{L/K}(\beta)$ ganz und in K, da A ganzabgeschlossen ist, also sogar in A.*

iv) *Es gilt für $x \in B$: $x \in B^\times \Leftrightarrow N_{L/K}(x) \in A^\times$*
"$\Rightarrow$" $xy = 1$ impliziert $N_{L/K}(x)N_{L/K}(y) = 1$. Daraus folgt $N_{L/K}(x) \in A^\times$.
"$\Leftarrow$" Es gilt mit $a \in A$

$$1 = a\prod_\sigma \sigma x = \underbrace{(a\prod_{\sigma \neq id} \sigma x)}_{y} x$$

Das so definierte y liegt in L und ist ganz über A, also folgt $y \in B$. Somit hat x ein Inverses in B, $x \in B^\times$.

Lemma 5.9.
Sei $\alpha_1, \ldots, \alpha_n$ eine in B gelegene Basis von L/K mit Diskriminante $d = d(\alpha_1, \ldots, \alpha_n)$. Dann gilt

$$dB \subseteq A\alpha_1 + \ldots + A\alpha_n \quad .$$

Beweis.
Sei $\alpha \in B$; schreibe

$$\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \quad \text{mit } a_i \in K \ .$$

Es gilt

$$\mathrm{tr}_{L/K}(\alpha\alpha_j) = \sum_i a_i \mathrm{tr}_{L/K}(\alpha_i\alpha_j) \quad ,$$

die a_i sind also Lösungen eines linearen Gleichungssystems mit Koeffizienten in A. Ihr Nenner ist durch

$$d = \det\Big(\mathrm{tr}_{L/K}(\alpha_i\alpha_j)\Big)$$

gegeben, also

$$d\alpha \in A\alpha_1 + \ldots + A\alpha_n \quad .$$

□

Definition 5.10
Eine Ganzheitsbasis von B über A (auch A–Basis von B genannt) ist ein System $\{\omega_i\}_{i=1\ldots n}$ $\omega_i \in B$, so dass sich jedes $b \in B$ eindeutig *als Linearkombination*

$$b = \sum a_i\omega_i$$

mit $a_i \in A$ schreiben lässt. Falls eine Ganzheitsbasis existiert, ist sie auch K–Basis von L (beachte 5.8(i)), also ist $n = [L : K]$. B besitzt genau dann eine Ganzheitsbasis, wenn B freier *A–Modul von Rang $[L : K]$ ist. Man sagt dann auch, L/K besitze eine Ganzheitsbasis.*

Im allgemeinen gibt es keine Ganzheitsbasis; ist jedoch A ein Hauptidealring, so kann man die Existenz einer Ganzheitsbasis beweisen. Dafür zitieren wir:

Satz 5.11 (Hauptsatz über Moduln über Hauptidealringe)**.**
Sei R ein Hauptidealring und M ein freier A–Modul von endlichem Rang n. Sei M' ein Untermodul von M.

i) Dann ist M' ein freier Modul von einem Rang kleiner gleich n.

ii) Es gibt eine Basis $\{b_1, \ldots, b_n\}$ von M, eine ganze Zahl $q \leq n$ und nicht–verschwindende Elemente $a_i \in R$, so dass

- *$\{a_ib_i\}$ mit $i = 1, \ldots, q$ eine Basis von M' ist*
- *a_i teilt a_{i+1} für $1 \leq i \leq q-1$.*

Beweis.
P. Samuel, Kapitel 1.5 □

Satz 5.12.
Sei A ein Hauptidealring, $K = \mathrm{Quot}(A)$, L eine endliche Körpererweiterung und B der ganze Abschluss von A in L. Dann ist jeder endlich erzeugte B–Untermodul $M \neq 0$ von L ein freier A–Modul von Rang $[L : K]$. Insbesondere gilt dies für B selbst, das somit eine Ganzheitsbasis besitzt.

Beweis.

- Sei $\{\alpha_i\}_{i=1,\dots n}$ mit $n = [L : K]$ eine Basis von L/K. Wegen Bemerkung 5.8(i) können wir nach Multiplikation mit dem Hauptnenner annehmen, dass $\alpha_i \in B$. Wegen Lemma 5.9 ist
$$dB \subseteq A\alpha_1 + \ldots + A\alpha_n \quad .$$

- Sei $\mu_i, \ldots, \mu_r$ ein B-Erzeugendensystem von M. Es gibt wegen 5.8(i) ein $a \in A$, so dass $a\mu_i \in B$ für alle μ_i. Also gilt
$$aM \subseteq B$$
somit
$$ad\, M \subseteq dB \subseteq A\alpha_1 + \ldots + A\alpha_n \quad = M_0 \quad .$$
adM ist Untermodul des freien A–Moduls M_0. Aus dem Hauptsatz über Moduln über Hauptidealringen folgt, dass adM frei ist, somit auch $M \cong ad\, M$. Aus $ad\, M \subseteq M_0 \subseteq M$ folgt
$$\operatorname{rank} M = \operatorname{rank}(adM) \leq \operatorname{rank} M_0 \leq \operatorname{rank} M \quad .$$

□

In allgemeineren Situationen hilft manchmal der folgende

Satz 5.13.
Seien L/K und L'/K galoisch von Grad n bzw. n' und sei $L \cap L' = K$. Seien $\{\omega_i\}_{i=1\dots n}$ bzw. $\{\omega'_i\}_{i=1\dots n'}$ Ganzheitsbasen mit Diskriminanten d und d' in A. Sind diese teilerfremd, so gibt es $x, x' \in A$ mit
$$1 = xd + x'd' \quad ,$$
So ist $\{\omega_i\omega'_j\}$ Ganzheitsbasis von LL'/K mit Diskriminante $d^{n'}(d')^n$.

Beweis.
ausgelassen. (Neukirch, §2). □

Anwendung 5.14

Sei $\mathcal{O}_K$ der ganze Abschluss von $\mathbb{Z} \in \mathbb{Q}$ in einem algebraischen Zahlenkörper K.

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

Nach Satz 5.12 besitzt jeder endlich erzeugte $\mathcal{O}_K$–Modul $\mathfrak{a}$ in K eine $\mathbb{Z}$–Basis $\alpha_1, \ldots, \alpha_n$ mit $n = [K : \mathbb{Q}]$:
$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$$
Die Diskriminante $d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i\alpha_j)^2$ hängt nicht von der Wahl der Basis ab: sei $\{\alpha'_i\}$ eine andere Basis
$$\alpha'_i = \sum T_{ij}\alpha_j$$
mit $\det T \in \mathbb{Z}^\times = \{\pm 1\}$, daher
$$d(\alpha'_1, \ldots, \alpha'_n) = (\det(T))^2 d(\alpha_1, \ldots, \alpha_n)$$

Definition 5.15
$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n)$ *heißt* Diskriminante *des* $\mathcal{O}_K$*–Moduls* $\mathfrak{a}$*. Insbesondere heißt*

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

mit $\{\omega_i\}$ *Ganzheitsbasis von* $\mathcal{O}_K$ Diskriminante *des Zahlkörpers* K*.*

Satz 5.16.
Sind $\mathfrak{a} \subseteq \mathfrak{a}'$ *zwei von Null verschieden endlich erzeugte* $\mathcal{O}_K$*–Untermodul von* K*, so ist der Index* $[\mathfrak{a}' : \mathfrak{a}]$ *endlich und es gilt*

$$d(\mathfrak{a}) = [\mathfrak{a}' : \mathfrak{a}]^2 d(\mathfrak{a}')$$

Beweis.
Nach Satz 5.11 gibt es eine $\mathbb{Z}$–Basis $\{\alpha_i\}$ von $\mathfrak{a}'$ und $t_i \in \mathbb{Z}$, so dass $\{t_i\alpha_i\}$ eine $\mathbb{Z}$–Basis von $\mathfrak{a}$ ist. Für die Diskriminante folgt

$$\begin{aligned} d(\mathfrak{a}) &= \det\Big(\sigma_i(t_j\alpha_j)\Big)^2 \\ &= \Big(\prod_{j=1}^{n} t_j\Big)^2 \det(\sigma_i\alpha_j)^2 = \Big(\prod_{j=1}^{n} t_j\Big)^2 d(\mathfrak{a}') \quad . \end{aligned}$$

Aber

$$[\mathfrak{a}' : \mathfrak{a}] = \prod_{j=1}^{n} t_j \quad .$$

□

6 Dedekind–Ringe

Betrachtung 6.1.
Sei $\mathcal{O}_K$ *der Ring der ganzen Zahlen eines algebraischen Zahlkörpers. In* $\mathcal{O}_K$ *ist jede Nicht–Einheit Produkt irreduzibler Elemente. Denn ist* α *nicht irreduzibel, so gibt es* $\beta, \gamma \in \mathcal{O}_K$ *mit* $\alpha = \beta \cdot \gamma$*. Es folgt*

$$N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta) N_{K/\mathbb{Q}}(\gamma)\,.$$

Wegen Bemerkung 5.8 (iv) ist $N_{K/\mathbb{Q}}(\beta) \neq \pm 1$ *und* $N_{K/\mathbb{Q}}(\gamma) \neq \pm 1$*, also sind die Normen von* β, γ *sind echt kleiner als die von* α*. Man fährt dann rekursiv fort. Im allgemeinen ist aber diese Zerlegung in irreduzible Elemente nicht eindeutig.*

Definition 6.2
Ein noetherscher, ganzabgeschlossener integrer Ring, in dem jedes von Null verschiedene Primideal ein maximales Ideal ist, heißt Dedekindring*.*

Satz 6.3.
Sei K *ein algebraischer Zahlkörper. Dann ist* $\mathcal{O}_K$ *ein Dedekindring.*

Beweis.

- Der Ring $\mathcal{O}_K$ ist noethersch, denn er ist nach Satz 5.12 ein endlich erzeugter freier $\mathbb{Z}$–Modul, und als endlich erzeugter Modul über dem noetherschen Ring $\mathbb{Z}$ selbst noethersch.

- Als ganzer Abschluss von $\mathbb{Z}$ in K ist $\mathcal{O}_K$ nach 4.10(ii) ganz abgeschlossen.
- Sei $\mathfrak{p} \neq (0)$ ein Primideal von $\mathcal{O}_K$. Dann ist $\mathfrak{p} \cap \mathbb{Z}$ ein Ideal von $\mathbb{Z}$ und wegen

$$(\mathfrak{p} + \mathbb{Z})/\mathfrak{p} \cong \mathbb{Z}/\mathfrak{p} \cap \mathbb{Z}$$

  auch prim, d.h. $\mathfrak{p} \cap \mathbb{Z} = (p)$ für eine geeignete Primzahl p. Wir behaupten nämlich, dass $\mathfrak{p} \cap \mathbb{Z} \neq (0)$ gilt. Dazu wählen wir ein nichtverschwindendes $y \in \mathfrak{p}$ und betrachten eine eine Gleichung

$$y^n + \ldots + a_0 = 0$$

  minimalen Grads für y mit $a_i \in \mathbb{Z}$. Dann muss $a_0 \neq 0$ gelten, denn sonst könnte man y ausklammern, und die Gleichung wäre nicht mehr minimalen Grades. Es folgt, dass $0 \neq a_0 \in \mathfrak{p} \cap \mathbb{Z}$.
- Es bleibt zu zeigen, dass $\bar{\mathcal{O}} := \mathcal{O}_K/\mathfrak{p}$ ein Körper ist. Es ist ein Ring, der als Unterring den Körper $\bar{\kappa} := \mathbb{Z}/p\mathbb{Z}$ enthält. Alle Elemente x von $\bar{\mathcal{O}}$ sind algebraisch über $\bar{\kappa}$; sei die Gleichung

$$x^n + \ldots + \beta_0 = 0$$

  minimal mit $\beta_i \in \bar{\kappa}$, wobei aus dem gleichen Grund wie oben $\beta_0 \neq 0$ gilt. Daraus folgt aber

$$x\Big[(-\beta_0)^{-1}(x^{n-1} + \ldots + \beta_1)\Big] = 1 \quad ,$$

  also hat jedes x ein Inverses in $\bar{\mathcal{O}}$.

□

In Dedekindringen gilt:

Theorem 6.4.
Sei $\mathcal{O}$ ein Dedekindring. Dann besitzt jedes von (0) und $(1) = R$ verschiedene Ideal $\mathfrak{a}$ von $\mathcal{O}$ eine bis auf Reihenfolge eindeutige Zerlegung

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

in Primideale von $\mathcal{O}$.

Zum Beweis benötigen wir zwei Lemmata.

Lemma 6.5.
Sei $\mathcal{O}$ ein Dedekindring, $\mathfrak{a} \neq (0)$ ein Ideal. Dann gibt es von 0 verschiedene Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ mit

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a} \quad .$$

Beweis.
Sei $\mathfrak{M}$ die Menge der Ideale $\mathfrak{a}$ von $\mathcal{O}$, $\mathfrak{a} \neq (0)$, für die es keine Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ gibt mit $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a}$. Da $\mathcal{O}$ noethersch ist, wird jede aufsteigende Idealkette aus $\mathfrak{M}$ stationär, d.h. $\mathfrak{M}$ ist bezüglich Inklusion induktiv geordnet. Wäre $\mathfrak{M} \neq \emptyset$, so gäbe es nach dem Zornschen Lemma ein maximales Element $\mathfrak{a} \in \mathfrak{M}$. Da dies kein Primideal sein kann – ein Primideal liegt nicht in $\mathfrak{M}$ –, gibt es Elemente $b_1, b_2 \in \mathcal{O}$ mit $b_1, b_2 \notin \mathfrak{a}$, aber $b_1b_2 \in \mathfrak{a}$. Setze

$$\mathfrak{a}_1 = (b_1) + \mathfrak{a} \qquad \mathfrak{a}_2 = (b_2) + \mathfrak{a} \quad .$$

Dann gilt

$$\mathfrak{a} \subsetneqq \mathfrak{a}_1 \qquad \mathfrak{a} \subsetneqq \mathfrak{a}_2 \qquad \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a} \, .$$

Wegen der Maximalität von $\mathfrak{a}$ ist $\mathfrak{a}_1 \notin \mathfrak{M},\ \mathfrak{a}_2 \notin \mathfrak{M}$. Das heißt, es gibt Primideale

$$\mathfrak{p}_{1,1} \dots \mathfrak{p}_{1,n} \subseteq \mathfrak{a}_1$$
$$\mathfrak{p}_{2,1} \dots \mathfrak{p}_{2,m} \subseteq \mathfrak{a}_2$$

Also

$$\mathfrak{p}_{1,1} \dots \mathfrak{p}_{1,n}\mathfrak{p}_{2,1} \dots \mathfrak{p}_{2,m} \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$$

im Widerspruch zu $\mathfrak{a} \in \mathfrak{M}$. □

Lemma 6.6.
Sei $\mathfrak{p}$ ein Primideal des Dedekindrings $\mathcal{O}$, $K = \mathrm{Quot}(\mathcal{O})$ und

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

(insbesondere gilt $\mathcal{O} \subseteq \mathfrak{p}^{-1}$). Dann ist für jedes Ideal $\mathfrak{a} \neq (0)$ von $\mathcal{O}$ das Ideal

$$\mathfrak{a}\mathfrak{p}^{-1} = \{ \sum_{i \text{ endl.}} a_i x_i | a_i \in \mathfrak{a},\ x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a} \quad .$$

Beweis.

- Ist $\mathfrak{p} = (0)$, so ist $\mathfrak{p}^{-1} = K$. Dann ist aber $\mathfrak{a}K = K \neq \mathfrak{a}$.
- Sei also $\mathfrak{p} \neq (0)$. Wähle $a \in \mathfrak{p},\ a \neq 0$. Finde mit Lemma 6.5 Primideale

  $$\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$$

  mit r minimal.
  Dann gibt es ein $i \in \{1, \dots, r\}$, so dass $\mathfrak{p}_i \subseteq \mathfrak{p}$ gibt. Denn sonst finde für jedes i ein $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$; für diese gilt immer noch

  $$a_1 \dots a_r \in \mathfrak{p} \quad ,$$

  was für das Primideal $\mathfrak{p}$ nicht sein kann. Ohne Beschränkung der Allgemeinheit sei $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Im Dedekindring ist aber $\mathfrak{p}_1$ auch maximal, also $\mathfrak{p} = \mathfrak{p}_1$. r war minimal, also gilt nicht $\mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq (a)$. Finde $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r \setminus (a)$. Daher gilt $a^{-1}b \notin \mathcal{O}$. Andererseits ist $b\mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$. Somit gilt $a^{-1}b \in \mathfrak{p}^{-1}$. Damit ist $\mathfrak{p}^{-1} \neq \mathcal{O}$.
- Sei nun $\mathfrak{a}$ ein Ideal in $\mathcal{O}$. Da $\mathcal{O}$ noethersch ist, ist $\mathfrak{a}$ endlich erzeugt; $\{\alpha_1, \dots, \alpha_n\}$ sei ein Erzeugendensystem. Angenommen, es gälte $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Wir schließen daraus für jedes $x \in \mathfrak{p}^{-1}$:

  $$x\alpha_i = \sum_j a_{ij}\alpha_j \qquad \text{mit} \quad a_{ij} \in \mathcal{O} \quad .$$

  Sei

  $$A = (x\delta_{ij} - a_{ij}) \quad ,$$

  dann gilt $A(\alpha_1, \dots, \alpha_n)^t = 0$, also mit Satz 4.4 $d\alpha_1 = d\alpha_2 = \dots = d\alpha_n = 0$ für $d = det\ A$. Also $d = 0$, x ist Nullstelle eines normierten Polynoms in $\mathcal{O}[X]$, also ganz über $\mathcal{O}$. $\mathcal{O}$ ist als Dedekindring ganz abgeschlossen, also $x \in \mathcal{O}$. Es folgt $\mathfrak{p}^{-1} = \mathcal{O}$. Dies wurde oben aber schon ausgeschlossen, also ist $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ zum Widerspruch geführt.

□

Beweis.
[von Satz 6.4]

- Existenz einer Zerlegung in Primideale. Sei

$$\mathcal{M} = \{\mathfrak{a} \subseteq \mathcal{O} \text{ Ideale}, \mathfrak{a} \neq (0), (1) | \mathfrak{a} \text{ besitzt keine Zerlegung in Primideale}\}$$

  Wäre $\mathcal{M} \neq \emptyset$, schließen wir wie im Beweis von Lemma 6.5 aus $\mathcal{O}$ noethersch auf die Existenz eines maximalen Elements $\mathfrak{a} \in \mathcal{M}$. $\mathfrak{a}$ kann kein Primideal sein. Daher gibt es ein maximales Ideal $\mathfrak{p}$ von $\mathcal{O}$ mit $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{a} \neq \mathfrak{p}$. Aus Lemma 6.6 folgt

$$\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}^{-1} \text{ und } \mathfrak{p} \subsetneqq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O} \quad .$$

  Da das Primideal $\mathfrak{p}$ im Dedekindring maximal ist, folgt $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Aus $\mathcal{O} \subseteq \mathfrak{p}^{-1}$ schließen wir

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

  Ferner ist $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$, sonst hätte man $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. Da $\mathfrak{a}$ maximal in $\mathcal{M}$, folgt, dass $\mathfrak{a}\mathfrak{p}^{-1}$ eine Zerlegung $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ besitzt, aus der die Existenz der Zerlegung $\mathfrak{a} = \mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p}$ von $\mathfrak{a}$ folgt.

- Eindeutigkeit der Zerlegung. Seien

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s \tag{5}$$

  zwei Zerlegungen in Primideale. Nun gilt für ein Primideal $\mathfrak{p}$ und zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$:

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p} \text{ oder } \mathfrak{b} \subseteq \mathfrak{p}$$

  was wir auch umschreiben

$$\mathfrak{p} | \mathfrak{a}\mathfrak{b} \quad \Rightarrow \quad \mathfrak{p} | \mathfrak{a} \text{ oder } \mathfrak{p} | \mathfrak{b} \quad .$$

  Dies sieht man so ein: sonst gäbe es $a \in \mathfrak{a} \setminus \mathfrak{p}$ und ein $b \in \mathfrak{b} \setminus \mathfrak{p}$; da $\mathfrak{p}$ ein Primideal ist, folgt daraus $ab \notin \mathfrak{p}$. Andererseits ist aber $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, Widerspruch.

  Wir können hier ohne Einschränkung annehmen, dass $\mathfrak{p}_1 | \mathfrak{q}_1$, also $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Also $\mathfrak{p}_1 = \mathfrak{q}_1$, da $\mathfrak{q}_1$ als Primideal im Dedekindring maximal ist. Wir multiplizieren dann (5) $\mathfrak{p}_1^{-1}$, beachten $\mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O} \Rightarrow$ und erhalten

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

  Induktiv fortfahrend erhält man die Eindeutigkeit der Zerlegung.

□

Somit hat man für jedes Ideal $\mathfrak{a} \neq (0)$ in einen Dedekindring $\mathcal{O}$ eine eindeutige Darstellung

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r} \qquad \nu_i \in \mathbb{N}$$

wobei $\mathfrak{p}_i$ paarweise verschiedene Primideale sind und $\nu_i \in \mathbb{N}$ gilt.

Wir führen auch noch ein paar vereinfachende Schreibweisen ein, die den Übergang von Zahlen zu Idealen vereinfachen: wir schreiben $\mathfrak{a}|a$ für $\mathfrak{a}|(a)$ und $(\mathfrak{a}, \mathfrak{b}) = 1$ für $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$

Definition 6.7
Sei K der Quotientenkörper eines Dedekindrings $\mathcal{O}$. Ein gebrochenes Ideal von K ist ein endlich erzeugter $\mathcal{O}$–Untermodul $\mathfrak{a} \neq (0)$ von K.

Bemerkungen 6.8.

(i) Ist $a \in K^\times$, so ist $(a) := a\mathcal{O}$ ein gebrochenes Ideal. Es heißt gebrochenes Hauptideal.

(ii) Ein $\mathcal{O}$–Untermodul $\mathfrak{a} \neq (0)$ von K ist genau dann ein gebrochenes Ideal, wenn es ein $c \in \mathcal{O}$ gibt, $c \neq 0$, mit $c\mathfrak{a} \subseteq \mathcal{O}$. Beweis:
Sei $\mathfrak{a}$ endlich erzeugt, $\{\alpha_1, \ldots, \alpha_r\}$ ein Erzeugenssystem von Elementen in K. Sei $c \in \mathcal{O}$ der Hauptnenner nach 5.8(i). Dann gilt $c\alpha_i \in \mathcal{O}$, also $c\mathfrak{a} \subseteq \mathcal{O}$.
Sei $c \neq 0$, $c \in \mathcal{O}$ mit $c\mathfrak{a} \subseteq \mathcal{O}$. Dann ist $\mathfrak{a}$ Untermodul des zu $\mathcal{O}$ isomorphen Moduls $c^{-1}\mathcal{O}$. Da $\mathcal{O}$ noethersch ist, ist $\mathfrak{a}$ als Untermodul endlich erzeugt.

(iii) Für gebrochene Ideale definieren wir Schnitt, Summe und Produkt wie für Ideale.

(iv) Gebrochene Ideale $\mathfrak{a}$ mit $\mathfrak{a} \subseteq \mathcal{O}$ sind genau die gewöhnlichen Ideale von $\mathcal{O}$. Wir nennen sie auch die ganzen Ideale von K.

Satz 6.9.
Die gebrochenen Ideale des Quotientenkörpers eines Dedekindrings $\mathcal{O}$ bilden eine abelsche Gruppe, die Idealgruppe J_K von K. Das Einselement ist $(1) = \mathcal{O}$ und das Inverse zu $\mathfrak{a}$ ist

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

Beweis.

- Assoziativität, Kommutativität und $\mathfrak{a}(1) = \mathfrak{a}\mathcal{O} = \mathfrak{a}$ ist klar.
- Sei $\mathfrak{p}$ ein Primideal. Nach Lemma 6.6 ist $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$, also $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$, da $\mathfrak{p}$ im Dedekindring maximal ist. Ist $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ ein ganzes Ideal, so ist $\mathfrak{b} = \mathfrak{p}_1^{-1} \ldots \mathfrak{p}_r^{-1}$ das Inverse zu $\mathfrak{a}$. Denn wegen $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ ist nach Definition von $\mathfrak{a}^{-1}$ sicher $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Ist umgekehrt $x \in \mathfrak{a}^{-1}$, so gilt

  $$x\mathfrak{a} \subseteq \mathcal{O} \quad ,$$

  damit $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$. Wegen $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ also $x \in \mathfrak{b}$. Somit gilt $\mathfrak{b} = \mathfrak{a}^{-1}$.
- Ist $\mathfrak{a}$ ein gebrochenes Ideal, so gibt es $c \in \mathcal{O}, c \neq 0$, so dass $c\mathfrak{a} \subseteq \mathcal{O}$ gilt. Also ist $c\mathfrak{a}$ ein ganzes Ideal. Somit ist $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ das Inverse zu $c\mathfrak{a}$. Auch für gebrochene Ideale ist $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$.

□

Korollar 6.10.
Jedes gebrochene Ideal $\mathfrak{a}$ eines Dedekindrings besitzt eine eindeutige Produktdarstellung

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

mit $\nu_\mathfrak{p} \in \mathbb{Z}$ und $\nu_\mathfrak{p} = 0$ für fast alle $\mathfrak{p}$. Mit anderen Worten: die Gruppe J_K ist die freie abelsche Gruppe über der Menge aller Primideale.

Beweis.
Nach Bemerkung 6.8(ii) ist für ein gebrochenes Ideal $\mathfrak{a}$ und geeignetes c das Ideal $c\mathfrak{a}$ ein ganzes Ideal. Also $\mathfrak{a} = (c\mathfrak{a})(c)^{-1}$. Jedes gebrochene Ideal ist also Quotient ganzer Ideale, die nach Theorem 6.4 eine eindeutige Zerlegung in Primideale besitzen. □

Bemerkungen 6.11.
Wir halten Eigenschaften der Exponenten $\nu_\mathfrak{p}$ fest:

(i) $\nu_\mathfrak{p}(\mathfrak{ab}) = \nu_\mathfrak{p}(\mathfrak{a}) + \nu_\mathfrak{p}(\mathfrak{b})$

(ii) $\mathfrak{b} \subseteq \mathcal{O} \Leftrightarrow \nu_\mathfrak{p}(\mathfrak{b}) \geq 0$

(iii) $\mathfrak{a} \subseteq \mathfrak{b} \Leftrightarrow \nu_\mathfrak{p}(\mathfrak{a}) \geq \nu_\mathfrak{p}(\mathfrak{b})$ *Denn in der Tat ist* $\mathfrak{a} \subseteq \mathfrak{b}$ *äquivalent zu* $\mathfrak{ab}^{-1} \subseteq \mathcal{O}$. *Wende dann (i) und (ii) an.*

(iv) $\nu(\mathfrak{a}+\mathfrak{b}) = \min\Big(\nu_\mathfrak{p}(\mathfrak{a}), \nu_\mathfrak{p}(\mathfrak{b})\Big)$ *Denn* $\mathfrak{a} \subseteq \mathfrak{a}+\mathfrak{b}$, *nach (iii) folgt* $\nu_\mathfrak{p}(\mathfrak{a}) \geq \nu_\mathfrak{p}(\mathfrak{a}+\mathfrak{b})$ *und analog für* $\mathfrak{b}$. $\mathfrak{a}+\mathfrak{b}$ *ist dann das kleinste Ideal, das* $\mathfrak{a}$ *und* $\mathfrak{b}$ *enthält.*

(v) $\nu_\mathfrak{p}(\mathfrak{a} \cap \mathfrak{b}) = \sup\Big(\nu_\mathfrak{p}(\mathfrak{a}), \nu_\mathfrak{p}(\mathfrak{b})\Big)$.

Definition 6.12

(i) Mit P_K werde die Untergruppe von J_K bezeichnet, die aus den gebrochenen Hauptidealen besteht, $(a) = a\mathcal{O}$ mit $a \in K^\times$.

(ii) Die Faktorgruppe

$$Cl_K = J_K/P_K$$

heißt Idealklassengruppe, kurz Klassengruppe des Körpers K.

Bemerkungen 6.13.

(i) Ein Dedekindring ist genau dann prinzipal, wenn seine Idealklassengruppe trivial ist.

(ii) Man hat die exakte Sequenz

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}^\times & \longrightarrow & K^\times & \longrightarrow & J_K & \longrightarrow & Cl_K \longrightarrow 0 \\ & & & & a & \mapsto & (a) & & \end{array}$$

das heißt, dass die Einheitengruppe $\mathcal{O}^\times$ den Verlust, die Klassengruppe Cl_K die Ausdehnung beim Übergang von Zahlen auf Ideale beschreibt.

Unser nächstes Ziel ist die Untersuchung der Objekte $\mathcal{O}^\times$ und Cl_K. Wir werden zeigen, dass für Zahlkörper die Klassengruppe Cl_K endlich ist.

7 Gitter

Wir haben $\mathbb{Z}$[i] als Menge von Gitterpunkten in der komplexen Zahlenebene betrachtet. Dies wurde von Minkowski (1864–1909) auf alle Zahlkörper verallgemeinert. In der älteren Literatur wird dies manchmal als "Geometrie der Zahlen" bezeichnet. Heute hat man allerdings andere geometrische Vorstellungen von einem Zahlkörper. Diese werden in Ansätzen im letzten Kapitel dieser Vorlesung skizziert.

Definition 7.1

(i) *Sei V ein n–dimensionaler reelle Vektorraum. Ein Gitter in V ist eine Untergruppe der Form*

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

mit linear unabhängigen Vektoren $v_1, \ldots, v_m$ von V. Das m–Tupel $(v_1, \ldots, v_m)$ heißt eine Basis und die Menge

$$\Phi = \{x_1v_1 + \ldots + x_mv_m | x_i \in R,\ 0 \leq x_i < 1\}$$

eine Grundmasche des Gitters.

(ii) *Das Gitter heißt vollständig oder eine $\mathbb{Z}$–Struktur von V, wenn $m = n$ gilt.*

Wir bemerken, dass ein Gitter Γ genau dann vollständig ist, wenn $\bigcup\limits_{\gamma\in\Gamma} (\Phi + \gamma) = V$ gilt.

Definition 7.2
Sei $G \subseteq V$ eine Untergruppe des n–dimensionalen $\mathbb{R}$–Vektorraums V. Dann heißt G diskrete Untergruppe, wenn alle $\gamma \in G$ isolierte Punkte von V sind. Das heißt: für jedes $\gamma \in G$ gibt es in der $\mathbb{R}$–Topologie von V eine Umgebung $U_\gamma \subseteq V$ mit

$$G \cap U_\gamma = \{\gamma\} \quad .$$

Dies führt auf die folgende basisabhängige Charakterisierung von Gittern:

Satz 7.3.
Eine Untergruppe $\Gamma \subseteq V$, $V \cong \mathbb{R}^n$ ist ein Gitter genau dann, wenn Γ diskret ist.

Beweis.

- Sei $\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$ ein Gitter von V und $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ eine Basis von V. Für

$$\gamma = \sum_{i=1}^{m} a_iv_i \ \in\ \Gamma \quad a_i \in \mathbb{Z}$$

ist

$$U_\gamma = \Big\{\sum_{i=1}^{n} x_iv_i |\ |a_i - x_i| < 1 \quad i = 1, \ldots, m\Big\}$$

eine solche Umgebung.

- Umgekehrt sei Γ eine diskrete Untergruppe von V und V_0 der von Γ in V aufgespannte Vektorraum. Setze

$$m := \dim\ V_0 \leq n \quad .$$

Sei $\{u_1, \ldots, u_m\ \in\ \Gamma\}$ eine Basis von V_0. Dann ist

$$\Gamma_0 := \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_m \quad \subseteq \Gamma$$

ein vollständiges Gitter in V_0.

- Wir behaupten, dass der Index $[\Gamma : \Gamma_0]$ endlich ist. Denn sei $\{\gamma_i\}$ ein Repräsentantensystem von Γ/Γ_0. Da Γ_0 im V_0 vollständig ist, können wir schreiben

$$\gamma_i = \mu_i + \gamma_{0i}$$

mit $\mu_i \in \Phi_0$ in der Grundmasche von Γ_0 und $\gamma_{0i} \in \Gamma_0$. Da die μ_i diskret in der beschränkten Masche Φ_0 liegen, muss ihre Anzahl endlich sein.

- Sei nun $q := [\Gamma : \Gamma_0]$, dann ist $q\Gamma \subseteq \Gamma_0$. Daher

$$\Gamma \subseteq \frac{1}{q}\Gamma_0 \subseteq \mathbb{Z}\Big(\frac{1}{q}u_1\Big) + \ldots + \mathbb{Z}\Big(\frac{1}{q}u_m\Big) \quad .$$

Nach dem Hauptsatz 5.12 über endlich erzeugte $\mathbb{Z}$–Moduln besitzt Γ eine $\mathbb{Z}$–Basis $\{v_1 \ldots v_r\}$, in der Tat $r = m$ wegen $\Gamma_0 \subseteq \Gamma$. Also $\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_r$. Die $\{v_i\}$ sind über $\mathbb{R}$ linear unabhängig, da sie V_0 aufspannen. Also ist Γ ein Gitter.

□

Lemma 7.4.
Ein Gitter Γ in V ist genau dann vollständig, wenn es eine beschränkte Teilmenge $M \subseteq V$ gibt, deren Verschiebungen V überdecken,

$$V = \bigcup_{\gamma \in \Gamma} (M + \gamma) \quad .$$

Beweis.

- Ist Γ vollständig, so wähle für M die Grundmasche.

- Für die Umkehrung sei V_0 der von Γ aufgespannte Unterraum von V. Sei $v \in V$. Da die Verschiebungen V überdecken, finde für jedes $n \in \mathbb{Z}$

$$nv = a_n + \gamma_n$$

mit $a_n \in M$ und $\gamma_n \in \Gamma$. Da M beschränkt ist, ist $\frac{1}{n}a_n$ Nullfolge. Somit gilt

$$v = \lim_{n\to\infty} \frac{1}{n} a_n + \lim_{n\to\infty} \frac{1}{n}\gamma_n = \lim_{n\to\infty} \frac{1}{n}\gamma_n \in V_0 \quad ,$$

da V_0 abgeschlossen ist.

□

Definition 7.5

(i) Ein <u>euklidischer Vektorraum</u> ist ein endlich–dimensionaler Vektorraum über $\mathbb{R}$ mit symmetrischer, positiv definiter Bilinearform $<,>: V \times V \longrightarrow \mathbb{R}$.

(ii) Wir haben auf V einen Volumensbegriff – genauer ein Haarsches Maß. Sei $\{e_1, \ldots, e_n\}$ eine Orthonormalbasis. Für n linear unabhängige Vektoren $v_1, \ldots, v_n$

$$v_i = \sum a_{ij} e_j$$

hat dann das Parallelepiped

$$\Phi(v_1, \ldots, v_n) = \{x_1 v_1 + \ldots + x_n v_n |\, x_i \in \mathbb{R}\ 0 \leq x_i < 1\}$$

per definitionem das Volumen

$$vol(\Phi) = |\det(a_{ij})| \quad .$$

Um einen basisunabhängigen Ausdruck für das Volumen zu bekommen, betrachten wir

$$\langle v_i, v_j \rangle = \sum a_{ik} a_{jl} \langle e_k, e_l \rangle = (AA^t)_{ij}$$

mit $A = (a_{ij})$, woraus folgt

$$vol(\Phi) = |\det \langle v_i, v_j \rangle|^{1/2} \quad .$$

(iii) Sei Γ ein vollständiges Gitter in V mit Grundmasche Φ. Dann setzen wir $vol(\Gamma) = vol(\Phi)$. Dies ist unabhängig von der Wahl der Gitterbasis: eine Übergangsmatrix und ihr Inverses haben ganzzahlige Koeffizienten, also Determinante ± 1. Das Volumen der Grundmaschen ist daher gleich.

Definition 7.6
Eine Teilmenge X von $V \cong \mathbb{R}^n$ heißt zentralsymmetrisch, falls mit $x \in X$ auch $-x \in X$ gilt; sie heißt konvex, falls mit $x, y \in X$ auch

$$\{ty + (1-t)x,\ 0 \leq t \leq 1\} \subseteq X$$

gilt.

Satz 7.7 (Minkowskischer Gitterpunktsatz)**.**
Sei Γ vollständiges Gitter in einem endlichen Vektorraum V, $\dim V = n$. Sei X eine zentralsymmetrische, konvexe Teilmenge von V. Ist dann

$$vol(X) > 2^n vol(\Gamma) \quad ,$$

so enthält X mindestens einen von Null verschiedenen Gitterpunkt.

Beweis.

- Es genügt zu zeigen: es gibt zwei verschiedene Punkte $\gamma_1, \gamma_2 \in \Gamma$ und

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

Denn für einen Punkt in Durchschnitt gilt

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2 \qquad x_1, x_2 \in X$$

Daher ist der Punkt $\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}(x_2 - x_1)$ der Mittelpunkt der Strecke von x_2 nach $-x_1$ und, weil X zentralsymmetrisch und konvex ist, in X. Andererseits ist wegen $\gamma_1 \neq \gamma_2, \gamma_i \in \Gamma$ der Punkt γ ein von Null verschiedener Gitterpunkt.

- Wären die Mengen $\frac{1}{2}X+\gamma$ paarweise disjunkt, so auch ihre Schnitte mit der Grundmasche. Daher

$$\begin{aligned} vol(\Phi) &\geq \sum_{\gamma\in\Gamma} vol\Big(\Phi \cap \big(\frac{1}{2}X+\gamma\big)\Big) \\ &= \sum_{\gamma\in\Gamma} vol\Big(\underbrace{(\Phi-\gamma)}_{\text{Translation um } -\gamma} \cap \frac{1}{2}X\Big) \end{aligned}$$

  Nun überdecken die Verschiebungen $\Phi-\gamma$ mit $\gamma\in\Gamma$ ganz V, also folgt

$$vol(\Phi) \geq vol(\frac{1}{2}X) = 2^{-n}vol(X)\,,$$

  in Widerspruch zur Annahme an $vol(X)$.

□

8 Minkowski–Theorie

Betrachtung 8.1.
Sei K ein algebraischer Zahlkörper, $n=[K:\mathbb{Q}]$ und

$$\tau_i:\ K\hookrightarrow\mathbb{C} \qquad i=1...n$$

die n verschiedenen komplexen Einbettlungen.
Betrachte alle Einbettungen gleichzeitig:

$$\begin{aligned} j:\ K\hookrightarrow K_{\mathbb{C}} &:= \prod_{\tau}\mathbb{C} \\ a &\mapsto j(a)=(\tau a)_\tau=(a_\tau)_\tau \end{aligned}$$

Wir versehen den $\mathbb{C}$–Vektorraum $K_{\mathbb{C}}$ mit einer hermetischen Metrik

$$\langle x,y\rangle = \sum_{\tau} x_\tau \bar{y}_\tau$$

Es gilt $\langle\cdot,y\rangle$ ist linear, $\overline{\langle x,y\rangle}=\langle y,x\rangle$ und $\langle x,x\rangle>0$ für $x\neq 0$.

Betrachtung 8.2.
Die Galoisgruppe $G(\mathbb{C}/\mathbb{R})$ wird erzeugt durch komplexe Konjugation

$$F:\ z\mapsto\bar{z}$$

$G(\mathbb{C}/\mathbb{R})$ operiert auch auf den Faktoren $\mathbb{C}$ von $K_{\mathbb{C}}$, aber auch auf $Hom_{\mathbb{Q}}(K,\mathbb{C})=\{\tau_1,\ldots,\tau_n\}$

$$(\tau:\ K\to\mathbb{C})\mapsto\big(\bar{\tau}:K\to\mathbb{C}\ \textit{mit}\ \bar{\tau}(x)=\overline{\tau(x)}\big)\ .$$

Also liefert F eine Involution $(F\ z)_\tau=\bar{z}_{\bar{\tau}}$. Für das hermitescheProdukt gilt

$$\langle Fx,Fy\rangle = F\langle x,y\rangle \quad .$$

Betrachtung 8.3.
Wir betrachten auf $K_{\mathbb{C}}$ die Linearform

$$\begin{aligned} \mathrm{tr}: \ K_{\mathbb{C}} &\to \mathbb{C} \\ (x_\tau)_\tau &\mapsto \sum_\tau x_\tau \quad . \end{aligned}$$

Sie ist invariant unter F: $\mathrm{tr} \circ F = F \circ \mathrm{tr}$ *und*

$$K \underset{j}{\longrightarrow} K_{\mathbb{C}} \underset{\mathrm{tr}}{\longrightarrow} \mathbb{C}$$

ist die übliche Spur von $K/\mathbb{Q}$, $\mathrm{tr}_{K/\mathbb{Q}}(a) = \mathrm{tr}(j\ a)$ für alle $a \in K$.

Betrachtung 8.4.
Sei $K_{\mathbb{R}} = K_{\mathbb{C}}^+ = \left[\prod_\tau \mathbb{C}\right]^+$ der unter F invariante Teilraum von $K_{\mathbb{C}}$, d.h.

$$K_{\mathbb{R}} = \{z \in K_{\mathbb{C}} \,|\, z_{\bar\tau} = \bar z_\tau\} \quad .$$

Für ein $a \in K$ gilt

$$a_{\bar\tau} = \bar\tau(a) = \overline{\tau(a)} = \overline{a_\tau} \quad ,$$

also $F(ja) = ja$. Also liegt das Bild von K im Unterraum $K_{\mathbb{R}}$:

$$j: \ K \hookrightarrow K_{\mathbb{R}} \quad .$$

Sei $\langle\cdot,\cdot\rangle = \langle\cdot,\cdot\rangle_{\mathbb{R}}: \quad K_{\mathbb{R}} \times K_{\mathbb{R}} \longrightarrow \mathbb{R}$ die Einschränkung des hermiteschen Produkts auf den $\mathbb{R}$–Vektorraum $K_{\mathbb{R}}$. Es nimmt seine Werte in $\mathbb{R}$ an, denn $x, y \in K_{\mathbb{R}}$ impliziert $\langle x, y\rangle \in \mathbb{R}$, da $F\langle x, y\rangle = \langle Fx, Fy\rangle = \langle x, y\rangle$ gilt. Ferner gilt für $x, y \in K_{\mathbb{R}}$

$$\langle x, y\rangle = \overline{\langle y, x\rangle} = \langle y, x\rangle \quad ,$$

so dass $K_{\mathbb{R}}$ ein euklidischer Vektorraum ist. Er heißt <u>Minkowski–Raum</u>. Das Skalarprodukt heißt <u>kanonische Metrik</u>, das zugehörige Volumen das <u>kanonische Maß</u>. Wegen $\mathrm{tr} \circ F = F \circ \mathrm{tr}$ *haben wir eine $\mathbb{R}$–Linearform*

$$\mathrm{tr}: \ K_{\mathbb{R}} \longrightarrow \mathbb{R} \quad .$$

Für alle $a \in K$ gilt $\mathrm{tr}_{k/\mathbb{Q}}(a) = \mathrm{tr} j(a)$.

Definition 8.5
Sei $Hom_{\mathbb{Q}}(K, \mathbb{C}) = \{\tau_1, \ldots, \tau_n\}$. Die Einbettungen $\rho_1, \ldots, \rho_r$ aus $Hom_{\mathbb{Q}}(K, \mathbb{C})$ mit Bild in $\mathbb{R}$,

$$\rho_i: \ K \longrightarrow \mathbb{R}$$

heißen <u>reell</u>, die nicht reellen heißen <u>komplex</u>. Die letzteren gruppieren sich in Paaren

$$\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s}: \quad K \longrightarrow \mathbb{C} \quad .$$

Offenbar ist $n = r + 2s$. Es ist

$$K_{\mathbb{R}} = \left\{(z_\tau) \in K_{\mathbb{C}} |\ z_\rho \in \mathbb{R},\ z_{\bar\sigma} = \overline{z_\sigma}\right\} \quad .$$

Satz 8.6.
Es gibt einen Isomorphismus von reellen Vektorräumen

$$f: K_{\mathbb{R}} \longrightarrow \prod_{\tau} \mathbb{R} \cong \mathbb{R}^{r+2s}$$
$$(z_\tau) \mapsto (x_\tau)$$

mit $x_\rho = z_\rho \quad x_\sigma = \mathrm{Re}\, z_\sigma \quad x_{\bar{\sigma}} = \mathrm{Im} z_\sigma$, *wobei* σ *nur über Repräsentanten von Paaren konjugierter Einbettungen läuft. Die kanonische Metrik ergibt das Skalarprodukt*

$$(x, y) = \sum_{\tau} a_\tau x_\tau y_\tau$$

mit a_τ *für* τ *reell,* $a_\tau = 2$ *für* τ *komplex.*

Beweis.
Die Isomorphie ist klar. Seien

$$(z_\tau) = (x_\tau + \mathrm{i}y_\tau) \qquad (z'_\tau) = (x'_\tau + \mathrm{i}y'_\tau) \in K_{\mathbb{R}}.$$

Wir rechnen

$$z_\rho \bar{z}_{\rho'} = x_\rho x_{\rho'}$$

und

$$z_\sigma \bar{z'_\sigma} + z_{\bar{\sigma}} \overline{z'_{\bar{\sigma}}} = z_\sigma \bar{z'_\sigma} + \bar{z_\sigma} z'_\sigma = 2\mathrm{Re}\, z_\sigma \bar{z'_\sigma} = 2(x_\sigma x'_\sigma + x_{\bar{\sigma}} x'_{\bar{\sigma}}) \quad .$$

□

Bemerkungen 8.7.
Das kanonische Maß auf $K_{\mathbb{R}}$ *unterscheidet sich vom Lebesgue–Maß auf* $\mathbb{R}^{r+2s}$ *durch einen Faktor,* $vol_{kan}(X) = 2^s vol_{Lebesgue}(X)$.

Satz 8.8.
Sei $\mathfrak{a} \neq 0$ *ein Ideal von* $\mathcal{O}_K$, *so ist* $\Gamma := j\mathfrak{a}$ *ein vollständiges Gitter in* $K_{\mathbb{R}}$ *mit Grundmaschenvolumen*

$$vol(\Gamma) = \sqrt{|d_K|}[\mathcal{O} : \mathfrak{a}] \quad .$$

Beweis.
Da $\mathbb{Z}$ prinzipal ist, existiert nach Satz 5.13 ein $\mathbb{Z}$–Basis $\alpha_1, \ldots, \alpha_n$ von $\mathfrak{a}$.

$$\Gamma = \mathbb{Z}j(\alpha_1) + \ldots + \mathbb{Z}j(\alpha_n) \quad .$$

Seien $\tau_1 \ldots \tau_n$. $K \hookrightarrow \mathbb{C}$ die verschiedenen Einbettungen. Betrachte die Matrix $A = (\tau_i \alpha_j)$. Es ist

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n) = (\det A)^2 = [\mathcal{O} : \mathfrak{a}]^2 d(\mathcal{O}_K) = [\mathcal{O} : \mathfrak{a}]^2 d_K$$

nach Satz 5.16. Andererseits ist

$$\langle j\alpha_i, j\alpha_k \rangle = \sum_l \tau_l \alpha_i \bar{\tau}_l \alpha_k = (AA^+)_{ik}$$

und somit nach Definition 7 (ii)

$$vol(\Gamma) = |\det \langle j\alpha_i, j\alpha_k \rangle|^{1/2} = |\det A| = [\mathcal{O}_K : \mathfrak{a}]\sqrt{|d_K|} \quad .$$

□

Satz 8.9.
Sei $\mathfrak{a} \neq 0$ ein ganzes Ideal von K und $c_\tau > 0$, $\tau \in Hom_{\mathbb{Q}}(K, \mathbb{C})$, reelle Zahlen mit $c_{\bar{\tau}} = c_\tau$ und

$$\prod c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,[\mathcal{O}_K : \mathfrak{a}] \quad .$$

Dann gibt es ein $a \in \mathfrak{a}$, $a \neq 0$ mit $|\tau a| < c_\tau$ für alle $\tau \in Hom_{\mathbb{Q}}(K, \mathbb{C})$.

Beweis.
Die Menge $X = \{(z_\tau) \in K_{\mathbb{R}} |\, |z_\tau| < c_\tau\}$ ist zentralsymmetrisch und konvex. Betrachte wieder

$$\begin{aligned} f : K_{\mathbb{R}} &\longrightarrow \prod_\tau \mathbb{R} \\ (z_\tau) &\mapsto (x_\tau) \end{aligned}$$

mit $x_\rho = z_\rho \quad x_\sigma = \mathrm{Re}\, z_\sigma \quad x_{\bar{\sigma}} = \mathrm{Im} z_{\bar{\sigma}}$. Dann ist

$$f(X) = \left\{(x_\tau) \in \prod_\tau \mathbb{R} |\, |x_\rho| < c_\rho,\ x_\sigma^2 + x_{\bar{\sigma}}^2 < c_\sigma^2\right\}$$

Nach Bemerkung 8.7 gilt

$$vol(X) = 2^s vol_{Lebesgue} f(X) = 2^s \prod_\rho 2c_\rho \prod_{\substack{\sigma \\ \uparrow \\ \text{aus jedem Paar eines}}} \pi c_\sigma^2 = 2^{s+r}\pi^s \prod_\tau c_\tau \quad .$$

Mit Hilfe von Satz 8.8 und der Annahme folgt

$$vol(X) > 2^{s+r}\pi^s \frac{2^s}{\pi^s}\sqrt{|d_K|}[\mathcal{O} : \mathfrak{a}] = 2^n vol(\Gamma) \quad .$$

Nach dem Minkowskischen Gitterpunktsatz 7.7 enthält X einen Punkt von Γ ungleich Null. Es gibt also ein $a \in \mathfrak{a}$, $a \neq 0$ mit $ja = (a_\tau) \in X$, also

$$|a_\tau| = |\tau(a)| < c_\tau \quad .$$

□

Wir brauchen auch eine multiplikative Version der Minkowski–Theorie.

Betrachtung 8.10.
Betrachte den Gruppenhomomorphismus

$$j :\ K^\times \longrightarrow K_{\mathbb{C}}^\times := \prod_\tau \mathbb{C}^\times \quad .$$

Wir führen auch die Normabbildung

$$\begin{aligned} N :\ K_{\mathbb{C}}^* &\longrightarrow \mathbb{C}^* \\ (z_\tau) &\mapsto \prod_\tau z_\tau \quad , \end{aligned}$$

ein. Dann ist

$$N_{K/\mathbb{Q}}(a) = N(ja) \qquad \text{für } a \in K^\times \quad .$$

Um ein Gitter, also eine additive Gruppe, zu erhalten, betrachten wir Logarithmen:

$$\begin{array}{rccc} l: & \mathbb{C}^\times & \longrightarrow & \mathbb{R} \\ & z & \mapsto & \log|z| \quad , \end{array}$$

und erhalten einen surjektiven Homomorphismus

$$l: K_{\mathbb{C}}^\times \longrightarrow \prod_\tau \mathbb{R}\,.$$

Es ergibt sich das folgende kommutative Diagramm:

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{C}}^\times & \xrightarrow{l} & \prod_\tau \mathbb{R} \\ {\scriptstyle N_{K/\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{tr}} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{C}^\times & \xrightarrow{l} & \mathbb{R} \end{array}$$

Auf allen Gruppen des Diagramms operiert wieder die Galoisgruppe durch F:

- *auf $K^\times$ trivial*
- *auf $K_{\mathbb{C}}^\times$ wie zuvor*
- *auf $x = (x_\tau) \in \prod_\tau \mathbb{R}$ durch $(Fx)_\tau = x_{\bar\tau}$.*

Es gilt offenbar

$$F \circ j = j \qquad F \circ l = l \circ F \qquad N \circ F = F \circ N \qquad \mathrm{tr} \circ F = \mathrm{tr}\,,$$

d.h. alle Morphismen sind $G(\mathbb{C}/\mathbb{R})$ Morphismen. Wir können daher zu den Fixgruppen übergehen:

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{l} & [\prod_\tau \mathbb{R}]^+ \\ {\scriptstyle N_{K/\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{tr}} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{R}^\times & \xrightarrow[l]{} & \mathbb{R} \end{array}$$

Wir beschreiben den $\mathbb{R}$–Vektorraum $[\prod_\tau \mathbb{R}]^+$ explizit:

$$Hom_{\mathbb{Q}}(K, \mathbb{C}) = \{\rho_1, \ldots, \rho_r, \sigma_1, \bar\sigma_1, \ldots, \sigma_s, \bar\sigma_s\}$$

Damit

$$[\prod_\tau \mathbb{R}]^+ = \prod_\rho \mathbb{R} \times \prod_{[\sigma]} [\mathbb{R} \times \mathbb{R}]^+ \quad .$$

Nun identifizieren wir

$$\begin{array}{rcl} [\mathbb{R} \times \mathbb{R}]^+ = \left\{(x,x) \in \mathbb{R}^2\right\} & \xrightarrow{\sim} & \mathbb{R} \\ (x,x) & \mapsto & 2x \end{array}$$

Also $[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$, wobei

$$\mathrm{tr}: [\prod_\tau \mathbb{R}]^+ \longrightarrow \mathbb{R}$$

übergeht in die Summe der Koordinaten.

$$l: K_{\mathbb{R}}^\times \longrightarrow [\prod_\tau \mathbb{R}]^+$$

geht über in

$$l: K_{\mathbb{R}}^{\times} \longrightarrow \mathbb{R}^{r+s}$$
$$l(x = (\log|x_{\rho_1}|, \ldots, \log|x_{\rho_r}|, \log|x_{\sigma_1}|^2, \ldots)$$

für $x \in K_{\mathbb{R}}^{\times} \subseteq \prod_{\tau} \mathbb{C}^{\times}$. *Insgesamt gilt*

$$K^{\times} \xrightarrow{j} K_{\mathbb{R}}^{\times} \xrightarrow{l} \mathbb{R}^{r+s}$$
$$a \mapsto (\log|\rho_1 a|, \ldots, \log|\sigma_s a|^2)\,.$$

9 Die Klassenzahl

Es soll gezeigt werden, dass die Idealklassengruppe $Cl_K = J_K/P_K$ eines algebraischen Zahlkörpers endlich ist.

Definition 9.1
Sei $\mathfrak{a} \neq (0)$ *ein Ideal in* $\mathcal{O}_K$. *Dann heißt*

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

die Absolutnorm *von* $\mathfrak{a}$.

Bemerkungen 9.2.

(i) Die Absolutnorm ist nach Satz 5.16 endlich.

(ii) Ist $\mathfrak{a} = (a)$ *ein Hauptideal, so gilt*

$$\mathfrak{N}\big((a)\big) = \big|N_{K/\mathbb{Q}}(a)\big| \quad .$$

Nach Satz 5.16 existiert eine $\mathbb{Z}$*–Basis von* $\mathcal{O}_K$, $\{\omega_1, \ldots, \omega_n\}$. *Dann ist* $\{a\omega_1, \ldots, a\omega_n\}$ *eine* $\mathbb{Z}$*–Basis von* $a\mathcal{O}_K$. *Ist* A *die Übergangsmatrix*

$$a\omega_i = \sum_j a_{ij}\omega_j \quad ,$$

so ist nach Satz 5.12

$$\big|N_{K/\mathbb{Q}}(a)\big| \underset{Def.}{=} |\det A| = [\mathcal{O}_K : \mathfrak{a}]\,.$$

(iii) Ergeben Betrachtungen für das Nullideal keinen Sinn – wie hier–, so ist es stillschweigend ausgeschlossen.

Satz 9.3.
Ist $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_r^{\nu_r}$ *die Primzerlegung eines Ideals* $\mathfrak{a} \neq 0$, *so gilt*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \ldots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r} \quad .$$

Beweis.

- Nach dem chinesischen Restsatz 2.13 gilt

$$\mathcal{O}_K/\mathfrak{a} \cong \bigoplus \mathcal{O}_K/\mathfrak{p}_i^{\nu_i}$$

Wir können uns also auf den Fall $\mathfrak{a} = \mathfrak{p}^\nu$ zurückziehen.

- In der Kette

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \ldots \supseteq \mathfrak{p}^\nu$$

ist wegen der Eindeutigkeit der Zerlegung in Primideale $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$.
Behauptung: $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ist ein $\mathcal{O}_K/\mathfrak{p}$–Vektorraum der Dimension Eins. Sei $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, dann gilt für das Ideal $\mathfrak{b} = \mathfrak{p}^{i+1} + (a)$

$$\mathfrak{p}^i \supset \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}\,.$$

Wir multiplizieren diese Inklusion in der Idealgruppe mit $\mathfrak{p}^{-i}$ und erhalten:

$$\mathcal{O} = \mathfrak{p}^i\mathfrak{p}^{-i} \supseteq \mathfrak{b}\mathfrak{p}^{-i} \supsetneq \mathfrak{p}^{i+1}\mathfrak{p}^{-i} = \mathfrak{p}$$

Das Primideal $\mathfrak{p}$ ist im Dedekindring maximal. Daher gilt $\mathcal{O} = \mathfrak{b}\mathfrak{p}^{-i}$, also $\mathfrak{b} = \mathfrak{p}^i$. Somit ist $a \mod \mathfrak{p}^{i+1}$ eine Basis von $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Es folgt sofort die Isomorphie $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{p}$, also gilt

$$\begin{aligned}\mathfrak{N}(\mathfrak{p}^\nu) &= [\mathcal{O}_K : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2]\ldots[\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu] = \\ &= [\mathcal{O}_K : \mathfrak{p}]^\nu = \mathfrak{N}(\mathfrak{p})^\nu \quad .\end{aligned}$$

□

Korollar 9.4.
Seien $\mathfrak{a}, \mathfrak{b} \neq 0$ Ideale, so gilt

$$\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}) \quad .$$

Wir setzen die Normfunktion auf die gebrochenen Ideale fort durch

$$\begin{aligned}\mathfrak{N} :\ & J_K \longrightarrow \mathbb{R}_+^* \\ & \mathfrak{N}\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})^{-1}\,.\end{aligned}$$

Diese Fortsetzung ist ein Gruppenhomomorphismus.

Lemma 9.5.
Sei $\mathfrak{a} \neq 0$ ein Ideal in $\mathcal{O}_K$. Dann gibt es ein $a \in \mathfrak{a}$, $a \neq 0$ mit

$$\left|N_{K/\mathbb{Q}}(a)\right| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a})$$

Beweis.
Sei $\varepsilon > 0$ vorgegeben. Wähle positive reelle Zahlen c_τ für alle $\tau \in Hom_Q(K, \mathbb{C})$ mit $c_\tau = c_{\bar{\tau}}$ und

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon$$

Nach Satz 8.9 finden wir $a_\varepsilon \in \mathfrak{a}$, $a_\varepsilon \neq 0$ mit $|\tau a_\varepsilon| < c_\tau$. Also gibt es für alle $\varepsilon > 0$ ein $a_\varepsilon \in \mathfrak{a}$ mit

$$\left|N_{K/\mathbb{Q}}(a_\varepsilon)\right| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon\,.$$

Da die Norm nur ganzzahlige Werte annehmen kann, muss es ein $a \in \mathfrak{a},\ a \neq 0$ mit der genannten Eigenschaft geben. □

Theorem 9.6 (Endlichkeit der Klassenzahl)**.** *Die Idealklassengruppe $Cl_K = J_K/P_K$ ist endlich. Ihre Ordnung*

$$h_K = |Cl_K|$$

heißt Klassenzahl des Körpers K.

Beweis.

- Ist $\mathfrak{p} \neq 0$ ein Primideal von $\mathcal{O}_K$, so ist $\mathfrak{p} \cap \mathbb{Z}$ ein Ideal von $\mathbb{Z}$. Wegen

  $$\mathfrak{p} + \mathbb{Z}/\mathfrak{p} \cong \mathbb{Z}/\mathfrak{p} \cap \mathbb{Z}$$

  ist der Quotient integer, also $\mathfrak{p} \cap \mathbb{Z} = (p)$ mit p prim; im Beweis von Satz 6.3 sahen wir $\mathfrak{p} \cap \mathbb{Z} \neq (0)$. Da $\mathcal{O}_K$ eine Ganzheitsbasis besitzt, ist $\mathcal{O}_K/\mathfrak{p}$ endliche Erweiterung von $\mathbb{Z}/(p) = \mathbb{F}_p$ mit $grad\ f \geq 1$. Daher gilt $\mathfrak{N}(\mathfrak{p}) = p^f$ mit einem geeigneten f (vergleiche auch Beispiel 12.5).

- Für eine feste Primzahl $p \in \mathbb{Z}$ gibt es nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = (p)$. Denn daraus folgt

  $$\begin{aligned} p\mathcal{O}_K &\subseteq \mathfrak{p} \quad , \\ \text{also } \mathfrak{p}|\ p\mathcal{O}_K &= \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_r^{\nu_r} \quad . \end{aligned}$$

  Zusammengenommen zeigt dies, dass es für jedes $M \in \mathbb{R}$ nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{N}(\mathfrak{p}) \leq M$ gibt. Da jedes Ideal $\mathfrak{a}$ von $\mathcal{O}_K$ eine Darstellung

  $$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_r^{\nu_r} \qquad \nu_i > 0$$

  besitzt und $\mathfrak{N}(\mathfrak{a}) = \prod \mathfrak{N}(\mathfrak{p}_i)^{\nu_i}$ gilt, gibt es für jedes $M \in \mathbb{R}$ auch nur endlich viele Ideale mit $\mathfrak{N}(\mathfrak{a}) \leq M$.

- Es genügt daher zu zeigen: jede Klasse $[\mathfrak{a}] \in Cl_K$ enthält ein ganzes Ideal $\mathfrak{a}_1$ mit

  $$\mathfrak{N}(\mathfrak{a}_1) \leq M := \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \quad .$$

  Sei $\mathfrak{a}$ ein beliebiger Repräsentant der Klasse. Wegen Bemerkung 5.8(i) gibt es $\gamma \in \mathcal{O}_K \setminus \{0\}$ mit

  $$\mathfrak{b} := \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K \quad .$$

  Nach Lemma 9.5 gibt es $\alpha \in \mathfrak{b},\ \alpha \neq 0$ mit

  $$\left|N_{K/\mathbb{Q}}(\alpha)\right| \leq M\mathfrak{N}(\mathfrak{b}) \quad .$$

Daher gilt

$$M \geq \big|N_{K/\mathbb{Q}}(\alpha)\big|\mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}\big((\alpha)\mathfrak{b}^{-1}\big) = \\ = \mathfrak{N}\big(\alpha\mathfrak{b}^{-1}\big)$$

Setze

$$\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}] \quad ,$$

da $\alpha\gamma^{-1} \in K^\times$. Offenbar ist die Abschätzung $\mathfrak{N}(\alpha\mathfrak{b}^{-1}) \leq M$ erfüllt; ferner folgt aus $\alpha \in \mathfrak{b}$, auch $(\alpha) \subseteq \mathfrak{b}$, also $(\alpha)\mathfrak{b}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1} \subseteq \mathcal{O}_K$, was heißt, dass $\alpha\mathfrak{b}^{-1}$ ist ein ganzes Ideal ist.

□

Bemerkungen 9.7.

(i) Die Endlichkeit der Klassenzahl besagt, dass der Übergang von Zahlen zu Idealen nicht ins Uferlose führt. Ist insbesondere $h_K = 1$, so ist $\mathcal{O}_K$ Hauptidealring.

(ii) Im allgemeinen ist $h_K > 1$. Für imaginär-quadratische Zahlkörper $K = \mathbb{Q}\big(\sqrt{d}\big)$ mit $d < 0$ quadratfrei gilt

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

Es ist nicht bekannt, ob es unendlich viele Zahlkörper mit $h_K = 1$ gibt. Die Berechnung von Klassenzahlen ist ein schwieriges Problem.

(iii) Wir skizzieren kurz die Beziehung zum großen Fermatschen Satz über ganzzahlige Lösungen der Gleichung

$$y^p = z^p - x^p$$

mit p prim. Diese Gleichung schreibt sich mit Hilfe einer p–ten Einheitswurzel ζ_p in der Form

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

Ist $h_p = h_{\mathbb{Q}(\zeta_p)} = 1$, so erhält man einen Widerspruch zur eindeutigen Zerlegbarkeit. Kummer zeigte, dass schon $p \nmid h_P$ ausreicht, um einen Widerspruch zu erzielen.

10 Der Dirichletsche Einheitensatz

Unsere zweite Aufgabe ist die Beschreibung der Einheitengruppe $\mathcal{O}_K^\times$ des Ringes der ganzen Zahlen eines Zahlkörpers K. Offenbar gilt

$$\mu(K) \subseteq \mathcal{O}_K^\times \quad ,$$

wobei $\mu(K)$ die endliche Gruppe der Einheitswurzeln ist, die in K liegen. Im allgemeinen ist $\mathcal{O}_K^\times$ aber nicht endlich. Sei r die Anzahl der reellen Einbettungen: $\rho : k \longrightarrow \mathbb{R}$ und s die Anzahl der Paare komplex konjugierter Einbettungen

$$\sigma, \bar{\sigma} : \ K \longrightarrow \mathbb{C} \quad .$$

Betrachtung 10.1.
Wir erinnern an die multiplikative Version der Minkowski–Theorie, insbesondere an das kommutative Diagramm aus Betrachtung 8.10:

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{l} & [\prod_\tau \mathbb{R}] \\ {\scriptstyle N_{K/\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{tr}} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{R}^\times & \xrightarrow{l} & \mathbb{R} \end{array}$$

Sei

$$\begin{array}{lcll} \mathcal{O}_K^\times & = & \{\varepsilon \in \mathcal{O}_K |\, N_{K/\mathbb{Q}}(\varepsilon) = \pm 1\} & \subseteq K^\times & \textit{Einheitengruppe} \\ S & = & \{y \in K_{\mathbb{R}}^\times |\, N(y) = \pm 1\} & \subseteq K_{\mathbb{R}}^\times & \textit{Norm Eins Hyperfläche} \\ H & = & \{x \in \left[\prod_\tau \mathbb{R}\right]^+ |\, \mathrm{tr}(x) = 0\} & \subseteq \left[\prod_\tau \mathbb{R}\right]^+ & \textit{Spur 0 Hyperebene} \end{array} \tag{6}$$

Wir betrachten die Abbildung

$$\lambda :\ \mathcal{O}_K^\times \xrightarrow{j} S \xrightarrow{l} H$$

und setzen

$$\Gamma = \lambda(\mathcal{O}_K^\times) \subseteq H \quad .$$

Satz 10.2.
Die Sequenz

$$1 \to \mu(K) \to \mathcal{O}_K^\times \xrightarrow{\lambda} \Gamma \to 0$$

ist exakt, d.h. $\ker \lambda = \mu(K)$.

Beweis.

- Sei $\varepsilon \in \mathcal{O}_K^\times$ mit $\lambda(\varepsilon) = 0$. Dann ist $|\tau\varepsilon| = 1$ für alle Einbettungen $\tau :\ K \to \mathbb{C}$. Die Punkte $j\varepsilon = (\tau\varepsilon)_\tau$ liegen in einem beschränkten Bereich von $K_{\mathbb{R}}$ und im Gitter $j(\mathcal{O}_K)$. Somit ist $\ker\lambda$ endliche Untergruppe von $K^\times$ und besteht daher aus Einheitswurzeln: $\ker\lambda \subseteq \mu(K)$.
- Sei umgekehrt $\zeta \in \mu(K)$ und $\tau :\ K \hookrightarrow \mathbb{C}$ eine Einbettung. Dann gilt:

  $$\log|\tau\zeta| = \log 1 = 0 \quad ,$$

  also $\mu(K) \subseteq \ker\lambda$.

□

Lemma 10.3.
Bis auf Assoziierte gibt es nur endlich viele Elemente $\alpha \in \mathcal{O}_K$ mit gegebener Norm $|N_{K/\mathbb{Q}}(\alpha)| = a$.

Beweis.
Sei $a \in \mathbb{Z}$. Wir zeigen, dass es in jeder Nebenklasse von $\mathcal{O}_K/a\mathcal{O}_K$ bis auf Assoziierte höchstens ein Element der Norm a gibt. Denn seien α, β solche Elemente,

$$\beta = \alpha + a\gamma \qquad \gamma \in \mathcal{O}_K$$

Dann ist

$$\frac{\alpha}{\beta} = 1 \pm \frac{N(\beta)}{\beta} \cdot \gamma \,,$$

wegen $\frac{N(\beta)}{\beta} \in \mathcal{O}_K$ liegt auch $\frac{\alpha}{\beta} \in \mathcal{O}_K$ und ähnlich $\frac{\beta}{\alpha} \in \mathcal{O}_K$. Also sind α und β assoziiert.
Daher gibt es höchstens $[\mathcal{O}_K : a\mathcal{O}_K]$ viele Elemente der Norm a. □

Satz 10.4.
Die Gruppe Γ *ist ein vollständiges Gitter im* $(r+s-1)$*–dimensionalen* $\mathbb{R}$*–Vektorraum* H*, also* $\Gamma \cong \mathbb{Z}^{r+s-1}$.

Beweis.

- Wir zeigen zunächst, dass $\Gamma = \lambda(\mathcal{O}_K^*)$ ein Gitter in H, also eine diskrete Untergruppe von H ist. Es ist $\lambda : \mathcal{O}_K^\times \longrightarrow H$ die Einschränkung von

$$K^\times \underset{j}{\longrightarrow} \prod_\tau \mathbb{C}^\times \xrightarrow{l} \prod_\tau \mathbb{R} \quad .$$

  auf $\mathcal{O}_K^\times$. Also reicht es, zu zeigen, dass der beschränkte Bereich

$$X_c = \{(x_\tau)_\tau \in \prod \mathbb{R} |\ |x_\tau| \le c\}$$

  für jedes $c > 0$ nur endlich viele Elemente von $\Gamma = lj(\mathcal{O}_K^\times)$ enthält. Betrachte dazu

$$Y_c = l^{-1}(X_c) = \left\{(z_\tau) \in \prod_\tau \mathbb{C}^\times |\ e^{-c} \le |z_\tau| \le e^c\right\}$$

  Dieser Bereich ist beschränkt und enthält nur endlich viele Punkte von $j(\mathcal{O}_K^\times)$, da dies eine Untermenge des Gitters $j(\mathcal{O}_K)$ ist. Also ist Γ ein Gitter in H, und offenbar

$$\dim_{\mathbb{R}} H = \dim_{\mathbb{R}}[\prod \mathbb{R}]^+ - 1 = r + s - 1 \quad .$$

- Die eigentliche Aussage ist: Γ ist ein *vollständiges* Gitter in H. Nach Lemma 7.4 müssen wir zeigen: es gibt eine beschränkte Menge $M \subseteq H$ mit

$$H = \bigcup_{\gamma \in \Gamma} (M + \gamma)$$

  Dazu reicht es, zu zeigen: es gibt eine beschränkte Menge $T \subseteq S$ mit

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

  Denn

$$l(Tj\varepsilon) = l(T) + lj(\varepsilon) \qquad \text{mit } lj\varepsilon \in \Gamma \quad .$$

  Setze dann

$$M = l(T) \,,$$

  und es gilt

$$H = \bigcup_{\gamma \in \Gamma} M + \gamma \,,$$

wobei auch M beschränkt ist: sei $x = (x_\tau) \in T$, also

$$\prod x_\tau = 1$$

Somit gilt $0 < b \leq |x_\tau| \leq a$ für unabhängige Konstanten a, b, so dass $l(T)$ beschränkt ist.

- Seien $c_\tau > 0$ für $\tau \in Hom_{\mathbb{Q}}(K, \mathbb{C})$ reelle Zahlen mit $c_\tau = \bar{c_\tau}$ und

$$c := \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} \quad .$$

Sei

$$X := \left\{(z_\tau) \in K_{\mathbb{R}} |\ |z_\tau| < c_\tau\right\}$$

Sei $y = (y_\tau) \in S$ beliebig, dann haben wir

$$Xy := \left\{(z_\tau) \in K_{\mathbb{R}} |\ |z_\tau| \leq c'_\tau\right\}$$

mit $c'_\tau = c_\tau |y_\tau|$. Es gilt weiterhin $c'_{\bar{\tau}} = c'_\tau$ und

$$\prod_\tau c'_\tau = \prod_\tau c_\tau \prod_\tau |y_\tau| = \prod_t c_\tau = C \quad ,$$

da (y_τ) in der Norm-Eins-Hyperfläche liegt. Wegen Satz 8.9 gibt es $a \in \mathcal{O}_K,\ a \neq 0$, mit

$$(\tau a)_\tau \in X_y \ .$$

Lemma 10.3 erlaubt es uns, Elemente $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K \quad \alpha_i \neq 0$ zu finden, so dass jedes $a \in \mathcal{O}_K$ mit Norm kleiner gleich C zu einen der α_i assoziiert ist.
Setze

$$T := S \cap \bigcup_{i=1}^{N} Xj(\alpha_i)^{-1}$$

Mit X ist auch $Xj(\alpha_i)^{-1}$ beschränkt, also ist auch T beschränkt. Wir behaupten

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} Tj\varepsilon \quad .$$

Denn sei $y \in S$. Nach Satz 8.9 gibt es $a \in \mathcal{O}_K$, $a \neq 0$ mit $ja \in Xy^{-1}$, also $ja = xy^{-1}$ mit $x \in X$. Wegen

$$\left|N_{K/\mathbb{Q}}(a)\right| = \left|N(xy^{-1})\right| = \left|N(x)\right| \leq C$$

ist a assoziiert zu einem der α_i: $\alpha_i = \varepsilon a$ mit $\varepsilon \in \mathcal{O}_K^\times$. Daher

$$y = x(ja)^{-1} = xj(\alpha_i^{-1}\varepsilon) \quad .$$

Nun ist $y \in S$, $j(\varepsilon) \in S$

$$xj(\alpha_i^{-1}) \in S \cap Xj(\alpha_i)^{-1} \subseteq T$$

Also $y \in Tj(\varepsilon)$, was zu zeigen war.

□

Theorem 10.5 (Dirichletscher Einheitensatz)**.** *Die Einheitengruppe $\mathcal{O}_K^\times$ von $\mathcal{O}_K$ ist das direkte Produkt der endlichen zyklischen Gruppe $\mu(K)$ und einer freien abelschen Gruppe von Range $r+s-1$:*

$$\mathcal{O}_K^\times \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}$$

Beweis.
In der exakten Sequenz

$$1 \to \mu(K) \to \mathcal{O}_K^\times \xrightarrow{\lambda} \Gamma \to 0$$

ist nach Satz 10.4 Γ eine freie abelsche Gruppe von Rang $r+s-1$. Ist $v_1 \dots v_{r+s-1}$ eine $\mathbb{Z}$–Basis von Γ, so wähle Urbilder ε_i in $\mathcal{O}_K^*$. Sei A die von ε_i erzeugte Untergruppe: λ vermittelt eine Isomorphie

$$A \xrightarrow[\lambda]{\sim} \Gamma$$

Also gilt $\mu(K) \cap A = \{1\}$ und somit $\mathcal{O}_K^\times \cong \mu(K) \times A$. □

Bemerkungen 10.6.

(i) Es gibt also $r+s-1$ Grundeinheiten $\varepsilon_1, \dots, \varepsilon$, die aber nicht eindeutig bestimmt sind, so dass jede Einheit $\varepsilon \in \mathcal{O}_K^\times$ sich eindeutig schreiben lässt als

$$\varepsilon = \zeta \epsilon_1^{\nu_1} \dots \varepsilon_{r+s-1}^{\nu_{r+s-1}}$$

mit $\zeta \in \mu(K)$ und $\nu_i \in \mathbb{Z}$. Der Dirichletsche Einheitensatz liefert eine vollständige Beschreibung der Einheitengruppe als abstrakte endlich-erzeugte abelsche Gruppe. Sie als konkrete Untergruppe von K zu beschreiben, erfordert die Angabe von Grundeinheiten: dies ist im allgemeinen ein sehr schwieriges Problem.

(ii) Die Einheitengruppe ist genau dann endlich, wenn $r+s-1=0$ gilt. Ist $r=1,\ s=0$, so folgt $n=[K:\mathbb{Q}]=1$, also $K=\mathbb{Q}$. Andernfalls ist K ein imaginär-quadratischer Zahlkörper: $K=\mathbb{Q}(\sqrt{d})$ $d<0$, quadratfrei. In diesem Fall ist $\mathcal{O}_K^\times = \{\pm 1\}$, außer für

$$K = \mathbb{Q}(\mathrm{i}) \qquad \mathcal{O}_K^\times = \{\pm 1, \pm \mathrm{i}\} \cong \mathbb{Z}_4$$

$$K = \mathbb{Q}(\sqrt{-3}) \qquad \mathcal{O}_K^\times = \left\{ \left(\frac{1+\sqrt{-3}}{2} \right)^j \ j = 0, \dots, 5 \right\} \cong \mathbb{Z}_6$$

(iii) Für einen reell-quadratischen Körper $K=\mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{N}$ quadratfrei ist

$$\mathcal{O}_K^\times = \{\pm 1\} \times \mathbb{Z}$$

Die Untergruppe der positiven Einheiten hat genau einen multiplikativen Erzeuger >1, die fundamentale Einheit. Denn mit $x \in \mathcal{O}_K^\times$ sind auch $-x, x^{-1}$ und $-x^{-1}$ Einheiten und nur die größte davon ist – für $x \neq 1$ – größer als Eins. Die Einheiten $-x, x^{-1}, -x, -x^{-1}$ sind von der Form

$$\pm a \pm b\sqrt{d} \quad ,$$

diejenigen >1 also als die größte mit $a>0$ und $b>0$.
Für eine Einheit gilt

$$N(x) = a^2 - b^2 d = \pm 1 \quad .$$

Im Fall $d = 2, 3 \mod 4$ sind $a, b \in \mathbb{Z}$. Man findet die fundamentale Einheit folgendermaßen: in der Folge $\{b^2 d\}$ nehme man die erste Zahl, die zu einer Quadratzahl benachbart ist. Als Beispiel betrachten wir $d = 7$. Die Folge bd^2 hat die Werte $7, 28, 63$, und in der Tat ist wegen $63 = 64 - 1$ die Zahl 63 benachbart zu einer Quadratzahl. Wir finden also $b = 3,\ a = 8$. Die fundamentale Einheit ist $\varepsilon = 8 + 3\sqrt{7}$.

Betrachtung 10.7.
Durch die Identifizierung $[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}$ wird H Unterraum des euklidischen Vektorraums $\mathbb{R}^{r+s}$, also selbst euklidischer Raum. Wir wollen das Volumen der Grundmarsche von

$$\Gamma = \lambda(\mathcal{O}_K^\times) \subseteq H$$

berechnen. Sei $\varepsilon_1, \ldots, \varepsilon_t$ mit $t = r + s - 1$ ein System von Grundeinheiten. Sei

$$\lambda_0 = \frac{1}{\sqrt{r+s}}(1, \ldots, 1) \in \mathbb{R}^{r+s}$$

λ_0 hat Länge 1 und steht senkrecht auf der Spur 0 Hyperebene:

$$< \lambda_0, h >= \frac{1}{\sqrt{r+s}} \sum_i h_i = \frac{1}{\sqrt{r+s}} \mathrm{tr} h = 0 \quad .$$

Damit ist mit

$$\lambda(\varepsilon_i) = (\lambda_1(\varepsilon_i) \ldots \lambda_{t+1}(\varepsilon_i)) \in \mathbb{R}^{t+1}$$

das Volumen

$$\begin{aligned} vol_{\mathbb{R}^t}\big(\lambda(\mathcal{O}_K^*)\big) &= vol_{\mathbb{R}^{t+1}}\big(< \lambda_0, \lambda(\varepsilon_1) \ldots \lambda(\varepsilon_t) > \big) \\ &= \pm \det \begin{pmatrix} \lambda_{01} & \lambda_1(\varepsilon_1) & \ldots & \lambda_1(\varepsilon_t) \\ \vdots & \vdots & & \vdots \\ \lambda_{0t+1} & \lambda_{t+1}(\varepsilon_1) & \ldots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix} \end{aligned} \tag{7}$$

Satz 10.8.
Es ist $vol_{\mathbb{R}^t}\big(\lambda(\mathcal{O}_K^*)\big) = \sqrt{r+s}R$, wobei R der Determinantenbetrag eines beliebigen Minors von Rang $t = r + s - 1$ der Matrix

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \ldots & \lambda_1(\varepsilon_t) \\ \vdots & & \vdots \\ \lambda_{t+1}(\varepsilon_1) & \ldots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix}$$

ist. Die Zahl R heißt Regulator des Körpers K.

Beweis.
Addiere in (7) alle Zeilen zu einer beliebigen, aber festen Zeile. Es ergeben sich in dieser Zeile lauter Nullen, außer in der ersten Spalte, in der $\sqrt{r+s}$ steht. □

11 Erweiterungen von Dedekindringen

Wir wollen nun einen Überblick über die Primideale eines algebraischen Zahlkörpes bekommen. Sei K ein Zahlkörper, $\mathcal{O}_K$ der Ring der ganzen Zahlen und $\mathfrak{p} \neq 0$ ein Primideal.

Dann haben wir gesehen, dass $\mathfrak{p} \cap \mathbb{Z} = (p)$ gilt. Es folgt $\mathfrak{p} \supseteq p\mathcal{O}_K$, also $\mathfrak{p} | p\mathcal{O}_K$. Es ist daher zentral zu verstehen, wie $p\mathcal{O}_K$ in Primideale zerfällt. Wir untersuchen gleich die folgende allgemeinere Situation:
Sei A ein Dedekindring, $K = \mathrm{Quot}(A)$ und L eine endliche Körpererweiterung von K. $\mathcal{O}$ sei der ganze Abschluss von A in L.

Satz 11.1.

(i) *$\mathcal{O}$ ist ein Dedekindring.*

(ii) *Jedes Ideal von $\mathcal{O}$, insbesondere $\mathcal{O}$ selbst, ist endlich erzeugter A–Modul.*

Beweis.
Hier nur für den Fall char $K = 0$ oder $|K| < \infty$.

- Als ganzer Abschluss ist $\mathcal{O}$ wegen 4.10(ii) ist ganzabgeschlossen.
- Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine Basis von L/K mit $d := d(\alpha_1, \ldots, \alpha_n) \neq 0$, vgl. Satz 5.7. Wir wählen $\alpha_i \in \mathcal{O}$ und folgern aus Lemma 5.9

$$\mathcal{O} \subseteq A\frac{\alpha_1}{d} + \ldots + A\frac{\alpha_n}{d} =: M \quad .$$

  M ist endlich erzeugter A–Modul und daher nach Satz 3.11(ii) noethersch. Jedes Ideal $\mathfrak{a}$ von $\mathcal{O}$ ist in M enthalten und daher endlich erzeugter A–Modul, und damit erst recht endlich erzeugter $\mathcal{O}$–Modul: man nehme einfach das A-Erzeugendensystem, das natürlich auch $\mathcal{O}$-Erzeugendensystem ist. Also ist $\mathcal{O}$ noethersch.

- Sei $\mathfrak{P}$ ein Primideal von $\mathcal{O}$, $\mathfrak{P} \neq 0$. Setze $\mathfrak{p} = A \cap \mathfrak{P}$. Da $\mathfrak{p}$ maximal im Dedekindring A ist, ist $A/\mathfrak{p}$ ein Körper. Der Integritätsring $\mathcal{O}/\mathfrak{P}$ ist ein endlich–dimensionaler $A/\mathfrak{p}$–Vektorraum und daher ein Körper: die Multiplikation mit jedem Element $\bar{x} \in \mathcal{O}/\mathfrak{P}$, $\bar{x} \neq 0$, ist ein injektiver Endomorphismus, daher surjektiv, so dass Inverse existieren.

□

Bemerkungen 11.2.
Sei $\mathfrak{p}$ ein Primideal von A, $\mathfrak{p} \neq 0$ und $\mathfrak{p} \neq A$. Dann gilt $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$.

Beweis.
Da im Dedekindring A die Zerlegung in Primideale eindeutig ist, gibt es ein Element $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Dann ist $\pi A = \mathfrak{p}\mathfrak{a}$ mit $\mathfrak{p} \not| \mathfrak{a}$, also $\mathfrak{p} + \mathfrak{a} = A$. Finde eine Zerlegung

$$1 = b + s$$

mit $b \in \mathfrak{p}$, $s \in \mathfrak{a}$. Dann ist $s \notin \mathfrak{p}$, da sonst $\mathfrak{p} = A$. Also

$$s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi A \quad .$$

Wäre $\mathfrak{p}\mathcal{O} = \mathcal{O}$, so würde folgen

$$s\mathcal{O} = s\mathfrak{p}\mathcal{O} \subseteq \pi\mathcal{O} \quad .$$

Damit finden wir aber $s = \pi x$ mit $x \in \mathcal{O} \cap K = A$, da A ganzabgeschlossen in K als Dedekindring. Es folgt $s \in (\pi) \subseteq \mathfrak{p}$, also ein Widerspruch. □

Sei $\mathfrak{p} \neq (0)$ ein Primideal von A; es zerfällt im Dedekindring $\mathcal{O}$ in eindeutiger Weise in ein Produkt von Primidealen

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} ,$$

wobei $\mathfrak{P}_i$ paarweise verschiedene Primideale von $\mathcal{O}$ sind und $e_i \geq 1$ gilt. Die Primideale $\mathfrak{P}_1 \dots \mathfrak{P}_r$ von $\mathcal{O}$ sind genau die Primideale von $\mathcal{O}$, für die $\mathfrak{P} \cap A = \mathfrak{p}$ gilt:

- gilt $\mathfrak{P} \cap A = \mathfrak{p}$, so ist $\mathfrak{p}\mathcal{O} = (\mathfrak{P} \cap A)\mathcal{O} \subseteq \mathfrak{P}$, also $\mathfrak{P} | \, \mathfrak{p}\mathcal{O}$.
- gilt $\mathfrak{P} | \, \mathfrak{p}\mathcal{O}$, so folgt $\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}$, uns damit $\mathfrak{p} \subseteq \mathfrak{P} \cap A$. Da aber $\mathfrak{p}$ maximal in A ist, folgt sogar $\mathfrak{p} = \mathfrak{P} \cap A$.

Wir führen auch noch die folgenden Schreibweisen ein: $\mathfrak{P} | \, \mathfrak{p}$, $\mathfrak{P}$ liegt über $\mathfrak{p}$, $\mathfrak{P}$ teilt $\mathfrak{p}$. $\mathfrak{P}$ ist Primteiler von $\mathfrak{p}$ in $\mathcal{O}$.

Definition 11.3
Mit obigen Bezeichnungen heißt

- $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$ *Verzweigungsindex von* $\mathfrak{P}_i$ *über* $\mathfrak{p}$.
- *Der Körpergrad* $f(\mathfrak{P}_i/\mathfrak{p}) = f_i = [\mathcal{O}/\mathfrak{P}_i : A/\mathfrak{p}]$ *heißt Restklassengrad oder Trägheitsgrad von* $\mathfrak{P}_i$ *über* $\mathfrak{p}$.

Satz 11.4. *(fundamentale Gleichung)*
Sei $\mathrm{char}\,(K) = 0$ *oder* $|K| < \infty$, $n = [L/K]$ *und* $\mathfrak{p}$ *Primideal von* A. *Betrachte wie oben die Zerlegung*

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \quad .$$

Dann gilt

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

Je kleiner also die Trägheitsgrade f_i *sind, desto fleißiger zerfällt das Primideal* $\mathfrak{p}$ *von* A *in Primideale von* $\mathcal{O}$.

Beweis.

- Aus dem chinesischen Restsatz 2.13 folgt

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

  Alle Größen sind $\kappa := A/\mathfrak{p}$–Vektorräume. Wir behaupten

  $$\dim_\kappa \mathcal{O}/\mathfrak{p}\mathcal{O} = n \qquad \dim_\kappa \mathcal{O}/\mathfrak{P}_i^{e_i} = e_i f_i \quad ,$$

  woraus die fundamentale Gleichung folgt. Nach 11.1(ii) ist $\mathcal{O}$ endlich erzeugter A–Modul, also sind alle Dimensionen endlich.

- Sei $\bar{\omega}_1, \ldots, \bar{\omega}_m$ eine κ-Basis von $\mathcal{O}/\mathfrak{p}\mathcal{O}$ und seien ω_i Repräsentanten von $\bar{\omega}_i$ in $\mathcal{O}$. Es reicht aus zu zeigen, dass $\omega_1, \ldots, \omega_m$ eine Basis von L/K ist. Dann folgt $m = n = [L : K]$.

  Wir zeigen zunächst, dass die $\omega_1, \ldots, \omega_m$ linear unabhängig über K sind. Bestünde eine lineare Abhängigkeitsbeziehung über K, so zeigt die Multiplikation mit dem Hauptnenner, dass auch eine lineare Abhängigkeitsbeziehung über A bestünde:

  $$a_1\omega_1 + \ldots + a_m\omega_m = 0 \quad ,$$

  mit $a_i \in A$, nicht alle $a_i = 0$. Sei $\mathfrak{a} = (a_1, \ldots, a_m)$ das von den Koeffizienten erzeugte Ideal in A. Wähle $a \in \mathfrak{a}^{-1}$ mit $a \notin \mathfrak{a}^{-1}\mathfrak{p}$. Das geht, denn wären alle $a \in \mathfrak{a}^{-1}$ in $\mathfrak{a}^{-1}\mathfrak{p}$, so gälte $\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}\mathfrak{p}$, also $A \subseteq \mathfrak{p}$.
  Es liegen also alle Produkte $aa_i \in A$, aber nicht alle in $\mathfrak{p}$. Wegen

  $$aa_1\omega_1 + \ldots + aa_m\omega_m = 0 \mod \mathfrak{p}$$

  haben wir einen Widerspruch zur linearen Unabhängigkeit der $\bar{\omega}_i$ über $\kappa = A/\mathfrak{p}$.

- Wir müssen zeigen, dass $\{\omega_i\}$ den Körper L auch über K erzeugt. Sei

  $$M = A\omega_1 + \ldots + A\omega_m \,;$$

  dies ist ein A–Modul in $\mathcal{O}$. Setze $N = \mathcal{O}/M$. Es war $\langle \bar{\omega_1}, \ldots, \bar{\omega_m} \rangle = \mathcal{O}/\mathfrak{p}\mathcal{O}$, daher gilt

  $$\mathcal{O} = M + \mathfrak{p}\mathcal{O} \quad .$$

  Die Betrachtung dieser Gleichung modulo M zeigt

  $$\mathfrak{p}N = N \quad .$$

  Nach Satz 11.1(ii) ist $\mathcal{O}$ endlich erzeugter A–Modul, also auch N. Sei $\{\alpha_i\}$ ein Erzeugendensystem von N. Da $\alpha_i \in N = \mathfrak{p}N$, finde $a_{ij} \in \mathfrak{p}$, so dass gilt

  $$\alpha_i = \sum_{j=1}^{s} a_{ij}\alpha_j \,.$$

  Sei $C := (a_{ij}) - I_{s\times s}$ und C' die zu C adjungierte Matrix. Wir haben

  $$C(\alpha_1, \ldots, \alpha_s)^t = 0 \,,$$

  und nach Satz 4.4 gilt $CC' = dI_{s\times s}$ mit $d := \det C$. Somit ist

  $$0 = C'C(\alpha_1, \ldots, \alpha_t)^t = (d\alpha_1, \ldots, d\alpha_s)^t \quad .$$

  Also $dN = 0$, d.h.

  $$d\mathcal{O} \subseteq M = A\omega_1 + \ldots + A\omega_m \quad .$$

  Nun ist $a_{ij} \in \mathfrak{p}$, also

  $$d = \det\big((a_{ij}) - I\big) = (-1)^s \mod \mathfrak{p} \quad ,$$

  also ist $d \neq 0$. Somit ist

  $$L = dL \subseteq K\omega_1 + \ldots + K\omega_m \quad ,$$

  also ist $\{\omega_i\}$ auch ein Erzeugendensystem. Es folgt $n = m$.

- Zur Berechnung von $\dim_\kappa \mathcal{O}/\mathfrak{P}_i^{e_i}$ betrachte die folgende absteigende Kette von κ–Vektorräumen:

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i^2/\mathfrak{P}_i^{e_i} \supseteq \ldots \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)\,.$$

  Wir behaupten, dass der Quotient $\mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1}$ als κ-Vektorraum isomorph zu $\mathcal{O}/\mathfrak{P}_i$ ist. Wegen $[\mathcal{O}/\mathfrak{P}_i : \kappa] = f_i$ erhalten wir dann sofort $\dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i f_i$. Sei $\alpha \in \mathfrak{P}_i^\nu \setminus \mathfrak{P}_i^{\nu+1}$. Betrachte den Homomorphismus

$$\begin{aligned} \mathcal{O} &\longrightarrow \mathfrak{P}_i^\nu/\mathfrak{P}_i^{\nu+1} \\ a &\mapsto a\alpha \mod \mathfrak{P}_i^{\nu+1} \quad . \end{aligned}$$

  Er hat Kern $\mathfrak{P}_i$ und ist surjektiv: denn

$$\mathfrak{P}_i^\nu = ggT(\mathfrak{P}_i^{\nu+1}, (\alpha))$$

  impliziert nach Bézout

$$\mathfrak{P}_i^\nu = \alpha\mathcal{O} + \mathfrak{P}_i^{\nu+1}$$

□

Sei $\operatorname{char} K = 0$ oder $|K| < \infty$. Nach 4.13(*iii*) existiert ein primitives Element $\theta \in L$, wir können also schreiben $L = K(\theta)$. Wegen Bemerkung 5.8(*i*) ist $\theta = \frac{\theta'}{a}$ mit $\theta' \in \mathcal{O}$, $a \in A \subset K$. Wir können also $\theta \in \mathcal{O}$ annehmen.

Definition 11.5
Das Ideal $\mathcal{F} = \{\alpha \in \mathcal{O} |\ \alpha\mathcal{O} \subseteq A[\theta]\}$ von $\mathcal{O}$ heißt <u>Führer</u> des Ringes $A[\theta]$. Es ist das größte Ideal von $\mathcal{O}$ in $A[\theta]$. Der Führer ist nicht leer: wegen Lemma 5.9 gilt für die Diskriminante:

$$d(1, \theta, \ldots, \theta^{n-1})\mathcal{O} \subseteq A[\theta] \quad ,$$

also $d(1, \theta, \ldots, \theta^{n-1}) \in \mathcal{F}$.

Satz 11.6.
Sei $\mathfrak{p}$ ein Primideal von A, das prim zum Führer $\mathcal{F}$ von $A[\theta]$ ist. Sei $p(X) \in A[X]$ das Minimalpolynom von θ über K. Sei

$$\bar{p}(X) = \bar{p}_1(X)^{e_1} \ldots \bar{p}_r(X)^{e_r} \tag{8}$$

die Zerlegung von $\bar{p}(X) = p(X) \mod \mathfrak{p}$ in paarweise verschiedene irreduzible Faktoren $\bar{p}_i \in (A/\mathfrak{p})[X]$ und $p_i \in A[X]$ eine beliebige Liftung von $\bar{p}_i$:

$$\bar{p}_i = p_i \mod \mathfrak{p} \quad .$$

Wir dürfen $\bar{p}_i$ und p_i als normiert voraussetzen. Dann sind die Ideale

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O} \quad i = 1 \ldots r$$

die Primideale über $\mathfrak{p}$ mit e_i wie in (8) und $f_i = \operatorname{grad} \bar{p}_i$. Also

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

Beweis.
Wir setzen $\mathcal{O}' = A[\theta]$ und $\bar{A} = A/\mathfrak{p}$.

- Wir behaupten
$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathcal{O}'/\mathfrak{p}\mathcal{O}' \tag{9}$$
Da $\mathfrak{p}\mathcal{O}$ und $\mathcal{F}$ teilerfremd sind, gilt $\mathfrak{p}\mathcal{O}+\mathcal{F} = \mathcal{O}$. Da $\mathcal{F} \subseteq \mathcal{O}'$, gilt erst recht $\mathfrak{p}\mathcal{O}+\mathcal{O}' = \mathcal{O}$. Also ist
$$\mathcal{O}' \longrightarrow \mathcal{O}/\mathfrak{p}\mathcal{O}$$
surjektiv mit Kern $\mathcal{O}' \cap \mathfrak{p}\mathcal{O}$. Es gilt $\mathcal{O}' \cap \mathfrak{p}\mathcal{O} = \mathfrak{p}\mathcal{O}'$, $\mathfrak{p}\mathcal{O}' \subseteq \mathcal{O}' \cap \mathfrak{p}\mathcal{O}$ ist klar. Andererseits
$$\mathfrak{p}\mathcal{O} \cap \mathcal{O}' = (\underbrace{\mathfrak{p}\mathcal{O}+\mathcal{F}}_{\mathcal{O}})(\mathfrak{p}\mathcal{O} \cap \mathcal{O}') \subseteq \mathfrak{p}\mathcal{O}' \quad .$$

- Wir behaupten
$$\mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \bar{A}[X]/(\bar{p}(X)) \quad ,$$
denn der Kern der Surjektion
$$A[X] \twoheadrightarrow \bar{A}[X]/(\bar{p}(X))$$
wird erzeugt von $\mathfrak{p}$ und $\Big(p(X)\Big)$. Also
$$A[X]/\mathfrak{p}A[X] + (p) \xrightarrow{\sim} \bar{A}[X]/(\bar{p}(X)) \quad .$$
Nun ist aber
$$\mathcal{O}' = A[\theta] \cong A[X]/p(X) \quad ,$$
somit
$$(A[X]/(p))/(\mathfrak{p}A[X] + (p)/(p)) \cong \mathcal{O}'/\mathfrak{p}\mathcal{O}' \quad .$$

- Den Ring $R := \bar{A}[X]\big/(\bar{p})$ untersuchen wir mit den chinesischen Restsatz:
$$\bar{A}[X]\big/(\bar{p}) \cong \oplus_{i=1}^{r} \bar{A}[X]\big/(\bar{p}_i(X))^{e_i} \quad .$$
  - Die Primideale von R sind die von $\bar{p}_i \mod \bar{p}$ erzeugten Hauptideale.
  - $[R\big/(\bar{p}_i) : \bar{A}] = \operatorname{grad} \bar{p}_i$
  - In R gilt
$$0 = \big(\bar{p}(x)\big) = \bigcap_{i=1}^{r} \Big(\bar{p}_i\Big)^{e_i}$$

- Wegen der Isomorphie
$$\bar{A}[X]\big/(\bar{p}) \xrightarrow{\sim} \mathcal{O}/\mathfrak{p}\mathcal{O}$$
$$\bar{f}(X) \mod \bar{p} \mapsto \bar{f}(\theta) \bmod \mathfrak{p}\mathcal{O}$$
haben wir in $\bar{\mathcal{O}} = \mathcal{O}/\mathfrak{p}\mathcal{O}$ die gleichen Verhältnisse: Die Primidiale $\bar{\mathfrak{P}}_i$ von $\bar{\mathcal{O}}$ entsprechen $(\bar{p}_i)$ und sind die von $p_i(\theta) \mod \mathfrak{p}\mathcal{O}$ erzeugten Hauptideale mit
$$[\bar{\mathcal{O}}\big/\bar{\mathfrak{P}}_i : A/\mathfrak{p}] = \operatorname{grad} \bar{p}_i$$
$$(0) = \bigcap_{i=1}^{r} \bar{\mathfrak{P}}_i^{e_i} \quad .$$

Sei nun $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$ das Urbild von $\bar{\mathfrak{P}}_i$ unter

$$\mathcal{O} \twoheadrightarrow \mathcal{O}/\mathfrak{p}\mathcal{O} \quad .$$

Dann durchläuft $\mathfrak{P}_i$ alle Primideale über $\mathfrak{p}$. Wegen $\mathcal{O}/\mathfrak{P}_i \cong \bar{\mathcal{O}}/\bar{\mathfrak{P}}_i$ ist

$$f_i = [\mathcal{O}/\mathfrak{P}_i : A/\mathfrak{p}] = \operatorname{grad} \bar{p}_i \quad .$$

$\mathfrak{P}_i^{e_i}$ ist das Urbild von $\bar{\mathfrak{P}}_i{}^{e_i}$ und

$$\mathfrak{p}\mathcal{O} \supseteq \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i} \quad ,$$

also

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

und damit

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

wegen der fundamentalen Gleichung $n = \sum_{i=1}^{r} e_i f_i$.

□

Definition 11.7
Sei $\mathfrak{p}$ ein Primideal von A und sei

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

die Zerlegung von $\mathfrak{p}$ in L.

(i) $\mathfrak{p}$ heißt vollzerlegt oder totalzerlegt, wenn

$$r = n = [L : K], \text{ also } e_i = f_i = 1 \text{ für alle } i \ .$$

(ii) $\mathfrak{p}$ heißt unzerlegt, wenn $r = 1$.

(iii) $\mathfrak{P}_i$ heißt unverzweigt über A (oder über K), wenn $e_i = 1$ und die Restklassenerweiterung $\mathcal{O}/\mathfrak{p}_i$ über $A/\mathfrak{p}$ separabel ist. (Im Zahlkörperfall ist $A/\mathfrak{p}$ ein endlicher Körper und die Erweiterung immer separabel.)
Anderenfalls heißt das Ideal $\mathfrak{P}_i$ verzweigt. Gilt $e_i > 1,\ f_i = 1$, so heißt $\mathfrak{P}_i$ reinverzweigt.

(iv) Das Primideal $\mathfrak{p}$ heißt unverzweigt, wenn alle $\mathfrak{P}_i$ über $\mathfrak{p}$ unverzweigt sind; andernfalls heißt es verzweigt. Insbesondere sind vollzerlegte Ideale unverzweigt.

(v) Die Erweiterung L/K heißt unverzweigt, wenn alle Primideale $\mathfrak{p}$ von A in L unverzweigt sind.

Es ist eher die Ausnahme, dass Primideale von K in L verzweigt sind.

Satz 11.8.
Ist $\operatorname{char} K = 0$ *oder* $|K| < \infty$, *so gibt es nur endlich viele in L verzweigte Primideale von K.*

Beweis.
Sei $\theta \in \mathcal{O}$ ein primitives Element von L, also $L = K(\theta)$.

$$p(X) = min_K(\theta) \in A[X]$$

sei das Minimalpolynom. Sei

$$d := d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0$$

die Diskriminante. Dann ist jedes zu d und zum Führer $\mathcal{F}$ von $A[\theta]$ teilerfremde Primideal $\mathfrak{p}$ von K unverzweigt. Denn nach Satz 11.6 sind alle $e_i = 1$, falls $\bar{p} = p \mod \mathfrak{p}$ keine mehrfachen Nullstellen in einem Zerfällungskörper besitzt. Dies ist der Fall, wenn die Diskriminante $\bar{d} = d \mod \mathfrak{p}$ von $\bar{p}$ ungleich Null ist, was hier nach Voraussetzung zutrifft. Die Restklassenkörpererweiterungen $\mathcal{O}/\mathfrak{P}_i$ über $A/\mathfrak{p}$ werden von $\theta \mod \mathfrak{P}_i$ erzeugt, also sind sie einfache Erweiterungen, also separabel. Daher ist $\mathfrak{p}$ unverzweigt. □

Definition 11.9
Die Diskriminante $d_{\mathcal{O}/A}$ ist das von allen Diskriminanten $d(\omega_1, \ldots, \omega_n)$ erzeugte Ideal von A, wobei alle Basen $\{\omega_i\}$ von L/K mit $\omega_i \in \mathcal{O}$ durchlaufen werden.
Man kann zeigen $\mathfrak{p}$ ist in L verzweigt $\Leftrightarrow$ $\mathfrak{p}$ teilt $d_{\mathcal{O}/A}$. (Für einen Beweis siehe etwa Samuel, Abschnitt 5.3, Theorem 1.)

Beispiele 11.10.
Das Zerlegungsgesetz von Primzahlen im quadratischen Zahlkörper $\mathbb{Q}(\sqrt{a})$ steht in Zusammenhang mit dem Gaußschen Reziprozitätsgesetz. Wir betrachten dazu die diophantische Gleichung

$$x^2 + bx = a$$

für gegebene $a, b \in \mathbb{Z}$. Ihre Lösbarkeit kann auf den Fall zurückgeführt werden, wenn b eine ungerade Primzahl ist, $b = p$, und $(a, p) = 1$ gilt. (Der Beweis dieser Aussage kommt als Übungsaufgabe.) Wir haben daher die Frage zu beantworten: ist die Gleichung

$$x^2 = a \mod p$$

lösbar? Das Legendresymbol ist folgendermaßen definiert:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & x^2 = a \mod p \quad \text{lösbar} \\ -1 & \text{unlösbar} \end{cases}$$

Sei p eine ungerade Primzahl. Die Gruppe $\mathbb{F}_p^\times$ ist zyklisch von der Ordnung $p-1$, die Gruppe $\mathbb{F}_p^{\times 2}$ der Quadrate hat Ordnung 2 und ist daher normal. Also ist das Legendresymbol multiplikativ,

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

und es folgt

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

Nun bedeutet $\left(\frac{a}{p}\right) = 1$, dass es $\alpha \in \mathbb{Z}$ gibt mit $\alpha^2 = a \mod p$. Wegen

$$X^2 - a = (X - \alpha)(X + \alpha) \mod p$$

zerlegt genau in diesem Fall das Minimalpolynom von α. Der Führer von $\mathbb{Z}[\sqrt{a}]$ in $\mathbb{Q}(\sqrt{a})$ ist ein Teiler von 2. Aus Satz 11.6 folgt daher: Für a quadratfrei und $(p, 2a) = 1$ gilt: $\left(\frac{a}{p}\right) = 1$ dann und nur dann, wenn p vollzerlegt in $\mathbb{Q}(\sqrt{a})$ ist.

12 Hilfsmittel aus der Algebra: Galoistheorie

Bemerkungen 12.1.

i) Sei L ein Körper und G eine Menge *von Körperautomorphismen. Dann ist*

$$L^G = \{x \in L |\, \sigma x = x \; \forall \sigma \in G\}$$

ein Unterkörper von L, der Fixkörper von G.

ii) Sei L/K eine Körpererweiterung. Dann ist die Menge der K–Automorphismen von L eine Gruppe, $G(L/K)$.

Theorem 12.2.
Sei L eine Erweiterung endlichen Grades eines Körpers K, mit $\mathrm{char}\,(K) = 0$ *oder $|K| < \infty$. Dann ist äquivalent:*

i) K ist der Fixkörper von $G(L/K)$, $K = L^{G(L/K)}$.

ii) Für jedes $\alpha \in L$ liegen alle Nullstellen des Minimalpolynoms von α in L.

iii) L wird von den Nullstellen eines Polynoms in $K[X]$ erzeugt.

Beweis.

- $(i) \Rightarrow (ii)$ Sei $\alpha \in L$ und $G = G(L/K)$. Das Polynom

$$f = \prod_{\sigma \in G} (X - \sigma\alpha)$$

ist unter G invariant. (Man beachte, dass G wegen 4.13(ii) endlich ist.) Aus der Annahme (i) folgt $f \in K[X]$. Wegen $f(\alpha) = 0$ wird das Polynom f von Minimalpolynom geteilt, woraus (ii) folgt.

- $(ii) \Rightarrow (iii)$
Nach 4.13(iii) existiert ein primitives Element $\theta \in L$. Sein Minimalpolynom hat alle Nullstellen in L, und diese erzeugen L, also folgt (iii)

- $(iii) \Rightarrow (i)$
Wegen (iii) wird L von einer endlichen Menge $\{x^{(1)}, \ldots, x^{(q)}\}$ aus Elementen von L und ihren Konjugierten $\{x_j^{(i)}, i = 1, \ldots q, j = 1 \ldots n\}$ über K erzeugt.
Für jeden K–Isomorphismus σ von L in eine Erweiterung von L werden diese Erzeuger permutiert. Also $\sigma(L) \subseteq L$. Da σ injektiv ist, gilt sogar $\sigma(L) = L$. Also gibt es nach 4.13(ii) genau $n := [L : K]$ verschiedene Körperautomorphismen von L über K. Sei $\alpha \in L$ invariant unter $G = G(L/K)$. Dann ist jedes $\sigma \in G$ ein $K(\alpha)$–Automorphismus von L. Davon gibt es genau $[L : K(\alpha)]$ viele mit Bild unter Erweiterung von L. Also

$$n = [L : K(\alpha)] \quad ,$$

und $K(\alpha) = K$, also $\alpha \in K$.
Man beachte, dass wir nebenbei gesehen haben, dass

$$|G| = n = [L : K]$$

gilt.

□

Definition 12.3

i) Gelten die Bedingungen aus Theorem 12.2, so heißt die Körpererweiterung L/K galoisch. $G(L/K)$ heißt Galoisgruppe von L/K.

ii) Wenn $G(L/K)$ abelsch bzw. zyklisch ist, so heißt L eine abelsche bzw. zyklische Erweiterung von K.

Man kann zeigen:

Theorem 12.4.

(i) Sei $|K| < \infty$ oder $\mathrm{char}\,(K) = 0$, L/K eine endliche Erweiterung und H eine Automorphismengruppe von L mit $L^H = K$. Dann ist L/K galoisch und $H = G(L/K)$.

(ii) Sei $\mathrm{char}\,(K) = 0$ oder $|K| < \infty$ und L/K eine galoische Erweiterung endlichen Grades mit Galoisgruppe G.
Sei $\mathcal{U}(G)$ die Menge der Untergruppen von G, halbgeordnet durch Inklusion.
Sei $\mathcal{Z}(L/K)$ die Menge der Zwischenkörper der Körpererweiterung, ebenfalls halbgeordnet durch Inklusion.
Dann sind die Abbildungen

$$\begin{aligned} k: \quad & \mathcal{U}(G) \longrightarrow Z(L/K) \\ & H \mapsto L^H \\ g: \quad & Z(L/K) \longrightarrow \mathcal{U}(G) \\ & K' \mapsto G(L/K') \end{aligned}$$

zueinander inverse monoton abnehmende Bijektionen; insbesondere ist für jeden Zwischenkörper K' die Erweiterung L/K' galoisch.

(iii) Die Erweiterung K/K' ist genau dann galoisch, wenn $g(K') = G(L/K')$ normale Untergruppe von G ist. Dann ist die Faktorgruppe

$$G(K'/K) = G(L/K) \,/\, G(L/K') \quad .$$

die Galoisgruppe.

Zum Beweis siehe Samuel Kapitel 6.1 oder Kapitel 1.2 von Algebra 2.

Beispiele 12.5.

(i) Sei $\mathrm{char}\,(K) = 0$ und L eine Erweiterung von Grad 2. Wie im Beispiel 4.14 sieht man, dass L von der Form $L = K(\alpha)$ ist mit α Nullstelle von $X^2 - d$ wobei $d \in K$ kein Quadrat ist. Die andere Nullstelle ist $-\alpha$, also gibt es nur einen nicht–trivialen K–Automorphismus

$$\sigma(a + b\alpha) = a - b\alpha \qquad mit \quad a, b \in K \quad .$$

Es gilt $\sigma^2 = id$, $L^{<\sigma>} = K$. Also ist L/K nach Theorem 12.4(i) galoisch mit Galoisgruppe

$$G(L/K) = \{id, \sigma\} \cong \mathbb{Z}_2 \quad .$$

(ii) *Sei* $\mathrm{char}\,(K) = 0$, ζ *eine primitive* n*–te Einheitswurzel und* $L = K(\zeta)$.
Das Minimalpolynom $F(X)$ *von* ζ *teilt* $X^n - 1$, *also sind alle seine Nullstellen* n*–te Einheitswurzeln. Wegen Theorem 12.2 ist* L/K *galoisch.* $\sigma \in G(L/K)$ *ist durch* $\sigma(\zeta)$ *bestimmt. Es ist*

$$\sigma(\zeta) = \zeta^{j(\sigma)}$$

mit $j(\sigma) \in \mathbb{Z}_n^\times$. *Aus*

$$\sigma\tau(\zeta) = \sigma(\zeta^{j(\tau)}) = \zeta^{j(\sigma)j(\tau)}$$

für $\sigma, \tau \in G(L/K)$ *folgt*

$$j(\sigma\tau) = j(\sigma)j(\tau) \quad .$$

Also existiert ein injektiver Gruppenhomomorphismus

$$G \hookrightarrow \mathbb{Z}_n^\times \quad .$$

Die Galoisgruppe ist also insbesondere abelsch. Für $K = \mathbb{Q}$ *ist der Gruppenhomomorphismus sogar surjektiv (Satz von Gauß, Satz 1.3.13 von Algebra 2). Alle Untergruppen einer abelschen Gruppe sind normal. Also ist für jeden Zwischenkörper* K' *von* L/K *die Erweiterung* K/K' *galoisch mit abelscher Galoisgruppe.*
Das Theorem von Kronecker und Weber besagt, dass in Falle $K = \mathbb{Q}$ *die Umkehrung gilt: ist* $G(K'/\mathbb{Q})$ *abelsch, so ist* K' *Unterkörper eines Kreisteilungskörpers.*

(iii) *Sei* $\mathbb{F}_q$ *ein endlicher Körper,* $|\mathbb{F}_q| = q$. *Dann ist* $q = p^s$ *mit* p *prim. Jede endliche Körpererweiterung vom Grad* n *ist von der Form* $\mathbb{F}_{q^n}/\mathbb{F}_q$.

$$\begin{array}{rccc} \sigma: & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_{q^n} \\ & x & \mapsto & x^q \end{array}$$

ist ein Automorphismus von $\mathbb{F}_{q^n}$ *der Ordnung* n. *Tatsächlich ist* $\mathbb{F}_{q^n}/\mathbb{F}_q$ *galoisch mit Galoisgruppe*

$$G(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle\sigma\rangle \cong \mathbb{Z}_n \quad .$$

Der ausgezeichnete Erzeuger σ *heißt* Frobenius–Automorphismus. *(Für Beweise siehe Kapitel 1.3.1 von Algebra 2.)*

13 Hilbertsche Verzweigungstheorie

Sei A ein Dedekindring, $K = \mathrm{Quot}(A)$. Sei L/K endlich galoisch und $G = G(L/K)$ die Galoisgruppe. Wir interessieren uns für die Wirkung von G auf den Primidealen von L.

Bemerkungen 13.1.

(i) *Der Ring* $\mathcal{O}$ *ist invariant unter der Wirkung von* G, *denn mit* $a \in \mathcal{O}$ *ist auch* $\sigma a \in \mathcal{O}$ *für alle* $\sigma \in G$. *Also operiert* G *auf* $\mathcal{O}$.

(ii) *Sei* $\mathfrak{P}/\mathfrak{p}$ *ein Primideal von* $\mathcal{O}$, *so ist auch* $\sigma\mathfrak{P}$ *für jedes* $\sigma \in G$ *ein Primideal von* $\mathcal{O}$ *mit* $\sigma\mathfrak{P}/\mathfrak{p}$. *Denn es ist*

$$\mathcal{O}/\mathfrak{P} \cong \mathcal{O}/\sigma\mathfrak{P}$$

und es gilt

$$\sigma\mathfrak{P} \cap A = \sigma(\mathfrak{P} \cap A) = \sigma\mathfrak{p} = \mathfrak{p} \quad .$$

Die Primideale $\sigma\mathfrak{P}$ *mit* $\sigma \in G$ *heißen die zu* $\mathfrak{P}$ konjugierten Primideale.

Satz 13.2.
G operiert transitiv auf der Menge aller über $\mathfrak{p}$ liegenden Primideale von $\mathcal{O}$, alle Primideale über $\mathfrak{p}$ sind also konjugiert.

Beweis.
Seien $\mathfrak{P}$ und $\mathfrak{P}'$ zwei Primideale über $\mathfrak{p}$. Angenommen, es gälte $\mathfrak{P}' \neq \sigma\mathfrak{P}$ für alle $\sigma \in G$. Nach dem chinesischen Restsatz gibt es dann ein $x \in \mathcal{O}$ mit

$$\begin{aligned} x &= 0 \qquad \mod \mathfrak{P}' \\ x &= 1 \qquad \mod \sigma\mathfrak{P} \quad \text{für alle } \sigma \in G \quad . \end{aligned}$$

Es ist dann wegen $x \in \mathfrak{P}'$

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{P}' \cap A = \mathfrak{p} \quad .$$

Andererseits ist $x \notin \sigma\mathfrak{P}$ für alle $\sigma \in G$, also $\sigma(x) \notin \mathfrak{P}$ für alle $\sigma \in G$. Somit

$$\prod_{\sigma \in G} \sigma(x) \notin \mathfrak{P} \cap A = \mathfrak{p} \quad ,$$

Widerspruch. □

Definition 13.3
Sei $\mathfrak{P}$ ein Primideal von $\mathcal{O}$. Dann heißt die Untergruppe

$$G_{\mathfrak{P}} = \{\sigma \in G |\, \sigma\mathfrak{P} = \mathfrak{P}\}$$

die Zerlegungsgruppe von $\mathfrak{P}$ über K. Der zugehörige Fixkörper

$$Z_{\mathfrak{P}} = \{x \in L |\, \sigma(x) = x \text{ für alle } x \in G_{\mathfrak{P}}\}$$

heißt Zerlegungskörper von $\mathfrak{P}$ über K.

Bemerkungen 13.4.

(i) Sei $\mathfrak{p}$ Primideal von A und $\mathfrak{P}/\mathfrak{p}$ Primideal von $\mathcal{O}$. Durchläuft σ ein Repräsentantsystem von $G/G_{\mathfrak{P}}$, so durchläuft $\sigma\mathfrak{P}$ die verschiedenen Primideale über $\mathfrak{p}$ genau einmal. Ihre Anzahl ist also

$$r = [G : G_{\mathfrak{P}}] \quad .$$

Insbesondere gilt

$$\begin{aligned} G_{\mathfrak{P}} = 1 &\Leftrightarrow Z_{\mathfrak{P}} = L \Leftrightarrow \mathfrak{p} \text{ ist vollzerlegt.} \\ G_{\mathfrak{P}} = G &\Leftrightarrow Z_{\mathfrak{P}} = K \Leftrightarrow \mathfrak{p} \text{ ist unzerlegt.} \end{aligned}$$

(ii) Für die Zerlegungsgruppen gilt

$$\sigma G_{\mathfrak{P}} \sigma^{-1} = G_{\sigma\mathfrak{P}}$$

für alle $\sigma \in G$, denn

$$\begin{aligned} \tau \in G_{\sigma\mathfrak{P}} \Leftrightarrow \tau\sigma\mathfrak{P} = \sigma\mathfrak{P} \quad &\Leftrightarrow \sigma^{-1}\tau\sigma\mathfrak{P} = \mathfrak{P} \\ &\Leftrightarrow \sigma^{-1}\tau\sigma \in G_{\mathfrak{P}} \Leftrightarrow \tau \in \sigma G_{\mathfrak{P}} \sigma^{-1} \quad . \end{aligned}$$

Satz 13.5.
Sei L/K galoisch vom Grad n, $\mathfrak{p}$ ein Primideal von A und

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \quad .$$

Dann gilt $e_1 = e_2 = \ldots = e_r = e$ und $f_1 = f_2 = \ldots = f_r = f$. Also gilt $n = e \cdot f \cdot r$ und

$$\mathfrak{p}\mathcal{O} = \prod_{\sigma \in G/G_{\mathfrak{P}}} (\sigma\mathfrak{P})^e \quad .$$

Beweis.
Setze $\mathfrak{P} = \mathfrak{P}_1$, also $\mathfrak{P}_i = \sigma\mathfrak{P}$ für geeignetes $\sigma \in G$. Der Isomorphismus

$$\sigma_i : \quad \mathcal{O} \longrightarrow \mathcal{O}$$

induziert einen Isomorphismus

$$\begin{array}{c} \mathcal{O}/\mathfrak{P} \xrightarrow{\sim} \mathcal{O}/\sigma_i\mathfrak{P} \\ a \mod \mathfrak{P} \mapsto \sigma_i a \mod \sigma_i\mathfrak{P} \end{array}$$

Daher ist

$$f_i = [\mathcal{O}/\sigma_i\mathfrak{P} : A/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : A/\mathfrak{p}]$$

für $i = 1 \dots r$. Wegen $\sigma_i(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$ folgt ferner

$$\mathfrak{P}^\nu | \, \mathfrak{p}\mathcal{O} \Leftrightarrow \sigma_i(\mathfrak{P}^\nu) | \, \sigma(\mathfrak{p}\mathcal{O}) \Leftrightarrow (\sigma_i\mathfrak{P})^\nu | \, \mathfrak{p}\mathcal{O} \quad ,$$

also $e_1 = e_2 = \ldots = e_r$. □

Satz 13.6.
Sei $\mathfrak{P}_Z := \mathfrak{P} \cap Z_{\mathfrak{P}}$ das unter $\mathfrak{P}$ liegende Primideal von $Z_{\mathfrak{P}}$. Also

$$\begin{array}{cc} L & \mathfrak{P} \\ ef \,| & | \\ Z_{\mathfrak{P}} & \mathfrak{P}_Z \\ r \,| & | \\ K & \mathfrak{p} \end{array}$$

Dann gilt

(i) $\mathfrak{P}_Z$ ist unzerlegt in L, d.h. $\mathfrak{P}$ ist das einzige Primideal über $\mathfrak{P}_Z$ in L.

(ii) $\mathfrak{P}$ hat über $Z_{\mathfrak{P}}$ den Verzweigungsindex e und den Trägheitsgrad f.

(iii) Der Verzweigungsindex und Trägheitsgrad von $\mathfrak{P}_Z$ über K sind jeweils 1.

Beweis.

(i) Wegen $G(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$ sind die über $\mathfrak{P}_Z$ liegenden Primideale $\sigma\mathfrak{P}$ mit $\sigma \in G(L/Z_{\mathfrak{P}})$ alle gleich $\mathfrak{P}$.

(ii),(iii) Wegen $|G| = n = ref$ und $r = [G : G_{\mathfrak{P}}]$ ist

$$|G_{\mathfrak{P}}| = ef = [L : Z_{\mathfrak{P}}] \quad .$$

Setze

$$\begin{aligned} e' &= e(\mathfrak{P}/\mathfrak{P}_Z) \qquad & e'' &= e(\mathfrak{P}_Z/\mathfrak{p}) \\ f' &= f(\mathfrak{P}/\mathfrak{P}_Z) \qquad & f'' &= f(\mathfrak{P}_Z/\mathfrak{p}) \end{aligned}$$

Es gilt

$$e = e'e'' \qquad f = f'f'' \quad .$$

Die fundamentale Gleichung 11.4 für die galoische Erweiterung $L/Z_{\mathfrak{P}}$ besagt

$$ef = [L : Z_{\mathfrak{P}}] = r'e'f' = e'f' \quad .$$

Also

$$ef = e'e''f'f'' = e'f' \quad ,$$

somit muss $e'' = f'' = 1$ gelten, und es folgt $e = e'$ und $f = f'$.

□

Sei $\sigma \in G_{\mathfrak{P}}$; dann induziert σ wegen $\sigma\mathcal{O} = \mathcal{O}$ und $\sigma\mathfrak{P} = \mathfrak{P}$ einen Automorphismus

$$\begin{aligned} \bar{\sigma} : \mathcal{O}/\mathfrak{P} &\xrightarrow{\sim} \mathcal{O}/\mathfrak{P} \\ a \mod \mathfrak{P} &\mapsto \sigma a \mod \mathfrak{P} \quad . \end{aligned}$$

der Restklassenkörper. Setze

$$\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P} \qquad \kappa(\mathfrak{p}) = A/\mathfrak{p} \quad .$$

Satz 13.7.
Die Erweiterung $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ ist normal, d.h. es gelten die Bedingungen aus Theorem 12.2, und man hat einen surjektiven Gruppenhomomorphismus

$$\begin{aligned} G_{\mathfrak{P}} &\twoheadrightarrow G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \\ \sigma &\mapsto \bar{\sigma} \quad . \end{aligned}$$

Beweis.

- Der Trägheitsgrad von $\mathfrak{P}_Z$ über K ist (siehe Satz 13.6)

  $$f'' = f(\mathfrak{P}_Z/\mathfrak{p}) = 1 \quad ,$$

  also hat $Z_{\mathfrak{P}}$ den gleichen Restklassenkörper wie K. Wir können daher

  $$Z_{\mathfrak{P}} = K \qquad G = G_{\mathfrak{P}}$$

  annehmen.

- Sei $\theta \in \mathcal{O}$ ein Repräsentant eines Elementes $\bar{\theta} \in \kappa(\mathfrak{P})$. Sei

  $$\begin{aligned} f(X) &= min_{\kappa}(\theta) \in A[X] \ , \quad \text{da } \mathcal{O} \text{ ganz} \\ \bar{g}(X) &= min_{\kappa(\mathfrak{p})}(\bar{\theta}) \in \kappa(\mathfrak{p})[X] \quad . \end{aligned}$$

  Da $\bar{\theta} = \theta \mod \mathfrak{P}$ Nullstelle von $\bar{f} = f \mod \mathfrak{p}$ ist, gilt $\bar{g}|\bar{f}$. Da L/K normal ist, zerfällt f über $\mathcal{O}$ in Linearfaktoren. Daher zerfallen $\bar{f}$ über $\kappa(\mathfrak{P})$ und somit auch $\bar{g}$ in Linearfaktoren. Also ist auch die Körpererweiterung $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ normal.

- Sei nun $\kappa(\mathfrak{p})$ endlich oder von Charakteristik Null und $\bar{\theta}$ ein primitives Element von $\kappa(\mathfrak{P})$ über $\kappa(\mathfrak{p})$. (Andernfalls betrachte man ein primitives Element für den größten separablen Zwischenkörper.) Sei

$$\bar{\sigma} \in G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) = G(\kappa(\mathfrak{p})(\theta)/\kappa(\mathfrak{p})) \; .$$

Dann ist $\bar{\sigma}\bar{\theta}$ Nullstelle von $\bar{g}$, also auch von $\bar{f}$. Also gibt es eine Nullstelle θ' von $f(X)$ mit

$$\theta' = \bar{\sigma}(\bar{\theta}) \mod \mathfrak{P} \quad .$$

Da θ' zu θ konjugiert ist, gibt es $\sigma \in G$ mit

$$\sigma\theta = \theta' \quad .$$

Also

$$\sigma\theta = \bar{\sigma}(\bar{\theta}) \mod \mathfrak{P} \; .$$

Also wird σ durch $G_{\mathfrak{P}} \to G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ auf $\bar{\sigma}$ abgebildet, da Übereinstimmung auf dem primitiven Element $\bar{\theta}$ vorliegt. Also ist die Abbildung surjektiv.

□

Definition 13.8

Der Kern $I_{\mathfrak{P}} \triangleq G_{\mathfrak{P}}$ der Surjektion

$$G_{\mathfrak{P}} \twoheadrightarrow G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

heißt Trägheitsgruppe von $\mathfrak{P}$ über $\mathfrak{p}$. Der Fixkörper

$$T_{\mathfrak{P}} = \{x \in L | \; \sigma x = x \text{ für alle } \sigma \in I_{\mathfrak{P}}\}$$

heißt Trägheitskörper von $\mathfrak{P}$ über K. Es gilt also

$$K \subseteq Z_{\mathfrak{P}} \subseteq T_{\mathfrak{P}} \subseteq L \quad ,$$

die letzten beiden Erweiterungen sind galoisch und wir haben die exakte Sequenz von Gruppen

$$1 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \to G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \to 1 \; .$$

Satz 13.9.
Die Erweiterung $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ ist normal und es gilt

$$\begin{aligned} G(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) &\xrightarrow{\sim} G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \quad , \\ G(L/T_{\mathfrak{P}}) &= I_{\mathfrak{P}} \end{aligned}$$

Ist die Restklassenkörpererweiterung $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ separabel, so ist

$$\begin{aligned} |I_{\mathfrak{P}}| &= [L : T_{\mathfrak{P}}] = e \\ [G_{\mathfrak{P}} : I_{\mathfrak{P}}] &= [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = f \quad . \end{aligned}$$

In diesem Fall gilt für das unter $\mathfrak{P}$ in $T_{\mathfrak{P}}$ liegende Ideal $\mathfrak{P}_T = \mathfrak{P} \cap \mathcal{O}_{T_{\mathfrak{P}}}$:

$$\begin{aligned} &(i) \quad e(\mathfrak{P}/\mathfrak{P}_T) \quad = e \quad f(\mathfrak{P}/\mathfrak{P}_T) = 1 \\ &(ii) \quad e(\mathfrak{P}_T/\mathfrak{P}_Z) = 1 \quad f(\mathfrak{P}_T/\mathfrak{P}_Z) = f \end{aligned}$$

Wir fassen die Situation zusammen:

Körper	*Ideale*	*Grade*(e, f)
L	$\mathfrak{P}$	
$\vert$	$\vert$	$(e, 1)$
$T_{\mathfrak{P}}$	$\mathfrak{P}_T$	
$\vert$	$\vert$	$(1, f)$
$Z_{\mathfrak{P}}$	$\mathfrak{P}_Z$	
$\vert$	$\vert$	$(1, 1)$
K	$\mathfrak{p}$	

und es gilt $\mathfrak{P}_T = \mathfrak{P}_Z \mathcal{O}_{T_{\mathfrak{P}}}$ *sowie* $\mathfrak{P}_T \mathcal{O}_L = \mathfrak{P}^e$. *Insbesondere gilt*

$$I_{\mathfrak{P}} = 1 \Leftrightarrow L = T_{\mathfrak{P}} \Leftrightarrow \mathfrak{p} \quad \textit{unverzweigt in } L\,.$$

Beweis.

- Die ersten Gleichungen sind Standard–Galoistheorie. Ist die Erweiterung $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ separabel, so ist

$$\begin{aligned} f &= [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = |G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))| \\ &= |G(T_{\mathfrak{P}}/Z_{\mathfrak{P}})| = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = [G_{\mathfrak{P}} : I_{\mathfrak{P}}]\,. \end{aligned}$$

  Aus $|G_{\mathfrak{P}}| = ef$ folgt die andere Gleichheit:

$$|I_{\mathfrak{P}}| = \frac{|G_{\mathfrak{P}}|}{[G : I_{\mathfrak{P}}]} = \frac{ef}{f} = e \quad .$$

- Es bleiben (i) und (ii) zu zeigen. Diese folgen aus

$$\kappa(\mathfrak{P}_T) = \kappa(\mathfrak{P}) \quad .$$

  Denn mit 13.6(iii) folgt dann

$$f = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = [\kappa(\mathfrak{P}_T) : \kappa(\mathfrak{P}_Z)] = f(\mathfrak{P}_T/\mathfrak{P}_Z)\,.$$

  Die fundamentale Gleichung zeigt $e(\mathfrak{P}_T : \mathfrak{P}_Z) = 1$, die Transitivität des Verzweigungsindex liefert

$$e(\mathfrak{P}/\mathfrak{P}_T) = e\,,$$

  und die fundamentale Gleichung zeigt $f(\mathfrak{P}/\mathfrak{P}_T) = f$.

- Um $\kappa(\mathfrak{P}_T) = \kappa(\mathfrak{P})$ zu zeigen, bemerken wir, dass die Trägheitsgruppe von $\mathfrak{P}$ über K die Automorphismen σ von L sind, die $\mathfrak{P}$ festlassen und

  erstens auf K die Identität sind
  zweitens auf $\mathcal{O}/\mathfrak{P}$ die Identität induzieren.

  Diese lassen aber nach Definition von $T_{\mathfrak{P}}$ auch $T_{\mathfrak{P}}$ fest, sind also auch in der Trägheitsgruppe von $\mathfrak{P}$ über $\mathfrak{P}_T$. Diese ist also eine Untergruppe von $I_{\mathfrak{P}}$. Satz 13.7, angewandt auf die Körpererweitung $L/T_{\mathfrak{P}}$ zeigt

$$G(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_T)) \subseteq I_{\mathfrak{P}}/I_{\mathfrak{P}},$$

  ist also trivial. Also gilt $\kappa(\mathfrak{P}) = \kappa(\mathfrak{P}_T)$.

□

14 Kreisteilungskörper

Wir wollen das Zerlegungsverhalten von Primzahlen in Kreisteilungskörpern studieren.

Satz 14.1.
Sei l eine Primzahl, $\nu \in \mathbb{N}$ und ζ eine primitive l^ν–te Einheitswurzel. Sei $\mathcal{O}$ der Ring der ganzen Zahlen von $\mathbb{Q}(\zeta)$ und $\lambda = 1 - \zeta$.
Dann ist das Hauptideal (λ) ein $\mathcal{O}$ Primideal vom Trägheitsgrad $f = 1$. Es gilt

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

mit $d = \varphi(l^\nu) := (l-1)l^{\nu-1} = [\mathbb{Q}(\zeta) : \mathbb{Q}]$. Ferner hat die Basis $1, \zeta, \ldots, \zeta^{d-1}$ von $\mathbb{Q}(\zeta)/\mathbb{Q}$ die Diskriminante

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s$$

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

Beweis.

- Das Minimalpolynom von ζ ist das sogenannte l^ν–te Kreisteilungspolynom (Satz 1.3.13 aus Algebra 2):

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

Setzen wir $X = 1$, so erhalten wir

$$\prod_{g \in (\mathbb{Z}_{l^\nu})^\times} (1 - \zeta^g) = l \tag{10}$$

Nun ist

$$1 - \zeta^g = \varepsilon_g (1 - \zeta)$$

mit

$$\varepsilon_g = \frac{1 - \zeta^g}{1 - \zeta} = 1 + \zeta + \ldots + \zeta^{g-1} \quad \in \quad \mathcal{O}\,,$$

also ist ε_g ganz. Sei $g' \in \mathbb{Z}$ mit $gg' = 1 \mod l^\nu$, so ist

$$\frac{1 - \zeta}{1 - \zeta^g} = \frac{1 - \zeta^{gg'}}{1 - \zeta^g} = 1 + \zeta^g + \ldots + \zeta^{g(g'-1)} \quad \in \quad \mathcal{O}\,.$$

Also ist ε_g Einheit. Die Gleichung (10) liefert

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

mit der Einheit $\varepsilon := \prod_g \varepsilon_g$. Es folgt $l\mathcal{O} = (\lambda)^{\varphi(l^\nu)}$. Wegen $\varphi(l^\nu) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ und

$$e((\lambda)/l) = \varphi(l^\nu)$$

folgt mit der fundamentalen Gleichung, dass $\varphi(l^\nu) = efr$, $r = 1$ und $f((\lambda)/l) = 1$ gilt.

- Seien $\zeta = \zeta_1, \zeta_2, \ldots, \zeta_d$ die Konjugierten von ζ. Das Minimalpolynom ist

$$\Phi_{l^\nu}(X) = \prod_{i=1}^{d}(X - \zeta_i) \quad ,$$

seine Ableitung

$$\Phi'_{l^\nu}(X) = \sum_{i=1}^{d}\prod_{\substack{j=1\\ j\neq i}}^{d}(X - \zeta_j) \quad ,$$

also

$$\Phi'_{l^\nu}(\zeta_i) = \prod_{\substack{j=1\\ j\neq i}}^{d}(\zeta_i - \zeta_j) \quad .$$

Es folgt für die Diskriminante

$$\pm d(1, \zeta, \ldots, \zeta^{d-1}) = \prod_{i\neq j}(\zeta_i - \zeta_j) = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\Phi'_{l^\nu}(\zeta))$$

- Aus

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

folgt durch Differenzieren nach X

$$l^{\nu-1}X^{l^{\nu-1}-1}\Phi_{l^\nu}(X) + (X^{l^{\nu-1}} - 1)\Phi'_{l^\nu}(X) = l^\nu X^{l^\nu - 1}$$

Einsetzen von ζ liefert mit $\zeta^{l^\nu} = 1$

$$(\zeta^{l^{\nu-1}} - 1)\Phi'_{l^\nu}(\zeta) = l^\nu \zeta^{-1} \quad .$$

Hierbei ist $\xi := \zeta^{l^{\nu-1}}$ eine primitive l–te Einheitswurzel. Es gilt wegen (10) mit $\nu = 1$

$$N_{\mathbb{Q}(\xi)/\mathbb{Q}}(1 - \xi) = \pm l \quad .$$

Die Schachtelungsformel 5.4 für die Norm zeigt

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \xi) = N_{\mathbb{Q}(\xi)/\mathbb{Q}} \circ N_{\mathbb{Q}(\zeta)/\mathbb{Q}(\xi)}(1 - \xi) = N_{\mathbb{Q}(\xi)/\mathbb{Q}}(1 - \xi)^{l^{\nu-1}} = l^{l^{\nu-1}} \quad .$$

Ferner ist $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{-1}) = \pm 1$, da ζ Einheit ist. Insgesamt folgt

$$\begin{aligned} d(1, \zeta, \ldots, \zeta^{d-1}) &= N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\Phi'_{l^\nu}(\zeta)) \\ &= \frac{N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(l^\nu)N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{-1})}{N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi - 1)} \\ &= \pm l^{\nu\varphi(l^\nu)} l^{-l^{\nu-1}} \\ &= \pm l^{\nu(l-1)l^{\nu-1} - l^{\nu-1}} \\ &= \pm l^{l^{\nu-1}(\nu l - \nu - 1)} = \pm l^s \end{aligned}$$

□

Satz 14.2.
Sei $n \in \mathbb{N}$, ζ eine primitive n–te Einheitswurzel und $\mathcal{O}$ der Ring der ganzen Zahlen von $\mathbb{Q}(\zeta)$. Dann ist $1, \zeta, \ldots, \zeta^{d-1}$ mit $d = \varphi(n)$ eine Ganzheitsbasis, also

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

Beweis.
Wir zeigen den Satz nur für den Fall, dass $n = l^\nu$ eine Primzahlpotenz ist. Der Fall allgemeiner n folgt mit Hilfe von Satz 5.13. Wegen

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s$$

und Lemma 5.9 ist

$$l^s\mathcal{O} \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O} \quad . \tag{11}$$

Sei wieder $\lambda = 1 - \zeta$. Aus Satz 14.1, genauer aus $f(\lambda\mathcal{O}/l) = 1$, folgt

$$\mathcal{O}/\lambda\mathcal{O} \cong \mathbb{Z}/l$$

also $\mathcal{O} = \mathbb{Z} + \lambda\mathcal{O}$ und erst recht

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

Multiplikation mit λ liefert

$$\lambda\mathcal{O} = \lambda^2\mathcal{O} + \lambda\mathbb{Z}[\zeta]$$

also $\mathcal{O} = \lambda^2\mathcal{O} + \mathbb{Z}[\zeta]$, da $\lambda = 1 - \zeta \in \mathbb{Z}[\zeta]$. Es folgt induktiv

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

für alle natürlichen t. Setze $t := s\varphi(l^\nu)$. Wegen

$$l\mathcal{O} = \lambda^{\varphi(l^\nu)}\mathcal{O}$$

nach Satz 14.1 folgt

$$\begin{aligned} \mathcal{O} &= \lambda^t\mathcal{O} + \mathbb{Z}[\zeta] = \lambda^{\varphi(l^\nu)s}\mathcal{O} + \mathbb{Z}[\zeta] \\ &= l^s\mathcal{O} + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta] \quad . \end{aligned}$$

□

Wir wollen jetzt das Zerlegungsgesetz von Primzahlen in $\mathbb{Q}(\zeta)$ angeben:

Satz 14.3.
Sei $n = \prod_p p^{\nu_p}$ die Primzerlegung von n und sei f_p die kleinste natürliche Zahl, so dass

$$p^{f_p} = 1 \mod \frac{n}{p^{\nu_p}} \quad .$$

Ein solches f_p existiert, da $m := \frac{n}{p^{\nu_p}}$ und p teilerfremd sind, also $\bar{p} \in (\mathbb{Z}/m)^\times$. Sei ζ primitive n–te Einheitswurzel. Dann besitzt p in $\mathbb{Q}(\zeta)$ die Zerlegung

$$p\mathcal{O} = (\mathfrak{p}_1 \ldots \mathfrak{p}_r)^{\varphi(p^{\nu_p})} \quad ,$$

wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ paarweise verschiedene Primideale vom gleichen Trägheitsgrad f_p sind. Insbesondere folgt:
Gilt $(p, n) = 1$, so ist $\nu_p = 0$, $\varphi(p^{\nu_p}) = \varphi(1) = 1$, also ist p unverzweigt.

Beweis.

- Wegen $\mathcal{O} = \mathbb{Z}[\zeta]$ ist der Führer von $\mathbb{Z}[\zeta]$ gleich 1, also ganz $\mathcal{O}$. Wir können also Satz 11.6 auf jede Primzahl anwenden. Es ist also zu zeigen

$$\Phi_n(X) = (p_1(X) \dots p_r(X))^{\varphi(p^{\nu_p})} \mod p \quad ,$$

wobei die $p_i \in \mathbb{F}_p[X]$ verschiedene irreduzible Polynome von Grad f_p sind.

- Sei nun $n = p^{\nu_p} m$ mit $(m, p) = 1$.
Durchlaufen ζ_i die primitiven m–ten und η_j die primitiven p^{ν_p}–ten Einheitswurzeln, so durchlaufen $\zeta_i \eta_j$ die primitiven n–ten Einheitswurzeln.
Also

$$\Phi_n(X) = \prod_{i,j} (X - \zeta_i \eta_j)$$

Wegen $X^{p^{\nu_p}} - 1 = (X-1)^{p^{\nu_p}} \mod p$ ist für jedes $\mathfrak{p}|p$ erfüllt $\eta_j = 1 \mod \mathfrak{p}$. Also sehen wir modulo $\mathfrak{p}$

$$\Phi_n(X) = \prod_i (X - \zeta_i)^{\varphi(p^{\nu^p})} = \Phi_m(X)^{\varphi(p^{\nu_p})} \mod \mathfrak{p} \quad .$$

Da die Polynome in $\mathbb{Z}[X]$ liegen, folgt

$$\Phi_n(X) = \Phi_m(X)^{\varphi(p^{\nu_p})} \mod p \quad .$$

Es bleibt zu zeigen, dass $\Phi_m(X) \mod p$ ein Produkt irreduzibler Polynome in $\mathbb{F}_p[X]$ von Grad f_p mit $p^{f_p} = 1 \mod m$ ist.

- Wir haben die Aussage also auf den Fall reduziert, wenn p *kein* Teiler von n ist, also $\varphi(p^{\nu_p}) = \varphi(1) = 1$ gilt. Da $\operatorname{char}(\mathcal{O}/\mathfrak{p}) = p$ für $\mathfrak{p}$ Teiler von p nicht n teilt, haben $X^n - 1$ und nX^{n-1} keine gemeinsamen Nullstelle in $\mathcal{O}/\mathfrak{p}$, also hat $X^n - 1 \mod \mathfrak{p}$ keine mehrfache Nullstelle. Die Abbildung

$$\mathcal{O} \twoheadrightarrow \mathcal{O}/\mathfrak{p}$$

bildet also die Gruppe $\mu_n = \langle \zeta \rangle$ der n–ten Einheitswurzeln bijektiv auf die n–ten Einheitswurzeln von $\mathcal{O}/\mathfrak{p}$ ab, ζ bleibt somit primitive n–te Einheitswurzel.

Der kleinste Erweiterungskörper von $\mathbb{F}_p$, der ζ enthält, ist grade $\mathbb{F}_{p^{f_p}}$, denn die Gruppe $\mathbb{F}_{p^{f_p}}^{\times}$ ist zyklisch von der Ordnung $p^{f_p} - 1$. Also ist $\mathbb{F}_{p^{f_p}}$ Zerfällungskörper von

$$\overline{\Phi_n(X)} := \Phi_n(X) \mod p \quad .$$

Als Teiler von $X^n - 1 \mod p$ hat $\overline{\Phi_n(X)}$ keine mehrfachen Nullstellen. Ist

$$\overline{\Phi_n} = \overline{p_1}(X) \dots \overline{p_r}(X)$$

die Zerlegung in irreduzible Faktoren in $\mathbb{F}_p[X]$, so ist jedes $\bar{p_i}$ Minimalpolynom einer primitiven n–ten Einheitswurzel $\bar{\zeta} \in \mathbb{F}_{p^{f_p}}^{\times}$, hat also Grad f_p.

□

Korollar 14.4.

(i) Eine Primzahl p ist in $\mathbb{Q}(\zeta)$ genau dann verzweigt, wenn

$$n = \begin{cases} 0 \mod p & \text{für } p \neq 2 \\ 0 \mod 4 & \text{für } p = 2 \end{cases} .$$

(ii) Eine Primzahl $p \neq 2$ ist in $\mathbb{Q}(\zeta)$ voll zerlegt genau dann, wenn $p = 1 \mod n$ ist.

Beweis.

(i) p verzweigt $\Leftrightarrow \varphi(p^{\nu_p}) \neq 1 \Leftrightarrow (p-1)p^{\nu_p - 1} \neq 1$.
Also für $p \neq 2 : p$ verzweigt $\Leftrightarrow \nu_p \geq 1$, d.h. $p|n$;
für $p = 2 : p$ verzweigt $\Leftrightarrow \nu_p \geq 2$, d.h. $4|n$.

(ii) p ist vollzerlegt $\Leftrightarrow \varphi(p^{\nu_p}) = 1$ und $f_p = 1$ für den Trägheitsgrad, also $p = 1 \mod \frac{n}{p^\nu}$. Da $p \neq 2$ vorausgesetzt wurde, folgt $\nu_p = 0$ und $p = 1 \mod n$.

□

Bemerkungen 14.5.
Ganzheitsbasis und Zerlegungsgesetz von $\mathbb{Q}(\zeta)$ sind also gut bekant. Nicht so Fundamentaleinheiten von $\mathbb{Z}[\zeta]^\times$ und die Klassengruppe $Cl_{\mathbb{Q}(\zeta)}$.

Lemma 14.6.
Sei ζ eine primitive p–te Einheitswurzel, wobei p eine ungerade Primzahl ist. Für die Gaußsche Summe

$$\tau = \sum_{a \in \mathbb{Z}_p^\times} \Big(\frac{a}{p}\Big)\zeta^a$$

gilt

$$\tau^2 = \Big(\frac{-1}{p}\Big)p \quad .$$

Beweis.

$$\tau^2 = \sum_{a,b} \Big(\frac{a}{p}\Big)\Big(\frac{b}{p}\Big)\zeta^{a+b} = \sum_{a,b} \Big(\frac{ab}{p}\Big)\zeta^{a+b}$$

Ersetze nun b durch ab:

$$\tau^2 = \sum_{a,b} \Big(\frac{ba^2}{p}\Big)\zeta^{a+ab} = \sum_{a,b} \Big(\frac{b}{p}\Big)\zeta^{a(b+1)}$$

Wir spalten die Summe auf, um die Identität

$$1 + \zeta + \ldots + \zeta^{p-1} = 0$$

benutzen zu können:

$$\begin{aligned} \tau^2 &= \sum_a \Big(\frac{-1}{p}\Big)\zeta^0 + \sum_{b \neq -1} \Big(\frac{b}{p}\Big)\zeta^{a(b+1)} \\ &= \Big(\frac{-1}{p}\Big)(p-1) + \sum_{b \neq -1} \Big(\frac{b}{p}\Big)(-1) \\ &= \Big(\frac{-1}{p}\Big)p - \sum_b \Big(\frac{b}{p}\Big) = \Big(\frac{-1}{p}\Big)p \quad , \end{aligned}$$

da das Legendre–Symbol gleich oft die Werte $+1$ und -1 annimmt. $\square$

Satz 14.7.
Seien l und p ungerade Primzahlen und ζ eine primitive l–te Einheitswurzel. Setze $l^* := \left(\frac{-1}{l}\right) l$. Dann gilt: p ist in $\mathbb{Q}(\sqrt{l^*})$ genau dann voll zerlegt, wenn p in $\mathbb{Q}(\zeta)$ in eine gerade Zahl von Primidealen zerfällt.

Beweis.

" $\Rightarrow$ " Sei p vollzerlegt in $\mathbb{Q}(\sqrt{l^*})$, d.h. $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$. Aus Lemma 14.6 folgt $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{l^*}) \subseteq \mathbb{Q}(\zeta)$. Es existiert $\sigma \in G(\mathbb{Q}(\zeta))/\mathbb{Q}$ mit $\sigma\mathfrak{p}_1 = \mathfrak{p}_2$. Dieses σ liefert eine Bijektion der disjunkten Mengen: $M_i := \{\mathfrak{P} \subseteq \mathbb{Z}[\zeta] \text{ Primideal mit } \mathfrak{P} \cap \mathbb{Q}(\sqrt{l^*}) = \mathfrak{p}_i\}$ mit $i = 1, 2$. Die Menge aller Primideale über p hat als disjunkte Vereinigung dieser gleichmächtigen Mengen eine gerade Zahl von Elementen.

" $\Leftarrow$ " Dann ist für jedes $\mathfrak{P}$ über p der Index der Zerlegungsgruppe $G_\mathfrak{P}$ in $G = G(\mathbb{Q}(\zeta)/\mathbb{Q})$ gerade. Also ist

$$[G : G_\mathfrak{P}] = [Z_\mathfrak{P} : \mathbb{Q}] \qquad \text{gerade .}$$

Da G zyklisch ist, folgt für den Zerlegungskörper

$$\mathbb{Q}(\sqrt{l^*}) \subseteq Z_\mathfrak{P} \quad .$$

Der Trägheitsgrad von $\mathfrak{P} \cap Z_\mathfrak{P}$ über (p) ist nach Satz 13.6(iii) gleich 1. Da

$$\left(\mathcal{O} \cap \mathbb{Q}(\sqrt{l^*})\right) / \left(\mathfrak{p} \cap \mathbb{Q}(\sqrt{l^*})\right)$$

ein Zwischenkörper zwischen $\mathbb{Z}/(p)$ und $(\mathcal{O} \cap Z_\mathfrak{P})/(\mathfrak{P} \cap Z_\mathfrak{P})$ ist, ist auch der Trägheitsgrad

$$f(\mathfrak{P} \cap \mathbb{Q}(\sqrt{l^*})/(p)) = 1 \quad .$$

Ebenso folgt $e(\mathfrak{P} \cap \mathbb{Q}(\sqrt{l^*})/(p)) = 1$, so dass p in $\mathbb{Q}(\sqrt{l^*})$ voll zerlegt ist.

$\square$

Theorem 14.8 (Gaußsches Reziprozitätsgesetz)**.** *Für zwei ungerade Primzahlen l und p gilt:*

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

Wir bemerken zwei "Ergänzungssätze":

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

Beweis.

- Der erste Ergänzungssatz folgt sofort aus der Tatsache, dass $\mathbb{F}_p^\times = (\mathbb{Z}_p)^\times$ zyklisch von der Ordnung $p - 1$ ist.

- Seinetwegen reicht es aus, zu zeigen, dass

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

gilt. Denn wir rechnen mit $l^* = (-1)^{\frac{l-1}{2}} l$

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

- In Beispiel 11.10 sahen wir:

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow p \text{ vollzerlegt in } \mathbb{Q}(\sqrt{a}) .$$

Mit Satz 14.7 folgt: $\left(\frac{l^*}{p}\right) = 1$ genau dann, wenn p in $\mathbb{Q}(\zeta_l)$ eine gerade Zahl r von Primidealen zerfällt. Hier ist $e = 1$, also $r = \frac{l-1}{f}$ nach Satz 14.3, mit $f \in \mathbb{N}$ minimal mit $p^f = 1 \mod l$.
r ist also genau dann gerade, wenn f ein Teiler von $\frac{l-1}{2}$ ist. Das ist aber äquivalent zu

$$p^{\frac{l-1}{2}} = 1 \mod 1 \quad .$$

Dann liegt aber $p \bmod l$ in der Untergruppe $\mathbb{F}_l^{\times 2}$ der Quadrate in der zyklischen Gruppe $\mathbb{F}_l^\times$, da $[\mathbb{F}_l^\times : \mathbb{F}_l^{\times 2}] = 2$. Also gilt genau dann $\left(\frac{p}{l}\right) = 1$.

□

15 Lokalisierung

Wir erinnern an Kapitel 4: sei A kommutativer Ring mit Eins und $S \subseteq A$ eine multiplikative Teilmenge. Der Ring

$$S^{-1}A = \left\{ \frac{a}{s} \middle| a \in A, s \in S \right\}$$

heißt Lokalisierung von A bei S. Wichtiges Beispiel ist das Komplement $S_\mathfrak{p} = A \setminus \mathfrak{p}$ eines Primideales. Der Ring $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$ heißt Lokalisierung von A bei $\mathfrak{p}$. In diesem Kapitel sei A immer integer und $0 \notin S$.

Satz 15.1.
Die Zuordnungen $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$ und $Q \mapsto Q \cap A$ sind zu einander inverse Bijektionen zwischen Primidealen $\mathfrak{q} \subseteq A \setminus S$ von A und den Primidealen Q von $S^{-1}A$.

Beweis.

- Ist $\mathfrak{q} \subseteq A \setminus S$ ein Primideal von A, so ist

$$Q := S^{-1}\mathfrak{q} = \left\{ \frac{a}{s} \middle| q \in \mathfrak{q}, s \in S \right\}$$

ein Primideal von $S^{-1}A$. Es ist offensichtlich ein Ideal. Es ist auch ein Primideal: aus $\frac{a}{s} \cdot \frac{a'}{s'} \in Q$, also $\frac{aa'}{ss'} = \frac{q}{s''}$ (mit evidenten Wertebereich für die Buchstaben) folgt

$$s''aa' = qss' \in \mathfrak{q} \quad .$$

Da $s'' \notin \mathfrak{q}$, folgt $aa' \in \mathfrak{q}$, also $a \in \mathfrak{q}$ oder $a' \in \mathfrak{q}$, somit $\frac{a}{s} \in Q$ oder $\frac{a'}{s'} \in Q$. Ferner gilt

$$\mathfrak{q} = Q \cap A \quad ,$$

denn aus $\frac{q}{s} = a \in Q \cap A$ folgt $q = as$, also $a \in \mathfrak{q}$, da $s \notin \mathfrak{q}$.

- Sei umgekehrt Q ein beliebiges Primideal von $S^{-1}A$. Dann ist $\mathfrak{q} := Q \cap A$ offensichtlich ein Primideal von A. Es gilt $\mathfrak{q} \subseteq A \setminus S$, denn mit $s \in \mathfrak{q} \cap S$ wäre auch $1 = s\frac{1}{s} \in Q$, da $\frac{1}{s} \in S^{-1}A$, also $Q = S^{-1}A$. Ferner ist

$$Q = S^{-1}\mathfrak{q} \quad ,$$

denn mit $\frac{a}{s} \in Q$ ist $a = \frac{a}{s} \cdot s \in Q \cap A = \mathfrak{q}$, also

$$\frac{a}{s} = a\frac{1}{s} \in S^{-1}\mathfrak{q} \quad .$$

□

Beispiele 15.2.
Sei X eine Menge von Primidealen von A,

$$S = A \setminus \cup_{\mathfrak{p} \in X} \mathfrak{p}$$

ist multiplikativ.

$$A_X = S^{-1}A = \left\{ \frac{f}{g} |\ f, g \in A, g \neq 0 \bmod \mathfrak{p} \text{ für alle } \mathfrak{p} \in X \right\}$$

Insbesondere liefert $X = \{\mathfrak{p}\}$ den Ring $A_\mathfrak{p}$.

Korollar 15.3.
Sei $\mathfrak{p}$ Primideal in A, so ist $A_\mathfrak{p}$ ein lokaler Ring, d.h. $A_\mathfrak{p}$ besitzt genau ein maximales Ideal, $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Man hat eine kanonische Einbettung

$$A/\mathfrak{p} \hookrightarrow A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} \ ,$$

durch die $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ zum Quotientenkörper des integren Rings $A/\mathfrak{p}$ wird. Ist insbesondere $\mathfrak{p}$ sogar ein maximales Ideal von A, so gilt

$$A/\mathfrak{p}^n \xrightarrow{\sim} A/\mathfrak{m}_\mathfrak{p}^n$$

für alle natürlichen n.

Beweis.

- Nach Satz 15.1 mit $S = A \setminus \mathfrak{p}$ entsprechen die in $\mathfrak{p}$ enthaltenen Primideale von A bijektiv den Primidealen von $A_\mathfrak{p}$. Also ist $\mathfrak{m}_\mathfrak{p} = S^{-1}\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ das einzige maximale Ideal von $A_\mathfrak{p}$.

- Wegen $\mathfrak{p} \subseteq \mathfrak{m}_\mathfrak{p} \cap A$ ist der Homomorphismus

$$\begin{aligned} f: \quad A/\mathfrak{p}^n &\to A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n \\ a \bmod \mathfrak{p} &\mapsto a \bmod \mathfrak{m}_\mathfrak{p}^n \end{aligned}$$

wohldefiniert.
Für $n = 1$ ist $\ker f = (\mathfrak{m}_\mathfrak{p} \cap A) \bmod \mathfrak{p} = \mathfrak{p} \bmod \mathfrak{p} = 0$, also ist f injektiv. Man sieht, dass $A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ sogar der Quotientenkörper von $A/\mathfrak{p}$ ist.

- Wir schieben eine Hilfsüberlegung ein für den Fall, dass $\mathfrak{p}$ maximal ist. Für jedes $s \in A \setminus \mathfrak{p}$ gilt
$$\mathfrak{p}^n + sA = A \quad ,$$
was aber heißt, dass $\bar{s} := s \bmod \mathfrak{p}^n$ eine Einheit in $A/\mathfrak{p}^n$ ist.
Für $n = 1$ folgt dies aus der Maximalität von $\mathfrak{p}$. Für beliebiges n wenden wir vollständige Induktion an:
$$\mathfrak{p} = \mathfrak{p}A = \mathfrak{p}(\mathfrak{p}^{n-1} + sA) \subseteq \mathfrak{p}^n + sA \subseteq A \quad .$$
Die erste Inklusion ist echt, da $s \notin \mathfrak{p}$. Da $\mathfrak{p}$ maximal ist, folgt $\mathfrak{p}^n + sA = A$.

- Injektivität von f: Sei $a \in A$ mit $a \in \mathfrak{m}_\mathfrak{p}^n$, also $a = \frac{b}{s}$ mit $b \in \mathfrak{p}^n$ und $s \in S$, $s \notin \mathfrak{p}$. Dann folgt $as = b \in \mathfrak{p}^n$, also $\bar{a}\bar{s} = 0 \bmod \mathfrak{p}^n$. Aus der Hilfsüberlegung folgt $\bar{s} \in (A/\mathfrak{p}^n)^\times$, also $\bar{a} = 0 \bmod \mathfrak{p}^n$.

- Surjektivität von f: Sei $\frac{a}{s} \in A_\mathfrak{p}$ mit $a \in A$ und $s \notin \mathfrak{p}$. Wegen der Hilfsüberlegung gibt es $a' \in A$ mit
$$a = a's \bmod \mathfrak{p}^n \quad .$$
Also
$$\frac{a}{s} = a' \bmod \mathfrak{p}^n A_\mathfrak{p} \quad .$$
Also liegt $\frac{a}{s} \bmod \mathfrak{m}_\mathfrak{p}^n$ in Bild von f.

□

Wir erinnern daran, dass lokaler Ring A ein eindeutig bestimmtes maximales Ideal $\mathfrak{m}$ hat. Ein Ring A ist tatsächlich genau dann lokal, wenn es ein Ideal $\mathfrak{m}$ gibt, so dass $A^\times = A \setminus \mathfrak{m}$ gilt.

Nach den Körpern sind die folgenden Ringe die einfachsten lokalen Ringe.

Definition 15.4
Ein diskreter Bewertungsring ist ein Hauptidealring $\mathcal{O}$ mit einem einzigen maximalen Ideal $\mathfrak{p} \neq 0$.

Betrachtung 15.5.
Das maximale Ideal $\mathfrak{p}$ eines diskreten Bewertungsrings $\mathcal{O}$ ist von der Form $\mathfrak{p} = (\pi) = \pi\mathcal{O}$ mit einen Primelement $\pi \in \mathcal{O}$. Da jedes $a \in \mathcal{O} \setminus \mathfrak{p}$ Einheit in $\mathcal{O}$ ist, liegt jedes andere Primelement von $\mathcal{O}$ auch in $\mathfrak{p}$. Also $\pi' = \lambda\pi$. Hauptidealringe sind faktoriell, also ist λ Einheit. Also ist π bis auf Assoziierte das einzige Primelement von $\mathcal{O}$. Jedes $a \in \mathcal{O} \setminus \{0\}$ lässt sich daher eindeutig in der Form
$$a = \varepsilon\pi^n \qquad \varepsilon \in \mathcal{O}^\times \quad n \geq 0$$
schreiben. Sei $0 \neq a \in K = \mathrm{Quot}(\mathcal{O})$, so hat a die eindeutige Darstellung
$$a = \varepsilon\pi^n$$
mit $\varepsilon \in \mathcal{O}^\times$ und $n \in \mathbb{Z}$. Somit gibt es eine Abbildung
$$\nu: \quad K \to \mathbb{Z} \cup \{\infty\}$$
$$a \mapsto \nu(a) = \begin{cases} \infty & \text{für } a = 0 \\ n & \text{für } a = \varepsilon\pi^n. \end{cases}$$
ν heißt Bewertung von K. Offensichtlich gilt
$$\nu(ab) = \nu(a) + \nu(b)$$
$$\nu(a+b) \geq \min\{\nu(a), \nu(b)\} \qquad a, b \in K$$

Die diskreten Bewertungsmenge treten als Lokalisierung von Dedekindring auf.

Satz 15.6.
Sei $\mathcal{O}$ ein Dedekindring und $S \subseteq \mathcal{O} \setminus \{0\}$ eine multiplikative Teilmenge. Denn ist es auch $S^{-1}\mathcal{O}$ ein Dedekindring.

Beweis.

- $S^{-1}\mathcal{O}$ ist integer. Aus Satz 15.1 folgt, dass jedes Primideal von $S^{-1}\mathcal{O}$ auch maximal ist, da dies in $\mathcal{O}$ gilt.
- Sei $\mathfrak{A}$ ein Ideal von $S^{-1}\mathcal{O}$ und $\mathfrak{a} := \mathcal{O} \cap \mathfrak{A}$. Dann ist $\mathfrak{A} = S^{-1}\mathfrak{a}$. Denn sei $\frac{a}{s} \in \mathfrak{A}$, $a \in \mathcal{O}$ und $s \in S$, dann ist
$$a = s\frac{a}{s} \in \mathfrak{A} \cap \mathcal{O} = \mathfrak{a}$$
Also
$$\frac{a}{s} = a\frac{1}{s} \in S^{-1}\mathfrak{a} \quad .$$
Die Inklusion $S^{-1}\mathfrak{a} \subseteq \mathfrak{A}$ ist klar. Mit $\mathfrak{a}$ ist auch $\mathfrak{A}$ endlich erzeugt und $S^{-1}\mathcal{O}$ somit noethersch.
- Es bleibt zu zeigen, dass $S^{-1}\mathcal{O}$ ganzabgeschlossen ist. Sei $x \in K = \mathrm{Quot}(\mathcal{O}) = \mathrm{Quot}(S^{-1}\mathcal{O})$ mit
$$x^n + \frac{a_1}{s_1}x^{n-1} + \ldots + \frac{a_n}{s_n} = 0$$
mit $\frac{a_i}{s_i} \in S^{-1}\mathcal{O}$. Multipliziere mit
$$(s_1 \ldots s_n)^n =: s^n \quad ,$$
also ist sx ganz über $\mathcal{O}$. Da $\mathcal{O}$ ganz abgeschlossen ist, folgt $sx \in \mathcal{O}$, also $x \in S^{-1}\mathcal{O}$.

□

Satz 15.7.
Sei $\mathcal{O}$ ein integrer noetherscher Ring. Der Ring $\mathcal{O}$ ist genau dann ein Dedekindring, wenn für alle Primideale $\mathfrak{p} \neq 0$ von $\mathcal{O}$ die Lokalisierung $\mathcal{O}_\mathfrak{p}$ ein diskreter Bewertungsring ist.

Beweis.

" $\Rightarrow$ " Sei $\mathcal{O}$ Dedekindring. Dann ist nach Satz 15.6 auch $\mathcal{O}_\mathfrak{p}$ ein Dedekindring. Jedes Primideal von $\mathcal{O}_\mathfrak{p}$ ist maximal und nach Satz 15.1 von der Form $\mathfrak{q}S^{-1}$ mit $\mathfrak{q} \subseteq \mathfrak{p}$, also gleich $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Es gibt also nur ein Primideal in $\mathcal{O}_\mathfrak{p}$.
Sei $\pi \in \mathfrak{m}_\mathfrak{p} \setminus \mathfrak{m}_\mathfrak{p}^2$. Da $\mathcal{O}_\mathfrak{p}$ Dedekindring ist und $\mathfrak{m}_\mathfrak{p}$ einziges Primideal ist, folgt $(\pi) = \mathfrak{m}_\mathfrak{p}^r$, also $r = 1$, da $\pi \notin \mathfrak{m}_\mathfrak{p}^2$. Induktiv sieht man
$$(\pi^n) = \mathfrak{m}_\mathfrak{p}^n \quad .$$
Da $\mathcal{O}_\mathfrak{p}$ ein Dedekindring ist, gilt für jedes Ideal $\mathfrak{a}$ von $\mathcal{O}_\mathfrak{p}$
$$\mathfrak{a} = \mathfrak{m}_\mathfrak{p}^n = (\pi^n) \quad \text{für ein } n \, .$$
Also ist $\mathfrak{a}$ Hauptideal und $\mathcal{O}_\mathfrak{p}$ prinzipal. Lokal ist $\mathcal{O}_\mathfrak{p}$ als Lokalisierung an $\mathfrak{p}$ sowieso.

" $\Leftarrow$ " Wir zeigen zunächst: ist $\mathcal{O}$ integer und noethersch, so gilt

$$\mathcal{O} = \cap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}} \quad ,$$

wobei $\mathfrak{p}$ alle von Null verschiedene Primideale von $\mathcal{O}$ durchläuft und der Durchschnitt in $K = \mathrm{Quot}(\mathcal{O})$ gebildet wird. Da $\mathcal{O}$ integer ist, gilt $\mathcal{O} \subseteq \mathcal{O}_{\mathfrak{p}}$, also $\mathcal{O} \subseteq \cap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$. Sei $\frac{a}{b} \in \cap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$ mit $a, b \in \mathcal{O}$. Dann ist

$$\mathfrak{a} := \{x \in \mathcal{O} |\, xa \in b\mathcal{O}\}$$

ein Ideal von $\mathcal{O}$. Es ist in keinem Primideal von $\mathcal{O}$ enthalten. Denn sei $\mathfrak{p}$ Primideal, dann gilt $\frac{a}{b} \in \mathcal{O}_{\mathfrak{p}}$; also kann man schrieben $\frac{a}{b} = \frac{c}{s}$ mit $c \in \mathcal{O}$ und $s \notin \mathfrak{p}$. Hieraus folgt

$$as = cb \quad ,$$

daher $s \in \mathfrak{a} \setminus \mathfrak{p}$. Also liegt $\mathfrak{a}$ in keinem maximalen Ideal von $\mathcal{O}$. Wegen 2.16(iii) folgt $\mathfrak{a} = \mathcal{O}$. Also $1 \in \mathfrak{a}$, also $a \in b\mathcal{O}$, also $\frac{a}{b} \in \mathcal{O}$.

Sind alle $\mathcal{O}_{\mathfrak{p}}$ diskrete Bewertungsringe, so sind sie als Hauptidealringe faktoriell und nach 4.10(i) ganz abgeschlossen. Also ist auch $\mathcal{O}$ als ihr Durchschnitt ganz abgeschlossen.
Jedes Primideal $\mathfrak{p}$ von $\mathcal{O}$ ist maximal, da aus $\mathfrak{p} \subseteq \mathfrak{m}$ folgt $\mathfrak{p}\mathcal{O}_{\mathfrak{m}} \subseteq \mathfrak{m}\mathcal{O}_{\mathfrak{m}}$. Also ist $\mathcal{O}$ Dedekindring.

□

Betrachtung 15.8.
Sei $\mathcal{O}$ ein Dedekindring, $\mathfrak{p} \neq 0$ ein Primideal. Dann ist $\mathcal{O}_{\mathfrak{p}}$ ein diskreter Bewertungsring mit zugehöriger Bewertung

$$v_{\mathfrak{p}} : \quad \mathrm{Quot}(\mathcal{O}) =: K \longrightarrow \mathbb{Z} \cup \{\infty\} \quad .$$

Ist $x \in K^{\times}$ und

$$x\mathcal{O} = (x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

die Primzerlegung des gebrochenen Hauptideals, dann ist

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

Denn für jedes feste Primideal $\mathfrak{q} \neq (0)$ von $\mathcal{O}$ mit $\mathfrak{q} \neq \mathfrak{p}$ gilt

$$\mathfrak{p}\mathcal{O}_{\mathfrak{q}} = \mathcal{O}_{\mathfrak{q}} \quad ,$$

da Elemente von $\mathfrak{p}$ Einheiten in $\mathcal{O}_{\mathfrak{q}}$ ergeben, also

$$x\mathcal{O}_{\mathfrak{q}} = \Big(\prod \mathfrak{p}^{\nu_{\mathfrak{p}}}\Big)\mathcal{O}_{\mathfrak{q}} = \mathfrak{q}^{\nu_{\mathfrak{q}}}\mathcal{O}_{\mathfrak{q}} = \mathfrak{m}_{\mathfrak{q}}^{\nu_{\mathfrak{q}}} \quad ,$$

also nach Definition von $v_{\mathfrak{q}}$ gilt $v_{\mathfrak{q}}(x) = \nu_{\mathfrak{q}}$. $v_{\mathfrak{p}}$ heißt Exponential–Bewertung von K bezüglich $\mathfrak{p}$.

Beispiele 15.9.
Sei $\mathcal{O} = \mathbb{Z}$, also $K = \mathbb{Q}$ und $\mathfrak{p} = (p) = p\mathbb{Z}$ für p prim. Dann ist die Lokalisierung nach p der Ring

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} |\, a, b \in \mathbb{Z}, p \nmid b\} \quad .$$

Sein einziges maximales Ideal ist

$$p\mathbb{Z}_{(p)} = \Big\{\frac{a}{b} |\, a, b \in \mathbb{Z}, p \nmid b, \ \textit{aber } p|a\Big\} \quad ,$$

seine Einheiten sind

$$\mathbb{Z}_{(p)}^{\times} = \Big\{ \frac{a}{b} |\, a, b \in \mathbb{Z}, p \nmid b \text{ und } p \nmid a \Big\} \quad .$$

Die zu $\mathbb{Z}_{(p)}$ gehörige Bewertung

$$v_p : \quad \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

$$\frac{a}{b} \mapsto v_p\Big(\frac{a}{b}\Big) = \begin{cases} 0 & \text{für } \frac{a}{b} = 0 \\ n - m & \text{für } a = p^n u \\ & \quad b = p^m v \\ & \text{mit } (u,p) = (v,p) = 1 \end{cases}$$

heißt p–adische Bewertung von $\mathbb{Q}$. $v_p(x-y)$ liefert eine Metrik auf $\mathbb{Q}$. Die Vervollständigung von $\mathbb{Q}$ bezüglich dieser Metrik heißt p–adische Zahlen.

Sei X eine Menge von Primidealen ungleich Null eines Dedekindrings $\mathcal{O}$ und

$$\mathcal{O}_X = \Big\{ \frac{f}{g} |\, f, g \in \mathcal{O},\ g \neq 0 \bmod g \text{ für alle } \mathfrak{p} \in X \Big\}$$

Nach Satz 15.6 ist dies ein Dedekindring, den wir beschreiben wollen. Nach Satz 15.1 sind seine Primideale $\mathfrak{p}_X := \mathfrak{p}\mathcal{O}_X$ mit $\mathfrak{p} \in X$. Für die Lokalisierung gilt

$$\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_X)_{\mathfrak{p}_X} \quad .$$

Denn

$$\mathcal{O}_{\mathfrak{p}} = \Big\{ \frac{a}{b} |\, a \in \mathcal{O}, b \notin \mathfrak{p}_X \Big\} = \Big\{ \frac{a}{1} / \frac{b}{1}, \frac{a}{1} \in \mathcal{O}_X, b \notin \mathfrak{p}_X \Big\} \subseteq (\mathcal{O}_X)_{\mathfrak{p}_X}$$

und

$$(\mathcal{O}_X)_{\mathfrak{p}_X} = \Big\{ \frac{a \cdot d}{b \cdot c} |\, a \in \mathcal{O}, b \notin X, c \notin \mathfrak{p} \Big\} \subseteq \mathcal{O}_{\mathfrak{p}} \quad .$$

Seien $Cl(\mathcal{O})$ und $Cl(\mathcal{O}_X)$ die Idealklassengruppen $\mathcal{O}$ bzw. von $\mathcal{O}_X$.

Satz 15.10.
Wir haben eine kanonische exakte Sequenz

$$1 \hookrightarrow \mathcal{O}^{\times} \underset{\varphi_1}{\longrightarrow} \mathcal{O}_X^{\times} \underset{\varphi_2}{\longrightarrow} \bigoplus_{\mathfrak{p} \notin X} K^{\times}/\mathcal{O}_{\mathfrak{p}}^{\times} \underset{\varphi_3}{\longrightarrow} Cl(\mathcal{O}) \underset{\varphi_4}{\longrightarrow} Cl(\mathcal{O}_X) \to 1 \,,$$

und es ist $K^{\times}/\mathcal{O}_{\mathfrak{p}}^{\times} \cong \mathbb{Z}$. Insbesondere ist $Cl(\mathcal{O}_X)$ als Quotient der endlichen Gruppe $Cl(\mathcal{O})$ endlich.

Beweis.

- φ_1 ist die Inklusion und daher injektiv. φ_2 wird iduziert durch

$$\mathcal{O}_X^{\times} \underset{Inklusion}{\hookrightarrow} K^{\times} \twoheadrightarrow K^{\times}/\mathcal{O}_{\mathfrak{p}}^{\times}$$

Sei $a \in \mathcal{O}_X^{\times}$ im Kern von φ_2. Dann ist $a \in \mathcal{O}_{\mathfrak{p}}^{\times}$ für alle $\mathfrak{p} \notin X$. Aber für $\mathfrak{p} \in X$ gilt $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_{\times})_{\mathfrak{p}_X}$, also ganz sicher auch $a \in \mathcal{O}_{\mathfrak{p}}^{\times}$. Also

$$a \in \cap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^{\times} = \mathcal{O}^{\times}$$

nach dem Beweis von Satz 15.7. Also $\ker \varphi_2 \subseteq \mathrm{im}\varphi_1$. Die andere Inklusion ist klar.

- φ_3 wird induziert durch

$$\varphi_3 : \bigoplus_{\mathfrak{p}\notin X} K^\times/\mathcal{O}_\mathfrak{p}^\times \to \{\mathfrak{a}\in J_K |\ \mathfrak{a} \text{ prim zu allen } \mathfrak{p}\in X\}$$
$$(\alpha_\mathfrak{p} \bmod \mathcal{O}_\mathfrak{p}^\times)_p \mapsto \prod_{\mathfrak{p}\notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} \quad ,$$

wobei $v_\mathfrak{p} : K^\times \to \mathbb{Z}$ die zu $\mathcal{O}_\mathfrak{p}$ gehörige Exponentialbewertung von $K^\times$ ist. Sei $(\alpha_\mathfrak{p} \bmod \mathcal{O}_\mathfrak{p}^\times)_\mathfrak{p}$ ein Element im Kern von φ_3, also

$$\prod_{\mathfrak{p}\notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} = (\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\alpha)} \quad ,$$

wobei wir das gebrochene Hauptideal (α) mit $\alpha\in K^\times$ in Primideale zerlegt haben. Wegen der eindeutigen Primzerlegung folgt

$$\begin{aligned} v_\mathfrak{p}(\alpha) &= 0 \qquad \text{für alle } \mathfrak{p}\in X \\ v_\mathfrak{p}(\alpha) &= v_\mathfrak{p}(\alpha_\mathfrak{p}) \qquad \forall \mathfrak{p}\notin X \ . \end{aligned}$$

Damit ist

$$\alpha \in \cap_{\mathfrak{p}\in X}\mathcal{O}_\mathfrak{p}^\times = \mathcal{O}_X^\times \quad ,$$

da

$$\mathcal{O}_X^\times = \cap_{\mathfrak{p}_X}(\mathcal{O}_X)_{\mathfrak{p}_X}^\times = \cap_{\mathfrak{p}\in X}\mathcal{O}_\mathfrak{p}^\times \quad ,$$

sowie

$$\alpha = \alpha_\mathfrak{p} \bmod \mathcal{O}_\mathfrak{p}^\times \quad .$$

Daher ist

$$\varphi_2(\alpha) = (\alpha \bmod \mathcal{O}_\mathfrak{p}^\times)_{\mathfrak{p}\notin X} = (\alpha_\mathfrak{p} \bmod \mathcal{O}_\mathfrak{p}^\times)_{\mathfrak{p}\notin X} \quad .$$

Also $\ker\varphi_3 \subseteq \mathrm{im}\varphi_2$.
Für die umgekehrte Inklusion zeigen wir: sei $\alpha\in\mathcal{O}_X^\times$,

$$\begin{aligned} \varphi_3\varphi_2(\alpha) = \varphi_3(\alpha \bmod \mathcal{O}_\mathfrak{p}^\times) &= [\prod_{\mathfrak{p}\notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha)}] \\ = [\prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\alpha)}] \qquad &\text{da } \alpha\in\mathcal{O}_X^\times \\ = [(\alpha)] = 0 \quad . \end{aligned}$$

- Schließlich ist

$$\begin{aligned} \varphi_4 : \quad Cl(\mathcal{O}) &\to Cl(\mathcal{O}_\times) \\ [\mathfrak{a}] &\mapsto [\mathfrak{a}\mathcal{O}_X] \quad . \end{aligned}$$

Insbesondere für $\mathfrak{p}\in X$ gilt

$$[\mathfrak{p}] \mapsto [\mathfrak{p}\mathcal{O}_X] \quad ,$$

wobei $\mathfrak{p}\mathcal{O}_X$ Primideal in $\mathcal{O}_X$ ist. Da $Cl(\mathcal{O}_X)$ durch die Klassen der Primideale erzeugt wird und alle Primideale von $\mathcal{O}_X$ von der Form $\mathfrak{p}\mathcal{O}_X$ mit $\mathfrak{p}\in X$ sind nach Satz 15.1, ist φ_4 surjektiv. Wegen $\mathfrak{p}\mathcal{O}_X = \mathcal{O}_X$ für alle $\mathfrak{p}\notin X$ gilt

$$\ker\varphi_4 = \left\{[\prod_{\mathfrak{p}\notin X} \mathfrak{p}^{\nu_p}]\right\} = \mathrm{im}\varphi_3 \quad .$$

- Schließlich gilt:

$$1 \to \mathcal{O}_\mathfrak{p}^\times \to K^\times \underset{v_\mathfrak{p}}{\to} \mathbb{Z} \to 1$$
$$a \mapsto v_\mathfrak{p}(a)$$

ist exakt, also

$$K^\times/\mathcal{O}_\mathfrak{p}^\times \cong \mathbb{Z}$$

□

Sei $\mathcal{O}_K$ der Ring der ganzen Zahlen eines Zahlkörpers K, S eine endliche Menge von Primidealen in $\mathcal{O}_K$.

Definition 15.11
Setze $\mathcal{O}_K^S := \mathcal{O}_K(S)$. $K^S := (\mathcal{O}_K^S)^\times$ heißt S–Einheitengruppe von K, $Cl_K^S := Cl(\mathcal{O}_K^S)$ heißt S–Idealklassengruppe von K.

Korollar 15.12.

(i) Cl_K^S ist als Quotient von $Cl(\mathcal{O}_K)$ modulo aller Klassen von Primidealen $\mathfrak{p} \in S$ endlich.

(ii) $K^S \cong \mu(K) \times \mathbb{Z}^{|S|+r+s-1}$

Beweis.

(ii) Für die Torsionsuntergruppe gilt

$$Tor\,(K^S) = \mu(K) = Tor\,(\mathcal{O}_K^\times) \quad .$$

Ferner haben wir die exakte Sequenz abelscher Gruppen

$$1 \to \mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1} \to K \to \bigoplus_{\mathfrak{p}\in S} K^\times/\mathcal{O}_\mathfrak{p}^\times \to Cl_K \to Cl_K^S \to 0$$

Der Rang der letzten beiden Gruppen ist wegen (i) Null. Also

$$rank\, K^S = rank\, \mathcal{O}_K^\times + rank \bigoplus_{\mathfrak{p}\in S} K^\times/\mathcal{O}_K^\times = r + s - 1 + |S|.$$

□

16 Eindimensionale Schemata

Betrachtung 16.1.
Zur Motivation der kommenden Begriffbildungen dient die folgende Betrachtung. Sei $f(x) \in \mathbb{C}[X]$. Man kann f als Funktion auf der komplexen Zahlenebene $\mathbb{C}$ sehen. Wir wollen die komplexe Zahlenebene algebraisch aus dem Ring $\mathbb{C}[X]$ gewinnen. Für $a \in \mathbb{C}$ ist

$$\Big\{ g(X) \in \mathbb{C}[X] |\, g(a) = 0 \Big\}$$

ein maximales Ideal $\mathfrak{p}_a = (x-a)$ *in* $\mathbb{C}[X]$. *Denn* $\mathfrak{p}_a$ *ist Kern des Einsetzungshomomorphismus*

$$\begin{array}{ccc} \mathbb{C}[X] & \to & \mathbb{C} \\ X & \mapsto & a \end{array}$$

und daher ist $\mathbb{C}[X]/\mathfrak{p}_a \cong \mathbb{C}$ *ein Körper. Mittels* $a \mapsto \mathfrak{p}_a = (x-a)$ *identifizieren wir* $\mathbb{C}$ *mit der Menge* $\operatorname{Max}(\mathbb{C}[X])$ *der maximalen Ideale von* $\mathbb{C}[X]$. *Wir sehen* $f \in \mathbb{C}[X]$ *als Funktion auf diesem Raum:*

$$f(\mathfrak{p}) := f(X) \bmod \mathfrak{p} \in \kappa(\mathfrak{p}) := \mathbb{C}[X]/\mathfrak{p} \quad .$$

f *nimmt seinen Wert ein Punkt* $\mathfrak{p}$ *also im Restklassenkörper* $\kappa(\mathfrak{p})$ *an.*

Die übliche Topologie von $\mathbb{C}$ *lässt sich algebraisch allerdings nicht beschreiben, sondern nur durch Gleichungen* $f(X)$ *definierte Punktmengen; also hier nur die endlichen Mengen und der ganze Raum. Wir erklären als abgeschlossen für jedes gegebene* $f \in \mathbb{C}[X]$

$$\begin{aligned} V(f) &= \left\{ \mathfrak{p} \in \operatorname{Max} \mathbb{C}[X] |\, f(\mathfrak{p}) = 0 \right\} \\ &= \left\{ \mathfrak{p} \in \operatorname{Max} \mathbb{C}[X] |\, \mathfrak{p} \supseteq (f) \right\} \\ &\subseteq \operatorname{Max} \mathbb{C}[X] \quad . \end{aligned}$$

Allgemeiner betrachten wir:

Definition 16.2
Sei $\mathcal{O}$ *ein beliebiger (kommutativer) Ring (mit Eins). Die Menge*

$$X := \operatorname{Spec}(\mathcal{O}) = \left\{ \mathfrak{p} \subseteq \mathcal{O},\ \mathfrak{p} \ \textit{Primideal} \right\}$$

heißt Spektrum *von* $\mathcal{O}$. X *wird mit der* Zariski–Topologie *versehen: für jedes Ideal* $\mathfrak{a} \subseteq \mathcal{O}$ *setzen wir*

$$V(\mathfrak{a}) := \left\{ \mathfrak{p} \in \operatorname{Spec} \mathcal{O} |\, \mathfrak{p} \supseteq \mathfrak{a} \right\} \quad .$$

Diese Mengen sind per definitionem abgeschlossen. Wegen des folgenden Lemmas bilden sie eine Topologie.

Lemma 16.3.
Es gilt

(i) $V(\mathcal{O}) = \emptyset \qquad V(0) = X$

(ii) $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$ *für Ideale* $\mathfrak{a}, \mathfrak{b}$ *in* $\mathcal{O}$.

(iii) $\cap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i)$ *für jede Familie von Idealen in* $\mathcal{O}$.

Beweis.

(i) und (ii) sind klar.

(iii) Aus $\mathfrak{p} \supseteq \mathfrak{a}$ oder $\mathfrak{p} \supseteq \mathfrak{b}$ folgt $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$, also

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b}) \quad .$$

Gilt $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ und $\mathfrak{p} \not\supseteq \mathfrak{b}$, gibt es $b \in \mathfrak{b} \setminus \mathfrak{p}$. Für alle $a \in \mathfrak{a}$ liegt $ab \in \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, folgt $a \in \mathfrak{p}$ für alle $a \in \mathfrak{a}$, somit $\mathfrak{a} \subseteq \mathfrak{p}$, also $\mathfrak{p} \in V(\mathfrak{a})$.

(iv) $\sum \mathfrak{a}_i \subseteq \mathfrak{p} \Leftrightarrow \mathfrak{a}_i \subseteq \mathfrak{p}$ für alle i, da $\sum \mathfrak{a}_i$ das kleinste Ideal ist, das alle $\mathfrak{a}_i$ umfasst.

□

Bemerkungen 16.4.

(i) X mit der Zariski–Topologie ist im allgemeinen nicht hausdorffsch.

(ii) Die abgeschlossenen Punkte von X entsprechen genau den maximalen Idealen von $\mathcal{O}$. Denn ist $\mathfrak{p}$ maximal, so ist $V(\mathfrak{p}) = \{\mathfrak{p}\}$, also $\mathfrak{p}$ abgeschlossen. Ist umgekehrt $\mathfrak{p} \in X$ abgeschlossen, so gilt $\{\mathfrak{p}\} = V(\mathfrak{a})$ für ein Ideal $\mathfrak{a}$, also $\mathfrak{p} \supseteq \mathfrak{a}$ und $\mathfrak{q} \supseteq \mathfrak{a}$, $\mathfrak{q}$ prim impliziert $\mathfrak{q} = \mathfrak{p}$. Also ist $\mathfrak{p}$ sogar ein maximales Ideal.

(iii) Die Elemente $f \in \mathcal{O}$ spielen die Rolle von Funktionen auf dem topologischen Raum X. Der "Wert"von f im Punkt $\mathfrak{p}$ wird durch

$$f(\mathfrak{p}) = f \mod \mathfrak{p}$$

definiert und ist ein Element von

$$\mathcal{O}/\mathfrak{p} \subseteq \mathrm{Quot}(\mathcal{O}/\mathfrak{p}) =: \kappa(\mathfrak{p})$$

Diese Werte liegen im allgemeinen in verschiedenen Körpern.

(iv) Die Zulassung nicht–maximaler Ideale als nicht–abgeschlossene Punkte ist sehr wichtig. Als Beispiel betrachten wir den Polynomring $\mathbb{C}[X]$. Das Primideal $\mathfrak{p} = (0) \in \operatorname{Spec} \mathbb{C}[X]$ ist nicht abgeschlossen. Sein Restklassenkörper $\kappa(\mathfrak{p}) = \mathbb{C}(X) = \mathrm{Quot}\mathbb{C}[X]$ ist der rationale Funktionenkörper. Der Wert von $f \in \mathbb{C}[X]$ in $\mathfrak{p}$ ist $f(X)$ selbst, aufgefasst als Element das rationalen Funktionenkörpers $\mathbb{C}(X)$, d.h. an der Unbestimmten X. Es gilt

$$\overline{\{(0)\}} = \bigcap_{V(\mathfrak{a}) \supseteq V(0)} V(\mathfrak{a}) = \bigcap_{\mathfrak{a} \subseteq (0)} V(\mathfrak{a}) = V((0)) = \operatorname{Spec} \mathbb{C}[X]\,.$$

Daher heißt $\mathfrak{p} = (0)$ auch <u>generischer Punkt</u> von $\operatorname{Spec} \mathbb{C}[X]$. Er liegt überall und nirgends.

Beispiele 16.5.
$X = \operatorname{Spec} \mathbb{Z}$: Man hat für jede Primzahl einen abgeschlossenen Punkt und den generischen Punkt (0) mit Abschluss X. Die nicht–leeren offenen Mengen sind $X \setminus \{p_1, \ldots, p_n\}$ mit endlich vielen Primzahlen. Die ganzen Zahlen $a \in \mathbb{Z}$ werden als Funktion auf X aufgefasst:

$$a(p) = a \mod p \in \mathbb{Z}/p\mathbb{Z} \quad .$$

Die Wertekörper sind also $\mathbb{Z}_2, \mathbb{Z}_3, \ldots$, an den Primzahlen und $\mathbb{Q}$ am generischen Punkt; jeder Primkörper tritt genau einmal auf.

Betrachtung 16.6.
Zur geometrischen Interpretation der Ringelemente von $\mathcal{O}$ als Funktionen auf $X = \operatorname{Spec} \mathcal{O}$ reicht die topologische Struktur von X nicht aus. Wir brauchen die <u>Strukturgarbe</u> auf X.
Sei $\mathcal{O}$ ein Dedekindring, $U \subseteq X := \operatorname{Spec} \mathcal{O}$ nicht–leer und offen. Dann ist der Ring der regulären Funktionen auf U gegeben durch

$$\mathcal{O}(U) = \left\{ \frac{f}{g} \,\middle|\, f, g \in \mathcal{O},\ g(\mathfrak{p}) = g \bmod \mathfrak{p} \neq 0 \text{ für alle } \mathfrak{p} \in U \right\} = S^{-1}\mathcal{O}$$

mit

$$S = \mathcal{O} \setminus \bigcup_{\mathfrak{p} \in U} \mathfrak{p} \quad .$$

Definition 16.7
Sei $\mathcal{O}$ ein Ring, $X = \operatorname{Spec}\mathcal{O}$, $U \subseteq X$ offen und nicht leer.

(i) Wir sagen, eine Abbildung

$$s: \quad U \longrightarrow \prod_{\mathfrak{p}\in U} \mathcal{O}_{\mathfrak{p}}$$

mit $s(\mathfrak{p}) \in \mathcal{O}_{\mathfrak{p}}$ für alle $\mathfrak{p} \in U$ sei lokal Quotient zweier Funktionen aus $\mathcal{O}$, wenn es für jedes $\mathfrak{p} \in U$ eine Umgebung $V \subseteq U$ mit $\mathfrak{p} \in V$ gibt, und Elemente $f, g \in \mathcal{O}$, so dass für alle $\mathfrak{q} \in V$ gilt

$$g(\mathfrak{q}) \neq 0 \quad \textit{und} \quad s(\mathfrak{q}) = \frac{f}{g} \in \mathcal{O}_{\mathfrak{q}} \quad .$$

(ii) Wir betrachten in der Folge die Zuordnung $U \mapsto \mathcal{O}(U)$, wobei $\mathcal{O}(U)$ die lokalen Quotienten auf U sind. Ist $\mathcal{O}$ ein Dedekindring – allgemeiner ein integrer Ring, in dem jedes Primideal ungleich (0) maximal ist–so stimmt dies mit der Definition in Betrachtung 16.6 überein.

(iii) Für $V \subseteq U$ offen in X und nicht leer induziert die kanonische Abbildung

$$\prod_{\mathfrak{p}\in U} \mathcal{O}_{\mathfrak{p}} \longrightarrow \prod_{\mathfrak{p}\in V} \mathcal{O}_{\mathfrak{p}}$$

einen Homomorphismus von Ringen

$$\rho_{UV}: \quad \mathcal{O}(U) \longrightarrow \mathcal{O}(V) \quad ,$$

die Restriktion von U nach V. Das System $\{\mathcal{O}(U), \rho_{UV}\}$ ist eine Garbe auf X, die Strukturgarbe $\mathcal{O}_X$.

Definition 16.8

(i) Eine Kategorie $\mathcal{C}$ besteht aus einer Klasse $Obj(\mathcal{C})$ von Objekten von $\mathcal{C}$ und einer Menge $Mor(A, B)$ von Morphismen zwischen Objekten A, B der Kategorie. Zu $A, B, C \in Obj(\mathcal{C})$ gibt es eine Komposition

$$\begin{aligned} Mor(B, C) \times Mor(A, B) &\to Mor(A, C) \\ (g, f) &\mapsto g \circ f \end{aligned}$$

Es gilt

1) $Mor(A, B) \cap Mor(A', B') = \emptyset$ außer wenn $A = A'$ und $B = B'$ gilt.

2) Für alle Objekte $A \in Obj(\mathcal{C})$ gibt es $\mathrm{id}_A \in Mor(A, A)$ mit

$$\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A \qquad \textit{füe alle } f \in Mor(A, B)$$

3) Die Komposition ist assoziativ.

(ii) Seien $\mathcal{C}$ und $\mathcal{C}'$ Kategorien. Ein kovarianter (kontravarianter) Funktor $F: \mathcal{C} \to \mathcal{C}'$ ordnet jedem Objekt $A \in Obj(\mathcal{C})$ ein Objekt $F(A) \in Obj(\mathcal{C}')$ zu und jedem Morphismus $f \in Mor(A, B)$ einen Morphismus $F(f) \in Mor(F(A), F(B))$ (bzw. $F(f) \in Mor(F(B), F(A))$, so dass gilt

1) $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ für alle $A \in Obj(\mathcal{C})$

2) $F(g \circ f) = F(g) \circ F(f)$ *(bzw.* $F(g \circ f) = F(f) \circ F(g)$*).*

Definition 16.9

(i) Sei X ein topologischer Raum. Dann ist X eine Kategorie zugeordnet, die wir ebenfalls mit X bezeichnen:

$$Obj(X) = \{U \subseteq X, U \text{ offen}\}$$
$$Mor(U,V) = \begin{cases} \text{Inklusion}, & \text{falls } U \subseteq V \\ \emptyset & \text{sonst.} \end{cases}$$

(ii) Eine Prägarbe auf X von (abelschen) Gruppen, Ringen ... ist ein kontravarianter Funktor F der Kategorie X in die Kategorie $\mathfrak{Ab}$ der abelschen Gruppen, $\mathfrak{G}$ der Gruppen, $\mathfrak{R}$ der Ringe ...

$$\begin{aligned} F: \quad & X \longrightarrow \mathfrak{Ab} \\ & U \mapsto F(U) \end{aligned}$$

Sei $U \subseteq V$ offen in X, so setzen wir

$$F(\text{Inklusion } U \to V) =: \rho_{UV}: \quad F(V) \longrightarrow F(U) \quad .$$

Aus den Axiomen 16 (ii) für einen Funktor folgt sofort:

$$\rho_{UU} = \mathrm{id}_{F(U)} \qquad \rho_{UW} = \rho_{VW} \circ \rho_{UV} \quad \text{für} \quad W \subseteq V \subseteq U \text{ offen in } X \ .$$

(iii) Die Elemente $s \in F(U)$ heißen Schnitte von F über U. Ist $V \subseteq U$, so schreibt man $\rho_{UV}(s) = s_{|V}$.

(iv) Eine Prägarbe F auf dem topologischen Raum X heißt Garbe, wenn für jede offene Überdeckung $\{U_i\}_{i \in I}$ einer offenen Menge U gilt

$$0 \to F(U) \to \prod_{i \in I} F(U_i) \rightrightarrows \prod_{i,j} F(U_i \cap U_j)$$

ist exakt. Das heißt:

(a) Sind $s, s' \in F(U)$ zwei Schnitte mit $s|_{U_i} = s'|_{U_i}$ für alle $i \in I$, so ist $s = s'$.

(b) Sei $s_i \in F(U_i)$ eine Familie von Schnitten mit

$$s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$$

für alle $i, j \in I$, so existiert ein $s \in F(U)$ mit $s_i|_{U_i} = s_i$.

(v) Sei $\{M_i\}_{i \in I}$ eine Familie von abelschen Gruppen, wobei I eine filtrierende Indexmenge ist, was heißt, dass I halbgeordnet ist durch $i \subseteq j$ und es zu $i, j \in I$ gibt ein $k \in I$ gibt mit $i \leq k$ und $j \leq k$. Ferner seien für $i \leq j$ Homomorphismen

$$\varphi_{ij}: \quad M_i \to M_j$$

gegeben mit

$$\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$$

für alle $i \leq j \leq k$.

Dann heißt

$$\varinjlim M_i = \dot{\bigcup_{i \in I}} M_i / \sim \quad ,$$

mit $x \in M_i$ und $y \in M_j$ äquivalent, falls es $k \geq i, j$ und und $x_k \in M_k$ gibt mit $\varphi_{ik}(X_k) = X_i$, $\varphi_{jk}(X_k) = X_j$, direkter Limes des direkten Systems $\{M_j, \varphi_{ij}\}$.

(vi) Der Halm einer Garbe F in $x \in X$ ist der direkter Limes

$$F_x = \varinjlim_{\substack{x \in U \subseteq X \, offen \\ \rho_{UV}}} F(U) \quad .$$

Ein Element aus F_x heißt Keim von F in x. Es wird präsentiert durch $s_U \in F(U)$ mit Identifikationen: $s_U \in F(U) \sim s_V \in F(V)$, wenn es $W \subseteq U \cap V$ gibt mit

$$(s_U)_{|W} = (s_V)_{|W} \quad .$$

Satz 16.10.
Sei $\mathcal{O}$ ein Ring und $X = \operatorname{Spec} \mathcal{O}$ versehen mit der Zariski-Topologie. Der Funktor

$$U \mapsto \mathcal{O}(U)$$

ist eine Ringgarbe auf X und wird mit $\mathcal{O}_X$ bezeichnet. Sie heißt Strukturgarbe von X. Der Halm von $\mathcal{O}_X$ im Punkt $\mathfrak{p} \in X$ ist

$$\mathcal{O}_{X,\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \quad .$$

Beweis.
Folgt unmittelbar aus den Definitionen. □

Definition 16.11
Das Paar $(\mathcal{O}_x, X)$ heißt affines Schema. Sei

$$\varphi : \quad \mathcal{O} \to \mathcal{O}'$$

ein Ringhomomorphismus und $X = \operatorname{Spec} \mathcal{O}$, $X' = \operatorname{Spec} \mathcal{O}'$. Dann induziert φ eine stetige Abbildung

$$\begin{aligned} f : \quad & X' \longrightarrow X \\ & \mathfrak{p}' \mapsto f(\mathfrak{p}') := \varphi^{-1}(\mathfrak{p}') \end{aligned}$$

und für jede offene Teilmenge U von X einen Ringhomomorphismus

$$\begin{aligned} f_U^* : \quad & \mathcal{O}_X(U) \longrightarrow \mathcal{O}_{X'}(f^{-1}(U)) \\ & s \mapsto s \circ f|_{f^{-1}(U)} \end{aligned}$$

Es gilt für $V \subseteq U$ offen in X und $U' := f^{-1}(U)$

$$\begin{array}{ccc} \mathcal{O}_X(U) & \xrightarrow{f_U^*} & \mathcal{O}_{X'}(U') \\ \downarrow{\scriptstyle \rho \circ V} & & \downarrow{\scriptstyle \rho_{U',V}} \\ \mathcal{O}_X(V) & \xrightarrow{f_V^*} & \mathcal{O}_{X'}(V') \end{array}$$

Somit induziert φ einen Garbenmorphismus

$$f^* : \quad \mathcal{O}_X \longrightarrow f_* \mathcal{O}_{X'}$$

(f, f^*) heißt Morphismus des affinen Schemas X' nach X. Sie entsprechen Morphismen der zu Grunde liegenden Ringe.

Beispiele 16.12.
Sei $\mathcal{O}$ ein noetherscher integrer Ring, in dem jedes Primideal ungleich (0) maximal ist.

(a) *Körper.*
Ist K ein Körper, so besteht $\operatorname{Spec} K$ aus einem einzigen Punkt (0), auf dem der Körper als Strukturgarbe sitzt. Ist $\bar{K}$ der algebraische Abschluss, dann induziert $K \hookrightarrow \bar{K}$ einen Schemamorphismus

$$\operatorname{Spec}(\bar{K}) \to \operatorname{Spec}(K) \quad .$$

Jedem Schema kann man eine Fundamentalgruppe zuordnen. Hier zeigt sich $\pi_1(\operatorname{Spec} \bar{K}) = 1$ und $\pi_1(\operatorname{Spec} K) = Gal(\bar{K}/K)$.

(b) *Bewertungsringe*
Sei $\mathcal{O}$ ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{p}$. $X = \operatorname{Spec} \mathcal{O}$ besteht aus zwei Punkten:

- *dem abgeschlossenen Punkt $x = \mathfrak{p}$ mit Restklassenkörper $\kappa(\mathfrak{p}) = \mathcal{O}/\mathfrak{p}$*
- *dem generischen Punkt $\eta = (0)$ mit Restklassenkörper*

$$\kappa(\eta) = K = \operatorname{Quot}(\mathcal{O})$$

Geometrische Vorstellung: X ist ein Punkt mit infinitesimaler Umgebung, die von generischen Punkt durchlaufen wird. Dazu die folgende Überlegung: Sei $\mathcal{O}$ ein Dedekindring und $\mathcal{O}_\mathfrak{p} = \left\{ \frac{f}{g} | f, g \in \mathcal{O}, g(\mathfrak{p}) \neq 0 \right\}$ die Lokalisierung in $\mathfrak{p}$. Es gibt keine Umgebung von $\mathfrak{p}$ in $\operatorname{Spec} \mathcal{O}$, auf der alle Funktionen $\frac{f}{g} \in \mathcal{O}_\mathfrak{p}$ definiert sind. Denn zu jedem Punkt $\mathfrak{q} \neq \mathfrak{p}$, $\mathfrak{q} \neq (0)$ gibt es nach dem chinesischen Restsatz ein $g \in \mathcal{O}$ mit

$$g = 0 \mod \mathfrak{q} \qquad \text{und} \qquad g = 1 \mod \mathfrak{p} \quad ,$$

so dass $\frac{1}{g} \in \mathcal{O}_\mathfrak{p}$ als Funktion nicht in $\mathfrak{q}$ definiert ist. Jedes Element ist aber in einer hinreichend kleinen Umgebung definiert, so dass alle $\frac{f}{g} \in \mathcal{O}_\mathfrak{p}$ auf einen "Umgebungskeim" von $\mathfrak{p}$ als Funktion leben. $\operatorname{Spec} \mathcal{O}_\mathfrak{p}$ darf man sich als solchen Umgebungskeim vorstellen.

(c) *Dedekindringe.*
Sei $X = \operatorname{Spec} \mathcal{O}$ mit $\mathcal{O}$ einem Dedekindring. Man stellt sich X als glatte Kurve vor. Die Inklusion $\mathcal{O} \hookrightarrow \mathcal{O}_\mathfrak{p}$ in eine Lokalisierung induziert für jeden Punkt $\mathfrak{p} \in X$ einen Morphismus

$$\varphi_\mathfrak{p} : \quad X_\mathfrak{p} = \operatorname{Spec} \mathcal{O}_\mathfrak{p} \longrightarrow X$$

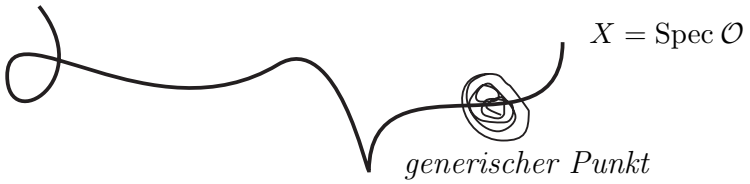
$X_\mathfrak{p}$ ist infinitesimale Umgebung von $\mathfrak{p}$ in X.

generischer Punkt

(d) *Singularitäten.*
Sei $\mathcal{O}$ noethersch, jedes von (0) verschiedene Primideal maximal, aber $\mathcal{O}$ nicht unbedingt ganz abgeschlossen. Beispiel:

- $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$ *mit* $d = 1 \mod 4$
- $\mathcal{O} = \mathbb{C}[X,Y]/(Y^2 - X^3)$

$X = \operatorname{Spec} \mathcal{O}$ ist eine Kurve, die in denjenigen Punkten Singularitäten besitzt, für die $\mathcal{O}_\mathfrak{p}$ kein diskreter Bewertungsring ist: das maximale Ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ wird nämlich nicht mehr durch ein einziges Element erzeugt wird.



Beispiel: $\mathcal{O} = \mathbb{C}[X,Y]/(Y^2 - X^3)$. Wegen der kanonischen Surjektion

$$\mathbb{C}[X,Y] \twoheadrightarrow \mathcal{O}$$

sind die Primideale von $\mathcal{O}$ in Bijektion zu den Primidealen von $\mathbb{C}[X,Y]$, die $(Y^2 - X^3)$ enthalten. Für abgeschlossene Punkte gilt also

$$(X - a, Y - b) \supseteq (Y^2 - X^3) \quad ,$$

es muss also $f, g \in \mathbb{C}[X,Y]$ geben mit

$$Y^2 - X^3 = f(X - a) + g(Y - b) \quad .$$

Setze $Y = b$ und $X = a$. Die abgeschlossene Punkte von $\operatorname{Spec} \mathcal{O}$ sind durch die Primideale

$$\mathfrak{p} = (X - a, Y - b) \mod (Y^2 - X^3)$$

mit $(a,b) \in \mathbb{C}^2$, $b^2 - a^3 = 0$ gegeben. Der einzige singuläre Punkt ist der Nullpunkt, der dem maximalen Ideal $\mathfrak{p}_0 = (\bar{X}, \bar{Y})$ mit $\bar{X} = X \mod (Y^2 - X^3)$ und $\bar{Y} = Y \mod (Y^2 - X^3)$ entspricht. $\mathfrak{p}_0\mathcal{O}_{\mathfrak{p}_0}$ wird von $\bar{X}$ und $\bar{Y}$ erzeugt, kann aber nicht durch ein einziges Element erzeugt werden.
Der Übergang zum ganzen Abschluss $\tilde{\mathcal{O}}$ von $\mathcal{O}$ führt nach dem Satz von Krull–Akizuki zu einem Dedekindring $\tilde{\mathcal{O}}$. Die Inklusion $\mathcal{O} \hookrightarrow \tilde{\mathcal{O}}$ induziert einen Morphismus

$$\operatorname{Spec} \tilde{\mathcal{O}} \to \operatorname{Spec} \mathcal{O} \quad ,$$

der geometrisch die Singularität auflöst.

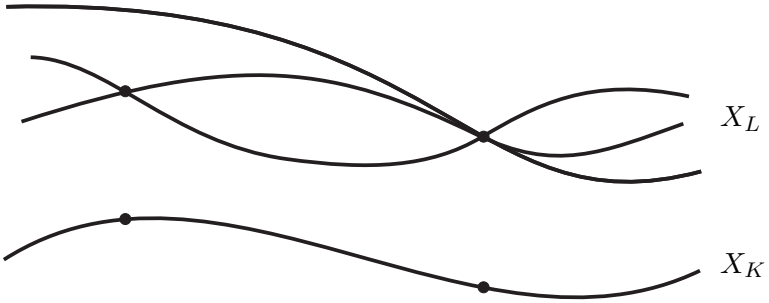
(e) *Erweiterungen.*
Sei $\mathcal{O}_K$ ein Dedekindring, $K = \operatorname{Quot}(\mathcal{O}_K)$, L/K eine endliche separable Erweiterung und $\mathcal{O}_L$ der ganze Abschluss von $\mathcal{O}_K$ in L. Sei $X_K = \operatorname{Spec} \mathcal{O}_K$ und $X_L = \operatorname{Spec} \mathcal{O}_L$, und sei der Schemahomomorphismus

$$f: \quad X_L \to X_K$$

induziert durch die Inklusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$. Sei $\mathfrak{p}$ ein maximales Ideal in $\mathcal{O}_K$ und

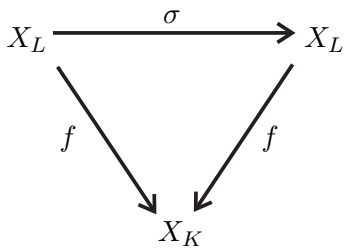
$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \quad .$$

Dann sind $\mathfrak{P}_1 \dots \mathfrak{P}_r$ die Punkte von X_L, die unter f auf $\mathfrak{p}$ abgebildet werden:



Verzweigungspunkte.

Dieses Bild ist nur korrekt, wenn die Restklassenkörper von $\mathcal{O}_K$ algebraisch abgeschlossen sind, z.B. für $\mathcal{O}_K = \mathbb{C}[X]$. Dann liegen wegen $\sum e_i f_i = n = [L : K]$ über jedem nicht verzweigten Punkt von X_K genau n Punkte von X_L. Ist L/K galoisch mit Galoisgruppe G, so induziert jedes $\sigma \in G$ durch $\sigma : \mathcal{O}_L \to \mathcal{O}_L$ einen Automorphismus des Schemas $\sigma : X_L \to X_L$. Da $\mathcal{O}_K$ punktweise fest bleibt, ist das Diagramm



kommutativ. Alle $\sigma \in G$ sind also Decktransformationen der Überlagerung X_L/X_K. Für die Gruppe $Aut_{X_K}(X_L)$ der Decktransformationen gilt

$$G(L/K) \cong Aut_{X_K}(X_L) \quad .$$

Dies ist der Anfang einer tiefen Beziehung zwischen Galoisgruppen und Fundamentalgruppen.

Index