Algebraische Zahlentheorie

Prof. Dr. Holger Brenner
Universität Osnabrück
Fachbereich Mathematik/Informatik

Wintersemester 2020-2021

Inhaltsverzeichnis

Vorwort

Dieses Skript gibt die Vorlesung Algebraische Zahlentheorie wieder, die ich im Wintersemester 2020/2021 im Masterstudiengang Mathematik an der Universität Osnabrück gehalten habe. Wegen Corona wurden die Vorlesungen vor leerem Publikum aufgezeichnet. Inhaltlich stehen die Zahlbereiche im Mittelpunkt, wobei quadratische Zahlbereiche und Kreisteilungsringe die Hauptbeispiele bilden, die immer wieder aufgegriffen werden. Es werden einige wenige Grundbegriffe aus der (kommutativen) Algebra und der Galoistheorie vorausgesetzt, die wichtigsten algebraischen Grundlagen wie Ganzheit, Dedekindbereich, Invariantenringe werden aber entwickelt. Hauptresultate sind die eindeutige Idealzerlegung, die Endlichkeit der Klassenzahl und der Einheitensatz von Dirichlet. Die Analogie zur funktionentheoretischen Situation wird zwar herausgestellt, aber nicht durchgängig in gleicher Konsequenz verfolgt. Zahlbereiche und ihre Spektren werden als endliche Erweiterungen von Spek $Z\mathbb{Z}\mathbb{Z}$ geometrisch realisiert, die relative Situation wird aber etwas vernachlässigt. Verzweigung und Zerlegung wird unter unterschiedlichen Aspekten behandelt.

Bei Frau Marianne Gausmann bedanke ich mich für die Erstellung der Pdf-Files und bei den Studierenden für einzelne Korrekturen und Anregungen.

Holger Brenner

1. Vorlesung - Einführung

Wir besprechen einige typische Situation, die zur algebraischen Zahlentheorie führen.

1.1. **Primfaktorzerlegung in $\mathbb{Z}$ und sonstwo.**

In den ganzen Zahlen $\mathbb{Z}$ gilt die eindeutige Primfaktorzerlegung, d.h. jede ganze Zahl $n \neq 0$ lässt sich als ein (bei einer negativen Zahl braucht man noch das Vorzeichen -1) Produkt von (positiven) Primzahlen schreiben, wobei die Anzahl der auftretenden Primzahlen, die Primfaktoren, eindeutig bestimmt ist. Beispielsweise ist

$$175 = 5 \cdot 5 \cdot 7 = 5 \cdot 7 \cdot 5 = 5^2 \cdot 7.$$

Für eine Primzahl ist diese Faktorzerlegung einfach die Zahl selbst. In einem größeren Ring, beispielsweise einem Körper, ergeben sich neue Darstellungsmöglichkeiten. Es ist in $\mathbb{R}$

$$7 = \frac{7}{5} \cdot 5 = 7 \cdot 5^{-1} \cdot 5 = 7 \cdot \pi^{-1}\pi.$$

Das sind natürlich Uneindeutigkeiten, die sich einfach daraus ergeben, dass es Elemente gibt, die ein Inverses besitzen. Wenn man an $7 = (-1)(-7)$ denkt, gibt es dieses Phänomen schon in $\mathbb{Z}$. Wir halten kurz die folgende Definition fest.

Definition 1.1. Ein Element u in einem kommutativen Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit $uv = 1$ gibt.

In $\mathbb{Z}$ sind nur 1 und -1 Einheiten, der Einfluss auf die Teilbarkeitstheorie ist daher sehr überschaubar. Ein kommutativer Ring ist genau dann ein Körper, wenn in ihm jedes von 0 verschiedene Element eine Einheit ist (der Nullring ist kein Körper, da in ihm sogar die 0 eine Einheit ist). Deshalb gibt es in einem Körper keine aussagekräftige Teilbarkeitstheorie. Ein anderes Phänomen sind die Faktorzerlegungen

$$7 = \sqrt{7} \cdot \sqrt{7} = \sqrt[3]{7} \cdot \sqrt[3]{7} \cdot \sqrt[3]{7} = \sqrt[4]{7} \cdot \sqrt[4]{7} \cdot \sqrt[4]{7} \cdot \sqrt[4]{7}.$$

In diesem Sinne kann man beliebig weitermachen, es gibt dann für die Zahl 7 beliebig lange zunehmend feinere Zerlegungen - aber keine Primfaktorzerlegung.

Betrachten wir genauer die Zerlegung

$$7 = \sqrt{7} \cdot \sqrt{7}.$$

Diese hat nichts mit Einheiten zu tun, sondern allein mit der Existenz der Quadratwurzel (oder in den weiteren Fällen mit der Existenz der dritten oder vierten Wurzel) der 7. Um eine solche Faktorzerlegung hinzuschreiben, braucht man nicht die vollen reellen Zahlen, sondern eben nur diese Wurzeln. Um die erste Gleichung ausdrücken zu können, braucht man nur das neue

Element $\sqrt{7}$ mit der charakteristischen Eigenschaft, dass das Produkt mit sich selbst gleich 7 ist. Doch allein diese Hinzunahme, also die Mengen $\mathbb{N} \cup \{\sqrt{7}\}$ bzw. $\mathbb{Z} \cup \{\pm\sqrt{7}\}$ liefert keine sinnvolle algebraische Struktur, da darin weder die Multiplikation $4 \cdot \sqrt{7}$ noch die Addition $4 + \sqrt{7}$ definiert ist. Da verliert man also viel zu viel. Man möchte „nur“ die Quadratwurzel aus 7 hinzutun, aber gleichzeitig sinnvolle algebraische Strukturen erhalten. Mit $\sqrt{7}$ muss dann auch beispielsweise $13 - 22\sqrt{7}$ drin sein. Zahlen von dieser Form sind offenbar additiv abgeschlossen und sind aber auch multiplikativ abgeschlossen, es gilt ja

$$\left(a + b\sqrt{7}\right)\left(c + d\sqrt{7}\right) \ = \ (ac + 7bd) + (ad + bc)\sqrt{7}$$

für beliebige $a, b, c, d \in \mathbb{Z}$. Diese Zahlen bilden also wieder einen kommutativen Ring, und zwar kann man ihn als Unterring der reellen Zahlen realisieren, weshalb die Assoziativität der Verknüpfungen direkt erfüllt ist. Wir haben also eine Ringerweiterung

$$\mathbb{Z} \ \subseteq \ \mathbb{Z}[\sqrt{7}] \ = \ \mathbb{Z} + \mathbb{Z}\sqrt{7} \ = \ \left\{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\right\} \ =: \ R,$$

wobei die ganzen Zahlen den Summen $a + b\sqrt{7}$ mit $b \ = \ 0$ entsprechen, wobei die Addition in R komponentenweise und die Multiplikation wie in $\mathbb{R}$ bzw. explizit wie oben bzw. distributiv unter Verwendung der einzigen relevanten Regel

$$\sqrt{7} \cdot \sqrt{7} \ = \ 7$$

erklärt ist. Die Darstellung $a + b\sqrt{7}$ eines Elementes aus R ist ferner eindeutig, d.h. $a + b\sqrt{7} \ = \ a' + b'\sqrt{7}$ ist nur bei

$$a \ = \ a'$$

und

$$b \ = \ b'$$

möglich. Anderfalls hätte man eine Gleichung

$$r \ = \ s\sqrt{7}$$

mit $r, s \in \mathbb{Z} \ \ r, s \neq 0$, woraus sich

$$\sqrt{7} \ = \ \frac{r}{s}$$

im Widerspruch zur Irrationalität von Quadratwurzeln auf Primzahlen ergibt, die aus der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ folgt, siehe Aufgabe 1.2. (der Spezialfall, die Irrationalität der Quadratwurzel aus 2, ist ein typisches Beispiel für einen Widerspruchsbeweis aus den Anfängervorlesungen, siehe Satz 4.6 (Mathematik für Anwender (Osnabrück 2020-2021))).

Aufgrund der definierenden Gleichung sieht man direkt, dass 7 in R nicht mehr prim ist, sondern nichttriviale Teiler, nämlich $\sqrt{7}$ besitzt, wobei wir aber die exakten Definitionen noch nicht fixiert haben. Zunächst muss man

sich klar machen, dass 7 (und $\sqrt{7}$) keine Einheit in R wird. Dies kann man aber wegen

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

sofort ausschließen. Was aber keineswegs klar ist, ob es in R weitere Faktorzerlegungen für 7 gibt, ob $\sqrt{7}$ prim ist, ob es neue Einheiten in R gibt, wie sich die Existenz von $\sqrt{7}$ auf die Faktorzerlegung von anderen ganzen Zahlen auswirkt. Um Zerlegungsphänome von der Bauart

$$7 \;=\; u(u^{-1}7)$$

mit einer Einheit u auszuschließen bzw. zu erkennen, müssen wir zuerst wissen, ob in R neue Einheiten dazukommen. Mit dem Argument von eben kann man direkt einsehen, dass ganze Zahlen $\neq 1,-1$ in R Nichteinheiten bleiben. Es gibt aber in der Tat eine Vielzahl von neuen Einheiten! Betrachten wir in R die Gleichung

$$(8+3\sqrt{7})(8-3\sqrt{7}) \;=\; 64-9\cdot 7 \;=\; 1,$$

die ja besagt, dass die beiden Elemente $8+3\sqrt{7}$ und $8-3\sqrt{7}$ zueinander invers sind und damit Einheiten sind. Damit sind auch alle Zahlen der Form $\pm\big(8+3\sqrt{7}\big)^n$ (mit $n\in\mathbb{Z}$) Einheiten, und das sind alle Einheiten von R, siehe die 25. Vorlesung. Die Existenz von Einheiten erschwert die Entscheidung, ob eine Faktorzerlegung auf Einheiten beruht oder auf eine Zerlegung in substantiell grundlegendere Bestandteile. Handelt es sich beispielsweise bei

$$(5+4\sqrt{7})(-5+4\sqrt{7}) \;=\; -25+16\cdot 7 \;=\; -25+112 \;=\; 87 \;=\; 3\cdot 29$$

um zwei wesentlich verschiedene Faktorzerlegungen der 87 in R? Hier haben wir schon zum zweiten Mal die dritte binomische Formel ausgenutzt, um durch eine Multiplikation von zwei Zahlen aus R wieder in $\mathbb{Z}$ zu landen. Wegen

$$3 \;=\; (2+\sqrt{7})(-2+\sqrt{7})$$

kann man aber die 3 weiter zerlegen. Der erste Faktor kommt auch in der Zerlegung

$$5+4\sqrt{7} \;=\; (2+\sqrt{7})(6-\sqrt{7})$$

vor. In der verfeinerten Zerlegung

$$87 \;=\; (2+\sqrt{7})(-2+\sqrt{7})(6-\sqrt{7})(6+\sqrt{7})$$

kommen somit beide obigen Zerlegungen vor, die sich daher als keine Primfaktorzerlegung erweisen. Das ist also wie bei

$$210 \;=\; 6\cdot 35 \;=\; 10\cdot 21 \;=\; 2\cdot 3\cdot 5\cdot 7,$$

allerdings mit dem Unterschied, dass es in R zunächst einmal keine systematische Methode gibt, Zahlen auf die Primeigenschaft zu überprüfen.

Eine wichtige Fragestellung der algebraischen Zahlentheorie ist, wie sich Teilereigenschaften und die Primfaktorzerlegungen von $\mathbb{Z}$ ändern, wenn man

zusätzliche Elemente hinzunimmt. Typischerweise werden dabei die Primfaktorzerlegungen zerstört, es entstehen aber neue Faktorzerlegungen (nicht unbedingt Primfaktorzerlegungen), die selbst wieder zahlentheoretischen Sachverhalte ausdrücken und sichtbar machen.

1.2. **Summe von Quadraten.**

Betrachten wir die Frage, welche natürlichen Zahlen die Summe von zwei Quadratzahlen sind. Anders formuliert, für welche n hat die Gleichung

$$n = x^2 + y^2$$

Lösungen mit ganzen Zahlen x, y? Es ist

$$0 = 0 + 0$$
$$1 = 1 + 0$$
$$2 = 1 + 1$$
$$3$$

$$4 = 4 + 0$$

$$5 = 4 + 1$$
$$6$$

$$7$$

$$8 = 4 + 4$$
$$9 = 9 + 0$$
$$10 = 9 + 1$$
$$11$$

$$12$$

$$13 = 9 + 4$$
$$14$$

$$15$$

$$16 = 16 + 0$$
$$17 = 16 + 1$$
$$18 = 9 + 9$$

19

$$20 = 16 + 4$$

21

Erkennt man hier schon eine Struktur? Es ist in der Zahlentheorie üblich, solche Fragen erst einmal für Primzahlen zu verstehen, und die Ergebnisse dann auf zusammengesetzte Zahlen zu übertragen. Von den Primzahlen ≤ 20 sind $3, 7, 11, 19$ keine Summe von zwei Quadraten, während $2, 5, 13$ und 17 es sind. Es fällt auf, dass die erste Reihe alle den Rest 3 bei Division durch 4 haben, und die zweite Reihe (von 2 abgesehen) den Rest 1. Hier zeigt sich, dass es sinnvoll ist, zu anderen, hier endlichen, Ringen überzugehen, um Fragen über natürliche oder ganze Zahlen zu beantworten. Die Restabbildung zur *Division mit Rest* durch 4 ist ein Ringhomomorphismus

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(4) = \{0, 1, 2, 3\},\ n \longmapsto n \mod 4.$$

Dabei ist in $\mathbb{Z}/(4)$ die Addition und die Multiplikation modulo 4 erklärt, also etwa $3 \cdot 3 = 9 = 1$. Die Abbildung respektiert also die Addition und die Multiplikation. Wenn nun die Gleichung

$$n = x^2 + y^2$$

in $\mathbb{Z}$ eine Lösung besitzt, so liefert das sofort auch eine Lösung modulo 4, nämlich

$$n = x^2 + y^2 \mod 4$$

bzw.

$$(n \mod 4) = (x \mod 4)^2 + (y \mod 4)^2$$

oder

$$\bar{n} = \bar{x}^2 + \bar{y}^2.$$

Nun sind aber in $\mathbb{Z}/(4)$ die Quadrate einfach

$$0^2 = 2^2 = 0$$

und

$$1^2 = 3^2 = 1$$

und damit sind $0, 1$ und 2 Summen von zwei Quadraten in $\mathbb{Z}/(4)$, aber nicht 3. Es bestätigt sich also bereits die obige Beobachtung, dass natürliche Zahlen (nicht nur Primzahlen), die den Rest 3 modulo 4 haben, nicht die Summe von zwei Quadraten sein können.

Für Primzahlen mit dem Rest 1 modulo 4 liefert die Betrachtung im Restklassenring $\mathbb{Z}/(4)$ natürlich nur, dass eine notwendige Bedingung erfüllt ist, woraus sich natürlich noch lange nicht auf eine Darstellung als Summe von zwei Quadraten schließen lässt. Die Zahl 21 zeigt auch, dass eine Zahl, die modulo 4 den Rest 1 besitzt, nicht notwendig selbst die Summe von zwei Quadraten ist.

Eine wichtige Umformulierung der Frage erhält man, wenn man wie oben zu einer quadratischen Erweiterung übergeht, nämlich zum *Ring der Gaußschen Zahlen*

$$\mathbb{Z}[\mathrm{i}] \;=\; \mathbb{Z} \oplus \mathbb{Z}\mathrm{i}$$

(einem Unterring der komplexen Zahlen). Dort können wir

$$n \;=\; x^2 + y^2 \;=\; (x + \mathrm{i}y)(x - \mathrm{i}y)$$

schreiben, wodurch die Frage, ob eine Zahl Summe von zwei Quadraten ist, mit der Frage der multiplikativen Zerlegung von natürlichen Zahlen in diesem neuen Ring in Zusammenhang gebracht wird. Insbesondere ist eine Primzahl, die Summe von zwei Quadraten ist, im Ring der Gaußschen Zahlen nicht mehr prim (die hingeschriebenen Faktoren können keine Einheiten sein).

Die Frage nach den Summen von zwei Quadraten werden wir abschliesend in Satz 9.11 beantworten.

1.3. **Pellsche Gleichung.**

Betrachten wir eine Zahlbereichserweiterung

$$\mathbb{Z} \;=\; \mathbb{Z}[\sqrt{D}] \;=\; \mathbb{Z} \oplus \mathbb{Z}\sqrt{D}$$

mit einer ganzen Zahl D, die beiden Fälle $D = 7$ und $D = -1$ haben wir schon etwas genauer in den Blick genommen (es sei D quadratfrei, enthalte also keinen Primfaktor mehrfach). Auch der Frage, wie in diesen Ringen die Einheiten aussehen, sind wir schon begegnet. Betrachten wir allgemein die Bedingung, ob es zu $a + b\sqrt{D}$ ein Element $c + e\sqrt{D}$ mit

$$\left(a + b\sqrt{D}\right)\left(c + e\sqrt{D}\right) \;=\; 1.$$

Wenn a und b nicht teilerfremd sind, so kann es keine Lösung geben, seien also a und b teilerfremd. Dann folgt aus

$$bc + ae \;=\; 0,$$

dass bis auf einen gemeinsamen Vorfaktor

$$c \;=\; fa$$

und

$$e \;=\; -fb$$

gilt, und der Vorfaktor muss 1 oder -1 sein. Die Frage nach den Einheiten ist also im Wesentlichen die Frage, ob

$$\left(a + b\sqrt{D}\right)\left(a - b\sqrt{D}\right) \;=\; a^2 - b^2 D \;=\; \pm 1.$$

Es geht also darum, welche ganzzahligen Lösungen bei gegebenem D die Gleichung

$$x^2 - y^2 D \;=\; \pm 1$$

besitzt. Man spricht von der *Pellschen Gleichung*, deren Lösungsverhalten wesentlich von D positiv oder negativ abhängt.

1.4. **Diophantische Gleichungen.**

Eine besondere Herausforderung innerhalb der Zahlentheorie sind diophantische Gleichungen.

Definition 1.2. Zu einem Polynom $F \in \mathbb{Z}[x_1, \ldots, x_n]$ heißt

$$F(x_1, \ldots, x_n) = 0$$

eine *diophantische Gleichung*. Unter einer Lösung einer diophantischen Gleichung versteht man ein ganzzahliges Zahlentupel $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, das in F eingesetzt 0 ergibt.

Die Pellsche Gleichung haben wir schon erwähnt, bei linearen diophantischen Gleichungen ist das Lösungsverhalten einfach zu verstehen, die Gleichung

$$x^2 + y^2 = z^2$$

ist die Frage nach *Pythagoreischen Tripeln*, was ebenfalls gut verstanden ist. Eine wesentliche Frage bei diophantischen Gleichungen ist, ob es überhaupt, eventuell abgesehen von trivialen Lösungen, ganzzahlige Lösungen gibt. Ein weiteres wichtiges Problem ist, ob es endlich viele oder unendlich viele ganzzahlige Lösungen gibt. Ein großes zahlentheoretisches Problem, das erst 1995 gelöst wurde, ist das Problem von Fermat, ob die Gleichung

$$x^n + y^n = z^n$$

mit $n \geq 3$ nichttriviale ganzzahlige Lösungen (x, y, z) besitzt, in denen alle Einträge nicht 0 sind.

Satz 1.3. *Die diophantische Gleichung*

$$x^n + y^n = z^n$$

besitzt für kein $n \geq 3$ eine ganzzahlige nichttriviale Lösung.

Beweis. Der Beweis für diese Aussage geht bei Weitem über den Inhalt einer Vorlesung über elementare oder algebraische Zahlentheorie hinaus. □

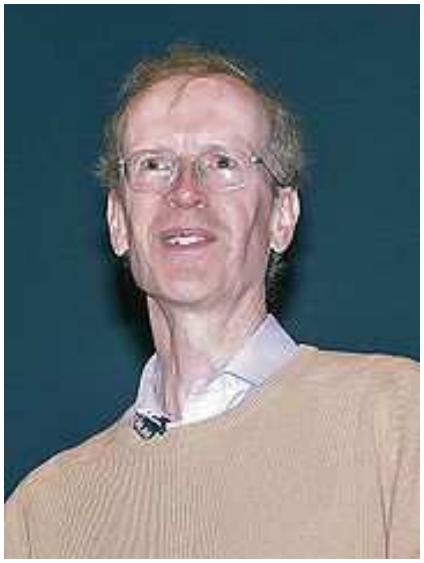
Der Beweis für diesen Satz verwendet die reichhaltige Theorie der elliptischen Kurven. Vor diesem Beweis wurden die besten Resultate zu diesem Problem mit Methoden der algebraischen Zahlentheorie erzielt, und zwar konnten sehr viele Exponenten erledigt werden. Die Grundidee geht folgendermaßen: Die Fermat-Gleichung erhält einen neuartigen Charakter, wenn man sie in dem Ring betrachten, der aus $\mathbb{Z}$ entsteht, wenn man eine n-te Einheitswurzel ζ hinzunimmt. Das ist eine Zahl, deren n-te Potenz 1 ist. Solche Einheitswurzeln gibt es innerhalb der komplexen Zahlen, beispielsweise ist $e^{2\pi \mathrm{i}/n}$ eine primitive n-te Einheitswurzel. Wichtig sind hier aber die algebraischen Eigenschaften. Jedenfalls kann man die etwas umgeschriebene Fermatgleichung

$$x^n - z^n = -y^n$$

unter Verwendung einer primitiven Einheitswurzel als

$$x^n - z^n \;=\; (x-z)(x-\zeta z)\cdots(x-\zeta^{n-1}z) \;=\; -y^n$$

schreiben. Somit hat man zwei ziemlich verschiedene Faktorzerlegungen einer Zahl. Wenn man jetzt noch was weiß, dass in diesem neuen Ring die eindeutige Primfaktorzerlegung gilt, so kann man (das sind dann immer noch mehrere Schritte) daraus einen Widerspruch ableiten. An dieser STelle gibt es eine schlechte und eine gute Nachricht: Diese Ringe besitzen häufig nicht die eindeutige Primfaktorzerlegung, das angedeutete Argument funktioniert aber auch noch dann, wenn man weiß, dass die sogenannte Klassengruppe des Ringes eine gewisse Eigenschaft erfüllt, die deutlich schwächer als die eindeutige Primfaktorzerlegung ist.



Andrew Wiles (*1953)

Für $n = 4$ ist die imaginäre Einheit i eine vierte primitive Einheitswurzel (wegen $\mathrm{i}^4 = 1$), in diesem Fall gilt

$$y^4 - z^4 \;=\; (x-z)(x-\mathrm{i}z)(x+z)(x+\mathrm{i}z) \;=\; -y^4$$

und man kann die Situation im Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ analysieren.

Beispiel 1.4. Als Kuriosität erwähnen wir, dass die von Euler vermutete teilweise Verallgemeinerung des Fermatschen Problems, dass die Gleichungen

$$x^4 + y^4 + z^4 \;=\; u^4,$$
$$x^5 + y^5 + z^5 + u^5 \;=\; v^5,$$

usw. keine ganzzahlige Lösung besitzen, also dass zwischen n n-ten Potenzen keine additive Beziehung bestehen kann, nicht gilt. Die einfachsten Gegenbeispiele sind

$$95800^4 + 217519^4 + 414560^4 \;=\; 422481^4$$

und

$$27^5 + 84^5 + 110^5 + 133^5 \;=\; 144^5.$$

1. Arbeitsblatt

1.1. Übungsaufgaben.

Aufgabe 1.1.* Zeige, dass $\sqrt{2}$ eine irrationale Zahl ist.

Aufgabe 1.2. Es sei p eine Primzahl. Zeige unter Verwendung der eindeutigen Primfaktorzerlegung von natürlichen Zahlen, dass die reelle Zahl $\sqrt{p}$ irrational ist.

Aufgabe 1.3. Zeige

$$\sqrt{10 + \sqrt{24} + \sqrt{40} + \sqrt{60}} \;=\; \sqrt{2} + \sqrt{3} + \sqrt{5}.$$

Aufgabe 1.4. Bestimme die Einheiten von $\mathbb{Z}$ und von $K[X]$, wobei K ein Körper sei.

Aufgabe 1.5. Berechne

$$\left(8 + 3\sqrt{7}\right)^2, \left(8 + 3\sqrt{7}\right)^3, \left(8 + 3\sqrt{7}\right)^4, \ldots .$$

Aufgabe 1.6. Finde die kleinste natürliche Zahl, die sich auf mehrfache Weise als Summe von zwei Quadratzahlen darstellen lässt.

Aufgabe 1.7. Es sei n eine natürliche Zahl, die modulo 8 den Rest 7 besitzt. Zeige, dass n nicht als Summe von drei Quadraten darstellbar ist.

Aufgabe 1.8. Bestimme für jede natürliche Zahl $n \leq 30$, ob sie sich als eine Summe von drei Quadratzahlen darstellen lässt.

Aufgabe 1.9. Bestimme für jede natürliche Zahl $n \leq 10$, auf wie viele verschiedene Arten sie sich als Summe von vier Quadratzahlen darstellen lässt, d.h. man bestimme die Anzahl der 4-Tupel

$$(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \text{ mit } x_1^2 + x_2^2 + x_3^2 + x_4^2 = n.$$

Aufgabe 1.10. Zu einer natürlichen Zahl n bezeichne $r(n)$ die Anzahl der Möglichkeiten, sie als Summe von vier Quadratzahlen darzustellen, d.h. $r(n)$ ist die Anzahl der 4-Tupel

$$(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \text{ mit } x_1^2 + x_2^2 + x_3^2 + x_4^2 = n.$$

Es sei u eine ungerade positive Zahl. Beweise die Beziehung

$$r(2u) = 3r(u)\,.$$

Tipp: Zu einem Tupel (x_1, x_2, x_3, x_4) kann man das Tupel $(x_1 - x_2, x_1 + x_2, x_3 - x_4, x_3 + x_4)$ betrachten.

Aufgabe 1.11. Es sei $K \subseteq \mathbb{R}$ ein Unterkörper. Zeige, dass dann auch $K[\mathrm{i}]$ ein Unterkörper von $\mathbb{C}$ ist.

Aufgabe 1.12.*

Finde zwei natürliche Zahlen, deren Summe 65 und deren Produkt 1000 ist.

Aufgabe 1.13. Zeige, dass die Untergruppe

$$\mathbb{Z} + \mathbb{Z} \cdot \sqrt{3} \subseteq \mathbb{R}$$

dicht ist.

Aufgabe 1.14. Sei H eine (additive) Untergruppe der reellen Zahlen $\mathbb{R}$. Zeige, dass entweder $H = \mathbb{Z}a$ mit einer eindeutig bestimmten nichtnegativen reellen Zahl a ist, oder aber H dicht in $\mathbb{R}$ ist.

Aufgabe 1.15. Skizziere ein Entscheidungsverfahren für die Frage, ob eine diophantische Gleichung in einer Variablen eine Lösung besitzt oder nicht.

Aufgabe 1.16. Finde mindestens eine ganzzahlige Lösung $(x, y) \in \mathbb{N}_+ \times \mathbb{N}_+$ für die diophantische Gleichung

$$x^k + 1 = y^n$$

für $k, n \geq 2$.

Aufgabe 1.17. Zeige, dass die Gleichung

$$\frac{2}{n} = \frac{1}{a} + \frac{1}{b}$$

in $\mathbb{N}$ bei $a, b \leq n$ nur die Lösungen $n = a = b$ besitzt.

Aufgabe 1.18. Zeige, dass die Gleichung

$$\frac{2}{n} = \frac{1}{a} + \frac{1}{b}$$

in $\mathbb{Z}$ auch Lösungen mit $a \neq b$ besitzt.

Aufgabe 1.19.*

Zeige, dass die Gleichung

$$\frac{2}{n} = \frac{1}{a} + \frac{1}{b}$$

in $\mathbb{N}$ auch Lösungen $a \neq b$ besitzt.

Aufgabe 1.20. Finde eine nichttriviale ganzzahlige Lösung für das Gleichungssystem $ab = c$ und $(a-1)d = c-1$.

Aufgabe 1.21. Es seien $v \geq u \geq 0$ natürliche Zahlen. Zeige, dass

$$x = v^2 - u^2,\ y = 2uv,\ z = u^2 + v^2$$

die Gleichung

$$x^2 + y^2 = z^2$$

erfüllen.

Aufgabe 1.22. Es sei K ein Körper, $n \in \mathbb{N}$ und sei M die Menge der n-ten Einheitswurzeln in K. Zeige, dass M eine Untergruppe der Einheitengruppe $K^\times$ ist.

Aufgabe 1.23. Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Beweise die folgenden Aussagen.

(1) Wenn $b_1, b_2 \in K$ zwei Lösungen der Gleichung $X^n = a$ sind und $b_2 \neq 0$, so ist ihr Quotient b_1/b_2 eine n-te Einheitswurzel.
(2) Wenn $b \in K$ eine Lösung der Gleichung $X^n = a$ und ζ eine n-te Einheitswurzel ist, so ist auch ζb eine Lösung der Gleichung $X^n = a$.

Aufgabe 1.24. Zeige: Um den Satz von Wiles für alle Exponenten $n \geq 3$ zu zeigen, genügt es, ihn für alle ungeraden Primzahlen als Exponenten zu beweisen.

Aufgabe 1.25. Es sei

$$x^n + y^n = z^n$$

eine Fermat-Gleichung. Zeige: wenn es keine nichttriviale Lösung (x, y, z) in natürlichen Zahlen gibt, so gibt es auch keine nichttriviale Lösung in ganzen Zahlen.

Aufgabe 1.26. Zeige unter Verwendung des Satzes von Wiles, dass die diophantische Gleichung

$$x^n + y^n + z^n = 0$$

für $n \geq 2$ keine von $(0, 0, 0)$ verschiedene Lösung besitzt.

Aufgabe 1.27.*

Zeige, dass in $\mathbb{Z}/(29)$ die Gleichung

$$x^4 + y^4 + z^4 = 0$$

nur die triviale Lösung $(0, 0, 0)$ besitzt.

Aufgabe 1.28. Bestätige die folgenden Identitäten.

(1)

$$1 + 2^3 = 3^2.$$

(2)

$$2^5 + 7^2 = 3^4.$$

(3)

$$13^2 + 7^3 = 2^9.$$

2. Vorlesung - Teilbarkeitseigenschaften

Schon in der ersten Vorlesung haben wir zahlentheoretische Fragestellungen algebraisch mit Ringen formuliert. In dieser Vorlesung werden wir grundlegende ringtheoretische Konzepte einführen, und zwar insbesondere solche, die mit der Teilbarkeit zu tun haben.

2.1. **Einige ringtheoretische Konzepte.**

In einem Körper folgt aus $xy = 0$, dass ein Faktor 0 sein muss. Diese Eigenschaft gilt nicht für beliebige Ringe. Ein Element $f \in R$ in einem kommutativen Ring heißt *Nichtnullteiler*, wenn aus $fg = 0$ stets $g = 0$ folgt. Man nennt einen Ring *nullteilerfrei*, wenn 0 der einzige Nullteiler ist.

Definition 2.1. Ein kommutativer, nullteilerfreier, von 0 verschiedener Ring heißt *Integritätsbereich*.

Der Ring $\mathbb{Z}$ der ganzen Zahlen und die Polynomringe $K[X]$ über einem Körper K sind Integritätsbereiche. Das sind für uns besonders wichtigste Beispiele. Ein Unterring eines Körpers ist ein Integritätsbereich.

Definition 2.2. Es sei R ein kommutativer Ring, und a, b Elemente in R. Man sagt, dass a das Element b *teilt* (oder dass b von a geteilt wird, oder dass b ein *Vielfaches* von a ist), wenn es ein $c \in R$ derart gibt, dass $b = c \cdot a$ ist. Man schreibt dafür auch $a|b$.

Eine Einheit kann man als einen Teiler der 1 auffassen. Idealtheoretisch kann man die Eigenschaft, dass a das Element b teilt, als Zugehörigkeit $b \in Ra$ auffassen.

Definition 2.3. Es sei R ein kommutativer Ring. Man sagt, dass zwei Elemente $a, b \in R$ *teilerfremd* sind, wenn jedes Element $c \in R$, das sowohl a als auch b teilt, eine Einheit ist.

Definition 2.4. Eine Nichteinheit p in einem kommutativen Ring heißt *irreduzibel* (oder *unzerlegbar*), wenn eine Faktorisierung $p = ab$ nur dann möglich ist, wenn einer der Faktoren eine Einheit ist.

Diese Begriffsbildung orientiert sich offenbar an den Primzahlen. Dagegen taucht das Wort „prim“ in der folgenden Definition auf.

Definition 2.5. Eine Nichteinheit $p \neq 0$ in einem kommutativen Ring R heißt *prim* (oder ein *Primelement*), wenn folgendes gilt: Teilt p ein Produkt ab mit $a, b \in R$, so teilt p einen der Faktoren.

Eine Einheit ist also nach Definition nie ein Primelement. Dies ist eine Verallgemeinerung des Standpunktes, dass 1 keine Primzahl ist. Dabei ist die 1 nicht deshalb keine Primzahl, weil sie „zu schlecht“ ist, sondern weil sie „zu gut“ ist. Für die ganzen Zahlen und für viele weitere Ringe fallen die beiden Begriffe prim und irreduzibel zusammen. Im Allgemeinen ist irreduzibel einfacher nachzuweisen, und prim ist der stärkere Begriff, jedenfalls für Integritätsbereiche.

Lemma 2.6. *In einem Integritätsbereich ist ein Primelement stets irreduzibel.*

Beweis. Angenommen, wir haben eine Zerlegung $p = ab$. Wegen der Primeigenschaft teilt p einen Faktor, sagen wir $a = ps$. Dann ist $p = psb$ bzw. $p(1 - sb) = 0$. Da p kein Nullteiler ist, folgt $1 = sb$, so dass also b eine Einheit ist. □

2.2. **Irreduzible Polynome.**

Beispiel 2.7. Ein nichtkonstantes Polynom $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$, wobei K einen Körper bezeichne, ist genau dann irreduzibel, wenn es keine Produktdarstellung $P = QR$ gibt, die die Gradbedingung

$$0 < \operatorname{grad}(Q) < \operatorname{grad}(P)$$

erfüllt.

Die irreduziblen Polynome sind gerade die irreduziblen Elemente im Polynomring $K[X]$ im Sinne der obigen allgemeinen ringtheoretischen Definition. Nach der weiter unten zu beweisenden Aussage könnte man auch von Primelementen bzw. Primpolynomen sprechen. Eine weitere wichtige Charakterisierung ist die Restklassencharakterisierung, die wir in Lemma 3.9 kennenlernen werden.

Beispiel 2.8. Die Irreduzibilität eines Polynoms hängt wesentlich vom Grundkörper ab. Zum Beispiel ist das reelle Polynom $X^2 + 1 \in \mathbb{R}[X]$ irreduzibel, dagegen zerfällt es als Polynom in $\mathbb{C}[X]$ als

$$X^2 + 1 = (X + \mathrm{i})(X - \mathrm{i}).$$

Ebenso ist das Polynom $X^2 - 5 \in \mathbb{Q}[X]$ irreduzibel, aber über $\mathbb{R}$ hat es die Zerlegung

$$X^2 - 5 = \left(X - \sqrt{5}\right)\left(X + \sqrt{5}\right).$$

Übrigens kann die Zerlegung über einem größeren Körper manchmal dazu benutzt werden um zu zeigen, dass ein Polynom über dem gegebenen Körper irreduzibel ist.

Die Existenz der Faktorzerlegung in der folgenden Aussage folgt unmittelbar aus der Definition von irreduzibel, für die Eindeutigkeit muss man aber wissen, dass in einem Polynomring die irreduziblen Polynome auch Primpolynome sind (siehe unten).

Lemma 2.9. *Es sei K ein Körper und sei $F \in K[X]$ ein von 0 verschiedenes Polynom. Dann gibt es eine (bis auf die Reihenfolge der Faktoren) eindeutige Produktdarstellung*

$$F = aF_1 \cdots F_r$$

mit $a \in K^\times$ und irreduziblen normierten Polynomen F_i, $i = 1, \ldots, r$.

Beweis. Siehe Aufgabe 2.27. □

2.3. **Hauptidealbereiche.**

Definition 2.10. Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealbereich*.

Satz 2.11. *Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Hauptidealbereich.*

Beweis. Zunächst ist $\mathbb{Z}$ ein Integritätsbereich. Es sei $I \subseteq \mathbb{Z}$ ein Ideal. Damit ist I insbesondere eine (additive) Untergruppe von $\mathbb{Z}$ und hat nach Satz 44.3 (Lineare Algebra (Osnabrück 2017-2018)) die Gestalt $I = \mathbb{Z}d$. Damit handelt es sich um ein Hauptideal. □

Satz 2.12. *Ein Polynomring über einem Körper ist ein Hauptidealbereich.*

Beweis. Es sei I ein von 0 verschiedenes Ideal in $K[X]$. Betrachte die nichtleere Menge

$$\{\operatorname{grad}(P) \mid P \in I,\, P \neq 0\}\,.$$

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \operatorname{grad}(F)$. Wir behaupten, dass $I = (F)$ ist. Die Inklusion $\supseteq$ ist klar. Zum Beweis von $\subseteq$ sei $P \in I$ gegeben. Aufgrund von Satz 19.4 (Lineare Algebra (Osnabrück 2017-2018)) gilt

$$P = FQ + R \text{ mit } \operatorname{grad}(R) < \operatorname{grad}(F) \text{ oder } R = 0\,.$$

Wegen $R \in I$ und der Minimalität von $\operatorname{grad}(F)$ kann der erste Fall nicht eintreten. Also ist $R = 0$ und P ist ein Vielfaches von F. □

In jedem Hauptidealbereich gibt es stes eine Zerlegung in irreduzible Elmente.

Lemma 2.13. *In einem Hauptidealbereich lässt sich jede Nichteinheit $a \neq 0$ als ein Produkt von irreduziblen Elementen darstellen.*

Beweis. Angenommen, jede Zerlegung $a = p_1 \cdots p_k$ enthalte nicht irreduzible Elemente. Dann gibt es in jedem solchen Produkt einen Faktor, der ebenfalls keine Zerlegung in irreduzible Faktoren besitzt. Wir erhalten also eine unendliche Kette $a_1 = a, a_2, a_3, \ldots$, wobei a_{n+1} ein nicht-trivialer Teiler von a_n ist. Somit haben wir eine echt aufsteigende Idealkette

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots.$$

Die Vereinigung dieser Ideale ist aber nach Aufgabe 2.13 ebenfalls ein Ideal und nach Voraussetzung ein Hauptideal. Dies ist ein Widerspruch. □

Über diese Aussage hinaus ist aber in einem Hauptidealbereich jedes irreduzible Element auch prim und damit gibt es auch stets eine Faktorzerlegung in Primelemente. Der Nachweis davon braucht einige Vorbereitungen, nämlich das *Lemma von Bezout* und das *Lemma von Euklid*.

Lemma 2.14. *Es sei R ein Hauptidealbereich und seien $a, b \in R$ teilerfremde Elemente. Dann kann man die 1 als Linearkombination von a und b darstellen, d.h. es gibt Elemente $r, s \in R$ mit $ra + sb = 1$.*

Beweis. Wir betrachten das von a und b erzeugte Ideal $I = (a, b)$. Da R ein Hauptidealbereich ist, gibt es ein $c \in R$ mit $(a, b) = (c)$. Daher ist c ein Teiler von a und von b. Die Teilerfremdheit impliziert, dass c eine Einheit ist. Wegen $c \in (a, b)$ gibt es eine Darstellung $c = ua + vb$. Multiplikation mit c^{-1} ergibt die Darstellung der 1. □

Lemma 2.15. *Es sei R ein Hauptidealbereich und $a, b, c \in R$. Es seien a und b teilerfremd und a teile das Produkt bc. Dann teilt a den Faktor c.*

Beweis. Da a und b teilerfremd sind, gibt es nach dem Lemma von Bezout Elemente $r, s \in R$ mit $ra + sb = 1$. Die Voraussetzung, dass a das Produkt bc teilt, schreiben wir als $bc = da$. Damit gilt

$$c = c1 = c(ra + sb) = cra + csb = acr + ads = a(cr + ds),$$

was zeigt, dass c ein Vielfaches von a ist. □

Korollar 2.16. *Sei R ein Hauptidealbereich. Dann ist ein Element genau dann prim, wenn es irreduzibel ist.*

Beweis. Ein Primelement in einem Integritätsbereich ist nach Lemma 2.6 stets irreduzibel. Sei also umgekehrt p irreduzibel, und nehmen wir an, dass p das Produkt ab teilt, sagen wir $pc = ab$. Nehmen wir an, dass a kein Vielfaches von p ist. Dann sind aber a und p teilerfremd, da eine echte Inklusionskette $(p) \subset (p, a) = (d) \subset R$ der Irreduzibilität von p widerspricht. Damit teilt p nach dem Lemma von Euklid den anderen Faktor b. □

2.4. **Eindeutige Primfaktorzerlegung.**

Definition 2.17. Ein Integritätsbereich heißt *faktorieller Bereich*, wenn jede Nichteinheit $f \neq 0$ sich als ein Produkt von Primelementen schreiben lässt.

Satz 2.18. *Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent.*

(1) *R ist faktoriell.*
(2) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und diese Zerlegung ist bis auf Umordnung und Assoziiertheit eindeutig.*
(3) *Jede Nichteinheit $f \neq 0$ besitzt eine Faktorzerlegung in irreduzible Elemente, und jedes irreduzible Element ist ein Primelement.*

Beweis. (1) $\Rightarrow$ (2). Sei $f \neq 0$ eine Nichteinheit. Die Faktorisierung in Primelemente ist insbesondere eine Zerlegung in irreduzible Elemente, so dass also lediglich die Eindeutigkeit zu zeigen ist. Dies geschieht durch Induktion über die minimale Anzahl der Primelemente in einer Faktorzerlegung. Wenn es eine Darstellung $f = p$ mit einem Primelement gibt, und $f = q_1 \cdots q_r$ eine weitere Zerlegung in irreduzible Faktoren ist, so teilt p einen der Faktoren q_i und nach Kürzen durch p erhält man, dass das Produkt der übrigen Faktoren

rechts eine Einheit sein muss. Das bedeutet aber, dass es keine weiteren Faktoren geben kann. Sei nun $f = p_1 \cdots p_s$ und diese Aussage sei für Elemente mit kleineren Faktorisierungen in Primelemente bereits bewiesen. Es sei

$$f = p_1 \cdots p_s = q_1 \cdots q_r$$

eine weitere Zerlegung mit irreduziblen Elementen. Dann teilt wieder p_1 einen der Faktoren rechts, sagen wir $p_1 u = q_1$. Dann muss u eine Einheit sein und wir können durch p_1 kürzen, wobei wir u^{-1} mit q_2 verarbeiten können, was ein zu q_2 assoziiertes Element ergibt. Das gekürzte Element $p_2 \cdots p_s$ hat eine Faktorzerlegung mit $s-1$ Primelementen, so dass wir die Induktionsvoraussetzung anwenden können. (2) $\Rightarrow$ (3). Wir müssen zeigen, dass ein irreduzibles Element auch prim ist. Sei also q irreduzibel und es teile das Produkt fg, sagen wir

$$qh = fg.$$

Für h, f und g gibt es Faktorzerlegungen in irreduzible Elemente, so dass sich insgesamt die Gleichung

$$qh_1 \cdots h_r = f_1 \cdots f_s g_1 \cdots g_t$$

ergibt. Es liegen also zwei Zerlegungen in irreduzible Element vor, die nach Voraussetzung im Wesentlichen übereinstimmen müssen. D.h. insbesondere, dass es auf der rechten Seite einen Faktor gibt, sagen wir f_1, der assoziiert zu q ist. Dann teilt q auch den ursprünglichen Faktor f. (3) $\Rightarrow$ (1). Das ist trivial. □

Satz 2.19. *Ein Hauptidealbereich ist ein faktorieller Ring.*

Beweis. Dies folgt sofort aus Korollar 2.16, Lemma 2.13 und Satz 2.18. □

Korollar 2.20. *Es sei R ein faktorieller Ring und seien a und b zwei Elemente $\neq 0$ mit Primfaktorzerlegungen*

$$a = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k} \text{ und } b = v \cdot p_1^{s_1} \cdot p_2^{s_2} \cdots p_k^{s_k}$$

(wobei die u, v Einheiten sind und die Exponenten auch 0 sein können). Dann gilt $a|b$ genau dann, wenn $r_i \leq s_i$ für alle Exponenten $i = 1, \ldots, k$ ist.

Beweis. Wenn die Exponentenbedingung erfüllt ist, so ist $s_i - r_i \geq 0$ und man kann

$$b = a\big(vu^{-1} p_1^{s_1 - r_1} \cdots p_k^{s_k - r_k}\big)$$

schreiben, was die Teilbarkeit bedeutet. Die Umkehrung folgt aus der Eindeutigkeit der Primfaktorzerlegung in einem faktoriellen Ring. □

2. Arbeitsblatt

2.1. Übungsaufgaben.

Zwei Elemente a und b eines kommutativen Ringes R heißen *assoziiert*, wenn es eine Einheit $u \in R$ derart gibt, dass $a = ub$ ist.

Aufgabe 2.1. Zeige, dass die Assoziiertheit in einem kommutativen Ring eine Äquivalenzrelation ist.

Aufgabe 2.2. Beweise die folgenden Eigenschaften zur Teilbarkeit in einem kommutativen Ring R

(1) Für jedes Element a gilt $1|a$ und $a|a$.
(2) Für jedes Element a gilt $a|0$.
(3) Gilt $a|b$ und $b|c$, so gilt auch $a|c$.
(4) Gilt $a|b$ und $c|d$, so gilt auch $ac|bd$.
(5) Gilt $a|b$, so gilt auch $ac|bc$ für jedes $c \in R$.
(6) Gilt $a|b$ und $a|c$, so gilt auch $a|rb+sc$ für beliebige Elemente $r, s \in R$.

Aufgabe 2.3. Zeige, dass in einem kommutativen Ring R folgende Teilbarkeitsbeziehungen gelten.

(1) Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.
(2) Ist R ein Integritätsbereich, so gilt hiervon auch die Umkehrung.

Aufgabe 2.4. Zeige, dass in einem kommutativen Ring R folgende Teilbarkeitsbeziehungen gelten.

(1) -1 ist eine Einheit, die zu sich selbst invers ist.
(2) Jede Einheit teilt jedes Element.
(3) Sind a und b assoziiert, so gilt $a|c$ genau dann, wenn $b|c$.
(4) Teilt a eine Einheit, so ist a selbst eine Einheit.

Aufgabe 2.5. Zeige, dass ein Unterring eines Körpers ein Integritätsbereich ist.

Aufgabe 2.6. Es sei R ein kommutativer Ring und seien f, g Nichtnullteiler in R. Zeige, dass das Produkt fg ebenfalls ein Nichtnullteiler ist.

Aufgabe 2.7. Was bedeutet die Eigenschaft, dass man in einem Integritätsbereich „kürzen“ kann? Beweise diese Eigenschaft.

Aufgabe 2.8.*

Es sei R ein kommutativer Ring. Zu jedem $f \in R$ sei

$$\mu_f \colon R \longrightarrow R,\, g \longmapsto fg,$$

die Multiplikation mit f. Zeige, dass μ_f genau dann bijektiv ist, wenn es surjektiv ist.

Man zeige durch ein Beispiel, dass in dieser Situation aus der Injektivität nicht die Bijektivität folgt.

Aufgabe 2.9.*

Es sei R ein kommutativer Ring und $f \in R$. Charakterisiere mit Hilfe der Multiplikationsabbildung

$$\mu_f \colon R \longrightarrow R,\, g \longmapsto fg,$$

wann f ein Nichtnullteiler und wann f eine Einheit ist.

Aufgabe 2.10. Zeige, dass $\mathbb{Z} \subseteq \mathbb{Q}$ eine Untergruppe, aber kein Ideal ist.

Aufgabe 2.11.*

Zeige, dass ein kommutativer Ring genau dann ein Körper ist, wenn er genau zwei Ideale enthält.

Aufgabe 2.12. Sei R ein kommutativer Ring und sei f_j, $j \in J$, eine Familie von Elementen in R. Es sei angenommen, dass die f_j zusammen das Einheitsideal erzeugen. Zeige, dass es eine endliche Teilfamilie f_j, $j \in J_0 \subseteq J$ gibt, die ebenfalls das Einheitsideal erzeugt.

Aufgabe 2.13. Sei R ein kommutativer Ring und sei

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots$$

eine aufsteigende Kette von Idealen. Zeige, dass die Vereinigung $\bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ ebenfalls ein Ideal ist. Zeige durch ein einfaches Beispiel, dass die Vereinigung von Idealen im Allgemeinen kein Ideal sein muss.

Aufgabe 2.14. Sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Zeige, dass p genau dann irreduzibel ist, wenn es genau zwei Hauptideale oberhalb von (p) gibt, nämlich (p) selbst und $(1) = R$.

Aufgabe 2.15. Zeige, dass im Polynomring $K[X]$ über einem Körper K die Variable X irreduzibel und prim ist.

Aufgabe 2.16. Bestimme im Polynomring $K[X]$, wobei K ein Körper sei, die Einheiten und die Assoziiertheit. Gibt es in den Assoziiertheitsklassen besonders schöne Vertreter?

Aufgabe 2.17. Beweise die Formel

$$X^u + 1 = (X+1)\big(X^{u-1} - X^{u-2} + X^{u-3} - \cdots + X^2 - X + 1\big)$$

für u ungerade.

Aufgabe 2.18.*

Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass ein Polynom vom Grad zwei oder drei genau dann irreduzibel ist, wenn es keine Nullstelle in K besitzt.

Aufgabe 2.19.*

Bestimme die Primfaktorzerlegung des Polynoms $X^6 - 1$ über den Körpern $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(7)$ und $\mathbb{Z}/(5)$.

Aufgabe 2.20. Man wende eine Form des Eisensteinkriteriums an, um die Irreduzibilität der folgenden Polynome aus $\mathbb{Q}[X]$ nachzuweisen.

(1) $X^4 + 2X^2 + 2$,
(2) $20X^5 - 15X^4 + 125X^3 - 10X + 4$,
(3) $X^4 + 9$.

Aufgabe 2.21. Bestimme im Polynomring $\mathbb{Z}/(2)[X]$ alle irreduziblen Polynome vom Grad $2, 3, 4$.

Aufgabe 2.22. Bestimme im Polynomring $\mathbb{Z}/(3)[X]$ alle normierten irreduziblen Polynome vom Grad 3.

Aufgabe 2.23. Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad 3. Zeige, dass F entweder eine oder drei reelle Nullstellen besitzt.

Aufgabe 2.24. Zeige, dass ein reelles Polynom von ungeradem Grad nicht irreduzibel ist.

Aufgabe 2.25.*

Zeige, dass das Polynom

$$X^3 - 3X + 1$$

über $\mathbb{Q}$ irreduzibel ist.

Aufgabe 2.26.*

Zeige, dass das Polynom

$$X^3 - 3X - 1$$

über $\mathbb{Q}$ irreduzibel ist.

Aufgabe 2.27. Es sei K ein Körper und sei $F \in K[X]$ ein von 0 verschiedenes Polynom. Zeige, dass es eine (bis auf die Reihenfolge der Faktoren) eindeutige Produktdarstellung

$$F = aF_1 \cdots F_r$$

mit $a \in K^\times$ und irreduziblen normierten Polynomen F_i, $i = 1, \ldots, r$, gibt.

Aufgabe 2.28.*

Es sei K ein Körper und sei $K[X]$ der Polynomring über K und sei $P \in K[X]$ ein Polynom, das eine Zerlegung in Linearfaktoren besitze. Es sei T ein Teiler von P. Zeige, dass T ebenfalls eine Zerlegung in Linearfaktoren besitzt, wobei die Vielfachheit eines Linearfaktors $X - a$ in T durch seine Vielfachheit in P beschränkt ist.

Aufgabe 2.29.*

(1) Es sei F ein normiertes Polynom aus $\mathbb{Z}[X]$ und es gebe eine Primzahl q mit der Eigenschaft, dass F modulo q, also aufgefasst in $\mathbb{Z}/(q)[X]$, irreduzibel sei. Zeige, dass dann schon F irreduzibel ist.
(2) Zeige, dass die erste Aussage für ein nichtnormiertes Polynom nicht stimmen muss.
(3) Es sei p eine Primzahl und $G \in \mathbb{Z}/(p)[X]$ ein normiertes Polynom. Zeige, dass es ein normiertes Polynom $F \in \mathbb{Z}[X]$ gibt, das modulo p mit G übereinstimmt und das zusätzlich irreduzibel ist.

Aufgabe 2.30. Zeige, dass $\mathbb{Z}[X]$ und der Polynomring in zwei Variablen $K[X, Y]$ über einem Körper K keine Hauptidealbereiche sind.

Aufgabe 2.31. Zeige, dass in $\mathbb{Z}[X]$ die Ideale

$$\mathfrak{a} = \left(X^6 + X^3 + 1, 6X^5 + 3X^2\right)$$

und

$$\mathfrak{b} = \left(X^6 + X^3 + 1, 3X^3 - 3, 9\right)$$

übereinstimmen. Bestimme die Anzahl der Elemente im Restklassenring.

Aufgabe 2.32.*

Es sei R ein kommutativer Ring und sei $p \in R$ ein Primelement. Zeige, dass p auch im Polynomring $R[X]$ prim ist.

Aufgabe 2.33. Sei K ein algebraisch abgeschlossener Körper. Bestimme in $K[X]$ die irreduziblen Polynome.

Aufgabe 2.34. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Zeige, dass es unendlich viele normierte irreduzible Polynome in $K[X]$ gibt.

Aufgabe 2.35. Es sei $P \in \mathbb{R}[X]$ ein nichtkonstantes Polynom mit reellen Koeffizienten. Zeige, dass man P als ein Produkt von reellen Polynomen vom Grad 1 oder 2 schreiben kann.

Aufgabe 2.36. Es sei $K \subseteq L$ eine Körpererweiterung und es sei $a \in L$. Zeige, dass die Einsetzungsabbildung, also die Zuordnung

$$\psi\colon\ K[X] \longrightarrow L,\ P \longmapsto P(a),$$

folgende Eigenschaften erfüllt (dabei seien $P, Q \in K[X]$).

(1) $(P + Q)(a) = P(a) + Q(a)$,
(2) $(P \cdot Q)(a) = P(a) \cdot Q(a)$,
(3) $1(a) = 1$.

Aufgabe 2.37. Es sei K ein Körper, $\varphi\colon\ V \to V$ ein Endomorphismus auf einem endlichdimensionalen K-Vektorraum und

$$K[X] \longrightarrow \mathrm{End}\,(V),\ P \longmapsto P(\varphi),$$

der zugehörige Einsetzungshomomorphismus. Vergleiche diese Situation mit dem durch ein Element $a \in L$ zu einer Körpererweiterung $K \subseteq L$ gegebenen Einsetzungshomomorphismus $P \mapsto P(a)$.

Die folgenden Aufgaben benutzen das Produkt von Idealen.

Zu zwei Idealen $\mathfrak{a}$ und $\mathfrak{b}$ in einem kommutativen Ring wird das *Produkt* durch

$$\mathfrak{a}\mathfrak{b} = \{a_1b_1 + a_2b_2 + \cdots + a_kb_k\}$$

mit $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$ definiert. Das ist das Ideal, das von allen Produkten ab (mit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$) erzeugt wird.

Für das n-fache Produkt eines Ideals $\mathfrak{a}$ mit sich selbst schreibt man $\mathfrak{a}^n$.

Aufgabe 2.38. Zeige, dass das Produkt von Hauptidealen wieder ein Hauptideal ist.

Aufgabe 2.39. Es seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale in einem kommutativen Ring R. Zeige, dass die Beziehung

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$$

gilt.

Aufgabe 2.40. Es sei $\mathfrak{a} \subseteq R$ ein Ideal in einem kommutativen Ring R. Zeige, dass die Potenzen $\mathfrak{a}^n$, $n \in \mathbb{N}_+$, alle dasselbe Radikal besitzen.

Aufgabe 2.41.*

Es seien I und J Ideale in einem kommutativen Ring R und sei $n \in \mathbb{N}$. Zeige die Gleichheit

$$(I+J)^n = I^n + I^{n-1}J + I^{n-2}J^2 + \cdots + I^2J^{n-2} + IJ^{n-1} + J^n.$$

3. Vorlesung - Zahlen und Funktionen

Wir haben in der letzten Vorlesung gesehen, dass sowohl die ganzen Zahlen $\mathbb{Z}$ als auch die Polynomringe $K[X]$ in einer Variablen über einem Körper K Hauptidealbereiche sind. Bei Polynomen denkt man direkt an Funktionen, Auswertung an einem Punkt, Nullstellen, Ableitung u.s.w. Wir werden im Verlaufe dieser Vorlesung sehen, dass diese Konzepte zu einem Großteil auch im zahlentheoretischen Kontext interpretierbar sind.

3.1. **Zahlen und Funktionen.**

Zwischen den ganzen Zahlen einerseits und den Polynomringen über einem Körper andererseits bestehen folgende Analogien, die wir hier schon mal festhalten und die wir im Laufe des Kurses vertiefen werden. Dabei haben diese Phänomene im funktionentheoretischen Kontext eine zumeist naheliegende Bedeutung, während sie im zahlentheoretischen Kontext erst erschlossen werden müssen. Dieser Prozess erlaubt es, eine geometrische Sprache in die Zahlentheorie einzuführen, die zu Beginn etwas gewöhnungsbedürftig ist, aber bald eine gute intuitive Unterstützung für das Verständnis der Zahlentheorie gibt. Wir erwähnen die folgenden Punkte, die wir hier nur kurz funktionentheoretisch erläutern. Mit der passenden Begrifflichkeit werden aus Analogien dann gemeinsame Konzepte.

Analogien

(1) Man kann die gleichen algebraischen Konzepte anwenden.
(2) Hauptidealbereich.
(3) Punktkonzept. Restekörper.
(4) Funktion. Nullstelle.
(5) Rationale Funktionen. Polstelle.
(6) Quotientenkörper.
(7) Bilder und Urbilder.
(8) Lokale und globale Eigenschaften.
(9) Erweiterungen der Quotientenkörper. Ganzheit.
(10) Gruppenoperation.
(11) Zerlegung.
(12) Verzweigung.
(13) Singularitäten.
(14) Projektiver Abschluss.

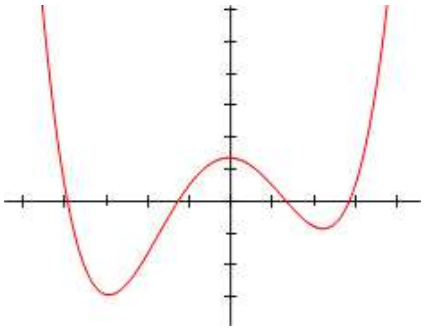
Unterschiede

(1) Nichtidentische Ringhomomorphismen von $K[T]$ in sich.
(2) Endlichkeit der Restekörper bei $\mathbb{Z}$. Dies gilt auch, wenn K ein endlicher Körper ist. Diese „Enge“ erzwingt häufig zusätzliche Gesetzmäßigkeiten.
(3) Analytische Methoden bei $K = \mathbb{R}$ oder $K = \mathbb{C}$.
(4) Topologische Methoden bei $K = \mathbb{R}$ oder $K = \mathbb{C}$.

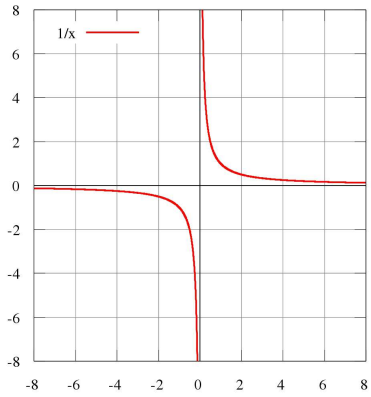
Einige Kommentare

Ein Polynom hat an jedem Punkt $a \in K$ einen Wert, eine besondere Rolle spielen die Nullstellen. Die Nullstellen können, wie bei x^2, eine größere Vielfachheit haben, und dies ist dann der Fall, wenn auch noch die Ableitung eine Nullstelle an dieser Stelle besitzt. Es gibt stets, außer beim Nullpolynom, nur endlich viele Nullstellen. Auch sonst wird jeder Wert, außer bei konstanten

Polynomen, nur endlich oft angenommen. Über den komplexen Zahlen ist jedes nichtkonstante Polynom surjektiv.



Aus Polynomen kann man durch Division auch rationale Funktionen bilden, beispielsweise $1/x$, diese sind nicht überall definiert und haben an endlich vielen Stellen, nämlich den Nullstellen des Nenners, Pole. Die Menge der rationalen Funktionen bildet wie die Menge der rationalen Zahlen einen Körper.



Die rationale Funktion $1/x$ besitzt an der Stelle 0 einen Pol.

So wie man endliche Erweiterungen

$$\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{7}] = \mathbb{Z}[T]/(T^2 - 7)$$

betrachten kann, kann man auch Erweiterungen wie

$$K[Y] \subseteq K[Y][X]/(X^2 - Y^3 + 5Y - 4)$$

betrachten, dabei wird beispielsweise einem Polynom, hier $Y^3 - 5Y + 4$, eine algebraische Quadratwurzel verpasst. Es wird also eine algebraische Funktion $\sqrt{y^3 - 5y + 4}$ adjungiert. Eine Besonderheit tritt auf, wenn man aus der Variablen Y selbst die Quadratwurzel zieht. Dann ist nämlich

$$K[Y][X]/(X^2 - Y) \cong K[X],$$

da man ja Y als Polynom in X ausdrücken kann. In diesem Fall ist also der algebraisch definierte Erweiterungsring selbst wieder isomorph zum Polynomring selbst! Jedes Polynom $P(X)$ in einer Variablen kann man in diesem Sinne als Ringerweiterung

$$K[Y] \subseteq K[Y,X]/(Y-P(X)) \cong K[X]$$

interpretieren. Das Polynom P definiert in diesem Sinne einen Ringhomomorphismus von $K[Y]$ nach $K[X]$. Ferner ist die Menge

$$V(Y-P(X)) = \left\{(x,y) \in K^2 \mid y = P(x)\right\}$$

der Graph des Polynoms P. Die Abbildung

$$K \longrightarrow K,\, x \longmapsto P(x),$$

kann man darin auch so auffassen, dass zuerst eine Bijektion zwischen K und dem Graphen gemacht wird und dann der Graph auf die vertikale Achse projiziert wird. Bei dieser Interpretation sieht man besonders schön, welche Punkte auf einen bestimmten Punkt b abgebildet werden, nämlich die Schnittpunkte des Graphen mit der durch b verlaufenden horizontalen Geraden. Es ist im Hinblick auf die zahlentheoretische Interpretation üblich, das Bild an der Hauptdiagonalen zu spiegeln, dass der Graph oberhalb der Zielgeraden liegt und die Punkte quasi herunterfallen. Das Urbild von b besteht bei dieser Veranschaulichung aus den Punkten, die oberhalb von b liegen, und man interessiert sich insbesondere dafür, wie diese Fasern mit b variieren. Bei einfachen Beispielen wie $P(x) = x^2$ fällt direkt ein regelmäßiges Zerlegungsverhalten der Fasern auf. Für reelles b besteht bei b positiv die Faser aus $\{\sqrt{b}, -\sqrt{b}\}$, bei $b = 0$ nur aus dem Nullpunkt und bei b negativ ist die Faser leer. Im Komplexen besteht die Faser für $b \neq 0$ stets aus zwei Punkten. Die Einzigkeit der 0 über der 0 wird in einem gewissen Sinne dadurch „aufgefangen“, dass dort auch die Ableitung gleich 0 ist, dort fallen die beiden Urbilder zusammen, es liegt „Verzweigung“ vor.

Ein vergleichbares Verhalten zeigt sich bei der Ringerweiterung

$$\mathbb{Z} \subseteq \mathbb{Z}[\mathrm{i}],$$

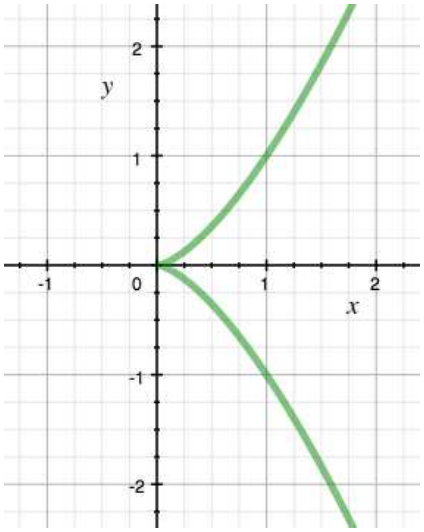
wenn man betrachtet, was dort mit den Primzahlen passiert. Für eine Primzahl p mit dem Rest 1 modulo 4 gibt es dort (das haben wir in der ersten Vorlesung angedeutet und werden wir im Laufe es Kurses genauer begründen) eine Faktorzerlegung

$$p = x^2 + \mathrm{i}y^2 = (x+\mathrm{i}y)(x-\mathrm{i}y)$$

in zwei neue Primelemente, eine Primzahl p mit dem Rest 3 modulo 4 bleibt eine Primzahl, wobei der Restklassenkörper aber p^2 viele Elemente besitzt, und für $p = 2$ gilt

$$2 = -\mathrm{i}(1+\mathrm{i})^2,$$

was dem Verzweigungsverhalten entspricht.



Ein weiteres Phänomen tritt auf, wenn man Erweiterungen der Form

$$K[Y] \subseteq K[Y][X]/(X^2 - Y^3)$$

betrachtet, die zugehörige Kurve

$$V(X^2 - Y^3) = \{(x, y) \mid x^2 = y^3\}$$

besitzt eine Singularität im Punkt $(0, 0)$, was bei dem Graphen eines Polynoms nicht vorkommen kann. Zahlentheoretisch treten bei Erweiterungen wie $\mathbb{Z} \subseteq \mathbb{Z}[X]/(X^2 - 27)$, also der Adjunktion von $\sqrt{27}$, ähnliche Phänomene auf. Deshalb haben wir bei quadratischen Erweiterungen quadratfreie Zahlen gefordert, was wir im Rahmen der Ganzheitstheorie aber noch weiter vertiefen müssen.

3.2. **Primideale.**

Was ist ein Punkt? Im funktionentheoretischen Kontext, wenn es darum geht, Polynome in einer Variablen auszuwerten, ist ein Punkt einfach ein Element von K, sagen wir $a \in K$. Durch Einsetzen erhält man einen Ringhomomorphismus

$$K[X] \longrightarrow K,\ F \longmapsto F(a),$$

einem Polynom wird also der Wert an der Stelle a zugeordnet. Diese Abbildung nennt man *Evaluation* Ev_a an der Stelle a. Ferner kennt man die Beziehung, dass $F(a) = 0$ genau dann ist, wenn $X - a$ im Polynomring ein Teiler von F ist, siehe Lemma 19.8 (Lineare Algebra (Osnabrück 2017-2018)). Dies bedeutet, dass der Kern der Evaluationsabbildung das von der Linearform $X - a$ erzeugte Hauptideal ist. Über den komplexen Zahlen gilt ferner, dass $a_1, \ldots, a_k \in \mathbb{C}$ alle Nullstellen von F sind, wenn für F die Faktorzerlegung

$$F = (X - a_1)^{r_1} \cdots (X - a_k)^{r_k}$$

gilt. Die Punkte a_i entsprechen also über die Linearformen $X - a_i$ den Primteilern von F. In einem gewissen Sinn entsprechen also Punkte speziellen Primelementen, in $\mathbb{C}[X]$ sind auch alle Primelemente von dieser linearen Form. Da nicht jeder Ring faktoriell ist, betrachtet man ausgehend vom Ring die sogenannten Primideale und entwickelt eine Theorie, in der diese Primideale zu Punkten eines geometrischen Objektes werden, und auf dem die Ringelemente zu Funktionen werden.

Definition 3.1. Ein Ideal $\mathfrak{p}$ in einem kommutativen Ring R heißt *Primideal*, wenn $\mathfrak{p} \neq R$ ist und wenn für $r, s \in R$ mit $r \cdot s \in \mathfrak{p}$ folgt: $r \in \mathfrak{p}$ oder $s \in \mathfrak{p}$.

Lemma 3.2. *Es sei R ein Integritätsbereich und $p \in R$, $p \neq 0$. Dann ist p genau dann ein Primelement, wenn das von p erzeugte Hauptideal (p) ein Primideal ist.*

Beweis. Siehe Aufgabe 3.9. □

Lemma 3.3. *Es sei R ein kommutativer Ring und $\mathfrak{p}$ ein Ideal in R. Dann ist $\mathfrak{p}$ genau dann ein Primideal, wenn der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist.*

Beweis. Sei zunächst $\mathfrak{p}$ ein Primideal. Dann ist insbesondere $\mathfrak{p} \subset R$ und somit ist der Restklassenring $R/\mathfrak{p}$ nicht der Nullring. Sei $fg = 0$ in $R/\mathfrak{p}$ wobei f, g durch Elemente in R repräsentiert seien. Dann ist $fg \in \mathfrak{p}$ und damit $f \in \mathfrak{p}$ oder $g \in \mathfrak{p}$. was in $R/\mathfrak{p}$ gerade $f = 0$ oder $g = 0$ bedeutet.

Ist umgekehrt $R/\mathfrak{p}$ ein Integritätsbereich, so handelt es sich nicht um den Nullring und daher ist $\mathfrak{p} \neq R$. Sei $f, g \notin \mathfrak{p}$. Dann ist $f, g \neq 0$ in $R/\mathfrak{p}$ und daher $fg \neq 0$ in $R/\mathfrak{p}$, also ist $fg \notin \mathfrak{p}$. □

Definition 3.4. Ein Ideal $\mathfrak{m}$ in einem kommutativen Ring R heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ ist und wenn es zwischen $\mathfrak{m}$ und R keine weiteren Ideale gibt.

Lemma 3.5. *Es sei R ein kommutativer Ring und $\mathfrak{m}$ ein Ideal in R. Dann ist $\mathfrak{m}$ genau dann ein maximales Ideal, wenn der Restklassenring $R/\mathfrak{m}$ ein Körper ist.*

Beweis. Siehe Aufgabe 3.7. □

Korollar 3.6. *Es sei R ein kommutativer Ring und $\mathfrak{m}$ ein maximales Ideal in R. Dann ist $\mathfrak{m}$ ein Primideal.*

Beweis. Dies folgt sofort aus den Charakterisierungen für Primideale und für maximale Ideale mit den Restklassenringen. □

Zu einem Primideal $\mathfrak{p}$ und insbesondere zu einem maximalen Ideal gehört die *Evaluationsabbildung*

$$R \longrightarrow R/\mathfrak{p},$$

wobei im maximalen Fall rechts ein Körper steht, der *Restklassenkörper* oder *Restekörper* (bei einem Primideal betrachtet man den Quotientenkörper als Restekörper). Die Restklassenkörper sind für das Studium des Ringes relevante Körper. Bei $R = \mathbb{Z}$ sind die Evaluationsabildungen gleich $\mathbb{Z} \to \mathbb{Z}/(p)$ bzw. (zum Nullideal) $\mathbb{Z} \to \mathbb{Q}$. Hier treten also alle Primkörper als Restekörper auf.

Lemma 3.7. *Es sei R ein Hauptidealbereich und $p \neq 0$ ein Element. Dann sind folgende Bedingungen äquivalent.*

(1) *p ist ein Primelement.*
(2) *$R/(p)$ ist ein Integritätsbereich.*
(3) *$R/(p)$ ist ein Körper.*

Beweis. Die Äquivalenz (1) $\Leftrightarrow$ (2) gilt in jedem kommutativen Ring (auch für $p = 0$), siehe Aufgabe 3.10, und (3) impliziert natürlich (2). Sei also (1) erfüllt und sei $a \in R/(p)$ von 0 verschieden. Wir bezeichnen einen Repräsentanten davon in R ebenfalls mit a. Es ist dann $a \notin (p)$ und es ergibt sich eine echte Idealinklusion $(p) \subset (a, p)$. Ferner können wir $(a, p) = (b)$ schreiben, da wir in einem Hauptidealring sind. Es folgt $p = cb$. Da c keine Einheit ist und p prim (also nach Lemma 2.6 auch irreduzibel) ist, muss b eine Einheit sein. Es ist also $(a, p) = (1)$, und das bedeutet modulo p, also in $R/(p)$, dass a eine Einheit ist. Also ist $R/(p)$ ein Körper. □

In einem Hauptideal besteht also die Menge der Primideale aus dem Nullideal und den maximalen Idealen.

Lemma 3.8. *Es sei K ein Körper und $P \in K[X]$, $P \neq 0$, ein Polynom. Dann ist P genau dann irreduzibel, wenn der Restklassenring $K[X]/(P)$ ein Körper ist.*

Beweis. Dies folgt direkt aus Satz 2.12 und Lemma 3.7. □

Wir erwähnen noch den folgenden Existenzsatz für Primideale.

Lemma 3.9. *Es sei R ein kommutativer Ring und sei $f \in R$ nicht nilpotent. Dann gibt es ein Primideal $\mathfrak{p}$ in R mit $f \notin \mathfrak{p}$.*

Beweis. Siehe Aufgabe 3.8. □

3.3. **Das Spektrum.**

Definition 3.10. Zu einem kommutativen Ring R nennt man die Menge der Primideale von R das *Spektrum* von R, geschrieben

$$\operatorname{Spek}(R).$$

Beispiel 3.11. Ein Körper hat bekanntlich nur zwei Ideale, nämlich das Einheitsideal K, das kein Primideal ist, und das Nullideal 0, das ein Primideal ist. Das Spektrum eines Körpers besteht also aus einem einzigen Punkt.

Bei einem Hauptidealbereich (dies gilt auch für Dedekindbereiche, die wir später einführen werden) besteht das Spektrum aus dem Nullideal 0 und den maximalen Idealen, die von der Form $\mathfrak{m} = (p)$ mit einem Primelement p sind.

Definition 3.12. Auf dem Spektrum eines kommutativen Ringes R ist die *Zariski-Topologie* dadurch gegeben, dass zu einer beliebigen Teilmenge $T \subseteq R$ die Mengen

$$D(T) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid T \not\subseteq \mathfrak{p}\}$$

als offen erklärt werden.

Für einelementige Teilmengen $T = \{f\}$ schreiben wir $D(f)$ statt $D(\{f\})$.

Lemma 3.13. *Die Zariski-Topologie auf dem Spektrum* $\operatorname{Spek}(R)$ *eines kommutativen Ringes R ist in der Tat eine Topologie.*

Beweis. Siehe Aufgabe 3.16. □

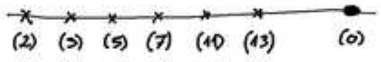
Wir betrachten das Spektrum stets als topologischen Raum. Die Primideale sind die Punkte dieses Raumes. Die Komplemente der offenen Mengen, also die abgeschlossenen Mengen in der Zariski-Topologie, werden mit

$$V(T) = \{\mathfrak{p} \in \operatorname{Spek}(R) \mid T \subseteq \mathfrak{p}\}$$

bezeichnet. Bei einem Hauptidealbereich ist die Zariski-Topologie besonders einfach, nur das gesamte Spektrum ist abgeschlossen und jede endliche Ansammlung von maximalen Idealen ist abgeschlossen. Dennoch ist auch in diesem Fall die Zariski-Topologie schon hilfreich. Wenn man beispielsweise aus topologischen Gründen weiß, dass eine Teilmenge abgeschlossenen sein muss, so folgt, dass es die gesamte Menge oder aber, dass sie endlich ist.

Beispiel 3.14. Für den Polynomring $R = K[X]$ in einer Variablen X über einem Körper K gibt es das Nullideal und die maximalen Ideale. Zu jedem Element $a \in K$ gehört die Linearform $X - a$ und das davon erzeugte maximale Ideal $(X - a)$. Deshalb stellt man sich das Spektrum $\operatorname{Spek}(K[X])$ zunächst als eine K-Gerade vor, mit dem fetten Punkt zum Nullideal als alles umfassenden Punkt. Bei K algebraisch abgeschlossen ist dies das gesamte Spektrum. Bei einem nicht algebraisch abgeschlossenen Körper kommt noch für jedes normierte irreduzible Polynom P vom Grad ≥ 2 das maximale Primideal (P) hinzu, das man aber im Bild schlecht skizzieren kann und sich „im Hintergrund“ vorstellt.

Beispiel 3.15. Die Primideale in $\mathbb{Z}$ sind einerseits die maximalen Ideale (p), wobei p eine Primzahl ist, und andererseits das Nullideal 0. Die maximalen Ideale bilden die abgeschlossenen Punkte von $\operatorname{Spek}(\mathbb{Z})$. Das Nullideal ist darin ein weiterer nicht abgeschlossener Punkt. Die einzige abgeschlossene Menge, in der dieser Punkt enthalten ist, ist die ganze Menge. Die abgeschlossenen Mengen in $\operatorname{Spek}(\mathbb{Z})$ sind neben der Gesamtmenge die endlichen Teilmengen aus maximalen Idealen.



So stellt man sich das Spektrum von $\mathbb{Z}$ vor. Die Verbindungslinien sollen vermitteln, dass es sich um ein eindimensionales Objekt handelt. Das Nullideal malt man fett, um anzudeuten, dass es sich um einen dichten Punkt handelt.

Man visualisiert $\operatorname{Spek}(\mathbb{Z})$ als eine (gedachte Gerade), auf der die Primzahlen diskret liegen, während der Nullpunkt ein fetter Punkt ist, der die gesamte Gerade repräsentiert.

Proposition 3.16. *Für das Spektrum $X = \operatorname{Spek}(R)$ eines kommutativen Ringes R gelten folgende Eigenschaften.*

(1) *Es ist $D(T) = D(\mathfrak{a})$, wobei $\mathfrak{a}$ das durch T erzeugte Ideal (Radikal) in R sei. Man kann sich also bei der Beschreibung der offenen Teilmengen auf die Radikale von R beschränken.*
(2) *Für eine Familie $\mathfrak{a}_i$, $i \in I$, von Idealen in R ist*
$$\bigcup_{i \in I} D(\mathfrak{a}_i) = D\left(\sum_{i \in I} \mathfrak{a}_i \right).$$
(3) *Für eine endliche Familie $\mathfrak{a}_i$, $i = 1, \ldots, n$, von Idealen in R ist*
$$\bigcap_{i=1}^{n} D(\mathfrak{a}_i) = D\left(\bigcap_{i=1}^{n} \mathfrak{a}_i \right) = D(\mathfrak{a}_1 \cdots \mathfrak{a}_n).$$
(4) *Es ist $D(\mathfrak{a}) = X$ genau dann, wenn $\mathfrak{a}$ das Einheitsideal ist.*
(5) *Es ist $D(\mathfrak{a}) \subseteq D(\mathfrak{b})$ genau dann, wenn $\mathfrak{a} \subseteq \operatorname{rad}(\mathfrak{b})$ gilt.*
(6) *Das Spektrum ist genau dann leer, wenn R der Nullring ist.*
(7) *Es ist $D(\mathfrak{a}) = \emptyset$ genau dann, wenn $\mathfrak{a}$ nur nilpotente Elemente enthält.*
(8) *Die offenen Mengen $D(f)$, $f \in R$, bilden eine Basis der Topologie.*
(9) *Eine Familie von offenen Mengen $D(\mathfrak{a}_i)$, $i \in I$, ist genau dann eine Überdeckung von X, wenn die Ideale $\mathfrak{a}_i$ zusammen das Einheitsideal erzeugen.*

Beweis. Siehe Aufgabe 3.17. □

3. Arbeitsblatt

3.1. Übungsaufgaben.

Die folgenden Aufgaben betrachten Ringeigenschaften am Beispiel von Ringen von stetigen Funktionen.

Aufgabe 3.1. Wir betrachten die Menge $R = C(\mathbb{R}, \mathbb{R})$ der stetigen Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Zeige, dass R (mit naheliegenden Verknüpfungen) ein kommutativer Ring ist. Handelt es sich um einen Integritätsbereich?

Aufgabe 3.2. Zeige, dass es im Ring der stetigen Funktionen $R = C(\mathbb{R}, \mathbb{R})$ Nichtnullteiler gibt, die unendlich viele Nullstellen besitzen.

Aufgabe 3.3. Es sei M ein metrischer Raum und $R = C(M, \mathbb{R})$ der Ring der stetigen Funktion auf M. Zeige, dass zwei zueinander assoziierte Elemente $f, g \in R$ die gleiche Nullstellenmenge besitzen, und dass die Umkehrung nicht gelten muss.

Aufgabe 3.4.*

Zeige, dass es stetige Funktionen

$$f, g\colon \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R},$$

mit $fg = 0$ derart gibt, dass für alle $\delta > 0$ weder $f|_{[0,\delta]}$ noch $g|_{[0,\delta]}$ die Nullfunktion ist.

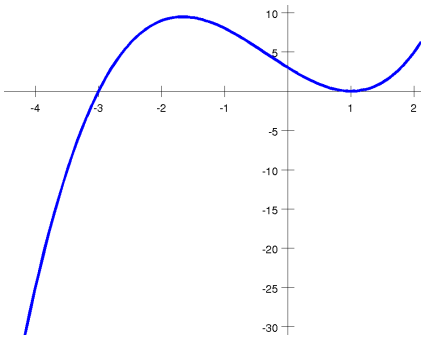
Aufgabe 3.5. Es seien X und Y topologische Räume und

$$\varphi\colon X \longrightarrow Y$$

eine stetige Abbildung. Zeige, dass dies einen Ringhomomorphismus

$$C(Y, \mathbb{R}) \longrightarrow C(X, \mathbb{R}),\ f \longmapsto f \circ \varphi,$$

induziert.



Aufgabe 3.6. Zeige, dass zu $a \in \mathbb{C}$ der Einsetzungshomomorphismus

$$\mathbb{C}[X] \longrightarrow \mathbb{C},\ X \longmapsto a,$$

mit der Evaluationsabbildung (in den Restekörper $\mathbb{C}[X]_{(X-a)}/(X-a)\,\mathbb{C}[X]_{(X-a)}$) zum Primideal $(X-a)$ übereinstimmt.

Aufgabe 3.7. Es sei $f \in \mathbb{C}[X]$, $f \neq 0$, und $a \in \mathbb{C}$. Zeige, dass die folgenden „Ordnungen“ von f an der Stelle a übereinstimmen.

(1) Die Verschwindungsordnung von f an der Stelle a, also die maximale Ordnung einer Ableitung mit $f^{(k)}(a) = 0$.
(2) Der Exponent des Linearfaktors $X - a$ in der Zerlegung von f.
(3) Die Ordnung von f an der Lokalisierung $\mathbb{C}[X]_{(X-a)}$ von $\mathbb{C}[X]$ am maximalen Ideal $(X-a)$.

Aufgabe 3.8. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $a \in K$ ein fixiertes Element. Bestimme den Kern des Einsetzungshomomorphismus

$$K[X] \longrightarrow K,\ X \longmapsto a.$$

Aufgabe 3.9. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $P \in K[X]$ ein nicht-konstantes Polynom. Zeige, dass der durch $X \mapsto P$ definierte Einsetzungshomomorphismus von $K[X]$ nach $K[X]$ injektiv ist und dass der durch P erzeugte Unterring $K[P] \subseteq K[X]$ isomorph zum Polynomring in einer Variablen ist.

Aufgabe 3.10. Es sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal in R. Zeige, dass I genau dann ein maximales Ideal ist, wenn der Restklassenring R/I ein Körper ist.

Aufgabe 3.11.*

Es sei R ein kommutativer Ring und $f \in R$ sei nicht nilpotent. Zeige, dass es ein Primideal $\mathfrak{p}$ mit $f \notin \mathfrak{p}$ gibt.

Aufgabe 3.12. Sei R ein Integritätsbereich und sei $0 \neq p \in R$ keine Einheit. Dann ist p genau dann ein Primelement, wenn das von p erzeugte Ideal $(p) \subset R$ ein Primideal ist.

Aufgabe 3.13. Sei R ein kommutativer Ring und $p \in R$, $p \neq 0$. Zeige, dass p genau dann ein Primelement ist, wenn der Restklassenring $R/(p)$ ein Integritätsbereich ist.

Aufgabe 3.14. Sei R ein vom Nullring verschiedener kommutativer Ring. Zeige unter Verwendung des Lemmas von Zorn, dass es maximale Ideale in R gibt.

Aufgabe 3.15. Zeige, dass ein maximales Ideal $\mathfrak{m}$ in einem kommutativen Ring R ein Primideal ist.

Aufgabe 3.16. Sei R ein kommutativer Ring und sei $\mathfrak{a}$ ein Ideal mit dem Restklassenring $S = R/\mathfrak{a}$. Zeige, dass die Ideale von S eindeutig denjenigen Idealen von R entsprechen, die $\mathfrak{a}$ umfassen.

Zeige, dass das Gleiche für Primideale, Radikalideale und maximale Ideale gilt.

Aufgabe 3.17. Bestimme sämtliche Primkörper.

Aufgabe 3.18. Es sei R ein kommutativer Ring. Zeige, dass R genau dann der Nullring ist, wenn sein Spektrum $\operatorname{Spek}(R)$ leer ist.

Aufgabe 3.19.*

Zeige, dass die Zariski-Topologie auf dem Spektrum $\operatorname{Spek}(R)$ eines kommutativen Ringes R in der Tat eine Topologie ist.

Aufgabe 3.20.*

Beweise Proposition 3.16.

Aufgabe 3.21. Skizziere das Spektrum von $\mathbb{Z}/(p)[X]$ für verschiedene Primzahlen p.

Aufgabe 3.22. Skizziere das Spektrum von $\mathbb{Z}[X]$.

4. Vorlesung - Nenneraufnahme

In diesem Kurs beweisen wir zwei Versionen zur eindeutigen Primfaktorzerlegung in Zahlbereichen, die beide Abschwächungen zur eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ sind. Die eine besagt, dass für einen Zahlbereich die eindeutige Primfaktorzerlegung von Elementen „lokal“ gilt (Satz 10.17 und Bemerkung 10.9). Die zweite Version besagt, dass man auf der Ebene der Ideale eine eindeutige Faktorzerlegung in Primideale erhält (Satz 12.2). Für die erste Version benötigen wir die Begriffe Nenneraufnahme, Lokalisierung und diskreter Bewertungsring.

4.1. **Multiplikative Systeme.**

Definition 4.1. Es sei R ein kommutativer Ring. Eine Teilmenge $S \subseteq R$ heißt *multiplikatives System*, wenn die beiden Eigenschaften

(1) $1 \in S$,
(2) Wenn $f, g \in S$, dann ist auch $fg \in S$,

gelten.

Es handelt sich also einfach um ein Untermonoid des multiplikativen Monoids eines Ringes. Wir erwähnen einige Beispiele von multiplikativen Systemen. Zunächst ist natürlich der Gesamtring, die Menge $\{1\}$, die Menge $\{0,1\}$ und die Einheitengruppe $R^\times$ ein multiplikatives System. Darüber hinaus erwähnen wir die folgenden Beispiele.

Beispiel 4.2. Es sei R ein kommutativer Ring und $f \in R$ ein Element. Dann bilden die Potenzen f^n, $n \in \mathbb{N}$, ein multiplikatives System.

Beispiel 4.3. Sei R ein Integritätsbereich. Dann bilden alle von 0 verschiedenen Elemente in R ein multiplikatives System, das mit $R^* = R \setminus \{0\}$ bezeichnet wird.

Beispiel 4.4. Die Nichtnullteiler bilden ein multiplikatives System in einem kommutativen Ring. Die 1 ist wie jede Einheit ein Nichtnullteiler, und wenn f und g Nichtnullteiler sind, so ist auch deren Produkt ein Nichtnullteiler, da aus $f(gh) = 0$ zunächst $gh = 0$ und daraus $h = 0$ folgt.

Beispiel 4.5. Es sei R ein faktorieller Bereich und sei M eine Menge von Primelementen. Dann ist die Menge aller Elemente aus R, in deren Primfaktorzerlegung ausschließlich Primelemente aus M vorkommen, ein multiplikatives System S. Es ist also

$$S = \left\{ u p_1^{r_1} \cdots p_k^{r_k} \mid u \in R^\times, p_i \in M \right\}.$$

Beispiel 4.6. Sei R ein kommutativer Ring und $\mathfrak{p}$ ein Primideal. Dann ist das Komplement $R \setminus \mathfrak{p}$ ein multiplikatives System. Dies folgt unmittelbar aus der Definition.

4.2. **Nenneraufnahme.**

Die Idee für die Nenneraufnahme zu einem multiplikativen System $S \subseteq R$ ist es, die Elemente aus S zu Einheiten, zu Nennern, zu machen. Dabei soll natürlich wieder ein sinnvoller Ring entstehen. Von den rationalen Zahlen kennt man die Eigenschaft, dass $\frac{r}{s} = \frac{r'}{s'}$ genau dann gilt, wenn $rs' = r's$ gilt, wodurch dir Gleichheit von Brüchen auf die Gleicheit innerhalb der ganzen Zahlen zurückgeführt wird. Diesen Ansatz muss man wegen möglicher Nullteiler etwas modifizieren.

Definition 4.7. Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Auf der Produktmenge $R \times S$ nennt man die durch

$$(r,s) \sim (r',s'),$$

falls es ein $t \in S$ mit $rs't = r'st$ gibt, die durch das multiplikative System gegebene *Überkreuzrelation*.

Wenn S nur aus Nichtnullteilern besteht, so braucht man den zusätzlichen Faktor t nicht.

Lemma 4.8. *Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Dann ist die Überkreuzrelation auf der Produktmenge $R \times S$ eine Äquivalenzrelation. Für die Äquivalenzklassen $\frac{r}{s} := [(r,s)]$ ist durch*

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

eine wohldefinierte Addition und durch

$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$$

eine wohldefinierte Multiplikation gegeben, derart, dass die Quotientenmenge ein kommutativer Ring wird.

Beweis. Siehe Aufgabe 4.9. □

Definition 4.9. Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Dann versteht man unter der *Nenneraufnahme* zu S die Quotientenmenge zur Überkreuzrelation auf $R \times S$ mit den in Lemma 4.8 beschriebenen Verknüpfungen. Die Nenneraufnahme wird mit R_S bezeichnet.

Es gibt einen natürlichen Ringhomomorphismus

$$R \longrightarrow R_S,\ r \longmapsto \frac{r}{1}.$$

Die Elemente $s \in S$ aus dem multiplikativen System werden in R_S zu Einheiten, und zwar ist $1/s$ das Inverse zu s. Wenn S nur aus Nuchtnullteilern besteht, so ist diese kanonische Abbildung injektiv. Wenn hingegen die 0 zu S gehört, so wird die Nenneraufnahme zum Nullring. Für die Nenneraufnahme an dem von einem Element f erzeugten multiplikativen System schreibt

man einfach R_f statt $R_{\{f^n|n\in\mathbb{N}\}}$. Die Nenneraufnahme an $R^* = R \setminus \{0\}$ in einem Integritätsbereich spielt eine besondere Rolle. Dort werden sämtliche Elemente $\neq 0$ zu Einheiten und es entsteht ein Körper.

Definition 4.10. Zu einem Integritätsbereich R ist der *Quotientenkörper* $Q(R)$ als die Menge der formalen Brüche

$$Q(R) = \left\{ \frac{r}{s} \mid r,s \in R,\, s \neq 0 \right\}$$

mit natürlichen Identifizierungen und Operationen definiert.

Lemma 4.11. *Es seien R und A kommutative Ringe und sei $S \subseteq R$ ein multiplikatives System. Es sei*

$$\varphi\colon\ R \longrightarrow A$$

ein Ringhomomorphismus derart, dass $\varphi(s)$ eine Einheit in A für alle $s \in S$ ist. Dann gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\tilde{\varphi}\colon\ R_S \longrightarrow A,$$

der φ fortsetzt.

Beweis. Damit die Ringhomomorphismen kommutieren muss

$$\tilde{\varphi}(1/s) = (\varphi(s))^{-1}$$

für $s \in S$ und damit $\tilde{\varphi}(a/s) = \varphi(a)(\varphi(s))^{-1}$ sein. Es kann also maximal einen solchen Ringhomomorphismus geben, der durch die letzte Gleichung definiert sein muss.

Es ist zu zeigen, dass dadurch ein wohldefinierter Ringhomomorphismus gegeben ist. Zum Nachweis der Wohldefiniertheit sei $\frac{a}{s} = \frac{b}{t}$ mit $s,t \in S$. Dies bedeutet, dass es ein $r \in S$ mit $rta = rsb$ gibt. Dann ist auch

$$\varphi(r)\varphi(t)\varphi(a) = \varphi(r)\varphi(s)\varphi(b)$$

und durch Multiplizieren mit der Einheit $\varphi(r)^{-1}\varphi(t)^{-1}\varphi(s)^{-1}$ folgt

$$\varphi(a)(\varphi(s))^{-1} = \varphi(b)(\varphi(t))^{-1}.$$

Wir zeigen exemplarisch für die Addition, dass ein Ringhomomorphismus vorliegt. Es ist

$$\begin{aligned}
\tilde{\varphi}\left(\frac{a}{s}+\frac{b}{t}\right) &= \tilde{\varphi}\left(\frac{at+bs}{st}\right) \\
&= \varphi(at+bs)\varphi(st)^{-1} \\
&= (\varphi(a)\varphi(t)+\varphi(s)\varphi(b))\varphi(s)^{-1}\varphi(t)^{-1} \\
&= \varphi(a)\varphi(s)^{-1}+\varphi(b)\varphi(t)^{-1} \\
&= \tilde{\varphi}\left(\frac{a}{s}\right)+\tilde{\varphi}\left(\frac{b}{t}\right).
\end{aligned}$$

□

4.3. **Lokale Ringe und Lokalisierung.**

Definition 4.12. Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal besitzt.

Jeder Körper ist ein lokaler Ring mit dem Nullideal als eindeutigem maximalen Ideal. Ein kommutativer Ring ist genau dann lokal, wenn seine Nichteinheiten ein Ideal bilden, das dann das einzige maximale Ideal ist.

Definition 4.13. Zu einem kommutativen lokalen Ring R nennt man den Restklassenkörper $R/\mathfrak{m}$ zum einzigen maximalen Ideal $\mathfrak{m}$ von R den *Restekörper* von R.

Definition 4.14. Sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal. Dann nennt man die Nenneraufnahme an $S = R \setminus \mathfrak{p}$ die *Lokalisierung* von R an $\mathfrak{p}$. Man schreibt dafür $R_\mathfrak{p}$. Es ist also

$$R_\mathfrak{p} := \left\{ \frac{f}{g} \mid f \in R,\, g \notin \mathfrak{p} \right\}.$$

Für eine Primzahl $p \in \mathbb{Z}$ besteht $\mathbb{Z}_{(p)}$ aus allen rationalen Zahlen, die man ohne p im Nenner schreiben kann.

Der folgende Satz zeigt, dass diese Namensgebung Sinn ergibt.

Satz 4.15. *Sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal in R. Dann ist die Lokalisierung $R_\mathfrak{p}$ ein lokaler Ring mit maximalem Ideal*

$$\mathfrak{p}R_\mathfrak{p} := \left\{ \frac{f}{g} \mid f \in \mathfrak{p},\, g \notin \mathfrak{p} \right\}.$$

Beweis. Die angegebene Menge ist in der Tat ein Ideal in der Lokalisierung

$$R_\mathfrak{p} = \left\{ \frac{f}{g} \mid f \in R,\, g \notin \mathfrak{p} \right\}.$$

Wir zeigen, dass das Komplement von $\mathfrak{p}R_\mathfrak{p}$ nur aus Einheiten besteht, so dass es sich um ein maximales Ideal handeln muss. Sei also $q = \frac{f}{g} \in R_\mathfrak{p}$, aber nicht in $\mathfrak{p}R_\mathfrak{p}$. Dann sind $f, g \notin \mathfrak{p}$ und somit gehört der inverse Bruch $\frac{g}{f}$ ebenfalls zur Lokalisierung. □

Das Ideal $\mathfrak{p}R_\mathfrak{p}$ ist dabei das Erweiterungsideal zu $\mathfrak{p}$ unter dem Ringhomomorphismus $R \to R_\mathfrak{p}$.

Satz 4.16. *Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann gilt*

$$R = \bigcap_{\mathfrak{m}\ maximal} R_\mathfrak{m},$$

wobei der Durchschnitt über alle maximale Ideale läuft und in $Q(R)$ genommen wird.

Beweis. Die Inklusion $\subseteq$ ist klar. Sei also $q \in Q(R)$ und sei angenommen, q gehöre zum Durchschnitt rechts. Für jedes maximale Ideal $\mathfrak{m}$ ist also $q \in R_{\mathfrak{m}} \subset Q(R)$, d.h. es gibt $f_{\mathfrak{m}} \notin \mathfrak{m}$ und $a_{\mathfrak{m}} \in R$ mit $q = \frac{a_{\mathfrak{m}}}{f_{\mathfrak{m}}}$. Wir betrachten das Ideal

$$(f_{\mathfrak{m}} : \mathfrak{m} \text{ maximal}).$$

Dieses Ideal ist in keinem maximalen Ideal enthalten, also muss es nach dem Lemma von Zorn das Einheitsideal sein. Es gibt also endlich viele maximale Ideale $\mathfrak{m}_i$, $i = 1, \ldots, n$ und $r_i \in R$ mit

$$r_1 f_1 + \cdots + r_n f_n = 1,$$

wobei $f_i = f_{\mathfrak{m}_i}$ gesetzt wurde. Damit ist

$$q = \frac{a_1}{f_1} = \ldots = \frac{a_n}{f_n}.$$

Wir schreiben

$$q = q(r_1 f_1 + \cdots + r_n f_n) = q r_1 f_1 + \cdots + q r_n f_n = a_1 r_1 + \cdots + a_n r_n.$$

Also gehört q zu R. □

Lemma 4.17. *Es sei R ein kommutativer Ring und sei $\mathfrak{p}$ ein Primideal. Dann ist der Quotientenkörper des Restklassenringes $R/\mathfrak{p}$ in natürlicher Weise isomorph zum Restekörper der Lokalisierung $R_{\mathfrak{p}}$. Es ist also*

$$Q(R/\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

Beweis. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccccc} R & \longrightarrow & R/\mathfrak{p} & \longrightarrow & Q(R/\mathfrak{p}) \\ \downarrow & & \varphi \downarrow & & \downarrow \psi \\ R_{\mathfrak{p}} & \longrightarrow & R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} & \longrightarrow & R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \end{array}$$

von Ringhomomorphismen, wobei φ und ψ zu konstruieren sind. Unter dem Ringhomomorphismus

$$R \longrightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$$

wird das Primideal $\mathfrak{p}$ auf 0 abgebildet, der Ringhomomorphismus φ ergibt sich als induzierter Homomorphismus. Unter φ werden Elemente $[r] \in R/\mathfrak{p}$, $[r] \neq 0$, die also durch $r \notin \mathfrak{p}$ repräsentiert werden, auf Einheiten abgebildet. Somit gibt es nach Lemma 4.11 eine Fortsetzung auf den Quotientenkörper

$$\psi\colon\ Q(R/\mathfrak{p}) \longrightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

Diese ist als Ringhomomorphismus zwischen Körpern injektiv. Ein Element des Restekörpers, das in der Lokalisierung $R_{\mathfrak{p}}$ durch r/s mit $s \notin \mathfrak{p}$ repräsentiert wird, wird unter ψ durch das Element $[r]/[s]$ getroffen (beachte $[s] \neq 0$). □

Der Restekörper zu einem Primideal $\mathfrak{p}$ wird mit $\kappa(\mathfrak{p})$ bezeichnet. Wenn $\mathfrak{m}$ ein maximales Ideal ist, so ist insbesondere der Restklassenkörper $R/\mathfrak{m}$ gleich dem Restklassenkörper der Lokalisierung $R_{\mathfrak{m}}$.

4. Arbeitsblatt

4.1. **Aufgaben.**

Aufgabe 4.1. Es sei R ein kommutativer Ring und I ein Ideal. Zeige, dass $\{1+x \mid x \in I\}$ ein multiplikatives System in R ist.

Aufgabe 4.2.* Es sei R ein kommutativer Ring, $S \subseteq R$ ein multiplikatives System und $I \subseteq R$ ein Ideal. Zeige, dass

$$J := \{f \in R \mid \text{Es gibt ein } s \in S \text{ mit } sf \in I\}$$

ein Ideal in R ist, dass I umfasst.

Aufgabe 4.3. Es sei $Y \subseteq \mathbb{R}$ eine fixierte Teilmenge. Zeige, dass die Menge

$$S = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ stetig, } f \text{ besitzt in } T \text{ keine Nullstelle}\}$$

ein multiplikatives System im Ring der stetigen Funktionen auf $\mathbb{R}$ ist.

Ein multiplikatives System S in einem kommutativen Ring R heißt *saturiert*, wenn folgendes gilt: Ist $g \in R$ und gibt es ein $f \in S$, das von g geteilt wird, so ist auch $g \in S$.

Sei R ein kommutativer Ring. Ein multiplikatives System $F \subseteq R$ nennt man einen *Ultrafilter*, wenn $0 \notin F$ ist und wenn F maximal mit dieser Eigenschaft ist.

Aufgabe 4.4. Es sei R ein kommutativer Ring. Zeige, dass die Menge der Nichtnullteiler in R ein saturiertes multiplikatives System bilden.

Aufgabe 4.5. Seien A, B kommutative Ringe und sei $\varphi : A \to B$ ein Ringhomomorphismus . Zeige, dass das Urbild $\varphi^{-1}(B^\times)$ der Einheitengruppe ein saturiertes multiplikatives System in A ist.

Aufgabe 4.6. Es sei R ein kommutativer Ring und sei $F \subseteq R$ ein multiplikatives System mit $0 \notin F$. Zeige, dass F genau dann ein Ultrafilter ist, wenn es zu jedem $g \in R$, $g \notin F$, ein $f \in F$ und eine natürliche Zahl n mit $fg^n = 0$ gibt.

Aufgabe 4.7. Sei R ein kommutativer Ring und sei $F \subset R$ ein Ultrafilter. Zeige, dass das Komplement von F ein minimales Primideal in R ist.

Aufgabe 4.8. Es sei R ein kommutativer Ring, $\mathfrak{a} \subseteq R$ ein Ideal und $M \subseteq R$ ein multiplikatives System mit $\mathfrak{a} \cap M = \emptyset$. Zeige mit dem Lemma von Zorn, dass es dann auch ein Primideal $\mathfrak{p}$ mit $\mathfrak{a} \subseteq \mathfrak{p}$ und mit $\mathfrak{p} \cap M = \emptyset$ gibt.

Aufgabe 4.9. Es sei R ein kommutativer Ring und $S \subseteq R$ ein multiplikatives System. Zeige, dass die Überkreuzrelation auf der Produktmenge $R \times S$ eine Äquivalenzrelation ist, und dass für die Äquivalenzklassen $\frac{r}{s} := [(r,s)]$ durch

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

eine wohldefinierte Addition und durch

$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$$

eine wohldefinierte Multiplikation gegeben ist, derart, dass die Quotientenmenge ein kommutativer Ring wird.

Aufgabe 4.10. Es sei R ein Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System, $0 \notin S$.

(1) Zeige, dass die Nenneraufnahme zu S, also R_S mit

$$R_S := \left\{ \frac{f}{g} \mid f \in R,\, g \in S \right\} \subseteq Q(R)$$

ein Unterring von $Q(R)$ ist.

(2) Zeige, dass nicht jeder Unterring von $Q(R)$ eine Nenneraufnahme ist.

Aufgabe 4.11. Es sei $T \subseteq \mathbb{P}$ eine Teilmenge der Primzahlen. Zeige, dass die Menge

$$R_T = \{q \in \mathbb{Q} \mid q \text{ lässt sich mit einem Nenner schreiben, in dem nur Primzahlen aus } T \text{ vorkommen}\}$$

ein Unterring von $\mathbb{Q}$ ist. Was ergibt sich bei $T = \emptyset$, $T = \{3\}$, $T = \{2,5\}$, $T = \mathbb{P}$?

Aufgabe 4.12. Es sei $R = \mathbb{Z}[\frac{2}{3}]$ der von $\mathbb{Z}$ und $2/3$ erzeugte Unterring von $\mathbb{Q}$. Zeige, dass R alle rationalen Zahlen enthält, die sich mit einer Potenz von 3 im Nenner schreiben lassen.

Aufgabe 4.13. Sei R ein kommutativer Ring und sei $f \in R$ mit zugehöriger Nenneraufnahme R_f. Beweise die R-Algebraisomorphie

$$R_f \cong R[T]/(Tf - 1).$$

Aufgabe 4.14. Es sei R ein kommutativer Ring und $f, g \in R$ Elemente. Zeige, dass die folgenden Eigenschaften äquivalent sind.

(1) Es ist $D(f) \subseteq D(g)$ (im Spektrum von R).
(2) Es ist $\operatorname{rad}((f)) \subseteq \operatorname{rad}((g))$.
(3) Es ist $f \in \operatorname{rad}((g))$.
(4) Es gibt $n \in \mathbb{N}$ mit $f^n \in (g)$
(5) Das Element g teilt eine Potenz von f.
(6) Es ist g eine Einheit in R_f.
(7) Es gibt einen R-Algebrahomomorphismus $R_g \to R_f$.

Aufgabe 4.15. Sei R ein kommutativer Ring, $f \in R$ ein Element und R_f die zugehörige Nenneraufnahme. Zeige, dass f genau dann nilpotent ist, wenn R_f der Nullring ist.

Aufgabe 4.16. Es sei R ein Hauptidealbereich mit Quotientenkörper $Q = Q(R)$. Zeige, dass jeder Zwischenring S, $R \subseteq S \subseteq Q$, eine Nenneraufnahme ist.

Aufgabe 4.17. Zeige, dass $\mathbb{Q}$ keine Algebra von endlichem Typ über $\mathbb{Z}$ ist.

Aufgabe 4.18. Sei R ein Integritätsbereich und $S \subseteq R$ ein multiplikatives System. Zeige, dass die Primideale in R_S genau denjenigen Primidealen in R entsprechen, die mit S einen leeren Durchschnitt haben.

Aufgabe 4.19. Sei R ein kommutativer Ring, sei $f \in R$ und sei $\mathfrak{a}$ ein Ideal. Zeige, dass $f \in \mathfrak{a}$ genau dann gilt, wenn für alle Lokalisierungen $R_{\mathfrak{p}}$ gilt, dass $f \in \mathfrak{a}R_{\mathfrak{p}}$ ist.

Aufgabe 4.20. Es sei R ein kommutativer Ring, $\mathfrak{a} \subseteq R$ ein Ideal und $S \subseteq R$ ein multiplikatives System. Zeige, dass es eine natürliche Ringisomorphie

$$(R/\mathfrak{a})_S = R_S/\mathfrak{a}R_S$$

gibt, wobei links die Nenneraufnahme am Bild des multiplikativen Systems in $R/\mathfrak{a}$ bezeichnet.

Aufgabe 4.21. Es sei R ein kommutativer Ring, $\mathfrak{a} \subseteq R$ ein Ideal und $S \subseteq R$ ein multiplikatives System. In der Nenneraufnahme R_S gelte

$$\mathfrak{a}R_S = (f_1, \ldots, f_n).$$

Zeige, dass es ein $g \in S$ und Elemente $a_1, \ldots, a_n \in R$ mit

$$\mathfrak{a}R_g = (a_1, \ldots, a_n)$$

gibt.

Aufgabe 4.22.*

Man gebe ein Beispiel einer integren, endlich erzeugten $\mathbb{C}$-Algebra R und eines multiplikativen Systems $S \subseteq R$, $0 \notin S$, an derart, dass die Nenneraufnahme R_S kein Körper ist, aber jedes maximale Ideal aus R zum Einheitsideal in R_S wird.

Aufgabe 4.23. Bestimme die Unterringe der rationalen Zahlen $\mathbb{Q}$, die lokal sind.

Aufgabe 4.24. Sei R ein kommutativer Ring. Zeige die Äquivalenz folgender Aussagen.

(1) R hat genau ein maximales Ideal
(2) Die Menge der Nichteinheiten $R \setminus R^\times$ bildet ein Ideal in R.

Aufgabe 4.25. Sei R ein lokaler Ring mit Restekörper K. Zeige, dass R und K genau dann die gleiche Charakteristik haben, wenn R einen Körper enthält.

Aufgabe 4.26. Es sei R ein kommutativer Ring und

$$\varphi\colon R \longrightarrow K$$

ein Ringhomomorphismus in einen Körper K. Zeige, dass es eine eindeutig bestimmte Faktorisierung

$$R \longrightarrow \kappa(\mathfrak{p}) \longrightarrow K$$

mit einem Restekörper $\kappa(\mathfrak{p})$ zu einem Primideal $\mathfrak{p}$ gibt.

Aufgabe 4.27.*

Es sei R ein lokaler Ring und $\mathfrak{a}$ ein Ideal von R. Zeige, dass

$$R^\times \longrightarrow (R/\mathfrak{a})^\times$$

surjektiv ist.

Aufgabe 4.28. Es sei

$$\varphi\colon\ R \longrightarrow S$$

ein Ringhomomorphismus zwischen den kommutativen Ringen R und S und es sei $\mathfrak{p} \in \operatorname{Spek}(S)$ ein Primideal. Zeige, dass es natürliche Ringhomomorphismen

$$R_{\varphi^{-1}(\mathfrak{p})} \longrightarrow S_{\mathfrak{p}}$$

(zwischen den Lokalisierungen) und

$$\kappa\big(\varphi^{-1}(\mathfrak{p})\big) \longrightarrow \kappa(\mathfrak{p})$$

(zwischen den Restekörpern) gibt.

Aufgabe 4.29. Sei R ein kommutativer Ring, $S \subseteq R$ ein multiplikatives System und M ein R-Modul. Definiere die „Nenneraufnahme“

$$M_S$$

und zeige, dass sie ein R_S-Modul ist.

5. Vorlesung - Endliche Körpererweiterungen

5.1. Das Spektrum unter Ringhomomorphismen.

Wir untersuchen, wie sich das Spektrum eines kommutativen Ringes unter einem Ringhomomorphismus verhält.

Proposition 5.1. *Es sei $\varphi\colon R \to S$ ein Ringhomomorphismus zwischen kommutativen Ringen. Dann gelten folgende Aussagen.*

(1) *Die Zuordnung*

$$\varphi^*\colon\ \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R),\ \mathfrak{p} \longmapsto \varphi^*(\mathfrak{p}) := \varphi^{-1}(\mathfrak{p}),$$

ist (wohldefiniert und) stetig.

(2) *Es ist $(\varphi^*)^{-1}(D(\mathfrak{a})) = D(\mathfrak{a}S)$ für jedes Ideal $\mathfrak{a} \subseteq R$.*

(3) *Für einen weiteren Ringhomomorphismus*

$$\psi\colon\ S \longrightarrow T$$

gilt $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Beweis. Die Abbildung ist nach Aufgabe 5.1 wohldefiniert. Zur Stetigkeit ist die Aussage (2) zu zeigen. Wir argumentieren mit den abgeschlossenen Mengen. Für ein Primideal $\mathfrak{q} \in \operatorname{Spek}(S)$ ist $\varphi^*(\mathfrak{q}) \in V(\mathfrak{a})$ genau dann, wenn $\mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{q})$ ist. Dies ist äquivalent zu $\varphi(\mathfrak{a}) \subseteq \mathfrak{q}$ und ebenso zu $\mathfrak{a}S \subseteq \mathfrak{q}$. (3) ist klar. □

Die in der vorstehenden Aussage eingeführte stetige Abbildung heißt *Spektrumsabbildung* (zu dem gegebenen Ringhomomorphismus). Bei einem Unterring

$$R \subseteq S$$

geht es einfach um die Zuordnung $\mathfrak{p} \mapsto \mathfrak{p} \cap R$. In diesem Fall spricht man auch von „Runterschneiden“.

Beispiel 5.2. Es sei K ein Körper und $P \in K[X]$ ein Polynom in einer Variablen. Wir betrachten den zugehörigen Ringhomomorphismus

$$K[Y] \longrightarrow K[X],\, Y \longmapsto P.$$

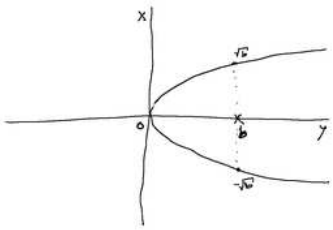
Das Urbild zu einem linearen Primideal $(X-a) \in K[X]$ ist das Primideal $(Y-P(a)) \in K[Y]$. Dies sieht man am einfachsten, wenn man die Hintereinanderschaltung

$$K[Y] \longrightarrow K[X] \xrightarrow{\mathrm{Ev}_a} K$$

betrachtet, die die Evaluation an $P(a)$ ist, und die Kerne beachtet. Deshalb liegt das kommutatives Diagramm

$$\begin{array}{ccc} K & \longrightarrow & \mathrm{Spek}\,(K[X]) \\ P\downarrow & & \downarrow \\ K & \longrightarrow & \mathrm{Spek}\,(K[Y]) \end{array}$$

vor, wobei in den Horizontalen die Zuordnungen $a \mapsto (X-a)$ bzw. $b \mapsto (Y-b)$ stehen und rechts die Spektrumsabbildung steht. Die Spektrumsabbildung ist also eine natürliche Erweiterung der durch das Polynom P direkt definierten Abbildung von K nach K, die zusätzlich noch alle Primideale berücksichtigt.

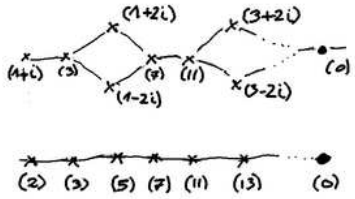


Sieht aus wie die Wurzel, soll aber die Quadrierung sein. Die Quadratabbildung sieht man, wenn man ausgehend von der hier vertikalen x-Achse horizontal auf den Graphen geht und dann nach unten projiziert. Diese Sichtweise betont, wie die Fasern zu variierendem b aussieht.

Im zahlentheoretischen Kontext betrachtet man meist eine Ringerweiterung $\mathbb{Z} \subseteq R$, ein Primideal aus R wird dabei unter der Spektrumsabbildung entweder auf das Nullideal (0) abgebildet oder aber auf ein Primhauptideal (p) zu einer Primzahl p. Diese Abbildung kann man auf zwei Arten versuchen zu verstehen, erstens, indem man die Primideale von R versucht zu verstehen und dann zu bestimmen, wohin diese abgebildet werden, oder aber zweitens, und dies ist im zahlentheoretischen Kontext produktiver, dadurch, dass man

versucht zu verstehen, welche Primideale oberhalb von (p) liegen. Diese Frage hängt unmittelbar mit der Frage zusammen, was mit der Primzahl p in der Ringerweiterung R geschieht, ob es eine Primzahl bleibt oder ob und wie es zerfällt. Die Faser über (p) ist direkt (siehe unten) die Menge der Primideale des Restklassenringes $R/(p)$, und dies ist bei einer ganzen Erweiterung ein endlicher Ring.

Beispiel 5.3. Zur Erweiterung $\mathbb{Z} \subseteq \mathbb{Z}[\mathrm{i}]$ stellt man sich die Spekrumsabbildung $\operatorname{Spek}(\mathbb{Z}[\mathrm{i}]) \to \operatorname{Spek}(\mathbb{Z})$ so vor, dass man zu einer Primzahl $p \in \mathbb{Z}$ versucht zu verstehen, welche Primideale in $\mathbb{Z}[\mathrm{i}]$ die Zahl p enthalten. Dabei entsteht das Bild unten.



Proposition 5.4. *Es sei R ein kommutativer Ring. Dann gelten folgende Aussagen.*

(1) *Zu einem Ideal $\mathfrak{a} \subseteq R$ und der Restklassenabbildung*

$$q\colon\ R \longrightarrow R/\mathfrak{a}$$

ist die Spektrumsabbildung

$$q^*\colon\ \operatorname{Spek}(R/\mathfrak{a}) \longrightarrow \operatorname{Spek}(R)$$

eine abgeschlossene Einbettung, deren Bild $V(\mathfrak{a})$ ist.

(2) *Zu einem multiplikativen System $M \subseteq R$ ist die zur kanonischen Abbildung*

$$\iota\colon\ R \longrightarrow R_M$$

gehörige Abbildung

$$\iota^*\colon\ \operatorname{Spek}(R_M) \longrightarrow \operatorname{Spek}(R)$$

injektiv, und das Bild besteht aus der Menge der Primideale von R, die zu M disjunkt sind.

(3) *Zu $f \in R$ ist die zur kanonischen Abbildung*

$$\iota\colon\ R \longrightarrow R_f$$

gehörige Abbildung

$$\iota^*\colon\ \operatorname{Spek}(R_f) \longrightarrow \operatorname{Spek}(R)$$

eine offene Einbettung, deren Bild gleich $D(f)$ ist.

Beweis. (1) folgt aus Aufgabe 3.13: Die Primideale in $R/\mathfrak{a}$ entsprechen über $\mathfrak{p} \mapsto q^{-1}(\mathfrak{p}) = \mathfrak{p} + \mathfrak{a}$ den Primidealen von R, die $\mathfrak{a}$ enthalten. Die angegebene Abbildung ist also bijektiv und hat das beschriebene Bild. Zu einem Ideal $\mathfrak{b} \subseteq R/\mathfrak{a}$ und einem Primideal $\mathfrak{p} \subseteq R/\mathfrak{a}$ ist genau dann $\mathfrak{b} \subseteq \mathfrak{p}$, wenn

$$\mathfrak{b} + \mathfrak{a} = q^{-1}(\mathfrak{b}) \subseteq \mathfrak{p} + \mathfrak{a}$$

gilt. Also ist das Bild von $V(\mathfrak{b})$ gleich $V(\mathfrak{b}+\mathfrak{a})$ und damit abgeschlossen. Für (2) siehe Aufgabe 4.18. (3). Da für ein Primideal $\mathfrak{p}$ und ein Element $f \in R$ die Beziehung $f \notin \mathfrak{p}$ genau dann gilt, wenn $\mathfrak{p}$ zum multiplikativen System $\{f^n \mid n \in \mathbb{N}\}$ disjunkt ist, folgt aus Teil (2), dass die Abbildung injektiv ist und dass ihr Bild gleich $D(f)$ ist. Das gleiche Argument, angewendet auf $g \in R$ bzw. $\frac{g}{1} \in R_f$ zeigt, dass das Bild von $D(g) \subseteq \operatorname{Spek}(R_f)$ gleich $D(fg)$ und damit offen ist. □

Lemma 5.5. *Es sei $\varphi\colon R \to S$ ein Ringhomomorphismus zwischen zwei kommutativen Ringen und es sei*

$$\varphi^*\colon \operatorname{Spek}(S) \longrightarrow \operatorname{Spek}(R),\ \mathfrak{p} \longmapsto \varphi^*(\mathfrak{p}),$$

die zugehörige Spektrumsabbildung. Dann ist die Faser über einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ gleich $\operatorname{Spek}\left((S/\mathfrak{q}S)_{\varphi(R\setminus\mathfrak{q})}\right)$. D.h. die Faser besteht aus allen Primidealen $\mathfrak{p} \in \operatorname{Spek}(S)$ mit $\mathfrak{q}S \subseteq \mathfrak{p}$ und mit $\mathfrak{p} \cap \varphi(R \setminus \mathfrak{q}) = \emptyset$.

Beweis. Aufgrund von Proposition 5.4 müssen wir nur die zweite Formulierung beweisen. Für ein Primideal $\mathfrak{p} \subseteq S$ gilt $\varphi^{-1}(\mathfrak{p}) = \mathfrak{q}$ genau dann, wenn sowohl $\varphi(\mathfrak{q}) \subseteq \mathfrak{p}$ als auch $\varphi(R \setminus \mathfrak{q}) \subseteq S \setminus \mathfrak{p}$ gilt. Die erste Bedingung ist zu $\mathfrak{q}S \subseteq \mathfrak{p}$ und die zweite Bedingung ist zu

$$\varphi(R \setminus \mathfrak{q}) \cap \mathfrak{p} = \emptyset$$

äquivalent. □

Insbesondere ist die Faser eines Spektrumsmorphismus über einem Punkt selbst wieder das Spektrum eines Ringes. Ein Spezialfall der vorstehenden Aussage ist, dass die Faser über einem maximalen Ideal $\mathfrak{m}$ gleich $\operatorname{Spek}(S/\mathfrak{m}S)$ ist, da in diesem Fall aus $\mathfrak{m}S \subseteq \mathfrak{p}$ sofort $\mathfrak{m} \subseteq \varphi^{-1}(\mathfrak{p})$ folgt und wegen der Maximalität Gleichheit gelten muss. Bei einem Integritätsbereich R und dem Nullideal erübrigt es sich, das Erweiterungsideal zu betrachten, die Faser wird einfach durch $\operatorname{Spek}\left(S_{\varphi(R\setminus\{0\})}\right)$ beschrieben.

Definition 5.6. Zu einem Ringhomomorphismus $\varphi\colon R \to S$ zwischen kommutativen Ringen und einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ nennt man

$$(S/\mathfrak{q}S)_{\varphi(R\setminus\mathfrak{q})}$$

den *Faserring* über $\mathfrak{q}$.

Die Aussage Lemma 5.5 bedeutet also, dass die Faser der Spektrumsabbildung über $\mathfrak{q}$ gleich dem Spektrum des Faserringes ist. Der Faserring beinhaltet dabei eine genauere algebraische Information, aus der die topologische

und mengentheoretische Information ablesbar ist. Wenn $\mathfrak{q}$ ein maximales Ideal von R ist, so braucht man die Nenneraufnahme nicht, der Faserring ist dann einfach gleich $S/\mathfrak{q}S$. Den Faserring kann man allgemein auch als $S \otimes_R \kappa(\mathfrak{q})$ realisieren.

Bemerkung 5.7. Wenn ein Ringhomomorphismus in der Form

$$R \longrightarrow R[X_1, \ldots, X_n]/(F_1, \ldots, F_s)$$

vorliegt, so wird der Faserring über einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ durch

$$\left(R/\mathfrak{q}[X_1, \ldots, X_n]/(\overline{F}_1, \ldots, \overline{F}_s)\right)_{\varphi(R\setminus\mathfrak{q})}$$

beschrieben, wobei $\overline{F}_j$ die Reduktion von F_j modulo $\mathfrak{q}$ bezeichnet. Dies bedeutet einfach, dass man die Koeffizienten der Polynome modulo $\mathfrak{q}$ interpretiert.

Bei $R = \mathbb{Z}$ und $S = \mathbb{Z}[X]/(F)$ und einem maximalen Ideal (p) zu einer Primzahl p ist der Faserring einfach $\mathbb{Z}/(p)[X]/(\overline{F})$. Dies ist also eine Algebra über dem endlichen Körper $\mathbb{Z}/(p)$. Wenn F ein normiertes Polynom vom Grad d ist, so ist diese Algebra endlich mit p^d Elementen, die man allein schon wegen der Endlichkeit explizit beschreiben kann. Wenn F über $\mathbb{Z}$ irreduzibel ist, so muss aber $\overline{F}$ nicht unbedingt irreduzibel sein. In der Tat ist es so, dass p genau dann ein Primelement in S bleibt, wenn $\overline{F}$ irreduzibel in $(\mathbb{Z}/(p))[X]$ ist. Genau in diesem Fall ist der Faserring ein Körper.

5.2. **Endliche Körpererweiterungen.**

Wir rekapitulieren nun die wichtigsten Ergebnisse der Körper- und Galoistheorie. In der Zahlentheorie geht man von einer endlichen Körpererweiterung $\mathbb{Q} \subseteq L$ aus, wobei L typischerweise durch die Hinzunahme gewisser algebraischer Zahlen definiert ist, und überlegt dann, was dies für die „entsprechende“ Erweiterung für $\mathbb{Z}$ bedeutet. Dabei greift man immer wieder auf die Körpererweiterung zurück.

Definition 5.8. Seien R und A kommutative Ringe und sei $R \to A$ ein fixierter Ringhomomorphismus. Dann nennt man A eine *R-Algebra*.

Jeder Ring ist in eindeutiger Weise eine $\mathbb{Z}$-Algebra. Der Polynomring $K[X]$ ist eine K-Algebra. Wenn ein Unterring $R \subseteq S$ vorliegt, so ist insbesondere S eine R-Algebra. Bei eine Unterringbeziehung $K \subseteq L$ zwischen Körpern spricht man von einem Unterkörper und einem Erweiterungskörper.

Definition 5.9. Sei L ein Körper und $K \subseteq L$ ein Unterkörper von L. Dann heißt L ein *Erweiterungskörper* (oder *Oberkörper*) von K und die Inklusion $K \subseteq L$ heißt eine *Körpererweiterung*.

Bei einer R-Algebra A ist A insbesondere ein R-Modul, siehe Aufgabe 5.10. Speziell ist bei einer Körpererweiterung $K \subseteq L$ der Erweiterungskörper L ein K-Vektorraum. Dies erlaubt es, Begriffe aus der linearen Algebra in dieser Situation anzuwenden.

Definition 5.10. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlichdimensionaler Vektorraum über K ist.

Definition 5.11. Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.

Der Grad einer endlichen Körpererweiterung $K \subseteq L$ wird mit

$$\operatorname{grad}_K L$$

bezeichnet. Dass man hier von Grad spricht und nicht einfach von Dimension hat seinen Grund darin, dass dieser Grad mit dem Grad von gewissen Polynomen zusammenhängt, worauf wir ausführlich zu sprechen kommen werden. Da bei einer Körpererweiterung $K \subseteq L$ sofort eine K-Vektorraumstruktur auf L zur Verfügung steht, ist es naheliegend, für das Studium der Körpererweiterungen die lineare Algebra einzusetzen. Dies ist besonders bei endlichen Körpererweiterungen ein schlagkräftiges Mittel. Durch diesen Apparat wird unter Anderem die additive Struktur auf L einfach beschreibbar, und man kann sich ganz auf die Multiplikation konzentrieren. Aber auch für diese ist die Vektorraumstruktur reich an Konsequenzen. Um ein typisches Beispiel für die lineare Argumentationsweise zu geben, betrachten wir eine endliche Körpererweiterung $K \subseteq L$ und ein beliebiges Element $x \in L$. Die Potenzen von x, also

$$x^0 = 1, x^1 = x, x^2, x^3, \ldots$$

bilden eine unendliche Familie (auch wenn es unter den Potenzen Wiederholungen geben kann). Da diese Potenzen alle zu L gehören und L ein endlichdimensionaler K-Vektorraum ist, kann diese unendliche Familie nicht linear unabhängig sein, sondern es muss eine Beziehung der Form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

geben, bei der nicht alle Koeffizienten $a_i \in K$ gleich 0 sind. Diese Beobachtung führt zu den Begriffen *algebraisches Element* und *Minimalpolynom*.

Definition 5.12. Es sei K ein Körper und A eine kommutative K-Algebra. Es sei $f \in A$ ein Element. Dann heißt f *algebraisch* über K, wenn es ein von 0 verschiedenes Polynom $P \in K[X]$ mit $P(f) = 0$ gibt.

Definition 5.13. Es sei K ein Körper und A eine K-Algebra. Es sei $f \in A$ ein über K algebraisches Element. Dann heißt das normierte Polynom $P \in K[X]$ mit $P(f) = 0$, welches von minimalem Grad mit dieser Eigenschaft ist, das *Minimalpolynom* von f.

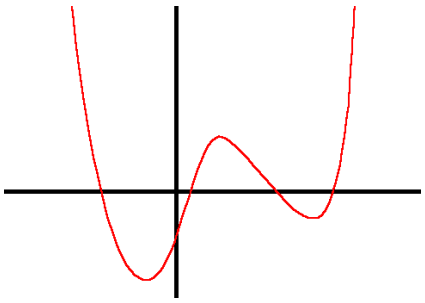
5.3. **Galoiserweiterungen.**

Wir erwähnen hier ohne Beweis einige Hauptresultate über die Galoisgruppe und Galoiserweiterungen.

Definition 5.14. Es sei $K \subseteq L$ eine Körpererweiterung. Dann nennt man die Automorphismengruppe

$$\operatorname{Gal}(L|K) = \operatorname{Aut}_K(L)$$

die *Galoisgruppe* der Körpererweiterung.



Unter einem K-Körperautomorphismus φ muss ein Element $x \in L$, dass Nullstelle eines Polynoms F aus $K[X]$ ist, auf eine Nullstelle dieses Polynoms abgebildet werden. Das schränkt die Möglichkeiten wesentlich ein.

Es ist eine grundlegende Frage, welche Eigenschaften eines Elementes $x \in L$ unter einem K-Algebraautomorphismus erhalten bleiben und welche nicht.

Lemma 5.15. *Es sei $K \subseteq L$ eine Körpererweiterung, $x \in L$, $F \in K[X]$ ein Polynom mit $F(x) = 0$ und sei $\varphi \in \operatorname{Gal}(L|K)$. Dann ist auch $F(\varphi(x)) = 0$.*

Satz 5.16. *Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist die Galoisgruppe $\operatorname{Gal}(L|K)$ endlich.*

Aus dem Lemma von Dedekind ergibt sich eine direkte Abschätzung zwischen der Ordnung der Galoisgruppe und dem Grad einer endlichen Körpererweiterung.

Satz 5.17. *Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist*

$$\#(\operatorname{Gal}(L|K)) \leq \operatorname{grad}_K L.$$

Eine wichtige Frage ist, wann in der vorstehenden Abschätzung Gleichheit vorliegt, wann es also so viele Automorphismen wie möglich gibt. Dies machen wir zur Grundlage der folgenden Definition. Es gibt eine Vielzahl an dazu äquivalenten Eigenschaften.

Definition 5.18. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Sie heißt eine *Galoiserweiterung*, wenn

$$\#(\operatorname{Gal}(L|K)) = \operatorname{grad}_K L$$

gilt.

5.4. **Endliche Körper.**

Wir erwähnen eine wichtige Besonderheit für Ringe in positiver Charakteristik.

Definition 5.19. Es sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte. Der *Frobeniushomomorphismus* ist der Ringhomomorphismus

$$R \longrightarrow R,\, f \longmapsto f^p.$$

Wir fassen die wichtigsten Resultate über endliche Körper ohne Beweise zusammen. Für Beweise siehe den Kurs über Galoistheorie.

Satz 5.20. *Es sei p eine Primzahl und $e \in \mathbb{N}_+$. Dann gibt es bis auf Isomorphie genau einen Körper mit $q = p^e$ Elementen.*

Notation 5.21. Sei p eine Primzahl und $e \in \mathbb{N}_+$. Der aufgrund von Satz 5.20 bis auf Isomorphie eindeutig bestimmte endliche Körper mit $q = p^e$ Elementen wird mit

$$\mathbb{F}_q$$

bezeichnet.

Lemma 5.22. *Es sei L ein endlicher Körper der Charakteristik p. Dann ist der Frobeniushomomorphismus*

$$\Phi\colon\, L \longrightarrow L,\, x \longmapsto x^p,$$

ein Automorphismus, dessen Fixkörper $\mathbb{Z}/(p)$ ist.

Satz 5.23. *Es sei p eine Primzahl und $m \in \mathbb{N}$, $q = p^m$. Dann ist die Körpererweiterung $\mathbb{F}_p \subseteq \mathbb{F}_q$ eine Galoiserweiterung mit einer zyklischen Galoisgruppe der Ordnung m, die vom Frobeniushomomorphismus erzeugt wird.*

5. Arbeitsblatt

5.1. **Aufgaben.**

Aufgabe 5.1. Seien R und S kommutative Ringe und sei $\varphi : R \to S$ ein Ringhomomorphismus. Sei $\mathfrak{p}$ ein Primideal in S. Zeige, dass das Urbild $\varphi^{-1}(\mathfrak{p})$ ein Primideal in R ist.

Zeige durch ein Beispiel, dass das Urbild eines maximalen Ideales kein maximales Ideal sein muss.

Aufgabe 5.2. Zeige, dass die Spektrumsabbildung zur Reduktion

$$R \longrightarrow R/\mathfrak{n}_R$$

eines kommutativen Ringes R eine Homöomorphie ist.

Aufgabe 5.3. Beschreibe das Spektrum $\operatorname{Spek}(R_{\mathfrak{p}})$ einer Lokalisierung eines kommutativen Ringes R an einem Primideal $\mathfrak{p}$.

Aufgabe 5.4.*

Bestimme für die Ringerweiterung

$$\mathbb{Z} \subseteq R = \mathbb{Z}[X]/\left(X^3+2X-1\right)$$

die Faserringe zu den Primzahlen $p = 2,3,5,11$. Bestimme insbesondere, ob sie reduziert sind, ob ein Körper vorliegt, wie viele Primideale sie enthalten und wie die Restekörper aussehen.

Zur vorstehenden Aufgabe vergleiche auch Aufgabe 18.9.

Aufgabe 5.5. Sei $R = \mathbb{Z}[X]/(X^4+X^3+X^2+X+1)$. Bestimme die Primideale in R, die über den Primzahlen $p = 2,3,5,7$ liegen.

Aufgabe 5.6. Es sei R ein kommutativer Ring. Bestimme die Fasern zur Spektrumsabbildung zur Ringerweiterung $R \subseteq R[X_1,\ldots,X_n]$.

Aufgabe 5.7.*

Sei K ein Körper und seien R und S integre, endlich erzeugte K-Algebren. Es sei

$$\varphi\colon R \longrightarrow S$$

ein K-Algebrahomomorphismus und $\mathfrak{n}$ ein maximales Ideal in S mit $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$. Die Abbildung induziere einen Isomorphismus $R_{\mathfrak{m}} \to S_{\mathfrak{n}}$. Zeige, dass es dann auch ein $f \in R$, $f \notin \mathfrak{m}$, gibt derart, dass $R_f \to S_{\varphi(f)}$ ein Isomorphismus ist.

Aufgabe 5.8. Sei R ein kommutativer Ring und sei $\mathfrak{m}$ ein maximales Ideal mit Lokalisierung $R_{\mathfrak{m}}$. Es sei $\mathfrak{a}$ ein Ideal, dass unter der Lokalisierungsabbildung zum Kern gehört. Zeige, dass dann $R_{\mathfrak{m}}$ auch eine Lokalisierung von $R/\mathfrak{a}$ ist.

Aufgabe 5.9. Bestimme die Fasern der Spektrumsabbildung zu $\mathbb{R}[X] \subseteq \mathbb{C}[X]$.

Aufgabe 5.10. Bestimme die Fasern der Spektrumsabbildung zu $\mathbb{Q}[X] \subseteq \mathbb{R}[X]$. Welche sind endlich?

Aufgabe 5.11. Seien R und A kommutative Ringe. Zeige, dass A genau dann eine R-Algebra ist, wenn A ein R-Modul ist, für den zusätzlich

$$r(ab) = (ra)b \text{ für alle } r \in R,\, a, b \in A$$

gilt.

Aufgabe 5.12. Sei G eine kommutative Gruppe. Zeige, dass G auf genau eine Weise die Struktur eines $\mathbb{Z}$-Moduls trägt. Kommutative Gruppen und $\mathbb{Z}$-Moduln sind also äquivalente Objekte.

Aufgabe 5.13.*

Es sei V ein Modul über dem kommutativen Ring R. Es seien $s_1, \ldots, s_k \in R$ und $v_1, \ldots, v_n \in V$. Zeige

$$\left(\sum_{i=1}^{k} s_i\right) \cdot \left(\sum_{j=1}^{n} v_j\right) = \sum_{1 \leq i \leq k,\, 1 \leq j \leq n} s_i \cdot v_j.$$

Aufgabe 5.14. Sei R ein kommutativer Ring, M und N zwei R-Moduln und sei

$$\varphi\colon\ M \longrightarrow N$$

ein Modulhomomorphismus. Zeige die folgenden Aussagen.

(1) Für einen R-Untermodul $S \subseteq M$ ist auch das Bild $\varphi(S)$ ein Untermodul von N.
(2) Insbesondere ist das Bild $\operatorname{bild}\varphi = \varphi(M)$ der Abbildung ein Untermodul von N.
(3) Für einen Untermodul $T \subseteq N$ ist das Urbild $\varphi^{-1}(T)$ ein Untermodul von M.
(4) Insbesondere ist der Kern $\varphi^{-1}(0)$ ein Untermodul von M.

Aufgabe 5.15.*

Es sei $K \subseteq L$ eine Körpererweiterung. Zeige, dass L ein K-Vektorraum ist.

Aufgabe 5.16.*

Bestimme den Grad der Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$.

Aufgabe 5.17. Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad 1. Zeige, dass $L = K$ ist.

Aufgabe 5.18. Es sei L ein Körper und sei

$$\varphi\colon\ L \longrightarrow L$$

ein Automorphismus. Zeige, dass die Einschränkung von φ auf den Primkörper von L die Identität ist.

Aufgabe 5.19. Bestimme in $\mathbb{Q}[\sqrt{7}]$ das Inverse von $2+5\sqrt{7}$.

Aufgabe 5.20. Es sei $K \subseteq L$ eine endliche Körpererweiterung und seien $v_1, \ldots, v_n \in L$ Elemente, die eine K-Basis von L bilden. Sei $x \in L$, $x \neq 0$. Zeige, dass auch $xv_1, \ldots, xv_n \in L$ eine K-Basis von L bilden.

Aufgabe 5.21.*

Es sei K ein Körper mit einer Charakteristik $\neq 2$ und es sei $K \subset L$ eine quadratische Körpererweiterung. Zeige, dass es dann ein $x \in L$, $x \notin K$, mit $x^2 \in K$ gibt.

Aufgabe 5.22. Es sei $\mathbb{C} \subseteq L$ eine endliche Körpererweiterung. Zeige $\mathbb{C} = L$.

Aufgabe 5.23.*

Beweise die „Gradformel“ für eine Kette von endlichen Körpererweiterungen $K \subseteq L \subseteq M$.

Aufgabe 5.24. Es sei $K \subseteq L$ eine Körpererweiterung vom Grad p, wobei p eine Primzahl sei. Es sei $x \in L$, $x \notin K$. Zeige, dass $K[x] = L$ ist.

Aufgabe 5.25. Bestimme den Grad von

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{5}, \sqrt[3]{2}].$$

Aufgabe 5.26.*

Zeige, dass es zu jeder natürlichen Zahl n eine Körpererweiterung $\mathbb{Q} \subseteq L$ vom Grad n gibt.

Aufgabe 5.27. Es sei $K \subseteq L$ eine endliche Körpererweiterung und sei $x_1, \ldots, x_n \in L$ eine K-Basis von L. Zeige, dass die Multiplikation auf L durch die Produkte

$$x_i x_j, 1 \leq i \leq j \leq n,$$

eindeutig festgelegt ist.

Aufgabe 5.28. Es seien $\mathbb{Q} \subseteq K \subset \mathbb{C}$ und $\mathbb{Q} \subseteq L \subset \mathbb{C}$ zwei endliche Körpererweiterungen von $\mathbb{Q}$ vom Grad d bzw. e. Es seien d und e teilerfremd. Zeige, dass dann

$$K \cap L = \mathbb{Q}$$

ist.

Aufgabe 5.29. Zeige, dass man $\sqrt{3}$ nicht als $\mathbb{Q}$-Linearkombination von 1 und $\sqrt{2}$ schreiben kann.

Aufgabe 5.30. Sei K ein Körper und sei p eine Primzahl. Es sei $a \in K$ ein Element, das in K keine p-te Wurzel besitzt. Zeige, dass das Polynom $X^p - a$ irreduzibel ist.

Aufgabe 5.31.*

Das Polynom $F = X^3 - 3X + 1 \in \mathbb{Q}[X]$ ist irreduzibel und definiert daher eine Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

vom Grad 3. Die Restklasse von X in L sei mit α bezeichnet. Zeige, dass auch die Elemente aus L

$$\beta = \alpha^2 - 2$$

und

$$\gamma = -\alpha^2 - \alpha + 2$$

Nullstellen von F sind.

Aufgabe 5.32.*

Es sei K ein Körper und $K \subseteq L$ eine Ringerweiterung vom Grad zwei. Zeige, dass es dann die folgenden drei Möglichkeiten gibt.

(1) L ist ein Körper.
(2) L ist von der Form $L = K[\epsilon]/\epsilon^2$.
(3) L ist der Produktring $L = K \times K$.

Aufgabe 5.33. Zeige, dass die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$ nicht endlich ist.

Aufgabe 5.34.*

Es sei M die Menge aller Zwischenkörper zwischen $\mathbb{Q}$ und $\mathbb{C}$. Für Körper $K_1, K_2 \in M$ setzen wir $K_1 \sim K_2$, falls es einen Körper $L \in M$ mit $K_1 \subseteq L$ und $K_2 \subseteq L$ endlich gibt.

(1) Zeige, dass $\sim$ eine Äquivalenzrelation ist.
(2) Ist $\mathbb{R} \sim \mathbb{C}$?
(3) Ist $\mathbb{Q} \sim \mathbb{C}$?

Aufgabe 5.35. Zeige, dass die Körpererweiterung $\mathbb{R} \subseteq \mathbb{R}(X)$, wobei $\mathbb{R}(X)$ den Körper der rationalen Funktionen bezeichnet, nicht endlich ist.

Aufgabe 5.36. Sei R ein kommutativer Ring mit endlich vielen Elementen. Zeige, dass R genau dann ein Integritätsbereich ist, wenn R ein Körper ist.

Aufgabe 5.37. Sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte (dabei ist p eine Primzahl). Zeige, dass die Abbildung

$$R \longrightarrow R,\ f \longmapsto f^p,$$

ein Ringhomomorphismus ist, den man den *Frobeniushomomorphismus* nennt.

Aufgabe 5.38. Sei R ein kommutativer Ring, der einen Körper der positiven Charakteristik $p > 0$ enthalte. Zeige, dass die e-te Hintereinanderschaltung des Frobeniushomomorphismus

$$F\colon\ R \longrightarrow R,\ f \longmapsto f^p,$$

durch $f \mapsto f^q$ mit $q = p^e$ gegeben ist.

Aufgabe 5.39. Es sei R ein kommutativer Ring der positiven Charakteristik $p > 0$. Zeige, dass die Spektrumsabbildung zum Frobeniushomomorphismus

$$R \longrightarrow R,\ f \longmapsto f^p,$$

eine Homöomorphie ist.

Aufgabe 5.40. Bestimme die Matrix des Frobeniushomomorphismus

$$\Phi\colon\ \mathbb{F}_q \longrightarrow \mathbb{F}_q$$

bezüglich einer geeigneten $\mathbb{F}_p$-Basis von $\mathbb{F}_q$ für $p = 2$ und $q = 4$ bzw. $q = 8$.

Aufgabe 5.41. Es sei p eine Primzahl mit $p = 3 \mod 4$ und sei

$$\mathbb{Z}/(p) \subseteq \mathbb{Z}/(p)[\mathrm{i}] = \mathbb{Z}/(p)[X]/X^2+1) = \mathbb{F}_{p^2}$$

die quadratische Körpererweiterung von $\mathbb{Z}/(p)$. Zeige, dass die Konjugation $\mathrm{i} \mapsto -\mathrm{i}$ mit dem Frobeniushomomorphismus $f \mapsto f^p$ übereinstimmt.

6. Vorlesung - Ganzheit

Die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{7}] = \mathbb{Q}[X]/(X^2-7)$$

kann man genauso gut als

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{7^3}] = \mathbb{Q}[Y]/(Y^2-7^3)$$

schreiben, einen Isomorphismus erhält man, indem man $X \mapsto Y/7$ schickt. Es liegen einfach zwei Beschreibungen des gleichen Körpers vor, wobei die erste etwas einfacher aussieht. Dagegen sind die beiden Restklassenringe $\mathbb{Z}[X]/(X^2-7)$ und $\mathbb{Z}[Y]/(Y^2-7^3)$ nicht zueinander isomorph. Durch $Y \mapsto 7X$ wird ein Ringhomomorphismus des zweiten Ringes in den ersten Ring festgelegt, der injektiv, aber nicht surjektiv ist, da X nicht im Bild liegt. Die Frage ist, wie man bei einer gegebenen endlichen Körpererweiterung $\mathbb{Q} \subseteq L$ einen „passenden“ Unterring $\mathbb{Z} \subseteq R \subseteq L$ finden kann. Jede Gleichungsbeschreibung $L = \mathbb{Q}[X]/(F)$ mit einem ganzzahligen Polynom $F \in \mathbb{Z}[X]$ führt zu einem Kandidaten $S = \mathbb{Z}[X]/(F)$. Es gibt aber im Allgemeinen keine beste beschreibende Gleichung. Stattdessen muss man mit dem Konzept der Ganzheit arbeiten, um die beste passende Ringerweiterung zu finden. Das entscheidende Argument für diesen Weg ist, dass man dabei die eindeutig bestimmte minimale singularitätenfreien Ringerweiterung von $\mathbb{Z}$ in L mit Quotientenkörper L erhält.

6.1. **Ganzheit.**

Definition 6.1. Es seien R und S kommutative Ringe und sei $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ heißt eine Gleichung der Form

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1 x + r_0 = 0,$$

wobei die Koeffizienten r_i, $i = 0, \ldots, n-1$, zu R gehören, eine *Ganzheitsgleichung* für x.

Definition 6.2. Es seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Ein Element $x \in S$ heißt *ganz* (über R), wenn x eine Ganzheitsgleichung mit Koeffizienten aus R erfüllt.

Wenn

$$R = K$$

ein Körper und S eine K-Algebra ist, so ist $x \in S$ algebraisch über K genau dann, wenn es ganz über K ist. Dies stimmt aber im Allgemeinen nicht, siehe Aufgabe 6.2.

Die einfachsten Ganzheitsgleichungen haben die Form $x^n - r = 0$ mit $r \in R$ bzw. $x^n = r$. Wenn also ein Element einer Ringerweiterung eine Wurzel eines Elementes aus R ist, so ist diese Wurzel ganz über dem Grundring. Trivialerweise sind die Elemente aus R ganz über R.

Beispiel 6.3. In der Ringerweiterung $\mathbb{Z} \subseteq \mathbb{Z}[\mathrm{i}]$ ist i ganz über $\mathbb{Z}$, wie die Ganzheitsgleichung

$$\mathrm{i}^2 = -1$$

zeigt. Auch für ein beliebiges Element $z = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ kann man direkt eine Ganzheitsgleichung angeben, nämlich

$$(a + b\mathrm{i})^2 - 2a(a + b\mathrm{i}) + a^2 + b^2 = 0.$$

Beispiel 6.4. Es sei R ein kommutativer Ring und

$$P = X^n + r_{n-1}X^{n-1} + \cdots + r_2X^2 + r_1X + r_0 \in R[X]$$

ein normiertes Polynom über R. Dann ist in der Ringerweiterung

$$R \subseteq R[X]/(P)$$

die Restklasse x von X im Restklassenring $S = R[X]/(P)$ ganz über R, da ja P unmittelbar die Ganzheitsgleichung

$$x^n + r_{n-1}x^{n-1} + \cdots + r_2x^2 + r_1x + r_0 = 0$$

liefert.

Definition 6.5. Es seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Dann nennt man die Menge der Elemente $x \in S$, die ganz über R sind, den *ganzen Abschluss* von R in S.

Definition 6.6. Es seien R und S kommutative Ringe und sei $R \subseteq S$ eine Ringerweiterung. Dann heißt S *ganz* über R, wenn jedes Element $x \in S$ ganz über R ist.

S ist genau dann ganz über R, wenn der ganze Abschluss von R in S gleich S ist.

Wir wollen zeigen, dass die Summe und das Produkt von zwei ganzen Elementen wieder ganz ist. Der vermutlich erste Gedanke, die jeweiligen Ganzheitsgleichungen miteinander „geschickt“ zu kombinieren, führt nicht zum Ziel. Stattdessen braucht man das folgende Kriterium für die Ganzheit.

Lemma 6.7. *Es seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Für ein Element $x \in S$ sind folgende Aussagen äquivalent.*

(1) *x ist ganz über R.*
(2) *Es gibt eine R-Unteralgebra T von S mit $x \in T$ und die ein endlicher R-Modul ist.*

(3) *Es gibt einen endlichen R-Untermodul M von S, der einen Nichtnullteiler aus S enthält, mit $xM \subseteq M$.*

Beweis. (1) $\Rightarrow$ (2). Wir betrachten die von den Potenzen von x erzeugte R-Unteralgebra $R[x]$ von S, die aus allen polynomialen Ausdrücken in x mit Koeffizienten aus R besteht. Aus einer Ganzheitsgleichung

$$x^n + r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1 x + r_0 = 0$$

ergibt sich

$$x^n = -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \cdots - r_1 x - r_0.$$

Man kann also x^n durch einen polynomialen Ausdruck von einem kleineren Grad ausdrücken. Durch Multiplikation dieser letzten Gleichung mit x^i kann man jede Potenz von x mit einem Exponenten $\geq n$ durch einen polynomialen Ausdruck von einem kleineren Grad ersetzen. Insgesamt kann man dann aber all diese Potenzen durch polynomiale Ausdrücke vom Grad $\leq n-1$ ersetzen. Damit ist

$$R[x] = R + Rx + Rx^2 + \cdots + Rx^{n-2} + Rx^{n-1}$$

und die Potenzen $x^0 = 1, x^1, x^2, \ldots, x^{n-1}$ bilden ein endliches Erzeugendensystem von $T = R[x]$.

(2) $\Rightarrow$ (3). Sei $x \in T \subseteq S$, T eine R-Unteralgebra, die als R-Modul endlich erzeugt sei. Dann ist $xT \subseteq T$, und T enthält den Nichtnullteiler 1.

(3) $\Rightarrow$ (1). Sei $M \subseteq S$ ein endlich erzeugter R-Untermodul mit $xM \subseteq M$. Seien $y_1, \ldots, y_n$ erzeugende Elemente von M. Dann ist insbesondere xy_i für jedes i eine R-Linearkombination der y_j, $j = 1, \ldots, n$. Dies bedeutet

$$xy_i = \sum_{j=1}^{n} r_{ij} y_j$$

mit $r_{ij} \in R$, oder, als Matrix geschrieben,

$$x \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} r_{1,1} & r_{1,2} & \ldots & r_{1,n} \\ r_{2,1} & r_{2,2} & \ldots & r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n,1} & r_{n,2} & \ldots & r_{n,n} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

Dies schreiben wir als

$$0 = \begin{pmatrix} x - r_{1,1} & -r_{1,2} & \ldots & -r_{1,n} \\ -r_{2,1} & x - r_{2,2} & \ldots & -r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ -r_{n,1} & -r_{n,2} & \ldots & x - r_{n,n} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}.$$

Nennen wir diese Matrix A (die Einträge sind aus S), und sei A^{adj} die adjungierte Matrix. Dann gilt $A^{\mathrm{adj}}Ay = 0$ (y bezeichne den Vektor $(y_1, \ldots, y_n)$) und nach der Cramerschen Regel ist

$$A^{\mathrm{adj}}A = (\det A)E_n,$$

also gilt $((\det A)E_n)y = 0$. Es ist also $(\det A)y_j = 0$ für alle j und damit

$$(\det A)z = 0$$

für alle $z \in M$. Da M nach Voraussetzung einen Nichtnullteiler enthält, muss $\det A = 0$ sein. Die Determinante ist aber ein normierter polynomialer Ausdruck in x vom Grad n, so dass eine Ganzheitsgleichung vorliegt. □

Korollar 6.8. *Es seien R und S kommutative Ringe und sei $R \subseteq S$ eine Ringerweiterung. Dann ist der ganze Abschluss von R in S eine R-Unteralgebra von S.*

Beweis. Die Ganzheitsgleichungen $X - r$, $r \in R$, zeigen, dass jedes Element aus R ganz über R ist. Seien $x_1 \in S$ und $x_2 \in S$ ganz über R. Nach der Charakterisierung der Ganzheit gibt es endliche R-Unteralgebren $T_1, T_2 \subseteq S$ mit $x_1 \in T_1$ und $x_2 \in T_2$. Sei $y_1, \ldots, y_n$ ein R-Erzeugendensystem von T_1 und $z_1, \ldots, z_m$ ein R-Erzeugendensystem von T_2. Wir können annehmen, dass $y_1 = z_1 = 1$ ist. Betrachte den endlich erzeugten R-Modul

$$T = T_1 \cdot T_2 = \langle y_i z_j,\, i = 1, \ldots, n,\, j = 1, \ldots, m \rangle,$$

der offensichtlich $x_1 + x_2$ und $x_1 x_2$ (und 1) enthält. Dieser R-Modul T ist auch wieder eine R-Algebra, da für zwei beliebige Elemente gilt

$$\Big(\sum r_{ij} y_i z_j\Big)\Big(\sum s_{kl} y_k z_l\Big) = \sum r_{ij} s_{kl} y_i y_k z_j z_l,$$

und für die Produkte gilt $y_i y_k \in T_1$ und $z_j z_l \in T_2$, so dass diese Linearkombination zu T gehört. Dies zeigt, dass die Summe und das Produkt von zwei ganzen Elementen wieder ganz ist. Deshalb ist der ganze Abschluss ein Unterring von S, der R enthält. Also liegt eine R-Unteralgebra vor. □

6.2. **Normale Integritätsbereiche.**

Definition 6.9. Seien R und S kommutative Ringe und $R \subseteq S$ eine Ringerweiterung. Man nennt R *ganz-abgeschlossen* in S, wenn der ganze Abschluss von R in S gleich R ist.

Definition 6.10. Ein Integritätsbereich heißt *normal*, wenn er ganz-abgeschlossen in seinem Quotientenkörper ist.

Definition 6.11. Sei R ein Integritätsbereich und $Q(R)$ sein Quotientenkörper. Dann nennt man den ganzen Abschluss von R in $Q(R)$ die *Normalisierung* von R.

Wichtige Beispiele für normale Ringe werden durch faktorielle Ringe geliefert.

Satz 6.12. *Sei R ein faktorieller Integritätsbereich. Dann ist R normal.*

Beweis. Sei $K = Q(R)$ der Quotientenkörper von R und $q \in K$ ein Element, das die Ganzheitsgleichung

$$q^n + r_{n-1} q^{n-1} + r_{n-2} q^{n-2} + \cdots + r_1 q + r_0 = 0$$

mit $r_i \in R$ erfüllt. Wir schreiben $q = a/b$ mit $a, b \in R$, $b \neq 0$, wobei wir annehmen können, dass die Darstellung gekürzt ist, dass also a und $b \in R$ keinen gemeinsamen Primteiler besitzen. Wir haben zu zeigen, dass b eine Einheit in R ist, da dann $q = ab^{-1}$ zu R gehört.

Wir multiplizieren die obige Ganzheitsgleichung mit b^n und erhalten in R

$$a^n + (r_{n-1}b)a^{n-1} + \left(r_{n-2}b^2\right)a^{n-2} + \cdots + \left(r_1 b^{n-1}\right)a + (r_0 b^n) = 0.$$

Wenn b keine Einheit ist, dann gibt es einen Primteiler p von b. Dieser teilt alle Summanden $(r_{n-i}b^i)a^{n-i}$ für $i \geq 1$ und daher auch den ersten, also a^n. Das bedeutet aber, dass a selbst ein Vielfaches von p ist im Widerspruch zur vorausgesetzten Teilerfremdheit. □

Korollar 6.13. *Es sei R ein normaler Integritätsbereich und $a \in R$. Wenn es ein Element $x \in Q(R)$ mit $x^k = a$ gibt, so ist bereits $x \in R$.*

Beweis. Die Voraussetzung bedeutet, dass $x \in Q(R)$ ganz über R ist, da es die Ganzheitsgleichung

$$X^k - a = 0$$

erfüllt. Also ist $x \in R$ wegen der Normalität. □

Die einfachsten Beispiele für irrationale reelle Zahlen sind $\sqrt{2}, \sqrt{3}, \sqrt{5}$ u.s.w. Diese Beobachtung wird durch die folgende Aussage wesentlich verallgemeinert.

Korollar 6.14. *Es sei $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die kanonische Primfaktorzerlegung der natürlichen Zahl n. Sei k eine positive natürliche Zahl und sei vorausgesetzt, dass nicht alle Exponenten α_i ein Vielfaches von k sind. Dann ist die reelle Zahl*

$$n^{\frac{1}{k}}$$

irrational.

Beweis. Die Zahl $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ kann nach Voraussetzung keine k-te Wurzel in $\mathbb{Z}$ besitzen, da in einer k-ten Potenz alle Exponenten zu Primzahlen Vielfache von k sind. Wegen der Faktorialität von $\mathbb{Z}$ und der daraus nach Satz 6.12 resultierenden Normalität kann es auch kein $x \in Q(\mathbb{Z}) = \mathbb{Q}$ mit $x^k = n$ geben. Daher ist die reelle Zahl $n^{\frac{1}{k}}$ irrational. □

Lemma 6.15. *Es sei R ein normaler Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System. Dann ist auch die Nenneraufnahme R_S normal.*

Beweis. Siehe Aufgabe 6.23. □

6.3. **Der ganze Abschluss in Erweiterungskörpern.**

Lemma 6.16. *Es sei R ein Integritätsbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Körpererweiterung. Der ganze Abschluss von R in L sei mit S bezeichnet. Dann ist L der Quotientenkörper von S.*

Beweis. Sei $f \in L$. Nach Voraussetzung ist L endlich über K. Daher erfüllt f eine Ganzheitsgleichung der Form

$$f^n + q_{n-1}f^{n-1} + \cdots + q_1 f + q_0 = 0$$

mit $q_i \in K$. Sei $r \in R$ ein gemeinsames Vielfaches der Nenner aller q_i, $i = 1, \ldots, n-1$. Multiplikation mit r^n ergibt dann

$$(rf)^n + q_{n-1}r(rf)^{n-1} + \cdots + q_1 r^{n-1}(rf) + q_0 r^n = 0.$$

Dies ist eine Ganzheitsgleichung für rf, da die Koeffizienten $q_{n-i}r^i$ nach Wahl von r alle zu R gehören. Damit ist $rf \in S$, da S der ganze Abschluss ist. Somit zeigt $f = \frac{rf}{r}$, dass f als ein Bruch mit einem Zähler aus S und einem Nenner aus $R \subseteq S$ darstellbar ist, also im Quotientenkörper $Q(S)$ liegt. □

Insbesondere zeigt die vorstehende Aussage, dass bei einer echten Körpererweiterung $K \subset L$ auch der ganze Abschluss von R echt größer als R ist. Für uns steht die Situation, wo $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung der rationalen Zahlen und S der ganze Abschluss von $\mathbb{Z}$ in L ist, im Mittelpunkt.

6. Arbeitsblatt

6.1. **Aufgaben.**

Aufgabe 6.1. Finde eine irreduzible Ganzheitsgleichung (über $\mathbb{Z}$) für die Eisensteinzahl $\omega = \frac{-1+\sqrt{-3}}{2}$.

Aufgabe 6.2. Sei R ein kommutativer Ring und A eine R-Algebra. Zeige, dass wenn R ein Körper ist, die Begriffe algebraisch und ganz für ein Element $x \in A$ übereinstimmen. Zeige ferner, dass für einen Integritätsbereich, der kein Körper ist, diese beiden Begriffe auseinander fallen.

Aufgabe 6.3.*

Es seien R und S Integritätsbereiche und sei $R \subseteq S$ eine ganze Ringerweiterung. Es sei $f \in R$ ein Element, das in S eine Einheit ist. Zeige, dass f dann schon in R eine Einheit ist.

Aufgabe 6.4. Sei $R \subseteq S$ eine ganze Ringerweiterung und sei $f \in R$. Zeige: Wenn f, aufgefasst in S, eine Einheit ist, dann ist f eine Einheit in R.

Aufgabe 6.5. Man gebe ein Beispiel einer ganzen Ringerweiterung $R \subseteq S$, wo es einen Nichtnullteiler $f \in R$ gibt, der ein Nullteiler in S wird.

Aufgabe 6.6.*

Berechne in

$$\mathbb{Z}/(7)[X]/(X^3 + 4X^2 + X + 5)$$

das Produkt

$$(2x^2 + 5x + 3) \cdot (3x^2 + x + 6)$$

(x bezeichne die Restklasse von X).

Aufgabe 6.7. Sei K ein Körper und sei A eine endlichdimensionale K-Algebra. Zeige direkt (ohne Lemma 6.7), dass A ganz über K ist.

Aufgabe 6.8. Es sei $R \subseteq S$ eine Ringerweiterung zwischen endlichen kommutativen Ringen R und S. Zeige, dass eine ganze Ringerweiterung vorliegt.

Aufgabe 6.9. Es sei R ein kommutativer Ring und

$$S = R[X_1, \ldots, X_n]/\mathfrak{a}$$

eine (als Algebra) endlich erzeugte R-Algebra, die ganz über R sei. Zeige, dass S ein endlich erzeugter R-Modul ist.

Aufgabe 6.10. Es sei $R \subseteq S$ eine ganze Erweiterung von Integritätsbereichen und sei $F \subseteq R$ ein multiplikatives System. Zeige, dass dann auch die zugehörige Erweiterung $R_F \subseteq S_F$ ganz ist.

Aufgabe 6.11.
(1) Es sei R ein Integritätsbereich. Zeige, dass R ganz-abgeschlossen im Polynomring $R[X]$ ist.
(2) Man gebe ein Beispiel für einen kommutativen Ring R, der im Polynomring nicht ganz-abgeschossen ist.

Aufgabe 6.12. Sei R ein Integritätsbereich. Zeige, dass R genau dann normal ist, wenn er mit seiner Normalisierung übereinstimmt.

Aufgabe 6.13. Sei R ein Integritätsbereich. Sei angenommen, dass die Normalisierung von R gleich dem Quotientenkörper $Q(R)$ ist. Zeige, dass dann R selbst schon ein Körper ist.

Aufgabe 6.14. Es sei R ein normaler Integritätsbereich und sei $S \subseteq R$ ein multiplikatives System. Zeige, dass dann auch die Nenneraufnahme R_S normal ist.

Aufgabe 6.15. Sei K ein Körper und sei $R_i \subseteq K$, $i \in I$, eine Familie von normalen Unterringen. Zeige, dass auch der Durchschnitt $\bigcap_{i \in I} R_i$ normal ist.

Aufgabe 6.16. Es sei R ein Integritätsbereich. Zeige, dass die folgenden Eigenschaften äquivalent sind.

(1) R ist normal.
(2) Für jedes Primideal $\mathfrak{p}$ ist die Lokalisierung $R_{\mathfrak{p}}$ normal.
(3) Für jedes maximale Ideal $\mathfrak{m}$ ist die Lokalisierung $R_{\mathfrak{m}}$ normal.

Aufgabe 6.17. Sei R ein normaler Integritätsbereich und $a \in R$. Es sei vorausgesetzt, dass a keine Quadratwurzel in R besitzt. Zeige, dass das Polynom $X^2 - a$ prim in $R[X]$ ist. Tipp: Verwende den Quotientenkörper $Q(R)$. Warnung: Prim muss hier nicht zu irreduzibel äquivalent sein.

Aufgabe 6.18. Sei R ein Integritätsbereich mit Normalisierung R^{norm}. Zeige, dass durch

$$\mathfrak{f} = \{g \in R \mid gR^{\mathrm{norm}} \subseteq R\}$$

ein Ideal in R gegeben ist.

Aufgabe 6.19. Sei k eine fixierte positive ganze Zahl und betrachte den Unterring

$$R = \mathbb{Z}[k\mathrm{i}] = \{a + ck\mathrm{i} \mid a, c \in \mathbb{Z}\} \subseteq \mathbb{Z}[\mathrm{i}].$$

Zeige die Isomorphie $R \cong \mathbb{Z}[X]/(X^2 + k^2)$ und dass $\mathbb{Z}[\mathrm{i}]$ ganz über R ist.

In den folgenden Aufgaben wird der Polynomring $K[X, Y]$ in zwei Variablen über einem Körper K verwendet. Diesen kann man definieren als $(K[X])[Y]$. Die Elemente in ihm, also die Polynome in zwei Variablen, haben die Gestalt

$$P = \sum_{i,j} a_{ij} X^i Y^j.$$

Wir interessieren uns für Restklassenringe vom Typ $R = K[X, Y]/(F)$. Die Nullstellenmenge von$F$ besteht aus der Menge derjenigen Punkte (x, y) in der Ebene, für die $F(x, y) = 0$ ist (dieses Nullstellengebilde ist eine geometrische Version des Ringes R).

Aufgabe 6.20. Sei K ein Körper und betrachte den Restklassenring

$$R = K[X,Y]/(X^2 - Y^3)\,.$$

Dies ist ein Integritätsbereich nach Aufgabe 6.17. Zeige, dass die Normalisierung von R gleich dem Polynomring $K[T]$ ist. Skizziere die Nullstellenmenge von $F = X^2 - Y^3$ in der reellen Ebene und finde eine Parametrisierung dieses Gebildes.

Polynomringe kann man entsprechend über jedem Grundring und mit beliebig vielen Variablen definieren.

Aufgabe 6.21. Es sei

$$P \;=\; X^2 - 3X + 7$$

und

$$Q \;=\; Y^3 - Y^2 + 4Y - 5.$$

Begründe, dass die Ringerweiterung

$$\mathbb{Z} \;\subseteq\; \mathbb{Z}[X,Y]/(P,Q)$$

ganz ist und finde eine Ganzheitsgleichung für $x + y$ und für xy (kleine Buchstaben bezeichnen die Restklassen der Variablen).

Aufgabe 6.22. Es sei R ein normaler Integritätsbereich und $R \subseteq S$ eine ganze Ringerweiterung. Sei $f \in R$. Zeige, dass für das von f erzeugte Hauptideal gilt:

$$R \cap (f)S \;=\; (f)R.$$

Aufgabe 6.23. Zeige, dass für natürliche Zahlen $a, b \geq 1$ und $n \geq 2$ die Zahl $a^n - b^n$ nicht ein Teiler von $a^n + b^n$ ist.

Aufgabe 6.24. Seien R, S, T kommutative Ringe und seien $\varphi : R \to S$ und $\psi : S \to T$ Ringhomomorphismen derart, dass S ganz über R und T ganz über S ist. Zeige, dass dann auch T ganz über R ist.

Aufgabe 6.25. Sei K ein Körper und betrachte den Ringhomomorphismus $\varphi\colon\ R = K[X,Y] \to K[T]$, der durch die Einsetzung

$$X \longmapsto (T-1)(T+1) \text{ und } Y \longmapsto T(T-1)(T+1)$$

gegeben ist. Finde ein von 0 verschiedenes Polynom $F \in K[X,Y]$ derart, dass F unter φ auf 0 abgebildet wird. Skizziere die Nullstellenmenge von F in der reellen Ebene.

Aufgabe 6.26. Definiere unter Anlehnung an die Parametrisierung der pythagoreischen Tripel einen Ringhomomorphismus

$$\mathbb{Z}[X,Y,Z]/(X^2+Y^2-Z^2) \longrightarrow \mathbb{Z}[U,V]\,.$$

Zeige, dass dieser injektiv, aber nicht surjektiv ist.

7. Vorlesung - Algebraische Zahlbereiche

7.1. **Zahlbereiche.**

Wir werden uns in diesem Kurs hauptsächlich für den ganzen Abschluss von $\mathbb{Z}$ in einem endlichen Erweiterungskörper der rationalen Zahlen $\mathbb{Q}$ interessieren.

Definition 7.1. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Dann nennt man den ganzen Abschluss von $\mathbb{Z}$ in L den *Ring der ganzen Zahlen* in L. Solche Ringe nennt man auch *Zahlbereiche*.

Den endlichen Erweiterungskörper L von $\mathbb{Q}$ nennt man übrigens einen *Zahlkörper*. Diese Zahlbereiche sind der Gegenstand der algebraischen Zahlentheorie. Wir interessieren uns in der algebraischen Zahlentheorie insbesondere für folgende Fragen.

(1) Wann ist ein Zahlbereich R ein Hauptidealbereich und wann ist er faktoriell?
(2) Wenn R kein Hauptidealbereich ist, gibt es dann andere Versionen, die die eindeutige Primfaktorzerlegung ersetzen? (Ja: Lokal und auf Idealebene, siehe Korollar 10.17, Satz 10.17, Bemerkung 10.9 einerseits und Satz 12.2 andererseits.)
(3) Wenn R kein Hauptidealbereich ist, kann man dann die Abweichung von der Eigenschaft, ein Hauptidealbereich zu sein, in irgendeiner Form messen? (Ja: Durch die sogenannte Klassengruppe. Siehe Satz 14.2 und Satz 26.6.)
(4) Was passiert mit den Primzahlen in den Zahlbereichen? Gibt es eine Regelmäßigkeit, wie diese in R zerlegt werden? (siehe Korollar 8.8.)
(5) Was kann man über die Einheiten in einem Zahlbereich sagen? (Siehe Satz 28.7.)
(6) Inwiefern reflektieren Eigenschaften von Zahlbereichen Eigenschaften der ganzen Zahlen selbst?

Satz 7.2. *Sei R ein Zahlbereich. Dann ist R ein normaler Integritätsbereich.*

Beweis. Nach Lemma 6.16 ist L der Quotientenkörper des Ganzheitsrings R. Ist $q \in Q(R) = L$ ganz über R, so ist q nach Aufgabe 6.22 auch ganz über $\mathbb{Z}$ und gehört selbst zu R. □

Ein Ganzheitsring ist im Allgemeinen nicht faktoriell.

Lemma 7.3. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und es sei $R \subseteq L$ ein Unterring mit den folgenden Eigenschaften:*

(1) *R ist ganz über $\mathbb{Z}$.*
(2) *Es ist $Q(R) = L$.*
(3) *R ist normal.*

Dann ist R der Ring der ganzen Zahlen von L.

Beweis. Siehe Aufgabe 7.1. □

Beispiel 7.4. Wir betrachten die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-3}]$, der die Ringe

$$\mathbb{Z}[\sqrt{-3}] = A \subseteq \mathbb{Z}[\omega] = B \subseteq \mathbb{Q}[\sqrt{-3}]$$

enthält, wobei $\omega = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}$ ist, d.h. $\mathbb{Z}[\omega]$ ist der Ring der Eisenstein-Zahlen. Der Quotientenkörper von beiden Ringen ist $\mathbb{Q}[\sqrt{-3}]$. Das Element ω erfüllt die Ganzheitsgleichung

$$\omega^2 + \omega + 1 = 0,$$

und somit ist $\mathbb{Z}[\omega]$ ganz über $\mathbb{Z}$. Ferner ist $\mathbb{Z}[\omega]$ normal. Dies ergibt sich aus Satz Anhang 2.7, Satz Anhang 2.8, Satz 2.19 und Satz 6.12. Nach Lemma 7.3 ist also insgesamt der Ring der Eisenstein-Zahlen der Ring der ganzen Zahlen in $\mathbb{Q}[\sqrt{-3}]$.

Satz 7.5. *Es sei R ein Zahlbereich und sei $f \in Q(R) = L$. Dann ist f genau dann ganz über $\mathbb{Z}$, wenn die Koeffizienten des Minimalpolynoms von f über $\mathbb{Q}$ alle ganzzahlig sind.*

Beweis. Das Minimalpolynom P von f über $\mathbb{Q}$ ist ein normiertes irreduzibles Polynom mit Koeffizienten aus $\mathbb{Q}$. Wenn die Koeffizienten sogar ganzzahlig sind, so liegt direkt eine Ganzheitsgleichung für f über $\mathbb{Z}$ vor.

Sei umgekehrt f ganz über $\mathbb{Z}$, und sei $S \in \mathbb{Z}[X]$ ein normiertes ganzzahliges Polynom mit $S(f) = 0$, das wir als irreduzibel in $\mathbb{Z}[X]$ annehmen dürfen. Wir betrachten $S \in \mathbb{Q}[X]$. Dort gilt

$$S = PT.$$

Da nach dem Lemma von Gauß ein irreduzibles Polynom von $\mathbb{Z}[X]$ auch in $\mathbb{Q}[X]$ irreduzibel ist, folgt $S = P$ und daher sind alle Koeffizienten von P ganzzahlig. □

7.2. **Ideale in Zahlbereichen.**

In $\mathbb{Z}$[i] ist jedes Ideal ein Hauptideal und es ist

$$(a + b\mathrm{i}) = \{m(a + b\mathrm{i}) + n\mathrm{i}(a + b\mathrm{i}) \mid m, n \in \mathbb{Z}\} \cong \mathbb{Z}^2$$

(die letzte Gleichung setzt voraus, dass es sich nicht um das Nullideal handelt). Eine ähnlich einfache Gruppenstruktur gilt für jedes Ideal in einem Zahlbereich, was wir in Korollar 8.5 beweisen werden.

Lemma 7.6. *Es sei R ein Zahlbereich. Dann enthält jedes von 0 verschiedene Ideal $\mathfrak{a} \subseteq R$ eine Zahl $m \in \mathbb{Z}$ mit $m \neq 0$.*

Beweis. Sei $0 \neq f \in \mathfrak{a}$. Dieses Element ist nach der Definition eines Zahlbereiches ganz über $\mathbb{Z}$ und erfüllt demnach eine Ganzheitsgleichung

$$f^n + k_{n-1}f^{n-1} + k_{n-2}f^{n-2} + \cdots + k_1 f + k_0 = 0$$

mit ganzen Zahlen k_i. Bei $k_0 = 0$ kann man die Gleichung mit f kürzen, da $f \neq 0$ ein Nichtnullteiler ist. So kann man sukzessive fortfahren und erhält schließlich eine Ganzheitsgleichung, bei der der konstante Term nicht 0 ist. Sei also in obiger Gleichung $k_0 \neq 0$. Dann ist

$$f\big(f^{n-1} + k_{n-1}f^{n-2} + k_{n-2}f^{n-3} + \cdots + k_1\big) = -k_0$$

und somit ist $k_0 \in (f) \cap \mathbb{Z} \subseteq \mathfrak{a}$. □

Lemma 7.7. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in R. Dann enthält $\mathfrak{a}$ Elemente $b_1, \ldots, b_n$, die eine $\mathbb{Q}$-Basis von L sind.*

Beweis. Es sei $v_1, \ldots, v_n$ eine $\mathbb{Q}$-Basis von L. Das Ideal $\mathfrak{a}$ enthält nach Lemma 7.6 ein Element $0 \neq m \in \mathfrak{a} \cap \mathbb{Z}$. Nach (dem Beweis von) Lemma 6.16 kann man $v_i = \frac{r_i}{n_i}$ mit $r_i \in R$ und $n_i \in \mathbb{Z} \setminus \{0\}$ schreiben. Dann sind die $m(n_i v_i) \in \mathfrak{a}$ und sie bilden ebenfalls eine $\mathbb{Q}$-Basis von L. □

7.3. **Spur und Norm.**

Zu einer R-Algebra S definiert jedes Element $f \in S$ einen R-Modulhomomorphismus $S \to S$, $x \mapsto fx$, die *Multiplikationsabbildung*. Wenn S eine endlich erzeugte freie R-Algebra ist, ihre additive Struktur also die Form $S = R^n$ besitzt, so wird dieser Multiplikationshomomorphismus bezüglich einer R-Basis von S durch eine $n \times n$-Matrix beschrieben, die die *Multiplikationsmatrix* (zu f bezüglich dieser Basis) heißt. In diesem Fall kann man Konzepte der Matrixtheorie der linearen Algebra auf diese Multiplikationsabbildung anwenden. Diese Situation liegt bei einer endlichen Körpererweiterung $K \subseteq L$ vor, aber auch ein Zahlbereich ist stets nach Korollar 8.6 eine freie $\mathbb{Z}$-Algebra. Aber auch wenn $R \subseteq S$ Integritätsbereiche sind mit S endlich erzeugt als R-Modul, so kann man auch im nichtfreien Fall über die Quotientenkörper die folgenden Konzepte anwenden.

Definition 7.8. Es sei R ein kommutativer Ring und sei S eine kommutative endliche freie R-Algebra. Zu einem Element $f \in S$ nennt man die Spur des R-Modulhomomorphismus

$$\mu_f \colon S \longrightarrow S,\, y \longmapsto fy,$$

die *Spur* von f. Sie wird mit $\operatorname{Spur}(f)$ bezeichnet.

Definition 7.9. Es sei R ein kommutativer Ring und sei S eine kommutative endliche freie R-Algebra. Zu einem Element $f \in S$ nennt man die Determinante des R-Modulhomomorphismus

$$\mu_f \colon S \longrightarrow S,\, y \longmapsto fy,$$

die *Norm* von f. Sie wird mit $N(f)$ bezeichnet.

Bei einer freien R-Algebra S ist die Spur

$$S \longrightarrow R,\, f \longmapsto \operatorname{Spur}(f),$$

R-linear und insbesondere additiv und die Norm

$$S \longrightarrow R,\, f \longmapsto N(f),$$

ist multiplikativ. Darin liegen ihre jeweiligen Bedeutungen, dass mit ihrer Hilfe additive bzw. multiplikative Eigenschaften von S in R widergespiegelt werden können. Einen Ringhomomorphismus von S nach R gibt es nur sehr selten, deshalb sind Spur und Norm in gewissem Sinne optimal.

Die Interpretation eines Elementes als lineare Abbildung hilft auch dabei, das Minimalpolynom zu bestimmen.

Lemma 7.10. *Es sei $K \subseteq L$ eine endliche Körpererweiterung und $f \in L$ ein Element mit der Multiplikationsabbildung*

$$\mu_f \colon L \longrightarrow L,\, y \longmapsto fy.$$

Dann ist in $K[X]$ das charakteristische Polynom von μ_y ein Vielfaches des Minimalpolynoms von f. Bei $L = K[f]$ stimmt das charakteristische Polynom mit dem Minimalpolynom überein.

Beweis. Die Zuordnung

$$L \longrightarrow \operatorname{End}(L),\, f \longmapsto \mu_f,$$

ist ein injektiver Ringhomomorphismus. Es sei χ das charakteristische Polynom von μ_f. Nach Cayley-Hamilton ist

$$\chi(\mu_f) = 0$$

im Endomorphismenring. Damit ist auch

$$\chi(f) = 0$$

in $K[X]$. Nach Satz 2.12 ist somit das Minimalpolynom ein Teiler des charakteristischen Polynoms. Bei $L = K[f]$ besitzt das Minimalpolynom und das charakteristische Polynom den gleichen Grad, also stimmen sie überein. □

Da wir noch nicht gezeigt haben, dass Zahlbereiche frei sind, verwenden wir Spur und Norm über die Quotientenkörper. Allerdings können wir hier schon begründen, dass die Spur und die Norm eines ganzen Elementes zum Grundring gehört.

Korollar 7.11. *Es sei R ein Zahlbereich und sei $f \in R$. Dann ist die Spur und die Norm von f ganzzahlig.*

Beweis. Eine Verfeinerung der Argumentation zu Lemma 7.10 zeigt, dass das charakteristische Polynom zu f eine Potenz des Minimalpolynoms zu f ist. Da nach Satz 7.5 die Koeffizienten des Minimalpolynoms ganzzahlig sind, überträgt sich dies auf das charakteristische Polynom. Spur und Norm treten aber nach Aufgabe 7.17 und Aufgabe 7.18 als Koeffizienten des charakteristischen Polynoms auf. □

7.4. **Einbettungen in die komplexen Zahlen.**

Satz 7.12. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann gibt es genau n Einbettungen von L in die komplexen Zahlen $\mathbb{C}$.*

Beweis. Nach dem Satz vom primitiven Element wird L durch ein Element erzeugt, es ist also

$$L = \mathbb{Q}(x) \cong \mathbb{Q}[X]/(F)$$

mit einem irreduziblen Polynom $F \in \mathbb{Q}[X]$ vom Grad n. Da F irreduzibel ist und da die Ableitung $F' \neq 0$ ist und kleineren Grad besitzt, folgt, dass F und F' teilerfremd sind. Nach Satz 2.12 ergibt sich, dass F und F' das Einheitsideal erzeugen, also $AF + BF' = 1$ ist. Wir betrachten diese Polynome nun als Polynome in $\mathbb{C}[X]$, wobei die polynomialen Identitäten erhalten bleiben. Über den komplexen Zahlen zerfallen F und F' in Linearfaktoren, und wegen der Teilerfremdheit bzw. der daraus resultierenden Identität haben F und F' keine gemeinsame Nullstelle. Daraus folgt wiederum, dass F keine mehrfache Nullstelle besitzt, sondern genau n verschiedene komplexe Zahlen $z_1, \ldots, z_n$ als Nullstellen besitzt. Jedes z_i definiert nun einen Ringhomomorphismus

$$\rho_i \colon L \cong \mathbb{Q}[X]/(F) \longrightarrow \mathbb{C},\ X \longmapsto z_i.$$

Da L ein Körper ist, ist diese Abbildung injektiv. Da dabei X auf verschiedene Elemente abgebildet wird, liegen n verschiedene Abbildungen vor. Es kann auch keine weiteren Ringhomomorphismen $L \to \mathbb{C}$ geben, da jeder solche durch $X \mapsto z$ gegeben ist und $F(z) = 0$ sein muss. □

Statt von komplexen Einbettungen spricht man auch von komplexen Realisierungen. Man beachte im vorstehenden Satz, dass das Bild von verschiedenen Einbettungen

$$\rho_i \colon L \longrightarrow \mathbb{C}$$

der gleiche Unterkörper von $\mathbb{C}$ sein kann. Dies gilt bereits für quadratische Erweiterungen wie $\mathbb{Q}[\mathrm{i}]$. Man hat die beiden Einbettung $\rho_1, \rho_2 \colon \mathbb{Q}[\mathrm{i}] \to \mathbb{C}$, wobei die eine Abbildung i auf i und die andere i auf $-\mathrm{i}$ schickt. Das Bild ist aber in beiden Fällen gleich.

Wenn das Bild einer Einbettung ganz in den reellen Zahlen liegt, so spricht man auch von einer *reellen Einbettung*. Die Anzahl der reellen Einbettungen

und die Anzahl der imaginären Einbettungen spielt eine wichtige Rolle in der algebraischen Zahlentheorie. Zu einem Element $z \in L$ nennt man die verschiedenen komplexen Zahlen

$$z_1 = \rho_1(z), \ldots, z_n = \rho_n(z)$$

zueinander konjugiert. Diese sind allesamt Nullstellen eines irreduziblen Polynoms F mit rationalen Koeffizienten vom Grad n.

Lemma 7.13. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und $z \in L$ ein Element. Es seien*

$$\rho_1, \ldots, \rho_n \colon L \longrightarrow \mathbb{C}$$

die verschiedenen komplexen Einbettungen und es sei $M = \{y_1, \ldots, y_k\}$ die Menge der verschiedenen Werte $\rho_i(z)$. Dann gilt in $\mathbb{C}[X]$ für das Minimalpolynom G von z die Gleichung

$$G = (X - y_1)(X - y_2) \cdots (X - y_k).$$

Beweis. Es sei $K \subseteq L$ der von z erzeugte Unterkörper von L. Es ist dann

$$K \cong \mathbb{Q}[X]/(G)$$

mit dem (normierten) Minimalpolynom G von z und K (bzw. G) haben den Grad m über $\mathbb{Q}$. Gemäß Satz 7.12 gibt es m Einbettungen $\sigma \colon K \to \mathbb{C}$, die den komplexen Nullstellen M' von G entsprechen, und daher ist

$$G = \prod_{\sigma} (X - \sigma(z)).$$

Die n Einbettungen $\rho_i \colon L \to \mathbb{C}$ induzieren jeweils eine Einbettung

$$\sigma_i = \rho_i|_K \colon K \longrightarrow \mathbb{C}$$

und somit ist $\rho_i(z) = \sigma_i(z)$, also $M \subseteq M'$. Andererseits lässt sich eine Einbettung $\sigma \colon K \to \mathbb{C}$ zu einer Einbettung $L \to \mathbb{C}$ fortsetzen, da L über K separabel ist und nach dem Satz vom primitiven Element von einem Element erzeugt wird und das zugehörige Minimalpolynom über $\mathbb{C}$ zerfällt. Daher ist auch $M' \subseteq M$. □

Lemma 7.14. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $\rho_i \colon L \to \mathbb{C}$ die n verschiedenen komplexen Einbettungen. Es sei $z \in L$ und $z_i = \rho_i(z)$, $i = 1, \ldots, n$. Dann ist*

$$N(z) = z_1 \cdots z_n \text{ und } \operatorname{Spur}(z) = z_1 + \cdots + z_n .$$

Beweis. Es sei zunächst $K = \mathbb{Q}[z]$ vom Grad k. Nach Lemma 7.10 ist das Minimalpolynom gleich dem charakteristischen Polynom und nach Lemma 7.13 ist das Minimalpolynom gleich $(X - z_1)(X - z_2) \cdots (X - z_k)$. Der Vergleich des konstanten Koeffizienten und des Koeffizienten zu X^{k-1} ergibt die Behauptung.

Im Allgemeinen sei

$$\mathbb{Q} \subseteq K = \mathbb{Q}[z] \subseteq L$$

und es sei M die Matrix über $\mathbb{Q}$, die die Multiplikation mit z auf K bezüglich einer $\mathbb{Q}$-Basis $y_1, \ldots, y_k$ beschreibt. Zu einer K-Basis $z_1, \ldots, z_\ell$ von L ist $y_i z_j$ eine $\mathbb{Q}$-Basis von L, und die Multiplikation mit z auf L wird durch die Blockmatrix

$$\begin{pmatrix} M & 0 & \ldots & 0 \\ 0 & M & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & M \end{pmatrix}$$

beschrieben. Deren Spur ist das ℓ-Fache der Spur von M und deren Determinante ist die ℓ-te Potenz der Determinante von M. Ebenso treten die verschiedenen komplexen Zahlen z_i jeweils ℓ-fach auf. □

Die verschiedenen Einbettungen für endliche Körpererweiterungen von $\mathbb{Q}$ führen auch zur Gittertheorie für Zahlbereiche, die wir ab der 25. Vorlesung behandeln.

7. Arbeitsblatt

7.1. **Aufgaben.**

Aufgabe 7.1. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und es sei $R \subseteq L$ ein Unterring mit den folgenden Eigenschaften:

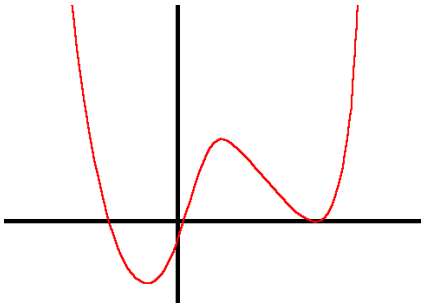
(1) R ist ganz über $\mathbb{Z}$.
(2) Es ist $Q(R) = L$.
(3) R ist normal.

Dann ist R der Ring der ganzen Zahlen von L.

Aufgabe 7.2. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Man gebe Beispiele für Unterringe $R \subseteq L$, die je zwei der folgenden Eigenschaften erfüllen, aber nicht die dritte.

(1) R ist ganz über $\mathbb{Z}$.
(2) Es ist $Q(R) = L$.
(3) R ist normal.

Aufgabe 7.3. Der abgebildete Graph gehört zu einem normierten ganzzahligen Polynom F. Kann $R = \mathbb{Z}[X]/(F)$ ein Zahlbereich sein?



Aufgabe 7.4. Es sei R ein Zahlbereich und es sei $R \subseteq S$ eine endliche Erweiterung von kommutativen Ringen. Es sei S ein normaler Integritätsbereich. Zeige, dass S ebenfalls ein Zahlbereich ist.

Aufgabe 7.5. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und R der zugehörige Zahlbereich. Zeige, dass es eine natürliche Bijektion zwischen Zahlbereichen $\mathbb{Z} \subseteq S \subseteq R$ und Zwischenkörpern $\mathbb{Q} \subseteq K \subseteq L$.

Aufgabe 7.6. Es seien R und S Zahlbereiche. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) R und S sind isomorph.
(2) Es gibt ein $f \in R$ und ein $g \in S$, beide nicht 0, derart, dass die Nenneraufnahmen R_f und S_g zueinander isomorph sind.
(3) Es gibt ein Primideal $\mathfrak{p}$ von R und ein Primideal $\mathfrak{q}$ von S derart, dass die Lokalisierungen $R_{\mathfrak{p}}$ und $S_{\mathfrak{q}}$ zueinander isomorph sind.
(4) Die Quotientenkörper $Q(R)$ und $Q(S)$ sind isomorph.

In den drei folgenden Aufgaben wird der Begriff des primitiven Polynoms verwendet:

Ein Polynom $F \in \mathbb{Z}[X]$ heißt *primitiv*, wenn die Koeffizienten von F teilerfremd sind.

Aufgabe 7.7. Es sei $F \in \mathbb{Z}[X]$ ein Polynom. Zeige, dass man F als $F = n\tilde{F}$ mit $n \in \mathbb{N}$ und primitivem $\tilde{F}$ schreiben kann.

Aufgabe 7.8. Es sei $F \in \mathbb{Z}[X]$ ein irreduzibles Polynom. Dann ist F, aufgefasst als Polynom in $\mathbb{Q}[X]$, ebenfalls irreduzibel.

Aufgabe 7.9. Seien $F, G \in \mathbb{Z}[X]$ primitive Polynome. Zeige, dass dann auch das Produkt FG primitiv ist.

Aufgabe 7.10. Es sei $F \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit dem zugehörigen Primideal

$$\mathfrak{p} = (F) \in \operatorname{Spek}(\mathbb{Q}[X]) \subseteq \operatorname{Spek}(\mathbb{Z}[X]),$$

wobei die letzte Inklusion zur Nenneraufnahme $\mathbb{Z}[X] \to \mathbb{Q}[X]$ im Sinne von Proposition 5.4 (3) gehört. Zeige, dass der Abschluss von $\mathfrak{p}$ in $\operatorname{Spek}(\mathbb{Z}[X])$ gleich $V(\mathfrak{a})$ mit

$$\mathfrak{a} = \{qF \mid q \in \mathbb{Q},\, qF \in \mathbb{Z}[X]\}$$

ist. Zeige ferner, dass zu isomorphen Restekörpern $\kappa(\mathfrak{p}_1)$ und $\kappa(\mathfrak{p}_2)$ die Restklassenringe $R/\mathfrak{a}_1$ und $R/\mathfrak{a}_2$ nicht isomorph sein müssen.

Aufgabe 7.11. Erstelle die Multiplikationsmatrix zum Element $7x^2-4x+5$ in der kubischen Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\big(X^3 - 6X^2 + 5X - 8\big).$$

Aufgabe 7.12. Erstelle die Multiplikationsmatrix zum Element $7x^2+3x-8$ in der kubischen Körpererweiterung

$$\mathbb{Q} = \mathbb{Q}[X]/\big(X^3 + 9X^2 - 2X + 5\big).$$

Aufgabe 7.13.*

Es seien p, q verschiedene Primzahlen und

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p}, \sqrt{q}] =: L$$

die zugehörige Körpererweiterung. Erstelle die Multiplikationsmatrix zu einem Element $a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq} \in L$ bezüglich der Basis $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$.

Aufgabe 7.14. Wir betrachten die quadratische Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}] = L$. Erstelle die Matrix der Multiplikationsabbildung zu $-4+9\sqrt{3}$ bezüglich der $\mathbb{Q}$-Basis $1, \sqrt{3}$ von L.

Aufgabe 7.15. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass die Abbildung

$$L \longrightarrow \operatorname{End}_K(L),\ f \longmapsto \mu_f,$$

ein injektiver Ringhomomorphismus ist.

Aufgabe 7.16. Es sei $K \subseteq M \subseteq L$ eine Körpererweiterung. Es sei $f \in M$ und B die beschreibende Matrix der Multiplikationsabbildung $\mu_f \colon M \to M$ bezüglich einer K-Basis von M. Zeige, dass bezüglich einer geeigneten K-Basis von L die Multiplikationsabbildung $\mu_f \colon L \to L$ durch eine Blockmatrix der Form

$$\begin{pmatrix} B & 0 & \ldots & 0 \\ 0 & B & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & B \end{pmatrix}$$

beschrieben wird.

Aufgabe 7.17. Zeige, dass die Definition Anhang 6.2 der Spur eines Modulhomomorphismus unabhängig von der gewählten Basis des freien Moduls ist.

Aufgabe 7.18. Es sei K ein Körper und es sei A eine $m \times n$-Matrix und B eine $n \times m$-Matrix über K. Zeige

$$\operatorname{Spur}(A \circ B) = \operatorname{Spur}(B \circ A).$$

Aufgabe 7.19. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K. Wie findet man die $\operatorname{Spur}(M)$ im charakteristischen Polynom χ_M wieder?

Aufgabe 7.20. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K. Wie findet man die Determinante von M im charakteristischen Polynom χ_M wieder?

Aufgabe 7.21. Es sei K ein Körper und sei M eine $n \times n$-Matrix über K mit der Eigenschaft, dass das charakteristische Polynom in Linearfaktoren zerfällt, also

$$\chi_M = (X - \lambda_1)^{\mu_1} \cdot (X - \lambda_2)^{\mu_2} \cdots (X - \lambda_k)^{\mu_k}.$$

Zeige, dass

$$\operatorname{Spur}(M) = \sum_{i=1}^{k} \mu_i \lambda_i$$

ist.

Aufgabe 7.22. Es sei

$$M \in \operatorname{Mat}_n(K)$$

eine Matrix mit n (paarweise) verschiedenen Eigenwerten. Zeige, dass die Spur von M die Summe der Eigenwerte ist.

Aufgabe 7.23. Es sei p eine Primzahl. Betrachte die endliche Körpererweiterung

$$\mathbb{Q} \subseteq L = \mathbb{Q}[X]/(X^3 - p)$$

vom Grad 3. Sei $f = aX^2 + bX + c \in L$ ein Element davon mit $a, b, c \in \mathbb{Q}$. Berechne das Minimalpolynom von f und man gebe die Koeffizienten davon explizit an. Bestimme insbesondere die Norm und die Spur von f.

Welche Bedingungen an a, b, c ergeben sich aus der Voraussetzung, dass f ganz über $\mathbb{Z}$ ist?

Aufgabe 7.24. Bringe für die Körpererweiterung $\mathbb{R} \subseteq \mathbb{C}$ die Konzepte Norm und Spur mit dem Betrag und dem Realteil einer komplexen Zahl in Verbindung.

Aufgabe 7.25. Berechne für das Element $2 + 4x + 5x^2$ in der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

die Norm und die Spur.

Aufgabe 7.26. Es sei $K \subseteq M \subseteq L$ eine Kette von quadratischen Körpererweiterungen. Zeige, dass für die Normen die Beziehung

$$N_K^L = N_K^M \circ N_M^L$$

gilt.

Aufgabe 7.27.*

Bestimme für sämtliche Elemente der Körpererweiterung

$$\mathbb{Z}/(2) \subseteq \mathbb{Z}/(2)[X]/\left(X^2 + X + 1\right)$$

die Multiplikationsmatrizen bezüglich der Basis $1, x$ sowie ihre Norm und ihre Spur.

Aufgabe 7.28. Bestimme für sämtliche Elemente der Körpererweiterung

$$\mathbb{Z}/(3) \subseteq \mathbb{Z}/(3)[X]/\left(X^2 - 2\right)$$

die Multiplikationsmatrizen bezüglich der Basis $1, x$ sowie ihre Norm und ihre Spur.

Aufgabe 7.29.*

Es sei $K \subseteq L$ eine endliche Körpererweiterung und $f \in L$. Zeige, dass es für die Eigenwerttheorie der K-linearen Multiplikationsabbildung

$$\mu_f \colon L \longrightarrow L$$

grundsätzlich nur zwei Möglichkeiten gibt.

Aufgabe 7.30. Sei K ein Körper und sei $P = X^n - c \in K[X]$ ein irreduzibles Polynom. Es sei

$$f = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0$$

ein Element in der einfachen endlichen Körpererweiterung $K \subseteq L = K[X]/(P)$ vom Grad n. Zeige, dass die Spur von f gleich na_0 ist.

Aufgabe 7.31. Sei p eine Primzahl und sei

$$L = \mathbb{Q}[X]/\big(X^3 - p\big)$$

der durch das irreduzible Polynom $X^3 - p$ definierte Erweiterungskörper von $\mathbb{Q}$. Es sei

$$f = 2 + 3x - 4x^2 \, .$$

(1) Finde die Matrix bezüglich der $\mathbb{Q}$-Basis $1, x, x^2$ von L der durch die Multiplikation mit f definierten $\mathbb{Q}$-linearen Abbildung.
(2) Berechne die Norm und die Spur von f.
(3) Bestimme das Minimalpolynom von f.
(4) Finde das Inverse von f.
(5) Berechne die Diskriminante der Basis $1, f, f^2$.

Aufgabe 7.32. Es sei $K \subseteq L$ eine Körpererweiterung, $f \in L$ und $M = K[f]$. Zeige, dass das charakteristische Polynom der Multiplikationsabbildung

$$\mu_f \colon L \longrightarrow L$$

eine Potenz des Minimalpolynoms von f ist.

Aufgabe 7.33. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und sei

$$\rho \colon L \longrightarrow \mathbb{C}$$

ein Ringhomomorphismus. Zeige, dass für jeden Körperautomorphismus

$$\varphi \colon L \longrightarrow L$$

auch $\rho \circ \varphi$ ein Ringhomomorphismus nach $\mathbb{C}$ ist, und dass daher die Galoisgruppe von L auf der Menge der komplexen Einbettungen von L operiert.

Aufgabe 7.34. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung. Zeige, dass genau dann eine Galoiserweiterung vorliegt, wenn die Bildkörper unter allen komplexen Einbettungen von L übereinstimmen.

Aufgabe 7.35. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es sei $F \in K[X]$ und $a \in K$. Zeige, dass a genau dann eine mehrfache Nullstelle von F ist, wenn $F'(a) = 0$ ist, wobei F' die formale Ableitung von F bezeichnet.

8. Vorlesung - Diskriminante

8.1. **Die Diskriminante.**

Das Hauptziel dieser Vorlesung ist es, die Diskriminante einzuführen und damit zu zeigen, dass Zahlbereiche stets eine $\mathbb{Z}$-Basis besitzen.

Definition 8.1. Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ Elemente in L. Dann wird die *Diskriminante* von $b_1, \ldots, b_n$ durch

$$\triangle(b_1, \ldots, b_n) = \det\left(\mathrm{Spur}\,(b_i b_j)_{i,j}\right)$$

definiert.

Die Produkte $b_i b_j$, $1 \leq i, j \leq n$, sind dabei Elemente in L, von denen man jeweils die Spur nimmt, die in K liegt. Man erhält also eine quadratische $n \times n$-Matrix über K. Deren Determinante ist nach Definition die Diskriminante. Im folgenden werden wir vor allem an der Diskriminante von speziellen Basen interessiert sein, so dass sich die Diskriminante als Invariante eines Zahlkörpers erweist.

Bei einem Basiswechsel verhält sich die Diskriminante wie folgt.

Lemma 8.2. *Es sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ K-Basen von L. Der Basiswechsel werde durch $c = Tb$ mit der Übergangsmatrix $T = (t_{ij})_{ij}$ beschrieben. Dann gilt für die Diskriminanten die Beziehung*

$$\triangle(c_1, \ldots, c_n) = (\det(T))^2 \triangle(b_1, \ldots, b_n).$$

Beweis. Ausgeschrieben haben wir die Beziehungen $c_i = \sum_{j=1}^n t_{ij} b_j$. Damit gilt

$$c_i c_k = \left(\sum_{j=1}^n t_{ij} b_j\right)\left(\sum_{m=1}^n t_{km} b_m\right) = \sum_{j,m} t_{ij} t_{km} b_j b_m.$$

Wir schreiben $c_{ik} := S(c_ic_k)$ und $b_{jm} := S(b_jb_m)$. Wegen der K-Linearität der Spur gilt

$$c_{ik} = S(c_ic_k) = S\left(\sum_{j,m} t_{ij}t_{km}b_jb_m\right) = \sum_{j,m} t_{ij}t_{km}S(b_jb_m) = \sum_{j,m} t_{ij}t_{km}b_{jm}.$$

Wir schreiben diese Gleichung mit den Matrizen $C = (c_{ik})$, $B = (b_{jm})$ und $T = (t_{ij})$ als

$$C = T^{\text{transp}}BT$$

und die Behauptung folgt dann aus dem Determinantenmultiplikationssatz und Satz 17.5 (Lineare Algebra (Osnabrück 2017-2018)). □

Bei einer endlichen Körpererweiterung $K \subseteq L$ in Charakteristik null ist die Spurabbildung $L \to K$ nicht die Nullabbildung, siehe Lemma 8.8 (Körper- und Galoistheorie (Osnabrück 2018-2019)) (2). Daraus ergibt sich auch das folgende Resultat.

Lemma 8.3. *Es sei $K \subseteq L$ eine separable endliche Körpererweiterung vom Grad n und sei $b_1, \ldots, b_n$ eine K-Basis von L. Dann ist*

$$\triangle(b_1, \ldots, b_n) \neq 0.$$

Satz 8.4. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in R. Es seien $b_1, \ldots, b_n \in \mathfrak{a}$ Elemente, die eine $\mathbb{Q}$-Basis von L bilden und für die der Betrag der Diskriminante*

$$|\triangle(b_1, \ldots, b_n)|$$

unter all diesen Basen aus $\mathfrak{a}$ minimal sei. Dann ist

$$\mathfrak{a} = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n.$$

Beweis. Zunächst sind wegen Korollar 7.11 die Spuren zu Elementen aus R ganzzahlig und somit sind auch die in Frage stehenden Diskriminanten ganzzahlig. Man kann also die Diskriminanten bzw. ihre Beträge untereinander der Größe nach vergleichen.

Es sei $f \in \mathfrak{a}$ ein beliebiges Element. Wir haben zu zeigen, dass sich f als eine $\mathbb{Z}$-Linearkombination $f = k_1b_1 + \cdots + k_nb_n$ mit $k_i \in \mathbb{Z}$ schreiben lässt, wenn die $b_1, \ldots, b_n \in \mathfrak{a}$ eine $\mathbb{Q}$-Basis von L mit minimalem Diskriminantenbetrag bilden. Es gibt eine eindeutige Darstellung

$$f = q_1b_1 + \cdots + q_nb_n$$

mit rationalen Zahlen $q_i \in \mathbb{Q}$. Sei angenommen, dass ein q_i nicht ganzzahlig ist, wobei wir $i = 1$ annehmen dürfen. Wir schreiben dann $q_1 = k + \delta$ mit $k \in \mathbb{Z}$ und einer rationalen Zahl δ (echt) zwischen 0 und 1. Dann ist auch

$$c_1 = f - kb_1 = \delta b_1 + \sum_{i=2}^{n} q_ib_i,\ b_2, \ldots, b_n$$

eine $\mathbb{Q}$-Basis von L, die in $\mathfrak{a}$ liegt. Die Übergangsmatrix der beiden Basen ist

$$T = \begin{pmatrix} \delta & q_2 & q_3 & \cdots & q_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Nach Lemma 8.2 gilt für die beiden Diskriminanten die Beziehung

$$\triangle(c_1, b_2, \ldots, b_n) = (\det(T))^2 \triangle(b_1, b_2, \ldots, b_n).$$

Wegen $(\det(T))^2 = \delta^2 < 1$ und da die Diskriminanten nach Lemma 8.3 nicht 0 sind, ist dies ein Widerspruch zur Minimalität der Diskriminante. □

Korollar 8.5. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal in R. Dann ist $\mathfrak{a}$ eine freie abelsche Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in \mathfrak{a}$ mit*

$$\mathfrak{a} = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n,$$

wobei die Koeffizienten in einer Darstellung eines Elementes aus $\mathfrak{a}$ eindeutig bestimmt sind.

Beweis. Nach Lemma 7.7 gibt es überhaupt Elemente $b_1, \ldots, b_n \in \mathfrak{a}$, die eine $\mathbb{Q}$-Basis von L bilden. Daher gibt es auch solche Basen, wo der (ganzzahlige) Betrag der Diskriminante minimal ist. Für diese gilt nach Satz 8.4, dass sie ein $\mathbb{Z}$-Erzeugendensystem von $\mathfrak{a}$ bilden. Die lineare Unabhängigkeit über $\mathbb{Q}$ sichert die Eindeutigkeit der Koeffizienten. □

Korollar 8.6. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Dann ist R eine freie abelsche Gruppe vom Rang n, d.h. es gibt Elemente $b_1, \ldots, b_n \in R$ mit*

$$R = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n$$

derart, dass die Koeffizienten in einer Darstellung eines Elementes eindeutig bestimmt sind.

Beweis. Dies folgt direkt aus Korollar 8.5, angewendet auf das Ideal $\mathfrak{a} = R$. □

Ein solches System von Erzeugern $b_1, \ldots, b_n$ nennt man auch eine *Ganzheitsbasis* von R. Insbesondere gibt es in einem Zahlbereich stets Ganzheitsbasen. Im Ring der Eisensteinzahlen ist $1, \sqrt{-3}$ keine Ganzheitsbasis, $1, \frac{-1+\sqrt{3}}{2}$ hingegen schon. Es ergibt sich ferner, dass man eine ganzzahlige Multiplikationsmatrix erhält, wenn man als Basis eine Ganzheitsbasis nimmt. Mit dieser kann man insbesondere die Spur und die Norm ausrechnen.

Definition 8.7. Es sei R der Zahlbereich zur endlichen Körpererweiterung $\mathbb{Q} \subseteq L$. Dann nennt man die Diskriminante einer Ganzheitsbasis von R die *Diskriminante* von R (und die *Diskriminante* von L).

Die Diskriminante eines Zahlbereichs (oder eines Zahlkörpers) ist eine wohldefinierte ganze Zahl. Nach Definition ist die Diskriminante so gewählt, dass sie betragsmäßig minimal unter allen Diskriminanten zu $\mathbb{Z}$-Basen aus R ist. Zwei solche Diskriminanten unterscheiden sich um ein Quadrat einer Einheit aus $\mathbb{Z}$, so dass auch das Vorzeichen wohldefiniert ist. Wir bezeichnen sie mit $\triangle_L$.

Die bisherigen Ergebnisse erlauben es, die Faserringe zu $\mathbb{Z} \subseteq R$ über einem Primideal (p) zumindest anzahlmäßig zu verstehen. Es handelt sich um endliche Ringe mit p^n Elementen. Insbesondere gibt es oberhalb von (p) stets Primideale und zwar höchstens n Stück.

Korollar 8.8. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und R der zugehörige Zahlbereich. Es sei $m \in \mathbb{Z}$. Dann gibt es einen Gruppenisomorphismus*

$$R/(m) \cong (\mathbb{Z}/(m))^n.$$

Für eine Primzahl $m = p$ ist $R/(m)$ eine Algebra der Dimension n über dem Körper $\mathbb{Z}/(p)$. Zu jeder Primzahl p gibt es Primideale $\mathfrak{p}$ in R mit $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Beweis. Nach Korollar 8.6 ist $R \cong \mathbb{Z}^n$ (als abelsche Gruppen), wobei die Standardbasis der Ganzheitsbasis $a_1, \ldots, a_n$ entsprechen möge. Das von m in R erzeugte Ideal besteht aus allen $\mathbb{Z}$-Linearkombinationen der $ma_1, \ldots, ma_n$ und somit entspricht das Ideal (unter dieser Identifizierung) der von $(m, 0, \ldots, 0), (0, m, 0, \ldots, 0), \ldots, (0, \ldots, 0, m)$ erzeugten Untergruppe von $\mathbb{Z}^n$. Die Restklassengruppe $R/(m)$ ist demnach gleich $(\mathbb{Z}/(m))^n$ und besitzt m^n Elemente. Aufgrund der Ganzheit ist nach Aufgabe 6.22 $mR \cap \mathbb{Z} = m\mathbb{Z}$ und aufgrund des Homomorphiesatzes hat man einen injektiven Ringhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow R/(m),$$

so dass $R/(m)$ eine von 0 verschiedene $\mathbb{Z}/(m)$-Algebra ist.

Für eine Primzahl p ist $R/(p)$ ein Vektorraum über $\mathbb{Z}/(p)$ der Dimension n. Deshalb gibt es darin (mindestens) ein maximales Ideal, und dieses entspricht nach Aufgabe 3.16 einem maximalen Ideal $\mathfrak{m}$ in R mit $p \in \mathfrak{m}$. Daher ist $(p) = (p)R \cap \mathbb{Z} \subseteq \mathfrak{m} \cap \mathbb{Z}$, und dieser Durchschnitt ist ein Primideal, also gleich (p). □

8.2. **Weitere Berechnungsmöglichkeiten.**

Lemma 8.9. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und es sei $b_1, \ldots, b_n$ eine $\mathbb{Q}$-Basis von L. Es seien $\tau_j \colon L \to \mathbb{C}$ die n verschiedenen Einbettungen in $\mathbb{C}$. Dann ist*

$$\triangle(b_1, \ldots, b_n) = (\det(\tau_j(b_k)))^2.$$

Beweis. Nach Lemma 7.14 ist die Spur eines Elementes $z \in L$ gleich der Summe $\sum_{j=1}^n \tau_j(z)$. Für ein Produkt wz ist somit

$$\operatorname{Spur}(wz) = \sum_{j=1}^n \tau_j(wz) = \sum_{j=1}^n \tau_j(w)\tau_j(z).$$

Insbesondere ist

$$\operatorname{Spur}(b_i b_k) = \sum_{j=1}^n \tau_j(b_i)\tau_j(b_k).$$

Somit ist

$$(\operatorname{Spur}(b_i b_k))_{1 \leq i,k \leq n} = (\tau_j(b_i))^{\mathrm{tr}}(\tau_j(b_k))$$

und daher nach Satz 17.4 (Lineare Algebra (Osnabrück 2017-2018))

$$\begin{aligned} \triangle(b_1, \ldots, b_n) &= \det(\operatorname{Spur}(b_i b_k)) \\ &= (\det(\tau_j(b_i)))^2. \end{aligned}$$

□

Besonders wichtig ist der Fall, wenn die Basis eine Basis eines Ideals oder eine Ganzheitsbasis ist. In dieser Situation fixieren wir die folgende Sprechweise.

Definition 8.10. Es sei R ein Zahlbereich vom Grad n und

$$\tau \colon R \longrightarrow \mathbb{C}^n$$

die komplexe Gesamteinbettung. Es sei $b_1, \ldots, b_n$ eine Ganzheitsbasis von R. Dann nennt man die komplexe $n \times n$-Matrix

$$(\tau_j(b_k))_{1 \leq j,k \leq n}$$

die *komplexe Ganzheitsmatrix* (zu dieser Basis).

Lemma 8.11. *Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung vom Grad n und es sei $b \in L$ derart, dass die Potenzen $1, b, b^2, \ldots, b^{n-1}$ eine $\mathbb{Q}$-Basis von L bilden. Es seien $\tau_j \colon L \to \mathbb{C}$ die n verschiedenen Einbettungen in $\mathbb{C}$. Dann ist*

$$\triangle(1, b, b^2, \ldots, b^{n-1}) = \prod_{1 \leq i < j \leq n} (\tau_i(b) - \tau_j(b))^2.$$

Beweis. Nach Lemma 8.9 ist die Diskriminante das Quadrat der Determinante der komplexen Matrix

$$\begin{pmatrix} 1 & \tau_1(b) & \tau_1(b)^2 & \dots & \tau_1(b)^{n-1} \\ 1 & \tau_2(b) & \tau_2(b)^2 & \dots & \tau_2(b)^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \tau_{n-1}(b) & \tau_{n-1}(b)^2 & \dots & \tau_{n-1}(b)^{n-1} \\ 1 & \tau_n(b) & \tau_n(b)^2 & \dots & \tau_n(b)^{n-1} \end{pmatrix}.$$

Dies ist eine Vandermonde-Matrix und ihre Determinante ist gleich

$$\prod_{i<j} (\tau_i(b) - \tau_j(b)).$$

□

8. Arbeitsblatt

8.1. **Aufgaben.**

Aufgabe 8.1. Sei R ein Zahlbereich und sei $f_1, \dots, f_n \in R$ eine $\mathbb{Z}$-Basis von R. Zeige, dass dann der Betrag der Diskriminante

$$|\triangle(f_1, \dots, f_n)|$$

minimal ist unter allen Diskriminanten von linear unabhängigen n-Tupeln aus R.

Aufgabe 8.2. Berechne die Diskriminante der Gaußschen Zahlen. Man gebe zwei wesentlich verschiedene $\mathbb{Z}$-Basen von $\mathbb{Z}[\mathrm{i}]$ an und überprüfe, dass die Diskriminanten übereinstimmen.

Aufgabe 8.3. Berechne die Diskriminante zur Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{i}]$$

zur Basis 1 und i und zur Basis $2 - 5\mathrm{i}$ und $4 + 7\mathrm{i}$.

Aufgabe 8.4. Bestimme die Diskriminante zur Basis $1, x, x^2$ der kubischen Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\big(X^3 - 5X^2 + 6X - 3\big) =: L.$$

Aufgabe 8.5.*

Sei K ein Körper der Charakteristik 0 und sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und sei $b_1, \dots, b_n$ eine K-Basis von L. Zeige, dass dann

$$\triangle(b_1, \dots, b_n) \neq 0.$$

Aufgabe 8.6. Es sei R ein Zahlbereich der Form $R = \mathbb{Z}[X]/(F)$ mit einem normierten Polynom $F \in \mathbb{Z}[X]$ vom Grad d. Zeige, dass x^i, $i = 0, \ldots, n-1$, eine Ganzheitsbasis von R ist.

Aufgabe 8.7.*

Finde ganze Zahlen a, b, c, d, e, f derart, dass die Determinante der Matrix

$$\begin{pmatrix} 6 & 10 & 15 \\ a & b & c \\ d & e & f \end{pmatrix}$$

gleich 1 ist.

Aufgabe 8.8. Es sei $(a_1, \ldots, a_n)$ ein teilerfremdes Tupel von ganzen Zahlen. Zeige, dass es eine $n \times n$-Matrix gibt, die das Tupel als eine Zeile enthält und deren Determinante gleich ± 1 ist.

Führe Induktion über das Minimum der Beträge des Tupels.

Mit der vorstehenden Aufgabe kann man auch die folgende Aufgabe lösen.

Aufgabe 8.9. Zeige, dass es in einem Zahlbereich stets Ganzheitsbasen gibt, die die 1 enthalten.

Aufgabe 8.10. Es sei $\mathbb{Q} \subseteq L = \mathbb{Q}[X]/(F)$ eine endliche Körpererweiterung mit einem normierten Polynom $F \in \mathbb{Z}[X]$ und sei R der zugehörige Zahlbereich. Zeige, dass es ein $g \in \mathbb{N}_+$ derart gibt, dass nach Nenneraufnahme an g eine Ringisomorphie

$$R_g = \mathbb{Z}_g[X]/(F)$$

vorliegt.

Aufgabe 8.11. Man gebe Beispiele für Zahlbereiche R, wo die Spur $R \to \mathbb{Z}$ surjektiv bzw. nicht surjektiv ist.

Aufgabe 8.12. Finde möglichst viele (nicht isomorphe) kommutative Ringe mit vier Elementen. Beweise, dass die Liste vollständig ist.

Aufgabe 8.13.*

Man gebe eine vollständige Liste aller kommutativer Ringe mit 6 Elementen.

Aufgabe 8.14. Sei p eine Primzahl und $q = p^n$, $n \geq 2$. Zeige, dass $\mathbb{Z}/(p^n)$ kein Vektorraum über $\mathbb{Z}/(p)$ sein kann.

Aufgabe 8.15. Es sei R ein endlicher reduzierter kommutativer Ring. Zeige, dass R ein Produkt von endlichen Körpern ist.

Aufgabe 8.16. Es sei p eine Primzahl und sei R eine endlichdimensionale $\mathbb{Z}/(p)$-Algebra der Dimension n. Zeige, dass R höchstens n Primideale besitzt.

Aufgabe 8.17. Sei R ein Zahlbereich und sei $f \in R$. Zeige, dass $N(f) \in (f)$ ist, dass also die Norm zum von f erzeugten Hauptideal gehört. Zeige durch ein Beispiel, dass dies für die Spur nicht gelten muss.

9. Vorlesung - Quadratische Zahlbereiche

9.1. **Quadratische Zahlbereiche.**

Wir beschreiben nun die bisher entwickelten Konzepte im Fall von quadratischen Zahlbereichen genauer. In diesen lassen sich sehr häufig viele Sachen mit einem vertretbaren Aufwand ausrechnen, zugleich zeigen sich aber auch schon viele typische Phänomene der allgemeinen Theorie.

Definition 9.1. Ein *quadratischer Zahlbereich* ist der Ring der ganzen Zahlen in einem Erweiterungskörper von $\mathbb{Q}$ vom Grad 2.

Notation 9.2. Zu einer quadratfreien Zahl $D \neq 0, 1$ bezeichnet man den zugehörigen quadratischen Zahlbereich, also den Ring der ganzen Zahlen in $\mathbb{Q}[\sqrt{D}]$, mit

$$A_D \, .$$

Eine quadratische Körpererweiterung der rationalen Zahlen wird durch ein normiertes irreduzibles Polynom beschrieben, das man durch quadratisches Ergänzen auf die Form $X^2 - q$ bringen kann. Durch Multiplikation mit einem Quadrat (siehe Aufgabe 9.1) kann man q durch eine quadratfreie ganze Zahl ersetzen. Die quadratische Körpererweiterung kann man also als $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{D}]$ mit einer quadratfreien Zahl $D \neq 0, 1$ ansetzen. Ein großer Unterschied besteht je nachdem, ob D positiv oder negativ ist. Im positiven Fall ist $\sqrt{D}$ eine reelle irrationale Zahl, im negativen Fall handelt es sich um eine imaginäre Zahl. Man definiert:

Definition 9.3. Es sei $D \neq 0, 1$ quadratfrei und sei A_D der zugehörige quadratische Zahlbereich. Dann heißt A_D *reell-quadratisch*, wenn D positiv ist, und *imaginär-quadratisch*, wenn D negativ ist.

Definition 9.4. Es sei $D \neq 0,1$ eine quadratfreie Zahl und sei $\mathbb{Q}[\sqrt{D}]$ die zugehörige quadratische Körpererweiterung und A_D der zugehörige quadratische Zahlbereich. Dann wird der Automorphismus (auf $\mathbb{Q}[\sqrt{D}]$, auf $\mathbb{Z}[\sqrt{D}]$ und auf A_D)

$$a+b\sqrt{D} \longmapsto a-b\sqrt{D}$$

als *Konjugation* bezeichnet.

Wir bezeichnen die Konjugation von z mit $\bar{z}$.

Bemerkung 9.5. Im imaginär-quadratischen Fall, wenn also $D < 0$ ist, so ist $\sqrt{D} = \mathrm{i}\sqrt{-D}$ mit $\sqrt{-D}$ reell. Die Konjugation schickt dies dann auf $-\sqrt{D} = -\mathrm{i}\sqrt{-D}$, so dass diese Konjugation mit der komplexen Konjugation übereinstimmt. Im reell-quadratischen Fall allerdings hat die Konjugation $\sqrt{D} \mapsto -\sqrt{D}$ nichts mit der komplexen Konjugation zu tun.

Bemerkung 9.6. Bei einer endlichen Körpererweiterung $K \subseteq L$ werden Norm und Spur eines Elementes $x \in L$ über die Determinante und die Spur der Multiplikationsabbildung $f\colon L \to L$ definiert. Im Fall einer quadratischen Erweiterung

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{D}]$$

sind diese beiden Invarianten einfach zu berechnen: Da 1 und $\sqrt{D}$ eine $\mathbb{Q}$-Basis bilden, ist $z = a+b\sqrt{D}$ und damit ist die Multiplikationsmatrix durch

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

gegeben. Somit ist

$$N(z) = a^2 - b^2 D = (a+b\sqrt{D})(a-b\sqrt{D}) = z\overline{z}$$

und

$$S(z) = 2a = (a+b\sqrt{D}) + (a-b\sqrt{D}) = z+\overline{z}.$$

Lemma 9.7. *Es sei $\mathbb{Q} \subset L$ eine quadratische Körpererweiterung und $f \in L$. Dann ist f genau dann ganz über $\mathbb{Z}$, wenn sowohl die Norm als auch die Spur von f zu $\mathbb{Z}$ gehören.*

Beweis. Dies folgt aus Satz 7.5, aus Satz 8.10 (Körper- und Galoistheorie (Osnabrück 2018-2019)), und aus der Gestalt des Minimalpolynoms (nämlich gleich $f^2 - S(f)f + N(f)$, falls $f \notin \mathbb{Q}$) im quadratischen Fall. □

Wir kommen zur expliziten Beschreibung eines quadratischen Zahlbereiches.

Satz 9.8. *Es sei $D \neq 0,1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Dann gilt*

$$A_D = \mathbb{Z}[\sqrt{D}], \text{ wenn } D = 2,3 \mod 4$$

und

$$A_D = \mathbb{Z}[\frac{1+\sqrt{D}}{2}], \text{ wenn } D = 1 \mod 4\,.$$

Beweis. Sei $x \in A_D$ gegeben, $x = a+b\sqrt{D}$, $a, b \in \mathbb{Q}$. Aus Lemma 9.7 folgt

$$N(x) = a^2 - Db^2 \in \mathbb{Z} \text{ und } S(x) = 2a \in \mathbb{Z}\,.$$

Aus der zweiten Gleichung folgt, dass $a = \frac{n}{2}$ mit $n \in \mathbb{Z}$ ist. Sei $b = \frac{r}{s}$ mit r, s teilerfremd, $s \geq 1$. Die erste Gleichung wird dann zu $\left(\frac{n}{2}\right)^2 - D\left(\frac{r}{s}\right)^2 = k \in \mathbb{Z}$ bzw. $n^2 - 4D\left(\frac{r}{s}\right)^2 = 4k$. Dies bedeutet, da r und s teilerfremd sind, dass $4D$ von s^2 geteilt wird. Da ferner D quadratfrei ist, folgt, dass $s = 1$ oder $s = 2$ ist. Im ersten Fall ist n ein Vielfaches von 2 (da n^2 ein Vielfaches von 4 ist), so dass $x \in \mathbb{Z}[\sqrt{D}]$ ist.

Sei also $s = 2$, was zur Bedingung

$$n^2 - Dr^2 = 4k$$

führt. Wir betrachten diese Gleichung modulo 4. Bei n und r gerade ist $x \in \mathbb{Z}[\sqrt{D}]$. Die einzigen Quadrate in $\mathbb{Z}/(4)$ sind 0 und 1, so dass für $D = 2, 3 \mod 4$ keine weitere Lösung existiert. Für $D = 1 \mod 4$ hingegen gibt es auch noch die Lösung $n = 1 \mod 2$ und $r = 1 \mod 2$, also n und r beide ungerade. Diese Lösungen gehören alle zu $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.

Die umgekehrte Inklusion $\mathbb{Z}[\sqrt{D}] \subseteq A_D$ ist klar, sei also $D = 1 \mod 4$. Dann ist aber

$$\left(\frac{1+\sqrt{D}}{2}\right)^2 - \frac{1+\sqrt{D}}{2} = \frac{1+D+2\sqrt{D}-2-2\sqrt{D}}{4} = \frac{D-1}{4} \in \mathbb{Z},$$

und dabei ist $\frac{D-1}{4}$ eine ganze Zahl, so dass dies sofort eine Ganzheitsgleichung über $\mathbb{Z}$ ergibt. □

In den im vorstehenden Satz beschriebenen Fällen kann man jeweils den Ring der ganzen Zahlen durch eine Variable und eine Gleichung beschreiben. Für $D = 2, 3 \mod 4$ ist

$$A_D \cong \mathbb{Z}[\sqrt{D}] \cong \mathbb{Z}[X]/(X^2 - D).$$

Für $D = 1 \mod 4$ setzt man häufig $\omega = \frac{1+\sqrt{D}}{2}$ für den Algebra-Erzeuger. Dieser Erzeuger erfüllt die Gleichung $\omega^2 - \omega - \frac{D-1}{4} = 0$. Wir haben also

$$A_D \cong \mathbb{Z}[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right).$$

Wir werden häufiger in beiden Fällen diese Ganzheitsbasis $1, \omega$ nennen, mit $\omega = \sqrt{D}$ im ersten Fall und

$$\omega = \frac{1+\sqrt{D}}{2}$$

im zweiten Fall.

Lemma 9.9. *Es sei $D \neq 0, 1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Dann ist die Diskriminante von A_D gleich*

$$\triangle = 4D, \text{ wenn } D = 2, 3 \mod 4$$

und

$$\triangle = D, \text{ wenn } D = 1 \mod 4\,.$$

Beweis. Im Fall $D = 2, 3 \mod 4$ ist nach Satz 9.8 $A_D = \mathbb{Z}[X]/(X^2 - D)$ und daher bilden 1 und X eine Ganzheitsbasis. Die möglichen Produkte zu dieser Basis sind in Matrixschreibweise

$$\begin{pmatrix} 1 & X \\ X & D \end{pmatrix}.$$

Wendet man darauf komponentenweise die Spur an so erhält man

$$\begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix}$$

und die Determinante davon ist $4D$.

Im Fall $D = 1 \mod 4$ ist hingegen

$$A_D = \mathbb{Z}[\omega]/\left(\omega^2 - \omega - \frac{D-1}{4}\right)$$

und eine Ganzheitsbasis ist 1 und ω. Die Matrix der Basisprodukte ist dann

$$\begin{pmatrix} 1 & \omega \\ \omega & \omega + \frac{D-1}{4} \end{pmatrix}.$$

Wendet man darauf die Spur an (die Spur von ω ist 1), so erhält man

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 + \frac{D-1}{2} \end{pmatrix}$$

und die Determinante davon ist

$$2\left(1 + \frac{D-1}{2}\right) - 1 = 2 + D - 1 - 1 = D.$$

□

9.2. **Die Summe von Quadraten.**

Wir haben nun die Mittel an der Hand, um die Zahlen, die die Summe von zwei Quadratzahlen sind, mit Hilfe des Ringes der Gaußschen Zahlen zu charakterisieren.

Satz 9.10. *Es sei p ein ungerade Primzahl. Dann sind folgende Aussagen äquivalent.*

(1) *p ist die Summe von zwei Quadraten, $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$.*
(2) *p ist die Norm eines Elementes aus $\mathbb{Z}[\mathrm{i}]$.*
(3) *p ist zerlegbar (nicht prim) in $\mathbb{Z}[\mathrm{i}]$.*

(4) -1 *ist ein Quadrat in* $\mathbb{Z}/(p)$.
(5) *Es ist* $p = 1 \mod 4$.

Beweis. Siehe Aufgabe 9.22. □

Satz 9.11. *Es sei* n *eine positive natürliche Zahl. Wir schreiben* $n = r^2 m$, *wobei jeder Primfaktor von* m *nur einfach vorkomme. Dann ist* n *die Summe von zwei Quadraten genau dann, wenn in der Primfaktorzerlegung von* m *nur* 2 *und Primzahlen vorkommen, die modulo* 4 *den Rest* 1 *haben.*

Beweis. Siehe Aufgabe 9.23. □

9.3. **Noethersche Ringe und Dedekindbereiche.**

Emmy Noether (1882-1935)

Definition 9.12. Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal darin endlich erzeugt ist.

Korollar 9.13. *Jeder Zahlbereich ist ein noetherscher Ring.*

Beweis. Nach Korollar 8.5 ist jedes von 0 verschiedene Ideal als additive Gruppe isomorph zu $\mathbb{Z}^n$, also ist insbesondere jedes Ideal als abelsche Gruppe endlich erzeugt. Insbesondere sind die Ideale dann als Ideale (also als R-Moduln) endlich erzeugt. □

Satz 9.14. *Zu einem Ideal* $\mathfrak{a} \neq 0$ *in einem Zahlbereich* R *ist der Restklassenring* $R/\mathfrak{a}$ *endlich.*

Beweis. Nach Lemma 7.6 gibt es ein $m \in \mathbb{Z} \cap \mathfrak{a}$, $m \neq 0$. Damit ist $mR \subseteq \mathfrak{a}$ und damit hat man eine surjektive Abbildung

$$R/(m) \longrightarrow R/\mathfrak{a}.$$

Der Ring links ist nach Korollar 8.8 endlich (mit m^n Elementen), also besitzt der Ring rechts auch nur endlich viele Elemente. □

Wir geben noch einen zweiten Beweis der vorstehenden Aussage.

Als kommutative Gruppe ist $R = \mathbb{Z}^n$. Sei $a \in \mathfrak{a}$, $a \neq 0$. Dann ist das von a erzeugte Hauptideal eine Untergruppe

$$aR \cong \mathbb{Z}^n \subseteq R \cong \mathbb{Z}^n.$$

Deshalb ist die Restklassengruppe $\mathbb{Z}^n/aR$ endlich und wegen der natürlichen Surjektion $\mathbb{Z}^n/aR \to R/\mathfrak{a}$ ist auch der Restklassenring endlich.

Satz 9.15. *Sei R ein Zahlbereich. Dann ist jedes von 0 verschiedene Primideal von R bereits ein maximales Ideal.*

Beweis. Sei $\mathfrak{p}$ ein Primideal $\neq 0$ in R. Dann ist der Restklassenring $R/\mathfrak{p}$ nach Lemma 3.3 ein Integritätsbereich und nach Satz 9.14 endlich. Ein endlicher Integritätsbereich ist aber nach Aufgabe 5.36 bereits ein Körper, so dass nach Lemma 3.5 ein maximales Ideal vorliegt. □

Richard Dedekind (1831-1916)

Die bisher etablierten Eigenschaften von Zahlbereichen lassen sich im folgenden Begriff zusammenfassen.

Definition 9.16. Einen Integritätsbereich R nennt man einen *Dedekindbereich*, wenn er noethersch und normal ist und wenn jedes von 0 verschiedene Primideal darin maximal ist.

Die Eigenschaft, dass jedes von 0 verschiedene Primideal maximal ist, bedeutet, dass die maximalen Ketten von Primidealen die Form $0 \subset \mathfrak{m}$ besitzen (wenn ein Körper vorliegt, so gibt es nur das einzige Primideal 0). Man sagt auch, dass die *Krulldimension* des Ringes gleich 1 ist.

Korollar 9.17. *Jeder Zahlbereich ist ein Dedekindbereich.*

Beweis. Dies folgt aus Satz 7.2, aus Korollar 9.13 und aus Satz 9.15. □

Satz 9.18. *Hauptidealbereiche sind Dedekindbereiche.*

Beweis. Die Normalität folgt aus Satz 2.19 und Satz 6.12. Die Eigenschaft noethersch folgt, da in einem Hauptidealbereich jedes Ideal sogar von einem Element erzeugt wird. Die Maximalität der von 0 verschiedenen Primideale folgt aus Lemma 3.7. □

9. Arbeitsblatt

9.1. **Aufgaben.**

Aufgabe 9.1.*

Betrachte die Quadratrestgruppe

$$\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\,,$$

wobei $\mathbb{Q}^{\times 2}$ die Untergruppe der Quadrate bezeichne. Zeige, dass es zu jeder Restklasse $x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ einen Repräsentanten aus $\mathbb{Z}$ gibt.

Aufgabe 9.2. Für einen Körper K bezeichnet $K^{\times 2} \subseteq K^\times$ die Untergruppe aller Quadrate. Bestimme für die folgenden Körper die Restklassengruppe

$$K^\times/K^{\times 2}\,.$$

(1) K ist ein endlicher Körper.
(2) $K = \mathbb{R}$.
(3) $K = \mathbb{C}$.
(4) $K = \mathbb{Q}$.

Aufgabe 9.3. Zeige, dass die Konjugation auf $\mathbb{Q}[\sqrt{D}]$ ein Körperautomorphismus und auf A_D ein Ringautomorphismus ist. Zeige, dass der Invariantenring gleich $\mathbb{Q}$ bzw. gleich $\mathbb{Z}$ ist.

Aufgabe 9.4. Es sei R ein quadratischer Zahlbereich. Zeige, dass die 1 Teil einer Ganzheitsbasis von R ist.

Aufgabe 9.5. Bestimme die Konjugation für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 9.6. Bestimme die Spur für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 9.7. Bestimme die Norm für $\sqrt{D}$ bzw. für ω in den verschiedenen expliziten Beschreibungen für die quadratischen Zahlbereiche.

Aufgabe 9.8.*

Berechne explizit die Diskriminante des quadratischen Zahlbereichs A_{-7}. Stelle die Multiplikationsmatrix bezüglich einer geeigneten Basis für das Element

$$f = \frac{3}{2} + \frac{5}{2}\sqrt{-7}$$

auf und berechne damit die Spur und die Norm von f.

Aufgabe 9.9. Bestimme den (Isomorphietyp des) Ganzheitsringes der quadratischen Körpererweiterung

$$\mathbb{Q} \subset \mathbb{Q}[X]/\left(X^2 + \frac{3}{2}X - \frac{5}{7}\right).$$

Aufgabe 9.10. Seien D und E zwei verschiedene quadratfreie Zahlen und seien A_D und A_E die zugehörigen quadratischen Zahlbereiche. Zeige

$$A_D \cap A_E = \mathbb{Z}.$$

Aufgabe 9.11.*

Bestimme ein Element aus $\mathbb{Z}[\sqrt{-11}]$, das unter allen Nichteinheiten minimale Norm besitzt. Begründe, dass dieses Element irreduzibel ist.

Aufgabe 9.12. Es sei $D \neq 0, 1$ quadratfrei. Bestimme die Restklassengruppe $A_D/\mathbb{Z}[\sqrt{D}]$.

Aufgabe 9.13. Sei D eine quadratfreie Zahl mit $D = 1 \mod 4$, und sei A_D der zugehörige quadratische Zahlbereich. Man gebe eine Ganzheitsgleichung für $\frac{1+\sqrt{D}}{2}$ über $\mathbb{Z}$ an. Man zeige, dass es keine echten Zwischenringe $\mathbb{Z}[\sqrt{D}] \subset R \subset A_D$ gibt.

Aufgabe 9.14. Es sei $D \neq 0,1$ eine quadratfreie Zahl, sei $R = \mathbb{Z}[\sqrt{D}]$ und sei A_D der zugehörige Ganzheitsring. Zeige, dass nach Nenneraufnahme an 2 ein Ringisomorphismus

$$R_2 \longrightarrow (A_D)_2$$

vorliegt.

Aufgabe 9.15. Bestimme für die quadratischen Zahlbereiche A_D mit negativem D sämtliche Einheiten.

Aufgabe 9.16.*

Für welche quadratfreien Zahlen mit

$$D = 1 \mod 4$$

ist $\frac{1+\sqrt{D}}{2}$ eine Einheit?

Aufgabe 9.17. Finde ein quadratfreies D derart, dass die natürliche Inklusion

$$\mathbb{Z}[\sqrt{D}] \subseteq A_D$$

die Eigenschaft besitzt, dass es zwei verschiedene Primideale $\mathfrak{q}$ und $\mathfrak{q}'$ in A_D gibt, die beide über dem gleichen Primideal $\mathfrak{p} \subset \mathbb{Z}[\sqrt{D}]$ liegen. Was ist $\mathfrak{p} \cap \mathbb{Z}$?

Aufgabe 9.18.*

Es sei $D \neq 0,1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Zeige, dass es für eine Primzahl p die folgenden drei Möglichkeiten:

(1) p ist prim in A_D.
(2) Es gibt ein Primideal $\mathfrak{p}$ in A_D derart, dass $(p) = \mathfrak{p}^2$ ist.
(3) Es gibt ein Primideal $\mathfrak{p}$ in A_D derart, dass $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ mit $\mathfrak{p} \neq \overline{\mathfrak{p}}$ ist.

Aufgabe 9.19. Es sei $D \neq 0,1$ eine quadratfreie Zahl und A_D der zugehörige quadratische Zahlbereich. Zeige, dass für eine ungerade Primzahl p, die kein Teiler von D ist, folgende Aussagen äquivalent sind.

(1) D ist ein Quadrat in $\mathbb{Z}/(p)$.
(2) Es gibt zwei Primideale in A_D oberhalb von (p).

Aufgabe 9.20. Es sei R ein quadratischer Zahlbereich. Zeige, dass es nur endlich viele Primzahlen mit der Eigenschaft gibt, dass der Faserring über $\mathbb{Z}/(p)$ nicht reduziert ist.

Aufgabe 9.21. Es sei R ein quadratischer Zahlbereich. Zeige, dass die Konjugation zu jeder Primzahl p einen $\mathbb{Z}/(p)$-Algebraisomorphismus des Faserringes über p in sich selbst induziert. Beschreibe diesen in den drei möglichen Fällen im Sinne von Aufgabe 5.29 bzw. Aufgabe 9.16.

Aufgabe 9.22. Sei $D \neq 0,1$ eine quadratfreie Zahl und betrachte die quadratische Erweiterung $\mathbb{Z} \subset \mathbb{Z}[\sqrt{D}]$. Es sei p ein Primfaktor von D und es sei vorausgesetzt, dass weder p noch $-p$ ein Quadratrest modulo D/p ist. Dann ist p irreduzibel in $\mathbb{Z}[\sqrt{D}]$, aber nicht prim.

Aufgabe 9.23. Es sei $R = \mathbb{Z}[\sqrt{7}]$. Bestimme die Primideale in R, die über $p = 29$ liegen und zeige, dass es sich um Hauptideale handelt.

Aufgabe 9.24. Es sei $R = \mathbb{Z}[\sqrt{15}]$. Bestimme die Primideale in R, die über $p = 17$ liegen (man gebe Idealerzeuger an). Handelt es sich um Hauptideale?

Aufgabe 9.25. Zeige, dass 2 im Ring $\mathbb{Z}[\sqrt{5}]$ irreduzibel, aber nicht prim ist. Wie sieht es in A_5 aus?

Aufgabe 9.26.*

Es sei p ein ungerade Primzahl. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) p ist die Summe von zwei Quadraten, $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$.
(2) p ist die Norm eines Elementes aus $\mathbb{Z}[\mathrm{i}]$.
(3) p ist zerlegbar (nicht prim) in $\mathbb{Z}[\mathrm{i}]$.
(4) -1 ist ein Quadrat in $\mathbb{Z}/(p)$.
(5) Es ist $p = 1 \mod 4$.

Aufgabe 9.27.*

Es sei n eine positive natürliche Zahl. Wir schreiben $n = r^2 m$, wobei jeder Primfaktor von m nur einfach vorkomme. Zeige, dass dann n genau dann die Summe von zwei Quadraten ist, wenn in der Primfaktorzerlegung von m nur 2 und Primzahlen vorkommen, die modulo 4 den Rest 1 haben.

Aufgabe 9.28.*

Zeige, dass -3 genau dann ein Quadratrest modulo einer Primzahl $p \neq 2$ ist, wenn $p = 0,1 \mod 3$ ist.

Aufgabe 9.29. Es sei $\mathbb{Z}[\omega]$ der Ring der Eisenstein-Zahlen und p eine ungerade Primzahl. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) Es gibt eine Darstellung $p = x^2 + xy + y^2$ mit $x, y \in \mathbb{Z}$.
(2) p ist die Norm eines Elementes aus $\mathbb{Z}[\omega]$.
(3) p ist zerlegbar (nicht prim) in $\mathbb{Z}[\omega]$.
(4) -3 ist ein Quadrat in $\mathbb{Z}/(p)$.
(5) Es ist $p = 0, 1 \mod 3$.

Aufgabe 9.30. Es sei D eine quadratfreie positive Zahl mit $D = 3 \mod 4$. Zeige, dass der Zahlbereich zur Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{i}, \sqrt{D}]$ echt größer als $\mathbb{Z}[\mathrm{i}, \sqrt{D}]$ ist.

Aufgabe 9.31.*

Sei R ein noetherscher, kommutativer Ring. Zeige, dass dann auch jeder Restklassenring $R/\mathfrak{a}$ noethersch ist.

Aufgabe 9.32. Zeige: Ein kommutativer Ring R ist noethersch genau dann, wenn es in R keine unendliche echt aufsteigende Idealkette

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \dots$$

gibt.

Aufgabe 9.33. Zeige, dass das Produkt $R \times S$ zu noetherschen Ringen R und S wieder noethersch ist.

Aufgabe 9.34. Es sei K ein Körper. Zeige, dass es in $K[X, Y]$ keine obere Schranke für die Anzahl der Erzeuger von Idealen (in einem minimalen Erzeugendensystem) gibt.

Tipp: Betrachte die Potenzen $(X, Y)^m$.

Aufgabe 9.35. Sei R ein noetherscher Integritätsbereich. Zeige, dass sich jedes Element aus R als ein Produkt von irreduziblen Elementen schreiben lässt.

Aufgabe 9.36. Es sei R ein kommutativer Ring und seien $f_1, \dots, f_n \in R$ Elemente, die das Einheitsideal erzeugen. Es sei vorausgesetzt, dass die Nenneraufnahmen R_{f_i} für $i = 1, \dots, n$ noethersch sind. Zeige, dass dann auch R noethersch ist.

Aufgabe 9.37. Sei K ein Körper und sei

$$K[X_n,\, n \in \mathbb{N}]$$

der Polynomring über K in unendlich vielen Variablen. Man beschreibe darin ein nicht endlich erzeugtes Ideal und eine unendliche, echt aufsteigende Idealkette.

Aufgabe 9.38. Man gebe ein Beispiel eines nicht-noetherschen Ringes, dessen Reduktion ein Körper ist.

Aufgabe 9.39.*

Zeige, dass ein Unterring $R \subseteq S$ eines noetherschen Ringes nicht noethersch sein muss.

Aufgabe 9.40. Es sei R ein faktorieller Zahlbereich und $\mathbb{Z} \subseteq R$ die zugehörige Erweiterung. Zu einer Primzahl p sei

$$p = q_1^{r_1} \cdots q_k^{r_k}$$

die Primfaktorzerlegung von p in R (die q_i seien also paarweise nicht assoziiert). Zeige, dass die Primideale $\mathfrak{p}$ von R mit der Eigenschaft $\mathfrak{p} \cap \mathbb{Z} = (p)$ genau die Primideale der Form $\mathfrak{p} = (q_i)$ sind.

Aufgabe 9.41. Sei R ein Dedekindbereich und seien $\mathfrak{p}$ und $\mathfrak{q}$ verschiedene Primideale $\neq 0$. Dann gibt es einen Ringisomorphismus

$$R/\mathfrak{p} \cap \mathfrak{q} \longrightarrow R/\mathfrak{p} \times R/\mathfrak{q}.$$

Aufgabe 9.42. Sei R ein Dedekindbereich und seien $\mathfrak{p}$ und $\mathfrak{q}$ zwei verschiedene Primideale. Dann ist

$$\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p} \cdot \mathfrak{q}.$$

Aufgabe 9.43. Man gebe ein Beispiel für einen Dedekindbereich, wo jeder Restklassenring $\neq 0$ unendlich ist, und für einen Dedekindbereich, der einen Körper enthält und wo alle echten Restklassenringe endlich sind.

10. Vorlesung - Diskrete Bewertungsringe

10.1. **Die Norm für Zahlbereiche.**

Nach Korollar 7.11 ist die Norm eines Elementes eines Zahlbereiches ganzzahlig.

Lemma 10.1. *Es sei R der Ganzheitsring einer endlichen Körpererweiterung $\mathbb{Q} \subseteq L$. Dann ist $f \in R$ genau dann eine Einheit, wenn $N(f) = \pm 1$ ist.*

Beweis. Wenn $f \in R$ eine Einheit ist, so ist $fg = 1$ mit einem $g \in R$ und aus der Multiplikativität der Norm folgt

$$N(f)N(g) = N(1) = 1,$$

woraus nach Korollar 7.11 $N(f) = \pm 1$ folgt. Die Umkehrung folgt aus Korollar 8.6 und daraus, dass dann die Multiplikationsabbildung zu f auf $R \cong \mathbb{Z}^n$ bijektiv ist. □

Lemma 10.2. *Es sei R ein Zahlbereich vom Grad d und $n \in \mathbb{Z}$. Dann ist die Norm von n in R gleich n^d.*

Beweis. Dies ist ein Spezialfall von Lemma 8.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)). □

10.2. **Die Norm von Idealen.**

Definition 10.3. Zu einem Ideal $\mathfrak{a} \neq 0$ in einem Zahlbereich R heißt die (endliche) Anzahl des Restklassenringes $R/\mathfrak{a}$ die *Norm* von $\mathfrak{a}$. Sie wird mit

$$N(\mathfrak{a})$$

bezeichnet.

Beispiel 10.4. Zu einem von 0 verschiedenen Ideal $(n) \subseteq \mathbb{Z}$ mit $n > 0$ ist die Norm einfach gleich n, da ja der Restklassenring $\mathbb{Z}/(n)$ genau n Elemente besitzt.

Lemma 10.5. *Es sei $\mathfrak{a} \neq 0$ ein Ideal in einem Zahlbereich R. Dann ist $N(\mathfrak{a}) \in \mathfrak{a}$.*

Beweis. Wir betrachten die Abbildung

$$\mathbb{Z} \longrightarrow R \longrightarrow R/\mathfrak{a}\,.$$

Der Ring rechts hat nach Definition $N(\mathfrak{a})$ Elemente. Deshalb gehört diese Zahl zum Kern der Gesamtabbildung. □

Die Norm eines Ideals berechnet man am besten, indem man nach und nach den Restklassenring vereinfacht. Ein entscheidender Schritt ist dabei, eine ganze Zahl $n \neq 0$ in dem Ideal zu finden, da man dann über dem endlichen

Ring $\mathbb{Z}/(n)$ arbeiten und weiter vereinfachen kann. Dieses Verfahren hilft aufgrund der folgenden Aussage auch bei der Berechnung der Norm von Elementen.

Lemma 10.6. *Es sei R ein Zahlbereich und $f \in R$, $f \neq 0$. Dann ist der Betrag der Norm von f gleich der Norm des Hauptideals fR.*

Beweis. Das Hauptideal Rf ist das Bild des injektiven Gruppenhomomorphismus

$$R \longrightarrow R,\, 1 \longmapsto f.$$

Dieser wird unter einer Identifizierung $R = \mathbb{Z}^n$ (also der Wahl einer Ganzheitsbasis von R) durch die zu f gehörende Multiplikationsmatrix M_f beschrieben. Es liegt insgesamt dias kommutative Diagramm

$$\begin{array}{ccccccc} R & \xrightarrow{\mu_f} & R & \longrightarrow & R/fR & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathbb{Z}^n & \xrightarrow{M_f} & \mathbb{Z}^n & \longrightarrow & \mathbb{Z}^n/\operatorname{bild} M_f & \longrightarrow & 0 \end{array}$$

mit vertikalen Isomorpien vor. Die Determinante von M_f ist die Norm von f, und die Anzahl der Elemente in der Restklassengruppe R/fR ist die Norm des Hauptideals. Daher folgt die Aussage aus Satz Anhang 7.1. □

Beispiel 10.7. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$ das Ideal

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

Wir behaupten, dass es kein Hauptideal ist und verwenden dabei, dass die Norm dieses Ideals gleich 2 ist. Wäre nämlich $\mathfrak{p} = (f)$ mit einem $f \in R$, so müsste nach . auch

$$|N(f)| = 2$$

gelten. Allerdings ist die Norm von $f = a + b\sqrt{-5}$ gleich $N(f) = a^2 + 5b^2$ und dies kann nicht gleich 2 sein.

Korollar 10.8. *Es sei f ein Element in einem Zahlbereich R. Dann ist $N(f) \in fR$. Insbesondere ist $\frac{N(f)}{f} \in R$ bei $f \neq 0$.*

Beweis. Dies folgt aus Lemma 10.6 und Lemma 10.5, angewendet auf das Hauptideal $\mathfrak{a} = (f)$. □

Die Norm $R \to \mathbb{Z}$ hat die Eigenschaft, dass oberhalb von 1 nur Einheiten liegen. Auch für die Elemente aus R, deren Norm gleich einer fixierten ganzen Zahl a ist, gibt es eine wichtige Gesetzmäßigkeit.

Lemma 10.9. *Es sei R der Ganzheitsring einer endlichen Körpererweiterung $\mathbb{Q} \subseteq K$ und sei $a \in \mathbb{Z}$. Dann gibt es endlich viele Elemente $f_1, \ldots, f_m \in R$ derart, dass jedes $f \in R$ mit $|N(f)| = a$ zu einem der f_i assoziiert ist.*

Beweis. Der Restklassenring $R/(a)$ ist endlich nach Lemma 10.2 und Lemma 10.6. Wir behaupten, dass Elemente aus der gleichen Nebenklasse zu $R/(a)$, die beide die Norm a besitzen, zueinander assoziiert sind (für die f_j wählen wir zu jeder Nebenklasse von $R/(a)$ einen Repräsentanten mit Norm a aus, falls es überhaupt ein solches Element gibt). Seien dazu $f, g, h \in R$ mit

$$f = g + ah$$

und mit $N(f) = N(g) = a$. Dann ist in $Q(R)$

$$\frac{f}{g} = \frac{g+ah}{g} = 1 + a\frac{h}{g} = 1 + \frac{N(g)}{g}h$$

und dies gehört zu R, da $\frac{N(g)}{g}$ nach Korollar 10.8 zu R gehört. Dies gilt auch, wenn man die Rollen von f und g vertauscht. Also teilen sich f und g gegenseitig und sind daher assoziiert. □

10.3. **Diskrete Bewertungsringe.**

Definition 10.10. Ein *diskreter Bewertungsring* R ist ein Hauptidealbereich mit der Eigenschaft, dass es bis auf Assoziiertheit genau ein Primelement in R gibt.

Einen Erzeuger des maximalen Ideals in einem diskreten Bewertungsring nennt man auch eine *Ortsuniformisierende*. Wir wollen zeigen, dass zu einem Zahlbereich R die Lokalisierung an einem jeden maximalen Ideal ein diskreter Bewertungsring ist.

Lemma 10.11. *Ein diskreter Bewertungsring ist ein lokaler, noetherscher Hauptidealbereich mit genau zwei Primidealen, nämlich* 0 *und dem maximalen Ideal* $\mathfrak{m}$.

Beweis. Ein diskreter Bewertungsring ist kein Körper. In einem Hauptidealbereich, der kein Körper ist, wird jedes maximale Ideal von einen Primelement erzeugt, und die Primerzeuger zu verschiedenen maximalen Idealen können nicht assoziiert sein. Also gibt es genau ein maximales Ideal. Nach Satz 9.18 ist ein Hauptidealbereich insbesondere ein Dedekindbereich, so dass es als weiteres Primideal nur noch das Nullideal gibt. □

Beispiel 10.12. Es sei K ein Körper, $K[X]$ der Polynomring und $R = K[X]_{(X)}$ die Lokalisierung am maximalen Ideal $\mathfrak{m} = (X)$. Dann ist R ein diskreter Bewertungsring. Die beiden einzigen Primideale von R sind $(0) \subset (X)$, und ein Hauptidealbereich liegt vor, da ja $K[X]$ ein Hauptidealbereich ist. Da es nur ein maximales Ideal gibt, kann es bis auf Assoziiertheit auch nur ein Primelement geben, nämlich X.

Beispiel 10.13. Es sei p eine Primzahl und sei $R = \mathbb{Z}_{(p)}$ die Lokalisierung am maximalen Ideal $\mathfrak{m} = (p)$. Dann ist R ein diskreter Bewertungsring. Die beiden einzigen Primideale von R sind $(0) \subset (p)$, und ein Hauptidealbereich

liegt vor, da ja $\mathbb{Z}$ ein Hauptidealbereich ist. Da es nur ein maximales Ideal gibt, kann es bis auf Assoziiertheit auch nur ein Primelement geben, nämlich p.

Definition 10.14. Zu einem Element $f \in R$, $f \neq 0$, in einem diskreten Bewertungsring mit Primelement p heißt die Zahl $n \in \mathbb{N}$ mit der Eigenschaft $f = up^n$, wobei u eine Einheit bezeichnet, die *Ordnung* von f. Sie wird mit $\operatorname{ord}(f)$ bezeichnet.

Die Ordnung ist also nichts anderes als der Exponent zum (bis auf Assoziiertheit) einzigen Primelement in der Primfaktorzerlegung. Sie hat folgende Eigenschaften.

Lemma 10.15. *Es sei R ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = (p)$. Dann hat die Ordnung*

$$R \setminus \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \operatorname{ord}(f),$$

folgende Eigenschaften.

(1) $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.
(2) $\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$.
(3) *Es ist $f \in \mathfrak{m}$ genau dann, wenn $\operatorname{ord}(f) \geq 1$ ist.*
(4) *Es ist $f \in R^\times$ genau dann, wenn $\operatorname{ord}(f) = 0$ ist.*

Beweis. Siehe Aufgabe 10.7. □

Wir wollen eine wichtige Charakterisierung für diskrete Bewertungsringe beweisen, die insbesondere beinhaltet, dass ein normaler lokaler Integritätsbereich mit genau zwei Primidealen bereits ein diskreter Bewertungsring ist. Dazu benötigen wir einige Vorbereitungen.

Lemma 10.16. *Sei S ein noetherscher lokaler kommutativer Ring. Es sei vorausgesetzt, dass das maximale Ideal $\mathfrak{m}$ das einzige Primideal von S ist. Dann gibt es einen Exponenten $n \in \mathbb{N}$ mit*

$$\mathfrak{m}^n = 0.$$

Beweis. Wir behaupten zunächst, dass jedes Element in R eine Einheit oder nilpotent ist. Sei hierzu $f \in R$ keine Einheit. Dann ist $f \in \mathfrak{m}$. Angenommen, f ist nicht nilpotent. Dann gibt es nach Lemma 3.9 ein Primideal $\mathfrak{p}$ in R mit $f \notin \mathfrak{p}$. Damit ergibt sich der Widerspruch $\mathfrak{p} \neq \mathfrak{m}$.

Es ist also jedes Element im maximalen Ideal nilpotent. Insbesondere gibt es für ein endliches Erzeugendensystem $f_1, \ldots, f_k$ von $\mathfrak{m}$ eine natürliche Zahl m mit $f_i^m = 0$ für alle $i = 1, \ldots, k$. Sei $n = km$. Dann ist ein beliebiges Element aus $\mathfrak{m}^n$ von der Gestalt

$$\left(\sum_{i=1}^k a_{i1} f_i\right)\left(\sum_{i=1}^k a_{i2} f_i\right) \cdots \left(\sum_{i=1}^k a_{in} f_i\right).$$

Ausmultiplizieren ergibt eine Linearkombination mit Monomen $f_1^{r_1} \cdots f_k^{r_k}$ und $\sum_{i=1}^k r_i = n$, so dass ein f_i mit einem Exponenten $\geq n/k = m$ vorkommt. Daher ist das Produkt 0. □

Satz 10.17. *Es sei R ein noetherscher lokaler Integritätsbereich mit der Eigenschaft, dass es genau zwei Primideale $0 \subset \mathfrak{m}$ gibt. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein diskreter Bewertungsring.*
(2) *R ist ein Hauptidealbereich.*
(3) *R ist faktoriell.*
(4) *R ist normal.*
(5) *$\mathfrak{m}$ ist ein Hauptideal.*

Beweis. (1) $\Rightarrow$ (2) folgt direkt aus der Definition 10.10.

(2) $\Rightarrow$ (3) folgt aus Satz 2.19.

(3) $\Rightarrow$ (4) folgt aus Satz 6.12.

(4) $\Rightarrow$ (5). Sei $f \in \mathfrak{m}$, $f \neq 0$. Dann ist $R/(f)$ ein noetherscher lokaler Ring mit nur einem Primideal (nämlich $\tilde{\mathfrak{m}} = \mathfrak{m}R/(f)$). Daher gibt es nach Lemma 10.16 ein $n \in \mathbb{N}$ mit $\tilde{\mathfrak{m}}^n = 0$. Zurückübersetzt nach R heißt das, dass $\mathfrak{m}^n \subseteq (f)$ gilt. Wir wählen n minimal mit den Eigenschaften

$$\mathfrak{m}^n \subseteq (f) \text{ und } \mathfrak{m}^{n-1} \not\subseteq (f)\,.$$

Wähle $g \in \mathfrak{m}^{n-1}$ mit $g \notin (f)$ und betrachte

$$h := \frac{f}{g} \in Q(R)$$

(es ist $g \neq 0$). Das Inverse, also $h^{-1} = \frac{g}{f}$, gehört nicht zu R, sonst wäre $g \in (f)$. Da R nach Voraussetzung normal ist, ist h^{-1} auch nicht ganz über R. Nach dem Modulkriterium Lemma 6.7 für die Ganzheit gilt insbesondere für das maximale Ideal $\mathfrak{m} \subset R$ die Beziehung

$$h^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$$

ist. Nach Wahl von g ist aber auch

$$h^{-1}\mathfrak{m} = \frac{g}{f}\mathfrak{m} \subseteq \frac{\mathfrak{m}^n}{f} \subseteq R.$$

Daher ist $h^{-1}\mathfrak{m}$ ein Ideal in R, das nicht im maximalen Ideal enthalten ist. Also ist $h^{-1}\mathfrak{m} = R$. Das heißt einerseits $h \in \mathfrak{m}$ und andererseits gilt für ein beliebiges $x \in \mathfrak{m}$ die Beziehung $h^{-1}x \in R$, also $x = h(h^{-1}x)$, also $x \in (h)$ und somit $(h) = \mathfrak{m}$.

(5) $\Rightarrow$ (1). Sei $\mathfrak{m} = (\pi)$. Dann ist π ein Primelement und zwar bis auf Assoziiertheit das einzige. Sei $f \in R$, $f \neq 0$ keine Einheit. Dann ist $f \in \mathfrak{m}$ und daher $f = \pi g_1$. Dann ist g_1 eine Einheit oder $g_1 \in \mathfrak{m}$. Im zweiten Fall ist wieder $g_1 = \pi g_2$ und $f = \pi^2 g_2$.

Wir behaupten, dass man $f = \pi^k u$ mit einem $k \in \mathbb{N}$ und einer Einheit u schreiben kann. Andernfalls könnte man $f = \pi^n g_n$ mit beliebig großem n schreiben. Nach Lemma 10.16 gibt es ein $m \in \mathbb{N}$ mit $(\pi^m) = \mathfrak{m}^m \subseteq (f)$. Bei $n \geq m+1$ ergibt sich $\pi^m = af = a\pi^{m+1}b$ und der Widerspruch $1 = ab\pi$.

Es lässt sich also jede Nichteinheit $\neq 0$ als Produkt einer Potenz des Primelements mit einer Einheit schreiben. Insbesondere ist R faktoriell. Für ein beliebiges Ideal $\mathfrak{a} = (f_1, \ldots, f_s)$ ist $f_i = \pi^{n_i} u_i$ mit Einheiten u_i. Dann sieht man leicht, dass $\mathfrak{a} = (\pi^n)$ ist mit $n = \min_i\{n_i\}$. □

Korollar 10.18. *Sei R ein Dedekindbereich und sei $\mathfrak{m}$ ein maximales Ideal in R. Dann ist die Lokalisierung*

$$R_{\mathfrak{m}}$$

ein diskreter Bewertungsring.

Beweis. Die Lokalisierung $R_{\mathfrak{m}}$ ist lokal nach Satz 4.15, so dass es lediglich die beiden Primideale 0 und $\mathfrak{m}R_{\mathfrak{m}}$ gibt. Ferner ist R noethersch. Da R normal ist, ist nach Lemma 6.15 auch die Lokalisierung $R_{\mathfrak{m}}$ normal. Wegen Satz 10.17 ist $R_{\mathfrak{m}}$ ein diskreter Bewertungsring. □

Bemerkung 10.19. Korollar 10.18 besagt in Verbindung mit Satz 10.17, dass wenn man bei einem Dedekindbereich und spezieller einem Zahlbereich R zur Lokalisierung $R_{\mathfrak{m}}$ an einem maximalen Ideal $\mathfrak{m}$ übergeht, dass dort die eindeutige Primfaktorzerlegung gilt.

Korollar 10.20. *Sei R ein Dedekindbereich. Dann ist R der Durchschnitt von diskreten Bewertungsringen.*

Beweis. Nach Satz 4.16 ist

$$R = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}},$$

wobei $\mathfrak{m}$ durch alle maximalen Ideale von R läuft. Nach Korollar 10.18 sind die beteiligten Lokalisierungen $R_{\mathfrak{m}}$ allesamt diskrete Bewertungsringe. □

10. Arbeitsblatt

10.1. **Aufgaben.**

Aufgabe 10.1. Sei R ein Zahlbereich und sei angenommen, dass jede ganze Zahl $n \in \mathbb{Z}$, $n \neq 0$, eine Primfaktorzerlegung in R besitzt. Zeige, dass dann R bereits faktoriell ist.

Aufgabe 10.2. Es sei $D \neq 0, 1$ quadratfrei und A_D der zugehörige quadratische Zahlbereich. Es Sei p eine Primzahl, die in A_D nicht träge sei. Beweise die Äquivalenz folgender Aussagen.

(1) p besitzt eine Primfaktorzerlegung in A_D.
(2) p ist nicht irreduzibel (also zerlegbar) in A_D.
(3) p oder $-p$ ist die Norm eines Elementes aus A_D.
(4) p oder $-p$ ist die Norm eines Primelementes aus A_D.

Aufgabe 10.3. Sei $D < 0$ quadratfrei und A_D der zugehörige imaginärquadratische Zahlbereich. Bestimme für $D \geq -12$ die Nichteinheiten $z \in A_D$ mit minimaler Norm.

Aufgabe 10.4. Betrachte in $\mathbb{Z}[\sqrt{-2}]$ die beiden Elemente

$$x = 4 + 7\sqrt{-2} \text{ und } y = 5 + 8\sqrt{-2}\,.$$

Bestimme den größten gemeinsamen Teiler der Normen $N(x)$ und $N(y)$ (in $\mathbb{Z}$) und das von x und y erzeugte Ideal in $\mathbb{Z}[\sqrt{-2}]$.

Aufgabe 10.5. Man gebe ein Beispiel für einen quadratischen Zahlbereich, wo die -1 als Norm eines Elementes auftritt, und ein Beispiel, wo dies nicht der Fall ist.

Aufgabe 10.6.*

Bestimme die Norm des Ideals (X^2+1) im Zahlbereich $\mathbb{Z}[X]/(X^4+1)$.

Aufgabe 10.7. Bestimme die Norm des Ideals (X^2+7) im Zahlbereich $\mathbb{Z}[X]/(X^3-2)$.

Aufgabe 10.8.*

(1) Zeige, dass in $\mathbb{Z}[X]$ die Ideale (X^4-7, X^3-5) und $(X+55,282)$ übereinstimmen.
(2) Bestimme die Norm des Ideals (X^3-5) im Zahlbereich
$$\mathbb{Z}[X]/\big(X^4-7\big)\,.$$
(3) Bestimme die Norm des Ideals (X^4-7) im Zahlbereich
$$\mathbb{Z}[X]/\big(X^3-5\big)\,.$$

Aufgabe 10.9.*

Es sei R ein Zahlbereich und es sei $\mathfrak{p} \neq 0$ ein Primideal. Zeige, dass die Norm von $\mathfrak{p}$ eine echte Primzahlpotenz ist.

Aufgabe 10.10.*

Bestimme im quadratischen Zahlbereich $\mathbb{Z}[\sqrt{3}]$ endlich viele Elemente f_1, $\ldots$, f_m, deren Norm 13 ist, und die die Eigenschaft erfüllen, dass jedes Element mit der Norm 13 zu einem der f_j assoziiert ist.

Aufgabe 10.11. Beschreibe das Spektrum eines diskreten Bewertungsringes.

Aufgabe 10.12. Sei R ein diskreter Bewertungsring und sei $\mathfrak{m} = (\pi)$. Es sei $K = R/(\pi)$ der Restklassenkörper von R. Zeige, dass es für jedes $n \in \mathbb{N}$ einen R-Modulisomorphismus

$$(\pi^n)/(\pi^{n+1}) \longrightarrow K$$

gibt.

Aufgabe 10.13. Es sei R ein diskreter Bewertungsring, dessen Restekörper $K = R/\mathfrak{m} = \mathbb{F}_q$ endlich mit q Elementen sei. Zeige, dass $R/\mathfrak{m}^n$ ein endlicher Ring mit q^n Elementen ist. Man folgere, dass zu $f \in R$ die Gleichheit

$$\#\left(R/(f)\right) = q^{\operatorname{ord}(f)}$$

gilt, und dass man die Ordnung von f aus der Größe des Restklassenringes berechnen kann.

Aufgabe 10.14. Sei R ein diskreter Bewertungsring mit Quotientenkörper Q. Zeige, dass es keinen echten Zwischenring zwischen R und Q gibt.

Aufgabe 10.15. Sei R ein diskreter Bewertungsring mit Quotientenkörper Q. Charakterisiere die endlich erzeugten R-Untermoduln von Q. Auf welche Form kann man ein Erzeugendensystem bringen?

Aufgabe 10.16. Es sei K ein Körper der Charakteristik 0 und sei $f \in K[X]$, $f \neq 0$, und $a \in K$. Zeige, dass die folgenden „Ordnungen“ von f an der Stelle a übereinstimmen.

(1) Die Verschwindungsordnung von f an der Stelle a, also die maximale Ordnung einer formalen Ableitung mit $f^{(k)}(a) = 0$.
(2) Der Exponent des Linearfaktors $X - a$ in der Zerlegung von f.
(3) Die Ordnung von f an der Lokalisierung $K[X]_{(X-a)}$ von $K[X]$ am maximalen Ideal $(X - a)$.

Aufgabe 10.17. Sei K ein Körper und $K(T)$ der Körper der rationalen Funktionen über K. Finde einen diskreten Bewertungsring $R \subset K(T)$ mit $Q(R) = K(T)$ und mit $R \cap K[T] = K$.

Aufgabe 10.18. Beweise für einen diskreten Bewertungsring die Eigenschaften der Ordnung, die in Lemma 10.15 formuliert sind.

Aufgabe 10.19. Sei p eine fixierte Primzahl. Zu jeder ganzen Zahl $n \neq 0$ bezeichne $\nu_p(n)$ den Exponenten, mit dem die Primzahl p in der Primfaktorzerlegung von n vorkommt.

a) Zeige: die Abbildung $\nu_p : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ ist surjektiv.

b) Zeige: es gilt $\nu_p(nm) = \nu_p(n) + \nu_p(m)$.

c) Finde eine Fortsetzung $\nu_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ der gegebenen Abbildung, die ein Gruppenhomomorphismus ist (wobei $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ mit der Multiplikation und $\mathbb{Z}$ mit der Addition versehen ist).

d) Beschreibe den Kern des unter c) beschriebenen Gruppenhomomorphismus.

Aufgabe 10.20.*

Wir betrachten im quadratischen Zahlbereich $R = A_{-5} = \mathbb{Z}[\sqrt{-5}]$ das Primideal $\mathfrak{p} = (2, 1 + \sqrt{-5})$. Zeige direkt, dass das Ideal $\mathfrak{p}R_\mathfrak{p}$ in der Lokalisierung $R_\mathfrak{p}$ ein Hauptideal ist.

Aufgabe 10.21. Sei $D \neq 1$ quadratfrei und $D = 1 \mod 4$. Finde in $\mathbb{Z}[\sqrt{D}]$ ein Primideal $\mathfrak{p}$ derart, dass die Lokalisierung an $\mathfrak{p}$ kein diskreter Bewertungsring ist.

Aufgabe 10.22.*

Sei K ein Körper und sei

$$\nu\colon\ (K^\times, \cdot, 1) \longrightarrow (\mathbb{Z}, +, 0)$$

ein surjektiver Gruppenhomomorphismus mit $\nu(f+g) \geq \min\{\nu(f), \nu(g)\}$ für alle $f, g \in K^\times$. Zeige, dass

$$R = \left\{ f \in K^\times \mid \nu(f) \geq 0 \right\} \cup \{0\}$$

ein diskreter Bewertungsring ist.

Aufgabe 10.23. Es sei $V = V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2_K$ der Einheitskreis über einem Körper K und es sei $P = (a, b) \in V$ ein Punkt.

(1) Zeige, dass der lokale Ring R von V im Punkt P ein diskreter Bewertungsring ist.
(2) Folgere, dass der Koordinatenring $K[X,Y]/(X^2+Y^2-1)$ normal ist (man kann K algebraisch abgeschlossen annehmen).
(3) Zeige, dass $K[X,Y]/(X^2+Y^2-1)$ nicht faktoriell ist.
(4) Bestimme die Ordnung von X und von $Y-1$ im lokalen Ring zum Punkt $(0,1)$.

Aufgabe 10.24. Sei K ein Körper. Eine *Potenzreihe in einer Variablen* über K ist ein formaler Ausdruck der Form

$$a_0 + a_1T + a_2T^2 + a_3T^3 + \dots \text{ mit } a_i \in K\,.$$

Es kann hier also unendlich viele von 0 verschiedene Koeffizienten a_i geben. Definiere eine Ringstruktur auf der Menge aller Potenzreihen, die die Ringstruktur auf dem Polynomring in einer Variablen fortsetzt. Zeige, dass dieser Ring ein diskreter Bewertungsring ist.

Aufgabe 10.25. Sei R ein Integritätsbereich mit Quotientenkörper $K = Q(R)$. Es sei $R = \bigcap_{i\in I} R_i$, wobei die $R_i \subset K$, $i \in I$, alle diskrete Bewertungsringe seien. Zeige: R ist normal.

Ein Modul, der außer 0 keine Torsionselemente enthält, heißt *torsionsfrei*.

Aufgabe 10.26. Zeige, dass ein torsionsfreier endlich erzeugter Modul M über einem diskreten Bewertungsring frei ist.

11. Vorlesung - Hauptdivisoren

11.1. **Die Ordnung an einem Primideal.**

Zu einem Dedekindbereich R und einem Primideal $\mathfrak{p} \neq 0$ ist nach Korollar 10.18 die Lokalisierung $R_{\mathfrak{p}}$ ein diskreter Bewertungsring und somit ergibt sich insgesamt eine Abbildung

$$R \setminus \{0\} \longrightarrow R_{\mathfrak{p}} \setminus \{0\} \xrightarrow{\text{ord}} \mathbb{N}\,.$$

Definition 11.1. Sei R ein Dedekindbereich, $\mathfrak{p} \neq 0$ ein Primideal in R und $f \in R$, $f \neq 0$. Dann heißt die Ordnung $\text{ord}\,(f)$ im diskreten Bewertungsring $R_{\mathfrak{p}}$ die *Ordnung* von f am Primideal $\mathfrak{p}$ (oder an der Primstelle $\mathfrak{p}$ oder in $R_{\mathfrak{p}}$). Sie wird mit $\text{ord}_{\mathfrak{p}}\,(f)$ bezeichnet.

Lemma 11.2. *Es sei R ein Dedekindbereich und $\mathfrak{p} \neq 0$ ein Primideal in R. Dann hat die Ordnung an $\mathfrak{p}$, also die Abbildung*

$$R \setminus \{0\} \longrightarrow \mathbb{N},\ f \longmapsto \text{ord}_{\mathfrak{p}}\,(f),$$

folgende Eigenschaften.

(1) $\mathrm{ord}_{\mathfrak{p}}(fg) = \mathrm{ord}_{\mathfrak{p}}(f) + \mathrm{ord}_{\mathfrak{p}}(g)$.
(2) $\mathrm{ord}_{\mathfrak{p}}(f+g) \geq \min(\mathrm{ord}_{\mathfrak{p}}(f), \mathrm{ord}_{\mathfrak{p}}(g))$.
(3) *Es ist* $f \in \mathfrak{p}$ *genau dann, wenn* $\mathrm{ord}_{\mathfrak{p}}(f) \geq 1$.

Beweis. (1) und (2) folgen direkt aus Lemma 10.15. Bei (3) ist zu beachten, dass für $f \in R$ gilt, dass $f \in \mathfrak{p}$ genau dann gilt, wenn $f \in \mathfrak{p}R_{\mathfrak{p}}$ ist. Letzteres bedeutet nämlich, dass $f = q_1 f_1 + \cdots + q_n f_n$ mit $f_i \in \mathfrak{p}$ und $q_i \in R_{\mathfrak{p}}$ ist, also $q_i = \frac{r_i}{s_i}$ mit $s_i \notin \mathfrak{p}$. Mit dem Hauptnenner $s = s_1 \cdots s_n$ ist dann $sf = a_1 f_1 + \cdots + a_n f_n \in \mathfrak{p}$, woraus $f \in \mathfrak{p}$ folgt. Damit folgt die Behauptung aus Lemma 10.15. □

Definition 11.3. Es sei R ein Dedekindbereich und $f \in R$, $f \neq 0$. Dann heißt die Abbildung, die jedem Primideal $\mathfrak{p} \neq 0$ in R die Ordnung $\mathrm{ord}_{\mathfrak{p}}(f)$ zuordnet, der durch f definierte *Hauptdivisor*. Er wird mit $\mathrm{div}(f)$ bezeichnet und als formale Summe

$$\mathrm{div}(f) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(f) \cdot \mathfrak{p}$$

geschrieben.

Die Ordnung an einem Primideal nennt man in diesem Zusammenhang auch die Verschwindungsordnung. Die Ordnung ist ja genau dann positiv, wenn f zum Primideal $\mathfrak{p}$ gehört, und dies ist genau dann der Fall, wenn unter der Abbildung

$$R \longrightarrow R/\mathfrak{p} \longrightarrow Q(R/\mathfrak{p})$$

das Element f auf 0 abgebildet wird, also an dieser Stelle verschwindet. Eine höhere Verschwindungsordnung bedeutet, dass f nicht nur einfach, sondern mit einer gewissen Vielfachheit verschwindet. Der Hauptdivisor zu f notiert also, mit welcher Verschwindungsordnung die Funktion f an den verschiedenen Primstellen verschwindet.

Bemerkung 11.4. Es sei R ein faktorieller Dedekindbereich. Dann lässt sich der Hauptdivisor zu einem Ringelement $f \in R$, $f \neq 0$, unmittelbar aus der Primfaktorzerlegung ablesen. Wenn

$$f = u p_1^{r_1} \cdots p_k^{r_k}$$

mit einer Einheit u und paarweise nicht assoziierten Primelementen p_i ist, so ist der Hauptdivisor zu f gleich

$$\mathrm{div}(f) = \sum_{i=1}^{k} r_i(p_i).$$

Dies beruht einfach darauf, dass die Ordnung von f in der Lokalisierung $R_{(p_i)}$ gleich r_i ist.

Lemma 11.5. *Es sei R ein Dedekindbereich. Dann hat die Abbildung, die einem Ringelement $\neq 0$ den Hauptdivisor zuordnet, also*

$$R \setminus \{0\} \longrightarrow \text{Hauptdivisoren}, \ f \longmapsto \mathrm{div}(f),$$

folgende Eigenschaften.

(1)
$$\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g).$$

(2)
$$\operatorname{div}(f+g) \geq \min(\operatorname{div}(f), \operatorname{div}(g)).$$

(3) *Es ist f genau dann eine Einheit, wenn* $\operatorname{div}(f) = 0$ *ist.*

Beweis. Dies folgt direkt aus Lemma 11.2 durch Betrachtung an den einzelnen Primidealen. □

Lemma 11.6. *Es sei R ein Dedekindbereich und $f \in R$, $f \neq 0$. Dann ist nur für endlich viele Primideale $\mathfrak{p} \neq 0$ in R die Ordnung* $\operatorname{ord}_{\mathfrak{p}}(f)$ *von 0 verschieden. Das heißt, dass der Hauptdivisor* $\operatorname{div}(f) = \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(f) \cdot \mathfrak{p}$ *eine endliche Summe ist.*

Beweis. Es ist $R/(f)$ nulldimensional, deshalb folgt die Aussage aus Aufgabe 11.1. □

Im zahlentheoretischen Kontext folgt die letzte Aussage auch direkt aus der Endlichkeit der Restklassenringe.

Beispiel 11.7. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$, also $R = A_{-5} = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2+5)$, das Ideal
$$\mathfrak{p} = (2, 1+\sqrt{-5}).$$
Nach Beispiel 10.7 ist dies kein Hauptideal. Wir wollen die Hauptdivisoren zu den beiden Idealerzeugern 2 und $1+\sqrt{-5}$ berechnen. Der erste Schritt ist dabei, die Primideale oberhalb des Elementes zu bestimmen, was am einfachsten durch eine Restklassenbetrachtung geschieht. Der Restklassenring modulo 2 ist
$$\begin{aligned} R/(2) &= \mathbb{Z}[X]/(X^2+5, 2) \\ &= \mathbb{Z}/(2)[X]/(X^2+5) \\ &= \mathbb{Z}/(2)[X]/(X^2+1) \\ &= \mathbb{Z}/(2)[X]/(X+1)^2. \end{aligned}$$
Dies ist ein nichtreduzierter Ring mit nur einem maximalen Ideal. In der Lokalisierung $R_{(2,1+\sqrt{-5})}$ gilt
$$2 = \frac{1}{\left(-2+\sqrt{5}\right)}\left(1+\sqrt{-5}\right)^2,$$
was zeigt, dass $1+\sqrt{-5}$ dort ein Erzeuger des maximalen Ideals ist und dass die Ordnung von 2 dort gleich 2 ist. Deshalb gilt
$$\operatorname{div}(2) = 2\mathfrak{p}.$$
Wegen
$$R/(1+\sqrt{-5}) = \mathbb{Z}[X]/(X^2+5, 1+X) = \mathbb{Z}/(6) = \mathbb{Z}/(2) \times \mathbb{Z}/(3)$$

ist $1+\sqrt{-5}$ auch noch im Primideal $\mathfrak{q} = (3, 1+\sqrt{-5})$ enthalten und besitzt dort ebenfalls die Ordnung 1. Daher ist

$$\operatorname{div}\left(1+\sqrt{-5}\right) = \mathfrak{p}+\mathfrak{q}.$$

11.2. **Effektive Divisoren.**

Definition 11.8. Es sei R ein Dedekindbereich. Ein *effektiver Divisor* ist eine formale Summe

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}\,,$$

die sich über alle Primideale $\mathfrak{p} \neq 0$ aus R erstreckt und wobei $n_{\mathfrak{p}}$ natürliche Zahlen sind mit $n_{\mathfrak{p}} = 0$ für fast alle $\mathfrak{p}$.

Lemma 11.6 zeigt, dass ein Hauptdivisor zu einem Ringelement $\neq 0$ wirklich ein effektiver Divisor ist. Ein effektiver Divisor gibt für jede Primstelle eine „Verschwindungsordnung“ an. Eine naheliegende Frage ist dann, ob dieses Ordnungsverhalten durch eine Funktion realisiert werden kann, also ob der Divisor ein Hauptdivisor ist. Wir werden im Weiteren sehen, dass die Frage, welche Divisoren Hauptdivisoren sind, eng mit der Frage nach der Faktorialität von Dedekindbereichen zusammenhängt. Der Zugang über Divisoren hat den Vorteil, dass er erlaubt (siehe weiter unten), eine Gruppe, die sogenannte *Divisorenklassengruppe* einzuführen, die die Abweichung von der Faktorialität messen kann. Die Menge der effektiven Divisoren wird mit $\operatorname{Eff}\operatorname{Div}(R)$ bezeichnet, es handelt sich um ein kommutatives additives Monoid, das als Monoid von den *Primdivisoren* $\mathfrak{p}$ erzeugt wird.

Definition 11.9. Es sei R ein Dedekindbereich und $\mathfrak{a} \neq 0$ ein von 0 verschiedenes Ideal in R. Dann nennt man den Divisor

$$\operatorname{div}(\mathfrak{a}) = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \cdot \mathfrak{p}$$

mit

$$m_{\mathfrak{p}} = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) := \min\left(\operatorname{ord}_{\mathfrak{p}}(f) | f \in \mathfrak{a},\ f \neq 0\right)$$

den *Divisor zum Ideal* $\mathfrak{a}$.

Bemerkung 11.10. Man kann den Divisor zu einem Ideal auch durch

$$\operatorname{div}(\mathfrak{a}) = \min\left\{\operatorname{div}(f) \mid f \in \mathfrak{a},\ f \neq 0\right\}$$

definieren, wobei das Minimum über Divisoren komponentenweise erklärt ist. Es gibt im Allgemeinen kein Element, das an allen Primstellen simultan das Minimum annimmt. Da zu einem einzelnen Element $0 \neq f \in \mathfrak{a}$ der zugehörige Hauptdivisor nur an endlich vielen Stellen von 0 verschieden ist, gilt das erst recht für den Divisor zu einem Ideal.

Die Ordnung $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$ kann man auch als Ordnung des Ideals $\operatorname{ord}(\mathfrak{a}R_{\mathfrak{p}})$ im diskreten Bewertungsring $R_{\mathfrak{p}}$ ansehen. Dabei ist $\mathfrak{a}R_{\mathfrak{p}}$ das Erweiterungsideal zu $\mathfrak{a}$ in $R_{\mathfrak{p}}$. Dieses Ideal hat einen Erzeuger p^k, wobei p ein Primelement im diskreten Bewertungsring ist; die Ordnung ist dann k.

Lemma 11.11. *Es sei R ein Dedekindbereich. Dann erfüllt die Zuordnung (für von 0 verschiedene Ideale)*

$$\mathfrak{a} \longmapsto \operatorname{div}(\mathfrak{a})$$

folgende Eigenschaften.

(1)
$$\operatorname{div}(\mathfrak{p}) = 1 \cdot \mathfrak{p}$$
für ein Primideal $\mathfrak{p} \neq 0$.

(2)
$$\operatorname{div}(\mathfrak{a} \cdot \mathfrak{b}) = \operatorname{div}(\mathfrak{a}) + \operatorname{div}(\mathfrak{b}).$$

(3) *Für* $\mathfrak{a} \subseteq \mathfrak{b}$ *ist* $\operatorname{div}(\mathfrak{a}) \geq \operatorname{div}\operatorname{div}(\mathfrak{b})$.

(4)
$$\operatorname{div}(\mathfrak{a} + \mathfrak{b}) = \min\{\operatorname{div}(\mathfrak{a}), \operatorname{div}(\mathfrak{b})\}.$$

Beweis. (1) Für jedes Element $f \in \mathfrak{p}$ gilt auch $f \in \mathfrak{p}R_{\mathfrak{p}}$ und daher ist $\operatorname{ord}_{\mathfrak{p}}(f) \geq 1$. Umgekehrt besitzt der diskrete Bewertungsring $R_{\mathfrak{p}}$ ein Element p, das das maximale Ideal $\mathfrak{p}R_{\mathfrak{p}}$ erzeugt und die Ordnung 1 hat. Man kann $p = \frac{a}{b}$ mit $a, b \in R$ und $b \notin \mathfrak{p}$ schreiben. Dabei ist $a \in \mathfrak{p}$ und a hat in $R_{\mathfrak{p}}$ die Ordnung 1.

Sei nun $\mathfrak{q} \neq \mathfrak{p}$ ein weiteres Primideal $\neq 0$. Da beide Ideale maximal sind gibt es ein Element $g \in \mathfrak{p}$, $g \notin \mathfrak{q}$. Dieses hat dann in $\mathfrak{q}$ die Ordnung 0.

(2) Fixiere ein Primideal $\mathfrak{p}$. Sei $h \in \mathfrak{a} \cdot \mathfrak{b}$ und schreibe $h = \sum_{i=1}^{k} f_i g_i$ mit $f_i \in \mathfrak{a}$ und $g_i \in \mathfrak{b}$. Dann ist nach Lemma 11.5

$$\begin{aligned} \operatorname{div}(h) &\geq \min\{\operatorname{div}(f_i g_i) : i = 1, \ldots, k\} \\ &\geq \min\{\operatorname{div}(f_i) + \operatorname{div}(g_i) : i = 1, \ldots, k\} \\ &\geq \operatorname{div}(\mathfrak{a}) + \operatorname{div}(\mathfrak{b}). \end{aligned}$$

Für die Umkehrung schreiben wir $\operatorname{div}(\mathfrak{a}) = \sum_{\mathfrak{q}} n_{\mathfrak{q}} \cdot \mathfrak{q}$ und $\operatorname{div}(\mathfrak{b}) = \sum_{\mathfrak{q}} m_{\mathfrak{q}} \cdot \mathfrak{q}$. Zu fixiertem $\mathfrak{p}$ gibt es ein $f \in \mathfrak{a}$ und ein $g \in \mathfrak{b}$ mit $\operatorname{ord}_{\mathfrak{p}}(f) = n_{\mathfrak{p}}$ und $\operatorname{ord}_{\mathfrak{p}}(g) = m_{\mathfrak{p}}$. Dann ist $fg \in \mathfrak{a}\mathfrak{b}$ und

$$\operatorname{ord}_{\mathfrak{p}}(fg) = \operatorname{ord}_{\mathfrak{p}}(f) + \operatorname{ord}_{\mathfrak{p}}(g) = n_{\mathfrak{p}} + m_{\mathfrak{p}}.$$

(3) Das ist trivial.

(4) Die Abschätzung „$\geq$“ folgt aus $\operatorname{div}(f + g) \geq \min(\operatorname{div}(f), \operatorname{div}(g))$. Die Abschätzung „$\leq$“ folgt aus Teil (3).

□

Definition 11.12. Es sei R ein Dedekindbereich und

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}$$

ein effektiver Divisor (wobei $\mathfrak{p}$ durch die Menge der Primideale $\neq 0$ läuft). Dann nennt man

$$\{f \in R \mid \operatorname{div}(f) \geq D\}$$

das *Ideal zum Divisor* D. Es wird mit $\mathrm{Id}(D)$ bezeichnet.

In der vorstehenden Definition verwenden wir die Konvention, dass in Ungleichungen der Ausdruck $\operatorname{div}(0)$ als ∞ zu verstehen ist. Damit gehört also 0 zu $\mathrm{Id}(D)$. Es ergibt sich sofort, dass es sich in der Tat um ein Ideal handelt. Es ist auch nicht das Nullideal, da wir zu den endlich vielen Primidealen $\mathfrak{p}_i$, $i = 1, \ldots, k$, mit $n_i = n_{\mathfrak{p}_i} > 0$ Elemente $0 \neq f_i \in \mathfrak{p}_i$ mit $\operatorname{ord}_{\mathfrak{p}_i}(f_i) = 1$ wählen können. Dann gehört aber das Produkt $f_1^{n_1} \cdots f_k^{n_k}$ zu dem zu D gehörenden Ideal.

Der folgende Satz zeigt, dass die beiden soeben eingeführten Zuordnungen zwischen den effektiven Divisoren und den von 0 verschiedenen Idealen in einem Dedekindbereich invers zueinander sind. Dies sollte man als eine einfache und übersichtliche Beschreibung für die Menge aller Ideale ansehen.

Satz 11.13. *Es sei R ein Dedekindbereich. Dann sind die Zuordnungen*

$$\mathfrak{a} \longmapsto \operatorname{div}(\mathfrak{a}) \text{ und } D \longmapsto \mathrm{Id}(D)$$

zueinander inverse Abbildungen zwischen der Menge der von 0 verschiedenen Ideale und der Menge der effektiven Divisoren. Diese Bijektion übersetzt das Produkt von Idealen in die Summe von Divisoren.

Beweis. Wir starten mit einem Ideal $\mathfrak{a} \neq 0$ und vergleichen $\mathfrak{a}$ und $\mathrm{Id}(\operatorname{div}(\mathfrak{a}))$. Sei zunächst $f \in \mathfrak{a}$. Es ist dann $\operatorname{ord}_{\mathfrak{p}}(f) \geq \min\{\operatorname{ord}_{\mathfrak{p}}(g) \mid g \in \mathfrak{a}\}$ für jedes Primideal $\mathfrak{p} \neq 0$, so dass natürlich $\operatorname{div}(f) \geq \operatorname{div}(\mathfrak{a})$ gilt. Also ist $f \in \mathrm{Id}(\operatorname{div}(\mathfrak{a}))$. Ist hingegen $f \notin \mathfrak{a}$, so gibt es nach Aufgabe 4.19 auch ein Primideal $\mathfrak{p} \neq 0$ mit $f \notin \mathfrak{a}R_{\mathfrak{p}}$. Da $R_{\mathfrak{p}}$ ein diskreter Bewertungsring ist, gilt $\operatorname{ord}_{\mathfrak{p}}(f) < \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$. Also ist $\operatorname{div}(f) \not\geq \operatorname{div}(\mathfrak{a})$ und somit $f \notin \mathrm{Id}(\operatorname{div}(\mathfrak{a}))$. Insbesondere ist die Abbildung injektiv. Die Surjektivität ergibt sich aus Lemma 11.11 (1) in Verbindung mit Lemma 11.11 (2), was auch den Zusatz ergibt. □

11. Arbeitsblatt

11.1. **Aufgaben.**

Aufgabe 11.1. Es sei R ein Zahlbereich. Zeige, dass der Ringhomomorphismus

$$R \longrightarrow \prod_{p \text{ Primzahl}} R/pR,\ f \longmapsto (f \bmod Rp)_{p \text{ Primzahl}},$$

wobei rechts das Produkt der Faserringe über alle Primzahlen steht, und komponentenweise die Restklassenbildung durchgeführt wird, injektiv ist.

Aufgabe 11.2. Bestimme den Hauptdivisor zu 840 in $\mathbb{Z}$.

Aufgabe 11.3. Bestimme den Hauptdivisor zu 840 in $\mathbb{Z}[\mathrm{i}]$.

Aufgabe 11.4. Bestimme den Hauptdivisor zur Gaußschen Zahl $5 + 7\mathrm{i}$.

Aufgabe 11.5. Es sei R ein Dedekindbereich und sei $f \in R$ als ein Produkt

$$f = up_1^{\nu_1} \cdots p_r^{\nu_r}$$

mit Primelementen p_i und einer Einheit u gegeben. Zeige, dass dann für den zugehörigen Hauptdivisor die Gleichheit

$$\operatorname{div}(f) = \nu_1(p_1) + \cdots + \nu_r(p_r)$$

gilt, wobei die (p_i) die von p_i erzeugten Primideale bezeichnen.

Aufgabe 11.6. Es sei R ein Dedekindbereich und $S \subseteq R$ ein multiplikatives System mit $0 \notin S$. Zeige, dass ein kommutatives Diagramm

$$\begin{array}{ccc} R \setminus \{0\} & \longrightarrow & \operatorname{EffDiv}(R) \\ \downarrow & & \downarrow \\ R_S \setminus \{0\} & \longrightarrow & \operatorname{EffDiv}(R_S) \end{array}$$

vorliegt, wobei die vertikale Abbildung rechts einfach diejenigen Komponenten $\mathfrak{p}$ eines effektiven Divisors D vergisst, die nicht zu $\operatorname{Spek}(R_S)$ gehören.

Aufgabe 11.7. Sei R ein Zahlbereich und $f, g \in R$, $f, g \neq 0$. Zeige ohne Verwendung des Bijektionssatzes, dass die Hauptdivisoren $\operatorname{div}(f)$ und $\operatorname{div}(g)$ genau dann gleich sind, wenn f und g assoziiert sind.

Aufgabe 11.8. Es sei R ein Zahlbereich und seien $f, g \in R$ von 0 verschiedene Elemente. Zeige, dass f genau dann ein Teiler von g ist, wenn für die Hauptdivisoren die Beziehung

$$\operatorname{div}(f) \leq \operatorname{div}(g)$$

gilt.

Aufgabe 11.9. Es sei R ein Zahlbereich und sei $f \in R$, $f \neq 0$. Zeige die beiden folgenden Äquivalenzen:

Das Element f ist genau dann prim, wenn der zugehörige Hauptdivisor $\operatorname{div}(f)$ die Gestalt $1\mathfrak{p}$ mit einem Primideal $\mathfrak{p} \neq 0$ besitzt.

Das Element f ist genau dann irreduzibel, wenn $\operatorname{div}(f)$ minimal unter allen effektiven Hauptdivisoren $\neq 0$ ist.

Aufgabe 11.10. Es sei $R = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5}$ der quadratische Zahlbereich zu $D = -5$. Betrachte in R die Zerlegung

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

Zeige, dass die beteiligten Elemente irreduzibel, aber nicht prim sind, und bestimme für jedes dieser vier Elemente die Primoberideale. Bestimme die Hauptdivisoren zu diesen Elementen.

Aufgabe 11.11. Es sei R ein noetherscher kommutativer Ring. Zeige, dass folgende Aussagen äquivalent sind.

(1) R hat Krulldimension 0.
(2) R ist ein artinscher Ring.
(3) R besitzt endlich viele Primideale, die alle maximal sind.
(4) Es gibt eine natürliche Zahl n mit $\mathfrak{m}^n = 0$ für jedes maximale Ideal $\mathfrak{m}$.
(5) Die Reduktion von R ist ein Produkt von Körpern.

Aufgabe 11.12. Beschreibe die nilpotenten Elemente von $\mathbb{Z}/(n)$ und die Reduktion von $\mathbb{Z}/(n)$.

Aufgabe 11.13. Sei $n \geq 2$ eine natürliche Zahl. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) n ist die Potenz einer Primzahl.
(2) Der Restklassenring $\mathbb{Z}/(n)$ ist zusammenhängend.
(3) Der Restklassenring $\mathbb{Z}/(n)$ ist lokal.
(4) Die Reduktion von $\mathbb{Z}/(n)$ ist ein Körper.
(5) Jeder Nullteiler von $\mathbb{Z}/(n)$ ist nilpotent.
(6) Der Restklassenring $\mathbb{Z}/(n)$ besitzt genau ein Primideal.
(7) Der Restklassenring $\mathbb{Z}/(n)$ besitzt genau ein maximales Ideal.

Aufgabe 11.14. Es sei R ein Dedekindbereich und $f \in R$, $f \neq 0$. Zeige, dass der Hauptdivisor $\operatorname{div}(f)$ mit dem Divisor zum Hauptideal (f) übereinstimmt.

Aufgabe 11.15. Es sei R ein Zahlbereich und $\mathfrak{a} \subseteq R$ ein von 0 verschiedenes Ideal mit einem Erzeugendensystem $\mathfrak{a} = (f_1, \ldots, f_n)$. Zeige

$$\operatorname{div}(\mathfrak{a}) = \min\{\operatorname{div}(f_i) \mid i = 1, \ldots, n\}.$$

Aufgabe 11.16. Zeige, dass unter der Korrespondenz (siehe Satz 11.13) zwischen Idealen $\neq 0$ und Divisoren in einem Dedekindbereich die Summe von Idealen dem Minimum von Divisoren entspricht.

12. Vorlesung - Der Satz von Dedekind

12.1. **Der Satz von Dedekind.**

Korollar 12.1. *Es sei R ein Dedekindbereich und seien $\mathfrak{a}$ und $\mathfrak{b}$ Ideale in R. Dann gilt $\mathfrak{a} \subseteq \mathfrak{b}$ genau dann, wenn es ein Ideal $\mathfrak{c}$ mit $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ gibt. Bei $\mathfrak{b} \neq 0$ ist $\mathfrak{c}$ eindeutig bestimmt.*

Beweis. Die Implikation „$\Leftarrow$“ gilt in beliebigen kommutativen Ringen. Die andere Implikation ist richtig, wenn $\mathfrak{a} = 0$ ist. Wir können also annehmen, dass die beteiligten Ideale von 0 verschieden sind. Die Bedingung impliziert nach Lemma 11.11 (3), dass $\operatorname{div}(\mathfrak{a}) \geq \operatorname{div}(\mathfrak{b})$ ist. Somit ist

$$\operatorname{div}(\mathfrak{a}) = \operatorname{div}(\mathfrak{b}) + E$$

mit einem effektiven Divisor E. Nach Satz 11.13 übersetzt sich dies zurück zu $\mathfrak{a} = \mathfrak{b} \cdot \operatorname{Id}(E)$, so dass mit $\mathfrak{c} = \operatorname{Id}(E)$ die rechte Seite erfüllt ist. □

DDR-Briefmarke

Die folgende Aussage heißt *Satz von Dedekind*. Sie liefert für jeden Zahlbereich auf der Idealebene einen Ersatz für die eindeutige Primfaktorzerlegung.

Satz 12.2. *Es sei R ein Dedekindbereich und $\mathfrak{a} \neq 0$ ein Ideal in R. Dann gibt es eine Produktdarstellung*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$$

mit (bis auf die Reihenfolge) eindeutig bestimmten Primidealen $\mathfrak{p}_i \neq 0$ aus R und eindeutig bestimmten Exponenten r_i, $i = 1, \ldots, k$.

Beweis. Wir benutzen Satz 11.13, also die bijektive Beziehung zwischen Idealen $\neq 0$ und effektiven Divisoren. Auf der Seite der Divisoren haben wir offenbar eine eindeutige Darstellung

$$\operatorname{div}(\mathfrak{a}) = \sum_{i=1}^{k} r_i \mathfrak{p}_i$$

mit geeigneten Primidealen $\mathfrak{p}_i$. Wendet man auf diese Darstellung die Abbildung $D \mapsto \operatorname{Id}(D)$ an, so erhält man links das Ideal zurück. Es genügt also zu

zeigen, dass der Divisor rechts auf das Ideal $\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ abgebildet wird. Dies folgt aber direkt aus Satz 11.13. □

Korollar 12.3. *Es sei R ein Dedekindbereich und $f \in R$, $f \neq 0$. Dann gibt es eine Produktdarstellung für das Hauptideal*

$$(f) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$$

mit (bis auf die Reihenfolge) eindeutig bestimmten Primidealen $\mathfrak{p}_i \neq 0$ aus R und eindeutig bestimmten Exponenten r_i, $i = 1, \ldots, k$.

Beweis. Dies folgt direkt aus Satz 12.2. □

12.2. **Chinesischer Restsatz für Dedekindbereiche.**

Wir kommen zum chinesischen Restsatz für Dedekindbereiche, der den klassischen chinesischen Restsatz für ganze Zahlen wesentlich verallgemeinert. Dazu erinnern wir kurz an Produktringe und idempotente Elemente.

Definition 12.4. Es seien $R_1, \ldots, R_n$ kommutative Ringe. Dann heißt das Produkt

$$R_1 \times \cdots \times R_n \,,$$

versehen mit komponentenweiser Addition und Multiplikation, der *Produktring* der R_i, $i = 1, \ldots, n$.

Definition 12.5. Ein Element e eines kommutativen Ringes heißt *idempotent*, wenn $e^2 = e$ gilt.

Die Elemente 0 und 1 sind trivialerweise idempotent, man nennt sie die trivialen idempotenten Elemente. In einem Produktring sind auch diejenigen Elemente, die in allen Komponenten nur den Wert 0 oder 1 besitzen, idempotent, also beispielsweise $(1, 0)$.

Lemma 12.6. *Es sei R ein kommutativer Ring und seien $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale mit $\mathfrak{a} + \mathfrak{b} = R$. Dann ist*

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

Beweis. Die Inklusion $\supseteq$ gilt immer. Sei also $x \in \mathfrak{a} \cap \mathfrak{b}$ und seien $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ Elemente mit $a + b = 1$. Dann ist

$$x = x \cdot 1 = x(a + b) = xa + xb \in \mathfrak{b}\mathfrak{a} + \mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

□

Lemma 12.7. *Es sei R ein kommutativer Ring und seien $\mathfrak{a}_j$, $j = 1, \ldots, n$, Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$. Dann ist*

$$R/\mathfrak{a}_1 \cdots \mathfrak{a}_n \cong R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n.$$

Beweis. Der allgemeine Fall folgt aus dem Fall für $n = 2$, so dass wir uns darauf beschränken. Die natürliche Abbildung

$$R \longrightarrow R/\mathfrak{a} \times R/\mathfrak{b}$$

hat den Durchschnitt $\mathfrak{a} \cap \mathfrak{b}$ als Kern. Dieser stimmt nach Lemma 12.6 mit dem Produkt $\mathfrak{a} \cdot \mathfrak{b}$ überein und wir erhalten einen injektiven Ringhomomorphismus

$$R/\mathfrak{a} \cdot \mathfrak{b} \longrightarrow R/\mathfrak{a} \times R/\mathfrak{b}.$$

Es ist also noch die Surjektivität nachzuweisen. Sei dazu (r, s) rechts gegeben. Es seien $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ mit $a + b = 1$. Dann ist $r - ar + s - sb$ ein Urbild. Dieses Element wird ja in der ersten Komponente auf

$$r - ar + s - sb = r + s - s(1 - a) = r + s - s = r$$

abgebildet und entsprechend in der zweiten Kompoente auf s. □

Satz 12.8. *Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ in einem Dedekindbereich mit der eindeutigen Primidealzerlegung*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Dann gibt es einen natürlichen Ringisomorphismus

$$R/\mathfrak{a} \cong R/\mathfrak{p}_1^{r_1} \times \cdots \times R/\mathfrak{p}_k^{r_k}.$$

Beweis. Da Dedekindbereiche eindimensional sind und die Primideale in der Zerlegung verschieden sind, gilt $\mathfrak{p}_i + \mathfrak{p}_j = R$ für $i \neq j$. Dies überträgt sich direkt auf die Potenzen. Somit folgt die Aussage aus Lemma 12.7. □

Beispiel 12.9. Wir betrachten

$$\mathbb{Z} \subseteq R = \mathbb{Z}[X]/(X^2 + 3) \subseteq \mathbb{Z}[Y]/(Y^2 + Y + 1) = S$$

mit $X \mapsto 2Y + 1$, die beide quadratische Erweiterungen von $\mathbb{Z}$ sind und wobei S der Ring der Eisenstein-Zahlen ist und die Normalisierung von R ist. Der Faserring zu R über 2 ist

$$\mathbb{Z}/(2)[X]/(X^2 + 3) = \mathbb{Z}/(2)[X]/(X^2 + 1) = \mathbb{Z}/(2)[X]/(X + 1)^2,$$

er ist also nicht reduziert. Der Fasering zu S über 2 ist

$$\mathbb{Z}/(2)[Y]/(Y^2 + Y + 1)$$

und dies ist ein Körper mit vier Elementen. In S liegt die Zerlegung in Primideale $(2) = (2)$ vor. In R kann man hingegen das Ideal (2) nicht als ein Produkt von Primidealen schreiben. Das einzige Primideal oberhalb von (2) in R ist $(2, X + 1)$. Das Quadrat davon ist aber bereits

$$\begin{aligned} (2, X + 1) \cdot (2, X + 1) &= (4, 2X + 2, X^2 + 2X + 1) \\ &= (4, 2X + 2, X^2 - 1) \\ &= (4, 2X + 2) \\ &\subset (2), \end{aligned}$$

wobei die letzte Inklusion echt ist. Der Restklassenring $R/(4, 2X + 2)$ besitzt 12 Elemente.

Korollar 12.10. *Es sei R ein Zahlbereich und p eine Primzahl. In R gelte die Idealzerlegung*

$$(p) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Dann gilt für den Faserring über p die Produktzerlegung

$$R/pR = R/\mathfrak{p}_1^{r_1} \times \cdots \times R/\mathfrak{p}_k^{r_k}.$$

Beweis. Dies folgt direkt aus Satz 12.8. □

Wir formulieren explizit die beiden folgenden Spezialfälle des chinesischen Restsatzes.

Korollar 12.11. *Es sei R ein Hauptidealbereich und $f \in R$, $f \neq 0$, ein Element mit kanonischer Primfaktorzerlegung*

$$f = p_1^{r_1} \cdots p_k^{r_k}.$$

Dann gilt für den Restklassenring $R/(f)$ die kanonische Isomorphie

$$R/(f) \cong R/(p_1^{r_1}) \times \cdots \times R/(p_k^{r_k}).$$

Korollar 12.12. *Es sei n eine positive natürliche Zahl mit kanonischer Primfaktorzerlegung*

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$$

(die p_i seien also verschieden und $r_i \geq 1$). Dann induzieren die kanonischen Ringhomomorphismen $\mathbb{Z}/(n) \to \mathbb{Z}/(p_i^{r_i})$ einen Ringisomorphismus

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{r_1}) \times \mathbb{Z}/(p_2^{r_2}) \times \cdots \times \mathbb{Z}/(p_k^{r_k}).$$

Zu gegebenen ganzen Zahlen $(a_1, a_2, \ldots, a_k)$ gibt es also genau eine natürliche Zahl $a < n$, die die simultanen Kongruenzen

$$a = a_1 \mod p_1^{r_1},\ a = a_2 \mod p_2^{r_2},\ \ldots,\ a = a_k \mod p_k^{r_k}$$

löst.

12.3. **Die Multipliktivität der Norm.**

Satz 12.13. *Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ in einem Zahlbereich R mit der eindeutigen Primidealzerlegung*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Dann ist

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{r_1} \cdots N(\mathfrak{p}_k)^{r_k}.$$

Beweis. Nach dem chinesischen Restsatz für Zahlbereiche ist

$$R/\mathfrak{a} = R/\mathfrak{p}_1^{r_1} \times \cdots \times R/\mathfrak{p}_k^{r_k}$$

und somit ist

$$N(\mathfrak{a}) = N(\mathfrak{p}_1^{r_1}) \cdots N(\mathfrak{p}_k^{r_k}).$$

Es ist also nur noch die Aussage für eine Primidealpotenz $\mathfrak{p}^r$ zu zeigen. Dies geschieht durch Induktion über r, wobei der Induktionsanfang klar ist. Es liegt wegen $\mathfrak{p}^{r+1} \subseteq \mathfrak{p}^r$ eine kurze exakte Sequenz

$$0 \longrightarrow \mathfrak{p}^r/\mathfrak{p}^{r+1} \longrightarrow R/\mathfrak{p}^{r+1} \longrightarrow R/\mathfrak{p}^r \longrightarrow 0$$

vor. Dabei ist

$$\mathfrak{p}^r/\mathfrak{p}^{r+1} = \mathfrak{p}^r R_{\mathfrak{p}}/\mathfrak{p}^{r+1}R_{\mathfrak{p}} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} = R/\mathfrak{p}.$$

Deshalb ist

$$\begin{aligned} N(\mathfrak{p}^{r+1}) &= \#\left(R/\mathfrak{p}^{r+1}\right) \\ &= \#\left(\mathfrak{p}^r/\mathfrak{p}^{r+1}\right) \cdot \#\left(R/\mathfrak{p}^r\right) \\ &= \#\left(R/\mathfrak{p}\right) \cdot \#\left(R/\mathfrak{p}^r\right) \\ &= N(\mathfrak{p}) \cdot N(\mathfrak{p})^r \\ &= N(\mathfrak{p})^{r+1}. \end{aligned}$$

□

Korollar 12.14. *Es sei R ein Zahlbereich und seien $\mathfrak{a}, \mathfrak{b} \neq 0$ Ideale in R. Dann ist*

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

Beweis. Dies folgt unmittelbar aus Satz 12.13. □

Bemerkung 12.15. Zu einem Zahlbereich R und einem Element $f \in R$, $f \neq 0$, kann man folgendermaßen den zugehörigen Hauptdivisor bzw. die Primidealzerlegung $(f) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ algorithmisch berechnen. Dabei arbeitet man im Restklassenring $R/(f)$ und man setzt voraus, dass für R selbst eine Restklassendarstellung über $\mathbb{Z}$ vorliegt. Für den Restklassenring $R/(f)$ hat man dann ebenfalls eine Restklassendarstellung und man weiß, dass dieser endlich ist, also grundsätzlich algorithmisch beherrschbar ist. Das erste Problem ist, die Primideale in R zu bestimmen, in denen f enthalten ist, doch diese entsprechen den maximalen Idealen $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ von $R/(f)$ (die zugehörigen Primideale in R seien mit $\mathfrak{p}_i$ bezeichnet). Dabei liegt dann ein Produktring

$$R/(f) = R_1 \times \cdots \times R_k$$

vor, wobei die R_j lokal mit Restklassenkörper $R/\mathfrak{m}_j = R/\mathfrak{p}_j$ sind. Wegen Satz 12.8 weiß man

$$R/\mathfrak{p}_j^{r_j} = R_j.$$

Man kann nun in R_j die Exponenten r_j jeweils als die minimalen Exponenten mit $\mathfrak{m}_j^r = 0$ bestimmen. Bei der Bestimmung der Exponenten hilft auch die Norm. Nach Satz 12.13 in Verbindung mit Lemma 10.6 ist

$$|N(f)| = \#\left(R/(f)\right) = N(\mathfrak{p}_1)^{r_1} \cdots N(\mathfrak{p}_k)^{r_k}$$

und aus

$$\#\left(R_j\right) = N(\mathfrak{p}_j)^{r_j}$$

kann man wieder die Exponenten r_j bestimmen.

12. Arbeitsblatt

12.1. **Aufgaben.**

Aufgabe 12.1. Es sei R ein Zahlbereich und sei $f \in R$, $f \neq 0$. Es sei $(f) = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ die Zerlegung in Primideale und es sei vorausgesetzt, dass f eine Primfaktorzerlegung besitzt. Zeige, dass die Primideale $\mathfrak{p}_i$ Hauptideale sind.

Aufgabe 12.2. Es sei $\mathfrak{a} \neq 0$ ein Ideal in einem Dedekindbereich. Zeige, dass es ein Ideal $\mathfrak{b} \neq 0$ derart gibt, dass $\mathfrak{ab}$ ein Hauptideal ist.

Aufgabe 12.3. Es sei K ein Körper. Wir betrachten in $K[X,Y]$ die beiden Primideale

$$\mathfrak{p} = (X) \subset (X,Y) = \mathfrak{m}.$$

Zeige, dass es kein Ideal $\mathfrak{a}$ mit

$$\mathfrak{p} = \mathfrak{a} \cdot \mathfrak{m}$$

gibt.

Aufgabe 12.4.*

Es sei $R = R_1 \times \cdots \times R_n$ ein Produkt aus kommutativen Ringen. Zeige, dass für die Einheitengruppe von R die Beziehung

$$R^\times = R_1^\times \times \cdots \times R_n^\times$$

gilt.

Aufgabe 12.5. Sei R ein kommutativer Ring und sei $f \in R$. Es sei f sowohl nilpotent als auch idempotent. Zeige, dass $f = 0$ ist.

Aufgabe 12.6. Seien R und S kommutative Ringe und sei $R \times S$ der Produktring $R \times S$. Zeige, dass die Teilmenge $R \times 0$ ein Hauptideal ist.

Aufgabe 12.7. Seien R ein kommutativer Ring und I, J Ideale in R. Sei weiter

$$\varphi\colon\ R \longrightarrow R/I \times R/J,\ r \longmapsto (r+I, r+J).$$

Zeige, dass φ genau dann surjektiv ist, wenn $I + J = R$ gilt. Wie sieht $\ker \varphi$ aus? Benutze jetzt den Homomorphiesatz um einzusehen, was das im Falle $R = \mathbb{Z}$ mit dem chinesischen Restsatz zu tun hat.

Aufgabe 12.8. Sei R ein kommutativer Ring und seien $I, J \subseteq R$ Ideale. Wir betrachten die Gruppenhomomorphismen

$$\varphi\colon\ R/I \cap J \longrightarrow R/I \times R/J,\ r \longmapsto (r,r),$$

und

$$\psi\colon\ R/I \times R/J \longrightarrow R/I + J,\ (s,t) \longmapsto s - t.$$

Zeige, dass φ injektiv ist, dass ψ surjektiv ist und dass

$$\operatorname{bild}\varphi\ =\ \operatorname{kern}\psi$$

ist. Sind φ und ψ Ringhomomorphismen?

Aufgabe 12.9. Es sei R ein kommutativer Ring und sei $e \in R$ ein idempotentes Element. Zeige, dass es eine natürliche Ringisomorphie

$$R_e\ \cong\ R/(1-e)$$

gibt.

Aufgabe 12.10. Es sei X ein topologischer Raum mit einer disjunkten Zerlegung

$$X\ =\ U \uplus V$$

aus offenen Teilmengen $U, V\ \subseteq\ X$. Zeige, dass die natürliche Abbildung

$$C(X,\mathbb{R}) \longrightarrow C(U,\mathbb{R}) \times C(V,\mathbb{R}),\ f \longmapsto (f|_U, f|_V),$$

bijektiv ist.

Aufgabe 12.11. Es seien R_1 und R_2 kommutative Ringe mit dem Produktring $R\ =\ R_1 \times R_2$. Zeige, dass es eine natürliche Homöomorphie

$$\operatorname{Spek}(R_1) \uplus \operatorname{Spek}(R_2) \longrightarrow \operatorname{Spek}(R_1 \times R_2).$$

gibt.

Aufgabe 12.12.*

Es seien $R_1, R_2, \ldots, R_n$ kommutative Ringe und sei

$$R\ =\ R_1 \times R_2 \times \cdots \times R_n$$

der Produktring.

(1) Es seien

$$I_1 \subseteq R_1, I_2 \subseteq R_2, \ldots, I_n \subseteq R_n$$

Ideale. Zeige, dass die Produktmenge

$$I_1 \times I_2 \times \cdots \times I_n$$

ein Ideal in R ist.

(2) Zeige, dass jedes Ideal $I \subseteq R$ die Form

$$I = I_1 \times I_2 \times \cdots \times I_n$$

mit Idealen $I_j \subseteq R_j$ besitzt.

(3) Sei

$$I = I_1 \times I_2 \times \cdots \times I_n$$

ein Ideal in R. Zeige, dass I genau dann ein Hauptideal ist, wenn sämtliche I_j Hauptideale sind.

(4) Zeige, dass R genau dann ein Hauptidealring ist, wenn alle R_j Hauptidealringe sind.

Aufgabe 12.13. Es sei R ein kommutativer Ring und sei $e \in R$ ein idempotentes Element. Zeige, dass auch $1 - e$ idempotent ist und dass die „zusammengesetzte“ Restklassenabbildung

$$R \longrightarrow R/(e) \times R/(1-e)$$

eine Bijektion ist.

Ein kommutativer Ring R heißt *zusammenhängend*, wenn er genau zwei idempotente Elemente (nämlich $0 \neq 1$) enthält.

Aufgabe 12.14. Sei R ein kommutativer lokaler Ring. Zeige, dass R zusammenhängend ist.

Aufgabe 12.15.*

Zeige, dass ein Integritätsbereich ein zusammenhängender Ring ist.

Aufgabe 12.16.*

(a) Bestimme für die Zahlen 3, 5 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung x der simultanen Kongruenzen

$$x = 2 \mod 3, \quad x = 4 \mod 5 \text{ und } x = 3 \mod 7\,.$$

Aufgabe 12.17. (a) Bestimme für die Zahlen 2, 3 und 7 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(7)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung x der simultanen Kongruenzen

$$x = 1 \mod 2, \quad x = 2 \mod 3 \text{ und } x = 2 \mod 7\,.$$

Aufgabe 12.18.*

a) Finde die Zahlen $z \in \{0,1,\ldots,9\}$ mit der Eigenschaft, dass die letzte Ziffer ihres Quadrates (in der Dezimaldarstellung) gleich z ist.

b) Finde die Zahlen $z \in \{0,1,\ldots,99\}$ mit der Eigenschaft, dass die beiden letzten Ziffern ihres Quadrates (in der Dezimaldarstellung) gleich z ist.

Aufgabe 12.19. Finde in $\mathbb{Q}[X]/(X^2-1)$ nichttriviale idempotente Elemente.

Aufgabe 12.20. Sei R ein faktorieller Bereich und $p \in R$ ein Primelement. Zeige, dass der Restklassenring $R/(p^n)$ nur die beiden trivialen idempotenten Elemente 0 und 1 besitzt.

Aufgabe 12.21. Es sei K ein Körper und sei $K[X]$ der Polynomring über K. Es seien $a_1,\ldots,a_n \in K$ verschiedene Elemente und

$$F \;=\; (X-a_1)\cdots(X-a_n)$$

das Produkt der zugehörigen linearen Polynome. Zeige, dass der Restklassenring $K[X]/(F)$ isomorph zum Produktring K^n ist.

Aufgabe 12.22.*

Das Polynom $X^3-7X^2+3X-21$ besitzt in $\mathbb{R}[X]$ die Zerlegung

$$X^3-7X^2+3X-21 \;=\; (X-7)(X^2+3)$$

in irreduzible Faktoren und daher gilt die Isomorphie

$$\mathbb{R}[X]/(X^3-7X^2+3X-21) \;\cong\; \mathbb{R}[X]/(X-7) \times \mathbb{R}[X]/(X^2+3).$$

a) Bestimme das Polynom kleinsten Grades, das rechts dem Element $(1,0)$ entspricht.

a) Bestimme das Polynom kleinsten Grades, das rechts dem Element $(0,1)$ entspricht.

Aufgabe 12.23.*

Schreibe den Restklassenring $\mathbb{Q}[X]/(X^4-1)$ als ein Produkt von Körpern, wobei lediglich die Körper $\mathbb{Q}$ und $\mathbb{Q}[\mathrm{i}]$ vorkommen. Schreibe die Restklasse von X^3+X als ein Tupel in dieser Produktzerlegung.

Aufgabe 12.24. Zeige, dass jeder echte Restklassenring von $\mathbb{C}[X]$ isomorph zu einem Produktring der Form

$$\mathbb{C}\times\cdots\times\mathbb{C}\times\mathbb{C}[X]/(X^2)\times\cdots\times\mathbb{C}[X]/(X^2)\times\mathbb{C}[X]/(X^3)\times\cdots \\ \times\mathbb{C}[X]/(X^3)\times\cdots\times\mathbb{C}[X]/(X^m)\times\cdots\times\mathbb{C}[X]/(X^m$$

ist.

Aufgabe 12.25. Realisiere den Produktring

$$\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}$$

als einen Restklassenring von $\mathbb{R}[X]$.

Aufgabe 12.26. Zeige, dass die folgenden K-Algebren zueinander isomorph sind.

(1) Der Produktring $K\times K\times K$.
(2) Der Restklassenring $K[X]/(X^3-X)$.
(3) Der Restklassenring $K[X,Y]/(X,Y)\cdot(X-1,Y-1)\cdot(X,Y-7)$.

Aufgabe 12.27.*

Bestimme in $\mathbb{Z}[\sqrt{7}]$ die Primideale, die $5-3\sqrt{7}$ enthalten, sowie den Hauptdivisor zu $5-3\sqrt{7}$.

Aufgabe 12.28.*

Es sei R ein Dedekindbereich und $\mathfrak{a}\neq 0$ ein Ideal. Zeige, dass $R/\mathfrak{a}$ ein Hauptidealring ist.

Aufgabe 12.29. Zeige, dass jedes Ideal $\mathfrak{a}$ in einem Dedekindbereich R von maximal zwei Elementen erzeugt wird.

Aufgabe 12.30. Es sei R ein Zahlbereich. Zeige, dass die Norm einen Monoidhomomorphismus

$$N\colon\ (\operatorname{Eff}\operatorname{Div}(R),+)\longrightarrow(\mathbb{N}_+,\cdot)$$

festlegt.

Aufgabe 12.31. Es sei R ein Zahlbereich und sei $T \subseteq \mathbb{N}$ die Menge aller Normen zu Idealen $\neq 0$ in R. Zeige, dass T ein multiplikatives System ist, das von gewissen Primzahlpotenzen p^i erzeugt wird.

Aufgabe 12.32. Zeige, dass es in einer endlichen integren Erweiterung $\mathbb{Z} \subseteq R$ Primideale $\mathfrak{p}$ derart geben kann, dass die Anzahl des Restklassenringes $R/\mathfrak{p}^r$ zu einer Primidealpotenz $\mathfrak{p}^r$ keine Potenz ist.

13. Vorlesung - Divisoren

13.1. **Divisoren.**

Die Menge der effektiven Divisoren zu einem Dedekindbereich bilden mit der natürlichen Addition ein kommutatives Monoid, aber keine Gruppe, da ja die Koeffizienten $n_{\mathfrak{p}}$ alle nichtnegativ sind. Lässt man auch negative ganze Zahlen zu, so gelangt man zum Begriff des Divisors, die eine Gruppe bilden. Auch den Begriff des Hauptdivisors kann man so erweitern, dass er nicht nur für ganze Elemente aus R, sondern auch für rationale Elemente, also Elemente aus dem Quotientenkörper $Q(R)$, definiert ist.

Definition 13.1. Es sei R ein Dedekindbereich. Ein *Divisor* ist eine formale Summe

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}\,,$$

die sich über alle Primideale $\mathfrak{p} \neq 0$ aus R erstreckt und wobei $n_{\mathfrak{p}}$ ganze Zahlen mit $n_{\mathfrak{p}} = 0$ für fast alle $\mathfrak{p}$ sind.

Für einen diskreten Bewertungsring lässt sich die Ordnung $\operatorname{ord}\colon R \setminus \{0\} \to \mathbb{N}$, $q \mapsto \operatorname{ord}(q)$, zu einer Ordnungsfunktion auf dem Quotientenkörper fortsetzen,

$$\operatorname{ord}\colon Q(R) \setminus \{0\} \longrightarrow \mathbb{Z},\ q \longmapsto \operatorname{div}(q),$$

siehe Aufgabe 13.1, wobei sich die Eigenschaften von Lemma 10.15 hierher übertragen.

Definition 13.2. Es sei R ein Dedekindbereich und $q \in Q(R)$, $q \neq 0$. Dann heißt die Abbildung, die jedem Primideal $\mathfrak{p} \neq 0$ in R die Ordnung $\operatorname{ord}_{\mathfrak{p}}(q)$ zuordnet, der durch q definierte *Hauptdivisor*. Er wird mit $\operatorname{div}(q)$ bezeichnet und als formale Summe

$$\operatorname{div}(q) = \sum_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(q) \cdot \mathfrak{p}$$

geschrieben.

Wenn man die rationale Funktion $q \in Q(R)$ als $q = \frac{f}{g}$ mit $f, g \in R$ ansetzt, so gilt

$$\operatorname{div}(q) = \operatorname{div}(f) - \operatorname{div}(g),$$

da dies punktweise an jedem Primideal gilt. Bei

$$\operatorname{ord}_{\mathfrak{p}}(q) < 0$$

sagt man auch, dass q einen *Pol* an der Stelle $\mathfrak{p}$ besitzt, und zwar mit der Polordnung $-\operatorname{ord}_{\mathfrak{p}}(q)$.

Die Menge der Divisoren bildet eine additive kommutative freie Gruppe, die wir mit $\operatorname{Div}(R)$ bezeichnen.

Lemma 13.3. *Es sei R ein Dedekindbereich mit Quotientenkörper $Q(R)$, und seien $q, q_1, q_2 \in Q(R) \setminus \{0\}$. Dann gelten folgende Aussagen.*

(1) *Es ist* $\operatorname{div}(q_1q_2) = \operatorname{div}(q_1) + \operatorname{div}(q_2)$.
(2) *Es ist* $\operatorname{div}(q_1 + q_2) \geq \min\{\operatorname{div}(q_1), \operatorname{div}(q_2)\}$.
(3) *Es ist $q \in R$ genau dann, wenn der Hauptdivisor* $\operatorname{div}(q)$ *effektiv ist.*
(4) *Zu jedem Divisor D gibt es ein $h \in R$ derart, dass $D + \operatorname{div}(h)$ effektiv ist.*

Beweis. Für (1) und (2) siehe Aufgabe 13.2, für (3) siehe Aufgabe 13.3, für (4) siehe Aufgabe 13.4. □

Es liegt also insbesondere ein Gruppenhomomorphismus

$$(Q(R))^\times \longrightarrow \operatorname{Div}(R),\ q \longmapsto \operatorname{div}(q),$$

vor. Das Bild unter diesem Gruppenhomomorphismus ist die Untergruppe der Hauptdivisoren, die wir mit H bezeichnen.

13.2. **Gebrochene Ideale.**

In Satz 11.13 haben wir eine Bijektion zwischen effektiven Divisoren und von 0 verschiedenen Idealen (und von effektiven Hauptdivisoren mit von 0 verschiedenen Hauptidealen) gestiftet. Von daher liegt die Frage nahe, welche „Ideal-ähnlichen“ Objekte den Divisoren entsprechen. Wir wollen also wissen, durch welche Objekte wir das Fragezeichen im folgenden Diagramm ersetzen müssen.

$$\begin{array}{ccc} \operatorname{Ideale}(R) & \xrightarrow{\sim} & \operatorname{Eff}\operatorname{Div}(R) \\ \downarrow & & \downarrow \\ ? & \xrightarrow{\sim} & \operatorname{Div}(R) \end{array}$$

Da wir einen Divisor D stets als $D = E - F$ mit effektiven Divisoren E und F schreiben können, liegt die Vermutung nahe, nach etwas wie dem Inversen (bezüglich der Multiplikation) eines Ideals zu suchen. Im Fall eines faktoriellen Dedekindbereichs entsprechen sich (bis auf die Einheiten) Elemente und Hauptdivisoren, und zwar sowohl auf der Ringebene (siehe Bemerkung 11.4) als auch auf der Ebene des Quotientenkörpers. Zu einer rationale Funktion q bzw. dem Hauptdivisor $\operatorname{div}(q)$ gehört in diesem Fall einfach der von q erzeugte R-Untermodul qR des Quotientenkörpers $Q(R)$. Im Fall der rationalen Zahlen sind dies Untergruppen der Form $\frac{1}{10}\mathbb{Z}$ oder $\frac{7}{3}\mathbb{Z}$. Für allgemeine

Integritätsbereiche führt man ganz allgemein die sogenannten gebrochenen Ideale ein.

Definition 13.4. Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann nennt man einen endlich erzeugten R-Untermodul $\mathfrak{f}$ des R-Moduls $Q(R)$ ein *gebrochenes Ideal*.

Lemma 13.5. *Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$ und sei $\mathfrak{f} \subseteq Q(R)$ eine Teilmenge. Dann sind folgende Aussagen äquivalent.*

(1) *$\mathfrak{f}$ ist ein gebrochenes Ideal.*
(2) *Es gibt ein endlich erzeugtes*[1] *Ideal $\mathfrak{a}$ in R und ein Element $r \in R$, $r \neq 0$, derart, dass*
$$\mathfrak{f} = \frac{\mathfrak{a}}{r} = \left\{ \frac{a}{r} \mid a \in \mathfrak{a} \right\}$$
gilt.

Beweis. Sei zunächst $\mathfrak{f}$ ein gebrochenes Ideal. Dann ist
$$\mathfrak{f} = R\left(\frac{a_1}{r_1}, \ldots, \frac{a_n}{r_n}\right).$$
Nach Übergang zu einem Hauptnenner kann man annehmen, dass $r = r_1 = \ldots = r_n$ ist. Dann hat man mit dem Ideal $\mathfrak{a} = (a_1, \ldots, a_n)$ eine Beschreibung der gewünschten Art. Ist umgekehrt $\mathfrak{f} = \frac{\mathfrak{a}}{r}$, so ist dies natürlich ein endlich erzeugter R-Untermodul von $Q(R)$. □

Wie für Ideale spielen diejenigen gebrochenen Ideale, die von einem Element erzeugt sind, eine besondere Rolle.

Definition 13.6. Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann nennt man ein gebrochenes Ideal der Form $\mathfrak{f} = Rq$ mit $q \in Q(R)$ ein *gebrochenes Hauptideal*.

Aus Lemma 13.5 ergibt sich sofort, dass für einen Hauptidealbereich jedes gebrochene Ideal ein gebrochenes Hauptideal ist.

Definition 13.7. Es sei R ein Integritätsbereich mit Quotientenkörper $Q(R)$. Dann definiert man für gebrochene Ideale $\mathfrak{f}$ und $\mathfrak{g}$ das *Produkt* $\mathfrak{f} \cdot \mathfrak{g}$ als den von allen Produkten erzeugten R-Untermodul von $Q(R)$, also
$$\mathfrak{f} \cdot \mathfrak{g} := R\langle gf : f \in \mathfrak{f}, g \in \mathfrak{g} \rangle,$$
wobei die Produkte in $Q(R)$ zu nehmen sind.

Wird das gebrochene Ideal $\mathfrak{f}$ als R-Modul von $f_1, \ldots, f_n$ erzeugt und wird das gebrochene Ideal $\mathfrak{g}$ von $g_1, \ldots, g_m$ erzeugt, so wird das Produkt $\mathfrak{fg}$ von den Produkten $f_i g_j$, $1 \leq i \leq n$, $1 \leq j \leq m$, erzeugt. Also ist das Produkt in der Tat wieder endlich erzeugt und damit ein gebrochenes Ideal. Für Ideale

[1] Dies ist bei R noethersch natürlich automatisch erfüllt.

stimmt natürlich das Idealprodukt mit dem hier definierten Produkt von gebrochenen Idealen überein. Das Produkt von gebrochenen Hauptidealen ist wieder ein gebrochenes Hauptideal.

In einem beliebigen Integritätsbereich bilden die gebrochenen Ideale $\neq 0$ keine Gruppe. Für stärkere Aussagen müssen wir jetzt wieder voraussetzen, dass R ein Dedekindbereich ist.

Definition 13.8. Zu einem gebrochenen Ideal $\mathfrak{f} \neq 0$ in einem Dedekindbereich R nennt man

$$\mathfrak{f}^{-1} := \{q \in Q(R) \mid q \cdot \mathfrak{f} \subseteq R\}$$

das zugehörige *inverse gebrochene Ideal*.

Lemma 13.9. *Es sei R ein Dedekindbereich. Dann gelten folgende Aussagen.*

(1) *Zu gebrochenen Idealen mit der Beziehung $\mathfrak{g} = r\mathfrak{f}$ mit $r \in Q(R)$, $r \neq 0$, gilt für die inversen gebrochenes Ideale die Beziehung $\mathfrak{g}^{-1} = r^{-1}\mathfrak{f}^{-1}$.*
(2) *Zu einem gebrochenen Ideal $\mathfrak{f}$ ist das inverse gebrochene Ideal in der Tat ein gebrochenes Ideal.*
(3) *Es ist $\mathfrak{f} \cdot \mathfrak{f}^{-1} = R$.*

Beweis. (1) Der R-Modulisomorphismus $\mathfrak{f} \to \mathfrak{g}$, $f \mapsto rf$, führt direkt zu einem Isomorphismus $\mathfrak{f}^{-1} \to r^{-1}\mathfrak{g}^{-1}$, $q \mapsto r^{-1}q$, da ja $q\mathfrak{f} \subseteq R$ zu $(r^{-1}q)(r\mathfrak{f}) \subseteq R$ äquivalent ist.

(2) Es ist klar, dass $\mathfrak{f}^{-1}$ ein von 0 verschiedener R-Untermodul von $Q(R)$ ist. Wenn $\mathfrak{f}$ durch $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$ erzeugt wird, so betrachten wir $\mathfrak{g} = \frac{\mathfrak{f}}{a}$ mit $a = a_1 \cdots a_n$, wobei jetzt $\mathfrak{g}$ ein Erzeugendensystem der Form $\frac{1}{c_1}, \ldots, \frac{1}{c_n}$ mit $c_i \in R$ besitzt. Die Bedingung

$$q\frac{1}{c_i} \in R$$

impliziert $q \in R$. Daher ist das inverse gebrochene Ideal zu $\mathfrak{g}$ selbst ein Ideal, also endlich erzeugt. Dies überträgt sich wegen (1) auf $\mathfrak{f}$.

(3) Für das Produkt ist offenbar

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

Wenn diese Inklusion echt wäre, so würde es auch ein maximales Ideal $\mathfrak{p}$ oberhalb von $\mathfrak{f} \cdot \mathfrak{f}^{-1}$ geben. Es sei $\mathfrak{f}_\mathfrak{p} = (\pi^n)$ mit einer Ortsuniformisierenden π und mit $n \in \mathbb{Z}$. Es gibt dann auch ein Element $f \in \mathfrak{f}$, das an der Stelle $\mathfrak{p}$ die Ordnung n besitzt. Dazu gibt es auch ein $q \in Q(R)$, das an der Stelle $\mathfrak{p}$ die Ordnung $-n$ und sonst überall eine hinreichend große Ordnung besitzt derart, dass $fq \in R$ ist. Dies ist ein Widerspruch, da fg an der Stelle $\mathfrak{p}$ die Ordnung 0 besitzt.

□

Beispiel 13.10. Wir betrachten im quadratischen Zahlbereich $\mathbb{Z}[\sqrt{-5}]$ das Ideal

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

Aufgrund der Gleichung

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

ist

$$\frac{1-\sqrt{-5}}{2} \cdot \mathfrak{a} \subseteq R, \frac{3}{1+\sqrt{-5}} \cdot \mathfrak{a} \subseteq R, 1 \cdot \mathfrak{a} \subseteq R\,.$$

Wir behaupten, dass das inverse gebrochene Ideal $\mathfrak{a}^{-1}$ gleich

$$\mathfrak{f} = R\left(1, \frac{1-\sqrt{-5}}{2}\right)$$

ist, wobei sich die Inklusion $\mathfrak{f} \subseteq \mathfrak{a}^{-1}$ aus der vorstehenden Zeile ergibt. Andererseits gilt wegen

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

für das Produkt

$$\mathfrak{a} \cdot \mathfrak{f} = R,$$

und dies impliziert nach Aufgabe 13.2 die Gleichheit $\mathfrak{f} = \mathfrak{a}^{-1}$.

Bemerkung 13.11. Ein gebrochenes Ideal $\mathfrak{f} \neq 0$ in einem Dedekindbereich ist ein sogenannter *invertierbarer Modul*. D.h. es ist *lokal isomorph* zum Ring selbst. Mit diesen Formulierungen ist folgendes gemeint: Für ein maximales Ideal (also für ein von 0 verschiedenes Primideal) $\mathfrak{p}$ ist $\mathfrak{f}R_{\mathfrak{p}} = \mathfrak{f}_{\mathfrak{p}}$ (dies ist die Lokalisierung eines Moduls an einem Primideal) ein endlich erzeugter $R_{\mathfrak{p}}$-Modul $\neq 0$, der zugleich im Quotientenkörper liegt. Solche Moduln sind isomorph zu $R_{\mathfrak{p}}$. Siehe Aufgabe 4.29.

Definition 13.12. Es sei R ein Dedekindbereich und

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}$$

ein Divisor (wobei $\mathfrak{p}$ durch die Menge der Primideale $\neq 0$ läuft). Dann nennt man

$$\{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$$

das *gebrochene Ideal zum Divisor* D. Es wird mit $\mathrm{Id}(D)$ bezeichnet.

Das folgende Lemma zeigt, dass man in der Tat ein gebrochenes Ideal erhält, und dass diese Definition mit der früheren Definition 11.12 verträglich ist.

Lemma 13.13. *Es sei R ein Dedekindbereich und $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p}$ ein Divisor. Dann ist die Menge $\{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$ ein gebrochenes Ideal. Ist D ein effektiver Divisor, dann ist das so definierte gebrochene Ideal ein Ideal und stimmt mit dem Ideal überein, das einem effektiven Divisor gemäß der Definition 11.12 zugeordnet wird.*

Beweis. Es sei $\mathfrak{f} = \{f \in Q(R) \mid \operatorname{div}(f) \geq D\}$. Gemäß der Konvention, dass $\operatorname{div}(0) = \infty$ zu interpretieren ist, ist $0 \in \mathfrak{f}$. Für Elemente $f_1, f_2 \in Q(R)$ mit $\operatorname{div}(f_1), \operatorname{div}(f_2) \geq D$ gilt nach Lemma 13.3

$$\operatorname{div}(f_1 + f_2) \geq \min(\operatorname{div}(f_1), \operatorname{div}(f_2)) \geq D$$

und

$$\operatorname{div}(rf) = \operatorname{div}(r) + \operatorname{div}(f) \geq D$$

für $r \in R$, da ja $\operatorname{div}(r)$ effektiv ist. Also liegt in der Tat ein R-Modul vor.

Bevor wir die endliche Erzeugtheit nachweisen, betrachten wir die zweite Aussage. Es sei also E ein effektiver Divisor. Wir haben zu zeigen, dass

$$\{f \in Q(R) \mid \operatorname{div}(f) \geq E\} = \{f \in R \mid \operatorname{div}(f) \geq E\}$$

ist, wobei die Inklusion $\supseteq$ klar ist. Die andere Inklusion folgt aus Lemma 13.3 (3).

Zum Nachweis der endlichen Erzeugtheit bemerken wir, dass es nach Lemma 13.3 (4) zu jedem Divisor D ein $r \in R$ derart gibt, dass $D' = D + \operatorname{div}(r)$ effektiv ist. Das zu D' gehörige gebrochene Ideal ist dann ein Ideal, also endlich erzeugt, und dies überträgt sich auf das gebrochene Ideal zu D. □

Definition 13.14. Es sei R ein Dedekindbereich und $\mathfrak{f} \neq 0$ ein von 0 verschiedenes gebrochenes Ideal. Dann nennt man den Divisor

$$\operatorname{div}(\mathfrak{f}) = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \cdot \mathfrak{p}$$

mit

$$m_{\mathfrak{p}} = \min(\operatorname{ord}_{\mathfrak{p}}(f) | f \in \mathfrak{f},\ f \neq 0)$$

den *Divisor zum gebrochenen Ideal* $\mathfrak{f}$.

Da das gebrochene Ideal $\mathfrak{f}$ nach Definition endlich erzeugt ist, muss man das Minimum nur über eine endliche Menge nehmen. Insbesondere ist der zugehörige Divisor wohldefiniert. Für ein Ideal stimmt diese Definition offensichtlich mit der alten überein.

Lemma 13.15. *Es sei R ein Dedekindbereich. Dann gelten folgende Aussagen.*

(1) *Es sei $\mathfrak{f}$ ein gebrochenes Ideal mit einer Darstellung $\mathfrak{f} = \frac{\mathfrak{a}}{h}$ mit $h \in R$ und einem Ideal $\mathfrak{a} \subseteq R$. Dann ist*

$$\operatorname{div}(\mathfrak{f}) = \operatorname{div}(\mathfrak{a}) - \operatorname{div}(h).$$

(2) *Zu einem Divisor D mit $E = D + \operatorname{div}(h)$ effektiv ist*

$$\operatorname{Id}(D) = \frac{\operatorname{Id}(E)}{h}.$$

Beweis. Siehe Aufgabe 13.24. □

Auch die Einzelheiten des Beweises des folgenden Satzes überlassen wir dem Leser, siehe Aufgabe 13.25.

Satz 13.16. *Es sei R ein Dedekindbereich. Dann sind die Zuordnungen*

$$\mathfrak{f} \longmapsto \operatorname{div}(\mathfrak{f}) \quad \textit{und} \quad D \longmapsto \operatorname{Id}(D)$$

zueinander inverse Abbildungen zwischen der Menge der von 0 verschiedenen gebrochenen Ideale und der Menge der Divisoren. Diese Bijektion ist ein Isomorphismus von Gruppen.

Beweis. Wir haben zu zeigen, dass die hintereinandergeschalteten Abbildungen jeweils die Identität ergeben. Dies kann man mittels Lemma 13.15 auf den effektiven Fall zurückführen. Die Zuordnung $\mathfrak{f} \mapsto \operatorname{div}(\mathfrak{f})$ führt die Multiplikation von gebrochenen Idealen in die Addition von Divisoren über, da dies an jedem diskreten Bewertungsring $R_{\mathfrak{p}}$ gilt. Wegen der Bijektivität liegt dann auch links eine Gruppe vor und die Abbildungen sind Gruppenisomorphismen. □

13. Arbeitsblatt

13.1. **Aufgaben.**

Aufgabe 13.1. Sei R ein diskreter Bewertungsring. Definiere zu einem Element $q \in Q(R)$, $q \neq 0$, die Ordnung

$$\operatorname{ord}(q) \in \mathbb{Z}\,.$$

Dabei soll die Definition mit der Ordnung für Elemente aus R übereinstimmen und einen Gruppenhomomorphismus $Q(R) \setminus \{0\} \to \mathbb{Z}$ definieren. Was ist der Kern dieses Homomorphismus?

Aufgabe 13.2. Es sei R ein Dedekindbereich. Zeige, dass die Abbildung, die einem Element $q \in Q(R)$, $q \neq 0$, den Hauptdivisor $\operatorname{div}(q)$ zuordnet, folgende Eigenschaften besitzt.

(1) Es ist $\operatorname{div}(q_1q_2) = \operatorname{div}(q_1) + \operatorname{div}(q_2)$.
(2) Es ist $\operatorname{div}(q_1 + q_2) \geq \min\{\operatorname{div}(q_1), \operatorname{div}(q_2)\}$.

Zeige insbesondere, dass diese Zuordnung einen Gruppenhomomorphismus

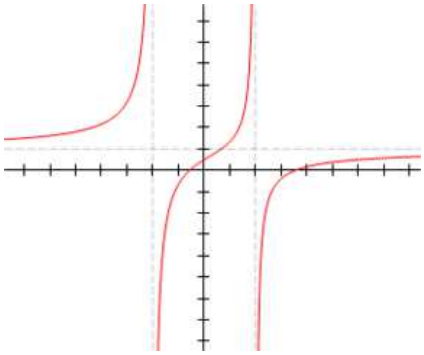
$$Q(R) \setminus \{0\} \longrightarrow \operatorname{Div}(R)$$

definiert und dass die Hauptdivisoren eine Untergruppe der Divisoren bilden.

Aufgabe 13.3.*

Es sei R ein Dedekindbereich mit Quotientenkörper $Q(R)$ und sei $q \in Q(R) \setminus \{0\}$. Zeige, dass $q \in R$ genau dann gilt, wenn der Hauptdivisor $\operatorname{div}(q)$ effektiv ist.

Aufgabe 13.4. Es sei R ein Dedekindbereich mit Quotientenkörper $Q(R)$ und sei D ein Divisor. Zeige, dass es ein $q \in R$ derart gibt, dass $D + \operatorname{div}(q)$ effektiv ist.



Aufgabe 13.5. Bestimme eine rationale Funktion $\mathbb{C} \to \mathbb{C}$, die an der Stelle $2 - \mathrm{i}$ einen Pol der Ordnung 4, in $-3 + 5\mathrm{i}$ eine Nullstelle der Ordnung 2 und in -3 einen Pol der Ordnung 3 besitzt.

Aufgabe 13.6. Es sei $f \neq 0$ eine rationale Funktion $f\colon \mathbb{C} \to \mathbb{C}$. Zeige, dass f in $a \in \mathbb{C}$ genau dann eine Nullstelle der Ordnung n besitzt, wenn f^{-1} in a einen Pol der Ordnung n besitzt.

Aufgabe 13.7. Es sei R ein quadratischer Zahlbereich. Definiere zu einem Divisor D den „konjugierten Divisor“ $\overline{D}$. Zeige, dass für $q \in Q(R)$, $q \neq 0$, die Beziehung

$$\overline{\operatorname{div}(q)} = \operatorname{div}(\overline{q})$$

gilt.

Aufgabe 13.8. Beweise, dass es zu einem Zahlbereich R einen Gruppenisomorphismus

$$Q(R)^\times / R^\times \longrightarrow H$$

gibt, wobei H die Gruppe der Hauptdivisoren bezeichnet.

Aufgabe 13.9. Bestimme in $\mathbb{Z}[\sqrt{-2}]$ einen größten gemeinsamen Teiler für $22 + 25\sqrt{-2}$ und $43 - 23\sqrt{-2}$.

Aufgabe 13.10. Es sei $R = \mathbb{Z}[\sqrt{-6}] \cong \mathbb{Z}[X]/(X^2+6)$. Berechne den Hauptdivisor zu

$$q = \frac{2}{3} - \frac{1}{4}\sqrt{-6}.$$

Aufgabe 13.11.*

Es sei

$$R = \mathbb{Z}[\sqrt{-6}] \cong \mathbb{Z}[X]/(X^2+6).$$

Berechne den Hauptdivisor zu

$$q = \frac{4}{5} + \frac{2}{3}\sqrt{-6}.$$

Aufgabe 13.12.*

Es sei $R = A_{14} = \mathbb{Z}[\sqrt{14}]$ der quadratische Zahlbereich zu $D = 14$. Berechne zu

$$q = \frac{3}{5} - \frac{1}{7}\sqrt{14}$$

den zugehörigen Hauptdivisor.

Aufgabe 13.13. Sei $R = A_{-15} = \mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$ der quadratische Zahlbereich zu $D = -15$. Berechne zu

$$q = \frac{3}{10} - \frac{5}{6}\sqrt{-15}$$

den zugehörigen Hauptdivisor und stelle ihn als Differenz zweier effektiver Divisoren dar.

Aufgabe 13.14. Sei $R = A_{-11} = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ der quadratische Zahlbereich zu $D = -11$. Berechne mittels des euklidischen Algorithmus den größten gemeinsamen Teiler von

$$35 + \sqrt{-11} \text{ und } -89 + 21\sqrt{-11}\,.$$

Aufgabe 13.15. Sei $R = A_{-7} = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ der quadratische Zahlbereich zu $D = -7$. Bestimme die Primfaktorzerlegung von

$$4 + 9\sqrt{-7}\,.$$

Aufgabe 13.16. Sei D quadratfrei mit $D = 3 \mod 4$ und $D < -1$. Zeige, dass $(2, 1+\sqrt{D})$ ein Primideal im quadratischen Zahlbereich A_D ist, aber kein Hauptideal. Folgere, dass diese Ringe nicht faktoriell sind.

Aufgabe 13.17. Im quadratischen Zahlbereich $A_6 \cong \mathbb{Z}[\sqrt{6}]$ gilt

$$2 \cdot 3 = \sqrt{6} \cdot \sqrt{6}\,.$$

Finde die Primfaktorzerlegungen (?) der beteiligten Faktoren und des Produktes.

Aufgabe 13.18. Im quadratischen Zahlbereich $A_{-6} \cong \mathbb{Z}[\sqrt{-6}]$ gilt

$$-2 \cdot 3 = \sqrt{-6} \cdot \sqrt{-6}\,.$$

Kann man diese Produkte weiter zerlegen, sind die beteiligten Faktoren prim?

Aufgabe 13.19. Sei D quadratfrei und betrachte $\mathbb{Z}[\sqrt{D}] \subseteq A_D$. Charakterisiere für die beiden Ringe, wann $\sqrt{D}$ prim ist.

Aufgabe 13.20. Bestimme in $\mathbb{Z}[\sqrt{-2}]$ einen größten gemeinsamen Teiler für $-169 + 2\sqrt{-2}$ und $-70 + 113\sqrt{-2}$.

Aufgabe 13.21. Sei $D \leq -2$ quadratfrei und betrachte $R = \mathbb{Z}[\sqrt{D}]$. Zeige, dass die einzige Faktorisierung (bis auf Einheiten) von D durch

$$D \;=\; \sqrt{D}\sqrt{D}$$

gegeben ist. Zeige damit, dass $\sqrt{D}$ irreduzibel ist. Zeige ferner, dass falls $-D$ keine Primzahl ist, dann auch $\sqrt{D}$ nicht prim in R ist.

Aufgabe 13.22. Bestimme einen Erzeuger für das gebrochene Ideal $\mathfrak{f} \subseteq \mathbb{Q}$, das durch die rationalen Zahlen

$$\frac{4}{7}, \frac{7}{10}, \frac{13}{8}$$

erzeugt wird.

Aufgabe 13.23. Der Floh Kurt lebt auf einem unendlichen Lineal und befindet sich in der Nullposition. Er verfügt über drei Sprünge, nämlich

$$\frac{11}{77}, \frac{25}{49}, \frac{82}{15}\,.$$

Berechne das zugehörige gebrochene Ideal, das seinem Lebensraum entspricht.

Aufgabe 13.24.*

Es sei $R = \mathbb{Z}[\mathrm{i}]$. Berechne einen Erzeuger für das gebrochene Ideal aus $Q(R) = \mathbb{Q}[\mathrm{i}]$, das durch die beiden Erzeuger

$$\frac{5}{7} \text{ und } \frac{-8+6\mathrm{i}}{5}$$

gegeben ist.

Aufgabe 13.25. Die Flöhin Paola lebt in der komplexen Ebene und befindet sich im Nullpunkt. Sie verfügt über drei Sprünge, nämlich

$$\frac{3}{4} - \frac{2}{5}\mathrm{i},\ 2 + \frac{2}{3}\mathrm{i},\ \frac{1}{7} + 7\mathrm{i}\,.$$

Man gebe eine einfache Beschreibung des gebrochenen Ideals, das ihrem Lebensraum entspricht.

Aufgabe 13.26. Sei $R = A_{-13} = \mathbb{Z}[\sqrt{-13}]$ der quadratische Zahlbereich zu $D = -13$. Berechne zu

$$q = \frac{2}{3} - \frac{5}{7}\sqrt{-13}$$

den zugehörigen Hauptdivisor und stelle ihn als Differenz zweier effektiver Divisoren dar.

Aufgabe 13.27.*

Es seien $\mathfrak{f}$ und $\mathfrak{g}$ gebrochene Ideale in einem Dedekindbereich R. Es gelte

$$\mathfrak{f} \cdot \mathfrak{g} = R.$$

Zeige, dass dann

$$\mathfrak{f} = \mathfrak{g}^{-1}$$

ist.

Aufgabe 13.28. Es sei $\mathfrak{a} \subseteq R$ ein Ideal in einem Dedekindbereich R mit dem zugehörigen effektiven Divisor E. Zeige, dass das inverse gebrochene Ideal

$$\mathfrak{a}^{-1} = \{q \in Q(R) \mid q \cdot \mathfrak{a} \subseteq R\}$$

gleich dem zu $-E$ gehörenden gebrochenen Ideal $\mathrm{Id}(-E)$ ist.

Aufgabe 13.29. Es sei R ein Zahlbereich und es seien $\mathfrak{f}$ und $\mathfrak{g}$ gebrochene Ideale.

(1) Zeige, dass wenn es ein $r \in Q(R)$, $r \neq 0$, mit
$$\mathfrak{g} = r\mathfrak{f}$$
gibt, dass dann die Multiplikation mit r, also
$$Q(R) \longrightarrow Q(R),\ f \longmapsto rf,$$
einen R-Modulisomorphismus
$$\mathfrak{f} \longrightarrow \mathfrak{g}$$
induziert.

(2) Zeige, dass wenn es irgendeinen R-Modulisomorphismus
$$\varphi\colon\ \mathfrak{f} \longrightarrow \mathfrak{g}$$
gibt, dass es dann schon ein $r \in Q(R)$ mit
$$\mathfrak{g} = r\mathfrak{f}$$
gibt, und dass der Isomorphismus eine Multiplikation ist.

Aufgabe 13.30. Zeige direkt, dass die gebrochenen Ideale $\neq 0$ eine Gruppe bilden, und dass die gebrochenen Hauptideale darin eine Untergruppe bilden.

Aufgabe 13.31. Zeige, dass man jedes gebrochene Ideal $\mathfrak{f}$ in einem Dedekindbereich R in der Form
$$\mathfrak{f} = \mathfrak{a} \cdot \mathfrak{b}^{-1}$$
mit Idealen $\mathfrak{a}$ und $\mathfrak{b}$ darstellen kann.

Aufgabe 13.32. Es sei K ein Körper und $K[X,Y]$ der Polynomring in zwei Variablen und $\mathfrak{m} = (X,Y)$. Zeige
$$\mathfrak{m} \cdot \mathfrak{m}^2 = \mathfrak{m} \cdot (X^2, Y^2).$$
Man folgere, dass die gebrochenen Ideale $\neq 0$ zu diesem Ring keine Gruppe bezüglich der Multiplikation von Idealen bilden kann.

Aufgabe 13.33. Es sei R ein Dedekindbereich. Zeige die folgenden Aussagen.

(1) Es sei $\mathfrak{f}$ ein gebrochenes Ideal mit einer Darstellung $\mathfrak{f} = \frac{\mathfrak{a}}{h}$ mit $h \in R$ und einem Ideal $\mathfrak{a} \subseteq R$. Dann ist
$$\operatorname{div}(\mathfrak{f}) = \operatorname{div}(\mathfrak{a}) - \operatorname{div}(h).$$

(2) Zu einem Divisor D mit $E = D + \operatorname{div}(h)$ effektiv ist
$$\operatorname{Id}(D) = \frac{\operatorname{Id}(E)}{h}.$$

Aufgabe 13.34. Führe die Einzelheiten im Beweis zu Satz 13.16 aus.

Aufgabe 13.35. Es sei $\mathfrak{a} = (f_1, \ldots, f_n)$ (mit $f_i \neq 0$) ein Ideal in einem Zahlbereich R und sei vorausgesetzt, dass das inverse gebrochene Ideal $\mathfrak{a}^{-1}$ die Gestalt

$$\mathfrak{a}^{-1} = (f_1^{-1}, \ldots, f_n^{-1})$$

hat. Zeige, dass $\mathfrak{a}$ ein Hauptideal sein muss.

Aufgabe 13.36. Es sei R ein Zahlbereich. Erweitere die (multiplikative) Normabbildung

$$\text{Ideale}\,(R) \longrightarrow (\mathbb{N}_+, \cdot),\ \mathfrak{a} \longmapsto N(\mathfrak{a}),$$

zu einem Gruppenhomomorphismus

$$\text{Gebrochene Ideale}\,(R) \longrightarrow \mathbb{Q}^\times.$$

Aufgabe 13.37. Finde eine (additive) Gruppe G und Gruppenhomomorphismen φ und ψ derart, dass das Diagramm

$$\begin{array}{ccc} \text{Gebrochene Ideale}\,(R) & \xrightarrow{\sim} & \text{Div}\,(R) \\ \text{Norm}\downarrow & & \downarrow\psi \\ \mathbb{Q}^\times & \xrightarrow{\varphi} & G \end{array}$$

kommutiert und dass φ injektiv ist.

14. Vorlesung - Die Divsorenklassengruppe

14.1. **Die Divisorenklassengruppe.**

In vielen Gebieten der Mathematik spielen homologische Methoden eine wichtige Rolle. Dabei wird den mathematischen Objekten eine Gruppe als Invariante zugeordnet, die relevante Information über das ursprüngliche Objekt beinhaltet aber zugleich deutlich einfacher strukturiert ist. Beispiele hierfür sind die Fundamentalgruppe in der Topologie, Homotopie- und Homologiegruppen in der algebraischen Topologie, Kohomologiegruppen zu Garben in der algebraischen Geometrie, ... Das Verschwinden dieser Gruppen charakterisiert dabei wichtige geometrische Eigenschaften. Die Konstruktion dieser Gruppen ist im Allgemeinen aufwändig und geht dabei häufig über den Weg von „sehr großen“ Gruppen modulo sehr großen Untergruppen (Normalteilern), wobei die Restklassengruppen dann „ziemlich klein“ sind. In diesen Zusammenhang fügt sich auch die Divisorenklassengruppe für algebraische Zahlbereiche ein.

Definition 14.1. Es sei R ein Dedekindbereich. Es sei $\operatorname{Div}(R)$ die Gruppe der Divisoren und $H \subseteq \operatorname{Div}(R)$ sei die Untergruppe der Hauptdivisoren. Dann nennt man die Restklassengruppe

$$\operatorname{KG}(R) = \operatorname{Div}(R)/H$$

die *Divisorenklassengruppe* von R.

Die Divisorenklassengruppe wird häufig auch als *Idealklassengruppe* oder einfach als *Klassengruppe* bezeichnet. Sie ist kommutativ und wird additiv geschrieben. Ihre Elemente sind Äquivalenzklassen und werden durch Divisoren repräsentiert, wobei zwei Divisoren genau dann die gleiche Klasse repräsentieren, wenn ihre Differenz ein Hauptdivisor ist. Sie heißen *Divisorklassen* oder *Idealklassen*. Wegen Satz 13.16 kann man die Divisorenklasse auch als die Restklassengruppe zur Gruppe der gebrochenen Ideale modulo der Untergruppe der gebrochenen Hauptideale erhalten. Ein späteres Hauptresultat, das aber einige Vorbereitungen braucht, wird sein, dass die Klassengruppe von Zahlbereichen endlich ist, siehe Satz 26.6. Sie ist eine wesentliche (ko)-homologische Invariante eines Zahlbereichs und enthält wesentliche Informationen über diesen. Generell lässt sich sagen, dass ihre Größe zum Ausdruck bringt, wie weit ein Zahlbereich von der Faktorialität entfernt ist. Der nächste Satz charakterisiert die Faktorialität dadurch, dass die Klassengruppe trivial ist.

Satz 14.2. *Es sei R ein Dedekindbereich und es bezeichne $\operatorname{KG}(R)$ die Divisorenklassengruppe von R. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein Hauptidealbereich.*
(2) *R ist faktoriell.*
(3) *Es ist $\operatorname{KG}(R) = 0$.*

Beweis. Die Implikation (1) $\Rightarrow$ (2) folgt aus Satz 2.19.

(2) $\Rightarrow$ (3). Sei also R faktoriell, und sei $\mathfrak{p}$ ein Primideal $\neq 0$. Sei $f \in \mathfrak{p}$, $f \neq 0$, mit Primfaktorzerlegung $f = p_1 \cdots p_s$. Da $\mathfrak{p}$ ein Primideal ist, muss einer der Primfaktoren zu $\mathfrak{p}$ gehören, sagen wir $p = p_1 \in \mathfrak{p}$. Dann ist $(p) \subseteq \mathfrak{p}$. Das von p erzeugte Ideal ist ein Primideal, und in einem Dedekindbereich ist nach Definition jedes von 0 verschiedene Primideal maximal, so dass hier $(p) = \mathfrak{p}$ gelten muss. Auf der Seite der Divisoren gilt aufgrund von Satz 11.13 $\operatorname{div}(p) = 1\mathfrak{p}$, so dass ein Hauptdivisor vorliegt. Also sind alle Erzeuger der Divisorengruppe Hauptdivisoren und somit ist überhaupt

$$\operatorname{Div}(R) = H$$

und die Divisorenklassengruppe ist trivial.

(3) $\Rightarrow$ (1). Sei nun $\operatorname{KG}(R) = 0$ vorausgesetzt. Wir zeigen zunächst, dass jedes Primideal $\mathfrak{p} \neq 0$ ein Hauptideal ist. Nach Voraussetzung ist der Divisor $\mathfrak{p}$ ein Hauptdivisor, so dass $\mathfrak{p} = \operatorname{div}(p)$ mit einem $p \in R$ gilt. Aufgrund von Satz 11.13 entspricht dies auf der Idealseite der Gleichung $\mathfrak{p} = (p)$, so dass

jedes Primideal ein Hauptideal ist. Für ein beliebiges Ideal $\mathfrak{a} \subseteq R$, $\mathfrak{a} \neq 0$, ist nach Satz 12.2

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Dies bedeutet aber, mit $\mathfrak{p}_i = (p_i)$, dass $\mathfrak{a}$ ein Hauptideal ist, das von $p_1^{r_1} \cdots p_k^{r_k}$ erzeugt wird. Also liegt ein Hauptidealbereich vor. □

Insofern ist die erste wichtige Frage bei einem Dedekindbereich, ob seine Klassengruppe gleich 0 ist oder nicht.

Beispiel 14.3. Wir behaupten, dass im quadratischen Zahlbereich $R = \mathbb{Z}[\sqrt{-5}]$ das Ideal

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

kein Hauptideal ist, was in Beispiel 10.7 gezeigt wurde, aber die Eigenschaft besitzt, dass das Quadrat davon ein Hauptideal ist. Insbesondere definiert die zugehörige Idealklasse ein von 0 verschiedenes Element in der Divsorenklassengruppe mit der Eigenschaft, dass das Doppelte davon trivial ist. Es ist

$$\mathfrak{p}^2 = (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) = (2).$$

Dabei ist die Inklusion $\subseteq$ klar und die umgekehrte Inklusion $\supseteq$ ergibt sich aus

$$-4 + (2 + 2\sqrt{-5}) - (-4 + 2\sqrt{-5}) = 2.$$

Wir betrachten nun das Ideal

$$\mathfrak{q} = (7, 3 + \sqrt{-5}).$$

Der Restklassenring ist

$$\mathbb{Z}/(7)[X]/(X^2 + 5, 3 + X) \cong \mathbb{Z}/(7),$$

so dass ein Primideal mit der Norm 7 vorliegt, das kein Hauptideal ist, da es kein Element mit Norm 7 gibt. Die beiden Ideale $\mathfrak{p}$ und $\mathfrak{q}$ definieren die gleiche Idealklasse. Dazu betrachten wir die Multiplikation

$$Q(R) \longrightarrow Q(R),\ h \longmapsto h\frac{3 + \sqrt{-5}}{2}.$$

Wegen

$$2 \cdot \frac{3 + \sqrt{-5}}{2} = 3 + \sqrt{-5} \in \mathfrak{q}$$

und

$$(1+\sqrt{-5}) \cdot \frac{3 + \sqrt{-5}}{2} = \frac{-2 + 4\sqrt{-5}}{2} = -1+2\sqrt{-5} = -7+2(3+\sqrt{-5}) \in \mathfrak{q}$$

induziert dies einen injektiven R-Modulhomomorphismus

$$\mathfrak{p} \longrightarrow \mathfrak{q},$$

der wegen

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

auch surjektiv ist. Somit ist

$$\mathfrak{p} \cdot (\frac{3+\sqrt{-5}}{2}) = \mathfrak{q}.$$

In Beispiel 24.11 wird darüber hinaus gezeigt, dass die Klassengruppe von R gleich $\mathbb{Z}/(2)$ ist.

14.2. **Die Divisorenklassengruppe unter Homomorphismen.**

Ein wichtiger Aspekt von homologischen Invarianten ist, dass sie nicht nur den Objekten Gruppen zuordnen, sondern auch den richtigen Abbildungen zwischen den Objekten Gruppenhomomorphismen. Wir besprechen zuerst den Fall einer Nenneraufnahme $R \to R_S$ zu einem multiplikativen System $S \subseteq R$ in einem Dedekindbereich. Nach Proposition 5.4 (2) entsprechen die Primideale von R_S den Primidealen von R, die mit S einen leeren Schnitt haben. Bei gegebenem S kann man also die Primideale von R dahingehend aufteilen, ob sie einen leeren oder einen nichtleeren Durchschnitt mit S haben.

Lemma 14.4. *Es sei R ein Dedekindbereich und es sei $S \subseteq R$, $0 \notin S$, ein multiplikatives System mit der Nenneraufnahme R_S. Dann liegt eine exakter Komplex*

$$1 \longrightarrow R^\times \longrightarrow R_S^\times \longrightarrow \mathbb{Z}^{(\{\mathfrak{p}|\mathfrak{p}\cap S\neq\emptyset\})} \longrightarrow \mathrm{KG}\,(R) \longrightarrow \mathrm{KG}\,(R_S) \longrightarrow 0$$

vor. Dabei ordnet die dritte Abbildung einer Einheit $f \in R_S^\times$ die Einschränkung des Hauptdivisors auf die angegebene Primidealmenge zu. Die vierte Abbildung ordnet einen Divisor $\sum_{\mathfrak{p}\cap S\neq\emptyset} n_\mathfrak{p}\mathfrak{p}$ auf die zugehörige Klasse in $\mathrm{KG}\,(R)$ *zu.*

Beweis. Die Injektivität links ist klar. Die Einheiten aus R haben überhaupt an jedem Primideal die Ordnung 0, deshalb ist an der nächsten Stelle die Zusammensetzung die triviale Abbildung. Sei $f \in R_S^\times$ derart, dass es unter der folgenden Abbildung auf 0 geht. Das bedeutet, das es an allen Primidealen, die nicht zu R_S gehören, die Ordnung 0 besitzt. Da es eine Einheit in R_S ist, hat es auch an allen Primidealen, die zu R_S gehören, und damit überhaupt an jedem Primideal von R die Ordnung 0 und ist somit eine Einheit in R.

Die dritte Abbildung ist einfach die Hauptdivisorabbildung, da in den Primidealen, die zu S disjunkt sind, die Ordnung einer Einheit aus R_S stets 0 ist und sich der relevante Teil des Hauptdivisors in den angegebenen Primidealen abspielt. Die zusammengesetzte Abbildung ist daher die Nullabbildung, da in der Klassengruppe die Hauptdivisoren zu 0 gemacht werden. Wenn ein Divisor $\sum_{\mathfrak{p}\cap S\neq\emptyset} n_\mathfrak{p}\mathfrak{p}$ in der Klassengruppe von R zu 0 wird, so bedeutet dies die Existenz eines $f \in Q(R) \setminus \{0\}$ mit

$$\mathrm{div}\,(f) = \sum_{\mathfrak{p}\cap S\neq\emptyset} n_\mathfrak{p}\mathfrak{p}.$$

Dabei sind dann insbesondere die Ordnungen von f an den Primidealen, die mit S einen leeren Durchschnitt haben, gleich 0, und dann gehört f zu R_S und ist dort eine Einheit.

Ein Divisor mit der angegebenen Trägermenge wird in der Klassengruppe von R_S zu 0, da diese Primideale in der Nenneraufnahme nicht überleben. Es sei $[D] \in \mathrm{KG}(R)$ eine Divisorklasse, repräsentiert durch $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$, die in der Divisorenklassengruppe von R_S zu 0 wird. Wir schreiben $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p} = \sum_{\mathfrak{p} \cap S \neq \emptyset} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\mathfrak{p} \cap S = \emptyset} n_{\mathfrak{p}} \mathfrak{p} = D_1 + D_2$. Unter der Abbildung wird dies nach $[D_2]$ abgebildet. Aus

$$D_2 = \mathrm{div}(f)$$

in der Divisorengruppe zu R_S folgt, dass die Differenz zwischen D und $\mathrm{div}(f)$ in der Divisorengruppe zu R mit Primidealen geschrieben werden kann, die zu S einen nichtleeren Durchschnitt haben. Diese Differenz kommt also von rechts. Die Surjektivität an der letzten Stelle ist klar. □

Die Abbildung $\mathrm{KG}(R) \to \mathrm{KG}(R_S)$ fügt sich in das kommutative Diagramm

$$\begin{array}{ccc} \mathrm{Div}(R) & \longrightarrow & \mathrm{Div}(R_S) \\ \downarrow & & \downarrow \\ \mathrm{KG}(R) & \longrightarrow & \mathrm{KG}(R_S) \end{array}$$

ein, wobei die obere horizontale Abbildung einen Divisor $\sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$ von R einfach auf denjenigen Divisor von R_S abbildet, bei dem die Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap S \neq \emptyset$ ignoriert („vergessen“) werden. Dies entspricht der Abbildung, bei der ein gebrochenes Ideal $\mathfrak{f}$ auf das Erweiterungsideal $\mathfrak{f}R_S$ abgebildet wird.

Lemma 14.5. *Zu einer Erweiterung von Dedekindbereichen $R \subseteq S$ gehört in funktorieller Weise ein Gruppenhomomorphismus*

$$\mathrm{KG}(R) \longrightarrow \mathrm{KG}(S),\ [\mathfrak{a}] \longmapsto [\mathfrak{a}S].$$

Beweis. Wir gehen von der Zuordnung aus, die jedem von 0 verschiedenen Ideal $\mathfrak{a}$ von R das Erweiterungsideal $\mathfrak{a}S$ zuordnet, das ebenfalls von 0 verschieden ist. Diese Zuordnung ist mit dem Produkt von Idealen verträglich. Deshalb liegt ein Monoidhomomorphismus vor. Ein gebrochenes Ideal kann man nach Aufgabe 13.29 in der Form $\mathfrak{a}\mathfrak{b}^{-1}$ mit Idealen $\mathfrak{a}, \mathfrak{b}$ schreiben und diesem das gebrochene Ideal $\mathfrak{a}S(\mathfrak{b}S)^{-1}$ zuordnen. Dies ist wohldefiniert und so erhält man einen Gruppenhomomorphismus von der Gruppe der gebrochenen Ideale $\neq 0$ von R in die Gruppe der gebrochenen Ideale $\neq 0$ von S. Das Erweiterungsideal eines Hauptideals ist wieder ein Hauptideal, und deshalb werden gebrochene Hauptideale auf gebrochene Hauptideale abgebildet. Der Satz vom induzierten Homomorphismus ergibt somit einen Gruppenhomomorphismus

$$\mathrm{KG}(R) \longrightarrow \mathrm{KG}(S).$$

□

Insgesamt liegt das kommutative Diagramm

$$\begin{array}{ccccc} \text{Gebrochene Hauptideale}\,(R) & \longrightarrow & \text{Gebrochene Ideale}\,(R) & \longrightarrow & \mathrm{KG}\,(R) \\ \downarrow & & \downarrow & & \downarrow \\ \text{Gebrochene Hauptideale}\,(S) & \longrightarrow & \text{Gebrochene Ideale}\,(S) & \longrightarrow & \mathrm{KG}\,(S) \end{array}$$

vor. Auf der Divisorebene wird dabei einem Primdivisor $\mathfrak{p}$ der Divisor zum Ideal $\mathfrak{p}S$ zugeordnet. Das Erweiterungsideal zu $\mathfrak{p}$ beschreibt dabei die Faser der Spektrumsabbildung $\operatorname{Spek}(S) \to \operatorname{Spek}(R)$ über $\mathfrak{p}$. Dies ist insbesondere bei endlichen Erweiterungen von Dedekindbereichen relevant. Man kann sich fragen, ob die Abbildung zwischen den Klassengruppen stets injektiv ist, oder ob umgekehrt ein nichttriviales Ideal zu einem Hauptideal werden kann. Dies ist in der Tat der Fall.

Beispiel 14.6. Wir betrachten im quadratischen Zahlbereich R zu $D = -5$ das Ideal $\mathfrak{p} = (2, 1+\sqrt{-5})$, das nach Beispiel 10.7 kein Hauptideal ist. Es sei S der ganze Abschluss von R (oder von $\mathbb{Z}$) im Erweiterungskörper $L = \mathbb{Q}[\sqrt{-5}, \sqrt{2}]$ vom Grad vier über $\mathbb{Q}$. Wir haben also eine Kette

$$\mathbb{Z} \subset R \subset S$$

von Zahlbereichen. Wir behaupten, dass das Erweiterungsideal

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

ein Hauptideal in S ist, und zwar behaupten wir, dass $\sqrt{2}$ ein Idealerzeuger davon ist. Dazu betrachten wir zunächst das rationale Element $z = \frac{\sqrt{2}+\sqrt{2}\cdot\sqrt{-5}}{2} = \frac{1+\sqrt{-5}}{\sqrt{2}} \in L$. Wegen

$$z^2 = \left(\frac{\sqrt{2}+\sqrt{2}\cdot\sqrt{-5}}{2}\right)^2 = \frac{2-2\cdot 5+4\sqrt{-5}}{4} = -2+\sqrt{-5} \in R$$

erfüllt z eine Ganzheitsgleichung über R und gehört somit zu S (ebenso, wenn im Zähler ein Minuszeichen steht). Die Gleichheit

$$\mathfrak{p}S = (\sqrt{2})$$

folgt einerseits aus

$$2 = \sqrt{2}\cdot\sqrt{2}$$

und

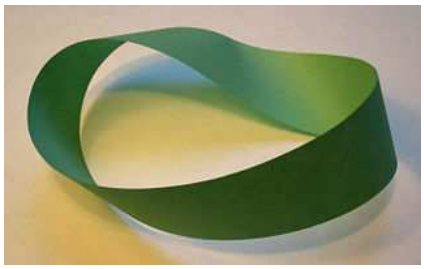
$$1+\sqrt{-5} = z\cdot\sqrt{2}$$

und andererseits aus

$$\begin{aligned} -\sqrt{2}\cdot 2 + \frac{1-\sqrt{-5}}{\sqrt{2}}(1+\sqrt{-5}) &= -\sqrt{2}\cdot 2 + \frac{6}{\sqrt{2}} \\ &= -\sqrt{2}\cdot 2 + 3\cdot\sqrt{2} \\ &= \sqrt{2}(-2+3) \\ &= \sqrt{2}. \end{aligned}$$

Es gilt sogar, dass man im zahlentheoretischen Kontext jede Klasse trivialisieren kann. Dies bedeutet aber nicht, dass es zu jedem Zahlbereich eine faktorielle Erweiterung gibt, da durch die Trivialisierung typischerweise „an anderer Stelle“ nichttriviale Klassen auftreten.

Beispiel 14.7. Wir betrachten den kommutativen Ring $R = \mathbb{R}[X,Y]/(X^2+Y^2-1)$, der dem Einheitskreis in dem Sinne entspricht, dass die Primideale der Form $(X-a,Y-b)$ darin den reellen Punkten des Kreis entsprechen. Dies ist ein Dedekindbereich, wobei die Normalität aus der Glattheit des Kreises folgt.



Das *Möbiusband*.

Das Ideal $\mathfrak{p} = (X, Y-1)$ ist ein Primideal darin, das kein Hauptideal ist. Für das Produkt dieses Ideals mit sich selbst haben wir

$$(X,Y-1)^2 = (X^2, XY-X, (Y-1)^2) = (Y-1),$$

wobei die Inklusion $\subseteq$ klar ist und sich die andere Inklusion aus

$$\begin{aligned} \frac{1}{2}\big(-X^2-(Y-1)^2\big) &= \frac{1}{2}\big(-1+Y^2-(Y-1)^2\big) \\ &= Y-1 \end{aligned}$$

ergibt. Da $Y-1$ in R keine Quadratwurzel (und auch nicht multipliziert mit einer Einheit) besitzt, ist $\mathfrak{p}$ kein Hauptideal. Dieses Ideal ist eine algebraische Realisierung des Möbiusbandes (ein Ideal definiert eine invertierbare Garbe und ein Geradenbündel; das Möbiusband ist das nichttriviale Geradenbündel auf dem Einheitskreis).

Wir betrachten den Ringhomomorphismus

$$\begin{aligned} R = \mathbb{R}[X,Y]/(X^2+Y^2-1) \longrightarrow S = \mathbb{R}[U,V]/(U^2+V^2-1), \\ (X,Y) \longmapsto (U^2-V^2, 2UV), \end{aligned}$$

des Ringes in sich (wir schreiben rechts S, um die unterschiedlichen Rollen zu betonen). Wegen

$$\begin{aligned} X^2+Y^2 &= (U^2-V^2)^2+(2UV)^2 \\ &= U^4-2U^2V^2+V^4+4U^2V^2 \\ &= U^4+2U^2V^2+V^4 \\ &= (U^2+V^2)^2 = 1 \end{aligned}$$

ist dies wohldefiniert (es handelt sich um die komplexe Quadrierung eingeschränkt auf den Einheitskreis). Es handelt sich um eine ganze Ringerweiterung. Das Erweiterungsideal zu $(X, Y-1)$ ist

$$(U^2-V^2, 2UV-1) = (1-2V^2, 2UV-1) = (U-V),$$

also ein Hauptideal. Dies beruht auf

$$U^2-V^2 = (U+V)(U-V),$$
$$2UV-1 = 2UV-U^2-V^2 = (V-U)(U-V)$$

und

$$U-V = V\big(U^2-V^2\big) - U(2UV-1).$$

14. Arbeitsblatt

14.1. **Aufgaben.**

Aufgabe 14.1. Es sei A_D ein quadratischer Zahlbereich und sei $\mathfrak{a}$ ein Ideal $\neq 0$ in A_D. Zeige, dass das konjugierte Ideal $\overline{\mathfrak{a}}$ in der Klassengruppe das Inverse zu $\mathfrak{a}$ ist.

Aufgabe 14.2. Es sei R ein Dedekindbereich und es seien $\mathfrak{f}$ und $\mathfrak{g}$ gebrochene Ideale. Zeige, dass die beiden gebrochenen Ideale genau dann die gleiche Klasse in der Divisorenklassengruppe definieren, wenn sie als R-Moduln isomorph sind.

Aufgabe 14.3. Es sei R ein Dedekindbereich. Zeige, dass ein exakter Komplex

$$1 \longrightarrow R^\times \longrightarrow Q(R)^\times \longrightarrow \operatorname{Div}(R) \longrightarrow \operatorname{KG}(R) \longrightarrow 0$$

vorliegt.

Aufgabe 14.4. Interpretiere Lemma 14.4 für die folgenden Fälle:

(1) S wird durch ein Element erzeugt.
(2) $S = R \setminus \{0\}$
(3) R_S ist faktoriell.
(4) $S = R \setminus \mathfrak{p}$.

Aufgabe 14.5. Es sei R ein Zahlbereich vom Grad d. Zeige, dass die Norm einen natürlichen Gruppenhomomorphismus

$$N\colon \operatorname{KG}(R) \longrightarrow \mathbb{Q}_+^\times/T$$

definiert, wobei T die Menge der Beträge von Normen von Elementen $\neq 0$ aus R bezeichnet. Zeige ferner, dass $\left(\mathbb{Q}_+^\times\right)^d \subseteq T$ gilt.

Aufgabe 14.6.*

Es sei S der ganze Abschluss von $\mathbb{Z}$ in der Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-5}, \sqrt{2}].$$

(1) Zeige, dass $z = \frac{\sqrt{2}+\sqrt{-10}}{2}$ zu S gehört.
(2) Zeige $\sqrt{-5} \in \mathbb{Z}[z]$.
(3) Zeige $\sqrt{2} \notin \mathbb{Z}[z]$.
(4) Bestimme eine Ganzheitsgleichung für z über $\mathbb{Z}[\sqrt{-5}]$.
(5) Bestimme eine Ganzheitsgleichung für z über $\mathbb{Z}$.

Aufgabe 14.7.*

Wir betrachten die Ringerweiterungen

$$\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{-5}] = R \subseteq \mathbb{Z}[\sqrt{-5}, \mathrm{i}] \subseteq T,$$

wobei T den ganzen Abschluss von $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{-5}, \mathrm{i}]$ bezeichnet. Zeige, dass das Erweiterungsideal zu

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

in T ein Hauptideal wird.

Aufgabe 14.8. Erkläre „geometrisch“, warum die Primideale der Form $(X - a, Y - b)$ des Ringes $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ keine Hauptideale sind.

Aufgabe 14.9. Es sei $R = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$. Zeige, dass alle Primideale von R der Form $(X - a, Y - b)$ mit $a, b \in \mathbb{R}$ die gleiche Divisorklasse festlegen.

Aufgabe 14.10. Zeige, dass der Ringhomomorphismus

$$K[X, Y]/(X^2+Y^2-1) \longrightarrow K[U, V]/(U^2+V^2-1),\ (X, Y) \longmapsto (U^2-V^2, 2UV),$$

über jedem Körper der Charakteristik $\neq 2$ ganz ist.

Aufgabe 14.11. Wir betrachten den kommutativen Ring

$$R = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$$

und das Ideal $\mathfrak{p} = (X, Y - 1)$ aus Beispiel 14.7. Zeige, dass der Ring $R_{\mathbb{C}} = \mathbb{C}[X, Y]/(X^2+Y^2-1)$ ein Hauptidealbereich ist und bestimme einen Erzeuger für das Erweiterungsideal $(X, Y - 1)R_{\mathbb{C}}$.

15. Vorlesung - Normalitätskriterien

15.1. **Normalitätskriterien.**

Es ist im Allgemeinen schwierig, den ganzen Abschluss von $\mathbb{Z}$, also den Zahlbereich, in einer endlichen Körpererweiterung $\mathbb{Q} \subseteq L$ zu bestimmen bzw. eine vorliegende Ringerweiterung

$$\mathbb{Z} \subseteq S = \mathbb{Z}[X_1, \ldots, X_m]/(F_1, \ldots, F_n) \subseteq L$$

als normal nachzuweisen. Es handelt es sich aber um ein lokales Problem, d.h. S ist genau dann normal, wenn $S_{\mathfrak{p}}$ für jedes Primideal $\mathfrak{p}$ normal ist, und dies ist genau dann der Fall, wenn für jede Primzahl p die Nenneraufnahme $S_{\mathbb{Z}\setminus\mathbb{Z}p}$ normal ist, siehe Aufgabe 6.16 und Aufgabe 15.1. Dies erlaubt den Übergang zu einem diskreten Bewertungsring als Basisring ($\mathbb{Z}_{(p)}$ statt $\mathbb{Z}$), was oft die Gleichungsbeschreibung vereinfacht und was es erlaubt, Eigenschaften der Faserringe S/pS besser zu verarbeiten. Das typische Verhalten ist, dass sich die Ringe $S_{\mathbb{Z}\setminus\mathbb{Z}p}$ bis auf endliche viele Primzahlen direkt als normal erweisen, und dass man einen Teil der verbleibenden Ringe über Eigenschaften der Faser erledigen kann, einen anderen Teil aber auch nicht.

Lemma 15.1. *Es sei B ein diskreter Bewertungsring mit Ortsuniformisierender p und sei $F \in B[X]$ ein normiertes irreduzibles Polynom. Sei $R = B[X]/(F)$. In der Zerlegung von F in $B/(p)[X]$ in irreduzible Faktoren, $F = F_1 \cdots F_s$, seien alle Faktoren einfach. Dann ist R der ganze Abschluss von B in $Q(B)[X]/(F)$ und insbesondere normal.*

Beweis. Wir können direkt annehmen, dass die F_i zu $B[X]$ gehören. Die maximalen Ideale von R sind (p, F_j) für $j = 1, \ldots, s$. Die Voraussetzung bedeutet für $B[X]$ die Beziehung $F_1 \cdots F_s = F + pH$ und für

$$R = B[X]/(F)$$

die Gleichheit

$$F_1 \cdots F_s = pH.$$

Da F_i und F_j teilerfremd sind, sind die F_i Einheiten in der Lokalisierung $R_{(p,F_j)}$ und daher ist

$$F_j = \frac{H}{F_1 \cdots F_{j-1} F_{j+1} \cdots F_s} \cdot p.$$

D.h. in $R_{(p,F_j)}$ ist das maximale Ideal ein Hauptideal mit dem Erzeuger p und daher liegt nach Satz 10.17 ein diskreter Bewertungsring vor. Somit ist R normal. □

Die Beispielklasse $\mathbb{Z}_{(2)}[X]/(X^2 - D)$, wo der Faserring immer einen mehrfachen Faktor besitzt, zeigt, dass Lemma 15.1 keine notwendige Voraussetzung für die Normalität ist. Die Bedingung, dass in der Primfaktorzerlegung von

F in $B/(p)[X]$ jeder Faktor einfach ist, kann man auch so formulieren, dass der Faserring

$$R/(p) \;=\; B[X]/(F,p) \;=\; B/(p)[X]/(F)$$

reduziert ist. Bei $F = F_1^{r_1} \cdots F_s^{r_s}$ in $B/(p)[X]$ gilt ja generell nach Satz 12.11 die Beziehung

$$B/(p)[X]/(F) \;=\; B/(p)[X]/(F_1^{r_1}) \times \cdots \times B/(p)[X]/(F_s^{r_s}),$$

und dies ist genau dann reduziert, wenn jeder Komponentenring reduziert ist, und dies ist genau dann der Fall, wenn jeder Komponentenring ein Körper ist, also genau bei $r_j = 1$ für alle j. Im Allgemeinen, wenn beispielsweise der Ring durch mehrere Variablen und Gleichungen beschrieben wird, ist die Beschreibung mit reduziert wichtiger, bei nur einer Gleichung lässt sich aber die Bedingung in Lemma 15.1 einfacher überprüfen.

Korollar 15.2. *Es sei B ein diskreter Bewertungsring mit Ortsuniformisierender p und sei $F \in B[X]$ ein normiertes irreduzibles Polynom. Es seien F und F' in $B/(p)[X]$ teilerfremd. Dann ist $R = B[X]/(F)$ normal und gleich dem ganzen Abschluss von B in $Q(B)[X]/(F)$.*

Beweis. Dies folgt aus Lemma 15.1 in Verbindung mit einer Variante von Aufgabe 7.35. □

Korollar 15.3. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes irreduzibles Polynom, $R = \mathbb{Z}[X]/(F)$. Dann ist bis auf endlich viele Primzahlen p der Ring*

$$R_{\mathbb{Z}\setminus(p)} \;=\; \mathbb{Z}_{(p)}[X]/(F)$$

normal.

Beweis. Wir betrachten F als irreduzibles Polynom in $\mathbb{Q}[X]$. In Charakteristik 0 sind F irreduzibel und F' teilerfremd. Deshalb gibt es Polynome $A, B \in \mathbb{Q}[X]$ mit $AF + BF' = 1$. Es sei $m \in \mathbb{Z}$ ein Hauptnenner der Koeffizienten von A und B. Dann gibt es Polynome $C, D \in \mathbb{Z}[X]$ mit $CF + DF' = m$. Für jede Primzahl p, die kein Teiler von m ist, gilt entsprechend $CF + DF' = m$ in $\mathbb{Z}/(p)[X]$ und m ist dort eine Einheit. Deshalb sind F, F' in $\mathbb{Z}/(p)[X]$ teilerfremd und die Normalität von $\mathbb{Z}_{(p)}[X]/(F)$ folgt aus Korollar 15.2. □

Beispiel 15.4. Wir betrachten das kubische Polynom $X^3 - 3X + 1 \in \mathbb{Q}[X]$, das nach Aufgabe 2.25 irreduzibel ist, und $R = \mathbb{Z}[X]/(X^3 - 3X + 1)$. Die Ableitung des Polynoms ist $3X^2 - 3$, und in $\mathbb{Z}[X]$ gilt die Gleichung

$$(6X + 3)(X^3 - 3X + 1) + (-2X^2 - X + 4)(3X^2 - 3) \;=\; -9.$$

Nach dem Beweis zu Korollar 15.3 ist daher $\mathbb{Z}_{(p)}[X]/(X^3 - 3X + 1)$ für jede Primzahl $p \neq 3$ normal. Über $p = 3$ ist der Faserring gleich

$$\mathbb{Z}/(3)[X]/(X^3 - 3X + 1) \;=\; \mathbb{Z}/(3)[X]/(X^3 + 1) \;=\; \mathbb{Z}/(3)[X]/(X + 1)^3.$$

Dies bedeutet, dass das einzige maximale Ideal in $\mathbb{Z}_{(3)}[X]/(X^3-3X+1)$ gleich $(3,X+1)$ ist. Wegen

$$\mathbb{Z}_{(3)}[X]/(X^3-3X+1,X+1) = \mathbb{Z}_{(3)}/((-1)^3-3(-1)+1) = \mathbb{Z}/(3)$$

ist aber $X+1$ ein Erzeuger von diesem maximalen Ideal und daher ist R überhaupt normal.

Lemma 15.5. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes irreduzibles Polynom, $R = \mathbb{Z}[X]/(F)$ und sei p eine Primzahl derart, dass in $\mathbb{Z}/(p)[X]$ die Zerlegung*

$$F = F_1^{r_1} \cdots F_s^{r_s}$$

mit irreduziblen Polynomen F_j gelte. Dann gilt in R die Gleichheit

$$pR = (p,F_1^{r_1}) \cdots (p,F_s^{r_s}).$$

Beweis. In $\mathbb{Z}/(p)[X]$ sind die F_j zueinander paarweise teilerfremd. Wir behaupten, dass in $\mathbb{Z}[X]/(F)$ die Gleichheit

$$(p) = (p,F_1^{r_1}) \cap \ldots \cap (p,F_s^{r_s}) = (p,F_1^{r_1}) \cdots (p,F_s^{r_s})$$

gilt, wobei die letzte Gleichheit auf Lemma 12.6 beruht. Zum Nachweis der linken Gleichheit sei

$$a = a_1p + b_1F_1^{r_1} = \ldots = a_sp + b_sF_s^{r_s},$$

es ist $a \in (p)$ zu zeigen. Modulo p ist

$$a = b_1F_1^{r_1} = \ldots = b_sF_s^{r_s}$$

in $\mathbb{Z}/(p)[X]/(F)$. Nach Satz 12.11 ist

$$\mathbb{Z}/(p)[X]/(F) = \mathbb{Z}/(p)[X]/(F_1^{r_1}) \times \cdots \times \mathbb{Z}/(p)[X]/(F_s^{r_s}).$$

Die Voraussetzung bedeutet, dass a in jeder Komponente 0 ist, also insgesamt gleich 0 ist. □

Korollar 15.6. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes irreduzibles Polynom, $R = \mathbb{Z}[X]/(F)$ und sei p eine Primzahl derart, dass der Faserring $\mathbb{Z}/(p)[X]/(F)$ reduziert ist. Dann ist pR das Produkt von Primidealen.*

Beweis. Dies folgt aus Lemma 15.5, da im reduzierten Fall die Exponenten $r_j = 1$ sind, und dann (p,F_j) Primideale sind, oder aus Lemma 15.1 in Verbindung mit Satz 12.2. □

Ohne die Voraussetzung reduziert ist die Aussage nicht richtig, siehe Beispiel 12.9.

Wir behandeln noch den Fall, wo die Algebra durch mehrere Variablen erzeugt wird. Dies ergibt auch einen weiteren Beweis für Lemma 15.1.

Lemma 15.7. *Es sei B ein diskreter Bewertungsring mit Ortsuniformisierender p und es sei $R = B[X_1,\ldots,X_n]/\mathfrak{a}$. eine endliche integre B-Algebra. Der Faserring R/pR sei reduziert. Dann ist R normal.*

Beweis. Es sei $\mathfrak{p}$ ein maximales Ideal von R. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccccc} B & \longrightarrow & R & \longrightarrow & R_{\mathfrak{p}} \\ \downarrow & & \downarrow & & \downarrow \\ B/(p) & \longrightarrow & R/pR & \longrightarrow & (R/pR)_{\mathfrak{p}} \cong R_{\mathfrak{p}}/pR_{\mathfrak{p}} \ . \end{array}$$

Als Lokalisierung eines nach Voraussetzung reduzierten Ringes ist der Ring rechts unten reduziert, also hier sogar ein Körper. Dies heißt aber, dass

$$(p)R_{\mathfrak{p}} \ = \ \mathfrak{p}R_{\mathfrak{p}}$$

gilt und das bedeutet, dass $R_{\mathfrak{p}}$ ein diskreter Bewertungsring ist. □

15.2. **Monogene Algebren.**

Definition 15.8. Eine R-Algebra A über einem kommutativen Ring R heißt *monogen*, wenn sie als $A = R[X]/\mathfrak{a}$ mit einem Ideal $\mathfrak{a} \subseteq R[X]$ geschrieben werden kann.

Nach dem Satz vom primitiven Element ist eine endliche separable Körpererweiterung $K \subseteq L$ stets monogen, was man auf jede endliche Körpererweiterung $\mathbb{Q} \subseteq L$ anwenden kann. Ferner ist nach Satz 9.8 jeder quadratische Zahlbereich monogen über $\mathbb{Z}$. Ein Zahlbereich ist genau dann monogen, wenn es ein Element mit der Eigenschaft gibt, dass seine Potenzen eine Ganzheitsbasis bilden.

Lemma 15.9. *Es sei $(B, \mathfrak{p}) \subseteq (S, \mathfrak{q})$ eine endliche Erweiterung von diskreten Bewertungsringen. Es sei $h \in S$ eine Ortsuniformisierende derart, dass*

$$\kappa(\mathfrak{p})[\overline{h}] \ = \ \kappa(\mathfrak{q})$$

gilt. Dann ist $S = B[h]$.

Beweis. Wir betrachten die endliche Erweiterung

$$R \ = \ B[h] \ \subseteq \ S,$$

die als identisch nachzuweisen ist. Es ist $\mathfrak{m} = B[h] \cap \mathfrak{q}$ das maximale Ideal von $B[h]$, der ebenfalls ein lokaler Ring ist, und es ist $\mathfrak{m}S = hS = \mathfrak{q}$. Ferner ist

$$B[h] + hS \ = \ S.$$

Für $f \in S$ gilt ja im Restekörper $\kappa(\mathfrak{q})$

$$\overline{f} \ = \ \overline{P}(\overline{h})$$

mit einem Polynom $\overline{P}$ über $\kappa(\mathfrak{p})$. In S gilt deshalb

$$f \ = \ P(h) + hg$$

mit $g \in S$. Nach dem Lemma von Nakayama gilt $R = S$. □

Beispiel 15.10. Wir betrachten die biquadratische Erweiterung

$$\mathbb{Z} \subseteq \mathbb{Z}[X,Y]/(X^2-7, Y^2-19).$$

Dieser Ganzheitsring lässt sich nicht in der Form $\mathbb{Z}[W]/(F)$ schreiben. Modulo (3) ist der Faserring gleich

$$\begin{aligned} \mathbb{Z}/(3)[X,Y]/(X^2-7, Y^2-19) &= \mathbb{Z}/(3)[X,Y]/(X^2-1, Y^2-1) \\ &= \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3), \end{aligned}$$

er besitzt also vier maximale Ideale, alle mit dem Restekörper $\mathbb{Z}/(3)$. Ein Ring der Form $\mathbb{Z}/(3)[W]/(F)$ kann aber nur drei maximale Ideale mit dem Restekörper $\mathbb{Z}/(3)$ besitzen, da es in $\mathbb{Z}/(3)$ nur drei Elemente gibt. Es folgt, dass der Ganzheitsring auch nicht über der Lokalisierung $\mathbb{Z}_{(3)}$ mit einem einzigen Algebraerzeuger beschrieben werden kann.

15. Arbeitsblatt

15.1. **Aufgaben.**

Aufgabe 15.1. Es sei B ein diskreter Bewertungsring, sei $u \in B^\times$ eine Einheit und sei $X^n - u$ irreduzibel in $B[X]$. Zeige, dass

$$R = B[X]/(X^n - u)$$

normal ist, falls n eine Einheit in B ist.

Aufgabe 15.2. Es sei B ein diskreter Bewertungsring, in dem 2 eine Einheit sei, und sei p eine Ortsuniformisierende von B. Bestimme, für welche m der Ring

$$R = B[X]/\left(X^2 - p^m\right)$$

ein normaler Integritätsbereich ist.

Aufgabe 15.3. Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und sei $S \subseteq L$ eine endliche Ringerweiterung von $\mathbb{Z}$. Zeige, dass S genau dann normal ist, wenn für jede Primzahl p die Nenneraufnahme $S_{\mathbb{Z}\setminus\mathbb{Z}p}$ normal ist.

Aufgabe 15.4. Bestimme für welche Primzahlen p das Polynom $X^2+3 \in \mathbb{Z}/(p)[X]$ irreduzibel ist bzw. in einfache Linearfaktoren zerfällt. Für welche Primzahlen ist $\mathbb{Z}_{(p)}[X]/(X^2-3)$ normal?

Aufgabe 15.5.*

(1) Zeige, dass das Polynom X^3+X+1 in $\mathbb{Z}[X]$ irreduzibel ist.
(2) Bestimme die Primfaktorzerlegung von X^3+X+1 in $\mathbb{Z}/(3)[X]$.
(3) Bestimme die Primfaktorzerlegung von X^3+X+1 in $\mathbb{Z}/(31)[X]$.

(4) Man finde eine positive Zahl n derart, dass für alle Primzahlen p, die n nicht teilen, der Faserring $\mathbb{Z}/(p)[X]/(X^3+X+1)$ reduziert ist.
(5) Bestimme, ob $\mathbb{Z}[X]/(X^3+X+1)$ ein Zahlbereich ist.

Aufgabe 15.6. Beweise Satz 9.8 mit Korollar 15.3 und einer Sonderbetrachtung für diejenigen Primzahlen, die dadurch nicht abgedeckt sind.

Es sei K ein Körper. Ein Polynom $P \in K[X]$ heißt *separabel*, wenn es über keinem Erweiterungskörper $K \subseteq L$ mehrfache Nullstellen besitzt.

Aufgabe 15.7.*

Es sei K ein Körper und sei $P \in K[X]$ ein Polynom. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) P ist separabel.
(2) Es gibt eine Körpererweiterung $K \subseteq L$ derart, dass P über L in einfache Linearfaktoren zerfällt.
(3) P und die Ableitung P' sind teilerfremd.
(4) P und die Ableitung P' erzeugen das Einheitsideal.

Aufgabe 15.8. Es sei K ein Körper und $P \in K[X]$ ein separables Polynom. Zeige, dass ein Teiler $F \in K[X]$ von P ebenfalls separabel ist.

Aufgabe 15.9. Es sei $F \in \mathbb{Z}[X]$ ein Polynom, das in $\mathbb{Q}[X]$ irreduzibel ist. Zeige, dass für alle Primzahlen p bis auf endlich viele Ausnahmen alle Primpolynome in der Primfaktorzerlegung von $F \in \mathbb{Z}/(p)[X]$ einfach sind.

Aufgabe 15.10. Es sei K ein Körper und

$$K[Y] \longrightarrow K[X] \cong K[Y][X]/(Y-X^n),\, Y \longmapsto X^n,$$

die n-te Potenzabbildung. Bestimme zu $b \in K$ den Faserring über $(Y-b)$. Wann sind alle Primfaktoren von X^n-b einfach?

Aufgabe 15.11. Es sei p eine Primzahl. Zeige, dass die Polynome $X^n-p \in \mathbb{Q}[X]$ für jedes $n \geq 1$ irreduzibel sind.

Aufgabe 15.12. Zeige, dass ein Polynom der Form $X^n-p^2 \in \mathbb{Q}[X]$ mit einer Primzahl p im Allgemeinen nicht irreduzibel ist.

Aufgabe 15.13. Es sei B ein diskreter Bewertungsring. Zu einem von 0 verschiedenen Polynom $P \in B[X]$ sei $\operatorname{ord}(P)$ die minimale Ordnung der Koeffizienten von P. Zeige

$$\operatorname{ord}(PQ) = \operatorname{ord}(P) + \operatorname{ord}(Q).$$

Aufgabe 15.14. Es sei R ein Dedekindbereich mit Quotientenkörper K und es sei $P \in R[X]$ ein Polynom mit teilerfremden Koeffizienten. Zeige

$$(P)R[X] = R[X] \cap (P)K[X].$$

Zeige ferner, dass die Voraussetzung über die Teilerfremdheit notwendig ist.

Aufgabe 15.15. Es sei R ein Integritätsbereich mit Quotientenkörper K und es sei $P \in R[X]$ ein Polynom mit teilerfremden Koeffizienten, das in $K[X]$ irreduzibel sei. Zeige, dass P auch in $R[X]$ irreduzibel ist.

Aufgabe 15.16. Es sei $P \in \mathbb{Z}[X]$ ein ganzzahliges normiertes Polynom, dass in $\mathbb{Q}[X]$ irreduzibel sei. Zeige, dass P auch in $\mathbb{Z}[X]$ irreduzibel ist.

Aufgabe 15.17. Es sei K ein Körper und A eine endlichdimensionale, reduzierte K-Algebra. Zeige, dass dann A ein endliches direktes Produkt von endlichen Körpererweiterungen von K ist.

16. Vorlesung - Kubische Zahlbereiche

16.1. **Reine kubische Gleichungen.**

Wir interessieren uns für den Ganzheitsring zur reinen kubischen Körpererweiterung $\mathbb{Q} \subseteq L = \mathbb{Q}[X]/(X^3 - q)$ mit $q \geq 2$. Wenn in der Primfaktorzerlegung von q eine Primzahl p mit einem Exponenten ≥ 3 vorkommt, so kann man p^3 vorziehen und erhält mit der neuen Variablen pX eine neue Darstellung der Körpererweiterung. Deshalb gehen wir direkt davon aus, dass in q nur Primzahlen mit einem Exponenten 1 oder 2 vorkommen. Wir können also $q = ab^2$ mit a und b quadratfrei und zueinander teilerfremd ansetzen.

Satz 16.1. *Es seien a und b teilerfremde quadratfreie natürliche Zahlen, nicht beide 1, und sei $\mathbb{Q} \subseteq \mathbb{Q}[X]/(X^3 - ab^2) = L$ die zugehörige kubische Körpererweiterung. Wir setzen $x = \sqrt[3]{ab^2}$ und $y = \sqrt[3]{a^2b}$. Dann gelten folgende Aussagen.*

(1) *x und y sind ganze Elemente in L.*
(2) *Es ist*

$$\begin{aligned} \mathbb{Z}[x,y] &\cong \mathbb{Z}[X,Y]/(XY - ab, X^2 - bY, Y^2 - aX) \\ &= \mathbb{Z}[X,Y]/(X^3 - ab^2, Y^3 - a^2b, XY - ab, X^2 - bY, Y^2 - aX) \\ &= S. \end{aligned}$$

(3) *Wenn* $a \neq \pm b \mod 9$ *gilt, so ist* S *der Ganzheitsring von* L*, und* $1, x, y$ *bilden eine Ganzheitsbasis.*
(4) *Bei* $a = \pm b \mod 9$ *gehört auch*

$$\begin{aligned} z &= \frac{1}{3}(1 + ax + by) \\ &= \frac{1}{3}\big(1 + ax + x^2\big) \end{aligned}$$

zum Ganzheitsring, und x, y, z *bilden eine Ganzheitsbasis.*

Beweis. Das Polynom besitzt $X^3 - ab^2$ keine rationale Nullstelle, ist also irreduzibel und somit liegt eine Körpererweiterung vom Grad 3 vor.

(1) Es ist unmittelbar klar, dass x zu L gehört und eine Ganzheitsgleichung erfüllt. Ferner ist

$$y = \sqrt[3]{a^2b} = \frac{1}{b}\sqrt[3]{ab^2}^2 = \frac{1}{b}x^2,$$

d.h. y gehört ebenfalls zu L, die Ganzheit ist klar.
(2) Wegen $X^3 = bYX = ab^2$ liegen auch diese kubischen Terme in dem Ideal. Wir haben durch $X \mapsto x$ und $Y \mapsto y$ einen surjektiven Ringhomomorpismus

$$S = \mathbb{Z}[X,Y]/(XY - ab, X^2 - bY, Y^2 - aX) \longrightarrow \mathbb{Z}[x,y],$$

da x und y die angegebenen Relationen erfüllen. Diese Relationen zeigen auch, dass rechts die Gruppe $\mathbb{Z} \oplus \mathbb{Z}x \oplus \mathbb{Z}y$ steht, da man alle Produkte darin schon ausdrücken kann. Eine weitere Relation kann es nicht geben, da $1, x, y$ über $\mathbb{Q}$ linear unabhängig sind.
(3) Wir zeigen nun, dass S unter der angegebenen Bedingung normal ist. Wenn eine Primzahl p weder in a noch in b vorkommt und nicht 3 ist, so ist

$$\begin{aligned} S_{\mathbb{Z}\setminus(p)} &= \mathbb{Z}_{(p)}[X,Y]/(XY - ab, X^2 - bY, Y^2 - aX) \\ &\cong \mathbb{Z}_{(p)}[X]/(X^3 - ab^2), \end{aligned}$$

da man $Y = \frac{X^2}{b}$ schreiben und überall ersetzen kann, da b in $\mathbb{Z}_{(p)}$ eine Einheit ist. Die entstehenden Erzeuger sind $X^3 - ab^2$ und Vielfache davon. Die Faser über p ist somit $\mathbb{Z}/(p)[X]/(X^3 - u)$ mit einer Einheit $u \in \mathbb{Z}/(p)$. Das beschreibende Polynom $X^3 - u$ und seine Ableitung $3X^2$ erzeugen das Einheitsideal (die Faser über p ist also reduziert) und damit ist nach Korollar 15.2 die Nenneraufnahme von S an $\mathbb{Z}\setminus(p)$ normal.

Sei nun p ein Teiler von a (wobei der Fall $p = 3$ erlaubt ist). Dann ist wieder $S_{\mathbb{Z}\setminus(p)} \cong \mathbb{Z}_{(p)}[X]/(X^3 - ab^2)$. Modulo p ist dies $\mathbb{Z}/(p)[X]/(X^3)$, somit ist das einzige Primideal oberhalb von (p) gleich (p, X). Da wir

$$a = p \cdot c$$

mit a und c teilerfremd schreiben können, gilt

$$p = \frac{X^2}{cb^2}X$$

und daher wird dieses Primideal von X erzeugt. Diese Nenneraufnahmen sind also auch normal.

Betrachten wir nun

$$p = 3$$

und nehmen weiter an, dass 3 weder in a noch in b vorkommt. Dann kann man wieder die Nenneraufnahme monogen als $\mathbb{Z}_{(3)}[X]/(X^3-ab^2)$ beschreiben. Modulo 3 ist dies

$$\mathbb{Z}/(3)[X]/(X^3 - ab^2) = \mathbb{Z}/(3)[X]/(X - ab^2)^3$$

und somit liegt über (3) das einzige Primideal $(3, X - ab^2)$. Wir bestimmen, unter welchen Bedingungen $X - ab^2$ ein Erzeuger dieses Ideals ist. Der Ring $\mathbb{Z}_{(3)}[X]/(X^3 - ab^2)$ modulo $X - ab^2$ ist

$$\begin{aligned} \mathbb{Z}_{(3)}/((ab^2)^3 - ab^2) &= \mathbb{Z}_{(3)}/((ab^2)^2 - 1) \\ &= \mathbb{Z}_{(3)}/((ab^2+1)(ab^2-1)), \end{aligned}$$

da in unserem Fall a und b Einheiten sind. Es geht darum, ob dieser Ring gleich $\mathbb{Z}/(3)$ ist oder nicht, und somit geht es darum, ob die Ordnung von $(ab^2+1)(ab^2-1)$ gleich 1 oder höher ist. Wir schreiben $a = 9u + r$ und $b = 9v + s$ und betrachten zuerst den Fall, wo $r = 1, 4, 7$ ist. Dann ist $ab^2+1 \neq 0 \mod 3$ und wir müssen $ab^2-1 = (9u+r)(9v+s)^2-1$ betrachten. Modulo 9 ist dies rs^2-1. Dabei gilt

$$rs^2 = 1 \mod 9$$

genau in den Fällen

$$(r, s) = (1, \pm 1), (4, \pm 4), (7, \pm 7).$$

Bei $r = 2, 5, 8$ ist $ab^2 - 1 \neq 0 \mod 3$ und wir müssen $ab^2 + 1 = (9u + r)(9v + s)^2 + 1 = rs^2 + 1 \mod 9$ betrachten. Dabei gilt

$$rs^2 = -1 \mod 9$$

genau in den Fällen

$$(r, s) = (2, \pm 2), (5, \pm 5), (8, \pm 8).$$

Unter der Voraussetzung $a \neq \pm b$ ist also der Exponent der 3 in $(ab^2+1)(ab^2-1)$ genau 1. Somit ist $3 \in (X-ab^2)$ und das einzige Primideal oberhalb von (3) ist in der Lokalisierung auch ein Hauptideal.

(4) Es ist

$$z = \frac{1}{3}(1 + ax + by) = \frac{1}{3}\big(1 + ax + x^2\big).$$

Die Koeffizienten des charakteristischen Polynoms dieses Elementes sind nach Aufgabe 16.2 gleich $\mathrm{Spur}\,(z) = 1$, $\frac{1}{9}(3-3aab^2) = \frac{1}{3}(1-a^2b^2)$ und

$$\begin{aligned} N(z) &= \frac{1}{27}\big(1-3aab^2+a^3ab^2+(ab^2)^2\big) \\ &= \frac{1}{27}\big(1-3a^2b^2+a^4b^2+a^2b^4\big) \\ &= \frac{1}{27}\big(1+a^2b^2(-3+a^2+b^2)\big). \end{aligned}$$

Unter der Bedingung $a = \pm b \mod 9$ ist $a^2 = b^2 = 1,4,7 \mod 9$, wir setzen $a^2 = 9m+t$ und $b^2 = 9n+t$. In diesen Fällen ist

$$1-a^2b^2 = \begin{cases} 0 \text{ bei } t=1\,, \\ -15 \text{ bei } t=4\,, \\ -48 \text{ bei } t=7 \end{cases} \qquad \mod 9,$$

also stets ein Vielfaches von 3. Ferner ist

$$\begin{aligned} & 1+a^2b^2(a^2+b^2-3) \\ = \;& 1+\big(81mn+9(m+n)r+r^2\big)(9(m+n)+2r-3) \\ = \;& 1+81A+18(m+n)r^2-27(m+n)r+9(m+n)r^2+2r^3-3r^2 \\ = \;& 81A+1+27(m+n)r^2-27(m+n)r+2r^3-3r^2 \\ = \;& 81A+1+27(m+n)(r^2-r)+2r^3-3r^2 \\ = \;& 81A'+1+2r^3-3r^2. \end{aligned}$$

Bei $t = 1,4$ ist dies sogar ein Vielfaches von 81. Bei $t = 7$ sind die hinteren Summanden zusammen gleich

$$1+2\cdot 7^3-3\cdot 7^2 = 540 = 27\cdot 20,$$

also ein Vielfaches von 27 und daher ist z ganz.

Wir zeigen nun, dass die von x,y,z erzeugte Algebra normal ist. Es sei

$$w = k+mx+nx^2$$

mit $k,m,n \in \mathbb{Q}$ ein Element, das über eine Ganzheitsgleichung erfüllt, und wir müssen zeigen, dass es zu $\mathbb{Z}[x,y,z]$ gehört. Aufgrund der Spurbedingung ist $3k$ ganzzahlig. Wir ziehen z (oder $3z$) von w ab und können dann $k = 0$ annehmen. Die weiteren Koeffizientenbedingungen an das charakteristische Polynom besagen, dass $3mnq$ und $m^3q+n^3q^2$ ganzzahlig sind. Da q kein Vielfaches von 3 ist, ist

$$\mathrm{ord}_{(3)}\,(mn) \geq -1,$$

also $\mathrm{ord}_{(3)}\,(m) \geq 0$ oder $\mathrm{ord}_{(3)}\,(n) \geq 0$, und

$$\mathrm{ord}_{(3)}\,(m^3+n^3q) \geq 0.$$

Im ersten Fall folgt wegen der letzten Bedingung auch die Bedingung im zweiten Fall und umgekehrt, d.h. die Ordnung von m und n an der

Stelle (3) ist $\neq 0$. Wegen der Normalität an den anderen Primzahlen folgt überhaupt, dass m und n ganzzahlig sind.

□

Korollar 16.2. *Es sei q eine Primzahl mit $q \neq \pm 1 \mod 9$ (was bei $q = 2 \mod 3$ stets der Fall ist). Dann ist der Ganzheitsring zur Körpererweiterung*

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/(X^3 - q)$$

gleich $\mathbb{Z}[X]/(X^3 - q)$.

Bei $q = 1, -1 \mod 9$ ist

$$z = \frac{1 + qx + x^2}{3}$$

ganz über $\mathbb{Z}[X]/(X^3 - q)$ mit dem Minimalpolynom

$$T^3 - T^2 + \frac{1 - q^2}{3}T - \frac{(q^2 - 1)^2}{27} = 0.$$

In diesem Fall besitzt der Ganzheitsring die Ganzheitsbasis $1, x, z$.

Beweis. Dies ist der Spezialfall von Satz 16.1 mit $a = q$ und $b = 1$. In diesem Fall ist

$$y = \sqrt[3]{q^2} = \sqrt[3]{q}^2 = x^2$$

und

$$S = \mathbb{Z}[x] = \mathbb{Z}[X]/(X^3 - q).$$

□

Beispiel 16.3. Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}] = K \subset \mathbb{R}.$$

Der Ganzheitsring ist

$$\mathbb{Z}[\sqrt[3]{2}] \cong \mathbb{Z}[X]/(X^3 - 2)$$

nach Korollar 16.2. Das ist keine Galoiserweiterung, da das Polynom $X^3 - 2$ über K (und reell) nicht zerfällt. Oberhalb von (2) liegt das einzige Primideal (X). Für eine ungerade Primzahl p mit $p = 2 \mod 3$ sind $p - 1$ und 3 teilerfremd und daher ist die dritte Potenz

$$\mathbb{Z}/(p) \longrightarrow \mathbb{Z}/(p),\ z \longmapsto z^3,$$

eine Bijektion. Insbesondere besitzt die 2 eine eindeutig bestimmte dritte Wurzel a und es gibt eine Faktorzerlegung

$$X^3 - 2 = (X - a)(X^2 + bX + c)$$

in $\mathbb{Z}/(p)[X]$, wobei der hintere Faktor irreduzibel ist. Deshalb liegen über (p) in der Erweiterung $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt[3]{2}]$ zwei Primideale, wobei deren Restekörper einerseits $\mathbb{Z}/(p)$ und andererseits $\mathbb{F}_{p^2}$ ist. Inssbesondere sind diese nicht zueinander isomorph. Bei $p = 5$ ist beispielsweise

$$3^3 = 2 \mod 5$$

und

$$X^3 - 2 = X^3 + 3 = (X+2)(X^2+3X+4)$$

und somit

$$\begin{aligned}\mathbb{Z}[\sqrt[3]{2}] \otimes_{\mathbb{Z}} \mathbb{Z}/(5) &= \mathbb{Z}[X]/(X^3-2) \otimes_{\mathbb{Z}} \mathbb{Z}/(5) \\ &= \mathbb{Z}/(5)[X]/(X^3-2) \\ &= \mathbb{Z}/(5)[X]/(X+2) \times \mathbb{Z}/(5)[X]/(X^2+3X+4) \\ &\cong \mathbb{Z}/(5) \times \mathbb{F}_{25}.\end{aligned}$$

Bei

$$p = 1 \mod 3$$

ist 3 ein Teiler von $p-1$ und daher gibt es drei dritte Einheitswurzeln in $\mathbb{Z}/(p)$. Wenn die 2 in $\mathbb{Z}/(p)$ eine dritte Wurzel besitzt, so besitzt sie sogar drei dritte Wurzeln und die Faser zerfällt in drei Punkte, deren Restekörper $\mathbb{Z}/(7)$ sind. Wenn die 2 in $\mathbb{Z}/(p)$ keine dritte Wurzel besitzt, so besteht die Faser aus einem einzigen Punkt, dessen Restekörper der Körper mit p^3 Elementen ist.

Sei $p = 7$. Dritte Einheitswurzeln sind $1, 2, 4$. Die andere dritte Potenz ist

$$6 = 3^3 = 5^3 = 6^3.$$

D.h. 2 ist keine dritte Potenz und $\mathbb{Z}/(7)[X]/(X^3-2)$ ist ein Körper mit 243 Elementen.

Sei $p = 13$. Die dritten Einheitswurzeln sind $1, 3, 9$. Die weiteren dritten Potenzen sind $-1 = 12, 8 = 2^3, 5 = 11^3$, die 2 ist also wieder keine dritte Potenz.

Sei $p = 19$. Die dritten Einheitswurzeln sind $1, 7, 11$. Die weiteren dritten Potenzen sind $-1 = 18, 8 = 2^3, 7 = 4^3, 11 = 5^3, 12 = 10^3$, die 2 ist also wieder keine dritte Potenz.

Sei $p = 31$. Die dritten Einheitswurzeln sind $1, 5, 25$.

Hier ist

$$2 = 4^3 = 20^3 = 7^3.$$

D.h. es ist

$$\begin{aligned}\mathbb{Z}[\sqrt[3]{2}] \otimes_{\mathbb{Z}} \mathbb{Z}/(31) &= \mathbb{Z}[X]/(X^3-2) \otimes_{\mathbb{Z}} \mathbb{Z}/(31) \\ &= \mathbb{Z}/(31)[X]/(X^3-2) \\ &= \mathbb{Z}/(31)[X]/(X-4)(X-7)(X-20) \\ &\cong \mathbb{Z}/(31) \times \mathbb{Z}/(31) \times \mathbb{Z}/(31),\end{aligned}$$

die Faser besteht also aus drei Punkten, die alle den Restekörper $\mathbb{Z}/(31)$ besitzen.

Die zusätzliche Ganzheitsgleichung ist bei einer Primzahl q erstmals bei $q = 17$ zu berücksichtigen.

Beispiel 16.4. Wir betrachten den Zahlbereich zur Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/(X^3 - 17),$$

dieser besitzt nach Korollar 16.2 die Beschreibung

$$R = \mathbb{Z}[x, z] \subseteq \mathbb{Q}[X](X^3 - 17)$$

mit

$$z = \frac{1 + 17x + x^2}{3}$$

und wobei z die Ganzheitsgleichung

$$T^3 - T^2 - 96T - 3072 = 0$$

erfüllt.

Lemma 16.5. *Es seien a und b teilerfremde quadratfreie natürliche Zahlen, nicht beide 1, und sei $\mathbb{Q} \subseteq \mathbb{Q}[X]/(X^3 - ab^2) = L$ die zugehörige kubische Körpererweiterung mit dem Ganzheitsring R. Dann gilt für die Diskriminante von R folgende Beschreibung.*

(1) *Bei $a \neq \pm b \mod 9$ ist die Diskriminante von R gleich $-27a^2b^2$.*
(2) *Bei $a = \pm b \mod 9$ ist die Diskriminante von R gleich $-3a^2b^2$.*

Beweis. Wir setzen $x = \sqrt[3]{ab^2}$ und $y = \sqrt[3]{a^2b}$. Nach Satz 16.1 ist der Ganzheitsring gleich $\mathbb{Z}[x, y]$ und $1, x, y$ ist eine Ganzheitsbasis, ferner ist $y = x^2/b$. Wir berechnen zuerst die Diskriminante zu $1, x, x^2$. Dabei ist $x^3 = ab^2$ und $x^4 = ab^2x$. Die Spur von x und von x^2 ist gleich 0, daher ist

$$\triangle(1, x, x^2) = \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3ab^2 \\ 0 & 3ab^2 & 0 \end{pmatrix} = -27a^2b^4.$$

Die Übergangsmatrix zwischen $1, x, x^2$ und $1, x, y$ hat die Determinante $1/b$, daher ist die Diskriminante des Zahlbereiches nach Lemma 8.2 gleich $-27a^2b^2$.

Im zweiten Fall bleibt die bisherige Rechnung gültig, doch ist jetzt $\frac{1}{3}(1 + ax + by), x, y$ eine Ganzheitsbasis. Die Übergangsmatrix zwischen den Basen $1, x, y$ und z, x, y ist

$$\begin{pmatrix} \frac{1}{3} & \frac{a}{3} & \frac{b}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

mit der Determinante $\frac{1}{3}$. Dies ergibt den Faktor $\frac{1}{9}$. □

16. Arbeitsblatt

16.1. **Aufgaben.**

Aufgabe 16.1. Es sei $n \in \mathbb{N}_+$, $q \in \mathbb{Z}$ und $a \neq 0$. Zeige

$$\mathbb{Q}[X]/(X^n - q) \cong \mathbb{Q}[Y]/(Y^n - a^n q).$$

Aufgabe 16.2.*

Es sei $q \geq 2$ eine natürliche Zahl. Bestimme für die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/(X^3 - q)$$

und ein Element $a+bx+cx^2$ die Multiplikationsmatrix bezüglich der $\mathbb{Q}$-Basis $1, x, x^2$, das charakteristische Polynom, die Norm und die Spur.

Aufgabe 16.3. Es sei b eine quadratfreie Zahl ≥ 2. Zeige, dass $\mathbb{Z}[X]/(X^3 - b^2)$ nicht normal ist.

Aufgabe 16.4. Es sei $q \geq 2$ und $L = \mathbb{Q}[X]/(X^3-q)$. Bestimme die Anzahl der reellen und die Anzahl der komplexen Einbettungen von L.

Aufgabe 16.5. Analysiere die Fasern über (p) zu $\mathbb{Z} \subseteq R$, wobei R der Zahlbereich zur kubischen Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[X]/(X^3 - 5)$ ist.

Aufgabe 16.6. Es sei R der Ganzheitsring zur kubischen Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[X]/(X^3-q)$. Zeige, dass die Faser über (3) aus mehr als einem Punkt bestehen kann.

Aufgabe 16.7.*

Es sei q eine Primzahl mit $q = \pm 1 \mod 9$ und

$$R = \mathbb{Z}[x, z] \subseteq \mathbb{Q}[X]/\big(X^3 - q\big)$$

mit $z = \frac{1+qx+x^2}{3}$ der zugehörige kubische Zahlbereich, siehe Korollar 16.2. Bestimme Darstellungen für x^2, xz, z^2 bezüglich der Ganzheitsbasis $1, x, z$.

Aufgabe 16.8.*

Es seien a und b teilerfremde quadratfreie natürliche Zahlen mit $a = \pm b \bmod 9$. Es sei $x = \sqrt[3]{ab^2}$, $y = \sqrt[3]{a^2b}$ und $z = \frac{1+ax+x^2}{3}$. Bestimme eine Ganzheitsbasis des zugehörigen Zahlbereichs zu $L = \mathbb{Q}[X]/(X^3 - ab^2)$ der Form $1, z, w$.

Drücke x und y durch die neue Basis aus.

Aufgabe 16.9. Es sei R der Zahlbereich zu einer kubischen Erweiterung. Zeige, dass R eine Restklassenbeschreibung mit (maximal) drei Variablen und drei Gleichungen besitzt.

Aufgabe 16.10.*

Es seien a, b verschiedene quadratfreie Zahlen $\neq 1$, die beide den Rest 1 modulo 4 haben. Es sei $x = \frac{1+\sqrt{a}}{2}$ und $y = \frac{1+\sqrt{b}}{2}$. Zeige, dass $z = \frac{1+\sqrt{ab}}{2}$ zu $\mathbb{Z}[x, y]$ gehört.

17. Vorlesung - Kreisteilungsringe

17.1. **Kreisteilungskörper.**

Wir rekapitulieren ohne Beweis die wichtigsten Ergebnisse über Kreisteilungskörper, wie sie in der Galoistheorie bewiesen werden.

Definition 17.1. Der n-te *Kreisteilungskörper* ist der Zerfällungskörper des Polynoms

$$X^n - 1$$

über $\mathbb{Q}$.

Die Kreisteilungskörper über $\mathbb{Q}$ bezeichnen wir mit K_n. Offenbar ist 1 eine Nullstelle von $X^n - 1$, daher kann man $X^n - 1$ durch $X - 1$ teilen und erhält

$$X^n - 1 = (X - 1)\big(X^{n-1} + X^{n-2} + \cdots + X + 1\big).$$

Wegen $1 \in \mathbb{Q}$ ist daher der n-te Kreisteilungskörper auch der Zerfällungskörper von

$$X^{n-1} + X^{n-2} + \cdots + X + 1\,.$$

Da $X^n - 1$ auf die in Lemma 2.10 (Körper- und Galoistheorie (Osnabrück 2018-2019)) beschriebene Art über $\mathbb{C}$ in Linearfaktoren zerfällt, nämlich

$$X^n - 1 = \prod_{k=0}^{n-1}(X - e^{k2\pi\mathrm{i}/n}),$$

kann man K_n als Unterkörper von $\mathbb{C}$ realisieren, und zwar ist K_n der von allen n-ten Einheitswurzeln erzeugte Unterkörper von $\mathbb{C}$. Dieser wird sogar schon von einer einzigen primitiven Einheitswurzel erzeugt.

Lemma 17.2. *Es sei $n \in \mathbb{N}_+$. Dann wird der n-te Kreisteilungskörper über $\mathbb{Q}$ von $e^{2\pi \mathrm{i}/n}$ erzeugt. Der n-te Kreisteilungskörper ist also*

$$K_n = \mathbb{Q}\big(e^{2\pi \mathrm{i}/n}\big) = \mathbb{Q}[e^{2\pi \mathrm{i}/n}].$$

Insbesondere ist jeder Kreisteilungskörper eine einfache Körpererweiterung von $\mathbb{Q}$.[2]

Statt $e^{\frac{2\pi \mathrm{i}}{n}}$ kann man auch jede andere n-te primitive Einheitswurzel aus $\mathbb{C}$ als Erzeuger nehmen.

Beispiel 17.3. Wir bestimmen einige Kreisteilungskörper für kleine n. Bei $n = 1$ oder 2 ist der Kreisteilungskörper gleich $\mathbb{Q}$. Bei $n = 3$ ist

$$X^3 - 1 = (X-1)\big(X^2 + X + 1\big)$$

und der zweite Faktor zerfällt

$$X^2 + X + 1 = \left(X + \frac{1}{2} - \mathrm{i}\frac{\sqrt{3}}{2}\right)\left(X + \frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}\right).$$

Daher ist der dritte Kreisteilungskörper der von $\sqrt{-3} = \sqrt{3}\mathrm{i}$ erzeugte Körper, es ist also $K_3 = \mathbb{Q}[\sqrt{-3}]$ eine quadratische Körpererweiterung der rationalen Zahlen.

Bei $n = 4$ ist natürlich

$$\begin{aligned} X^4 - 1 &= \big(X^2 - 1\big)\big(X^2 + 1\big) \\ &= (X-1)(X+1)\big(X^2+1\big) \\ &= (X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i}). \end{aligned}$$

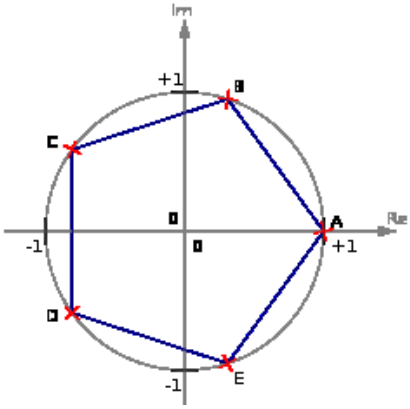
Der vierte Kreisteilungskörper ist somit $\mathbb{Q}[\mathrm{i}] \cong \mathbb{Q}[X]/(X^2+1)$, also ebenfalls eine quadratische Körpererweiterung von $\mathbb{Q}$.

Lemma 17.4. *Es sei p eine Primzahl. Dann ist der p-te Kreisteilungskörper gleich*

$$\mathbb{Q}[X]/\big(X^{p-1} + X^{p-2} + \cdots + X^1 + 1\big)\,.$$

Insbesondere besitzt der p-te Kreisteilungskörper den Grad $p-1$ über $\mathbb{Q}$.

[2] Dies ist natürlich auch klar aufgrund des Satzes vom primitiven Element.



Beispiel 17.5. Der fünfte Kreisteilungskörper wird von der komplexen Zahl $e^{2\pi i/5}$ erzeugt. Er hat aufgrund von Lemma 17.4 die Gestalt

$$K_5 \cong \mathbb{Q}[X]/\big(X^4+X^3+X^2+X+1\big),$$

wobei die Variable X als $e^{2\pi i/5}$ (oder eine andere primitive Einheitswurzel) zu interpretieren ist. Sei $x = e^{2\pi i/5}$ und setze $v = x - x^2 - x^3 + x^4 = -(2x^3+2x^2+1)$. Aus Symmetriegründen muss dies eine reelle Zahl sein. Es ist

$$\begin{aligned} v^2 &= 4x^6+4x^4+1+8x^5+4x^3+4x^2 \\ &= 4x+4x^4+1+8+4x^3+4x^2 \\ &= 5+4\big(x^4+x^3+x^2+x+1\big) \\ &= 5. \end{aligned}$$

Es ist also $v = \sqrt{5}$ (die positive Wurzel) und somit haben wir eine Folge von quadratischen Körpererweiterungen

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}] \subset K_5.$$

Die Menge der n-ten Einheitswurzeln in $\mathbb{C}$ bilden eine zyklische Gruppe der Ordnung n und die primitiven Einheitswurzeln sind die Erzeuger davon. Ihre Anzahl stimmt damit generell mit der Anzahl der Erzeuger der additiven Gruppe $(\mathbb{Z}/(n),\cdot,0)$ überein. Diese Anzahl bekommt einen eigenen Namen.

Definition 17.6. Zu einer natürlichen Zahl n bezeichnet $\varphi(n)$ die Anzahl der Elemente von $(\mathbb{Z}/(n))^\times$. Man nennt $\varphi(n)$ die *Eulersche Funktion*.

Definition 17.7. Es sei $n \in \mathbb{N}_+$ und seien $z_1,\ldots,z_{\varphi(n)}$ die primitiven komplexen Einheitswurzeln. Dann heißt das Polynom

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - z_i) \in \mathbb{C}[X]$$

das n-te *Kreisteilungspolynom*.

Lemma 17.8. *Die Koeffizienten der Kreisteilungspolynome liegen in* $\mathbb{Z}$.

Satz 17.9. *Die Kreisteilungspolynome* Φ_n *sind irreduzibel über* $\mathbb{Q}$.

Satz 17.10. *Der* n*-te Kreisteilungskörper* K_n *über* $\mathbb{Q}$ *hat die Beschreibung*

$$K_n \,=\, \mathbb{Q}[X]/(\Phi_n),$$

wobei Φ_n *das* n*-te Kreisteilungspolynom bezeichnet. Der Grad des* n*-ten Kreisteilungskörpers ist* $\varphi(n)$.

Satz 17.11. *Es sei* K_n *der* n*-te Kreisteilungskörper. Dann ist* $\mathbb{Q} \subseteq K_n$ *eine Galoiserweiterung mit der Galoisgruppe*

$$\mathrm{Gal}\,(K_n|\mathbb{Q}) \,\cong\, (\mathbb{Z}/(n))^\times.$$

Dabei entspricht der Einheit $a \in (\mathbb{Z}/(n))^\times$ *derjenige Automorphismus* $\varphi_a \in \mathrm{Gal}\,(K_n|\mathbb{Q})$*, der eine* n*-te Einheitswurzel* ζ *auf* ζ^a *abbildet.*

17.2. **Kreisteilungsringe.**

Definition 17.12. Es sei $n \in \mathbb{N}_+$. Der Ring der ganzen Zahlen im n-ten Kreisteilungskörper heißt n-ter *Kreisteilungsring*.

Wir bezeichnen diesen Kreisteilungsring mit R_n und möchten die Gleichheit $R_n = \mathbb{Z}[X]/(\Phi_n)$ nachweisen, was bedeutet, dass der Kreisteilungsring durch die selbe Gleichung beschrieben wird wie der Kreisteilungskörper. Für $n = 3$ ist der Kreisteilungsring der Ring der Eisensteinzahlen, und für diesen gilt in der Tat die Beschreibung $\mathbb{Z}[u]/(u^2+u+1)$ und für $n = 4$ ist der vierte Kreisteilungsring der Ring der Gaußschen Zahlen $\mathbb{Z}[u]/(u^2+1)$, und u^2+1 ist das vierte Kreisteilungspolynom. Aber schon für diese niedrigen Zahlen ist das Resultat nicht selbstverständlich, sondern beruht auf der expliziten Beschreibung der quadratischen Zahlbereiche im Sinne von Satz 9.8.

Wir werden die Behauptung zuerst für eine Primzahl $n = p$ zeigen. Wenn ζ eine primitive p-te Einheitswurzel ist, so spielt das Element $1-\zeta$ eine besondere Rolle.

Lemma 17.13. *Es sei* p *eine Primzahl und sei* $\zeta \in \mathbb{C}$ *eine primitive* p*-te Einheitswurzel. Dann ist das einzige Primideal im* p*-ten Kreisteilungsring oberhalb von* (p) *das Primhauptideal* $(1-\zeta)$.

Beweis. Wir setzen

$$S \,:=\, \mathbb{Z}[\zeta] \,\cong\, \mathbb{Z}[Y]/(Y^{p-1}+Y^{p-2}+\cdots+Y^2+Y+1) \,\subseteq\, R_p \,\subseteq\, \mathbb{C}.$$

Das p-te Kreisteilungspolynom zerfällt

$$X^{p-1}+X^{p-2}+\cdots+X^2+X+1 \,=\, \prod_{k=1}^{p-1}(X-\zeta^k),$$

über $\mathbb{C}$ und auch über S. Für $X = 1$ ergibt sich speziell die Gleichung

$$p = \prod_{k=1}^{p-1}(1-\zeta^k).$$

Aufgrund der endlichen geometrischen Reihe ist

$$\frac{1-\zeta^k}{1-\zeta} = 1+\zeta+\zeta^2+\cdots+\zeta^{k-1}$$

und dieses Element gehört zu S. Da k zwischen 1 und $p-1$ ist, gibt es jeweils ein ℓ mit $k \cdot \ell = 1 \mod p$. Wegen $\zeta^p = 1$ und

$$\begin{aligned}\frac{1-\zeta}{1-\zeta^k} &= \frac{1-\zeta^{k\ell}}{1-\zeta^k} \\ &= \frac{1-(\zeta^k)^\ell}{1-\zeta^k} \\ &= 1+\zeta^k+(\zeta^k)^2+\cdots+(\zeta^k)^{\ell-1}\end{aligned}$$

gehört dieses Element ebenfalls zu S, d.h. die Elemente $\frac{1-\zeta^k}{1-\zeta}$ sind Einheiten in S. Deshalb ist

$$p = \prod_{k=1}^{p-1}(1-\zeta^k) = \prod_{k=1}^{p-1}\frac{1-\zeta^k}{1-\zeta}(1-\zeta) = u\cdot(1-\zeta)^{p-1}$$

mit einer Einheit u aus S. Deshalb gilt in S und damit auch im ganzen Abschluss R_p die Idealgleichheit $(p) = ((1-\zeta)^{p-1})$.

Im ganzen Abschluss liegt nach Satz 12.2 eine Idealzerlegung

$$(1-\zeta) = \mathfrak{p}_1\cdots\mathfrak{p}_r$$

vor und daher gilt dort

$$(p) = ((1-\zeta)^{p-1}) = \mathfrak{p}_1^{p-1}\cdots\mathfrak{p}_r^{p-1}.$$

Da der Grad der Erweiterung gleich $p-1$ ist, folgt direkt $r = 1$ und somit, dass $(1-\zeta)$ ein Primideal ist, und zwar das einzige über (p). □

Lemma 17.14. *Es sei p eine Primzahl und sei $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Dann ist der p-te Kreisteilungsring gleich $\mathbb{Z}[\zeta]$.*

Beweis. Wir zeigen, dass

$$\mathbb{Z}[\zeta] \cong \mathbb{Z}[Y]/(Y^{p-1}+Y^{p-2}+\cdots+Y^2+Y+1)$$

bereits normal ist, also mit seinem ganzen Abschluss übereinstimmt. Dazu genügt es zu zeigen, dass die Lokalisierung von $\mathbb{Z}[\zeta]$ an jedem Primideal $\mathfrak{q}$ ein diskreter Bewertungsring ist. Es sei

$$\mathfrak{q}\cap\mathbb{Z} = (q)$$

mit einer Primzahl q und wir machen eine Fallunterscheidung je nachdem, ob $q = p$ ist oder nicht. Bei $q = p$ zeigt Lemma 17.13, dass $\mathfrak{q} = (\zeta-1)$ ein

Hauptideal ist, was sich auf die Lokalisierung überträgt. Bei $q \neq p$ lokalisieren wir die Situation an (q). Da X^p-1 und seine Ableitung pX^{p-1} teilerfremd in $\mathbb{Z}_{(q)}[X]$ sind, gilt dies auch für das Kreisteilungspolynom und seine Ableitung. Deshalb sind die Primteiler des Kreisteilungspolynoms in $\mathbb{Z}/(q)[X]$ einfach. Somit sind die Lokalisierungen oberhalb von (q) nach Lemma 15.1 diskrete Bewertungsringe. □

Insbesondere ist $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ eine Ganzheitsbasis des Kreisteilungsringes.

Beispiel 17.15. Es sei $R = \mathbb{Z}[X]/(X^4+X^3+X^2+X+1) = \mathbb{Z}[x]$ der fünfte Kreisteilungsring. Wir verwenden den Zwischenring (vergleiche Beispiel 17.5)

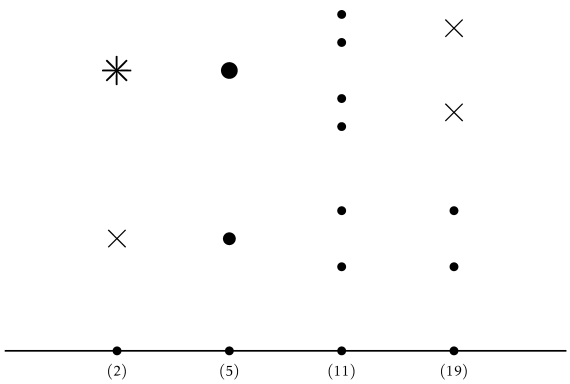
$$\begin{array}{rcl} \mathbb{Z} & \subseteq & \mathbb{Z}[\sqrt{5}] \\ & \subseteq & \mathbb{Z}[W]/(W^2-W-1) \\ & = & S \\ & \subseteq & \mathbb{Z}[X]/(X^4+X^3+X^2+X+1) \\ & = & S[X]/(X^2+XW+1) \end{array}$$

mit

$$w = \frac{v+1}{2} = x^3+x^2+1$$

und $v^2 = 5$. Wir beschreiben exemplarisch das Verhalten von Primzahlen in diesem Zahlbereich. Zu einer Primzahl p kommen als Restekörper der Primideale in R oberhalb von (p) nach Korollar 8.8 nur die Körper $\mathbb{Z}/(p), \mathbb{F}_{p^2}, \mathbb{F}_{p^3}, \mathbb{F}_{p^4}$ in Frage (die Möglichkeit $\mathbb{F}_{p^3}$ werden wir gleich ausschließen), und zwar muss es in den Restekörpern fünf Einheitswurzeln (über (5) fallen die zusammen) geben. Wegen Satz 9.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) ist dies genau dann der Fall, wenn p^e-1 ein Vielfaches von 5 ist. Daraus ergeben sich die Möglichkeiten $e = 1, 2, 4$. Wir geben Beispiele für typisches Zerlegungsverhalten.

Sei $p = 2$. Es ist $S/2S$ ein Körper mit vier Elementen und es ist $R/2S$ ein Körper mit 16 Elementen.



Das exemplarische Zerlegungsverhalten im fünften Kreisteilungsring umd im quadratischen Zahlbereich zu $\sqrt{5}$.

Sei $p = 5$. Hier ist über $\mathbb{Z}/(5)$

$$(X-1)(X^4+X^3+X^2+X+1) = X^5-1 = (X-1)^5$$

und somit $X^4+X^3+X^2+X+1 = (X-1)^4$. Es gibt also nur ein Primideal oberhalb von (5) und dessen Restklassenkörper ist $\mathbb{Z}/(5)$, was auch von Lemma 17.13 her klar ist.

Bei $q = 11$ sind $1, 3, 4, 5, 9$ fünfte Einheitswurzeln und das Kreisteilungspolynom hat die Zerlegung

$$X^4+X^3+X^2+X+1 = (X-3)(X+2)(X-4)(X-5).$$

Oberhalb von (11) liegen in $\operatorname{Spek}(R)$ vier Primideale, alle mit dem Restekörper $\mathbb{Z}/(11)$. Dabei liegen $(X-3)$ und $(X-4)$ über $(W-4)$ und $(X+2)$ und $(X-5)$ über $(W-8)$ in S.

Bei $p = 19$ ist $9^2 = 5 = 10^2$, in S gibt es somit zwei Primideale oberhalb von (19), beide mit dem Restekörper $\mathbb{Z}/(19)$. In $\mathbb{Z}/(19)$ gibt es aber keine fünfte Einheitswurzeln, deshalb liegen oberhalb von (19) in R zwei Primideale, beide mit dem Restekörper $\mathbb{F}_{361}$. Über (19) liegt die Faktorzerlegung

$$X^4+X^3+X^2+X+1 = \big(X^2+5X+1\big)\big(X^2+15X+1\big)$$

vor.

Lemma 17.16. *Es sei p eine Primzahl und ζ eine primitive p-te Einheitswurzel. Dann ist die Diskriminante der $\mathbb{Q}$-Basis $1, \zeta, \zeta^2, \dots, \zeta^{p-2}$ des p-ten Kreisteilungskörpers gleich*

$$\triangle(1, \zeta, \zeta^2, \dots, \zeta^{p-2}) = \pm p^{p-2}.$$

Beweis. Das p-te Kreisteilungspolynom ist

$$\Phi_p = X^{p-1}+X^{p-2}+\cdots+X^2+X+1 = (X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{p-1}).$$

Es ist nach Lemma 8.11

$$\begin{aligned}\triangle(1, \zeta, \zeta^2, \dots, \zeta^{p-2}) &= \prod_{0\le i<j\le p-2} (\zeta^i-\zeta^j)^2 \\ &= \pm \prod_{0\le i,j\le p-2,\, i\ne j} (\zeta^i-\zeta^j).\end{aligned}$$

Wenn man die Übergangsmatrix zwischen den beiden Basen $1, \zeta, \zeta^2, \dots, \zeta^{p-2}$ und $\zeta, \zeta^2, \dots, \zeta^{p-2}, \zeta^{p-1}$ betrachtet, so ist deren Determinante gleich ± 1 und deshalb kann man wegen Lemma 8.2 genauso gut $\pm\prod_{1\le i,j\le p-1,\, i\ne j}(\zeta^i-\zeta^j)$ berechnen.

Wir verwenden nun zwei verschiedene Möglichkeiten, die Ableitung des Kreisteilungspolynoms zu bestimmen. Die Ableitung von Φ_p ist nach der Produktregel gleich

$$\sum_{k=1}^{p-1} (X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{p-1})/(X-\zeta^k)\,.$$

Wenn man darin ζ^i, $i = 1, \ldots, p-1$, einsetzt, so werden alle Summanden mit der einzigen Ausnahme für $k = i$ zu 0, und der verbleibende Summand ist

$$\Phi_p'(\zeta^i) = \prod_{1 \leq j \leq p-1,\, j \neq i} (\zeta^i - \zeta^j).$$

Somit ist die Diskriminante gleich

$$\pm \prod_{i=1}^{p-1} \Phi_p'(\zeta^i) = \pm \prod_{\varphi} \Phi_p'(\varphi(\zeta)) = \pm \prod_{\varphi} \varphi(\Phi_p'(\zeta)) = \pm N(\Phi_p'(\zeta)),$$

wobei φ die Galoisgruppe durchläuft und Lemma 7.14 verwendet wurde. Aufgrund von

$$X^p - 1 = (X-1)\Phi_p$$

gilt für die Ableitung auch die Beziehung

$$pX^{p-1} = (X-1)\Phi_p' - \Phi_p.$$

Wenn man darin ζ einsetzt, so erhält man

$$p\zeta^{p-1} = p\zeta^{-1} = (\zeta - 1)\Phi_p'(\zeta)$$

und somit

$$\Phi_p'(\zeta) = p\zeta^{-1}(\zeta-1)^{-1}.$$

Die Norm von $\zeta - 1$ ist

$$N(\zeta - 1) = \prod_{k=1}^{p-1} (\zeta^k - 1) = \pm \Phi_p(1) = \pm p.$$

Deshalb ist die Diskriminante nach Lemma 8.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)) und Lemma 10.2 gleich

$$\begin{aligned} \pm N(\Phi_p'(\zeta)) &= \pm N(p\zeta^{-1}(\zeta-1)^{-1}) \\ &= \pm N(p) N(\zeta^{-1}) N((\zeta-1)^{-1}) \\ &= \pm p^{p-1} \cdot \frac{1}{p} \\ &= \pm p^{p-2} \end{aligned}$$

□

Lemma 17.17. *Es sei p eine Primzahl, $q = p^r$ und ζ eine primitive p^r-te Einheitswurzel und Dann ist die Diskriminante der $\mathbb{Q}$-Basis $1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(p^r)-1}$ des p^r-ten Kreisteilungskörpers gleich*

$$\triangle(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(p^r)-1}) = \pm p^{p^{r-1}(rp-r-1)}.$$

Beweis. Dies wird ähnlich wie Lemma 17.16 bewiesen. □

Satz 17.18. *Sei $n \in \mathbb{N}_+$ und sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Dann ist der n-te Kreisteilungsring gleich $\mathbb{Z}[\zeta]$.*

Beweis. Dies wird zuerst ausgehend von Lemma 17.14 für Primzahlpotenzen bewiesen. Bei $n = p_1^{r_1} \cdot p_k^{r_k}$ ergibt sich eine Ganzheitsbasis des Ganzheitsringes wegen der nach Lemma 17.17 teilerfremden Diskiminanten aus den Produkten der Ganzheitsbasen der einzelnen Kreisteilungsringen zu den Primzahlpotenzen. □

Es ist also

$$R_n = \mathbb{Z}[X]/(\Phi_n),$$

wobei Φ_n das n-te Kreisteilungspolynom bezeichnet.

17. Arbeitsblatt

17.1. **Aufgaben.**

Aufgabe 17.1.*

Schreibe den 5-ten Kreisteilungskörper K_5 als quadratische Körpererweiterung von $\mathbb{Q}[\sqrt{5}]$.

Aufgabe 17.2.*

Wie viele Unterkörper besitzt der Kreisteilungskörper K_{13}?

Aufgabe 17.3. Es sei p eine Primzahl. Betrachte das Polynom

$$P = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1.$$

Zeige, dass P irreduzibel in $\mathbb{Q}[X]$ ist.

Aufgabe 17.4. Es sei L der neunte Kreisteilungskörper über $\mathbb{Q}$. Zeige

$$L \cap \mathbb{R} \cong \mathbb{Q}[X]/\big(X^3 - 3X + 1\big).$$

Aufgabe 17.5.*

Es sei K_n der n-te Kreisteilungskörper über $\mathbb{Q}$ und

$$L_n = K_n \cap \mathbb{R}.$$

Zeige, dass bei $n \geq 3$ die Körpererweiterung $L_n \subseteq K_n$ den Grad 2 besitzt.

Aufgabe 17.6. Es sei $n \in \mathbb{N}$ ungerade. Zeige, dass der n-te Kreisteilungskörper mit dem $2n$-ten Kreisteilungskörper übereinstimmt.

Aufgabe 17.7. Bestimme die Kreisteilungspolynome Φ_n für $n \leq 15$.

Aufgabe 17.8. Zeige, dass für $n \geq 2$ der konstante Koeffizient der Kreisteilungspolynome Φ_n immer 1 ist.

Aufgabe 17.9. Zeige, dass für verschiedene n auch die Kreisteilungspolynome Φ_n verschieden sind, dass aber die Kreisteilungskörper gleich sein können.

Aufgabe 17.10.*

Es sei $n \in \mathbb{N}_+$. Zeige, dass in $\mathbb{C}[X]$ die Gleichung

$$X^n - 1 = \prod_{d|n} \Phi_d$$

gilt.

Aufgabe 17.11.*

Es sei $\mathbb{Q} \subseteq K_n$ (in $\mathbb{C}$) der n-te Kreisteilungskörper und sei ζ eine n-te primitive Einheitswurzel. Wir betrachten die Elemente ζ^i, $i \in (\mathbb{Z}/(n))^\times$.

a) Zeige, dass für eine Primzahl $n = p$ diese Elemente eine $\mathbb{Q}$-Basis von K_n bilden.

b) Es sei p eine Primzahl und $n = p^2$. Zeige, dass diese Elemente keine $\mathbb{Q}$-Basis von K_n bilden.

Aufgabe 17.12. Es sei $n \in \mathbb{N}$, $\mathbb{Q} \subseteq K_n$ der n-te Kreisteilungskörper und sei ζ eine n-te primitive Einheitswurzel.

(1) Zeige, dass für jedes k die (benachbarten) Einheitswurzeln
$$\zeta^k, \zeta^{k+1}, \ldots, \zeta^{k+\varphi(n)-1}$$
eine $\mathbb{Q}$-Basis von K_n.
(2) Bilden die primitiven n-ten Einheitswurzeln stets eine $\mathbb{Q}$-Basis von K_n?

Aufgabe 17.13. Bestimme die Norm und die Spur der n-ten komplexen Einheitswurzeln im n-ten Kreisteilungskörper.

Aufgabe 17.14. Es sei $\zeta_n \in \mathbb{C}$ eine n-te primitive Einheitswurzel, und $K = \mathbb{Q}[\zeta_n]$ der zugehörige Kreisteilungskörper. Zeige, dass es galoissche Körpererweiterungen $K \subseteq L$ gibt, deren Galoisgruppe zyklisch der Ordnung n ist.

Aufgabe 17.15. Zeige, dass das achte Kreisteilungspolynom X^4+1 über allen endlichen Primkörpern $\mathbb{F}_p$ reduzibel ist.

Hinweis: Zeige, dass $\mathbb{F}_{p^2}$ für $p \neq 2$ bereits eine primitive achte Einheitswurzel enthält.

Aufgabe 17.16.*

Es sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen und $n \in \mathbb{N}$. Es sei a der größte gemeinsame Teiler von n und $q-1$. Zeige, dass es in $\mathbb{F}_q$ genau a n-te Einheitswurzeln gibt.

Man folgere, dass es n n-te Einheitswurzeln in $\mathbb{F}_q$ genau dann gibt, wenn n ein Teiler von $q-1$ ist.

Aufgabe 17.17. Es sei p eine Primzahl und n eine natürliche Zahl, die wir als $n = kp^a$ schreiben mit k und p teilerfremd. Zeige, dass der n-te Kreisteilungskörper über $\mathbb{F}_p$ gleich $\mathbb{F}_q$ ist (mit $q = p^e$), wobei q die minimale echte Potenz von p mit der Eigenschaft ist, dass $q-1$ ein Vielfaches von k ist. Zeige insbesondere, dass es ein solches q gibt.

Aufgabe 17.18. Es sei K_p der p-te Kreisteilungskörper zu einer Primzahl p und sei ζ eine primitive p-te Einheitswurzel. Bestimme die Übergangsmatrix und ihre Determinante für die $\mathbb{Q}$-Basen

$$1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$$

und

$$\zeta, \zeta^2, \ldots, , \zeta^{p-2}, \zeta^{p-1}$$

von K_p.

Aufgabe 17.19.*

Bestimme die Zwischenkörper des 7-ten Kreisteilungskörpers K_7. Dabei soll jeweils eine Restklassendarstellung explizit angegeben werden.

Aufgabe 17.20. Es sei K_n der n-te Kreisteilungskörper, $n \geq 3$. Zeige, dass es einen Zwischenkörper L, $\mathbb{Q} \subseteq L \subseteq K_n$, gibt, der eine quadratische Körpererweiterung von $\mathbb{Q}$ ist.

Aufgabe 17.21.*

Es sei ζ eine primitive 7. Einheitswurzel. Wir betrachten das Element

$$y = \zeta + \zeta^2 - \zeta^3 + \zeta^4 - \zeta^5 - \zeta^6 \in \mathbb{Z}[\zeta] = R_7$$

im siebten Kreisteilungsring.

(1) Skizziere $1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6$ und verorte y geometrisch.
(2) Berechne y^2.
(3) Bestimme einen quadratischen Zahlbereich, der im siebten Kreisteilungsring enthalten ist.

Für eine weitgehende Verallgemeinerung dieses Sachverhaltes siehe Lemma 23.8.

Aufgabe 17.22. Analysiere für den zwölften Kreisteilungsring R_{12} das Zerlegungsverhalten für die Primzahlen $p \leq 20$. Studiere dabei auch das Zerlegungsverhalten in den Zwischenringen $R_3 = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, $R_4 = \mathbb{Z}[\mathrm{i}]$ und $\mathbb{Z}[\sqrt{3}]$.

18. Vorlesung - Verzweigung

18.1. **Verzweigungsverhalten.**

Schon mehrfach haben wir das Wort „Verzweigung“ fallen lassen. Jetzt werden wir diesen Begriff verschiedene Präzisierungen und Charakterisierungen angeben.

Definition 18.1. Zu einem injektiven Ringhomomorphismus $R \subseteq S$ zwischen diskreten Bewertungsringen nennt man die Ordnung einer Ortsuniformisierenden von R in S die *Verzweigungsordnung* der Erweiterung.

Statt Verzweigungsordnung sagt man auch *Verzweigungsindex*. Bei einer Erweiterung von Dedekindbereichen

$$\varphi\colon R \longrightarrow S$$

und Primidealen $\mathfrak{q}$ über $\mathfrak{p}$ nennt man die Verzweigungsordnung von

$$R_{\mathfrak{p}} \longrightarrow S_{\mathfrak{q}}$$

auch die Verzweigungsordnung von $\mathfrak{q}$ über $\mathfrak{p}$ oder einfach von $\mathfrak{q}$, da ja $\mathfrak{p}$ durch $\mathfrak{q}$ bestimmt ist. Wenn man von $\mathfrak{p}$ ausgeht, hängt im Allgemeinen die Verzweigungsordnung von den darüber liegenden Primidealen ab.

Definition 18.2. Ein injektiver Ringhomomorphismus $R \subseteq S$ zwischen diskreten Bewertungsringen heißt *verzweigt*, wenn seine Verzweigungsordnung ≥ 2 ist.

Bei einer Erweiterung von Dedekindbereichen $\varphi\colon R \to S$ sagt man auch, dass ein Primideal $\mathfrak{q}$ aus S verzweigt, wenn

$$R_{\mathfrak{p}} \longrightarrow S_{\mathfrak{q}}$$

mit $\mathfrak{p} = R \cap \mathfrak{q}$ verzweigt, und man sagt, dass ein Primideal $\mathfrak{p}$ von R in S verzweigt, wenn es darüber ein Primideal $\mathfrak{q}$ gibt, in dem Verzweigung stattfindet (es darf also auch noch Primideale darüber geben, in denen keine Verzweigung stattfindet).

Lemma 18.3. *Es sei $R \subseteq S$ eine endliche Erweiterung von Zahlbereichen und es sei $\mathfrak{p}$ ein Primideal von R. Es sei*

$$\mathfrak{p}S = \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k}$$

die Idealzerlegung des Erweiterungsideales $\mathfrak{p}S$ im Sinne von Korollar 12.3. Dann ist r_j die Verzweigungsordnung von

$$R_{\mathfrak{p}} \longrightarrow S_{\mathfrak{q}_j}.$$

Insbesondere findet über $\mathfrak{p}$ genau dann Verzweigung statt, wenn ein $r_j \geq 2$ ist.

Beweis. Dies beruht darauf, dass $\mathfrak{p}$ in $S_{\mathfrak{q}_j}$ die Ordnung r_j besitzt, was auf Lemma 11.11 (1) beruht. □

Beispiel 18.4. Es sei K ein algebraisch abgeschlossener Körper. Wir betrachten den Ringhomomorphismus

$$\varphi\colon\ K[Y] \longrightarrow K[X],\ Y \longmapsto X^n,$$

zu $n \geq 2$, der der Abbildung

$$K \longrightarrow K,\ x \longmapsto x^n = y$$

entspricht. Zu einem maximalen Ideal $(X - a)$ ist

$$\varphi^{-1}(X - a) = (Y - a^n),$$

und oberhalb von $(Y - b)$ liegen die maximalen Ideale $(X - a)$ mit

$$a^n = b.$$

Dies ist die idealtheoretische Interpretation der n-ten Potenzierung. Insbesondere liegen die Ringhomomomorphismen

$$K[Y]_{(Y-b)} \longrightarrow K[X]_{(X-a)},\ Y \longmapsto X^n$$

zwischen diskreten Bewertungsringen vor. Dabei wird die Ortsuniformisierende $(Y - b)$ auf

$$X^n - b = X^n - a^n = (X - a)(X^{n-1} + X^{n-2}a^1 + \cdots + Xa^{n-2} + a^{n-1})$$

abgebildet. In dieser Produktdarstellung ist der linke Faktor die Ortsuniformisierende des zweiten Bewertungsringes. Der zweite Faktor wird, wenn man für X die Zahl a einsetzt, zu na^{n-1}. Wenn n und a beide Einheiten in K sind, so ist dieser Faktor eine Einheit in $K[X]_{(X-a)}$ und daher ist die Verzweigungsordnung gleich 1, es liegt also keine Verzweigung vor. Wenn hingegen n keine Einheit ist, wenn also die Charakteristik von K ein Teiler von n ist, so liegt Verzweigung vor. Wenn $n = p$ die positive Charakteristik ist, so ist $X^p - a^p$ und die Verzweigungsordnung ist in jedem Punkt gleich p. Wenn $a = 0$ ist, so ist die Verzweigungsordnung direkt gleich n im Nullpunkt.

18.2. **Verzweigung und Ableitung.**

Lemma 18.5. *Es seien R, S Dedekindbereiche und es sei*

$$R \subseteq S = R[X]/(F)$$

eine monogene endliche Ringerweiterung. Es Dann ist ein Primideal $\mathfrak{p}$ von R mit perfektem Restekörper in S genau dann unverzweigt, wenn F und F' in $\kappa(\mathfrak{p})[X]$ teilerfremd sind.

Beweis. Es sei $\mathfrak{p}$ ein maximales Ideal von R und

$$\mathfrak{p}S = \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k}$$

die Zerlegung des Erweiterungsideales $\mathfrak{p}S$ in Ideale, die es nach Satz 12.2 gibt. Das bedeutet insbesondere, dass die Ortsuniformisierende p zu $\mathfrak{p}$ in $S_{\mathfrak{q}_j}$ die Ordnung r_j besitzt. Es liegt nach Lemma 18.3 genau dann Verzweigung vor, wenn $r_j \geq 2$ für mindestens ein j gilt. Der Faserring ist unter Verwendung von Satz 12.8 gleich

$$\kappa(\mathfrak{p})[X]/(F) = S/\mathfrak{p}S = S/\mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k} = S/\mathfrak{q}_1^{r_1} \times \cdots \times S/\mathfrak{q}_k^{r_k}.$$

Dieser Ring ist genau dann reduziert, wenn $r_j = 1$ für alle j gilt. Deshalb folgt die Aussage aus Lemma Anhang 8.3. □

Beispiel 18.6. Es sei D eine quadratfreie Zahl $\neq 0, 1$ mit

$$D = 2, 3 \mod 4$$

und A_D der zugehörige quadratische Zahlbereich, der nach Satz 9.8 die Restklassenbeschreibung $A_D = \mathbb{Z}[X]/(X^2 - D)$ besitzt. Die Ableitung von

$$F = X^2 - D$$

ist $2X$ und somit ist, um das Verzweigungsverhalten zu verstehen, nach Lemma 18.5 das Ideal $(2X, X^2 - D)$ zu betrachten. Wenn $p \neq 2$ und kein Teiler von D ist, so ist dies über $\mathbb{Z}/(p)$ das Einheitsideal und es liegt keine Verzweigung vor. Wenn p ein Teiler von D oder $p = 2$ ist, so liegt Verzweigung mit Verzweigungsordnung 2 vor.

Bei $D = 1 \mod 4$ ist nach Satz 9.8 $A_D = \mathbb{Z}[Y]/(Y^2 - Y - \frac{D-1}{4})$. Die Ableitung ist $2Y - 1$. Oberhalb von $p = 2$ findet keine Verzweigung statt. Sei also $p \neq 2$. Modulo p ist

$$\begin{aligned}(Y^2 - Y - \frac{D-1}{4}, 2Y - 1) &= (4Y^2 - 4Y - D + 1, 2Y - 1) \\ &= 1 - 2 - D + 1 \\ &= D.\end{aligned}$$

Deshalb liegt Verzweigung genau in den Primteilern von D vor.

Korollar 18.7. *Es sei K ein algebraisch abgeschlossener Körper, $P \in K[X]$ ein nichtkonstantes Polynom und*

$$K[Y] \longrightarrow K[X] \cong K[Y][X]/(Y - P(X)),\ Y \longmapsto P(X),$$

der zugehörige Einsetzungshomomorphismus. Dann ist ein Primideal $(X-a)$ *genau dann verzweigt, wenn* $P'(a) = 0$ *ist, und über einem Primideal* $(Y-b)$ *liegt genau dann Verzweigung vor, wenn es ein* $a \in K$ *mit* $P(a) = b$ *und* $P'(a) = 0$ *gibt.*

Beweis. Wir wenden Lemma 18.5 auf die endliche Erweiterung $K[Y] \subseteq K[Y][X]/(Y - P(X))$ an. Da K algebraisch abgeschlossen ist, ist K vollkommen und der Restekörper zu jedem maximalen Ideal ist gleich K. Verzweigung oberhalb von $(Y - b)$ ist also die Frage, ob $F = Y - P(X)$ und $F' = -P'(X)$ im Restekörper teilerfremd sind. Dabei ist Y als b zu interpretieren, es geht also darum, ob $P(X) - b$ und $P'(X)$ teilerfremd sind. Dies ist genau dann der Fall, wenn diese beiden Polynome keine gemeinsame Nullstelle in K besitzen. □

Beispiel 18.8. Es sei K ein Körper der Charakteristik $p > 0$. Wir betrachten die Ringerweiterung

$$K(t)[Y] \subseteq K(t)[Y][X]/(X^p - t) = K(t)[X]/(X^p - t)[Y] \cong K(x)[Y],$$

die Erweiterung spielt sich also im Wesentlichen im Grundkörper ab. Es ist

$$(X^p - t)' = pX^{p-1} = 0,$$

deshalb sind das beschreibende Polynom und seine Ableitung nirgendwo teilerfremd. Dennoch ist

$$K(t)[Y]_{(Y)} \longrightarrow K(x)[Y]_{(Y)}$$

unverzweigt, da Y in beiden Ringen die Ortsuniformisierende ist. Dies zeigt auch, dass Lemma 18.5 ohne die Voraussetzung über die Perfektheit nicht gilt.

Satz 18.9. *Es sei* R *ein Dedekindbereich mit Quotientenkörper* $K = Q(R)$, *es sei* $K \subseteq L$ *eine separable Körpererweiterung und* S *der ganze Abschluss von* R *in* L. *Dann gibt es nur endlich viele Primideale von* R, *über denen Verzweigung stattfindet.*

Beweis. Es sei

$$L = K[x] = K[X]/(F)$$

mit einem normierten Polynom F, was es nach dem Satz vom primitiven Element gibt. Wir betrachten die endlichen Abbildungen

$$R \subseteq R[x] \cong R[X]/(F) \subseteq S$$

wobei S die Normalisierung von $R[x]$ ist. Es sei

$$S = R[x][\frac{g_1}{f_1}, \ldots, \frac{g_n}{f_n}]$$

mit $g_i, f_i \in R[x]$ und wobei wir $f_i \in R$ annehmen dürfen. Sei

$$f = \prod f_i \neq 0.$$

Dann ist

$$R_f[x] \,=\, R[x]_f \,=\, S_f.$$

Das heißt, dass oberhalb von R_f der Ganzheitsring durch ein Element erzeugt wird. Da es oberhalb von (f) nur endlich viele Primideale in R gibt, genügt es zu zeigen, dass in $D(f)$ nur endlich viele Primideale verzweigen. Wir können also

$$S \,=\, R[x]$$

als monogen annehmen. Wir betrachten das von F und F' erzeugte Ideal in $R[X]$. Wegen der Separabilität der generischen Körpererweiterung erzeugen diese Polynome in $K[X]$ das Einheitsideal, was in $R[X]$ bedeutet, dass es Polynome P, Q gibt mit

$$FP + F'Q \,=\, g \,\in\, R$$

mit $g \,\neq\, 0$. Dies heißt wiederum, dass in $R_g[X]$ die beiden Polynome das Einheitsideal erzeugen. Somit findet nach Lemma 18.5 auf $D(g)$ keine Verzweigung statt. Oberhalb von g gibt es aber auch wieder nur endlich viele Primideale und die Primideale aus $D(g)$ verzweigen nicht. □

18.3. **Verzweigung und Faserringe.**

In Lemma 15.1 und Lemma 15.7 haben wir von der Reduziertheit der Faserringe auf die Normalität des (lokalisierten) Zahlbereiches geschlossen. Wir werden sehen, dass diese Reduziertheit direkt mit der Unverzweigtheit zusammenhängt und dass diese somit stärker als die Normalität ist.

Satz 18.10. *Es sei $R \subseteq S$ eine endliche Erweiterung von Zahlbereichen und es sei $\mathfrak{p}$ ein Primideal von R. Es sei*

$$\mathfrak{p}S \,=\, \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k}$$

die Idealzerlegung des Erweiterungsideales $\mathfrak{p}S$ im Sinne von Korollar 12.3. Dann ist $\mathfrak{p}$ in S genau dann verzweigt, wenn der Faserring zu S über $\mathfrak{p}$ nicht reduziert ist.

Beweis. Nach Korollar 12.3 liegt in S eine Produktzerlegung

$$\mathfrak{p}S \,=\, \mathfrak{q}_1^{r_1} \cdots \mathfrak{q}_k^{r_k}$$

vor und nach Satz 12.8 ist

$$S/\mathfrak{p}S \,\cong\, S/\mathfrak{q}_1^{r_1} \times \cdots \times S/\mathfrak{q}_k^{r_k}.$$

Dieser Restklassenring, der der Faserring zu S über $\mathfrak{p}$ ist, ist genau dann reduziert, wenn alle Exponenten r_i gleich 1 sind. Dies charakterisiert nach Lemma 18.3 auch die Unverzweigtheit. □

Beispiel 18.11. Es sei p eine Primzahl und $R \,=\, \mathbb{Z}[X]/(X^p - p)$. Für eine Primzahl $q \,\neq\, p$ ist der Faserring über (q) gleich $\mathbb{Z}/(q)[X]/(X^p - p)$. Da p eine Einheit in $\mathbb{Z}/(q)$ ist, sind $X^p - p$ und die Ableitung pX^{p-1} teilerfremd in

$\mathbb{Z}/(q)[X]$ und daher ist nach Korollar 15.2 $\mathbb{Z}_p[X]/(X^p-p)$ normal und die Verzweigungsordnung von

$$\mathbb{Z}_{(q)} \longrightarrow R_{\mathfrak{q}},$$

wobei $\mathfrak{q}$ ein Primideal oberhalb von (q) bezeichnet, ist gleich 1. Für $q = p$ ist das einzige Primideal oberhalb von (p) das Hauptideal (X), die Verzweigungsordnung in p ist gleich p. Deshalb ist insgesamt R der Zahlbereich zu $\mathbb{Q} \subset \mathbb{Q}[X]/(X^p-p)$, und er ist nur im Punkt (p) verzweigt.

Beispiel 18.12. Es seien p, q verschiedene Primzahlen und

$$R = \mathbb{Z}[X]/(X^p-q).$$

Für eine Primzahl $r \neq p, q$ ist der Faserring über (r) gleich $\mathbb{Z}/(r)[X]/(X^p-q)$. Da p und q Einheiten in $\mathbb{Z}/(r)$ sind, gilt

$$(X^p-q, pX^{p-1}) = (X^p-q, X^{p-1}) = (q, X^{p-1}) = (q) = 1$$

in $\mathbb{Z}/(r)[X]$, d.h. X^p-q und die Ableitung pX^{p-1} sind teilerfremd in $\mathbb{Z}/(r)[X]$ und daher ist nach Korollar 15.2 $\mathbb{Z}_r[X]/(X^p-q)$ normal und die Verzweigungsordnung von

$$\mathbb{Z}_{(r)} \longrightarrow R_{\mathfrak{r}},$$

wobei $\mathfrak{r}$ ein Primideal oberhalb von (r) bezeichnet, ist gleich 1.

Für $r = q$ ist das einzige Primideal oberhalb von (q) das Hauptideal (X), die Verzweigungsordnung in q ist gleich p.

Für $r = p$ ist der Faserring gleich

$$\mathbb{Z}/(p)[X]/(X^p-q) = \mathbb{Z}/(p)[X]/(X-q)^p.$$

Das einzige Primideal oberhalb von (p) ist also $(X-q, p)$, was im Allgemeinen kein Hauptideal ist. Der Ring R ist im Allgemeinen nicht der ganze Abschluss, wobei die Singularität oberhalb von (p) liegt.

18.4. **Verzweigung und Diskriminante.**

Die Faserringe zu einem Zahlbereich über einer Primzahl p sind im Allgemeinen kein Körper, sie sind aber freie endlich erzeugte $\mathbb{Z}/(p)$-Algebren und daher ist dort auch die Spur und die Diskriminante (allerdings aber nur bis auf eine Einheit) definiert. Unter der *Spurform* auf einer freien K-Algebra A versteht man die symmetrische Bilinearform

$$A \times A \longrightarrow K,\ (x,y) \longmapsto \operatorname{Spur}(xy).$$

Satz 18.13. *Es sei K ein vollkommener Körper und A eine endlichdimensionale K-Algebra. Dann sind folgende Aussagen äquivalent.*

(1) *A ist reduziert.*
(2) *A ist ein Produkt von Körpern.*
(3) *Die Spurform ist nichtausgeartet.*
(4) *Die Diskriminante zu einer K-Basis von A ist ungleich* 0.

Beweis. Die Äquivalenz von (1) und (2) ist klar aufgrund von Aufgabe 17.17. Sei (2) erfüllt, $A = L_1 \times \cdots \times L_r$. Wegen der Voraussetzung vollkommen sind die Körpererweiterungen $K \subseteq L_j$ separabel. Die Spur $A \to K$ setzt sich zusammen aus der Summe der Spuren zu den Körpererweiterungen, da man von diesen jeweils Basen wählen kann und sich diese zu einer Gesamtbasis von A zusammensetzen. Bezüglich einer solchen Basis sind die Multiplikationsmatrizen Diagonalblockmatrizen. Bei $x \in A$ von 0 verschieden ist auch eine Komponente x_j in einem Körper L_j von 0 verschieden. Im Körperfall ist die Spurform nichtausgeartet und daher gibt es $y_j \in L_j$ (das wir in A auffassen können) mit $S(x, y_j) = S(x_j y_j) \neq 0$. (3) und (4) sind äquivalent. Wenn die Spurform nicht ausgeartet ist, so besitzt die Gramsche Matrix davon eine von 0 verschiedene Determinante, und umgekehrt, siehe Aufgabe 38.13 (Lineare Algebra (Osnabrück 2017-2018)) bzw. Lemma 8.3.

Sei nun A nicht reduziert. Zu einem nilpotenten Element f ist das Minimalpolynom gleich X^m und damit ist auch das charakteristische Polynom gleich X^n, wobei n den Grad der Erweiterung bezeichnet (für einen Körper A wurde dies in Lemma 7.10 gezeigt, es gilt aber auch sonst). Deshalb ist die Spur von f nach Aufgabe 7.19 gleich 0. Zu einem nilpotenten Element f und einem beliebigen Element x ist auch fx nilpotent und daher ist, wenn es ein nichttriviales nilpotentes Element gibt, die Spurform ausgeartet. □

Lemma 18.14. *Es sei R ein Zahlbereich, $f \in R$ und p eine Primzahl. Dann ist die Spur von f modulo p gleich der im Faserring $R/(p)$ über $\mathbb{Z}/(p)$ berechneten Spur von $\overline{f} \in R/(p)$.*

Beweis. Nach Korollar 8.6 ist R ein freier $\mathbb{Z}$-Modul, dessen Rang der Grad n der zugrunde liegenden Körpererweiterung ist, und nach Korollar 8.8 ist der Faserring über $\mathbb{Z}/(p)$ eine n-dimensionale $\mathbb{Z}/(p)$-Algebra. In beiden Fällen kann man also die Spur über die Multiplikationsmatrix bezüglich einer Basis berechnen. Sei eine $\mathbb{Z}$-Basis $b_1, \ldots, b_n$ von R fixiert. Eine $\mathbb{Z}$-Basis von R wird modulo p zu einer $\mathbb{Z}/(p)$-Basis von $R/(p)$, siehe den Beweis zu Korollar 8.8. In der Multiplikationsmatrix zu f bezüglich $b_1, \ldots, b_n$ stehen die ganzen Zahlen c_{ij}, die durch

$$fb_i = \sum_{j=1}^{n} c_{ij} b_j$$

gegeben sind. Da $R \to R/(p)$ ein Ringhomomorphismus ist, folgt

$$\overline{fb}_i = \sum_{j=1}^{n} \overline{c}_{ij} \overline{b}_j$$

und daher ist die Multiplikationsmatrix zu $\overline{f}$ bezüglich $\overline{b}_1, \ldots, \overline{b}_n$ einfach die komponentenweise reduzierte Matrix. Deshalb ist insbesondere die Reduktion

der Spur

$$\text{Spur}\,(f) \;=\; \sum_{i=1}^{n} c_{ii}$$

gleich $\sum_{i=1}^{n} \overline{c}_{ii}$, also gleich der Spur der Reduktion. □

Satz 18.15. *Es sei R ein Zahlbereich mit Diskriminante $\triangle_R$. Es sei p eine Primzahl. Dann ist p genau dann ein Teiler von $\triangle_R$, wenn der Faserring zu R über p nicht reduziert ist.*

Beweis. Es sei $b_1, \ldots, b_n$ eine Ganzheitsbasis von R. Die Matrix M mit den Einträgen $\text{Spur}\,(b_i b_j)$ ist die Gramsche Matrix der Spurform. Die Gramsche Matrix M' der Spurform zu $R/(p)$ über $\mathbb{Z}/(p)$ bezüglich der $\mathbb{Z}/(p)$-Basis $\overline{b}_1, \ldots, \overline{b}_n$ entsteht daraus nach Lemma 18.14 durch komponentenweise Reduktion. Da das Berechnen der Determinante mit beliebigen Ringwechseln verträglich ist, ist die Determinante von M' gleich der Determinante von M (also der Diskriminante von R) modulo p genommen. Somit ist p genau dann ein Teiler der Diskriminante von R, wenn die Diskriminante des Faserringes gleich 0 ist. Dies ist nach Satz 18.13 äquivalent dazu, dass der Faserring nicht reduziert ist. □

18. Arbeitsblatt

18.1. **Aufgaben.**

In den nächsten Aufgaben verwenden wir die folgende Definition.

Ein Körper K heißt *vollkommen*, wenn jedes irreduzible Polynom $P \in K[X]$ separabel ist.

Aufgabe 18.1. Es sei K ein vollkommener Körper und $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass $K \subseteq L$ eine separable Körpererweiterung ist.

Aufgabe 18.2. Zeige, dass jeder Körper der Charakteristik 0 vollkommen ist.

Aufgabe 18.3. Zeige, dass jeder algebraisch abgeschlossene Körper vollkommen ist.

Aufgabe 18.4. Zeige, dass ein endlicher Körper vollkommen ist.

Aufgabe 18.5.*

Es sei K ein Körper der Charakteristik p. Zeige, dass K genau dann vollkommen ist, wenn der Frobeniushomomorphismus auf K surjektiv ist.

Aufgabe 18.6. Zeige, dass der Körper $\mathbb{F}_p(X)$ der rationalen Funktionen nicht vollkommen ist.

Aufgabe 18.7. Zeige mit Hilfe der Ableitung, dass der Zahlbereich

$$S = \mathbb{Z}[X]/\big(X^3 - 3X + 1\big)$$

für $p = 2, 5$ nicht verzweigt und für $p = 3$ verzweigt ist.

Aufgabe 18.8.*

Zeige mit Hilfe der Ableitung, dass der Zahlbereich

$$S = \mathbb{Z}[Y]/\big(Y^4 - Y^3 - 4Y^2 + 4Y + 1\big)$$

für $p = 2$ nicht verzweigt und für $p = 3, 5$ verzweigt ist.

Aufgabe 18.9.*

Sei $F = X^3 + 2X - 1 \in \mathbb{Z}[X]$.

(1) Zeige, dass F und F' in $\mathbb{Q}[X]$ das Einheitsideal erzeugen. Man gebe explizit eine Darstellung der 1 an.
(2) Zeige, dass das von F und F' erzeugte Ideal in $\mathbb{Z}[X]$ eine minimale positive ganze Zahl $n > 0$ enthält.
(3) Bestimme, für welche Primzahlen p der Faserring

$$\mathbb{Z}/(p)[X]/\big(X^3 + 2X - 1\big)$$

reduziert ist.
(4) Bestimme für diejenigen Primzahlen p, für die der Faserring nicht reduziert ist, die Primfaktorzerlegung von $X^3 + 2X - 1$ in $\mathbb{Z}/(p)[X]$.
(5) Ist $R = \mathbb{Z}[X]/(X^3 + 2X - 1)$ ein Zahlbereich?

Aufgabe 18.10. Es seien $R \subseteq S$ und $S \subseteq T$ endliche Erweiterungen von Dedekindbereichen. Es sei $\mathfrak{p}$ ein Primideal von R, das in S verzweigt. Zeige, dass dann $\mathfrak{p}$ auch in T verzweigt.

Aufgabe 18.11. Es seien $S \subseteq T$ ineinander enthaltene Zahlbereiche. Zeige, dass ein Primteiler der Diskriminante von S auch ein Teiler der Diskriminante von T ist.

Aufgabe 18.12. Es sei R der p-te Kreisteilungsring zu einer ungeraden Primzahl p. Zeige unter Verwendung von Aufgabe 17.20, Aufgabe 18.11, Lemma 17.16 und Lemma 9.9, dass R die Quadratwurzel aus $(-1)^{(p-1)/2}p$ enthält.

19. Vorlesung - Differentiale und Verzweigung

19.1. **Kähler-Differentiale.**

Wir besprechen eine weitere Möglichkeit, Verzweigung zu erfassen, nämlich mit der Hilfe von Kähler-Differentialen. Dies ist ein sehr allgemeines Konzept, das dazu dient, die geometrische Idee eines Tangentialraumes bzw. Tangentialbündels algebraisch zu realisieren. Wir erwähnen hier nur die Grundzüge der Konstruktion und die wesentlichen Eigenschaften ohne Beweis. Beweise finden sich im Anhang.

Definition 19.1. Es sei R ein kommutativer Ring und A eine kommutative R-Algebra. Der von allen Symbolen $d(a)$, $a \in A$, erzeugte A-Modul, modulo den Identifizierungen

$$d(ab) = ad(b) + bd(a) \text{ für alle } a, b \in A$$

und

$$d(ra + sb) = rd(a) + sd(b) \text{ für alle } r, s \in R \text{ und } a, b \in A\,,$$

heißt *Modul der Kähler-Differentiale* von A über R. Er wird mit

$$\Omega_{A|R}$$

bezeichnet.

Bei dieser Konstruktion startet man also mit dem freien A-Modul F mit da, $a \in A$ als Basis und bildet den A-Restklassenmodul zu demjenigen Untermodul, der von den Elementen

$$d(ab) - ad(b) - bd(a)\,(a, b \in A)$$

und

$$d(ra + sb) - rd(a) - sd(b)\,(r, s \in R \text{ und } a, b \in A)$$

erzeugt wird. Die Abbildung

$$d\colon\ A \longrightarrow \Omega_{A|R},\ a \longmapsto d(a) = da,$$

heißt die *universelle Derivation*. Man prüft sofort nach, dass es sich um eine R-Derivation handelt.

Grundlage für konkrete Berechnungen bilden die folgenden Lemmata.

Lemma 19.2. *Es sei R ein kommutativer Ring und $A = R[X_1, \ldots, X_n]$ der Polynomring in n Variablen über R. Dann ist der Modul der Kähler-Differentiale der freie A-Modul zur Basis*

$$dX_1, dX_2, \ldots, dX_n\,.$$

Die universelle Derivation ist bezüglich dieser Basis durch

$$A \longrightarrow AdX_1 \oplus \cdots \oplus AdX_n,\ F \longmapsto dF = \frac{\partial F}{\partial X_1}dX_1 + \cdots + \frac{\partial F}{\partial X_n}dX_n,$$

gegeben.

Lemma 19.3. *Es sei R ein kommutativer Ring und es seien A und B kommutative R-Algebren und*

$$\varphi\colon\ A \longrightarrow B$$

ein R-Algebrahomomorphismus. Dann ist die Sequenz

$$\Omega_{A|R} \otimes_A B \longrightarrow \Omega_{B|R} \longrightarrow \Omega_{B|A} \longrightarrow 0$$

von B-Moduln exakt. Dabei geht $da \otimes b$ auf $bd\varphi(a)$ und db (in $\Omega_{B|R}$) auf db (in $\Omega_{B|A}$).

Lemma 19.4. *Es sei R ein kommutativer Ring und es sei A eine kommutative endlich erzeugte R-Algebra, die als*

$$A = R[X_1, \ldots, X_n]/(F_1, \ldots, F_k)$$

gegeben sei. Dann ist

$$\Omega_{A|R} = \bigoplus_{i=1}^{n} AdX_i/(dF_1, \ldots, dF_k).$$

Korollar 19.5. *Es sei K ein Körper, $P \in K[X]$ ein nichtkonstantes Polynom und*

$$K[Y] \longrightarrow K[X] \cong K[Y][X]/(Y - P(X)),\ Y \longmapsto P(X),$$

der zugehörige Einsetzungshomomorphismus. Dann gilt für den Modul der Kähler-Differentiale die Beschreibung

$$\Omega_{K[X]|K[Y]} \cong K[X]/(P').$$

Beweis. Nach Korollar 19.4 ist (mit $R = K[Y]$ und $A = R[X]/(Y - P(X))$)

$$\Omega_{K[X]|K[Y]} = \Omega_{K[Y][X]/(Y-P(X))|K[Y]} = K[X]/d(Y - P(X)) = K[X]/(P').$$

□

Diese Isomorphie ist so zu verstehen, dass die 1 in $K[X]/(P')$ dem Differential dX entspricht. Man könnte den Sachverhalt auch als die Gleichung

$$\Omega_{K[X]|K[Y]} = K[X]/(P')dX$$

ausdrücken.

Wenn K algebraisch abgeschlossen ist, so ist $P' = (X - a_1) \cdots (X - a_s)$ und $K[X]/(P') \cong K^s$. Die vorstehende Aussage zeigt somit insbesondere, dass der Modul der Kähler-Differentiale nur lokalisiert in den maximalen Idealen $(X - a_j)$, die den Nullstellen der Ableitung entsprechen, von 0 verschieden ist. Ein entsprechendes Verhalten gilt generell im Fall einer separablen Erweiterung von Dedekindbereichen.

Lemma 19.6. *Es sei $R \subseteq S$ eine endliche Erweiterung von Dedekindbereichen derart, dass die Körpererweiterung $Q(R) \subseteq Q(S)$ der Quotientenkörper separabel sei. Dann gelten folgende Aussagen.*

(1) *Es ist $\left(\Omega_{S|R}\right)_{S\setminus\{0\}} = 0$.*

(2) *Es gibt ein* $s \in S$, $s \neq 0$, *mit* $\big(\Omega_{S|R}\big)_s = 0$.
(3) *Es gibt ein* $r \in R$, $r \neq 0$, *mit* $\big(\Omega_{S|R}\big)_r = 0$.
(4) *Es gibt endlich viele Primideale* $\mathfrak{q} \in \operatorname{Spek}(S)$ *mit* $\big(\Omega_{S|R}\big)_{\mathfrak{q}} \neq 0$.
(5) *Es gibt ein* $r \in R$, $r \neq 0$, *und ein* $m \in \mathbb{N}$ *mit* $r^m\big(\Omega_{S|R}\big) = 0$. *Insbesondere ist* $\Omega_{S|R}$ *ein* S/r^mS*-Modul.*

Beweis. (1) Nach Lemma Anhang 9.6 ist

$$\big(\Omega_{S|R}\big)_{S\setminus\{0\}} = \Omega_{Q(S)|R} = \Omega_{Q(S)|Q(R)}.$$

Somit folgt die Aussage aus dem Satz vom primitiven Element in Verbindung mit Korollar 19.4.
(2) Folgt aus (1) aufgrund der endlichen Erzeugtheit von $\Omega_{S|R}$.
(3) Folgt aus (2), man kann für r die Norm von s nehmen, die ja nach Korollar 10.8 (im zahlentheoretischen Kontext) ein Vielfaches von s ist.
(4) Folgt aus (2) und daraus, dass es in einem Dedekindbereich nur endlich viele Primideale oberhalb eines Elementes $\neq 0$ gibt.
(5) Folgt aus (3) und der endlichen Erzeugtheit.

□

In der Aussage Lemma 19.6 (5) könnte man auf den Exponenten m verzichten, wenn man r abändert. Aber aus Teil (3) ergibt sich die Aussage mit dem Exponenten. Man denke bei r an eine Primzahl aus $\mathbb{Z}$, man versucht dann, eine annullierende Potenz mit einem möglichst kleinen Exponenten zu finden.

Lemma 19.7. *Es sei* $D \neq 0, 1$ *eine quadratfreie Zahl und* R *der zugehörige quadratische Zahlbereich. Dann ist*

$$\Omega_{R|\mathbb{Z}} \cong R/\Big(2\sqrt{D}\Big)$$

bei $D = 2, 3 \mod 4$ *und*

$$\Omega_{R|\mathbb{Z}} \cong R/\Big(\sqrt{D}\Big)$$

bei $D = 1 \mod 4$.

Beweis. Im ersten Fall ist nach Satz 9.8 $R \cong \mathbb{Z}[X]/(X^2 - D)$ und daher nach Korollar 19.4

$$\Omega_{R|\mathbb{Z}} = RdX/d\big(X^2 - D\big) = RdX/2XdX \cong R/2X = R/2\sqrt{D}.$$

Im zweiten Fall ist

$$R \cong \mathbb{Z}[Y]/\left(Y^2 - Y - \frac{D-1}{4}\right)$$

mit $Y = \frac{1+\sqrt{D}}{2}$. Somit ist

$$\begin{aligned}\Omega_{R|\mathbb{Z}} &= RdY/d\left(Y^2 - Y - \frac{D-1}{4}\right)\\ &= RdY/(2Y-1)dY\\ &= RdY/\sqrt{D}dY\\ &\cong R/\sqrt{D}.\end{aligned}$$

□

Beispiel 19.8. Es sei p eine Primzahl und R der p-te Kreisteilungsring, also

$$R = \mathbb{Z}[X]/\big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\big)$$

nach Lemma 17.14. Nach Korollar 19.4 ist der Modul der Kähler-Differentiale gleich

$$\begin{aligned}\Omega_{R|\mathbb{Z}} &\cong R/\big((p-1)X^{p-2} + (p-2)X^{p-2} + \cdots + 3X^2 + 2X + 1\big)\\ &\cong \mathbb{Z}[X]/\big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1,\\ &\qquad (p-1)X^{p-2} + (p-2)X^{p-3} + \cdots + 3X^2 + 2X + 1\big).\end{aligned}$$

Das beschreibende Ideal ist auf den ersten Blick schwer zu durchschauen. Da $X^p - 1$ zum Ideal des Kreisteilungsringes gehört, gehört auch die Ableitung zum beschreibenden Ideal des Kählermoduls. Es ist ja

$$X^p - 1 = (X-1)\big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\big)$$

und somit

$$\begin{aligned}pX^{p-1}dX &= d(X^p - 1)\\ &= d\big((X-1)\big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\big)\big)\\ &= \big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\big)dX + (X-1)\\ &\qquad \big((p-1)X^{p-2} + (p-2)X^{p-3} + \cdots + 3X^2 + 2X + 1\big)dX.\end{aligned}$$

Damit ist insbesondere

$$pdX = 0$$

in $\Omega_{R_p|\mathbb{Z}}$, da ja X eine Einheit ist. Somit ist der Kählermodul ein R_p/pR_p-Modul und insbesondere ein $\mathbb{Z}/(p)$-Modul. Daher und wegen Lemma Anhang 9.11 ist

$$\Omega_{R_p|\mathbb{Z}} = \Omega_{R_p|\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}/(p) = \Omega_{R_p/pR_p|\mathbb{Z}/(p)}.$$

Da der Faserring über p die Form

$$R_p/pR_p = \mathbb{Z}/(p)[X]/\big((X-1)^{p-1}\big) = \mathbb{Z}/(p)[Y]/\big(Y^{p-1}\big)$$

besitzt, ist wegen $(Y^{p-1})' = -Y^{p-2}$ insgesamt

$$\Omega_{R_p|\mathbb{Z}} = \Omega_{\mathbb{Z}/(p)[Y]/(Y^{p-1})|\mathbb{Z}/(p)} \cong \mathbb{Z}/(p)[Y]/\big(Y^{p-2}\big).$$

Dies ist ein freier $\mathbb{Z}/(p)$-Modul mit der (in X geschriebenen) Basis $dX, XdX, \ldots, X^{p-3}dX$ (also vom Rang $p-2$).

Beispiel 19.9. Es sei p eine Primzahl und $R = \mathbb{Z}[X]/(X^p - p)$, vergleiche Beispiel 18.11. Der Modul der Kähler-Differentiale ist

$$\Omega_{R|\mathbb{Z}} = R/\big(px^{p-1}\big)dx$$

und das annullierende Ideal ist

$$\big(px^{p-1}\big) = \big(x^{2p-1}\big).$$

Die Norm von deshalb ist die Anzahl der Elemente im Modul der Kähler-Differentiale gleich p^{2p-1}.

Beispiel 19.10. Es sei $q = \pm 1 \mod 9$ eine Primzahl und $R = \mathbb{Z}[x,z] \subset \mathbb{Q}[X]/(X^3-q)$ mit $z = \frac{1+qx+x^2}{3}$ der Ganzheitsring, vergleiche Satz 16.1. Der Modul der Kähler-Differentiale wird als R-Modul von dx und dz erzeugt. Wir behaupten, dass der Erzeuger dz überflüssig ist, obwohl er als Algebraerzeuger nicht überflüssig ist. Dabei gilt

$$3dz = d3z = d\big(1+qx+x^2\big) = qdx + 2xdx = (q+2x)dx.$$

Ferner ist unter Verwendung von Aufgabe 16.7

$$xdz + zdx = dxz = d\left(\frac{1-q^2}{3}x + qz\right) = \frac{1-q^2}{3}dx + qdz,$$

woraus wir

$$(x-q)dz = -zdx - \frac{1-q^2}{3}dx = -\left(z + \frac{1-q^2}{3}\right)dx$$

gewinnen. Schließlich ist

$$2zdz = dz^2 = d\left(\frac{q^2-1}{9} + \frac{-q^3-q}{9}x + \frac{q^2+2}{3}z\right) = \frac{-q^3-q}{9}dx + \frac{q^2+2}{3}dz,$$

woraus wir

$$\left(2z - \frac{q^2+2}{3}\right)dz = \frac{-q^3-q}{9}dx$$

gewinnen. Wir können also verschiedene Vielfache von dz als Vielfache von dx ausdrücken. Wir betrachten das von den Vorfaktoren erzeugte Ideal in R, also

$$\left(3, x-q, 2z - \frac{q^2+2}{3}\right).$$

Dieses Ideal enthält $q^3 - q$ und Im Restklassenring wird also x zu q und z wird zu

$$\frac{1+qx+x^2}{3} = \frac{1+2q^2}{3}.$$

Somit enthält das Ideal die Zahlen $3, q^3-q$ und

$$2\frac{1+2q^2}{3} - \frac{q^2+2}{3} = q^2.$$

Da 3 und q teilerfremd ist, enthält es auch die 1 und somit gibt es auch eine Darstellung von dz als Vielfaches von dx.

19.2. **Verzweigung und Differentiale.**

Lemma 19.11. *Es sei K ein vollkommener Körper und A eine lokale endlichdimensionale K-Algebra. Dann ist A genau dann reduziert (also ein Körper) wenn der Modul der Kählerdifferentiale $\Omega_{A|K}$ gleich 0 ist.*

Beweis. Wenn R reduziert ist, so liegt eine endliche Körpererweiterung $K \subseteq A$ vor, die wegen der Vollkommenheit des Grundkörpers separabel ist und deshalb nach dem Satz vom primitiven Element von einem Elment erzeugt ist, sagen wir $A = K[x] = K[X]/(F)$. Nach Lemma Anhang 8.3 erzeugen F und F' das Einheitsideal und somit folgt aus $F'(x)dx = 0$, dass sogar $dx = 0$ ist. Somit folgt die Aussage aus Korollar 19.4.

Sei nun angenommen, dass A nicht reduziert ist. Es ist zu zeigen, dass es nichttriviale Kählerdifferentiale gibt. Da A eine lokale Algebra ist, ist ein Element darin entweder eine Einheit oder gehört zum maximalen Ideal. Zu einer Einheit $x \in A$, $x \notin K$, ist $K[x]$ ein Erweiterungskörper von K. Indem wir so den Grundkörper vergrößern, können wir wegen Lemma 19.3 annehmen, dass nur die Elemente aus $K \setminus 0$ Einheiten in A sind. Dann ist

$$A = K[x_1, \ldots, x_n]$$

und die x_i gehören zum maximalen Ideal $\mathfrak{m}$. Indem wir die Restklassenabbildung

$$A \longrightarrow A/\mathfrak{m}^2$$

betrachten und Lemma Anhang 9.8 heranziehen, können wir davon ausgehen, dass die Situation

$$A = K[X_1, \ldots, X_n]/(X_iX_j,\, 1 \leq i \leq j \leq n)$$

vorliegt, wobei mindestens ein Erzeuger $x_1 \neq 0$ ist. Mit dem gleichen Lemma können wir modulo $(x_2, \ldots, x_n)$ gehen und erhalten die Situation $K[X]/(X^2)$. Dafür zeigt Korollar 19.4, dass $dx \neq 0$ ist. □

Satz 19.12. *Es sei R ein Zahlbereich. Dann ist die Ringerweiterung $\mathbb{Z} \subseteq R$ in einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ genau dann verzweigt, wenn*

$$\left(\Omega_{R|\mathbb{Z}}\right)_{\mathfrak{q}} \neq 0$$

ist.

Beweis. Es sei $\mathfrak{p} = \mathbb{Z} \cap \mathfrak{q}$, und wir können wegen Lemma Anhang 9.6 direkt zu

$$B = \mathbb{Z}_{\mathfrak{p}} \longrightarrow A = R_{\mathbb{Z}\setminus\mathfrak{p}}$$

übergehen. Die Bedingung

$$\left(\Omega_{R|\mathbb{Z}}\right)_{\mathfrak{q}} = \left(\Omega_{A|B}\right)_{\mathfrak{q}} = \Omega_{A_{\mathfrak{q}}|B} \neq 0$$

ist äquivalent zu

$$\Omega_{A|B} \otimes_A A/\mathfrak{q} = \Omega_{A_{\mathfrak{q}}|B} \otimes_{A_{\mathfrak{q}}} A_{\mathfrak{q}}/\mathfrak{q} \neq 0,$$

da ja $\Omega_{A_\mathfrak{q}|B}$ ein endlicher erzeugter $A_\mathfrak{q}$-Modul über dem lokalen Ring $A_\mathfrak{q}$ ist. Wegen der natürlichen Surjektion

$$A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q} \longrightarrow A_\mathfrak{q}/\mathfrak{q}$$

ist dies auch äquivalent zu

$$\Omega_{A_\mathfrak{q}|B} \otimes_{A_\mathfrak{q}} A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q} \neq 0.$$

Nach Lemma Anhang 9.11 angewendet auf

$$\begin{array}{ccc} A_\mathfrak{q} & \longrightarrow & A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q} \\ \uparrow & & \uparrow \\ B & \longrightarrow & B/\mathfrak{p} = \kappa(\mathfrak{p}) \end{array}$$

ist

$$\Omega_{A_\mathfrak{q}|B} \otimes_{A_\mathfrak{q}} A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q} = \Omega_{A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q}|B/\mathfrak{p}}$$

und dies ist die Lokalisierung von $\Omega_{A/\mathfrak{p}|B/\mathfrak{p}}$ an $\mathfrak{q}$. Somit ist die Lokalisierung von $\Omega_{A|B}$ an $\mathfrak{q}$ genau dann von 0 verschieden, wenn $\Omega_{A/A\mathfrak{p}|B/\mathfrak{p}}$ lokalisiert an $\mathfrak{q}$ von 0 verschieden ist. Die Bedingung an den Modul der Kähler-Differentiale spielt sich somit allein in der speziellen Faser über $\mathfrak{p}$ ab. Nach (dem Beweis zu) Satz 18.10 liegt in $\mathfrak{q}$ genau dann Verzweigung vor, wenn $R/\mathfrak{q} = A/\mathfrak{q}$ nicht reduziert ist. Deshalb folgt die Aussage aus Lemma 19.11. □

19. Arbeitsblatt

19.1. **Aufgaben.**

Aufgabe 19.1. Bestimme $\Omega_{\mathbb{C}|\mathbb{R}}$.

Aufgabe 19.2. Es sei $K \subseteq L$ eine separable endliche Körpererweiterung. Zeige $\Omega_{L|K} = 0$.

Aufgabe 19.3. Bestimme $\Omega_{\mathbb{Z}[\mathrm{i}]|\mathbb{Z}}$.

Aufgabe 19.4. Es sei R ein kommutativer Ring und

$$A = R[X_1, \ldots, X_n]/(X_n - f(X_1, \ldots, X_{n-1}))$$

mit einem Polynom $f \in R[X_1, \ldots, X_{n-1}]$ (die Nullstellenmenge ist also der Graph zu f). Zeige auf zwei verschiedene Arten, dass $\Omega_{A|R}$ ein freier A-Modul vom Rang $n-1$ ist.

Aufgabe 19.5. Zeige, dass zu $R = K[X,Y]/(XY)$ der Modul der Kähler-Differentiale $\Omega_{R|K}$ im Nullpunkt nicht frei ist.

Aufgabe 19.6.*

Es sei A ein kommutativer Ring und $S \subseteq A$ ein multiplikatives System. Zeige

$$\Omega_{A_S|A} = 0.$$

Aufgabe 19.7. Es sei A ein kommutativer Ring und $S \subseteq A$ ein multiplikatives System. Es sei $A \subseteq B \subseteq A_S$ ein Zwischenring. Zeige

$$\Omega_{B|A} = 0.$$

Aufgabe 19.8. Es sei $K \subseteq L$ eine endliche separable Körpererweiterung und sei $K[X] \subseteq L[X]$ die zugehörige endliche Erweiterung der Polynomringe in einer Variablen. Zeige $\Omega_{L[X]|K[X]} = 0$.

Aufgabe 19.9. Interpretiere Lemma 19.3 für einen Grundkörper K und einen K-Algebrahomomorphismus

$$K[Y] \longrightarrow K[X],\ Y \longmapsto F(X),$$

Aufgabe 19.10. Es sei R ein kommutativer Ring und A eine kommutative R-Algebra. Zeige, dass der Kern der universellen Derivation

$$A \longrightarrow \Omega_{R|A},\ f \longmapsto df,$$

eine R-Unteralgebra von A ist.

Es sei R ein kommutativer Ring und M ein R-Modul. Zu einem Element $x \in M$ heißt

$$\operatorname{Ann}_R(x) = \{r \in R \mid rx = 0\}$$

der *Annullator* von x.

Es sei R ein kommutativer Ring und M ein R-Modul. Der *Annullator* von M ist

$$\operatorname{Ann}_R(M) = \{r \in R \mid rx = 0 \text{ für alle } x \in M\}.$$

Aufgabe 19.11. Es sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Zeige, dass der Annullator des R-Moduls $R/\mathfrak{a}$ gleich $\mathfrak{a}$ ist.

Aufgabe 19.12. Es sei R ein kommutativer Ring, M ein R-Modul und $I \subseteq R$ ein Ideal mit $IM = 0$. Zeige, dass M in natürlicher Weise ein R/I-Modul ist.

Aufgabe 19.13. Es sei $A = R[X]/\mathfrak{a}$ eine monogene R-Algebra und es sei $\mathfrak{b} = \operatorname{Ann}(dX)$ der Annullator von dX im Modul der Kähler-Differentiale $\Omega_{A|R}$. Zeige

$$\Omega_{A|R} \cong A/\mathfrak{b}.$$

Aufgabe 19.14. Es sei R ein Zahlbereich. Zeige, dass es eine natürliche Zahl $n \in \mathbb{N}_+$ gibt, die den Modul der Kähler-Differentiale $\Omega_{R|\mathbb{Z}}$ annulliert.

Aufgabe 19.15. Es sei R ein quadratischer Zahlbereich mit dem Modul der Kähler-Differentiale $\Omega_{R|\mathbb{Z}}$. Zeige, dass der Annullator von $\Omega_{R|\mathbb{Z}}$ von einem Element erzeugt wird, und dass die Norm eines solchen Erzeugers im Betrag mit der Diskriminante des Zahlbereiches übereinstimmt.

Aufgabe 19.16. Es sei A_D der quadratische Zahlbereich zur quadratfreien Zahl $D = 2, 3 \mod 4$. Zeige, dass die Elemente des Moduls der Kähler-Differentiale $\Omega_{A_D|\mathbb{Z}}$ gleich

$$(a + b\sqrt{D})d\sqrt{D},\ a = 0, 1, 2, \ldots, 2D - 1,\ b = 0, 1,$$

sind.

Aufgabe 19.17.*

Es sei A_D der quadratische Zahlbereich zur quadratfreien Zahl $D = 1 \mod 4$. Zeige, dass die Elemente des Moduls der Kähler-Differentiale $\Omega_{A_D|\mathbb{Z}}$ (mit $A_D = \mathbb{Z}[y]/\left(y^2 - y - \frac{D-1}{4}\right)$ gemäß Satz 9.8) gleich

$$ady,\ a = 0, 1, 2, \ldots, |D| - 1,$$

sind.

Aufgabe 19.18. Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung und $\mathbb{Z} \subseteq S \subseteq K$ eine Ringerweiterung mit $Q(S) = K$ und sei R der ganze Abschluss von S in K. Zeige, dass die natürliche Abbildung

$$\Omega_{S|\mathbb{Z}} \otimes_{\mathbb{Z}} R \longrightarrow \Omega_{R|\mathbb{Z}},\ ds \otimes r \longmapsto rds,$$

surjektiv ist.

Aufgabe 19.19. Es sei $D = 1 \mod 4$ eine quadratfreie Zahl $\neq 1$ und sei

$$S = \mathbb{Z}[\sqrt{D}] \subseteq R = \mathbb{Z}[\frac{1+\sqrt{D}}{2}].$$

Zeige, dass in $\Omega_{R|\mathbb{Z}}$ die Beziehung

$$\frac{1+\sqrt{D}}{2} d\sqrt{D} = d\frac{1+\sqrt{D}}{2}$$

gilt.

Aufgabe 19.20. Zeige anhand der Ringerweiterungen $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{-3}] = S \subseteq \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = R$, dass in Lemma 19.3 die Abbildung

$$\Omega_{S|\mathbb{Z}} \otimes_S R \longrightarrow \Omega_{R|\mathbb{Z}},\ ds \otimes r \longmapsto rds,$$

nicht injektiv sein muss.

Aufgabe 19.21. Wir betrachten den Modul der Kähler-Differentiale $\Omega_{\mathbb{Z}[\mathrm{i}]|\mathbb{Z}}$ zum Ring der Gaußschen Zahlen. Zeige, dass es zu dem Kähler-Differential

$$\omega = \mathrm{i}d\mathrm{i}$$

kein Element $f \in \mathbb{Z}[\mathrm{i}]$ mit $df = \omega$ gibt.

Aufgabe 19.22. Es sei A_D der quadratische Zahlbereich zur quadratfreien Zahl $D = 1 \mod 4$. Zeige, dass es zu jedem Kähler-Differential $\omega \in \Omega_{A_D|\mathbb{Z}}$ ein $f \in A_D$ mit

$$df = \omega$$

gibt.

Aufgabe 19.23.*

Bestimme zum Zahlbereich $\mathbb{Z} \subseteq R = \mathbb{Z}[X]/(X^3 - 3X + 1)$ den Modul der Kähler-Differentiale und den Verzweigungsort. Bestimme ferner die Anzahl der Elemente im Modul der Kähler-Differentiale.

Aufgabe 19.24.*

Es sei p eine ungerade Primzahl und

$$R_p = \mathbb{Z}[X]/\big(X^{p-1} + \cdots + X^2 + X + 1\big)$$

der p-te Kreisteilungsring. Zeige, dass im Modul der Kähler-Differentiale die Gleichheit

$$X^{p-2}dX = \left(\sum_{k=0}^{p-3}(k+1)X^k\right)dX$$

gilt.

Aufgabe 19.25.*

Es sei p eine ungerade Primzahl,

$$R_p = \mathbb{Z}[X]/\big(X^{p-1} + \cdots + X^2 + X + 1\big)$$

R_p der p-te Kreisteilungsring mit dem Modul der Kähler-Differentiale (vergleiche Beispiel 19.8)

$$\Omega_{R_p|\mathbb{Z}} \cong \mathbb{Z}/(p)[X]/(X-1)^{p-2}dX.$$

Zeige, dass es zu jedem Kähler-Differential

$$\omega = \big(a_{p-3}X^{p-3} + \cdots + a_2X^2 + a_1X + a_0\big)dX$$

mit $0 \leq a_j < p$ ein $f \in R_p$ mit $df = \omega$ gibt.

Aufgabe 19.26. Es sei $\mathbb{Z} \subseteq R = \mathbb{Z}[X](X^n - a)$ eine reine Wurzelerweiterung von $\mathbb{Z}$. Zeige, dass der Modul der Kähler-Differentiale $\Omega_{R|\mathbb{Z}}$ durch an annulliert wird.

Aufgabe 19.27.*

Es sei $R_8 = \mathbb{Z}[X]/(X^4+1)$ der achte Kreisteilungsring. Zeige, dass der Modul der Kähler-Differentiale $\Omega_{R_8|\mathbb{Z}}$ von 4 annulliert wird, aber nicht von 2. Beschreibe die Modulstruktur von $\Omega_{R_8|\mathbb{Z}}$.

Aufgabe 19.28.*

Beschreibe den Modul der Kähler-Differentiale $\Omega_{R_9|\mathbb{Z}}$ und bestimme insbesondere seine Anzahl, wobei $R_9 = \mathbb{Z}[Y]/(Y^6+Y^3+1)$ den neunten Kreisteilungsring bezeichnet.

Dabei ist Aufgabe 2.31 hilfreich.

Aufgabe 19.29.*

Beschreibe den Modul der Kähler-Differentiale $\Omega_{R_9|R_3}$ und bestimme insbesondere seine Anzahl, wobei R_n den n-ten Kreisteilungsring bezeichnet.

Aufgabe 19.30.*

Studiere Lemma 19.3 am Beispiel der Kreisteilungsringe $\mathbb{Z} \subseteq R_3 \subseteq R_9$.

Aufgabe 19.31.*

Es sei p eine Primzahl und $r \geq 1$. Beschreibe den Modul der Kähler-Differentiale $\Omega_{R_{p^r}|R_p}$ und bestimme insbesondere seine Anzahl, wobei R_n den n-ten Kreisteilungsring bezeichnet.

Aufgabe 19.32. Es sei p eine Primzahl und R_p der p-te Kreisteilungsring. Bestimme den Kern der universellen Derivation

$$d\colon\ R_p \longrightarrow \Omega_{R_p|\mathbb{Z}},\ f \longmapsto df.$$

Aufgabe 19.33. Es sei R ein Zahlbereich und sei $S \subseteq R$ der Kern der universellen Derivation

$$d\colon\ R \longrightarrow \Omega_{R|\mathbb{Z}},\ f \longmapsto df.$$

Zeige, dass der Quotientenkörper von S gleich $Q(R)$ ist.

Aufgabe 19.34.*

Es sei

$$R = A_{-15} = \mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$$

der quadratische Zahlbereich zu -15 und S der Zahlbereich zu $\mathbb{Q}[\sqrt{3},\sqrt{-5}]$, der R enthält. Zeige

$$\Omega_{S|R} = 0.$$

20. Vorlesung - Zerlegungsverhalten

20.1. **Zerlegungsverhalten.**

Wir besprechen nun systematisch, wie eine Primzahl p in einem Zahlbereich R zerlegt wird, also wie viele Primideale von R oberhalb von (p) liegen, wie diese sich zueinander verhalten und wie die Abhängigkeit von p aussieht. Viele Eigenschaften hängen dabei allein vom Faserring R/pR ab, von dem wir nach Korollar 8.8 wissen, dass R/pR als additive Gruppe isomorph zu $(\mathbb{Z}/(p))^n$ ist, wenn n der Grad der Erweiterung ist.

Definition 20.1. Es sei $R \subseteq S$ eine endliche Erweiterung von kommutativen Ringen, sei $\mathfrak{p}$ ein Primideal von R und $\mathfrak{q}$ ein Primideal von S über $\mathfrak{p}$. Dann nennt man den Grad der Erweiterung der Restekörper $\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q})$ den *Trägheitsgrad* von $\mathfrak{q}$ über $\mathfrak{p}$.

Bemerkung 20.2. Wenn $R \subseteq S$ eine endliche Erweiterung von Dedekindbereichen ist und $\mathfrak{m}$ ein maximales Ideal von R ist und $\mathfrak{n}$ ein maximales Ideal von S über $\mathfrak{m}$, so ist der Trägheitsgrad einfach der Grad der Körpererweiterung

$$R/\mathfrak{m} \longrightarrow S/\mathfrak{n}$$

(der Trägheitsgrad im Nullideal ist einfach der Grad der Erweiterung der Quotientenkörper). Wenn R und damit auch S ein Zahlbereich ist, so sind diese Körper stets endlich von gleicher Charakteristik p, und daher liegt eine Erweiterung der Form $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ mit $q = p^e$ und $q' = p^{e'}$ vor.

Lemma 20.3. *Es sei R ein kommutativer Ring und $R \subseteq S$ eine endliche Erweiterung der Form $S = R[X]/(F)$ mit einem normierten Polynom $F \in R[X]$ vom Grad d. Es sei $\mathfrak{p}$ ein Primideal von R. Dann ist die Summe über alle Trägheitsgrade zu Primidealen über $\mathfrak{p}$ durch d beschränkt.*

Beweis. Durch Übergang mittels $R \to \kappa(\mathfrak{p})$ kann man direkt annehmen, dass $R = K$ ein Körper ist und dass das Primideal das Nullideal ist. Es liegt dann die endliche Erweiterung $K \subseteq K[X]/(F) =: B$ vor. Die Primideale von S oberhalb von $\mathfrak{p}$ entsprechen den Primidealen von B und damit den irreduziblen Teilern von F in $K[X]$. Sei $F = F_1^{n_1} \cdots F_k^{n_k}$ die Primfaktorzerlegung von F in $K[X]$. Die relevanten Körpererweiterungen sind dann die

$$K \subseteq K[X]/(F_j).$$

Die Aussage folgt daher direkt aus Gradeigenschaften von Polynomen über einem Körper. □

Satz 20.4. *Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Körpererweiterung vom Grad n und S der ganze Abschluss von R in L. Es sei $\mathfrak{p}$ ein von 0 verschiedenes Primideal von R mit der Primidealzerlegung*

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_k^{e_k}$$

in S. Die Körpererweiterungen $\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q}_j)$ haben die Trägheitsgrade f_j. Dann ist

$$n = \sum_{j=1}^{k} e_j f_j.$$

Beweis. Nach dem chinesischen Restsatz für Dedekindbereiche ist

$$S/\mathfrak{p}S = S/\mathfrak{q}_1^{e_1} \times \cdots \times S/\mathfrak{q}_k^{e_k}.$$

Wir können über dem diskreten Bewertungsring $R_{\mathfrak{p}}$ argumentieren, also davon ausgehen, dass R ein diskreter Bewertungsring mit dem maximalen Ideal $\mathfrak{p}$ ist. Die angeführten Restklassenringe ändern sich dadurch nicht. Es ist S ein freier R-Modul vom Rang n und somit ist

$$S/\mathfrak{p}S = S \otimes_R R/\mathfrak{p}$$

ein $R/\mathfrak{p}$-Vektorraum der Dimension n. Oben rechts steht das Produkt der $R/\mathfrak{p}$-Vektorräume $S/\mathfrak{q}_j^{e_j}$ und es ist zu zeigen, dass deren $R/\mathfrak{p}$-Dimension gleich $e_j f_j$ ist. Dies zeigen wir durch Induktion über $e = e_j$, wobei der Induktionsanfang für $e = 1$ die Definition des Trägheitsgrades f_j ist. Wegen $\mathfrak{q}^{e+1} \subseteq \mathfrak{q}^e$ liegt eine kurze exakte Sequenz

$$0 \longrightarrow \mathfrak{q}^e/\mathfrak{q}^{e+1} \longrightarrow S/\mathfrak{q}^{e+1} \longrightarrow S/\mathfrak{q}^e \longrightarrow 0$$

vor. Dabei ist

$$\mathfrak{q}^e/\mathfrak{q}^{e+1} = \mathfrak{q}^e S_{\mathfrak{q}}/\mathfrak{q}^{e+1}S_{\mathfrak{q}} = S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}} = S/\mathfrak{q}.$$

Deshalb folgt die Aussage aufgrund der Vektorraumadditivität in kurzen exakten Sequenzen. □

Die in diesem Satz auftretende Gleichung nennt man auch *fundamentale Gleichung*. Nach Lemma 18.3 liegt genau dann Verzweigung oberhalb von $\mathfrak{p}$ vor, wenn einer der Verzweigungsindizes e_j größer als 1 ist.

Die beiden extremen Möglichkeiten für das Zerlegungsverhalten bekommen einen eigenen Namen.

Definition 20.5. Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Körpererweiterung vom Grad n und S der ganze Abschluss von R in L. Ein von 0 verschiedenes Primideal $\mathfrak{p}$ von R heißt *voll zerlegt* in S, wenn es n Primideale in S oberhalb von $\mathfrak{p}$ gibt.

Im voll zerlegten Fall ist $e_j = f_j = 1$ für $j = 1, \ldots, n$. Es liegt keine Verzweigung von und alle Restekörper stimmen mit dem Grundkörper $R/\mathfrak{p}$ überein.

Definition 20.6. Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Körpererweiterung vom Grad n und S der ganze Abschluss von R in L. Ein von 0 verschiedenes Primideal $\mathfrak{p}$ von R heißt *unzerlegt* in S, wenn es genau ein Primideal in S oberhalb von $\mathfrak{p}$ gibt.

In diesem Fall ist $n = ef$.

Beispiel 20.7. Wir betrachten die Ringerweiterung $\mathbb{R}[X] \subset \mathbb{C}[X]$. Auf der Ebene der Quotientenkörper liegt die quadratische Körpererweiterung der zugehörigen Funktionenkörper $\mathbb{R}(X) \subset \mathbb{C}(X)$ vor, und $\mathbb{C}[X]$ ist der ganze Abschluss von $\mathbb{R}[X]$ in $\mathbb{C}(X)$. Die Primideale $\neq 0$ von $\mathbb{R}[X]$ sind von der Form $(X-a)$ mit $a \in \mathbb{R}$ oder von der Form (X^2+bX+c) mit einem quadratischen Polynom ohne reelle Nullstelle. Die Restekörper in diesem zweiten Fall sind isomorph zu $\mathbb{C}$. Die Primideale in $\mathbb{C}[X]$ sind alle von der Form $(X-a)$ mit $a \in \mathbb{C}$.

In der Erweiterung liegt über dem Primideal $(X-a)$ das entsprechende Ideal, dieses Ideal ist also unzerlegt, die Verzweigungsordnung ist 1 und die Restekörpererweiterung ist $\mathbb{R} \subset \mathbb{C}$, der Trägheitsgrad ist also 2. Zu einem Primideal (X^2+bX+c) zu einem Polynom ohne reelle Nullstelle seien z und $\overline{z}$ die zueinander konjugierten komplexen Nullstellen. In $\mathbb{C}[X]$ gilt die Idealzerlegung $(X^2+bX+c) = (X-z)(X-\overline{z})$. Die Verzweigungsordnungen sind also 1 und in den Restekörpern liegt ein Isomorphismus vor, die Trägheitsgrade sind also 1. Diese Primideale sind voll zerlegt.

Beispiel 20.8. Es sei $R = \mathbb{Z}[X]/(X^4+X^3+X^2+X+1) = \mathbb{Z}[x]$. Wir beschreiben exemplarisch das Verhalten von Primzahlen in diesem Zahlbereich. Sei zuerst $q = 5$. Hier ist über $\mathbb{Z}/(5)$

$$(X-1)(X^4+X^3+X^2+X+1) = X^5-1 = (X-1)^5$$

und somit $X^4+X^3+X^2+X+1 = (X-1)^4$. Es gibt also nur ein Primideal oberhalb von (5) und dessen Restklassenkörper ist $\mathbb{Z}/(5)$, der Trägheitsgrad ist also 1 und der Verzweigungsindex ist 4.

Das Zerlegungsverhalten der anderen Primzahlen $q \neq 5$ versuchen wir mit Hilfe eines Zwischenringes zu verstehen. Sei

$$v = x - x^2 - x^3 + x^4.$$

Eine direkte Rechnung (siehe Beispiel 17.5) zeigt $v^2 = 5$, d.h. es liegt ein Zwischenring

$$\mathbb{Z} \subset \mathbb{Z}[\sqrt{5}] \subset \mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathbb{Z}[x^3+x^2] = S \subset \mathbb{Z}[x]$$

vor, wobei der Ganzheitsring zu $\sqrt{5}$ mit Satz 9.8 bestimmt wurde.

Für

$$q = 1, 4 \mod 5$$

ist 5 ein Quadrat modulo q. Über diesen Primzahlen liegen in S zwei Primideale, beide mit dem Restekörper $\mathbb{Z}/(q)$ und dem Trägheitsgrad 1. Über diesen Primzahlen zerfällt das fünfte Kreisteilungspolynom in zwei Faktoren vom Grad 2. Ob es weiter in Linearfaktoren zerfällt, hängt von q ab.

Bei $q = 11$ sind $1, 3, 4, 5, 9$ fünfte Einheitswurzeln in $\mathbb{Z}/(11)$ und das Kreisteilungspolynom hat die Zerlegung

$$X^4 + X^3 + X^2 + X + 1 = (X-3)(X+2)(X-4)(X-5).$$

Über (11) liegen also vier Primideale, jeweils mit dem Trägheitsgrad 1. Ein entsprechendes Verhalten gilt für alle Primzahlen q mit $q = 1 \mod 5$ nach Korollar 23.3.

Bei $q = 4 \mod 5$ gibt es nur die 1 als fünfte Einheitswurzel und es gilt

$$X^4 + X^3 + X^2 + X + 1 = \left(X^2 + \frac{\sqrt{5}+1}{2}X + 1\right)\left(X^2 - \frac{\sqrt{5}-1}{2}X + 1\right),$$

wobei für $\sqrt{5}$ eine Quadratwurzel von 5 aus $\mathbb{Z}/(q)$ einzusetzen ist. Bei $q = 19$ ist beispielsweise $9^2 = 5$ und daher ist

$$X^4 + X^3 + X^2 + X + 1 = \big(X^2 + 5X + 1\big)\big(X^2 + 15X + 1\big).$$

Bei $q = 3 \mod 5$

Es ist einfach Beispiele von Zahlbereichen anzugeben, in denen jedes Primideal des Grundringes zerlegt (also nicht unzerlegt) ist. Für das folgende Beispiel siehe auch Korollar 22.9.

Beispiel 20.9. Es seien $a, b \in \mathbb{Z}$ verschiedene quadratfreie Zahlen, sei

$$\mathbb{Q} \subset L = \mathbb{Q}[\sqrt{a}, \sqrt{b}]$$

die zugehörige Körpererweiterung vom Grad 4 und sei

$$T = \mathbb{Z}[\sqrt{a}, \sqrt{b}] \subseteq S$$

der Ganzheitsring von $\mathbb{Z}$ in L, wobei für dieses Beispiel der Unterschied zwischen T und S irrelevant ist. Wir bestimmen die Faser über einem Primideal zu einer Primzahl p. Der beschreibende Ring ist

$$T\otimes_{\mathbb{Z}}\mathbb{Z}/(p) \,=\, \mathbb{Z}[X,Y]/(X^2-a,Y^2-b)\otimes_{\mathbb{Z}}\mathbb{Z}/(p) \,=\, \mathbb{Z}/(p)[X,Y]/(X^2-a,Y^2-b).$$

Wir beschränken uns auf Primzahlen ≥ 3, die weder a noch b teilen, was bedeutet, dass die zugehörigen Restklassen Einheiten in $\mathbb{Z}/(p)$ sind. Wenn a (entsprechend für b) ein Quadrat in $\mathbb{Z}/(p)$ ist, sagen wir

$$a \,=\, r^2 \,=\, (-r)^2,$$

so ist

$$\begin{array}{rl} & \mathbb{Z}/(p)[X,Y]/(X^2-a,Y^2-b) \\ = & \mathbb{Z}/(p)[X,Y]/((X-r)(X+r),Y^2-b) \\ = & (\mathbb{Z}/(p)[Y]/(Y^2-b))[X]/((X-r)(X+r)) \\ = & (\mathbb{Z}/(p)[Y]/(Y^2-b))\times(\mathbb{Z}/(p)[Y]/(Y^2-b)), \end{array}$$

wobei die letzte Identifizierung durch $X\mapsto(r,-r)$ gegeben ist. Der Faserring ist also ein Produktring und kein Körper und (p) zerfällt in T und dann auch in S in zumindest zwei Primideale.

Wenn hingegen sowohl a als auch b Nichtquadrate in $\mathbb{Z}/(p)$ sind, so ist das Produkt ab ein Quadrat, sagen wir $ab \,=\, s^2 \,=\, (-s)^2$. Dann gelten, da ja a eine Einheit ist, in $\mathbb{Z}/(p)[X,Y]$ die Idealgleichheiten

$$\begin{array}{rcl} (X^2-a,Y^2-b) & = & (X^2-a,aY^2-ab) \\ & = & (X^2-a,aY^2-s^2) \\ & = & (X^2-a,X^2Y^2-s^2) \\ & = & (X^2-a,(XY-s)(XY-s)) \end{array}$$

und damit ist

$$\begin{array}{rcl} \mathbb{Z}/(p)[X,Y]/(X^2-a,Y^2-b) & = & \mathbb{Z}/(p)[X,Y]/(X^2-a,(XY-s)(XY-s)) \\ & = & (\mathbb{Z}/(p)[X]/(X^2-a))[Y]/(XY-s)(XY-s) \\ & = & (\mathbb{Z}/(p)[X]/(X^2-a))[Y]/\Big(Y-\frac{s}{X}\Big)\Big(Y-\frac{s}{X}\Big) \\ & = & (\mathbb{Z}/(p)[X]/(X^2-a))\times(\mathbb{Z}/(p)[X]/(X^2-a)), \end{array}$$

es liegt also wieder ein Produktring vor.

20. Arbeitsblatt

20.1. **Aufgaben.**

Aufgabe 20.1. Es sei $R\subseteq S$ eine endliche Erweiterung von kommutativen Ringen, sei $\mathfrak{p}$ ein Primideal von R und $\mathfrak{q}$ ein Primideal von S über $\mathfrak{p}$. Zeige, dass eine endliche Körpererweiterung der Restekörper $\kappa(\mathfrak{p})\subseteq\kappa(\mathfrak{q})$ vorliegt.

Aufgabe 20.2. Zeige, dass bei einem quadratischen Zahlbereich jedes numerisch mögliche Zerlegungsverhalten im Sinne der fundamentalen Gleichung auch auftritt.

Aufgabe 20.3. Es sei $K \subseteq L$ eine endliche separable Körpererweiterung und sei $K[X] \subseteq L[X]$ die zugehörige endliche Erweiterung der Polynomringe in einer Variablen. Beweise die fundamentale Gleichung in diesem Fall.

Aufgabe 20.4. Bestimme für den kubischen Zahlbereich $\mathbb{Z}[\sqrt[3]{2}]$, welche der numerisch möglichen Zerlegungsverhalten im Sinne der fundamentalen Gleichung wirklich auftreten.

Aufgabe 20.5. Bestimme das Zerlegungsverhalten von Primzahlen in dem durch die biquadratische Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}, \sqrt{5}]$$

gegebenen Zahlbereich.

21. Vorlesung - Invariantenringe

21.1. **Invariantenringe.**

Es sei $\mathbb{Q} \subseteq L$ eine endliche Körpererweiterung und $\mathbb{Z} \subseteq R$ der zugehörige Zahlbereich. Welche Besonderheiten gelten für R, wenn die Körpererweiterung eine Galoiserweiterung ist, wenn also die Anzahl der $\mathbb{Q}$-Algebraautomorphismen von L mit dem Grad der Erweiterung übereinstimmt. Wir werden gleich sehen, dass die Körperautomorphismen auf R Ringautomorphismen induzieren und dass daher die Galoisgruppe auch auf R operiert. Dies bewirkt, dass es auf R bzw. $\operatorname{Spek}(R)$ Symmetrien gibt. Wir fixieren einige Sprechweisen. Unter der Operation einer Gruppe G auf einem kommutativen Ring als Gruppe von Ringautomorphismen versteht man einen Gruppenhomomorphismus $G \to \operatorname{Aut} R$.

Definition 21.1. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiert (von rechts). Dann bezeichnet man

$$R^G = \{f \in R \mid f\sigma = f \text{ für alle } \sigma \in G\}$$

als den *Invariantenring* (oder *Fixring*) von R unter der Operation von G.

Dies ist eine Verallgemeinerung des aus der Galoistheorie bekannten Konzeptes eines Fixkörpers. Eine endliche Körpererweiterung ist nach Satz 16.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) genau dann galoissch, wenn der Fixkörper von L unter der Operation der Galoisgruppe $\operatorname{Gal}(L|K)$ gleich K ist.

Satz 21.2. *Es sei R ein normaler Integritätsbereich mit Quotientenkörper K und sei $K \subseteq L$ eine Galoiserweiterung. Es sei S der ganze Abschluss von R in L. Dann operiert die Galoisgruppe $G = \mathrm{Gal}\,(L|K)$ auf S mit Invariantenring R.*

Beweis. Es sei $\sigma \in G$ und $f \in S$. Es sei

$$0 = f^n + r_{n-1}f^{n-1} + \cdots + r_2 f^2 + r_1 f + r_0$$

eine Ganzheitsgleichung für f über R. Dann ist

$$\begin{aligned} 0 &= \sigma\big(f^n + r_{n-1}f^{n-1} + \cdots + r_2 f^2 + r_1 f + r_0\big) \\ &= \sigma(f)^n + \sigma(r_{n-1})\sigma(f)^{n-1} + \cdots + \sigma(r_2)\sigma(f)^2 + \sigma(r_1)\sigma(f) + \sigma(r_0) \\ &= \sigma(f)^n + r_{n-1}\sigma(f)^{n-1} + \cdots + r_2\sigma(f)^2 + r_1\sigma(f) + r_0 \end{aligned}$$

und somit erfüllt auch $\sigma(f)$ eine Ganzheitsgleichung über R, also $\sigma(f) \in S$. Deshalb lässt sich σ zu einer Abbildung von S nach S einschränken.

Die Gleichheit $S \cap K = R$ ist klar, da R als normal vorausgesetzt wird. Deshalb ist

$$S^G \subseteq S \cap L^G = S \cap K = R,$$

die umgekehrte Inklusion $R \subseteq S^G$ ist klar. □

Korollar 21.3. *Es sei $\mathbb{Q} \subseteq K$ eine Galoiserweiterung und $\mathbb{Z} \subseteq R$ die zugehörige Erweiterung der Zahlbereiche. Dann operiert die Galoisgruppe G auf R mit Invariantenring $R^G = \mathbb{Z}$.*

Beweis. Dies folgt direkt aus Satz 21.2. □

Beispiel 21.4. Eine quadratische Körpererweiterung $\mathbb{Q} \subseteq L = \mathbb{Q}[\sqrt{D}]$ mit einer quadratfreien ganzen Zahl $D \neq 0, 1$ ist stets eine Galoiserweiterung, wobei die Galoisgruppe neben der Identität aus der Konjugation $\sqrt{D} \mapsto -\sqrt{D}$ besteht. Diese Konjugation wirkt nach Satz 21.2 oder direkt nach Aufgabe 9.3 und Aufgabe 9.5 auch auf dem zugehörigen quadratischen Zahlbereich, mit $\mathbb{Z}$ als Invriantenring.

Wir beschreiben nun generell Eigenschaften von Invariantenringen zu einer Operation einer endlichen Gruppe.

Proposition 21.5. *Es sei G eine Gruppe, die auf einem Integritätsbereich R als Gruppe von Ringautomorphismen operiere. Dann gelten folgende Eigenschaften.*

1. *Der Invariantenring R^G ist ein Integritätsbereich.*
2. *Die Operation induziert eine Operation von G auf dem Quotientenkörper $Q(R)$ als Gruppe von Körperautomorphismen.*
3. *Es ist $Q\big(R^G\big) \subseteq (Q(R))^G$.*
4. *Es ist*

$$R \cap (Q(R))^G = R^G.$$

Beweis. (1) ist wegen $R^G \subseteq R$ klar. (2). Es sei $K = Q(R)$ der Quotientenkörper von R. Zu jedem $\sigma \in G$ setzt sich der Ringautomorphismus $f \mapsto f\sigma$ aufgrund der universellen Eigenschaft der Nenneraufnahme zu einem Körperautomorphismus $\frac{f}{g} \mapsto \frac{f\sigma}{g\sigma}$ fort. (3). Ein Element aus dem Quotientenkörper $Q\big(R^G\big)$ hat die Form $\frac{f}{g}$ mit invarianten Elementen $f, g \in R^G$. Es ist also insbesondere invariant unter der induzierten Operation auf K. Daher gilt $Q\big(R^G\big) \subseteq (Q(R))^G$. (4). Die Inklusion $R^G \subseteq R \cap Q(R)^G$ ist direkt klar. Die andere Inklusion ergibt sich, da die Operation von G auf $Q(R)$ eingeschränkt auf R die ursprüngliche Operation ist. Wenn also $f \in R$ ist und aufgefasst in $Q(R)$ invariant ist, so ist es überhaupt invariant. □

Bei einer endlichen Gruppe gilt in Proposition 21.5 (3) sogar Gleichheit, wie die folgende Aussage zeigt.

Lemma 21.6. *Es sei G eine endliche Gruppe, die auf einem Integritätsbereich als Gruppe von Ringautomorphismen operiere. Dann ist*

$$Q\big(R^G\big) = (Q(R))^G.$$

Beweis. Die Inklusion $Q\big(R^G\big) \subseteq (Q(R))^G$ gilt nach Proposition 21.5 (3) für jede Gruppe. Zum Beweis der Umkehrung seien $f, g \in R$, $g \neq 0$, mit $\frac{f}{g} \in (Q(R))^G$ gegeben. Wir betrachten

$$h = \prod_{\sigma \in G,\, \sigma \neq e_G} g\sigma.$$

Dann gelten in $Q(R)$ die Identitäten

$$\begin{aligned} \frac{f}{g} &= \frac{hf}{hg} \\ &= \frac{hf}{\Big(\prod_{\sigma \in G,\, \sigma \neq e_G} g\sigma\Big) g} \\ &= \frac{hf}{\prod_{\sigma \in G} g\sigma}. \end{aligned}$$

Nach Voraussetzung ist der Bruch und in dieser Darstellung offenbar auch der Nenner (siehe Aufgabe 21.7) invariant. Also muss auch der Zähler invariant sein und somit ist $\frac{f}{g} \in \big(R^G\big)$. □

Lemma 21.7. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere. Dann ist $R^G \subseteq R$ eine ganze Erweiterung.*

Beweis. Zu $f \in R$ betrachten wir das Produkt

$$P = \prod_{\sigma \in G} (X - f\sigma) \in R[X].$$

Die Koeffizienten dieses Polynoms gehören zum Invariantenring R^G. Ferner ist P normiert und es ist $P(f) = 0$ (da ja $X - fe_G = X - f$ ein Linearfaktor ist). Somit liefert P eine Ganzheitsgleichung für f über R^G und daher ist $R^G \subseteq R$ ganz. □

21.2. **Invariantenring und Quotientenraum.**

Es sei R ein kommutativer Ring, G eine endliche Gruppe, die auf R als Gruppe von Ringautomorphismen und damit nach Proposition 5.1 auch auf $X = \operatorname{Spek}(R)$ als Gruppe von Homöomorphismen operiere. Dann hat man einerseits den topologischen Quotienten X/G und andererseits den Invariantenring R^G und damit dessen Spektrum $\operatorname{Spek}\left(R^G\right)$. Der topologische Quotient ist einfach der Bahnenraum versehen mit der Bildtopologie. Wir zeigen nach einigen Vorbereitungen, dass diese zwei geometrischen Objekte gleich sind, also dass

$$X/G = \operatorname{Spek}\left(R^G\right)$$

gilt. Dabei werden wir zeigen, dass die Spektrumsabbildung

$$\iota^*\colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

(die zur Inklusion $R^G \subseteq R$ gehört) die Eigenschaften eines topologischen Quotienten erfüllt.

Korollar 21.8. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere. Dann ist die Spektrumsabbildung*

$$\iota^*\colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

surjektiv und abgeschlossen. Insbesondere trägt $\operatorname{Spek}\left(R^G\right)$ *die Bildtopologie unter dieser Abbildung.*

Beweis. Dies folgt aus Lemma 21.7 und aus Satz Anhang 5.3. □

Lemma 21.9. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere und es sei*

$$\iota^*\colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

die zugehörige Spektrumsabbildung. Dann gilt für $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spek}(R)$ die Äquivalenz: $\iota^*(\mathfrak{p}) = \iota^*(\mathfrak{q})$ genau dann, wenn es ein $\sigma \in G$ mit $\sigma^*(\mathfrak{p}) = \mathfrak{q}$ gibt. Das heißt, dass die Bahnen der Operation von G auf $\operatorname{Spek}(R)$ *mit den Fasern von ι^* übereinstimmen.*

Beweis. Wenn $\sigma^*(\mathfrak{p}) = \sigma^{-1}(\mathfrak{p}) = \mathfrak{q}$ ist und $f \in R^G \cap \mathfrak{q}$, so ist auch $f = f\sigma \in \mathfrak{p}$, also ist

$$\iota^*(\mathfrak{p}) = R^G \cap \mathfrak{p} = R^G \cap \mathfrak{q} = \iota^*(\mathfrak{q}).$$

Primideale in derselben Bahn besitzen also den gleichen Bildpunkt unter der Spektrumsabbildung.

Zum Beweis der Umkehrung betrachten wir die Faser über $\mathfrak{r} \in \operatorname{Spek}\left(R^G\right)$ und es sei $\mathfrak{p}$ ein Element dieser Faser, welches es nach Korollar 21.8 gibt. Wir müssen zeigen, dass jedes Primideal $\mathfrak{q}$ der Faser in der Bahn durch $\mathfrak{p}$ liegt, dass es also ein $\sigma \in G$ mit $\sigma^*(\mathfrak{p}) = \mathfrak{q}$ gibt. Wir nehmen an, dass dies nicht der Fall sei, und es sei $\mathfrak{q}$ ein Primideal der Faser über $\mathfrak{r}$, das aber nicht zur Bahn durch $\mathfrak{q}$ gehört. Aus $\mathfrak{q} \neq \sigma^*(\mathfrak{p})$ (für alle $\sigma \in G$) folgt $\mathfrak{q} \not\subseteq \sigma^*(\mathfrak{p})$, da andernfalls die Faser im Widerspruch zu Lemma Anhang 5.5 nicht nulldimensional wäre. Nach Lemma 11.10 (Kommutative Algebra) ist dann auch

$$\mathfrak{q} \not\subseteq \bigcup_{\sigma \in G} \sigma^*(\mathfrak{p}) =: T.$$

Sei $f \in \mathfrak{q}$, $f \notin T$. Die Menge T wird unter der Gruppenoperation auf sich selbst abgebildet, daher ist auch $f\sigma \notin T$. Somit ist auch $g = \prod_{\sigma \in G} f\sigma \notin T$. Andererseits ist aber $g \in R^G$ und $g \in \mathfrak{q}$, also ergibt sich der Widerspruch $g \in R^G \cap \mathfrak{q} = \mathfrak{r} \subseteq \mathfrak{p} \subseteq T$. □

Satz 21.10. *Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G durch Ringautomorphismen operiere und es sei*

$$\iota^* \colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

die zugehörige Spektrumsabbildung. Dann ist $\left(\operatorname{Spek}\left(R^G\right), \iota^*\right)$ der Quotient der Gruppenoperation von G auf $\operatorname{Spek}(R)$.

Beweis. Die Abbildung

$$\iota^* \colon \operatorname{Spek}(R) \longrightarrow \operatorname{Spek}\left(R^G\right)$$

ist nach Korollar 21.8 surjektiv, so dass nach Lemma 21.9 die Punkte aus $\operatorname{Spek}\left(R^G\right)$ den Bahnen der Gruppenoperation entsprechen. Daher ist $\operatorname{Spek}\left(R^G\right)$ ein mengentheoretischer Quotient. Nach Korollar 21.8 trägt $\operatorname{Spek}\left(R^G\right)$ die Bildtopologie, so dass es sich auch um einen topologischen Quotienten handelt. □

Korollar 21.11. *Es sei $\mathbb{Q} \subseteq K$ eine Galoiserweiterung und $\mathbb{Z} \subseteq R$ die zugehörige Erweiterung der Zahlbereiche. Es sei $p \in \mathbb{Z}$ eine Primzahl und seien $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec}(R)$ Primideale oberhalb von (p). Dann sind die lokalen Ringe $R_{\mathfrak{p}}$ und $R_{\mathfrak{q}}$ und die Restekörper $\kappa(\mathfrak{p})$ und $\kappa(\mathfrak{q})$ zueinander isomorph.*

Beweis. Nach Korollar 21.3 ist $R^G = \mathbb{Z}$. Wenn $\mathfrak{p}$ und $\mathfrak{q}$ auf das gleiche Primideal in $\mathbb{Z}$ runterschneiden, so gibt es nach Lemma 21.9 einen Automorphismus

$$\sigma \colon R \longrightarrow R$$

mit $\sigma^{-1}(\mathfrak{p}) = \mathfrak{q}$. Dazu gehört ein Isomorphismus

$$R_{\mathfrak{p}} \longrightarrow R_{\mathfrak{q}}$$

und ein Isomorphismus der Restekörper. □

21. Arbeitsblatt

21.1. **Aufgaben.**

Aufgabe 21.1. Man gebe ein Beispiel für einen Integritätsbereich R und einer Gruppenoperation einer endlichen Gruppe G auf R derart, dass nicht jeder Zwischenring S, $R^G \subseteq S \subseteq R$, der Invariantenring zu einer Untergruppe von G ist.

Aufgabe 21.2. Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Galoiserweiterung vom Grad n und sei S der ganze Abschluss von R in L. Interpretiere den Satz über die Galoiskorrespondenz für die normalen Zwischenringe zwischen R und S. Welche Gruppen wirken auf diesen Ringen und wie sehen die Invariantenringe aus?

Aufgabe 21.3.*

Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit einer Galoisgruppe G. Es sei S der ganze Abschluss von R in L und es sei $f \in S$ ein Element derart, dass $f\sigma$, $\sigma \in G$, eine R-Basis von S ist. Es sei $H \subseteq G$ eine Untergruppe mit den Nebenklassen

$$H_1 = H, H_2, \ldots, H_k\,.$$

Zeige, dass die Familie

$$f_j = \sum_{\sigma \in H_j} f\sigma$$

zu $j = 1, \ldots, k$ eine R-Basis des Invariantenringes S^H ist.

Aufgabe 21.4. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere. Zeige die folgende Aussagen.

(1) Für die Einheiten gilt

$$\left(R^G\right)^\times = R^G \cap R^\times.$$

(2) Wenn R ein Körper ist, so ist auch R^G ein Körper.

Aufgabe 21.5. Es sei R ein kommutativer Ring und G eine Gruppe, die auf R als Gruppe von Ringautomorphismen operiere. Zeige, dass die Operation genau dann trivial ist, wenn $R^G = R$ ist.

Aufgabe 21.6. Es sei S ein kommutativer Ring mit $2 \neq 0$ und $a \in S$. Zeige, dass die Gruppe $\mathbb{Z}/(2) \cong \{1,-1\}$ auf der quadratischen Erweiterung

$$R := S[X]/(X^2 - a)$$

als Gruppe von S-Algebrahomomorphismen operiert, indem -1 durch $X \mapsto -X$ wirkt. Bestimme den Fixring zu dieser Operation.

Aufgabe 21.7. Es sei G eine endliche Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere. Zeige, dass zu jedem $f \in R$ sowohl $\sum_{\sigma \in G} f\sigma$ als auch $\prod_{\sigma \in G} f\sigma$ zum Fixring R^G gehören.

Aufgabe 21.8. Es sei R ein kommutativer Ring, auf dem eine endliche Gruppe G als Gruppe von Ringautomorphismen operiere. Zeige die folgenden Aussagen.

(1) Zu jedem $k \in \mathbb{N}$ und jedem $f \in R$ ist der Ausdruck

$$\psi_k(f) = \sum_{T \subseteq G,\, \#(T)=k} \prod_{\sigma \in T} f\sigma$$

invariant.
(2) Wenn R einen Körper der Charakteristik 0 enthält, so erzeugen die $\psi_k(f)$, $f \in R$, $k \in \mathbb{N}$, den Invariantenring.
(3) Teil (2) gilt nicht ohne die Voraussetzung an die Charakteristik.

Aufgabe 21.9. Es sei R ein Dedekindbereich, $Q(R) \subseteq L$ eine endliche Körpererweiterung und S der ganze Abschluss von R in L. Zeige, dass die Galoisgruppe $\mathrm{Gal}\,(L|K)$ in natürlicher Weise auf der Divisorengruppe $\mathrm{Div}\,(S)$ operiert.

Aufgabe 21.10. Es sei R ein Dedekindbereich, $Q(R) \subseteq L$ eine endliche Körpererweiterung und S der ganze Abschluss von R in L. Zeige, dass die Galoisgruppe $\mathrm{Gal}\,(L|K)$ in natürlicher Weise auf der Divisorenklassengruppe $\mathrm{KG}\,(S)$ operiert.

Aufgabe 21.11. Es sei K ein Körper. Zeige, dass auf $K[X,Y]/(XY)$ eine Gruppenoperation von $\mathbb{Z}/(2)$ gegeben ist, indem das nichttriviale Gruppenelement X und Y vertauscht. Bestimme den Fixring zu dieser Operation.

Aufgabe 21.12. Es sei $n \in \mathbb{N}_+$. Betrachte auf dem rationalen Funktionenkörper $\mathbb{C}(X)$ die Gruppe der $\mathbb{C}$-Körperautomorphismen, die durch $X \mapsto \zeta_n X$ erzeugt wird, wobei ζ_n eine primitive n-te Einheitswurzel bezeichnet. Bestimme den Fixkörper $\mathbb{C}(X)^{\mathbb{Z}/(n)}$.

Aufgabe 21.13. Es sei K ein Körper der positiven Charakteristik p. Wir betrachten die durch $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ erzeugte zyklische Gruppe und ihre natürliche Operation auf $K[X,Y]$. Zeige, dass der Invariantenring gleich

$$K[Y, X^p - XY^{p-1}]$$

ist.

Aufgabe 21.14. Es sei K ein unendlicher Körper. Wir betrachten auf dem Körper $K(X,Y)$ die Operation von $K^\times$, wobei $\lambda \in K^\times$ durch $X \mapsto \lambda X$, $Y \mapsto \lambda Y$ auf $K[X,Y]$ wirkt und diese Wirkung auf den Quotientenkörper fortgesetzt wird. Zeige, dass der Fixring zu dieser Operation gleich $K\left(\frac{X}{Y}\right)$ ist.

Aufgabe 21.15. Es sei G eine Gruppe, die auf einem kommutativen lokalen Ring als Gruppe von Ringautomorphismen operiere. Zeige, dass der Fixring R^G ebenfalls lokal ist.

Aufgabe 21.16. Es sei R ein kommutativer Ring, auf dem eine Gruppe G als Gruppe von Ringautomorphismen operiere. Es sei $\mathfrak{a} \subseteq R$ ein Ideal, das unter der Gruppenoperation invariant ist (es gelte also $f\sigma \in \mathfrak{a}$ für $f \in \mathfrak{a}$ und jedes $\sigma \in G$). Zeige die folgenden Aussagen.

(1) Es gibt eine natürliche Operation von G auf dem Restklassenring $R/\mathfrak{a}$.
(2) Es gibt einen Ringhomomorphismus
$$\psi\colon\ R^G/\left(\mathfrak{a} \cap R^G\right) \longrightarrow (R/\mathfrak{a})^G.$$
(3) Die Abbildung ψ aus Teil (2) ist injektiv.
(4) Wenn G endlich ist und R einen Körper der Charakteristik 0 enthält, so ist ψ surjektiv.

Aufgabe 21.17. Es sei G eine endliche Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere mit dem Invariantenring $S = R^G$. Es sei $T \subseteq S$ ein multiplikatives System. Zeige, dass es eine natürliche Operation von G auf R_T gibt, und dass der zugehörige Invariantenring gleich S_T ist.

Aufgabe 21.18. Es sei G eine endliche Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere mit dem Invariantenring $S = R^G$. Es sei $\mathfrak{p} \in \operatorname{Spek}(S)$ ein Primideal. Zeige, dass es eine natürliche Operation von G auf dem Faserring $(R/\mathfrak{p}R)_{S\setminus\mathfrak{p}}$ gibt. Zeige, dass der zugehörige Invariantenring den Restekörper $\kappa(\mathfrak{p})$ enthält. Zeige durch ein Beispiel, dass dabei der Restekörper echt kleiner sein kann.

Aufgabe 21.19. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere mit dem Invariantenring $S = R^G$. Zeige, dass G in natürlicher Weise auch auf dem Polynomring $R[X]$ operiert, und dass der zugehörige Invariantenring gleich $S[X]$ ist.

Aufgabe 21.20. Es sei G eine endliche Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen operiere. Es sei $f \in R$. Zeige, dass das Polynom

$$P = \prod_{\sigma \in G} (X - f\sigma) \in R[X]$$

unter der natürlichen Operation von G auf dem Polynomring $R[X]$ invariant ist.

Betrachte unter diesem Aspekt nochmal Aufgabe 21.5 und Aufgabe 21.6.

Aufgabe 21.21. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L. Es sei $H \subseteq G$ eine Untergruppe mit dem Fixkörper M, $K \subseteq M \subseteq L$. Zeige, dass der Ganzheitsring T von R in M gleich dem Invariantenring S^H ist.

Aufgabe 21.22. Es sei $R \subseteq S$ eine Erweiterung von kommutativen Ringen. Zeige, dass die Automorphismengruppe $\mathrm{Aut}_R(S)$ in natürlicher Weise auf dem Modul der Kähler-Differentiale $\Omega_{S|R}$ R-linear operiert.

Aufgabe 21.23.*

Es sei K_5 der fünfte Kreisteilungskörper und R_5 der fünfte Kreisteilungsring. Bestimme die 3×3-Matrizen, die die Operation der Galoisgruppe $\mathrm{Gal}(K_5|\mathbb{Q})$ auf dem Modul der Kähler-Differentiale bezüglich der Basis aus Beispiel 19.8 beschreiben.

Aufgabe 21.24. Es sei K_7 der fünfte Kreisteilungskörper und R_7 der fünfte Kreisteilungsring. Bestimme die 5×5-Matrizen, die die Operation der Galoisgruppe $\mathrm{Gal}(K_7|\mathbb{Q})$ auf dem Modul der Kähler-Differentiale bezüglich der Basis aus Beispiel 19.8 beschreiben.

Aufgabe 21.25. Es sei G eine Gruppe und M eine Menge. Es sei $\mathrm{Perm}(M)$ die Gruppe der Permutationen auf M. Zeige folgende Aussagen.

(1) Wenn G auf M operiert, so ist die Abbildung
$$G \longrightarrow \mathrm{Perm}\,(M),\ g \longmapsto (x \mapsto gx),$$
ein Gruppenhomomorphismus.
(2) Wenn umgekehrt ein Gruppenhomomorphismus
$$\varphi\colon\ G \longrightarrow \mathrm{Perm}\,(M),$$
vorliegt, so wird durch
$$G \times M \longrightarrow M,\ (g,x) \longmapsto (\varphi(g))(x),$$
eine Gruppenoperation von G auf M definiert.

Aufgabe 21.26. Es sei $n \in \mathbb{N}$. Betrachte die Gruppenoperation der n-ten Einheitswurzeln durch Multiplikation auf $\mathbb{C}$. Bestimme die Bahnen und die Isotropiegruppen dieser Operation. Kann man die Quotientenabbildung durch eine polynomiale Funktion realisieren?

22. Vorlesung - Zerlegung in Galoiserweiterungen

22.1. **Das Zerlegungsverhalten bei Galoiserweiterungen.**

Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung vom Grad n. Die Galoisgruppe, d.h. die Gruppe der K-Algebraautomorphismen von L, besteht also aus n Automorphismen. Die Untergruppen der Galoisgruppe entsprechen nach dem Satz über die Galoiskorrespondenz den Zwischenkörpern der Erweiterung. Die Galoisgruppe operiert nach Satz 21.2 auch auf dem ganzen Abschluss S von R in L. Hier besprechen wir Untergruppen, ihre zugehörigen Zwischenkörper und Zwischenringe, die mit dem Zerlegungsverhalten von Primidealen unter der Erweiterung $R \subseteq S$ zusammenhängen. Zuerst formulieren wir, wie sich die fundamentale Gleichung aus Satz 20.4 im Galoisfall vereinfacht.

Lemma 22.1. *Es sei R ein Dedekindbereich mit Quotientenkörper K, $K \subseteq L$ eine Galoiserweiterung vom Grad n und sei S der ganze Abschluss von R in L. Es sei $\mathfrak{p}$ ein von 0 verschiedenes Primideal von R. Dann stimmen in der Primidealzerlegung*
$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_k^{e_k}$$
die Exponenten e_i überein und ebenso stimmen die Trägheitsgrade f_i überein. Dabei ist
$$n = kef.$$

Beweis. Es seien $\mathfrak{q}$ und $\mathfrak{q}'$ Primideale oberhalb von $\mathfrak{p}$. Nach Lemma 21.9 gibt es einen Automorphismus $\sigma \in \mathrm{Gal}\,(L|K)$ mit $\sigma(\mathfrak{q}) = \mathfrak{q}'$. Daher gibt es einen $R_{\mathfrak{p}}$-Algebraisomorphismus $\sigma\colon\ S_{\mathfrak{q}} \to S_{\mathfrak{q}'}$, weshalb die Verzweigungsordnungen gleich sind, und einen $\kappa(\mathfrak{p})$-Isomorphismus der Restekörper
$$\kappa(\mathfrak{q}) \longrightarrow \kappa(\mathfrak{q}'),$$

weshalb die Trägheitsgrade gleich sind. Die Formel aus Satz 20.4 nimmt daher die angegebene Gestalt an. □

Es sei $\mathfrak{p}$ ein Primideal aus R und seien $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ die Primideale von S oberhalb von $\mathfrak{p}$. Gemäß Lemma 21.9 und wie eben verwendet lassen sich diese Primideale ineinander mit isomorphen Restekörpern überführen. Dies bedeutet natürlich nicht, dass der Gruppenhomomorphismus

$$G \longrightarrow \operatorname{Perm}(\mathfrak{q}_1, \ldots, \mathfrak{q}_k)$$

bijektiv ist, wobei rechts die Permutationsgruppe zur Faser über $\mathfrak{p}$ steht. Dabei ist die Bijektivität oft schon wegen der Anzahl ausgeschlossen. Wenn der Grad n ist, und wenn, im total zerlegten Fall, die Faser aus n Primidealen besteht, so steht links (im Galoisfall) eine Gruppe mit n Elementen und rechts eine Gruppe mit $n!$ Elementen, was nur bei $n \leq 2$ übereinstimmt. Wenn hingegen, im unzerlegten Fall, die Faser aus nur einem Primideal besteht, so steht rechts die triviale Gruppe. Ein Automorphismus $\sigma \in G$ gehört genau dann zum Kern, wenn jedes Primideal der Faser unter σ auf sich selbst abgebildet wird. Diese Bedingung führt, auf ein einzelnes Primideal angewendet, zum Begriff der Zerlegungsgruppe.

Definition 22.2. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Dann nennt man

$$G_{\mathfrak{q}} = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

die *Zerlegungsgruppe* zu $\mathfrak{q}$.

Man spricht auch von der *Isotropiegruppe* oder dem *Stabilisator* zu $\mathfrak{q}$. Man beachte, dass die Bedingung besagt, dass $\mathfrak{q}$ auf sich selbst abgebildet wird, nicht, dass die Einschränkung auf $\mathfrak{q}$ die Identität ist.

Lemma 22.3. *Es sei R ein Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S über $\mathfrak{p}$. Dann gelten folgende Eigenschaften.*

1. *Die Zerlegungsgruppe $G_{\mathfrak{q}}$ ist genau dann trivial, wenn $\mathfrak{p}$ voll zerlegt ist.*
2. *Die Zerlegungsgruppe $G_{\mathfrak{q}}$ ist genau gleich G, wenn $\mathfrak{p}$ unzerlegt ist.*
3. *Zu einem weiteren Primideal $\mathfrak{q}'$ oberhalb von $\mathfrak{p}$ sind die Zerlegungsgruppen $G_{\mathfrak{q}}$ und $G_{\mathfrak{q}'}$ isomorph.*
4. *Es ist*
$$\#(G_{\mathfrak{q}}) = ef,$$
wobei e der gemeinsame Verzweigungsindex und f der gemeinsame Trägheitsgrad der Primideale oberhalb von $\mathfrak{p}$ ist.

Beweis. (1) und (2) sind klar und folgen auch aus (4).

(3). Nach Lemma 21.9 gibt es ein $\tau \in G$ mit $\tau(\mathfrak{q}) = \mathfrak{q}'$. Mittels τ kann man direkt den Isomorphismus

$$G_{\mathfrak{q}} \longrightarrow G_{\mathfrak{q}'},\ \sigma \longmapsto \tau \circ \sigma \circ \tau^{-1},$$

angeben. Es ist ja

$$\left(\tau \circ \sigma \circ \tau^{-1}\right)(\mathfrak{q}') = \tau(\sigma(\tau^{-1}(\mathfrak{q}'))) = \tau(\sigma(\mathfrak{q})) = \tau(\mathfrak{q}) = \mathfrak{q}'.$$

(4). Wir zerlegen G abhängig davon, auf welches Primideal $\mathfrak{q}$ abgebildet wird, also

$$G = \biguplus_{\mathfrak{q}'} \{\rho \in G \mid \rho(\mathfrak{q}) = \mathfrak{q}'\}.$$

Dabei ist die Untergruppe $G_{\mathfrak{q}}$ ein Teil davon und die anderen Teile sind die Nebenklassen zu dieser Untergruppe, da ja

$$\{\rho \in G \mid \rho(\mathfrak{q}) = \mathfrak{q}'\} = \tau G_{\mathfrak{q}},$$

wenn τ ein fixierter Automorphismus ist, der $\mathfrak{q}$ in $\mathfrak{q}'$ überführt. Insbesondere sind diese Nebenklassen alle gleich groß. Wenn es k Primideale in der Faser gibt, und die Körpererweiterung den Grad n hat und die Galoisgruppe somit n Elemente besitzt, so enthält die Zerlegungsgruppe $\frac{n}{k}$ Elemente, was nach Lemma 22.1 mit ef übereinstimmt. □

Definition 22.4. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Dann nennt man den Fixkörper zur Zerlegungsgruppe $G_{\mathfrak{q}}$ den *Zerlegungskörper* zu $\mathfrak{q}$. Er wird mit $Z_{\mathfrak{q}}$ bezeichnet.

Den Ganzheitsring zum Zerlegungskörper nennt man *Zerlegungsring*.

Lemma 22.5. *Es sei R ein Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S über $\mathfrak{p}$. Dann gelten folgende Eigenschaften.*

(1) *Es gibt einen natürlichen Gruppenhomomorphismus*

$$G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}\,(\kappa(\mathfrak{q})|\kappa(\mathfrak{p})).$$

(2) *Wenn die Erweiterung der Restekörper separabel ist, so handelt es sich bereits um eine Galoiserweiterung, und der Gruppenhomomorphismus ist surjektiv.*
(3) *Wenn $\mathfrak{q}$ zusätzlich unverzweigt ist, so liegt ein Isomorphismus vor.*

Beweis. (1) Sei $\sigma \in G_{\mathfrak{q}}$, also $\sigma^{-1}(\mathfrak{q}) = \mathfrak{q}$. Dies induziert einen Ringautomorphismus (der R fest lässt)

$$\sigma\colon\ S_{\mathfrak{q}} \longrightarrow S_{\mathfrak{q}}$$

und einen Körperautomorphismus

$$\sigma\colon\ \kappa(\mathfrak{q}) \longrightarrow \kappa(\mathfrak{q}),$$

der $\kappa(\mathfrak{p})$ fest lässt, also ein Element der Galoisgruppe zur Körpererweiterung $\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q})$. Diese Zuordnung ist insgesamt ein Gruppenhomomorphismus aufgrund der Kommutativität des Diagramms

$$\begin{array}{ccccc} S_{\mathfrak{q}} & \stackrel{\sigma}{\longrightarrow} & S_{\mathfrak{q}} & \stackrel{\tau}{\longrightarrow} & S_{\mathfrak{q}} \\ \downarrow & & \downarrow & & \downarrow \\ \kappa(\mathfrak{q}) & \stackrel{\sigma}{\longrightarrow} & \kappa(\mathfrak{q}) & \stackrel{\tau}{\longrightarrow} & \kappa(\mathfrak{q}) \ . \end{array}$$

(2) Nach Aufgabe 22.6 können wir davon ausgehen, indem wir K durch den Zerlegungskörper und $\mathfrak{p}$ durch den Schnitt von $\mathfrak{q}$ mit dem Zerlegungsring ersetzen, dass die Zerlegungsgruppe die volle Galoisgruppe ist, dass also $\mathfrak{q}$ das einzige Primideal oberhalb von $\mathfrak{p}$ ist. Aufgrund der Voraussetzung über die Separabilität können wir nach dem Satz vom primitiven Element

$$\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q}) = \kappa(\mathfrak{p})[z]$$

ansetzen, wobei wir unmittelbar $z \in S$ annehmen können. Es sei $P \in R[X]$ das Minimalpolynom von z über R. Es ist also $P(z) = 0$ in S und damit insbesondere $P(z) = 0$ in $\kappa(\mathfrak{q})$. Da $K \subseteq L$ eine Galoiserweiterung ist, zerfällt wegen Satz 16.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) P in $L[X]$ und damit wegen Satz 21.2 auch in $S[X]$ in Linearfaktoren. Dies gilt dann auch in $\kappa(\mathfrak{q})[X]$ und überträgt sich auf das Minimalpolynom von z über $\kappa(\mathfrak{p})$, was wiederum nach Satz 16.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) bedeutet, dass die Restekörpererweiterung galoissch ist.

Es sei nun

$$\tau\colon\ \kappa(\mathfrak{q}) = \kappa(\mathfrak{p})[z] \longrightarrow \kappa(\mathfrak{q}) = \kappa(\mathfrak{p})[z]$$

ein $\kappa(\mathfrak{p})$-Körperautomorphismus, der den Erzeuger z auf ein Element $w \in \kappa(\mathfrak{q})$ schickt, das wir wiederum als repräsentiert durch eine Nullstelle w von P annehmen dürfen. Nach Korollar 15.9 (Körper- und Galoistheorie (Osnabrück 2018-2019)) gehört dazu ein K-Automorphismus von L, der z in w überführt, und dessen Einschränkung stimmt mit τ überein, da er auf einem Erzeuger damit übereinstimmt.

(3) Nach Lemma 22.3 (4) ist im unverzweigten Fall $\#\,(G_{\mathfrak{q}}) = f$ und dies ist nach Definition der Grad der Körpererweiterung

$$\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q}).$$

Da nach (2) die Restekörpererweiterung galoissch ist, besitzt deren Galoisgruppe ebenfalls f Elemente und deshalb folgt aus der Surjektivität bereits die Bijektivität.

□

Definition 22.6. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Dann nennt man

$$I_{\mathfrak{q}} = \left\{\sigma \in G_{\mathfrak{q}} \mid \sigma|_{\kappa(\mathfrak{q})} = \mathrm{Id}\right\}$$

die *Trägheitsgruppe* zu $\mathfrak{q}$.

Es liegt also eine Kette von Untergruppen

$$I_{\mathfrak{q}} \subseteq G_{\mathfrak{q}} \subseteq G$$

vor.

Definition 22.7. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Dann nennt man den Fixkörper zur Trägheitsgruppe $I_{\mathfrak{q}}$ den *Trägheitskörper* zu $\mathfrak{q}$. Er wird mit $T_{\mathfrak{q}}$ bezeichnet.

Lemma 22.8. *Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{q}$ ein Primideal von S. Die Erweiterung der Restekörper sei separabel. Dann ist die Ordnung der Trägheitsgruppe $I_{\mathfrak{q}}$ gleich dem Verzweigungsindex von $\mathfrak{q}$. Insbesondere ist die Trägheitsgruppe genau dann trivial, wenn in $\mathfrak{q}$ keine Verzweigung vorliegt.*

Beweis. Nach Lemma 22.5 (2) liegt eine kurze exakte Sequenz

$$0 \longrightarrow I_{\mathfrak{q}} \longrightarrow G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}\left(\kappa(\mathfrak{q})|\kappa(\mathfrak{p})\right) \longrightarrow 0$$

vor. Die Ordnung der Galoisgruppe rechts ist der Trägheitsgrad f und die Ordnung der Zerlegungsgruppe $G_{\mathfrak{q}}$ ist nach Lemma 22.3 gleich ef, wobei e den Verzweigungsindex bezeichnet. Deshalb ist die Ordnung der Trägheitsgruppe gleich e. □

Wir besprechen weiter Besonderheiten in der zahlentheoretischen Situation, die insbesondere damit zusammenhängen, dass Körpererweiterungen zwischen endlichen Körper zyklisch sind und vom Frobenius (bzw. einer Frobeniuspotenz) erzeugt werden.

Korollar 22.9. *Es sei R ein Zahlbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit einer nicht zyklischen Galoisgruppe G. Dann sind alle Primideale $\mathfrak{p}$ aus R bis auf endlich viele Ausnahmen im ganzen Abschluss von R in L zerlegt.*

Beweis. Es sei $\mathfrak{p}$ nicht verzweigt und sei $\mathfrak{q}$ ein Primideal oberhalb von $\mathfrak{p}$. Nehmen wir an, dass $\mathfrak{p}$ unzerlegt ist, dass also $\mathfrak{q}$ das einzige Primideal darüber ist. Dann liegt nach Lemma 22.5 (3) ein Gruppenisomorphismus

$$G = G_{\mathfrak{q}} \longrightarrow \mathrm{Gal}\left(\kappa(\mathfrak{q})|\kappa(\mathfrak{p})\right)$$

vor. Da die Gruppe rechts nach Satz 5.23 bzw. nach Korollar 16.10 (Körper- und Galoistheorie (Osnabrück 2018-2019)) zyklisch ist, ergibt sich ein Widerspruch zur Voraussetzung. □

Bemerkung 22.10. Es sei $R \subseteq S$ eine Erweiterung von Zahlbereichen zu einer Galoiserweiterung $Q(R) = K \subseteq Q(S) = L$ mit Galoisgruppe G. Wenn ein Primideal $\mathfrak{p}$ aus R unverzweigt in S und $\mathfrak{q}$ ein Primideal darüber ist, so liegt nach Lemma 22.5 (3) ein kanonischer Isomorphismus zwischen der Zerlegungsgruppe $G_{\mathfrak{q}}$ und der zyklischen Galoisgruppe $\mathrm{Gal}\,(\kappa(\mathfrak{q})|\kappa(\mathfrak{p}))$, die vom Frobenius bzw. einer Frobeniuspotenz (siehe Korollar 16.10 (Körper- und Galoistheorie (Osnabrück 2018-2019))) erzeugt wird. Man nennt daher auch den entsprechenden Erzeuger der Zerlegungsgruppe $G_{\mathfrak{q}}$ den *Frobenius*. Dafür schreibt man

$$(\mathfrak{q}, L/K)$$

und spricht vom Frobenius. Es ist also $(\mathfrak{q}, L/K) \in G_{\mathfrak{q}} \subseteq G$, und man betrachtet diesen Frobenius als Element der Galoisgruppe. Wenn $\mathfrak{q}'$ ein weiteres Primideal über $\mathfrak{p}$ ist, so sind nach Lemma 22.3 die Zerlegungsgruppen über

$$G_{\mathfrak{q}} \longrightarrow G_{\mathfrak{q}'},\ \sigma \longmapsto \tau \circ \sigma \circ \tau^{-1},$$

zueinander isomorph und zwar konjugiert in G. Insbesondere sind dann die Frobenii zueinander konjugiert und bilden eine Konjugationsklasse. Wenn zusätzlich eine abelsche Erweiterung vorliegt, so stimmen diese Frobenius-Automorphismen überein und hängen nur von dem Primideal $\mathfrak{p}$ aus R ab. Man bezeichnet diesen Frobenius mit $(\mathfrak{p}, L/K)$ und spricht vom *Artinsymbol*.

Nikolai Grigorjewitsch Tschebotarjow (1894-1947)

Der *Dichtigkeitssatz von Tschebotarjowsch* besagt, dass bei einer Galoiserweiterung $\mathbb{Q} \subseteq L$ mit (der Einfachheit halber kommutativen) Galoisgruppe G die Menge der Primzahlen, für die ein bestimmtes Gruppenelement $g \in G$ der Frobenius ist, gleichverteilt ist. Insbesondere ist die „Wahrscheinlichkeit“, dass die Identität der Frobenius ist, was ja einfach bedeutet, dass die Zerlegungsgruppe trivial ist, was wiederum nach Lemma 22.3 (1) bedeutet, dass p voll zerlegt ist, gleich $1/\#\,(G)$ ist.

22. Arbeitsblatt

22.1. **Aufgaben.**

Aufgabe 22.1. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L, sei $\mathfrak{p}$ ein Primideal von R mit der Faser $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$. Zeige, dass es einen natürlichen Gruppenhomomorphismus

$$G \longrightarrow \operatorname{Perm}(\mathfrak{q}_1, \ldots, \mathfrak{q}_k)$$

gibt, und dass dessen Kern gleich $\bigcap_{j=1}^{k} G_{\mathfrak{q}_j}$ ist.

Aufgabe 22.2. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit einer kommutativen Galoisgruppe G. Es sei S der ganze Abschluss von R in L und sei $\mathfrak{p}$ ein Primideal von R. Zeige, dass die Zerlegungsgruppen $G_{\mathfrak{q}}$ für alle Primideale $\mathfrak{q}$ aus S oberhalb von $\mathfrak{p}$ übereinstimmen.

Aufgabe 22.3. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L, sei $\mathfrak{p}$ ein Primideal von R mit der Faser $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$. Zeige, dass der Divisor $\sum_{j=1}^{k} \mathfrak{q}_j$ unter der natürlichen Operation der Galoisgruppe auf der Divisorengruppe invariant ist.

Aufgabe 22.4. Es sei G eine Gruppe, die auf einem kommutativen Ring R als Gruppe von Ringautomorphismen und damit auf $\operatorname{Spek}(R)$ operiere. Es sei $\mathfrak{p} \in \operatorname{Spek}(R)$. Zeige, dass der Stabilisator $G_{\mathfrak{p}}$ auf dem lokalen Ring $R_{\mathfrak{p}}$ und auf dem Restekörper $\kappa(\mathfrak{p})$ in natürlicher Weise operiert.

Aufgabe 22.5.*

Es sei R ein Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq M$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei T der ganze Abschluss von R in M. Es sei $N \subseteq G$ ein Normalteiler von G mit Restklassengruppe $H = G/N$ und es sei $S = T^N$ und $L = M^N$ der zugehörige Zwischenring bzw. Zwischenkörper, auf dem H galoissch operiert mit Fixring R bzw. Fixkörper K. Es sei $\mathfrak{r}$ ein Primideal von T über $\mathfrak{q}$ in S. Zeige, dass zwischen den Zerlegungsgruppen ein natürlicher surjektiver Gruppenhomomorphismus

$$G_{\mathfrak{r}} \longrightarrow H_{\mathfrak{q}}$$

besteht, dessen Kern gleich $N \cap G_{\mathfrak{r}}$ ist.

Aufgabe 22.6. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung. Es sei S der ganze Abschluss von R in L, $\mathfrak{q}$ ein Primideal in S und $Z_{\mathfrak{q}}$ der zugehörige Zerlegungskörper. Zeige, dass $K \subseteq Z_{\mathfrak{q}}$ galoissch ist.

Aufgabe 22.7. Es sei R eine Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung. Es sei S der ganze Abschluss von R in L, $\mathfrak{q}$ ein Primideal in S und $Z_{\mathfrak{q}}$ der zugehörige Zerlegungskörper. Zeige, dass $K \subseteq Z_{\mathfrak{q}}$ galoissch ist.

Aufgabe 22.8. Es sei R ein Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei S der ganze Abschluss von R in L und seien $\mathfrak{q}$ und $\mathfrak{q}'$ Primideale von S über $\mathfrak{p}$. Zeige, dass es ein natürliches kommutatives Diagramm

$$\begin{array}{ccc} G_{\mathfrak{q}} & \longrightarrow & \mathrm{Gal}\,(\kappa(\mathfrak{q})|\kappa(\mathfrak{p})) \\ \downarrow & & \downarrow \\ G_{\mathfrak{q}'} & \longrightarrow & \mathrm{Gal}\,(\kappa(\mathfrak{q}')|\kappa(\mathfrak{p})) \end{array}$$

von Gruppenhomomorphismen gibt, wobei die vertikalen Abbildungen Isomorphismen sind.

Aufgabe 22.9. Bestimme für den Zahlbereich $\mathbb{Z}[\mathrm{i}]$ den Zerlegungskörper und den Trägheitskörper für die Primideale oberhalb von $(2), (3), (5)$.

Aufgabe 22.10. Zeige, dass eine kubische Körpererweiterung $\mathbb{Q} \subseteq L$ im Allgemeinen nicht galoissch ist, „obwohl“ die Körpererweiterungen $\mathbb{Z}/(p) \subseteq \kappa(\mathfrak{q})$ für jedes maximale Ideal $\mathfrak{q}$ des zugehörigen Zahlbereiches S (mit $p \in \mathfrak{q}$) galoissch ist. Man folgere, dass in diesem Fall die Gruppenhomomorphismen aus Lemma 22.5 nicht surjektiv sind.

Aufgabe 22.11. Man gebe ein Beispiel für eine Galoiserweiterung $\mathbb{Q} \subseteq L$ derart, dass nicht jeder Zwischenkörper der Erweiterung als Zerlegungskörper eines Primideals des zugehörigen Zahlbereichs auftritt.

Aufgabe 22.12. Wir betrachten die Galoiserweiterung $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{7}]$ mit der Galoisgruppe

$$G = \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2).$$

Bestimme die Zerlegungsgruppe und die Trägheitsgruppe für die Primideale im zugehörigen Zahlbereich oberhalb von (7).

Aufgabe 22.13. Es sei $q \in \mathbb{Q}$ eine rationale Zahl, die in $\mathbb{Q}$ keine dritte Wurzel besitzt, so dass $\mathbb{Q} \subseteq L = \mathbb{Q}[X]/(X^3 - q)$ eine Körpererweiterung vom Grad 3 ist. Zeige, dass das Polynom $X^3 - q$ in L genau eine Nullstelle hat und dass diese Körpererweiterung nicht galoissch ist.

Aufgabe 22.14.*

Wir betrachten die Galoiserweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\zeta, \sqrt[3]{2}],$$

wobei $\zeta = \frac{-1+\mathrm{i}\sqrt{3}}{2}$ die dritte Einheitswurzel bezeichnet. Man gebe Beispiele für Primzahlen $p \geq 5$ derart, dass darüber im zugehörigen Zahlbereich zwei bzw. drei bzw. sechs Primideale liegen.

Aufgabe 22.15.*

Wir betrachten die Galoiserweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\zeta, \sqrt[3]{2}],$$

wobei $\zeta = \frac{-1+\mathrm{i}\sqrt{3}}{2}$ die dritte Einheitswurzel bezeichnet. Man gebe ein Beispiel für eine Primzahl derart, dass die Zerlegungsgruppen der Primideale im zugehörigen Zahlbereich verschieden sind.

Aufgabe 22.16. Bestimme für die reelle Quadratabbildung

$$\mathbb{R}[Y] \longrightarrow \mathbb{R}[X],\ Y \longmapsto X^2,$$

den Zerlegungskörper und den Trägheitskörper für die Primideale $\mathfrak{q}$ in $\mathbb{R}[X]$.

Aufgabe 22.17. Es sei $P \in \mathbb{C}[X]$ ein nichtkonstantes Polynom mit der Eigenschaft, dass

$$\mathbb{C}[Y] \longrightarrow \mathbb{C}[X],\ Y \longmapsto P,$$

eine Galoiserweiterung (im Funktionenkörper) ist. Zeige, dass die Zerlegungsgruppe zu einem Primideal $(X-a)$ bis auf endlich viele Ausnahmen trivial ist, und dass sie stets mit der Trägheitsgruppe übereinstimmt.

Aufgabe 22.18. Es sei R ein Dedekindbereich mit Quotientenkörper $K = Q(R)$ und sei $K \subseteq M$ eine endliche Galoiserweiterung mit Galoisgruppe G. Es sei T der ganze Abschluss von R in M. Es sei $N \subseteq G$ ein Normalteiler von G mit Restklassengruppe $H = G/N$ und es sei $S = T^N$ und $L = M^N$ der zugehörige Zwischenring bzw. Zwischenkörper, auf dem H galoissch operiert mit Fixring R. Es sei $\mathfrak{r}$ ein Primideal von T über $\mathfrak{q}$ in S und $\mathfrak{p}$ in R. Zeige, dass ein kommutatives Diagramm

$$\begin{array}{ccc} G_{\mathfrak{r}} & \longrightarrow & \mathrm{Gal}\,(\kappa(\mathfrak{r})|\kappa(\mathfrak{p})) \\ \downarrow & & \downarrow \\ H_{\mathfrak{q}} & \longrightarrow & \mathrm{Gal}\,(\kappa(\mathfrak{q})|\kappa(\mathfrak{p})) \end{array}$$

von Gruppenhomomorphismen vorliegt, wobei die horizontalen Abbildungen von Lemma 22.5 herrühren (alle Erweiterungen der Restekörper seien separabel), die linke Abbildung von Aufgabe 22.5 herrührt und die rechte vertikale Abbildung durch die Körperkette

$$\kappa(\mathfrak{p}) \subseteq \kappa(\mathfrak{q}) \subseteq \kappa(\mathfrak{r})$$

gegeben ist.

Aufgabe 22.19. Bestimme für einen quadratischen Zahlbereich $\mathbb{Q} \subseteq R$, für welche Primzahlen p das Artinsymbol $(p, Q(R)/\mathbb{Q})$ die Identität oder die Konjugation ist.

Aufgabe 22.20.* Es sei $R = \mathbb{Z}[X]/(X^3 - 3X + 1)$. Bestätige für die Primzahlen

$$p = 2, 5, 7, 11, 13, 17,$$

dass in $R/(p) = \mathbb{Z}/(p)[X]/(X^3 - 3X + 1)$ eine der Beziehung

$$X^p = \begin{cases} X \\ X^2 - 2 \\ -X^2 - X + 2 \end{cases}$$

gilt. Wie sieht es bei $p = 3$ aus?

Aufgabe 22.21.* Es sei $R = \mathbb{Z}[X]/(X^3 - 3X + 1)$. Es sei $p \neq 3$ eine Primzahl und K eine Restekörper von $\mathbb{Z}/(p)[X]/(X^3 - 3X + 1)$. Zeige, dass in K eine der Beziehung

$$X^p = \begin{cases} X \\ X^2 - 2 \\ -X^2 - X + 2 \end{cases}$$

gilt. Wie sieht es bei $p = 3$ aus?

Die Situation der beiden vorstehenden Aufgaben wird in Aufgabe 23.16 wieder aufgegriffen.

Aufgabe 22.22. Berechne die Potenzen X^p in $\mathbb{Z}/(p)[X]/(X^3 - 2)$ für die Primzahlen

$$p = 2, 3, \ldots.$$

Gibt es da irgendeine Regelmäßigkeit?

Aufgabe 22.23.*

Es sei ζ eine primitive neunte Einheitswurzel in einem Körper L. Zeige, dass die Elemente

$$\zeta+\zeta^8, \zeta^2+\zeta^7 \text{ und } \zeta^4+\zeta^5$$

die Nullstellen des Polynoms X^3-3X+1 sind.

Aufgabe 22.24. Es sei $\mathbb{Q} \subseteq L$ eine Galoiserweiterung mit einer abelschen Galoisgruppe G und es sei S der zugehörige Zahlbereich. Es sei $N \subseteq G$ eine Untergruppe mit der Restklassengruppe $H = G/N$ und $R = S^N \subseteq K = L^N$. Es sei p eine Primzahl und $\mathfrak{q}$ ein unverzweigtes Primideal von S oberhalb von (p) und $\mathfrak{p} = \mathfrak{q} \cap R$. Zeige unter Verwendung des kommutativen Diagrammes

$$\begin{array}{ccc} G_{\mathfrak{q}} & \longrightarrow & \mathrm{Gal}\,(\kappa(\mathfrak{q})|\mathbb{Z}/(p)) \\ \downarrow & & \downarrow \\ H_{\mathfrak{p}} & \longrightarrow & \mathrm{Gal}\,(\kappa(\mathfrak{p})|\mathbb{Z}/(p)) \end{array}$$

aus Aufgabe 22.18, dass das Artinsymbol $(p, L/\mathbb{Q})$ auf das Artinsymbol $(p, K/\mathbb{Q})$ abgebildet wird.

23. Vorlesung - Zerlegung in Kreisteilungsringen

23.1. **Zerlegung im Kreisteilungsring.**

Wir besprechen die Ergebnisse der letzten Vorlesungen genauer anhand der Kreisteilungsringe. Nach Satz 17.11 liegt eine Galoiserweiterung vor. Auf das Verständnis der Kreisteilungsringe bauen wir einen Beweis des quadratischen Reziprozitätsgesetzes auf.

Lemma 23.1. *Es sei $R_n = \mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring. Dann sind für eine ungerade Primzahl q folgende Aussagen äquivalent.*

1. *q ist ein Teiler von n.*
2. *Das Primideal (q) verzweigt in R_n.*
3. *Das Kreisteilungspolynom Φ_n ist über $\mathbb{Z}/(q)$ nicht separabel.*
4. *Das Polynom X^n-1 ist über $\mathbb{Z}/(q)$ nicht separabel.*
5. *Der Ring $\mathbb{Z}/(q)[X]/(X^n-1)$ ist nicht reduziert.*

Beweis. Von (1) nach (2). Wenn q ein Teiler von n ist, so ist eine q-te Einheitswurzel auch eine n-te Einheitswurzel. Die q-ten Einheitswurzeln lassen sich also als eine Potenz einer primitiven n-ten Einheitswurzel erhalten und deshalb gilt für die Kreisteilungskörper $K_q \subseteq K_n$. Damit ist auch $R_q \subseteq R_n$. Nach Lemma 17.16 in Verbindung mit Satz 18.15 und Satz 18.10 verzweigt (q) in R_q und damit nach Aufgabe 18.10 auch in R_n.

Die Äquivalenz von (2) und (3) ist klar aufgrund von Satz 18.10, Aufgabe 15.7 und Satz 17.18. Von (3) nach (4) ist klar wegen Aufgabe 15.8. Die Äquivalenz von (4) und (5) ist klar.

Von (4) nach (1). Wenn q kein Teiler von n ist, so ist n eine Einheit in $\mathbb{Z}/(q)$ und somit sind X^n-1 und $(X^n-1)'=nX^{n-1}$ teilerfremd über $\mathbb{Z}/(q)$, was nach Aufgabe 15.7 die Separabilität bedeutet. □

Satz 23.2. *Es sei $R_n=\mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring und es sei q eine Primzahl, die kein Teiler von n sei. Es sei f die multiplikative Ordnung von q in $(\mathbb{Z}/(n))^\times$. Dann liegen oberhalb von (q) in $\operatorname{Spek}(R_n)$ genau $\frac{\varphi(n)}{f}$ Primideale, deren Restekörper gleich $\mathbb{F}_{q^f}$ sind.*

Beweis. Nach Voraussetzung ist q kein Teiler von n und damit eine Einheit in $\mathbb{Z}/(n)$. Es gibt deshalb eine wohldefinierte Ordnung f, also die kleinste positive Zahl mit $q^f=1 \mod n$. Dabei ist f ein Teiler von $\varphi(n)$, der Ordnung der Einheitengruppe $(\mathbb{Z}/(n))^\times$. Nach Aufgabe 17.16 ist $\mathbb{F}_{q^f}$ der kleinste Erweiterungskörper von $\mathbb{Z}/(q)$, der n verschiedene Einheitswurzeln enthält.

Wegen Lemma 22.1 und Lemma 23.1 ist lediglich zu zeigen, dass $\mathbb{F}_{q^f}$ der Restekörper der Primideale oberhalb von (q) ist. Betrachten wir also $\mathbb{Z}/(q)[X]/(\Phi_n)$. Da $\mathbb{F}_{q^f}$ eine primitive n-te Einheitswurzel enthält, gibt es eine surjektive Abbildung

$$\mathbb{Z}/(q)[X]/(X^n-1) \longrightarrow \mathbb{F}_{q^f}.$$

Diese faktorisiert nach Lemma 19.9 (Körper- und Galoistheorie (Osnabrück 2018-2019)) durch

$$\mathbb{Z}/(q)[X]/(\Phi_m) \longrightarrow \mathbb{F}_{q^f},$$

wobei m ein Teiler von n ist und dann gibt es auch eine Surjektion

$$\mathbb{Z}/(q)[X]/(X^m-1) \longrightarrow \mathbb{F}_{q^f}.$$

Wenn m ein echter Teiler von n wäre, so würde sich ein Widerspruch ergeben, da dann das Bild von X eine Ordnung $<n$ hätte. □

Die beiden Extremfälle des Zerlegungsverhaltens kann man folgendermaßen herausarbeiten.

Korollar 23.3. *Es sei $R_n=\mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring. Dann sind für eine ungerade Primzahl q folgende Aussagen äquivalent.*

1. *n ist ein Teiler von $q-1$.*
2. *$q=1 \mod n$.*
3. *In $\mathbb{Z}/(q)$ gibt es n n-te Einheitswurzeln.*
4. *Das Polynom X^n-1 zerfällt über $\mathbb{Z}/(q)$ in verschiedene Linearformen.*
5. *Das Kreisteilungspolynom Φ_n zerfällt über $\mathbb{Z}/(q)$ in verschiedene Linearformen.*
6. *Über (q) liegen $\varphi(n)$ Primideale von R_n.*
7. *Das Kreisteilungspolynom Φ_n hat eine Nullstelle in $\mathbb{Z}/(q)$ und q ist nicht verzweigt.*

Beweis. Die Äquivalenz von (1) und (2) und die von (3) und (4) ist klar. Die Einheitengruppe von $\mathbb{Z}/(q)$ ist nach Satz 9.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)) zyklisch mit $q-1$ Elementen, das n-te Potenzieren wird unter dieser Identifizierung zum n-ten Multiplizieren,

$$\mathbb{Z}/(q-1) \longrightarrow \mathbb{Z}/(q-1),\, y \longmapsto ny.$$

Die n-ten Einheitswurzeln entsprechen dabei dem Kern dieser Abbildung. Wenn n ein Teiler von $q-1$ ist, so sei $q-1 = na$. In diesem Fall sind $0, a, 2a, \ldots, (n-1)a$ die verschiedenen Elemente des Kerns, was die Implikation von (1) nach (3) beweist. Umgekehrt besitzt der Kern wie jede Untergruppe von $\mathbb{Z}/(q-1)$ einen Erzeuger a, der ein Teiler von $q-1$ ist. Wenn der Kern aus n Elementen besteht, so ist $an = q-1$, was die andere Implikation beweist.

Von (4) nach (5) ist klar, da das Kreisteilungspolynom ein Teiler von X^n-1 ist. Die Äquivalenz von (5) und (6) ist auch klar, da $\mathbb{Z}/(q)[X]/(\Phi_n)$ der Faserring über (q) ist und da das Kreisteilungspolynom den Grad $\varphi(n)$ besitzt. Die Eigenschaft (5) impliziert unmittelbar den ersten Teil von (7). Wäre q verzweigt in R_n, so wäre q nach Lemma 23.1 ein Teiler von n, sagen wir $n = qc$, und dann wäre

$$X^n - 1 = (X^c - 1)^q$$

über $\mathbb{Z}/(q)$. Doch dann hätte das Kreisteilungspolynom mehrfache Nullstellen.

Von (7) nach (3). Zunächst ist nach Lemma 23.1 q kein Teiler von n, d.h. q ist eine Einheit in $\mathbb{Z}/(n)$. Es sei f die (multiplikative) Ordnung von q in $(\mathbb{Z}/(n))^\times$. Dann gibt es in $\mathbb{F}_{q^f}$ n verschiedene n-te Einheitswurzeln. Nach Voraussetzung gibt es eine Nullstelle ζ des Kreisteilungspolynoms Φ_n über $\mathbb{Z}/(p)$. Dessen Potenzen durchlaufen in $\mathbb{F}_{q^f}$ die n-ten Einheitswurzeln. Da die Potenzen aber zu $\mathbb{Z}/(q)$ gehören, ist $f = 1$. □

Korollar 23.4. *Es sei $R_n = \mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring und es sei q eine Primzahl, die kein Teiler von n sei. Dann sind folgende Aussagen äquivalent.*

1. *Das Element q erzeugt die Einheitengruppe von $\mathbb{Z}/(n)$.*
2. *Über (q) liegt ein Primideal in R_n, d.h. (q) ist unzerlegt im Kreisteilungsring.*
3. *Das Kreisteilungspolynom Φ_n ist irreduzibel über $\mathbb{Z}/(q)$.*

Beweis. Die Eigenschaft (1) bedeutet, dass die Ordnung von q in der Einheitengruppe $(\mathbb{Z}/(n))^\times$ gleich $\varphi(n)$ ist. Somit folgt die Äquivalenz von (1) und (2) aus Satz 23.2. Die Äquivalenz zu (3) ist angesichts der Voraussetzung über die Unverzweigtheit und der expliziten Beschreibung der Kreisteilungsringe klar. □

Bemerkung 23.5. Nach Satz 17.11 in Verbindung mit Satz 21.2 und Satz 17.18 operiert die Galoisgruppe

$$\mathrm{Gal}\,(\mathbb{Q}|K_n) \cong (\mathbb{Z}/(n))^\times$$

auf dem n-ten Kreisteilungsring

$$R_n = \mathbb{Z}[X]/(\Phi_n)$$

derart, dass $a \in (\mathbb{Z}/(n))^\times$ durch die Substitution $X \mapsto X^a$ wirkt. Es sei q eine Primzahl, die kein Teiler von n sei, und es sei $\mathfrak{q}$ ein Primideal oberhalb von (q). Das Element q gehört zur Einheitengruppe $(\mathbb{Z}/(n))^\times$, seine Ordnung sei f, vergleiche Satz 23.2. Zu q gehört der Automorphismus ψ von R_n, der X auf die q-te Potenz von X abbildet, wobei dies nur von der Restklasse von q modulo n abhängt. Dieser stimmt auf dem Faserring $R_n/(q)R_n$ der Charakteristik q mit dem Frobeniushomomorphismus überein, da er auf einem Erzeuger damit übereinstimmt und da der Frobenius auf $\mathbb{Z}/(q)$ die Identität ist. Daher gilt $\psi(\mathfrak{q}) = \mathfrak{q}$ nach Aufgabe 5.39 und ψ gehört zur Zerlegungsgruppe $G_\mathfrak{q}$. Da q die Ordnung f besitzt, und die Zerlegungsgruppe nach Lemma 22.3 (4) f Elemente besitzt, wird die Zerlegungsgruppe von diesem Element erzeugt. Da ψ auf dem Faserring den Frobenius induziert, gilt dies auch auf dessen Restekörpern. Somit wird unter der in Lemma 22.5 (3) beschriebenen natürlichen Korrespondenz zwischen der Zerlegungsgruppe und der Galoisgruppe der Restekörpererweiterungen die Substitution $X \mapsto X^q$ auf den Frobenius abgebildet. Damit ist insbesondere zu jeder Primzahl q das Frobenius-Element (siehe Bemerkung 22.10) im Fall von Kreisteilungsringen explizit gegeben.

Der in der letzten Vorlesung erwähnte Dichtigkeitssatz von Tschebotarjowsch beinhaltet unter Verwendng der vorstehenden Bemerknug im Fall von Kreisteilungsringen den Satz von Dirichlet über Primzahlen in einer arithmetischen Progression. Er besagt, dass die Primzahlen modulo den teilerfremden Resten zu einer gegebenen Zahl n gleichverteilt sind.

23.2. **Das quadratische Reziprozitätsgesetz.**

Das quadratische Reziprozitätsgesetz gehört zu den Hauptresultaten der Zahlentheorie und wurde erstmals von Gauß bewiesen. Es seien p und q verschiedene ungerade Primzahlen. Es geht dann um die Frage, ob p in $\mathbb{Z}/(q)$ ein Quadrat ist, also eine Quadratwurzel besitzt, oder eben nicht. Die Aussage des Satzes ist nun, dass dies in einer direkten Beziehung zu der „reziproken Eigenschaft“ steht, ob q in $\mathbb{Z}/(p)$ ein Quadrat ist. Es gibt eine Reihe von ziemlich verschiedenen Beweise für diesen Satz, auch relativ elementare, siehe beispielsweise die Einführung in die elementare und algebraische Zahlentheorie. Der Nachteile dieser elementaren Beweise ist, dass sie konzeptionell eher undurchsichtig sind. Man kann die Beweise Zeile für Zeile nachprüfen, fragt sich letztlich aber dennoch, warum die Aussage überhaupt stimmt.

Definition 23.6. Für eine ungerade Primzahl p und eine zu p teilerfremde Zahl $k \in \mathbb{Z}$ definiert man das *Legendre-Symbol*, geschrieben $\left(\frac{k}{p}\right)$ (sprich „k nach p“), durch

$$\left(\frac{k}{p}\right) := \begin{cases} 1, \text{ falls } k \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1, \text{ falls } k \text{ kein quadratischer Rest modulo } p \text{ ist.} \end{cases}$$

Für einfache Eigenschaften des Legendre-Symbols siehe den Anhang. Für Vielfache von p im Zähler setzt man das Legendre-Symbol gleich 0. Für die Beziehung zwischen quadratischen Resten und Kreisteilungsringen ist das folgende Konzept entscheidend.

Definition 23.7. Es sei p eine ungerade Primzahl und $\zeta = e^{2\pi \mathrm{i}/p}$ die erste primitive komplexe Einheitswurzel. Dann nennt man

$$g = \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta^r$$

die (erste) *quadratische Gaußsumme*.

Lemma 23.8. *Es sei p eine ungerade Primzahl. Dann gilt für das Quadrat der ersten quadratischen Gaußsumme die Gleichung*

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

Beweis. Die hintere Gleichung beruht auf Satz Anhang 10.8. Nach Definition ist

$$g = \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta^r = \sum_{r=1}^{p-1} \left(\frac{r}{p}\right) \zeta^r.$$

Daher ist

$$\begin{aligned} g^2 &= \left(\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) \zeta^r\right) \left(\sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \zeta^s\right) \\ &= \sum_{1 \le r,s \le p-1} \left(\frac{rs}{p}\right) \zeta^{r+s}. \end{aligned}$$

Mit der neuen Variablen

$$s = rt$$

können wir dies als

$$\begin{aligned} \sum_{1 \le r,t \le p-1} \left(\frac{rrt}{p}\right) \zeta^{r+rt} &= \sum_{1 \le r,t \le p-1} \left(\frac{t}{p}\right) \zeta^{r(1+t)} \\ &= \sum_{1 \le r,t \le p-1,\, t \ne p-1} \left(\frac{t}{p}\right) \zeta^{r(1+t)} + \sum_{1 \le r \le p-1} \left(\frac{-1}{p}\right) \zeta^0 \end{aligned}$$

$$= \sum_{1\leq r,t\leq p-1,\, t\neq p-1} \left(\frac{t}{p}\right)\zeta^{r(1+t)} + (p-1)\left(\frac{-1}{p}\right).$$

Für $t \neq -1$, also t zwischen 1 und $p-2$, ist jedenfalls $\xi = \zeta^{1+t}$ auch eine primitive p-te Einheitswurzel. Für ein solches fixiertes t ist

$$\sum_{1\leq r\leq p-1} \left(\frac{t}{p}\right)\xi^r = \left(\frac{t}{p}\right)\sum_{1\leq r\leq p-1}\xi^r = -\left(\frac{t}{p}\right).$$

Die obige Summe ist also

$$-\sum_{1\leq t\leq p-2}\left(\frac{t}{p}\right) + (p-1)\left(\frac{-1}{p}\right) = -\sum_{1\leq t\leq p-1}\left(\frac{t}{p}\right) + p\left(\frac{-1}{p}\right) = p\left(\frac{-1}{p}\right),$$

da es nach Satz Anhang 10.1 gleich viele Quadrate wie Nichtquadrate in $(\mathbb{Z}/(p))^\times$ gibt. □

Diese Aussage bedeutet insbesondere, dass im p-ten Kreisteilungsring die quadratische Erweiterung zu p oder $-p$ liegt, wobei das Vorzeichen im Lemma mitbestimmt wird.

Lemma 23.9. *Es seien p und q verschiedene ungerade Primzahlen. Es sei S der quadratische Zahlbereich zu $\left(\frac{-1}{p}\right)p$ und es sei R_p der p-te Kreisteilungsring. Es sei f die multiplikative Ordnung von q in $(\mathbb{Z}/(p))^\times$. Dann sind folgende Aussagen äquivalent.*

1. *Es ist $\left(\frac{-1}{p}\right)p$ ein Quadrat in $\mathbb{Z}/(q)$.*
2. *Über (q) liegen in $\operatorname{Spek}(S)$ zwei Primideale.*
3. *Über (q) liegt in $\operatorname{Spek}(R_p)$ eine gerade Anzahl von Primidealen.*
4. *Es ist f ein Teiler von $\frac{p-1}{2}$*
5. *q ist ein Quadrat in $\mathbb{Z}/(p)$.*

Beweis. Die Äquivalenz von (1) und (2) ist klar nach Aufgabe 9.19. Von (2) nach (3). Nach Lemma 23.8 gilt $S \subseteq R_p$, sodass diese Richtung aus Lemma 22.1 folgt, da sich der nichttrivale Automorphismus der quadratischen Erweiterung zu einem Automorphismus des Kreisteilungsringes fortsetzt, der die beiden Fasern vertauscht. Von (3) nach (2). Es sei $\mathfrak{q}$ ein Primideal über (q). Nach Lemma 22.3 (3) ist

$$\#(G_{\mathfrak{q}}) = \operatorname{grad}_{\mathbb{Z}/(q)}\kappa(\mathfrak{q}) = f$$

und nach Voraussetzung ist wegen Lemma 22.1 $\frac{p-1}{f}$ gerade. Nach Aufgabe 22.6 ist $\frac{p-1}{f}$ auch die Anzahl der Primideale über (q) im Zerlegungsring und die Restekörper sind $\mathbb{Z}/(q)$. Da der Index der Zerlegungsgruppe in der zyklischen Galoisgruppe

$$\operatorname{Aut}(R_p) \cong (\mathbb{Z}/(p))^\times \cong (\mathbb{Z}/(p-1),+,0)$$

gerade ist, umfasst der Zerlegungskörper den quadratischen Zahlbereich. Deshalb sind auch dessen Restekörper gleich dem Grundkörper und es liegt im Zahlbereich Zerlegung vor.

Die Äquivalenz von (3) und (4) ist klar aufgrund von Satz 23.2. (4) bedeutet, dass

$$q^{\frac{p-1}{2}} = 1 \mod p,$$

deshalb folgt die Äquivalenz von (4) und (5) aus dem Euler-Kriterium. □

Satz 23.10. *Es seien p und q verschiedene ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} -1\,, & \textit{wenn } p = q = 3 \mod 4\,, \\ 1\,, & \textit{sonst}\,. \end{cases}$$

Beweis. Nach Lemma 23.9 ist unter Verwendung von Lemma Anhang 10.4 und Satz Anhang 10.8

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{\left(\frac{-1}{p}\right) p}{q}\right) \\ &= \left(\frac{\left(\frac{-1}{p}\right)}{q}\right) \cdot \left(\frac{p}{q}\right) \\ &= \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) \cdot \left(\frac{p}{q}\right) \\ &= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) \\ &= \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) \\ &= (-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}} \cdot \left(\frac{p}{q}\right). \end{aligned}$$

□

Rationale Zahlen

23. Arbeitsblatt

23.1. **Aufgaben.**

Aufgabe 23.1. Wo wird im Beweis zu Lemma 23.1 verwendet, dass $q \neq 2$ ist. Welche der angeführten Eigenschaften gelten bei $n = q = 2$, welche nicht? Wie sieht es bei $q = 2$ und $n = 4$ aus?

Aufgabe 23.2. Interpretiere Satz 23.2 im Fall $n = 3$, also im Fall der Eisenstein-Zahlen $R_3 = \mathbb{Z}[\frac{-1+\mathrm{i}}{2}]$. Vergleiche insbesondere mit Aufgabe 9.29.

Aufgabe 23.3. Interpretiere Satz 23.2 im Fall $n = 4$, also im Fall der Gaußschen Zahlen $R_4 = \mathbb{Z}[\mathrm{i}]$. Vergleiche insbesondere mit Aufgabe 9.26.

Aufgabe 23.4. Bestimme das Zerlegungsverhalten im Kreisteilungsring R_7 für die Primzahlen $q = 2, 3, 5, 7, 11, 13, 17, 19$.

Aufgabe 23.5. Bestimme das Zerlegungsverhalten im Kreisteilungsring R_8 für die Primzahlen $q = 2, 3, 5, 7, 11, 13, 17, 19$.

Aufgabe 23.6. Bestimme das Zerlegungsverhalten im Kreisteilungsring R_9 für die Primzahlen $q = 2, 3, 5, 7, 11, 13, 17, 19$.

Aufgabe 23.7. Es sei p eine Primzahl und sei R_p der p-te Kreisteilungsring. Bestimme die Zerlegungsgruppe und die Trägheitsgruppe zu einem Primideal $\mathfrak{q}$ über (p).

Aufgabe 23.8. Es sei $R_n = \mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring und sei p eine Primzahl, die n nicht teile. Es sei f die multiplikative Ordnung von p in der Einheitengruppe $(\mathbb{Z}/(n))^\times$. Zeige, dass p^r genau dann die Norm eines Ideals von R_n ist, wenn r ein Vielfaches von f ist.

Aufgabe 23.9. Untersuche Korollar 23.3 für den Fall $q = 2$, insbesondere bei $n = 1$ und $n = 2$.

Aufgabe 23.10. Zeige, dass Korollar 23.3 (7) ohne die Bedingung der Unverzweigtheit nicht zu den anderen Eigenschaften der Aussage äquivalent ist.

Zur folgenden Aufgabe vergleiche Aufgabe 21.3.

Aufgabe 23.11. Es sei p eine Primzahl und

$$R_p = \mathbb{Z}[X]/\left(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\right)$$

der p-te Kreisteilungsring. Es sei

$$H \subseteq (\mathbb{Z}/(p))^\times \cong \mathrm{Gal}\,(K_p|\mathbb{Q})$$

eine Untergruppe der Galoisgruppe, und es seien

$$H_1 = H,\, H_2, \ldots, H_k \subseteq (\mathbb{Z}/(p))^\times$$

die Nebenklassen zu H. Zeige, dass der Invariantenring R_p^H die Ganzheitsbasis

$$f_j = \sum_{a \in H_j} X^a$$

zu $j = 1, \ldots, k$ besitzt.

Aufgabe 23.12. Bestimme die Ganzheitsbasen für die Unterringe zu sämtlichen Untergruppen der Galoisgruppe in der Situation von Aufgabe 23.11 für $p = 5$.

Aufgabe 23.13.*

Bestimme die Ganzheitsbasen für die Unterringe zu sämtlichen Untergruppen der Galoisgruppe in der Situation von Aufgabe 23.11 für $p = 7$.

Aufgabe 23.14. Bestimme die Ganzheitsbasen für die Unterringe zu sämtlichen Untergruppen der Galoisgruppe in der Situation von Aufgabe 23.11 für $p = 11$.

Aufgabe 23.15.*

Es sei $S = \mathbb{Z}[2\zeta] \subseteq R_5$ der durch 2ζ erzeugte Unterring des fünften Kreisteilungsringes, wobei $\zeta = e^{2\pi \mathrm{i}/5}$ die erste primitive fünfte Einheitswurzel bezeichnet.

(1) Bestimme eine Gleichung für S über $\mathbb{Z}$.
(2) Zeige, dass die Galoisoperation auf dem fünften Kreisteilungskörper keine Gruppenoperation auf S induziert.
(3) Bestimme $S \cap \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Die folgende Aufgabe gibt in Verbindung mit Aufgabe 22.24 eine natürliche Erklärung für das in Aufgabe 22.20 beobachtete Verhalten.

Aufgabe 23.16.*

Wir betrachten die Körperkette

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3-3X+1\right) \subseteq K_9$$

und die zugehörige Kette von Zahlbereichen

$$\mathbb{Z} \subseteq \mathbb{Z}[X]/\left(X^3-3X+1\right) \subseteq R_9.$$

Wenn ζ eine neunte primitive Einheitswurzel bezeichnet, so sei

$$X = \zeta + \zeta^{-1},$$

vergleiche Aufgabe 22.23. Zeige, dass für jede Primzahl $p \neq 3$ in

$$\mathbb{Z}/(p)[X]/\left(X^3-3X+1\right)$$

eine der Beziehung

$$X^p = \begin{cases} X \\ X^2-2 \\ -X^2-X+2 \end{cases}$$

gilt. Zeige ferner, dass es allein von der Restklasse von p modulo 9 abhängt, welche der drei Fälle gilt.

Aufgabe 23.17.*

Zeige, dass im sechsten Kreisteilungsring R_6 weder $\sqrt{6}$ noch $\sqrt{-6}$ enthalten ist.

Aufgabe 23.18. Es sei p eine ungerade Primzahl und

$$g = \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta^r$$

die (erste) quadratische Gaußsumme. Es sei σ ein Automorphismus des p-ten Kreisteilungsringes. Zeige $\sigma(g) = g$ genau dann gilt, wenn unter den Isomorphismen

$$\operatorname{Aut}(R_p) \cong (\mathbb{Z}/(p))^\times \cong (\mathbb{Z}/(p-1),+,0)$$

σ durch eine gerade Zahl repräsentiert wird.

Aufgabe 23.19.*

Berechne mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze das Legendre-Symbol

$$\left(\frac{53}{311}\right).$$

Aufgabe 23.20.*

Berechne mit Hilfe des quadratischen Reziprozitätsgesetzes und seiner Ergänzungssätze das Legendre-Symbol

$$\left(\frac{563}{1231}\right).$$

Bemerkung: 563 und 1231 sind Primzahlen.

Aufgabe 23.21.*

Beschreibe mittels geeigneter Kongruenzbedingungen diejenigen ungeraden Primzahlen p mit der Eigenschaft, dass 7 ein Quadratrest modulo p ist.

Gibt es unendlich viele solche Primzahlen?

24. Vorlesung - Gitter

24.1. **Gitter.**

In der nächsten Vorlesung werden wir einen Zahlbereich über seine reellen und komplexen Einbettungen als Gitter in einem reellen Vektorraum realisieren. Hier besprechen wir die dazu notwendigen Begrifflichkeiten aus der konvexen Geometrie.

Definition 24.1. Es seien $v_1, \ldots, v_n$ linear unabhängige Vektoren im $\mathbb{R}^n$. Dann heißt die Untergruppe $\mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ ein *Gitter* im $\mathbb{R}^n$.

Manchmal spricht man auch von einem vollständigen Gitter. Als Gruppen sind sie isomorph zu $\mathbb{Z}^n$, hier interessieren aber auch Eigenschafen der Einbettung in $\mathbb{R}^n$. Ein Gitter heißt *rational*, wenn die erzeugenden Vektoren zu $\mathbb{Q}^n$ gehören. Das durch die Standardvektoren $e_1, \ldots, e_n$ erzeugte Gitter heißt *Standardgitter*.

Lemma 24.2. *Es seien $v_1, \ldots, v_n$ und $w_1, \ldots, w_n$ Basen im $\mathbb{R}^n$. Dann stimmen die zugehörigen Gitter $\Gamma = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ und $\Delta = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$ genau dann überein, wenn ihre Übergangsmatrix ganzzahlig mit Determinante ± 1 ist.*

Beweis. Es seien M und N die (reellen) Übergangsmatrizen zwischen den beiden Basen, dabei gilt

$$M \circ N = E_n$$

und

$$\det M \cdot \det N = 1$$

nach dem Determinantenmultiplikationsatz. Seien die Gitter gleich. Dann folgt aus $v_j \in \Delta$, dass in

$$v_j = \sum_{i=1}^{n} c_{ij} w_i$$

die Koeffizienten c_{ij} ganzzahlig sind und damit sind die Übergangsmatrizen ganzzahlig. Ihre Determinanten sind somit auch ganzzahlig und aus der Determinantenbedingung folgt, dass die Determinanten 1 oder -1 sein müssen, da dies die einzigen Einheiten in $\mathbb{Z}$ sind.

Wenn beide Übergangsmatrizen ganzzahlig sind, so gilt

$$\Gamma \subseteq \Delta \subseteq \Gamma$$

und damit Gleichheit. □

Beispiel 24.3. Das Standardgitter Γ im $\mathbb{R}^2$ wird durch die Standardbasis e_1, e_2 erzeugt, aber auch durch die beiden Vektoren $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$, siehe Lemma 24.2.

Satz 24.4. *Zu einem Gitter $\Gamma = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n \subseteq \mathbb{R}^n$ ist die topologische Restklassengruppe $\mathbb{R}^n/\Gamma$ isomorph zum n-dimensionalen Torus $S^1 \times \cdots \times S^1$ (mit n Faktoren).*

Beweis. Nach Aufgabe 24.3 können wir davon ausgehen, dass Γ das Standardgitter $\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ ist. Für dieses gilt

$$\mathbb{R}^n/(\mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n) = (\mathbb{R}/\mathbb{Z}e_1) \times \cdots \times (\mathbb{R}/\mathbb{Z}e_n) = S^1 \times \cdots \times S^1.$$

□

24.2. **Konvexe Mengen.**

Definition 24.5. Eine Teilmenge $T \subseteq \mathbb{R}^n$ heißt *konvex*, wenn mit je zwei Punkten $P, Q \in T$ auch jeder Punkt der Verbindungsstrecke, also jeder Punkt der Form

$$rP + (1-r)Q \text{ mit } r \in [0,1]\,,$$

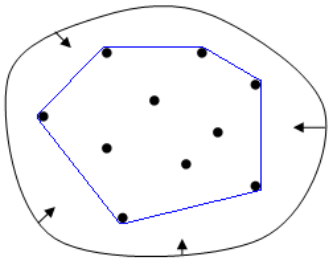
ebenfalls zu T gehört.

Der Durchschnitt von konvexen Teilmengen ist wieder konvex. Daher kann man definieren.

Definition 24.6. Zu einer Teilmenge $U \subseteq \mathbb{R}^n$ heißt die kleinste konvexe Teilmenge T, die U umfasst, die *konvexe Hülle* von U.

Die konvexe Hülle ist einfach der Durchschnitt von allen konvexen Teilmengen, die U umfassen.

Im zweidimensionalen kann man sich die konvexe Hülle so vorstellen, dass man eine Schnur um die fixierten Punkte aus U legt und die Schnur dann zusammen zieht. Dreidimensional nehme man ein Stofftuch.



Definition 24.7. Zu einem durch linear unabhängige Vektoren $v_1, \ldots, v_n$ gegebenen Gitter bezeichnet man die konvexe Hülle der Vektoren $\epsilon_1 v_1 + \cdots + \epsilon_n v_n$ mit $\epsilon_i \in \{0, 1\}$ als die *Grundmasche* (oder *Fundamentalmasche*) des Gitters.

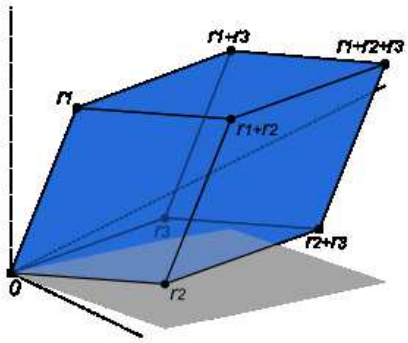
Die in der vorstehenden Definition auftauchenden Vektoren sind die Eckpunkte des von den Basisvektoren $v_1, \ldots, v_n$ erzeugten Parallelotops. Die Elemente der Grundmasche selbst sind alle Vektoren der Form

$$r_1 v_1 + \cdots + r_n v_n \text{ mit } r_i \in [0, 1]$$

Wir werden die Grundmasche häufig mit $\mathfrak{M}$ bezeichnen. Zu einem Gitterpunkt P nennt man die Menge $P + \mathfrak{M}$ eine *Masche* des Gitters. Ein beliebiger Punkt $Q \in \mathbb{R}^n$ hat eine eindeutige Darstellung $Q = t_1 v_1 + \cdots + t_n v_n$ und damit ist

$$Q = (\lfloor t_1 \rfloor v_1 + \cdots + \lfloor t_n \rfloor v_n) + ((t_1 - \lfloor t_1 \rfloor) v_1 + \cdots + (t_n - \lfloor t_n \rfloor) v_n),$$

wobei der erste Summand zum Gitter gehört und der zweite Summand zur Grundmasche. Insbesondere haben zwei verschiedene Maschen nur Randpunkte, aber keine inneren Punkte gemeinsam.



Da ein Gitter keine wohldefinierte Gitterbasis besitzt, gibt es eine wohldefinierte Grundmasche nur dann, wenn eine Gitterbasis fixiert wurde, siehe Beispiel 24.3. Allerdings, und dies ist entscheidend, ist das Volumen einer Grundmasche unabhängig von der Gitterbasis und hängt nur vom Gitter selbst ab. Dies folgt aus Lemma 24.2 in Verbindung mit Satz 67.2 (Analysis (Osnabrück 2014-2016)). Das Volumen eines Parallelotops und insbesondere einer Grundmasche kann man mit den beiden folgenden Sätzen berechnen. Vergleiche die Definition der Diskriminante und Lemma 8.9

Satz 24.8. *Es sei $v_1, \ldots, v_n$ eine Basis im $\mathbb{R}^n$ und sei P das davon erzeugte Parallelotop. Dann gilt für das Borel-Lebesgue-Maß λ auf $\mathbb{R}^n$*

$$\lambda(P) = |\det(v_1, \ldots, v_n)|,$$

wobei in der Matrix die Koordinaten von v_i bezüglich der Standardbasis stehen.

Beweis. Dies ist der entscheidende Schritt zum Beweis zu Satz 67.2 (Analysis (Osnabrück 2014-2016)), siehe den Beweis dort. □

Satz 24.9. *Es sei $(V, \langle -, - \rangle)$ ein euklidischer Vektorraum, sei $v_1, \ldots, v_n$ eine Basis von V und sei P das davon erzeugte Parallelotop. Dann gilt für das Borel-Lebesgue-Maß λ_V auf V*

$$\lambda_V(P) = (\det(\langle v_i, v_j \rangle)_{1 \leq i,j \leq n})^{1/2}.$$

Beweis. Für den Beweis siehe Satz 67.8 (Analysis (Osnabrück 2014-2016)). □

24.3. **Der Gitterpunktsatz von Minkowski.**

Hermann Minkowski (1864-1909)

Definition 24.10. Eine Teilmenge $T \subseteq \mathbb{R}^n$ heißt *zentralsymmetrisch*, wenn mit jedem Punkt $P \in T$ auch der Punkt $-P$ zu T gehört.

Definition 24.11. Ein topologischer Raum X heißt *kompakt* (oder *überdeckungskompakt*), wenn es zu jeder offenen Überdeckung

$$X = \bigcup_{i \in I} U_i \quad \text{mit } U_i \text{ offen und einer beliebigen Indexmenge } I$$

eine endliche Teilmenge $J \subseteq I$ derart gibt, dass

$$X = \bigcup_{i \in J} U_i$$

ist.

Nach dem Satz von Heine-Borel ist eine Teilmenge des $\mathbb{R}^n$ genau dann kompakt, wenn sie beschränkt und abgeschlossen ist. Ein weiterer im Folgenden wichtiger Aspekt ist, dass disjunkte kompakte Teilmengen $Y, Z \subseteq \mathbb{R}^n$ einen positiven Abstand haben, dass es also ein $d > 0$ mit

$$d(P, Q) > d$$

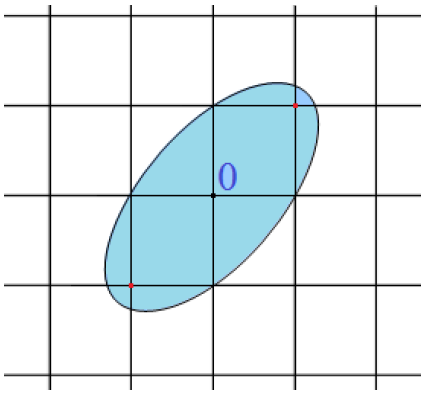
für alle $P \in X$ und $Q \in Y$ gibt, siehe Aufgabe 24.14. Es wird auch der Minimalabstand angenommen, siehe Aufgabe 24.15.

Der folgende Satz heißt *Gitterpunktsatz von Minkowski*.

Satz 24.12. *Sei Γ ein Gitter im $\mathbb{R}^n$ mit Grundmasche $\mathfrak{M}$. Es sei T eine konvexe, kompakte, zentralsymmetrische Teilmenge in $\mathbb{R}^n$, die zusätzlich die Volumenbedingung*

$$\mathrm{Vol}(T) \geq 2^n \,\mathrm{Vol}(\mathfrak{M})$$

erfülle. Dann enthält T mindestens einen von 0 verschiedenen Gitterpunkt.



Beweis. Wir betrachten das verdoppelte Gitter 2Γ. Ist $v_1, \ldots, v_n$ eine Basis für Γ, so ist $2v_1, \ldots, 2v_n$ eine Basis für 2Γ. Wir bezeichnen die Grundmasche von 2Γ mit $\mathfrak{N}$, für ihr Volumen gilt $\mathrm{Vol}(\mathfrak{N}) = 2^n \mathrm{Vol}(\mathfrak{M})$. Zu jeder Masche $\mathfrak{N}_Q = Q + \mathfrak{N}$, $Q \in 2\Gamma$, betrachten wir den Durchschnitt

$$T_Q = T \cap \mathfrak{N}_Q.$$

Da T kompakt und insbesondere beschränkt ist, gibt es nur endlich viele Maschen derart, dass dieser Durchschnitt nicht leer ist. Seien diese Maschen (bzw. ihre Ausgangspunkte bzw. ihre Durchschnitte) mit $\mathfrak{N}_i$ (bzw. Q_i bzw. T_i) $i \in I$, bezeichnet (da der Nullpunkt aufgrund der Konvexität und der Zentralsymmetrie zu T gehört, umfasst I zumindest 2^n Elemente). Die in die Grundmasche $\mathfrak{N}$ verschobenen Durchschnitte bezeichnen wir mit

$$\tilde{T}_i := T_i - Q_i.$$

Wir behaupten zunächst, dass die $\tilde{T}_i$ nicht paarweise disjunkt sind. Sei also angenommen, sie wären paarweise disjunkt. Mindestens eines der T_i (und damit der $\tilde{T}_i$) hat positives Volumen, sagen wir für $i = 1$. Wegen der angenommenen Disjunktheit sind insbesondere

$$X := \tilde{T}_1 \text{ und } Y := \bigcup_{i \in I, i \neq 1} \tilde{T}_i$$

disjunkt zueinander. Wir haben also zwei disjunkte kompakte Teilmengen, und diese besitzen einen Minimalabstand d (d.h. zu jedem Punkt aus X liegen in einer d-Umgebung keine Punkte aus Y, siehe Aufgabe 24.14). Sei $x \in X$ ein innerer Punkt (den es gibt, da X konvex ist und ein positives Volumen besitzt) und sei $y \in Y$. Mit S sei die Verbindungsstrecke von x nach y bezeichnet, die ganz in $\mathfrak{N}$ verläuft. Wir wählen einen Punkt $s \in S$, der weder zu X noch zu Y gehört (solche Punkte gibt es wegen des Minimalabstandes). Da s sowohl zu X als auch zu Y einen Minimalabstand besitzt, gibt es eine ϵ-Umgebung B von s, die disjunkt zu X und Y ist. Wir können

ferner annehmen, dass B ganz innerhalb von $\mathfrak{N}$ liegt (wegen der Wahl von x). Als eine Ballumgebung hat B ein positives Volumen, was zu folgendem Widerspruch führt.

$$\begin{aligned}
\mathrm{Vol}(\mathfrak{N}) &\geq \mathrm{Vol}(X \cup Y \cup B) \\
&= \mathrm{Vol}\left(\bigcup_{i\in I} \tilde{T}_i\right) + \mathrm{Vol}(B) \\
&> \sum_{i\in I} \mathrm{Vol}(\tilde{T}_i) \\
&= \sum_{i\in I} \mathrm{Vol}(T_i) \\
&= \mathrm{Vol}(T) \\
&\geq 2^n \,\mathrm{Vol}(\mathfrak{M}) \\
&= \mathrm{Vol}(\mathfrak{N}).
\end{aligned}$$

Es gibt also Indizes $i \neq j$ und einen Punkt $z \in \tilde{T}_i \cap \tilde{T}_j$ (z muss selbst nicht zu T gehören). Sei

$$z_i := z + Q_i \in T_i \text{ und } z_j := z + Q_j \in T_j\,.$$

Wegen $Q_i, Q_j \in 2\Gamma$ ist auch $Q_i - Q_j \in 2\Gamma$ und daher

$$0 \neq \frac{Q_i - Q_j}{2} \in \Gamma.$$

Aus $z_j \in T$ folgt (wegen der Zentralsymmetrie) auch $-z_j \in T$ und wegen der Konvexität von T ergibt sich

$$\frac{Q_i - Q_j}{2} = \frac{1}{2}(z_i - z) - \frac{1}{2}(z_j - z) = \frac{1}{2}z_i - \frac{1}{2}z_j \in T.$$

Wir haben also einen von Nullpunkt verschiedenen Gitterpunkt in T gefunden. □

24. Arbeitsblatt

24.1. **Aufgaben.**

Aufgabe 24.1. Zeige, dass der Einheitskreis

$$S^1_{\mathbb{R}} = \{z \in \mathbb{R}[\mathrm{i}] \cong \mathbb{C} \mid |z| = 1\}$$

isomorph zu $\mathbb{R}/\mathbb{Z}$ ist.

Aufgabe 24.2. Charakterisiere die Restklassengruppe eines Gitters $\Gamma \subseteq \mathbb{R}^n$.

Aufgabe 24.3. Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{R}^n$ vollständige Gitter. Zeige, dass es eine $\mathbb{R}$-lineare Abbildung

$$\mathbb{R}^n \longrightarrow \mathbb{R}^n$$

gibt, die einen Gruppenisomorphismus

$$\Gamma_1 \longrightarrow \Gamma_2$$

induziert.

Aufgabe 24.4. Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{R}^n$ rationale vollständige Gitter. Zeige, dass es eine $\mathbb{Q}$-lineare Abbildung

$$\mathbb{Q}^n \longrightarrow \mathbb{Q}^n$$

gibt, die einen Gruppenisomorphismus

$$\Gamma_1 \longrightarrow \Gamma_2$$

induziert.

Aufgabe 24.5. Es seien $\Gamma_1, \Gamma_2 \subseteq \mathbb{R}^n$ rationale vollständige Gitter. Zeige, dass es ein rationales Gitter $\Gamma \subseteq \mathbb{R}^n$ mit $\Gamma_1, \Gamma_2 \subseteq \Gamma$ gibt.

Aufgabe 24.6. Alle Springmäuse leben in $\mathbb{Z}^2$ und verfügen über zwei Sprünge, nämlich den Sprung $\pm(3,4)$ und den Sprung $\pm(5,2)$. Wie viele Springmaus-Populationen gibt es? Die Springmäuse Albert, Beate, Erich, Heinz, Sabine und Frida sitzen in den Positionen

$$(14,11),\ (13,15),\ (17,12),\ (15,19),\ (16,16) \text{ und } (12,20)\,.$$

Welche Springmäuse können sich begegnen?

Aufgabe 24.7. Sind alle Vierecke konvex?

Aufgabe 24.8. Zeige, dass der Durchschnitt von konvexen Mengen wieder konvex ist.

Aufgabe 24.9. Sei U eine Teilmenge des $\mathbb{R}^n$. Zeige, dass ein Punkt $Q \in \mathbb{R}^n$ genau dann zur konvexen Hülle von U gehört, wenn es endlich viele Punkte $P_i \in U$, $i \in I$, und reelle Zahlen r_i, $i \in I$, mit $r_i \in [0,1]$, $\sum_{i \in I} r_i = 1$ und mit

$$Q = \sum_{i \in I} r_i P_i$$

gibt.

Aufgabe 24.10. Es sei X ein Hausdorffraum und es sei $Y \subseteq X$ eine Teilmenge, die die induzierte Topologie trage. Es sei Y kompakt. Zeige, dass Y abgeschlossen in X ist.

Aufgabe 24.11. Es sei X ein topologischer Raum und es seien $Y_1, \ldots, Y_n \subseteq X$ kompakte Teilmengen. Zeige, dass auch die Vereinigung $Y = \bigcup_{i=1}^{n} Y_i$ kompakt ist.

Aufgabe 24.12. Es sei X ein Hausdorff-Raum, $Y \subseteq X$ eine kompakte Teilmenge und $P \notin Y$ ein Punkt. Zeige, dass es offene disjunkte Mengen $U, V \subseteq X$ mit $Y \subseteq U$ und $P \in V$ gibt.

Aufgabe 24.13. Es sei X ein Hausdorff-Raum und seien $Y, Z \subseteq X$ kompakte Teilmengen, die zueinander disjunkt seien. Zeige, dass es offene disjunkte Mengen $U, V \subseteq X$ mit $Y \subseteq U$ und $Z \subseteq V$ gibt.

Aufgabe 24.14. Es sei X ein metrischer Raum und seien $Y, Z \subseteq X$ kompakte Teilmengen, die zueinander disjunkt seien. Zeige, dass es ein $d > 0$ derart gibt, dass für beliebige Punkte $P \in Y$ und $Q \in Z$ die Abstandsbedingung $d(P, Q) \geq d$ gilt.

Aufgabe 24.15. Es seien $X, Y \subseteq \mathbb{R}^n$ kompakte Teilmengen. Zeige, dass es Punkte $x \in X$ und $y \in Y$ mit der Eigenschaft gibt, dass für beliebige Punkte $P \in X$ und $Q \in Y$ die Abschätzung

$$d(x, y) \leq d(P, Q)$$

gilt.

Tipp: Betrachte die Produktmenge $S \times T \subseteq \mathbb{R}^n \times \mathbb{R}^n \cong \mathbb{R}^{2n}$ und darauf die Abbildung $(x, y) \mapsto \sum_{i=1}^{n} (x_i - y_i)^2$. Argumentiere dann mit Satz 36.12 (Analysis (Osnabrück 2014-2016)).

Aufgabe 24.16. Skizziere zum Gitter $\mathbb{Z}^2$ in $\mathbb{R}^2$ drei Teilmengen, die die Maßbedingung des Gitterpunksatzes von Minkowski erfüllen, die den Nullpunkt, aber keine weiteren Gitterpunkte enthalten, und die jeweils zwei der drei Bedingungen konvex, kompakt und zentralsymmetrisch erfüllen.

25. Vorlesung - Zahlbereiche als Gitter

25.1. **Zahlbereiche als Gitter.**

Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung vom Grad n. Gemäß Satz 7.12 gibt es n verschiedene Einbettungen von K in $\mathbb{C}$. Diese kann man zur komplexen Gesamteinbettung

$$\tau\colon K \longrightarrow \mathbb{C}^n$$

zusammenfassen. Insbesondere ist das Bild des Ganzheitsringes R unter dieser Abbildung interessant und erlaubt einen Zugang zu R, bei dem Methoden der diskreten Geometrie, der linearen Algebra, der Maßtheorie eingesetzt werden können. Nach Korollar 8.6 ist

$$R \cong \mathbb{Z}^n,$$

wobei die Standardbasis einer Ganzheitsbasis $b_1, \ldots, b_n$ von R entspricht. Diese legt die komplexe Ganzheitsmatrix

$$(\tau_j(b_k))_{1 \leq j,k \leq n}$$

fest. Sie definiert ein „komplexes Gitter“ im $\mathbb{C}^n$, das Quadrat ihrer Determinante ist nach Lemma 8.9 die Diskriminante, u.s.w. Allerdings entwickeln die angesprochen Methoden ihre Schlagkraft deutlicher, wenn man zu der komplexen Gesamteinbettung eine reelle Version entwickelt.

Bei einer Einbettung

$$\sigma\colon K \longrightarrow \mathbb{C}$$

unterscheidet man, ob das Bild innerhalb der reellen Zahlen liegt oder nicht. Im ersten Fall spricht man von einer *reellen Einbettung*. Wenn σ keine reelle Einbettung ist, so spricht man von einer komplexen Einbettung, in diesem Sinn ist also eine reelle Einbettung nicht komplex. Zu einer komplexen Einbettung σ ist auch die konjugiert-komplexe Einbettung

$$\overline{\sigma} : K \xrightarrow{\sigma} \mathbb{C} \xrightarrow{\text{komplexe Konjugation}} \mathbb{C}$$

eine komplexe Einbettung, und zwar ist $\sigma \neq \overline{\sigma}$, denn sonst wäre σ eine reelle Einbettung. Komplexe Einbettungen treten also immer paarweise auf. Es sei r die Anzahl der reellen Einbettungen und $2s$ die Anzahl der komplexen Einbettungen, also s sei die Anzahl der Paare von komplexen Einbettungen. Dann gilt

$$n = r + 2s.$$

Häufig fixiert man zu jedem Paar von komplexen Einbettungen eine Einbettung davon, da sich die andere daraus direkt ablesen lässt. Die Wahl ist dabei willkürlich. Alle numerisch möglichen Kombinationen von r und s treten auch auf.

Es seien ρ_i, $i = 1, \ldots, r$ die reellen Einbettungen und σ_j, $j = 1, \ldots, s$ Repräsentanten der Paare von komplexen Einbettungen. Dies definiert eine Gesamteinbettung

$$K \longrightarrow \mathbb{R}^r \times \mathbb{C}^s,$$

die wir die *reelle Gesamteinbettung* nennen. Wenn man einzelne komplexe Einbettungen durch ihre konjugierten Einbettungen ersetzt, so ergibt sich ein natürlicher $\mathbb{R}$-linearer Isomorphismus. Dabei gilt als reeller Vektorraum

$$\mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^r \times \mathbb{R}^{2s} = \mathbb{R}^n,$$

d.h. die reelle Dimension des Einbettungsraumes stimmt mit dem Grad der Körpererweiterung überein. Zwischen der reellen Gesamteinbettung und der komplexen Gesamteinbettung besteht der Zusammenhang

$$\begin{array}{ccc} K & \xrightarrow{\tau^{\mathbb{R}}} & \mathbb{R}^r \times \mathbb{C}^s \\ & \tau \searrow & \downarrow \psi \\ & & \mathbb{C}^{r+2s} \end{array},$$

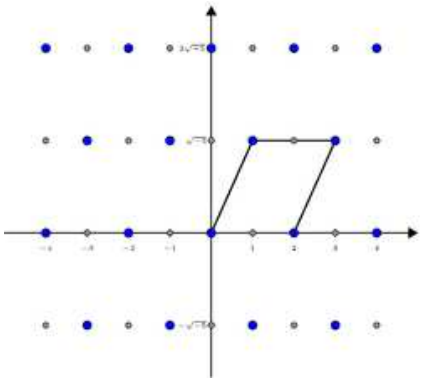
wobei ψ in den ersten r Komponenten die natürliche Einbettung $\mathbb{R} \subset \mathbb{C}$ und in den hinteren Komponenten die Abbildung $\mathbb{C} \to \mathbb{C} \times \mathbb{C}$, $z \mapsto (z, \overline{z})$, ist. Somit ist ψ eine $\mathbb{R}$-lineare Abbildung. Ein Element $b \in K$ wird unter der reellen Gesamteinbettung auf

$$\tau^{\mathbb{R}}(b) = \begin{pmatrix} \rho_1(b) \\ \vdots \\ \rho_r(b) \\ \text{Re } (\sigma_1(b)) \\ \text{Im } (\sigma_1(b)) \\ \vdots \\ \text{Re } (\sigma_s(b)) \\ \text{Im } (\sigma_s(b)) \end{pmatrix}$$

und unter der komplexen Gesamteinbettung auf

$$\tau(b) = \begin{pmatrix} \rho_1(b) \\ \vdots \\ \rho_r(b) \\ \sigma_1(b) \\ \overline{\sigma}_1(b) \\ \vdots \\ \sigma_s(b) \\ \overline{\sigma}_s(b) \end{pmatrix}$$

abgebildet.



Das Gitter zum Zahlbereich $\mathbb{Z}[\sqrt{-5}]$ und zum Ideal $(2, 1+\sqrt{-5})$ (blau, mit einer Grundmasche).

Die reelle Gesamtabbildung ist trivialerweise injektiv, da sie ja sogar in jeder einzelnen Komponente injektiv ist. Für die Gittertheorie der algebraischen Zahlen (Minkowski-Theorie) ist aber entscheidend, dass das Bild des Rings der ganzen Zahlen ein Gitter in diesem $\mathbb{R}^n$ ist, also nicht in einem reellen Untervektorraum kleinerer Dimension liegt. Der Zahlbereich wird auf ein Gitter abgebildet, eine Ganzheitsbasis auf eine Gitterbasis.

Definition 25.1. Es sei R ein Zahlbereich vom Grad n mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Es sei

$$\tau^{\mathbb{R}} \colon R \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^r \times \mathbb{R}^{2s}$$

die reelle Gesamteinbettung. Es sei $b_1, \ldots, b_n$ eine Ganzheitsbasis von R. Dann nennt man die reelle $n \times n$-Matrix

$$\left(\tau_j^{\mathbb{R}}(b_k)\right)_{1 \leq j,k \leq n}$$

die *reelle Ganzheitsmatrix* (zu dieser Basis).

Die reelle Ganzheitsmatrix steht mit der komplexen Ganzheitsmatrix in dem oben durch ψ beschriebenen Zusammenhang.

Satz 25.2. *Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung vom Grad n mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Es sei*

$$\tau^{\mathbb{R}} \colon K \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$$

die reelle Gesamteinbettung. Dann ist das Bild des Ganzheitsringes von K unter τ ein Gitter in $\mathbb{R}^n$

Beweis. Es sei $b_1, \ldots, b_n$ eine Ganzheitsbasis von R. Es ist zu zeigen, dass die $\tau^{\mathbb{R}}(b_k)$, $k = 1, \ldots, n$, linear unabhängig sind. Über die $\mathbb{R}$-lineare Abbildung

$$\mathbb{R}^r \times \mathbb{R}^{2s} \longrightarrow \mathbb{C}^r \times \mathbb{C}^{2s}, \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ u_1 \\ v_1 \\ \vdots \\ u_s \\ v_s \end{pmatrix} \longmapsto \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ u_1 + \mathrm{i}v_1 \\ u_1 - \mathrm{i}v_1 \\ \vdots \\ u_s + \mathrm{i}v_s \\ u_s - \mathrm{i}v_s \end{pmatrix},$$

erhält man aus der reellen Gesamteinbettung die komplexe Gesamteinbettung. Wären die Elemente $\mathbb{R}$-linear abhängig, so würde das auch für die Bilder unter der komplexen Gesamteinbettung gelten. Doch dies wäre ein Widerspruch zur Tatsache, dass die Diskriminante von $b_1, \ldots, b_n$ nicht 0 ist, siehe Lemma 8.3. $\square$

Wir werden dieses Gitter im $\mathbb{R}^n$ zumeist mit Γ oder Γ_R oder Γ_K bezeichnen. Die reelle Gesamteinbettung liefert einen Gruppenisomorphismus $R \cong \Gamma \subseteq \mathbb{R}^n$.

Beispiel 25.3. Es sei $D < 0$ quadratfrei und A_D der zugehörige imaginär-quadratische Zahlbereich. Dann liefert eine fixierte Einbettung $A_D \subseteq \mathbb{Q}[\sqrt{D}] \subseteq \mathbb{C} \cong \mathbb{R}^2$ direkt eine Realisierung als Gitter im Sinne von Satz 25.2. Dem Element $q_1 + q_2\sqrt{D} = q_1 + q_2\sqrt{|D|}\mathrm{i}$ entspricht in der reellen Ebene das Element $\begin{pmatrix} q_1 \\ q_2\sqrt{-D)} \end{pmatrix} = \begin{pmatrix} q_1 \\ q_2\sqrt{|D|)} \end{pmatrix}$. Die Ganzheitsbasis $1, \sqrt{D}$ bei $D = 2, 3 \mod 4$ bzw. $1, \frac{1+\sqrt{D}}{2}$ bei $D = 1 \mod 4$ (vergleiche Satz 9.8) wird unter der reellen Gesamteinbettung auf die reelle Ganzheitsmatrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{|D|} \end{pmatrix}$$

bzw.

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|D|}}{2} \end{pmatrix}$$

abgebildet.

Beispiel 25.4. Es sei $D \geq 2$ quadratfrei und $A_D \subseteq \mathbb{Q}[\sqrt{D}] = K$ der zugehörige reell-quadratische Zahlbereich. Es sei $\sqrt{D}$ einerseits ein fixierte Quadratwurzel aus D in A_D und andererseits die positive reelle Quadratwurzel. Die Abbildung

$$K \longrightarrow \mathbb{R}^2, (q_1 + q_2\sqrt{D}) \longmapsto \begin{pmatrix} q_1 + q_2\sqrt{D} \\ q_1 - q_2\sqrt{D} \end{pmatrix},$$

ist dann die reelle Gesamteinbettung und liefert insbesondere eine explizite Realisierung von A_D als Gitter im Sinne von Satz 25.2. Das Gitter hängt wie die Ganzheitsbasis für A_D vom Rest von D modulo 4 ab, siehe Satz 9.8.

Die Ganzheitsbasis $1, \sqrt{D}$ bei $D = 2, 3 \mod 4$ bzw. $1, \frac{1+\sqrt{D}}{2}$ bei $D = 1 \mod 4$ (vergleiche Satz 9.8) wird unter der reellen Gesamteinbettung auf die reelle Ganzheitsmatrix

$$\begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}$$

bzw.

$$\begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix}$$

abgebildet.

Wenn $\mathbb{Q} \subseteq K$ eine Galoiserweiterung mit einer fixierten reellen Einbettung ρ ist, so sind alle Einbettungen reell, und die gesamte Gitterabbildung wird durch

$$R \longrightarrow \mathbb{R}^n,\ f \longmapsto (\rho(\sigma(f)), \sigma \in \operatorname{Gal}(K|\mathbb{Q}))$$

realisiert.

Beispiel 25.5. Die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}[X]/(X^3 - 3X + 1) = K$ ist eine Galoiserweiterung, wenn $\alpha \in \mathbb{R}$ eine Nullstelle von $X^3 - 3X + 1$, so sind auch $\beta = \alpha^2 - 2$ und $\gamma = -\alpha^2 - \alpha + 2$ Nullstellen, siehe Aufgabe 5.31. Die Galoisgruppe permutiert diese Nullstellen. Der Automorphismus, der α auf $\alpha^2 - 2$ abbildet, schickt α^2 auf

$$\left(\alpha^2 - 2\right)^2 = \alpha^4 - 4\alpha^2 + 4 = 3\alpha^2 - \alpha - 4\alpha^2 + 4 = -\alpha^2 - \alpha + 4.$$

Wegen

$$R = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2$$

wird die gesamte Gitterabbildung durch

$$R \cong \mathbb{Z}^3 \longrightarrow \mathbb{R}^3,\ a + b\alpha + c\alpha^2 \longmapsto \begin{pmatrix} a + b\alpha + c\alpha^2 \\ a + b(\alpha^2 - 2) + c(-\alpha^2 - \alpha + 4) \\ a + b(-\alpha^2 - \alpha + 2) + c(\alpha + 2) \end{pmatrix},$$

gegeben. Die Basis $1, \alpha, \alpha^2$ wird auf die Gitterbasis

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \alpha \\ \alpha^2 - 2 \\ -\alpha^2 - \alpha + 4 \end{pmatrix}, \begin{pmatrix} \alpha^2 \\ -\alpha^2 - \alpha + 4 \\ \alpha + 2 \end{pmatrix}$$

abgebildet.

Wenn man $1, \alpha, \beta$ als Ganzheitsbasis nimmt, so wird die Abbildung durch

$$R \cong \mathbb{Z}^3 \longrightarrow \mathbb{R}^3,\ a + b\alpha + d\beta \longmapsto \begin{pmatrix} a + b\alpha + d\beta \\ a + b\beta + d(-\alpha - \beta) \\ a + b(-\alpha - \beta) + d\alpha \end{pmatrix},$$

beschrieben. Diese Basis wird dann auf die Gitterbasis

$$\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}\alpha\\ \beta\\ -\alpha-\beta\end{pmatrix}, \begin{pmatrix}\beta\\ -\alpha-\beta\\ \alpha\end{pmatrix}$$

abgebildet.

Satz 25.6. *Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Es sei $\mathfrak{M}$ eine Grundmasche des Gitters Γ_R unter der reellen Gesamteinbettung*

$$\tau^{\mathbb{R}}\colon\ R \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^r \times \mathbb{R}^{2s}.$$

Dann ist das Volumen der Grundmasche bezüglich der euklidischen Standardmetrik des $\mathbb{R}^r \times \mathbb{R}^{2s}$ gleich

$$\operatorname{Vol}(\mathfrak{M}) \ = \ \frac{1}{2^s}\sqrt{|\triangle_R|}.$$

Beweis. Wir haben die Zusammenstellung zu allen komplexen Einbettungen

$$\tau\colon\ R \longrightarrow \mathbb{C}^{r+2s}$$

und die reelle Gittereinbettung

$$\tau^{\mathbb{R}}\colon\ R \longrightarrow \mathbb{R}^r \times \mathbb{C}^s,$$

die durch die Einbettung

$$\mathbb{R}^r \times \mathbb{C}^s \longrightarrow \mathbb{C}^{r+2s},\ (x_1,\ldots,x_r;z_1,\ldots,z_s) \longmapsto (x_1,\ldots,x_r;z_1,\overline{z_1},\ldots,z_s,\overline{z_s})$$

miteinander verbunden sind.

Zu einer $\mathbb{Q}$-Basis $b_1,\ldots,b_n$ von $Q(R)$ haben wir einerseits die reelle Ganzheitsmatrix

$$\begin{pmatrix}
\rho_1(b_1) & \rho_1(b_2) & \ldots & \ldots & \rho_1(b_n)\\
\vdots & \vdots & \ddots & \ddots & \vdots\\
\rho_r(b_1) & \rho_r(b_2) & \ldots & \ldots & \rho_r(b_n)\\
\operatorname{Re}\,(\sigma_1(b_1)) & \operatorname{Re}\,(\sigma_1(b_2)) & \ldots & \ldots & \operatorname{Re}\,(\sigma_1(b_n))\\
\operatorname{Im}\,(\sigma_1(b_1)) & \operatorname{Im}\,(\sigma_1(b_2)) & \ldots & \ldots & \operatorname{Im}\,(\sigma_1(b_n))\\
\vdots & \vdots & \ddots & \ddots & \vdots\\
\operatorname{Re}\,(\sigma_s(b_1)) & \operatorname{Re}\,(\sigma_s(b_2)) & \ldots & \ldots & \operatorname{Re}\,(\sigma_s(b_n))\\
\operatorname{Im}\,(\sigma_s(b_1)) & \operatorname{Im}\,(\sigma_s(b_2)) & \ldots & \ldots & \operatorname{Im}\,(\sigma_s(b_n))
\end{pmatrix}$$

und andererseits die komplexe Ganzheitsmatrix

$$\begin{pmatrix} \rho_1(b_1) & \rho_1(b_2) & \dots & \dots & \rho_1(b_n) \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \rho_r(b_1) & \rho_r(b_2) & \dots & \dots & \rho_r(b_n) \\ \sigma_1(b_1) & \sigma_1(b_2) & \dots & \dots & \sigma_1(b_n) \\ \overline{\sigma}_1(b_1) & \overline{\sigma}_1(b_2) & \dots & \dots & \overline{\sigma}_1(b_n) \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \sigma_s(b_1) & \sigma_s(b_2) & \dots & \dots & \sigma_s(b_n) \\ \overline{\sigma}_s(b_1) & \overline{\sigma}_s(b_2) & \dots & \dots & \overline{\sigma}_s(b_n) \end{pmatrix}.$$

Wenn man diese komplexe Matrix mit der Matrix (diese steht links)

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 1 & 1 & & & \\ & & & -\mathrm{i} & \mathrm{i} & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

multipliziert, wobei der quadratische Block sich auf σ_j und $\overline{\sigma}_j$ bezieht, so erhält man in der Zeile zu σ_j das Doppelte des Realteils von σ_j und in der darauf folgenden Zeile das Doppelte des Imaginärteils von σ_j. Die Determinante der zuletzt notierten Matrix ist 2i. Wenn man diese Multiplikation für jede komplexe Doppelzeile durchführt (s Multiplikationen), so erhält man die Matrix, die aus der reellen Ganhzeitsmatrix hervorgeht, indem man die hinteren $2s$ Zeilen jeweils mit 2 multipliziert. Deshalb gilt insgesamt

$$2^{2s}\big(\det\big(\tau_j^{\mathbb{R}}(b_k)\big)\big) \;=\; 2^s\mathrm{i}^s(\det\left(\tau_j(b_k)\right)).$$

Nach Lemma 8.9 und Satz 24.8 ist

$$\begin{aligned} \sqrt{|\triangle(b_1,\dots,b_n)|} &= |(\det\left(\tau_j(b_k)\right))| \\ &= 2^s\big(\det\big(\tau_j^{\mathbb{R}}(b_k)\big)\big) \\ &= 2^s\,\mathrm{Vol}(\mathfrak{M}). \end{aligned}$$

□

Beispiel 25.7. Es sei $D < 0$ quadratfrei und A_D der zugehörige imaginärquadratische Zahlbereich. Es gibt also $s = 1$ Paare von zueinander komplexkonjugierten Einbettungen. Zur Ganzheitsbasis $1, \sqrt{D}$ bei $D = 2, 3 \mod 4$ bzw. $1, \frac{1+\sqrt{D}}{2}$ bei $D = 1 \mod 4$ gehört wie in Beispiel 25.3 berechnet die reelle Ganzheitsmatrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{|D|} \end{pmatrix}$$

bzw.

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|D|}}{2} \end{pmatrix}.$$

Deren Determinante, also bis auf das Vorzeichen der Flächeninhalt der Grundmasche des Gitters, ist

$$\det \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{|D|} \end{pmatrix} = \sqrt{|D|}$$

bzw.

$$\det \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|D|}}{2} \end{pmatrix} = \frac{\sqrt{|D|}}{2}.$$

Die Diskriminante ist nach Lemma 9.9 gleich $4D$ bzw. D. In beiden Fällen erhält man also eine direkte Bestätigung von Satz 25.6.

Beispiel 25.8. Es sei $D > 2$ quadratfrei und A_D der zugehörige reell-quadratische Zahlbereich. Es gibt also zwei reelle Einbettungen und somit ist $s = 0$. Zur Ganzheitsbasis $1, \sqrt{D}$ bei $D = 2, 3 \mod 4$ bzw. $1, \frac{1+\sqrt{D}}{2}$ bei $D = 1 \mod 4$ gehört wie in Beispiel 25.4 berechnet die reelle Ganzheitsmatrix

$$\begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}$$

bzw.

$$\begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix}$$

Deren Determinante ist

$$\det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix} = -2\sqrt{D}$$

bzw.

$$\det \begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix} = \frac{1-\sqrt{D}}{2} - \frac{1+\sqrt{D}}{2} = -\sqrt{D}.$$

Die Diskriminante ist nach Lemma 9.9 gleich $4D$ bzw. D. In beiden Fällen erhält man also wieder eine direkte Bestätigung von Satz 25.6.

Satz 25.9. *Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Es sei $\mathfrak{a} \subseteq R$ ein von 0 verschiedenes Ideal und es sei $\mathfrak{N}$ eine Grundmasche des vollständigen Gitters $\tau^{\mathbb{R}}(\mathfrak{a})$. Dann ist das Volumen von $\mathfrak{N}$ (bezüglich der euklidischen Standardmetrik des $\mathbb{R}^r \times \mathbb{R}^{2s}$) gleich*

$$\mathrm{Vol}(\mathfrak{N}) = \frac{1}{2^s}\sqrt{|\triangle_R|} \cdot N(\mathfrak{a}).$$

Beweis. Das wird ähnlich wie Satz 25.6 bewiesen. □

25. Arbeitsblatt

25.1. **Aufgaben.**

Aufgabe 25.1.*

Es sei R ein Zahlbereich ohne reelle Einbettung. Zeige, dass die Norm eines jeden Elementes $x \in R$, $x \neq 0$, positiv ist.

Aufgabe 25.2. Bestimme die Anzahl der reellen und der komplexen Einbettungen von

$$K = \mathbb{Q}[X]/\big(X^3 + 2X - 1\big).$$

Aufgabe 25.3. Es sei $P \in \mathbb{Z}[X]$ ein normiertes irreduzibles Polynom vom Grad d und $K = \mathbb{Q}[X]/(P)$. Woran erkennt man am Graphen von P die Anzahl der reellen Einbettungen und die Anzahl der Paare von komplexen Einbettungen von K?

Aufgabe 25.4. Bestimme für $\mathbb{Z}$ für die Ganzheitsbasis 1 (und die Ganzheitsbasis -1) die komplexe Ganzheitsmatrix und die reelle Ganzheitsmatrix.

Aufgabe 25.5. Bestimme für die Ganzheitsbasis $1, \mathrm{i}$ von $\mathbb{Z}[\mathrm{i}]$ die komplexe Ganzheitsmatrix und die reelle Ganzheitsmatrix. Bestimme den Flächeninhalt der Grundmasche des zugehörigen Gitters.

Aufgabe 25.6.*

Bestimme die reelle Ganzheitsmatrix zur Ganzheitsbasis $1, \sqrt[3]{2}, \sqrt[3]{4}$ des kubischen Zahlbereiches $\mathbb{Z}[\sqrt[3]{2}]$.

Aufgabe 25.7.*

Bestimme die reelle Ganzheitsmatrix zur Ganzheitsbasis $\zeta, \zeta^2, \zeta^3, \zeta^4$ des fünften Kreisteilungsringes, wobei $\zeta = e^{\frac{2\pi \mathrm{i}}{5}} = \cos\frac{2\pi}{5} + \mathrm{i}\sin\frac{2\pi}{5}$ die primitive fünfte Einheitswurzel ist.

Aufgabe 25.8. Bestimme die reelle Ganzheitsmatrix zur Ganzheitsbasis $1, X, X^2, X^3$ des achten Kreisteilungsringes

$$R_8 = \mathbb{Z}[X]/\big(X^4 + 1\big).$$

Verwende, dass die komplexen Einbettungen dadurch gegeben sind, dass X auf eine primitive achte Einheitswurzel abgebildet wird, und dass diese die Gestalt $\zeta = \pm\frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}\mathrm{i}$ besitzen.

Aufgabe 25.9. Es sei $\mathbb{Q} \subseteq K$ eine Galoiserweiterung vom Grad n. Zeige, dass für die Anzahl r der reellen Einbettungen $r = 0$ oder $r = n$ gilt.

Aufgabe 25.10. Bestimme sämtliche quadratischen Zahlbereiche R mit der Eigenschaft, dass der Flächeninhalt der Grundmasche des zugehörigen Gitters Γ_R gleich 1 ist.

Aufgabe 25.11. Studiere den Beweis zu Satz 25.6 am Beispiel von $\mathbb{Z}$[i]

Aufgabe 25.12.*

Überprüfe Satz 25.6 am Beispiel des kubischen Zahlbereiches $\mathbb{Z}[\sqrt[3]{2}]$ (siehe Lemma 16.5 zur Berechnung der Diskriminante und Aufgabe 25.6 zur Bestimmung der reellen Ganzheitsmatrix).

26. Vorlesung - Die Endlichkeit der Klassenzahl

26.1. Die Endlichkeit der Klassenzahl.

Das Ziel dieser Vorlesung ist es, die Endlichkeit der Idealklassengruppe eines Zahlbereichs zu beweisen. Dies geschieht mit den Gittermethoden der beiden letzten Vorlesungen. Diese Methoden erlauben es prinzipiell auch, die Idealklassengruppe algorithmisch zu berechnen und zu entscheiden, ob ein Zahlbereich faktoriell ist oder nicht.

Lemma 26.1. *Es sei R ein Zahlbereich. Dann gibt es nur endlich viele Ideale $\mathfrak{a}$ in R, deren Norm unterhalb einer gewissen Zahl liegt.*

Beweis. Es genügt zu zeigen, dass es zu einer natürlichen Zahl n nur endlich viele Ideale $\mathfrak{a}$ in R mit $N(\mathfrak{a}) = n$ gibt. Sei also $\mathfrak{a}$ ein solches Ideal. Dann ist $n \in \mathfrak{a}$ nach Lemma 10.5 und damit entspricht $\mathfrak{a}$ einem Ideal aus $R/(n)$. Dieser Ring ist aber nach Satz 9.14 endlich und besitzt somit überhaupt nur endlich viele Ideale. □

Lemma 26.2. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und s Paaren von komplexen Einbettungen. Es sei $\mathfrak{a} \neq 0$ ein Ideal. Es sei d_τ eine Familie von n positiven reellen Zahlen zu jeder reellen oder komplexen Einbettung, wobei für konjugiert komplexe Einbettungen die gleiche Zahl vorliege. Ferner gelte*

$$\prod_\tau d_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|} N(\mathfrak{a})$$

Dann gibt es ein $f \in \mathfrak{a}$, $f \neq 0$, mit der Eigenschaft

$$|\tau(f)| < d_\tau$$

für alle τ.

Beweis. Wir nummerieren die Einbettungen mit $1, \dots, r$ für die reellen und $r+1, r+2, \dots, r+2s-1, r+2s$ durch, wobei die konjugiert-komplexen Einbettungen nebeneinander stehen. Wir betrachten die Menge

$$\begin{aligned} M &= \big\{(x_1, \dots, x_r, x_{r+1}, \dots, x_{r+2s}) \in \mathbb{R}^{r+2s} \mid |x_j| < d_j \\ &\quad \text{für } j = 1, \dots, r,\ x_{r+j}^2 + x_{r+j+1}^2 < d_{r+j}^2 \text{ für } j = 1, 3, \dots, 2s-1\big\}. \end{aligned}$$

Dies ist eine Produktmenge aus r Intervallen der Länge $2d_j$ und s Kreisscheiben mit den Radien d_j. Diese Menge ist offensichtlich zentralsymmetrisch und konvex ist. Die Menge ist so nicht kompakt. Wir können aber jedes r_j derart verkleinern, dass die Bedingung nach wie vor erfüllt ist und dann in der entsprechenden Menge $\leq$ statt $<$ schreiben. Da die Menge ein Produkt aus Intervallen und Kreisen ist, ist ihr Volumen gleich

$$2^r \prod_{j=1}^{r} d_j \cdot \pi^s \prod_{j=r+1}^{r+2s} d_j \;=\; 2^r \pi^s \prod_{j=1}^{n} d_j$$

(man beachte, dass der Flächeninhalt des Kreises durch das zweifache Vorkommen der höheren d_j berücksichtigt wird). Nach Voraussetzung und nach Satz 25.9 ist dieses Volumen größer als

$$\begin{aligned} 2^r \pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|} N(\mathfrak{a}) &= 2^{r+s} \sqrt{|\Delta|} N(\mathfrak{a}) \\ &= 2^{r+s} 2^s \operatorname{Vol}(\mathfrak{N}) \\ &= 2^n \operatorname{Vol}(\mathfrak{N}), \end{aligned}$$

wobei $\mathfrak{N}$ die Grundmasche des Gitters zum Ideal $\mathfrak{a}$ unter der reellen Gesamteinbettung bezeichnet. Nach dem Gitterpunktsatz von Minkowski gibt es einen Gitterpunkt $\neq 0$, der in M liegt. D.h. es gibt ein $f \in \mathfrak{a}$ mit $|\tau_j(f)| < d_j$ für alle j. □

Korollar 26.3. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und s Paaren von komplexen Einbettungen. Es sei d_τ eine Familie von positiven reellen Zahlen zu jeder reellen oder komplexen Einbettung, wobei für konjugiert komplexe Einbettungen die gleiche Zahl vorliege. Ferner gelte*

$$\prod_{\tau} d_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|}$$

Dann gibt es ein $f \in R$, $f \neq 0$, mit der Eigenschaft

$$|\tau(f)| < d_\tau$$

für alle τ.

Beweis. Dies folgt direkt aus Lemma 26.2, angewendet auf das Einheitsideal $\mathfrak{a} = R$. □

Korollar 26.4. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und mit s Paaren von komplexen Einbettungen. Dann enthält jedes Ideal $\mathfrak{a} \neq 0$ ein Element $f \in \mathfrak{a}$, $f \neq 0$, das die Normschranke*

$$|N(f)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|} N(\mathfrak{a})$$

erfüllt.

Beweis. Für jede Wahl von positiven reellen Zahlen d_τ (wobei τ die komplexen Einbettungen durchläuft, und wobei die Paarbedingung für nichtreelles τ gelte) mit

$$\prod_\tau d_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta|} N(\mathfrak{a})$$

gibt es nach Lemma 26.2 ein $f \in \mathfrak{a}$, $f \neq 0$, mit

$$|\tau(f)| < d_\tau$$

für jede komplexe Einbettung τ. Nach Lemma 7.14 ist somit

$$|N(f)| = \prod_\tau |\tau(f)| < \prod_\tau d_\tau.$$

Würde es kein f mit Betragsnorm unterhalb (einschließlich) der angegebenen Grenze geben, könnte man daraus direkt einen Widerspruch produzieren. □

Lemma 26.5. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und mit s Paaren von komplexen Einbettungen. Dann enthält jede Idealklasse aus der Klassengruppe ein Ideal $\mathfrak{a} \subseteq R$, das die Normschranke*

$$N(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|}$$

erfüllt.

Beweis. Es sei $\mathfrak{c}$ die Idealklasse. Die inverse Idealklasse $\mathfrak{c}^{-1}$ sei durch das Ideal $\mathfrak{b} \subseteq R$ repräsentiert, siehe Lemma 13.5. Nach Korollar 26.4 gibt es ein $f \in \mathfrak{b}$ mit

$$N(f) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|} N(\mathfrak{b}).$$

Dann ist $f \cdot \mathfrak{b}^{-1}$ ein Ideal, da ja $\mathfrak{b}^{-1}$ alle Elemente aus $\mathfrak{b}$ nach R multipliziert, und das $\mathfrak{c}$ repräsentiert. Nach Korollar 12.14 ist

$$N(f \cdot \mathfrak{b}^{-1}) = N(f) N(\mathfrak{b})^{-1} \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|} N(\mathfrak{b}) N(\mathfrak{b})^{-1} = \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|}.$$

□

Satz 26.6. *Es sei R ein Zahlbereich. Dann ist die Divisorenklassengruppe von R eine endliche Gruppe.*

Beweis. Nach Lemma 26.5 wird jede Klasse in der Klassengruppe durch ein Ideal mit einer Norm repräsentiert, die durch die dort angegebene Schranke beschränkt ist. D.h., dass die Ideale mit einer Norm unterhalb dieser Schranke alle Klassen repräsentieren. Nach Lemma 26.1 gibt es aber überhaupt nur endlich viele Ideale mit einer Norm unterhalb einer gegebenen Schranke. □

Das im Beweis verwendete Lemma bietet prinzipiell eine Abschätzung für die Anzahl der Klassengruppe.

Definition 26.7. Es sei R ein Zahlbereich. Dann nennt man die Anzahl der Elemente in der Klassengruppe von R die *Klassenzahl* von R.

Es ist üblich, die Klassenzahl mit h_R (oder h_K, wenn K der Quotientenkörper ist) zu bezeichnen.

Korollar 26.8. *Es sei R ein Zahlbereich und sei $\mathfrak{a}$ ein Ideal in R. Dann gibt es ein $n \geq 1$ derart, dass $\mathfrak{a}^n$ ein Hauptideal ist.*

Beweis. Für das Nullideal ist die Aussage richtig, sei also $\mathfrak{a}$ von 0 verschieden. Die zugehörige Idealklasse $[\mathfrak{a}]$ besitzt aufgrund von Satz 26.6 in der Idealklassengruppe endliche Ordnung, d.h., dass für ein $n \geq 1$

$$[\mathfrak{a}^n] = [\mathfrak{a}]^n = 0$$

ist. Dies bedeutet aber gerade, dass $\mathfrak{a}^n$ ein Hauptideal ist. □

Wir formulieren noch explizit die folgenden Kriterien für Faktorialität.

Korollar 26.9. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und s Paaren von komplexen Einbettungen. Es sei vorausgesetzt, dass jedes Primideal $\mathfrak{p}$ in R, das die Normbedingung*

$$N(\mathfrak{p}) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|}$$

erfüllt, ein Hauptideal sei. Dann ist R faktoriell.

Beweis. Es sei $\mathfrak{a}$ ein Ideal $\neq 0$ unterhalb der angegebenen Normschranke. Nach Satz 12.2 ist $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ mit Primidealen $\mathfrak{p}_i$, und wegen Korollar 12.14 sind die Normen dieser Primideale ebenfalls unter der Schranke. Da all diese Primideale nach Voraussetzung Hauptideale sind, ist auch $\mathfrak{a}$ ein Hauptideal. Da nach Lemma 26.5 jede Idealklasse durch ein Ideal unterhalb der Normschranke repräsentiert wird, bedeutet dies, dass jede Idealklasse durch ein Hauptideal repräsentiert wird. Das heißt die Klassengruppe ist trivial und damit ist nach Satz 14.2 der Ring R faktoriell. □

Korollar 26.10. *Es sei R ein Zahlbereich mit Diskriminante $\triangle$ und s Paaren von komplexen Einbettungen. Es sei vorausgesetzt, dass jede Primzahl p, die die Normbedingung*

$$p \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle|}$$

erfüllt, ein Primfaktorzerlegung besitzt. Dann ist R faktoriell.

Beweis. Es sei $\mathfrak{p}$ ein Primideal derart, dass $N(\mathfrak{p})$ unterhalb der angegebenen Schranke liegt, und es sei $\mathbb{Z}p = \mathfrak{p} \cap \mathbb{Z}$ mit einer Primzahl p. Nach Korollar 8.8 ist die Norm von $\mathfrak{p}$ gleich p^i mit $i \leq n$, so dass auch p unterhalb der Schranke ist und somit nach Voraussetzung eine Primfaktorzerlegung für p besteht. Daraus folgt aber, dass $\mathfrak{p}$ ein Hauptideal ist. Aus Korollar 26.9 folgt die Behauptung. □

Korollar 26.11. *Es sei $D \neq 0, 1$ eine quadratfreie Zahl und sei A_D der zugehörige quadratische Zahlbereich mit Diskriminante $\triangle$. Es sei vorausgesetzt, dass jede Primzahl p mit*

$$p \leq \begin{cases} \frac{2\sqrt{|\triangle|}}{\pi} & \text{bei } D < 0\,, \\ \frac{\sqrt{|\triangle|}}{2} & \text{bei } D > 0\,. \end{cases}$$

in A_D eine Primfaktorzerlegung besitzt. Dann ist A_D faktoriell.

Beweis. Für $D < 0$ folgt dies direkt aus Korollar 26.10, für $D > 0$ erfordert dies eine zusätzliche Überlegung. □

Beispiel 26.12. Es sei $R = \mathbb{Z}[\sqrt{-5}]$, also $D = -5$ und $\triangle = -20$. Jede Idealklasse enthält ein Ideal $\mathfrak{a}$ der Norm

$$N(\mathfrak{a}) \leq \frac{2\sqrt{20}}{\pi},$$

so dass nur Ideale mit Norm 2 zu betrachten sind. Ein Ideal $\mathfrak{a}$ mit $N(\mathfrak{a}) = 2$ ist ein Primideal $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = (2)$. Daher ist

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

die einzige Möglichkeit. Nach Beispiel 10.7 ist $\mathfrak{p}$ kein Hauptideal. Daher ist die Idealklassengruppe isomorph zu $\mathbb{Z}/(2)$, wobei das Nullelement durch die Hauptdivisoren (oder Hauptideale) repräsentiert wird und das andere Element durch $\mathfrak{p}$.

Beispiel 26.13. Es sei $R = A_{-19}$ der quadratische Zahlbereich zu $D = -19$, also $A_{-19} = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ bzw. $A_{-19} \cong \mathbb{Z}[Y]/(Y^2 - Y + 5)$. Wir wissen aufgrund von Satz Anhang 2.9, dass R nicht euklidisch ist. Dennoch ist R faktoriell und nach Satz . ein Hauptidealbereich und die Klassengruppe ist trivial. Hierfür benutzen wir Korollar 26.11, d.h. wir haben für alle Primzahlen $p \leq \frac{2\sqrt{|\triangle|}}{\pi}$ zu zeigen, dass sie eine Primfaktorzerlegung in R besitzen. Diese Abschätzung wird nur von $p = 2$ erfüllt. Für $p = 2$ ist der Restklassenring

$$R/(2) \cong \mathbb{Z}/(2)[Y]/(Y^2 + Y + 1)$$

ein Körper, so dass 2 träge in R ist und insbesondere eine Primfaktorzerlegung besitzt.

Beispiel 26.14. Wir wollen zeigen, dass der fünfte Kreisteilungsring

$$R_5 = \mathbb{Z}[X]/\big(X^4+X^3+X^2+X+1\big)$$

faktoriell ist. Es gibt vier komplexe Einbettungen und die Diskriminante ist nach Lemma 17.16 gleich ± 125. Wegen

$$\left(\frac{2}{\pi}\right)^2 \sqrt{125} < 5$$

ist nach Korollar 26.10 nur zu überprüfen, ob die Primzahlen $p = 2, 3$ in R_5 eine Primfaktorzerlegung besitzen. Da $\mathbb{Z}/(2)[X]/(X^4+X^3+X^2+X+1)$ und $\mathbb{Z}/(3)[X]/(X^4+X^3+X^2+X+1)$ Körper sind (vergleiche Satz 23.2), sind 2 und 3 sogar Primelemente in R_5.

Bemerkung 26.15. Für ein vorgegebenes quadratfreies D kann man grundsätzlich effektiv entscheiden, ob der quadratische Zahlbereich A_D faktoriell ist oder nicht. Für $D < 0$ ist dies genau für

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

der Fall. Es war bereits von Gauß vermutet worden, dass dies alle sind, es wurde aber erst 1967 von Heegner und Stark bewiesen. Man weiß auch, für welche von diesen D der Ganzheitsbereich euklidisch ist, nämlich nach Satz Anhang 2.9 für $D = -1, -2, -3, -7, -11$, aber nicht für die anderen vier Werte.

Für $D > 0$ wird vermutet, dass für unendlich viele Werte der Ganzheitsbereich faktoriell ist. Für $D < 100$ liegt ein faktorieller Bereich für die Werte

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47,$$

$$53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$$

vor. Dagegen weiß man (Chatland und Davenport 1950), für welche positiven D der Ganzheitsbereich A_D euklidisch ist, nämlich für

$$D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

26. Arbeitsblatt

26.1. **Aufgaben.**

Aufgabe 26.1. Es sei R ein Zahlbereich und $\mathfrak{a} \neq 0$ ein Ideal in R. Zeige, dass es ein Element $f \in \mathfrak{a}$ mit der Eigenschaft gibt, dass für alle maximale Ideale $\mathfrak{m}$ gilt:

$$f \in \mathfrak{m} \text{ genau dann, wenn } \mathfrak{a} \subseteq \mathfrak{m}\,.$$

Aufgabe 26.2. Es sei R ein Zahlbereich und $\mathfrak{a} \neq 0$ ein Ideal in R. Zeige, dass es eine natürliche Zahl $m \in \mathbb{N}$ derart gibt, dass das inverse Ideal $\mathfrak{a}^{-1}$ zu $\mathfrak{a}^m$ äquivalent ist.

Aufgabe 26.3. Es sei R ein Zahlbereich. Zeige, dass es ein $f \in R$, $f \neq 0$, mit der Eigenschaft gibt, dass die Nenneraufnahme R_f faktoriell ist.

Aufgabe 26.4. Es sei $X = \operatorname{Spek}(R)$ das Spektrum eines Zahlbereiches. Zeige, dass jede offene Menge von X von der Form $D(f)$ mit einem $f \in R$ ist.

Aufgabe 26.5. Zeige mit Korollar 26.11, dass der Ring der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}]$ faktoriell ist.

Aufgabe 26.6. Sei $R = A_{13}$ der quadratische Zahlbereich zu $D = 13$. Zeige mittels Korollar 26.11, dass R faktoriell ist.

Aufgabe 26.7. Sei $R = A_{-43}$ der quadratische Zahlbereich zu $D = -43$. Zeige mittels Korollar 26.11, dass R faktoriell ist.

Aufgabe 26.8. Sei $R = A_{-67}$ der quadratische Zahlbereich zu $D = -67$. Zeige mittels Korollar 26.11, dass R faktoriell ist.

Aufgabe 26.9. Es sei D quadratfrei und sei A_D der zugehörige quadratische Zahlbereich. Ferner sei D ein Vielfaches von 5 und $D = 2, 3 \mod 4$. Zeige: A_D ist nicht faktoriell.

Tipp: Siehe Aufgabe 10.2.

Aufgabe 26.10. Zeige, dass der siebte Kreisteilungsring R_7 faktoriell ist.

Aufgabe 26.11.*

Zeige, dass der achte Kreisteilungsring $R_8 = \mathbb{Z}[X]/(X^4 + 1)$ faktoriell ist.

Bemerkung: Der Betrag der Diskriminante von R_8 ist 256.

27. Vorlesung - Einheitswurzeln

27.1. **Einheitswurzeln in Zahlbereichen.**

Eine Einheitswurzel in einem kommutativen Ring R ist das gleiche wie eine Torsionseinheit, also ein Element $x \in R$ mit $x^n = 1$ für ein $n \in \mathbb{N}_+$. Die Menge aller Einheitswurzeln bilden eine Untergruppe der Einheitengruppe $R^\times$. Wir bezeichnen sie mit $\mu(R)$. Ebenso bildet die Menge aller n-ten Einheitswurzeln eine Untergruppe, die wir mit $\mu_n(R)$ bezeichnen. Da eine n-te Einheitswurzel eine Nullstelle des Polynoms $X^n - 1$ ist, gibt es über einem Körper und damit auch über einem Integritätsbereich nach Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) maximal n Nullstellen. Für einen Integritätsbereich ist also $\mu_n(R)$ eine endliche Gruppe mit höchstens n Elementen. Nach Satz 9.5 (Körper- und Galoistheorie (Osnabrück 2018-2019)) handelt es sich um eine zyklische Gruppe. Wenn sie die Ordnung n besitzt, so nennt man einen Erzeuger eine *primitive Einheitswurzel*. Für die abstrakte multiplikative geschrieben zyklische Gruppe mit n Elementen schreiben wir μ_n und die Eigenschaft, dass ein Körper K n n-te Einheitswurzeln besitzt schreiben wir kurz als $\mu_n \subseteq K$.

Lemma 27.1. *Es sei R ein normaler Integritätsbereich mit Quotientenkörper $Q(R)$. Dann ist $\mu(R) = \mu(Q(R))$.*

Beweis. Die Inklusion $\mu(R) \subseteq \mu(Q(R))$ ist klar. Sei $q \in \mu(Q(R))$, sagen wir $q^n = 1$. Da q die Ganzheitsgleichung

$$X^n - 1 = 0$$

erfüllt, folgt aus der Normalität direkt, dass $q \in R$ gehört. □

Diese Beobachtung kann man für Zahlbereiche anwenden. Wir werden im Folgenden die Aussagen für die Zahlbereiche formulieren, wobei die Argumente teilweise über die Quotientenkörper, also über endliche Erweiterungen von $\mathbb{Q}$, gehen, teilweise über den Zahlbereich selbst. Ohne die Voraussetzung normal ist die Aussage nicht richtig, wie das folgende Beispiel zeigt.

Beispiel 27.2. Wir betrachten den Ring

$$R = \mathbb{Z}[2\mathrm{i}] \subseteq \mathbb{Z}[\mathrm{i}] \subseteq \mathbb{Q}[\mathrm{i}] = K.$$

Der Quotientenkörper von R ist $\mathbb{Q}[\mathrm{i}]$, R ist nicht normal. In R gibt es nur die Einheitswurzeln 1 und -1, im Quotientenkörper gibt es dagegen die Einheitswurzeln $1, -1, \mathrm{i}, -\mathrm{i}$.

Lemma 27.3. *Es sei R ein Zahlbereich, für den es zumindest eine reelle Einbettung gebe. Dann ist die Gruppe der Einheitswurzeln $\mu(R)$ gleich $\{1, -1\}$.*

Beweis. Dies folgt direkt aus einer Inklusion $R \subseteq Q(R) \subseteq \mathbb{R}$, da es in $\mathbb{R}$ nur die beiden Einheitswurzeln 1 und -1 gibt und da Einheitswurzeln unter einem Ringhomomorphismus auf Einheitswurzeln abgebildet werden. □

In den komplexen Zahlen gibt es alle Einheitswurzeln. Die Kreisteilungskörper und Kreisteilungsringe zeigen, dass man Einheitswurzeln in endlichen Erweiterungen von $\mathbb{Q}$ bzw. $\mathbb{Z}$ realisieren lassen. Die folgenden Aussagen zeigen, dass die Kreisteilungskörper im Wesentlichen durch ihre enthaltenen Einheitswurzeln bestimmt sind.

Lemma 27.4. *Es sei K ein Körper der Charakteristik 0 und sei $n \in \mathbb{N}$. Dann enthält K genau dann eine primitive n-te Einheitswurzel, wenn für den n-ten Kreisteilungskörper $K_n \subseteq K$ gilt.*

Beweis. Die eine Richtung ist klar. Für die Rückrichtung sei $\zeta \in K$ eine primitive n-te Einheitswurzel. Dies definiert einen Einsetzungshomomorphismus

$$\mathbb{Q}[X]/(X^n - 1) \longrightarrow K,\, X \longmapsto \zeta.$$

Somit gibt es nach Lemma 19.9 (Körper- und Galoistheorie (Osnabrück 2018-2019)) einen induzierten Ringhomomorphismus

$$\mathbb{Q}[X]/(\Phi_d) \longrightarrow K$$

mit einem Teiler d von n. Doch dann gibt es auch einen Ringhomomorphismus

$$\mathbb{Q}[X]/(X^d - 1) \longrightarrow K,\, X \longmapsto \zeta.$$

Bei $d < n$ ist dies ein Widerspruch zur Ordnung von ζ. Also ist $d = n$ und es gibt einen Ringhomomorphismus

$$K_n = \mathbb{Q}[X]/(\Phi_n) \longrightarrow K.$$

□

Lemma 27.5. *Die Einheitswurzelgruppe des n-ten Kreisteilungskörpers K_n ist*

$$\mu(K_n) = \mu_n$$

bei n gerade und

$$\mu(K_n) = \mu_{2n}$$

bei n ungerade.

Beweis. Nach Konstruktion der Kreisteilungskörper ist klar, dass K_n die n-ten Einheitswurzeln enthält. Wenn n ungerade und ζ eine primitive n-te Einheitswurzel ist, so ist $-\zeta$ eine primitive $2n$-te Einheitswurzel und somit sind die Inklusionen $\supseteq$ klar. Es ist also noch zu zeigen, dass die Kreisteilungskörper keine weiteren Einheitswurzeln enthält. Dazu können wir annehmen, dass n gerade ist. Sei ξ eine zusätzliche Einheitswurzel der Ordnung m. Wir können annehmen, dass m gerade und ein echtes Vielfaches von n ist, da die von ξ und einer primitiven n-ten Einheitswurzel ζ erzeugte Untergruppe wieder endlich und zyklisch und ihre Ordnung ein Vielfaches der beiden Ordnungen sein muss. Aus $\mu_m \subseteq K_n$ folgt $K_m \subseteq K_n$ nach Lemma 27.4. Es ist $m = 2^r p_1^{r_1} \cdots p_k^{r_k}$ und $n = 2^s p_1^{s_1} \cdots p_k^{s_k}$ mit $r \geq s \geq 1$ und $r_j \geq s_j \geq 1$. Da ein Exponent echt größer ist, ergibt sich ein Widerspruch zu Satz 17.10.

□

Lemma 27.6. *Es sei R ein Zahlbereich. Dann ist $\mu(R)$ endlich und zyklisch.*

Beweis. Wir argumentieren in der endlichen Erweiterung $\mathbb{Q} \subseteq K = Q(R)$, die den Grad d habe. Wir behaupten zunächst, dass die Ordnungen in $\mu(K)$ beschränkt ist. Nehmen wir an, dass dies nicht der Fall ist, und sei r_n, $n \in \mathbb{N}$, eine streng wachsende (und damit unbeschränkte) Folge von natürlichen Zahlen, die als Ordnungen von Elementen aus $\mu(K)$ vorkommen. Dann gilt nach Lemma 27.4 für die Kreisteilungskörper

$$K_{r_n} \subseteq K.$$

Für der Grad d gilt dann unter Verwendung von Satz 17.10

$$d \geq \operatorname{grad}_{\mathbb{Q}} K_{r_n} = \varphi(r_n).$$

Wenn in den Primfaktorzerlegungen der Folgenglieder r_n unendlich viele Primzahlen p_m vorkommen, so ist

$$d \geq p_m - 1.$$

Wenn hingegen in den Primfaktorzerlegungen nur endlich viele Primzahlen vorkommen, so gibt es darin eine Teilfolge mit Primzahlpotenzen p^{s_k} als Teiler mit $s_k \to \infty$. In diesem Fall ist $d \geq (p-1)p^{s_k-1}$. In beiden Fällen ergibt sich ein Widerspruch zur Endlichkeit von d. Die Endlichkeit der Gruppe folgt daher mit Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)). Die Zyklizität folgt aus Satz 9.5 (Körper- und Galoistheorie (Osnabrück 2018-2019)). □

Lemma 27.7. *Es sei R der imaginär-quadratische Zahlbereich mit Diskriminante $\triangle$. Dann stimmt die Einheitengruppe $R^\times$ mit der Einheitswurzelgruppe $\mu(R)$ überein. Für diese gibt es die folgenden drei Möglichkeiten.*

(1) *Bei $\triangle = -3$ ist $\mu(R) \cong \mathbb{Z}/(6)$.*
(2) *Bei $\triangle = -4$ ist $\mu(R) \cong \mathbb{Z}/(4)$.*
(3) *Bei $\triangle \leq -5$ ist $\mu(R) = \{1, -1\} \cong \mathbb{Z}/(2)$.*

Beweis. Wegen der expliziten Gestalt der Norm und Lemma 10.1 ist die Einheitengruppe endlich, stimmt also mit der Einheitswurzelgruppe überein. Es sei A der quadratische Zahlbereich zur quadratfreien Zahl $D \leq -1$. Bei $D = -1$ ist A der Ring der Gaußschen Zahlen und es gibt die vier Einheiten $1, -1, \mathrm{i}, -\mathrm{i}$, und es ist $\triangle = -4$ nach Lemma 9.9. Dies ist der einzige quadratische Zahlbereich mit Diskriminante -4. Bei $D = \triangle = -3$ liegt der Ring der Eisensteinzahlen vor, siehe Beispiel 7.4. Er ist zugleich der dritte und der sechste Kreisteilungsring und seine Einheitswurzelgruppe ist nach Lemma 27.5 gleich $\mathbb{Z}/(6)$. Sei also die Diskriminante ≤ -5. Die Norm von $a + b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ (mit $a, b \in \mathbb{Q}$) ist durch $a^2 + b^2 |D|$ gegeben. Wenn das Element zum Ganzheitsring gehört, so sind bei $D = 2, 3 \mod 4$ nach Satz 9.8 die Koeffizienten a, b ganzzahlig und aus $|D| \geq 2$ folgt $b = 0$ und aus Lemma 10.1 folgt $a = \pm 1$. Bei $D = 1 \mod 4$ sind ebenfalls nach Satz

9.8 die Koeffizienten a, b ganzzahlige Vielfache von $1/2$ und aus $|D| \geq 7$ folgt wieder $b = 0$ und $a = \pm 1$. □

Zu einer kommutativen Gruppe H bezeichnen wir die Menge der Automorphismen mit $\mathrm{Aut}(H)$. Dies ist selbst eine Gruppe mit der Hintereinanderschaltung als Verknüpfung. Für die kommutative Gruppe $\mathbb{Z}/(n)$ ist ein Gruppenhomomorphismus in sich durch das Bild des Erzeugers festgelegt, und ein Automorphismus liegt genau dann vor, wenn der Erzeuger auf einen Erzeuger abgebildet wird. Deshalb ist

$$\mathrm{Aut}\,(\mathbb{Z}/(n)) \cong (\mathbb{Z}/(n))^\times,$$

einer Einheit a rechts entspricht der Gruppenhomomorphismus $x \mapsto ax$. Für μ_n, die multiplikativ geschriebene zyklische Gruppe der Ordnung n, gilt entsprechend

$$\mathrm{Aut}\,(\mu_n) \cong (\mathbb{Z}/(n))^\times,$$

und der Einheit a entspricht das Potenzieren $x \mapsto x^a$. Die Beschreibung der Galoisgruppe für Kreisteilungskörper aus Satz 17.11 kann man somit als einen Gruppenisomorphismus

$$\mathrm{Gal}\,(K_n|\mathbb{Q}) \cong \mathrm{Aut}(\mu_n)$$

verstehen. Zwischen diesen beiden Gruppen besteht nun stets der folgende Zusammenhang.

Lemma 27.8. *Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung mit der Galoisgruppe G und es sei*

$$\mu(K) = \mu_n$$

die Einheitswurzelgruppe zu K. Dann operiert G in natürlicher Weise auf $\mu(K)$, d.h. es gibt einen Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Aut}(\mu(K)) = (\mathbb{Z}/(n))^\times,\ \sigma \longmapsto (\zeta \mapsto \sigma(\zeta)).$$

Wenn eine Galoiserweiterung vorliegt, so ist diese Abbildung surjektiv.

Beweis. Nach Voraussetzung enthält K die n-ten Einheitswurzeln und damit ist $K_n \subseteq K$ nach Lemma 27.4. Insbesondere ist $\mu(K) = \mu(K_n)$. Die Abbildung

$$\mathrm{Gal}\,(K_n|\mathbb{Q}) \longrightarrow \mathrm{Aut}(\mu(K)) \cong (\mathbb{Z}/(n))^\times$$

ist nach Satz 17.11 ein Isomorphismus. Wenn $\mathbb{Q} \subseteq K$ galoissch ist, so ist K nach Korollar 16.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)) auch galoissch über K_n und die $\mathbb{Q}$-Automorphismen lassen sich wegen Korollar 15.8 (Körper- und Galoistheorie (Osnabrück 2018-2019)) nach K fortsetzen. □

27. Arbeitsblatt

27.1. **Aufgaben.**

Aufgabe 27.1. Es sei R ein kommutativer Ring und $f \in R$ ein nilpotentes Element. Zeige, dass $1 + f$ eine Einheit ist.

Aufgabe 27.2. a) Es sei K ein Körper. Zeige, dass die Einheitengruppe von K nicht zyklisch unendlich ist.

b) Es sei R ein kommutativer Ring, dessen Charakteristik nicht zwei ist. Zeige, dass die Einheitengruppe von R nicht zyklisch unendlich ist.

c) Beschreibe einen kommutativen Ring, dessen Einheitengruppe zyklisch unendlich ist.

Aufgabe 27.3. Bestimme die zweiten Einheitswurzeln in $\mathbb{Z}/(105)$.

Zu einer kommutativen Gruppe G nennt man

$$\{g \in G \mid g \text{ hat endliche Ordnung}\}$$

die *Torsionsuntergruppe* von G.

Eine kommutative Gruppe G heißt *torsionsfrei*, wenn für jedes Element $x \in G$, $x \neq 0$, und $n \in \mathbb{N}_+$ gilt $nx \neq 0$.

Aufgabe 27.4. Zeige, dass die Torsionsuntergruppe einer kommutativen Gruppe G in der Tat eine Untergruppe ist.

Aufgabe 27.5. Es sei $T \subseteq G$ die Torsionsuntergruppe einer kommutativen Gruppe G. Zeige, dass die Restklassengruppe G/T torsionsfrei ist.

Aufgabe 27.6. Es sei R ein kommutativer Ring. Zeige, dass die Einheitswurzeln in R die Torsionsuntergruppe der Einheitengruppe ist.

Aufgabe 27.7.*

Zeige, dass es in der Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ zu jedem $n \in \mathbb{N}_+$ Elemente gibt, deren Ordnung gleich n ist.

Aufgabe 27.8. Zeige, dass die Restklassengruppe $\mathbb{Q}/\mathbb{Z}$ unendlich ist und jedes Element eine endliche Ordnung besitzt.

Aufgabe 27.9. Zeige, dass die Menge

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

mit der Multiplikation in $\mathbb{Q}[\mathrm{i}]$ eine kommutative Gruppe ist.

Aufgabe 27.10. Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[\mathrm{i}]^\times$ ererbten Gruppenstruktur. Berechne die ersten vier Potenzen von $\frac{3}{5} + \frac{4}{5}\mathrm{i} \in S^1_{\mathbb{Q}}$.

Aufgabe 27.11. Es sei

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}[\mathrm{i}] \mid |z| = 1\}$$

der rationale Einheitskreis mit der aus $\mathbb{Q}[\mathrm{i}]^\times$ ererbten Gruppenstruktur. Zeige, dass die Gruppen $S^1_{\mathbb{Q}}$ und $\mathbb{Q}/\mathbb{Z}$ nicht isomorph sind.

Aufgabe 27.12.*

Bestimme für den siebten Kreisteilungsring

$$R_7 = \mathbb{Z}[X]/\big(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1\big)$$

das Minimalpolynom für $Y = X + X^{-1} = X + X^6$. Ist Y eine Einheit?

Aufgabe 27.13. Bestimme für den neunten Kreisteilungsring

$$R_9 = \mathbb{Z}[X]/(\Phi_9)$$

das Minimalpolynom für $Y = X + X^{-1}$. Ist Y eine Einheit?

Aufgabe 27.14.*

Bestimme für den elften Kreisteilungsring $R_{11} = \mathbb{Z}[X]/(\Phi_{11})$ das Minimalpolynom für $Y = X + X^{-1} = X + X^{10}$. Ist Y eine Einheit?

Aufgabe 27.15. Bestimme für die Kreisteilungsringe $R_n = \mathbb{Z}[X]/(\Phi_n)$ mit $n = 1, 2, \ldots, 12$, ob das Element $X + X^{-1}$ eine Einheit ist oder nicht.

Aufgabe 27.16. Bestimme die Einheiten im Ring $\mathbb{Z}[\sqrt{-3}]$.

Aufgabe 27.17. Es sei $K \subseteq L$ eine endliche Körpererweiterung und sei $\mu_n(L)$ (zu $n \in \mathbb{N}_+$) die Gruppe der n-ten Einheitswurzeln in L. Zeige, dass es zu jedem n einen natürlichen Gruppenhomomorphismus

$$\operatorname{Gal}(L|K) \longrightarrow \operatorname{Aut}(\mu_n(L))$$

gibt.

Aufgabe 27.18. Es sei $\mathbb{Q} \subseteq K$ eine endliche Galoiserweiterung und sei H der Kern des Gruppenhomomorphismus

$$\operatorname{Gal}(K|\mathbb{Q}) \longrightarrow \operatorname{Aut}(\mu(K)),\ \sigma \longmapsto (\zeta \mapsto \sigma(\zeta)),$$

aus Lemma 27.8. Zeige $K^H = K_n$, wobei n die Anzahl der Einheitswurzeln in K bezeichnet.

Aufgabe 27.19. Man gebe ein Beispiel für eine endliche Galoiserweiterung $\mathbb{Q} \subseteq K$ derart, dass der Gruppenhomomorphismus

$$\operatorname{Gal}(K|\mathbb{Q}) \longrightarrow \operatorname{Aut}(\mu(K)),\ \sigma \longmapsto (\zeta \mapsto \sigma(\zeta)),$$

aus Lemma 27.8 nicht injektiv ist.

Aufgabe 27.20. Betrachte die endlichen Körpererweiterungen

$$\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{i}] \subseteq \mathbb{Q}[\mathrm{i}, \sqrt[3]{1+\mathrm{i}}] = K.$$

Zeige, dass der Gruppenhomomorphismus

$$\operatorname{Gal}(K|\mathbb{Q}) \longrightarrow \operatorname{Aut}(\mu(K)),\ \sigma \longmapsto (\zeta \mapsto \sigma(\zeta)),$$

aus Lemma 27.8 nicht surjektiv ist.

Aufgabe 27.21. Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung und R der zugehörige Zahlbereich. Zeige, dass es einen natürlichen Gruppenhomomorphismus

$$\operatorname{Gal}(K|\mathbb{Q}) \longrightarrow \operatorname{Aut}(R^\times)$$

gibt.

Aufgabe 27.22. Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung und R der zugehörige Zahlbereich. Zeige, dass es Gruppenhomomorphismen

$$\operatorname{Gal}(K|\mathbb{Q}) \longrightarrow \operatorname{Aut}(R^\times) \longrightarrow \operatorname{Aut}(\mu(K))$$

derart gibt, dass die Gesamtabbildung der Homomorphismus aus Lemma 27.8 ist.

Aufgabe 27.23. Es sei $\mathbb{Q} \subseteq K$ eine endliche Galoiserweiterung mit zugehörigem Zahlbereich R. Zeige, dass die folgenden Eigenschaften äquivalent sind.

(1) Die Einheiten bilden ein Algebraerzeugendensystem von R über $\mathbb{Z}$.
(2) Für jeden Zahlbereich $S \subset R$ ist die Einheitengruppe $S^\times$ eine echte Teilmenge von $R^\times$.
(3) Die Wirkung der Galoisgruppe auf $R^\times$ ist treu.

Aufgabe 27.24.*

Man gebe ein Beispiel von zwei Zahlbereichen R und S, die als Ringe nicht isomorph sind, aber die Eigenschaft haben, dass sowohl die additiven Strukturen $(R, +, 0)$ und $(S, +, 0)$ als Gruppen isomorph als auch die multiplikativen Strukturen $(R, \cdot, 1)$ und $(S, \cdot, 1)$ als Monoide isomorph sind.

28. Vorlesung - Der Dirichletsche Einheitensatz

28.1. **Der Dirichletsche Einheitensatz.**

Es sei R der Ganzheitsring zur endlichen Körpererweiterung $\mathbb{Q} \subseteq K$. In Satz 25.2 haben wir gesehen, dass das Bild der reellen Gesamteinbettung

$$\tau^{\mathbb{R}}(R) = \Gamma_R \subset \mathbb{R}^r \times \mathbb{C}^s$$

ein Gitter in $\mathbb{R}^r \times \mathbb{C}^s$ ist, wobei r die Anzahl der reellen Einbettungen und s die Anzahl der Paare von komplexen Einbettungen bezeichnet. Zu jedem von 0 verschiedenen Element $f \in R$ ist $\tau^{\mathbb{R}}(f)$ in jeder reellen Komponente und in jeder komplexen Komponente von 0 verschieden (Real- oder Imaginärteil kann aber 0 sein). Um die Einheitengruppe von R zu verstehen, betrachten wir die Abbildung

$$\left(\mathbb{R}^\times\right)^r \times \left(\mathbb{C}^\times\right)^s \longrightarrow \mathbb{R}^{r+s}, (x_1, \ldots, x_r; z_{r+1}, \ldots, z_{r+s}) \longmapsto$$
$$\left(\ln|x_1|, \ldots, \ln|x_r|; \ln\left(|z_{r+1}|^2\right), \ldots, \ln\left(|z_{r+s}|^2\right)\right).$$

$$\ln|z_j\overline{z_j}| = \ln\left(|z_j|^2\right) = 2\ln|z_j|$$

heranzieht. Insgesamt haben wir die Verknüpfung der folgenden Abbildungen

$$K^\times \xrightarrow{\tau^{\mathbb{R}}} \left(\mathbb{R}^\times\right)^r \times \left(\mathbb{C}^\times\right)^s \xrightarrow{|-|} \left(\mathbb{R}^\times\right)^r \times \left(\mathbb{R}^\times\right)^s \xrightarrow{\ln(-), 2\ln(-)} \mathbb{R}^r \times \mathbb{R}^s,$$

wobei die funktionalen Ausdrücke komponentenweise zu verstehen sind. Da die Einbettungen und der Betrag multiplikativ sind und der Logarithmus die Multiplikation in die Addition überführt, liegt insgesamt ein Gruppenhomomorphismus

$$(K^\times, 1, \cdot) \longrightarrow (\mathbb{R}^{r+s}, 0, +)$$

vor. Wir sprechen von der *logarithmischen Gesamtabbildung* und bezeichnen sie mit L. Diese ist insbesondere für die Einheitengruppe $R^\times \subseteq K^\times$ wichtig.

Lemma 28.1. *Es sei R der Ganzheitsring zu einer endlichen Körpererweiterung $\mathbb{Q} \subseteq K$ mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Dann besitzt die logarithmische Gesamtabbildung*

$$L\colon\ K^\times \longrightarrow \mathbb{R}^{r+s}$$

die folgenden Eigenschaften.

(1) *Der Kern von L eingeschränkt auf $R^\times$ ist die Gruppe der Einheitswurzeln $\mu(R)$ und insbesondere eine endliche zyklische Gruppe.*
(2) *Das Bild $L(R^\times)$ liegt in der Hyperebene*

$$H \ = \ \left\{ (v_1, \ldots, v_{r+s}) \mid \sum_{j=1}^{r+s} v_j = 0 \right\} \ \subset \ \mathbb{R}^{r+s}.$$

(3) *Das Bild $L(R^\times)$ ist eine diskrete Untergruppe von $H \subset \mathbb{R}^{r+s}$.*

Beweis. (1) Für L liegt die Faktorisierung

$$R^\times \xrightarrow{\tau^{\mathbb{R}}} \Gamma \setminus \{0\} \xrightarrow{\ell} \mathbb{R}^{r+s}$$

vor. Ein Element $f \in K^\times$ wird genau dann unter L auf den Nullvektor abgebildet, wenn $\tau(f)$ in jeder reellen oder komplexen Komponente den Betrag 1 besitzt. Diese Elemente liegen somit alle in einer beschränkten Teilmenge von $\mathbb{R}^r \times \mathbb{C}^s$ aber ja auch im Gitter Γ. Daher ist diese Menge endlich und daher ist wegen der Injektivität von τ auch die zugrunde liegende Menge in R endlich. Also haben diese Elemente endliche Ordnung und sind Einheitswurzeln. Umgekehrt ist ein Torsionselement der Einheitengruppe von R in jeder Einbettung ein Torsionselement und hat daher den Betrag 1, wird also unter L auf 0 abgebildet.

(2) Sei $f \in R^\times$ eine Einheit und sei

$$(\rho_1(f), \ldots, \rho_r(f); \sigma_{r+1}(f), \overline{\sigma_{r+1}}(f), \ldots, \sigma_{r+s}(f), \overline{\sigma_{r+s}}(f)$$

das totale komplexe Einbettungstupel. Nach Lemma 7.14 ist die Norm von f gleich

$$\begin{aligned} & \rho_1(f) \cdots \rho_r(f) \sigma_{r+1}(f) \cdot \overline{\sigma_{r+1}}(f) \cdots \sigma_{r+s}(f) \cdot \overline{\sigma_{r+s}}(f) \\ = \ & \rho_1(f) \cdots \rho_r(f) \left|\sigma_{r+1}(f)\right|^2 \cdots \left|\sigma_{r+s}(f)\right|^2. \end{aligned}$$

Nach Lemma 10.1 ist der Betrag davon gleich 1. Unter der komponentenweise genommenen Abbildung

$$\ln(|-|)\colon\ \left(\mathbb{R}^\times\right)^r \times \left(\mathbb{C}^\times\right)^{2s} \longrightarrow \mathbb{R}^r \times \mathbb{R}^{2s}$$

wird dieses Produkt auf die Summe abgebildet, somit gilt

$$\sum_{j=1}^{r} \ln|\rho_j(f)| + \sum_{i=1}^{s} \ln|\sigma_{r+i}(f)| + \sum_{i=1}^{s} \ln|\overline{\sigma_{r+i}}(f)|$$

$$\begin{aligned} &= \sum_{j=1}^{r} \ln|\rho_j(f)| + 2\sum_{i=1}^{s} \ln|\sigma_{r+i}(f)| \\ &= 0. \end{aligned}$$

Die letzte Gleichung bedeutet gerade, dass $L(f)$ auf der Hyperebene H liegt.

(3) Es ist zu zeigen, dass das Bild $L(R^\times)$ mit jeder beschränkten Teilmenge von H einen endlichen Durchschnitt besitzt. Das Urbild einer beschränkten Teilmenge unter ℓ ist aber auch beschränkt, und der Durchschnitt mit dem Gitter Γ ist endlich.

□

Die Hyperebene im vorstehenden Lemma hat die reelle Dimension $r+s-1$, und darin ist das Bild eine diskrete Untergruppe. Es wird sich herausstellen, dass das Bild in dieser Hyperebene sogar ein Gitter ist, also von $r+s-1$ linear unabhängigen Vektoren erzeugt wird. Wir erläutern die Situation anhand von Beispielen kleinen Grades.

Beispiel 28.2. Zu quadratfreiem $D < 0$ und zugehörigem imaginär-qua/-dratischen Zahlbereich $A_D \subseteq \mathbb{C}$ (vergleiche Beispiel 25.3) ist die logarithmische Gesamtabbildung durch

$$A_D \setminus \{0\} \longrightarrow \mathbb{R},\ (a+bi\sqrt{|D|}) \longmapsto \ln\left(a^2+b^2|D|\right),$$

gegeben. Der minimale Wert von $a^2+b^2|D|$ ist 1 und das Bild der logarithmischen Abbildung liegt in $\mathbb{R}_{\geq 0}$. Hieran sieht man erneut, dass es in A_D nur Einheitswurzeln als Einheiten gibt, vergleiche Lemma 27.7.

Beispiel 28.3. Zu quadratfreiem $D \geq 2$ und zugehörigem reell-quadratischen Zahlbereich A_D mit der Gitterrealisierung

$$A_D \longrightarrow \mathbb{R}^2,\ (a+b\sqrt{D}) \longmapsto \begin{pmatrix} a+b\sqrt{D} \\ a-b\sqrt{D} \end{pmatrix},$$

(vergleiche Beispiel 25.4) ist die logarithmische Gesamtabbildung durch

$$A_D \setminus \{0\} \longrightarrow \mathbb{R}\times\mathbb{R},\ (a+b\sqrt{D}) \longmapsto \begin{pmatrix} \ln\left|a+b\sqrt{D}\right| \\ \ln\left|a-b\sqrt{D}\right| \end{pmatrix},$$

gegeben. Diese induziert für die Einheiten den Gruppenhomomorphismus

$$A_D^\times \longrightarrow \mathbb{R}\times\mathbb{R},\ (a+b\sqrt{D}) \longmapsto \begin{pmatrix} \ln\left|a+b\sqrt{D}\right| \\ \ln\left|a-b\sqrt{D}\right| \end{pmatrix},$$

wobei das Bild (wegen Lemma 28.1 (2) oder direkt) auf der Gegendiagonalen landet. Somit liegt ein Gruppenhomomorphismus $\left(A_D^\times, \cdot, 1\right) \to (\mathbb{R}, +, 0)$ vor. Der Kern besteht aus $\{1,-1\}$ und das Bild ist eine diskrete Untergruppe von $\mathbb{R}$. Wir werden gleich sehen, dass das Bild die Form $\mathbb{Z}v$ mit $v \neq 0$ besitzt.

Beispiel 28.4. Wir knüpfen an Beispiel 25.5 an, also

$$R = \mathbb{Z}[X]/\big(X^3 - 3X + 1\big).$$

Unter der logarithmischen Gesamtabbildung wird das Ringelement $a + b\alpha + c\alpha^2$ auf

$$\begin{pmatrix} \ln|a + b\alpha + c\alpha^2| \\ \ln|a + b(\alpha^2 - 2) + c(-\alpha^2 - \alpha + 4)| \\ \ln|a + b(-\alpha^2 - \alpha + 2) + c(\alpha + 2)| \end{pmatrix}$$

bzw. $a + b\alpha + d\beta$ auf

$$\begin{pmatrix} \ln|a + b\alpha + d\beta| \\ \ln|a + b\beta + d(-\alpha - \beta)| \\ \ln|a + b(-\alpha - \beta) + d\alpha| \end{pmatrix}$$

abgebildet. Die Einheiten α bzw. β werden auf

$$\begin{pmatrix} \ln|\alpha| \\ \ln|\beta| \\ \ln|-\alpha - \beta| \end{pmatrix}$$

bzw.

$$\begin{pmatrix} \ln|\beta| \\ \ln|-\alpha - \beta| \\ \ln|\alpha| \end{pmatrix}$$

und diese Vektoren liegen auf der durch $x + y + z = 0$ definierten Ebene. Die lineare Unabhängigkeit dieser beiden Vektoren kann man über die Determinante zeigen.

Die numerischen Werte der Nullstellen des Polynoms sind ungefähr

$$\alpha \sim 1,532,\ \beta \sim 0,347,\ \gamma \sim -1,879\,.$$

Die Determinante der oberen 2×2-Untermatrix ist ungefähr

$$\begin{aligned} \ln|\alpha| \ln|\alpha + \beta| - \ln\left(|\beta|\right)^2 &\sim 0,426 \cdot 0,631 - (-1.058)^2 \\ &\sim 0,89 \\ &\neq 0. \end{aligned}$$

Die Bilder der beiden Einheiten α und β sind also linear unabhängig und daher besteht zwischen den Einheiten selbst in R keine Beziehung der Form

$$\alpha^m = \beta^n$$

für $(m, n) \neq (0, 0)$.

Bemerkung 28.5. Zu einem Körperautomorphismus φ der Ordnung $k \neq 1, 2$ auf einer endlichen Körpererweiterung $\mathbb{Q} \subseteq K$ mit einer reellen Einbettung $K \subseteq \mathbb{R}$ und einem Element $\alpha \in K$ mit

$$\varphi(\alpha) \neq \pm\alpha$$

sind α und $\varphi(\alpha)$ exponentiell unabhängig, d.h. es besteht keine Relation der Form

$$\alpha^m = \varphi(\alpha)^n$$

mit $(m,n) \neq (0,0)$. Aus

$$\varphi(\alpha) = \alpha^q$$

mit einem positiven rationalen Exponenten $q = \frac{m}{n}$ folgt ja

$$\alpha = \varphi^k(\alpha) = \alpha^{q^k},$$

woraus sich wegen der reellen Einbettung $q^k = 1$ ergibt, was ausgeschlossen ist. Daher sind auch die Logarithmen der Beträge von α und $\varphi(\alpha)$ linear unabhängig über $\mathbb{Q}$. Wenn die Einheitengruppe den Rang 1 besitzt, so muss bei rein reellen Erweiterungen zwischen den Einheiten α und $\varphi(\alpha)$ bis auf das Vorzeichen eine exponentielle Relation bestehen. Im reell-quadratischen Fall sind in der Tat für eine Einheit $a + b\sqrt{D}$ wegen

$$(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D = \pm 1$$

die beiden zueinander konjugierten Elemente auch bis eventuell auf das Vorzeichen zueinander invers.

Lemma 28.6. *Es sei R ein Zahlbereich mit der zugehörigen reellen Gesamteinbettung*

$$\tau^{\mathbb{R}} \colon R \longrightarrow \mathbb{R}^r \times \mathbb{C}^s$$

und der Teilmenge

$$\begin{aligned} U &= \{(x_1, \ldots, x_r; z_{r+1}, \ldots, z_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s \mid |x_1| \\ &\quad \cdots |x_r| \cdot |z_{r+1}|^2 \cdots |z_{r+s}|^2 = 1\}. \end{aligned}$$

Dann gibt es eine beschränkte Teilmenge $T \subseteq U$ mit

$$U = \bigcup_{u \in R^\times} T \cdot \tau^{\mathbb{R}}(u).$$

Beweis. Es sei $d = r + 2s$ der Grad der Körpererweiterung. Nach Lemma 7.14 gehört $\tau^{\mathbb{R}}(u)$ zu einer Einheit $u \in R^\times$ zu U. Ferner ist U mit komponentenweiser Multiplikation abgeschlossen in $\mathbb{R}^d$. Es seien $c_1, \ldots, c_d$ positive reelle Zahlen mit $c_j = c_{j+1}$ für die komplex-konjugierten Stellen und mit

$$c := c_1 \cdots c_d > \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle_K|}.$$

Wir betrachten die durch c definierte beschränkte Teilmenge

$$A := \{(x_1, \ldots, x_d) \in \mathbb{R}^d \mid |x_j| < c_j \text{ alle } j\}.$$

Zu einem Element $y = (y_1, \ldots, y_d) \in \mathbb{R}^d$ ohne Nulleintrag ist die mit y multiplizierte Menge gleich

$$\begin{aligned} yA &= \{(y_1 x_1, \ldots, y_d x_d) \in \mathbb{R}^d \mid |x_j| < c_j \text{ alle } j\} \\ &= \{(z_1, \ldots, z_d) \in \mathbb{R}^d \mid |z_j| < |y_j|\, c_j \text{ alle } j\}. \end{aligned}$$

Nach Lemma 10.9 gibt es in R für jede vorgegebene Norm bis auf Assoziiertheit nur endlich viele Elemente mit dieser Norm. Da als Norm nur ganze Zahlen auftreten, gilt dies auch für die Elemente unterhalb einer fixierten

Norm. Deshalb gibt es von 0 verschiedene Elemente $f_1, \ldots, f_n \in R$ derart, dass jedes Element $g \in R$ mit $N(g) \leq c$ zu einem der f_i assoziiert ist.

Wir betrachten nun

$$T := U \cap \left(\bigcup_{i=1}^{n} \tau^{\mathbb{R}}(f_i^{-1})A \right)$$

und behaupten

$$U = \bigcup_{u \in R^\times} T \cdot \tau^{\mathbb{R}}(u),$$

wobei die Inklusion $\supseteq$ klar ist. Zum Beweis der anderen Inklusion sei $y \in U$. Wir betrachten $y^{-1}A$. Wegen $|y_1| \cdots |y_d| = 1$ gilt, dass das Produkt der Grenzen in $y^{-1}A$ wieder gleich c ist und damit die eingangs fixierte Bedingung erfüllt. Nach Korollar 26.3 gibt es ein von 0 verschiedenes $f \in R$ mit $\tau^{\mathbb{R}}(f) \in y^{-1}A$, sagen wir

$$\tau^{\mathbb{R}}(f) = y^{-1}x$$

mit $x \in A$. Da die $\tau^{\mathbb{R}}(f)$ komponentenweise durch die c_j beschränkt sind, ist der Betrag der Norm von f durch c beschränkt. Daher gibt es ein f_i aus unserer endlichen Auswahlmenge und eine Einheit u mit $f = uf_i$. Somit ist

$$y = x\tau^{\mathbb{R}}(f^{-1}) = \tau^{\mathbb{R}}(f_i^{-1})x\tau^{\mathbb{R}}(u^{-1})$$

und

$$x\tau^{\mathbb{R}}(u^{-1}) \in A.$$

□

Peter Gustav Lejeune Dirichlet (1805-1859)

Der folgende Satz heißt *Dirichletscher Einheitensatz.*

Satz 28.7. *Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Dann ist*

$$R^\times = \mathbb{Z}^{r+s-1} \times \mu$$

mit einer endlichen zyklischen Gruppe μ.

Beweis. Die logarithmische Gesamtabbildung

$$L\colon\ R^\times \longrightarrow \mathbb{R}^{r+s}$$

hat nach Lemma 28.1 den Kern

$$\mu\ =\ \mu(R)$$

und das Bild $L(R^\times)$ ist eine diskrete Untergruppe von

$$H\ =\ \left\{(v_1,\ldots,v_{r+s})\mid \sum_{j=1}^{r+s} v_j = 0\right\}\ \subset\ \mathbb{R}^{r+s}.$$

Unter der Faktorisierung

$$R^\times \xrightarrow{\tau^{\mathbb{R}}} \left(\mathbb{R}^\times\right)^r \times \left(\mathbb{C}^\times\right)^s \xrightarrow{\ell} \mathbb{R}^r\times\mathbb{R}^s$$

mit $\ell\ =\ (\ln|-|\,,2\ln|-|)$ ist die Menge

$$\begin{aligned} U\ \ =\ \ & \{(x_1,\ldots,x_r;z_{r+1},\ldots,z_{r+s})\in\mathbb{R}^r\times\mathbb{C}^s\mid |x_1| \\ & \cdots|x_r|\cdot|z_{r+1}|^2\cdots|z_{r+s}|^2=1\}\end{aligned}$$

aus Lemma 28.6 das Urbild von H. Die Überdeckung

$$U\ =\ \bigcup_{u\in R^\times} T\cdot\tau^{\mathbb{R}}(u)$$

mit einer beschränkten Teilmenge $T\ \subseteq\ U$, die es nach Lemma 28.6 gibt, übersetzt sich zu

$$H\ =\ \bigcup_{u\in R^\times} \ell(T)+L(u).$$

Da $\ell(T)$ ebenfalls beschränkt ist, folgt aus Aufgabe 28.4, dass die Bildgruppe $L(R^\times)$ ein Gitter in H ist.

Es liegt also eine kurze exakte Sequenz

$$0\ \longrightarrow\ \mu(R)\ \longrightarrow\ R^\times\ \longrightarrow\ L(R^\times)\cong\mathbb{Z}^{r+s-1}\ \longrightarrow\ 0$$

vor. Indem man für die Standardvektoren rechts Urbilder in $R^\times$ wählt, erhält man auch eine Darstellung

$$R^\times\ \cong\ \mu(R)\times\mathbb{Z}^{r+s-1}.$$

□

Definition 28.8. Eine Familie von Einheiten $u_1,\ldots,u_m\ \in\ R$ in einem Zahlbereich R heißt ein System von *Fundamentaleinheiten*, wenn man jede Einheit u von R in eindeutiger Weise als

$$u\ =\ \zeta u_1^{n_1}\cdots u_m^{n_m}$$

mit einer Einheitswurzel ζ und ganzzahligen Exponenten n_j schreiben kann.

Bemerkung 28.9. Satz 28.7 besagt insbesondere, dass es Systeme von Fundamentaleinheiten gibt, und dass stets

$$m = r + s - 1$$

ist, wenn wieder r die Anzahl der reellen und s die Anzahl der Paare von komplexen Einbettungen bezeichnet. Bei einer Zerlegung

$$R^\times = \mu(R) \times \mathbb{Z}^m$$

kann man eine Basis von $\mathbb{Z}^m$ und insbesondere die Standardbasis als System von Fundamentaleinheiten nehmen. Man beachte, dass weder die Zerlegung noch die dazu äquivalente Auswahl von Fundamentaleinheiten in irgendeiner Form kanonisch ist. Es liegt eine natürliche Untergruppenbeziehung

$$\mu(R) \subseteq R^\times$$

vor und damit gibt es auch einen natürlichen Restklassenhomomorphismus

$$R^\times \longrightarrow R^\times/\mu(R),$$

und der Satz besagt eben, dass diese Restklassengruppe eine freie kommutative Gruppe vom Rang $r + s - 1$ ist, also isomorph zu $\mathbb{Z}^{r+s-1}$, es gibt aber keine natürliche Identifizierung dieser Restklassengruppe mit $\mathbb{Z}^{r+s-1}$. Aus einer surjektiven Gesamtabbildung

$$R^\times \longrightarrow R^\times/\mu(R) \xrightarrow{\cong} \mathbb{Z}^{r+s-1}$$

erhält man eine freie Untergruppe von $R^\times$, indem man jedem Element der Standardbasis rechts ein Urbild aus $R^\times$ zuordnet und von dieser Abbildung das Bild nimmt. Dies führt dann zu einer Zerlegung

$$R^\times \cong \mu(R) \times \mathbb{Z}^m.$$

Korollar 28.10. *Es sei D eine quadratfreie Zahl und $R = A_D$ der zugehörige quadratische Zahlbereich.*

(1) *Wenn D positiv ist, so ist die Einheitengruppe isomorph zu $\{1, -1\} \times \mathbb{Z}$.*
(2) *Wenn D negativ ist, so ist die Einheitengruppe endlich.*

Beweis. Dies folgt unmittelbar aus Satz 28.7 in Verbindung mit Lemma 27.3. □

28. Arbeitsblatt

28.1. **Aufgaben.**

Aufgabe 28.1. Zeige, dass zu einer endlichen Körpererweiterung $\mathbb{Q} \subseteq K$ die Menge

$$\left\{x \in K^\times \mid |\tau(x)| = 1 \text{ für alle Einbettungen } \tau\right\}$$

eine Untergruppe der Einheitengruppe von K ist, die die Einheitswurzelgruppe $\mu(K)$ umfasst, und dass die Einheitswurzelgruppe im Allgemeinen kleiner ist.

Aufgabe 28.2. Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung mit ausschließlich reellen Einbettungen. Es sei $K \subseteq L$ eine quadratische Körpererweiterung und L besitze keine reelle Einbettung. Zeige, dass ein kommutatives Diagramm

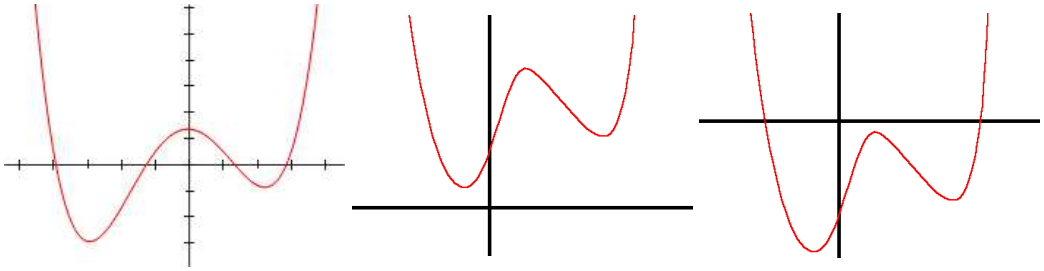
$$\begin{array}{ccccc} K^\times & \xrightarrow{\tau^{\mathbb{R}}} & (\mathbb{R}^\times)^r & \xrightarrow{\ln|-|} & \mathbb{R}^r \\ \downarrow & & \downarrow & & \downarrow \cdot 2 \\ L^\times & \xrightarrow{\tau^{\mathbb{R}}} & (\mathbb{C}^\times)^r & \xrightarrow{2\ln|-|} & \mathbb{R}^r \end{array}$$

existiert, wobei die Abbildungen rechts komponentenweise zu verstehen sind und wobei die horizontalen Abbildungen die logarithmischen Gesamtabbildungen sind.

Aufgabe 28.3. Skizziere die Situation in Lemma 28.6 für verschiedene Zahlbereiche von kleinem Grad.

Aufgabe 28.4. Es sei V ein euklidischer Vektorraum, $\Delta \subseteq V$ eine diskrete Untergruppe und $B \subseteq V$ eine beschränkte Teilmenge derart, dass $\bigcup_{v\in\Delta} v + B = V$ ist. Zeige, dass Δ ein Gitter ist.

Aufgabe 28.5. Im Folgenden sind die Graphen zu normierten irreduziblen Polynomen F vom Grad 4 mit ganzzahligen Koeffizienten abgebildet. Es sei R der Zahlbereich zur Körpererweiterung $\mathbb{Q} \subseteq K = \mathbb{Q}[X]/(F)$. Bestimme den Rang der Einheitengruppe $R^\times$.



a) b) c)

Aufgabe 28.6.*

Es sei R ein Zahlbereich und es seien $u, v \in R^\times$ Einheiten und a, b von 0 verschiedene ganze Zahlen mit $u^a = v^b$. Zeige, dass es ganze Zahlen c, d und Einheitswurzeln $\zeta, \xi \in \mu(R)$ und eine Einheit w derart gibt, dass $u = \zeta w^c$ und $v = \xi w^d$ gilt.

Aufgabe 28.7. Es sei R ein Zahlbereich und $u \in R^\times$ eine Einheit, die keine Einheitswurzel sei. Zeige, dass man aus u nur zu endlich vielen Exponenten Wurzeln ziehen kann.

Aufgabe 28.8. Es sei R ein Zahlbereich und sei $u \in R^\times$ Teil eines Systems von Fundamentaleinheiten. Zeige, dass u keinerlei Wurzel besitzt.

Aufgabe 28.9.*

Es sei R ein Zahlbereich und sei $u \in R^\times$ derart, dass ζu, wobei ζ eine Einheitswurzel in R bezeichnet, in R keinerlei Wurzel besitze. Zeige, dass dann u Teil eines Systems von Fundamentaleinheiten ist.

Aufgabe 28.10. Es sei R ein Zahlbereich mit $r \geq 1$ reellen Einbettungen und s Paaren von komplexen Einbettungen. Es gelte $r + s \geq 3$ und es sei $R \subseteq \mathbb{R}$ eine fixierte reelle Einbettung. Zeige, dass es zu jedem $\delta > 0$ Einheiten $u \in R$ mit $1 < u \leq 1 + \delta$ gibt.

Aufgabe 28.11. Es sei $S = \mathbb{Z}[Y]/(Y^2 - 6Y + 1)$ und p eine ungerade Primzahl derart, dass $Y^2 - 6Y + 1$ in $\mathbb{Z}/(p)[X]$ irreduzibel ist. Zeige, dass Y kein Erzeuger der multiplikativen Gruppe von $\mathbb{Z}/(p)[Y]/(Y^2 - 6Y + 1)$ ist.

Aufgabe 28.12.*

Es sei $R = \mathbb{Z}[X]/(F)$ ein Zahlbereich mit einem normierten ganzzahligen irreduziblen Polynom F. Sei $n \in \mathbb{N}_+$ fixiert. Es sei p eine Primzahl mit den folgenden Eigenschaften.

(1) n und $p-1$ sind nicht teilerfremd.
(2) F ist irreduzibel in $\mathbb{Z}/(p)[X]$.
(3) Die Restklasse von X in $L = \mathbb{Z}/(p)[X]/(F)$ ist ein Erzeuger der multiplikativen Gruppe $L^\times$

Zeige, dass dann X in R keine n-te Wurzel besitzt.

Aufgabe 28.13. Es sei $R = \mathbb{Z}[X]/(F)$ ein Zahlbereich mit einem normierten ganzzahligen irreduziblen Polynom F. Sei $n \in \mathbb{N}_+$ fixiert. Es sei p eine Primzahl derart, dass $p-1$ nicht teilerfremd zu n sei. Es sei L ein Restekörper des Faserringes R/pR mit der Eigenschaft, dass die Restklasse von X in L ein Erzeuger der multiplikativen Gruppe $L^\times$ sei. Zeige, dass dann X in R keine n-te Wurzel besitzt.

Aufgabe 28.14.*

Es sei $R = \mathbb{Z}[X]/(X^3 - 3X + 1)$. Zeige mit Aufgabe 28.13, dass die Restklasse x von X in R keine dritte Wurzel besitzt.

Aufgabe 28.15.*

Wir betrachten das Polynom $F = X^3 - 3X + 1$ über $\mathbb{Z}/(7)$.

(1) Zeige, dass F ein irreduzibles Polynom in $\mathbb{Z}/(7)[X]$ ist.
(2) Es sei x die Restklasse von X in $\mathbb{Z}/(7)[X]/(X^3 - 3X + 1)$. Berechne x^7 und x^{49}.
(3) Zeige, dass x in $\mathbb{Z}/(7)[X]/(X^3 - 3X + 1)$ eine dritte Wurzel besitzt.

Aufgabe 28.16. Es seien G und H kommutative Gruppen und sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus.

(1) Zeige, dass dies einen Homomorphismus

$$\operatorname{tor}(G) \longrightarrow \operatorname{tor}(H)$$

zwischen den Torsionsuntergruppen und einen Homomorphismus

$$G/\operatorname{tor}(G) \longrightarrow H/\operatorname{tor}(H)$$

derart induziert, dass sich ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{tor}(G) & \longrightarrow & G & \longrightarrow & G/\operatorname{tor}(G) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \operatorname{tor}(H) & \longrightarrow & H & \longrightarrow & H/\operatorname{tor}(H) & \longrightarrow & 0 \end{array}$$

mit exakten Zeilen ergibt.

(2) Sei φ injektiv. Zeige, dass dann auch die induzierten Homomorphismen aus (1) injektiv sein müssen.

(3) Sei φ surjektiv. Müssen die induzierten Homomorphismen aus (1) surjektiv sein?

Aufgabe 28.17. Es seien R und S Zahlbereiche und sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Zeige, dass ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu(R) & \longrightarrow & R^\times & \longrightarrow & R^\times/\mu(R) & \longrightarrow & 1 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mu(S) & \longrightarrow & S^\times & \longrightarrow & S^\times/\mu(S) & \longrightarrow & 1 \end{array}$$

von Gruppenhomomorphismen mit exakten Zeilen existiert, und dass die vertikalen Homomorphismen injektiv sind.

Aufgabe 28.18.*

Es seien R und S Zahlbereiche und sei $\varphi\colon R \to S$ ein Ringhomomorphismus vom Grad d. Es sei $u \in R^\times$ eine Einheit, die in $R^\times/\mu(R)$ keinerlei Wurzel besitze (dazu ist äquivalent, dass u Teil eines Systems von Fundamentaleinheiten ist). Es sei $v \in S$ mit

$$u = v^n.$$

Zeige, dass n ein Teiler von d ist.

Aufgabe 28.19. Es sei R_n der n-te Kreisteilungsring und $S_n = R_n \cap \mathbb{R}$, vergleiche Aufgabe 17.5. Zeige, dass die Restklassengruppe $R_n^\times/S_n^\times$ endlich sind.

Aufgabe 28.20.*

Es sei p eine Primzahl, R_p der p-te Kreisteilungsring und $S_p = R_p \cap \mathbb{R}$, vergleiche Aufgabe 17.5. Zeige, dass für die Einheitengruppen die Beziehung

$$R_p^\times = \mu(R_p) \cdot S_p^\times$$

gilt. D.h. die Einheitengruppe wird von den Einheitswurzeln und den reellen Einheiten erzeugt.

Aufgabe 28.21. Es sei R ein Zahlbereich und sei $u \in R^\times$ Teil eines Systems von Fundamentaleinheiten von R. Zeige, dass es eine Erweiterung von Zahlbereichen $R \subseteq S$ derart gibt, dass u in S nicht zu einem System von Fundamentaleinheiten gehört.

Aufgabe 28.22.*

Man gebe Beispiele für eine endliche Galoiserweiterung $\mathbb{Q} \subseteq K$ mit zugehörigem Zahlbereich R derart, dass der natürliche Gruppenhomomorphismus

$$\operatorname{Gal}(K|\mathbb{Q}) \longrightarrow \operatorname{Aut}(R^\times)$$

(1) bijektiv,
(2) injektiv und nicht surjektiv,
(3) surjektiv und nicht injektiv,
(4) weder injektiv noch surjektiv

ist.

Aufgabe 28.23. Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung mit Galoisgruppe G und sei R der zugehörige Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Zeige, dass die Galoisgruppe in natürlicher Weise auf der Gruppe $\mathbb{Z}^{r+s-1}$ durch lineare Automorphismen wirkt.

Aufgabe 28.24. Es sei R ein reell-quadratischer Zahlbereich. Zeige, dass die Konjugation auf

$$R^\times/\{\pm 1\} \cong \mathbb{Z}$$

als Negation wirkt.

Aufgabe 28.25. Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung mit Galoisgruppe G und sei R der zugehörige Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Zeige, dass die Galoisgruppe in natürlicher Weise auf der Gruppe $\mathbb{Z}^{r+s-1}$ durch lineare Automorphismen wirkt.

Aufgabe 28.26.*

Wir betrachten den Zahlbereich $R = \mathbb{Z}[X]/(X^3 - 3X + 1)$. Es ist (vergleiche Beispiel 25.5)

$$\operatorname{Gal}(R|\mathbb{Z}) \cong \mathbb{Z}/(3) = \langle \varphi \rangle$$

und

$$R^\times/\{\pm 1\} \cong \mathbb{Z}^2$$

Bestimme die Matrix, die die Wirkung von φ auf $\mathbb{Z}^2$ beschreibt.

Aufgabe 28.27. Es sei R ein kommutativer Ring und A eine kommutative R-Algebra. Zeige, dass durch

$$A^\times \longrightarrow \Omega_{A|R},\ f \longmapsto \frac{df}{f},$$

ein Gruppenhomomorphismus von der Einheitengruppe in den Modul der Kähler-Differentiale definiert wird.

Die vorstehende Abbildung heißt *logarithmische Ableitung*.

Aufgabe 28.28.*

Beschreibe die logarithmische Ableitung explizit für die imaginär-quadratischen Zahlbereiche.

Aufgabe 28.29.*

Es sei p eine Primzahl und R_p der p-te Kreisteilungsring. Zeige, dass durch die logarithmische Ableitung ein Gruppenhomomorphismus

$$\mu(R_p) \longrightarrow \Omega_{R_p|\mathbb{Z}}$$

gegeben ist, dessen Kern gleich $\{\pm 1\}$ ist.

Aufgabe 28.30.*

Es sei R ein Zahlbereich mit r reellen und s Paaren von komplexen Einbettungen. Es sei $f \in R$, $f \neq 0$, ein Element mit der Primidealzerlegung

$$(f) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}.$$

Zeige, dass die Einheitengruppe $R_f^\times$ der Nenneraufnahme R_f isomorph zu $\mu(R) \times \mathbb{Z}^{r+s+k-1}$ ist.

29. Vorlesung - Fundamentaleinheiten

Wir besprechen in verschiedenen Beispielen genauer, wie die Einheitengruppe eines Zahlbereiches aussieht und wie Fundamentaleinheiten zu finden sind. Nach dem Dirichletschen Einheitensatz, den wir in der letzten Vorlesung bewiesen haben, ist der Rang der Einheitengruppe eines Zahlbereichs R mit r reellen Einbettungen und s Paaren von komplexen Einbettungen gleich $r+s-1$.

Der Rang der Einheitengruppe $r+s-1$ ist in zwei Fällen gleich 0, nämlich bei $R = \mathbb{Z}$ und wenn R ein imaginär-quadratischer Zahlbereich ist. In diesem Fall wurden die möglichen Einheitengruppen (= Einheitswurzelgruppen) in Lemma 27.7 besprochen. Für den Rang $r+s-1 = 1$, also $r+s = 2$, gibt es die folgenden Möglichkeiten:

(1) $r = 2$ und $s = 0$. Dann ist der Grad der Körpererweiterung gleich 2 und es handelt sich um eine reell-quadratische Körpererweiterung.
(2) $r = 1$ und $s = 1$. Dann ist der Grad der Körpererweiterung gleich 3. Das Minimalpolynom der Körpererweiterung ist ein kubisches Polynom mit genau einer reellen Nullstelle, beispielsweise $\mathbb{Q} \subset K \cong \mathbb{Q}[X]/(X^3 - 2)$.
(3) $r = 0$ und $s = 2$. Dann ist der Grad der Körpererweiterung gleich 4. Das Minimalpolynom der Körpererweiterung ist ein Polynom vom Grad 4 ohne reelle Nullstelle. Ein Beispiel ist $\mathbb{Q} \subset K \cong \mathbb{Q}[X]/(X^4 + X^3 + X^2 + X + 1)$, der fünfte Kreisteilungskörper.

29.1. **Fundamentaleinheiten im reell-quadratischen Fall.**

Lemma 29.1. *Es sei A_D ein reell-quadratischer Zahlbereich zu quadratfreiem $D \geq 2$ und sei $A_D \subseteq \mathbb{R}$ eine fixierte reelle Einbettung. Dann besitzt $A_D^\times \cap \mathbb{R}_{>1}$ ein Minimum und dieses ist eine Fundamentaleinheit.*

Beweis. Die Einheitengruppe von A_D ist nach Korollar 28.10 isomorph zu $\{1, -1\} \times \mathbb{Z}$, alle Einheiten sind von der Form $\pm u^n$ mit $n \in \mathbb{Z}$ und einer Fundamentaleinheit u. Diese Beschreibung gilt auch in der Einbettung nach $\mathbb{R}$. Mit u ist genauso $-u$ und u^{-1} eine Fundamentaleinheit. Damit können wir $u > 1$ annehmen. Zwischen 1 und u kann es keine weitere Einheit aus A_D geben, da sie ja die Form $\pm u^n$ besitzt, was bei negativem Vorzeichen negativ ist und bei (positivem Vorzeichen und) $n \leq 0$ zwischen 0 und 1 liegt. Für $n \geq 2$ ist $u^n > u$. □

Wir werden die Fundamentaleinheit > 1 (bezüglicher einer reellen Einbettung) häufig als die Fundamentaleinheit schlechthin bezeichnen. Man beachte, dass das Bild der Einbettung $A_D \subseteq \mathbb{R}$ eine dichte Teilmenge ist. Zwischen 1 und der gewählten Fundamentaleinheit u gibt es also unendlich viele Zahlen aus A_D, aber eben keine weiteren Einheiten.

Lemma 29.2. *Es sei A_D ein reell-quadratischer Zahlbereich zu quadratfreiem $D \geq 2$ und sei $A_D \subseteq \mathbb{R}$ eine fixierte reelle Einbettung. Dann sind für jede Einheit $a + b\sqrt{D} \in A_D^\times \cap \mathbb{R}_{>1}$ die Komponenten a und b positiv.*

Beweis. Mit $a + b\sqrt{D}$ sind auch $-a - b\sqrt{D}, a - b\sqrt{D}, -a + b\sqrt{D}$ Einheiten, wobei diese drei Elemente kleiner als 1 sind, da konjugierte Elmente im quadratischen Fall bis eventuell auf das Vorzeichen invers zueinander sind. Deshalb ist $a+b\sqrt{D} > a-b\sqrt{D}$, woraus $b > 0$ folgt, und $a+b\sqrt{D} > -a+b\sqrt{D}$, woraus $a > 0$ folgt. □

Lemma 29.3. *Es sei A_D ein reell-quadratischer Zahlbereich zu quadratfreiem $D \geq 2$ und sei $A_D \subseteq \mathbb{R}$ eine fixierte reelle Einbettung. Dann ist die Fundamentaleinheit $a + b\sqrt{D} \in A_D^\times \cap \mathbb{R}_{>1}$ dadurch charakterisiert, dass bei ihr unter allen Einheiten $a' + b'\sqrt{D} \in A_D^\times \cap \mathbb{R}_{>1}$ die erste Komponente minimal ist.*

Beweis. Nach Lemma 29.1 gibt es eine Fundamentaleinheit $a + b\sqrt{D}$, und diese ist unter den Einheiten oberhalb von 1 minimal. Sei $a' + b'\sqrt{D}$ eine weitere solche Einheit > 1. Dann ist diese von der Form

$$\begin{aligned} a' + b'\sqrt{D} &= \left(a + b\sqrt{D}\right)^n \\ &= a^n + \binom{n}{2} a^{n-2} b^2 D + \ldots \left(\binom{n}{1} a^{n-1} b^1 + \ldots \right) \sqrt{D} \end{aligned}$$

mit $n \geq 2$. Bei $a \geq 1$ folgt daraus sofort, dass $a' \geq a$, und bei $a < 1$ kommt wegen Lemma 29.2 nach Satz 9.8 nur $a = \frac{1}{2}$ in Frage, was überhaupt (unabhängig von der Einheitenbedingung) das Minimum für die erste Komponente ist. □

Explizit geht es bei $D = 2, 3 \mod 4$ um die Lösungen der Gleichung

$$a^2 - Db^2 = \pm 1$$

mit a, b ganzzahlig und bei $D = 1 \mod 4$ um Lösungen der Gleichung

$$\left(\frac{a}{2}\right)^2 - D\left(\frac{b}{2}\right)^2 = \pm 1$$

mit a, b ganzzahlig mit $a + b$ geradzahlig, was auf die ganzzahlige Gleichung

$$a^2 - Db^2 = \pm 4$$

führt. Diese Gleichung (en) nennt man auch die *Pellsche Gleichung*, wobei der Sprachgebrauch nicht einheitlich ist. Die Gleichung in der letzten Form erfasst jedenfalls alle Möglichkeiten, wobei nicht jede Lösung zu einer Einheit führt, beispielsweise entspricht

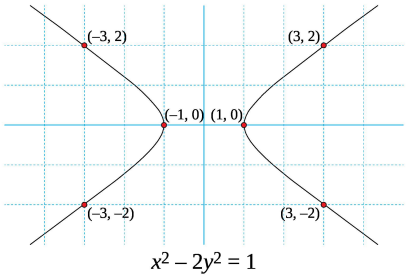
$$(a, b) = (2, 0)$$

direkt keiner Lösung (die Hälfte davon aber wiederum schon).

Bemerkung 29.4. Mit Lemma 29.3 kann man prinzipiell konstruktiv eine Fundamentaleinheit bestimmen, indem man zu aufsteigendem $a > 0$ (ganzzahlig oder ein ganzzahliges Vielfaches von $\frac{1}{2}$) untersucht, ob die Gleichung

$$a^2 - b^2 D = \pm 1$$

eine Lösung in b besitzt, wofür nur endlich viele Kandidaten zu überprüfen sind. Man hat aber von vornherein keine Schranke für a, daher weiß man nicht, wie schnell diese Methode zum Erfolg führt.



Beispiel 29.5. In $\mathbb{Z}[\sqrt{2}]$ ist wegen

$$(1+\sqrt{2})(1-\sqrt{2}) \;=\; 1-2 \;=\; -1$$

das Element $1+\sqrt{2}$ eine Einheit. Nach Lemma 29.3 handelt es sich um die eindeutig bestimmte Fundamentaleinheit > 1.

Beispiel 29.6. Wir suchen in $\mathbb{Z}[\sqrt{3}]$ gemäß Bemerkung 29.4 nach der Fundamentaleinheit, nach Satz 9.8 müssen wir nur $a+b\sqrt{3}$ mit ganzzahligen $a, b \geq 1$ überprüfen, ob

$$N(a+b\sqrt{3}) \;=\; a^2-3b^2 \;=\; \pm 1$$

gilt. Für $a = 1$ gibt es keine Lösung, und bei $a = 2$ ist mit $b = 1$ eine Lösung gefunden. Somit ist $2+\sqrt{3}$ die Fundamentaleinheit. Die anderen Einheiten oberhalb von 1 sind $\left(2+\sqrt{3}\right)^2 = 7+4\sqrt{3}$, $\left(2+\sqrt{3}\right)^3 = 26+15\sqrt{3}$, u.s.w.

Für quadratfreies $D \geq 2$ kann man so algorithmisch die Fundamentaleinheit $u > 1$ des quadratischen Zahlbereiches A_D bestimmen. Für kleine D ergibt sich die folgende Tabelle.

D	2	3	5	6	7	10	11	13	14	15
u	$1+\sqrt{2}$	$2+\sqrt{3}$	$\frac{1+\sqrt{5}}{2}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$18+5\sqrt{13}$	$15+4\sqrt{14}$	$4+\sqrt{15}$

Die Norm der Fundamentaleinheit ist wie von jeder Einheit gleich 1 oder -1. Es ist eine interessante Frage, ob die Fundamentaleinheit die Norm 1 oder -1 ist. Für $D = 2, 5, 10, 13, 17, \ldots$ ist die Norm der Fundamentaleinheit gleich -1.

29.2. **Weitere Beispiele.**

Beispiel 29.7. Wir betrachten den Zahlbereich $R = \mathbb{Z}[\sqrt[3]{2}]$ vom Grad 3, eine Ganzheitsbasis ist $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ nach Korollar 16.2. Es ist

$$(1-\sqrt[3]{2})(1+\sqrt[3]{2}+\sqrt[3]{2}^2) \;=\; 1-\sqrt[3]{2}^3 \;=\; 1-2 \;=\; -1.$$

d.h. das Element $1-\sqrt[3]{2}$ ist eine Einheit, und zwar keine Einheitswurzel.

In Fröhlich/Taylor wird erwähnt, dass in $\mathbb{Q}[\sqrt[3]{23}]$ das Element

$$2166673601 + 761875860\sqrt[3]{23} + 267901370\sqrt[3]{23}^2$$

eine Fundamentaleinheit ist.

Beispiel 29.8. Der fünfte Kreisteilungskörper (vergleiche Beispiel 17.5) die Gestalt

$$K_5 \cong \mathbb{Q}[X]/\big(X^4 + X^3 + X^2 + X + 1\big)$$

und die komplexen Einbettungen sind durch $X \mapsto e^{j2\pi \mathrm{i}/5}$ mit $j = 1, 2, 3, 4$ gegeben, wobei die Einbettungen zu 1 und 4 und zu 2 und 3 zueinander komplex-konjugiert sind. Es gibt keine reelle Einbettung und es ist $r = 0$ und $s = 2$. Der Rang der Einheitengruppe ist also 1 nach Satz 28.7. Wegen $\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}] \subset K_5$ gibt es einen reellen Zwischenkörper und dieser enthält auch schon eine Einheitengruppe vom Rang 1. Es ist

$$\frac{1+\sqrt{5}}{2} = x^4 + x + 1 = -x^2 - x^3$$

und wegen

$$\frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = -1$$

ist dies eine Einheit im quadratischen Zahlbereich zu 5, und zwar nach Lemma 29.3 die Fundamentaleinheit > 1.

29.3. **Der Regulator.**

Definition 29.9. Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen und es sei $u_1, \ldots, u_{r+s-1}$ ein System von Fundamentaleinheiten. Dann nennt man den Betrag der Determinante der reellen $(r+s-1) \times (r+s-1)$-Matrix

$$\begin{pmatrix} L_1(u_1) & \ldots & L_1(u_{r+s-1}) \\ \vdots & \ddots & \vdots \\ L_{r+s-1}(u_1) & \ldots & L_{r+s-1}(u_{r+s-1}) \end{pmatrix},$$

wobei $L = (L_1, \ldots, L_{r+s})$ die logarithmische Gesamtabbildung bezeichnet, den *Regulator* von R. Er wird mit $\mathrm{Reg}(R)$ bezeichnet.

Man beachte, dass in der Definition des Regulators nur $r+s-1$ Komponenten der (logarithmischen) Gesamtabbildung verwendet werden. Das Bild der Einheiten liegt ja in einer Hyperebene des $\mathbb{R}^{r+s}$, ist also dort nicht volldimensional. Wir werden gleich sehen, dass es zur Berechnung egal ist, welche Komponente man weglässt. Wenn $r+s = 1$ ist (wie bei $\mathbb{Z}$ oder einem imaginär-quadratischen Zahlbereich), so ist die Definition als 1 zu interpretieren (Determinante der leeren Matrix).

Lemma 29.10. *Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen und es sei $u_1, \ldots, u_{r+s-1}$ ein System von Fundamentaleinheiten von R. Es sei Λ das von $L(u_1), \ldots, L(u_{r+s-1})$ im Untervektorraum $H = \left\{(v_1, \ldots, v_{r+s}) \mid \sum_{j=1}^{r+s} v_j = 0\right\} \subset \mathbb{R}^{r+s}$ erzeugte Gitter. Dann besteht zwischen dem Regulator und dem Volumen einer Grundmasche $\mathfrak{M}$ von Λ der Zusammenhang*

$$\sqrt{r+s} \cdot \operatorname{Reg}(R) = \operatorname{vol}(\mathfrak{M}).$$

Beweis. Siehe Aufgabe 29.16. □

Dies zeigt insbesondere, dass es bei der Definition des Regulators auf die Reihenfolge der Einbettungen nicht ankommt und man eine beliebige Komponente weglassen kann.

Bemerkung 29.11. Es sei $D \geq 2$ quadratfrei und A_D der zugehörige reellquadratische Zahlbereich. Es sei $A_D \subseteq \mathbb{R}$ eine reelle Einbettung und sei u eine Fundamentaleinheit von R. Dann ist der Regulator von A_D gleich

$$\operatorname{Reg}(A_D) = |\ln |u||.$$

An dieser Definition sieht man direkt, dass wenn man u durch eine der anderen Fundamentaleinheiten $-u, u^{-1}, -u^{-1}$ ersetzt, dies zum gleichen Ergebnis führt: Das Vorzeichen wird durch den inneren Betrag und die Inversenbildung durch den äußeren Betrag aufgefangen. Auch von der gewählten Einbettung hängt es nicht ab, da ja die andere Einbettung aus der gegebenen Einbettung durch einen Automorphismus hervorgeht und dabei u auf eines der drei Elemente abgebildet wird.

29. Arbeitsblatt

29.1. **Aufgaben.**

Aufgabe 29.1. Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung vom Grad d und sei R der zugehörige Zahlbereich. Zeige, dass für Rang der Einheitengruppe $R^\times$ die Abschätzungen

$$\operatorname{rang} R^\times \leq d - 1$$

und

$$\operatorname{rang} R^\times \geq \begin{cases} \frac{d}{2} - 1, & \text{bei } d \text{ gerade,} \\ \frac{d-1}{2}, & \text{bei } d \text{ ungerade,} \end{cases}$$

gelten.

Aufgabe 29.2.*

(1) Zeige die Gleichheit

$$\left|\ln\left|\frac{1+\sqrt{5}}{2}\right|\right| = \left|\ln\left|\frac{1-\sqrt{5}}{2}\right|\right|.$$

(2) Stimmt diese Gleichung auch ohne die äußeren Beträge?
(3) Wie sieht es aus, wenn man die inneren Beträge weglässt?

Aufgabe 29.3. Wir betrachten auf den von 0 verschiedenen reellen Zahlen $\mathbb{R}^\times$ die folgende Menge von vier Abbildungen.

$$G = \{\text{Identität}\,, \text{Negation}\,, \text{Invertierung, Negation des Inversen}\}.$$

(1) Zeige, dass G eine kommutativen Gruppe ist. Was ist die Ordnung der Abbildungen? Was ist der Isomorphietyp der Gruppe?
(2) Die Gruppe G operiert in natürlicher Weise auf $\mathbb{R}^\times$. Bestimme die Bahnen zu dieser Operation, wie viele Elemente besitzen die Bahnen? Gibt es Fixpunkte?
(3) Bestimme ein übersichtliches Repräsentantensystem für die Operation aus (2).

Aufgabe 29.4. Bestimme für den quadratischen Zahlbereich A_D zu $D = 5$ die Fundamentaleinheit > 1.

Aufgabe 29.5. Bestimme für den quadratischen Zahlbereich A_D zu $D = 6$ die Fundamentaleinheit > 1.

Aufgabe 29.6. Bestimme für den quadratischen Zahlbereich A_D zu $D = 7$ die Fundamentaleinheit > 1.

Aufgabe 29.7. Zeige, dass man Lemma 29.3 auch mit der zweiten Komponente formulieren kann. Zeige ferner, dass die erste Komponente nur in der Fundamentaleinheit minimal ist, während die zweite Komponente mehrfach minimal sein kann.

Aufgabe 29.8. Zeige, dass die Einheitengruppe von $\mathbb{Z}[\sqrt{5}]$ isomorph zu $\{1,-1\} \times \mathbb{Z}$ ist.

Aufgabe 29.9. Es sei $R = \mathbb{Z}[Y]/(Y^2 - 6Y + 1)$. Zeige, dass die Restklasse y von Y in R kein Quadrat ist, wohl aber im Quotientenkörper $Q(R)$.

Aufgabe 29.10. Es sei u die Fundamentaleinheit von $R = \mathbb{Z}[\sqrt{2}]$. Bestimme die multiplikative Ordnung von u in R/pR für $p = 2, 3, 5, 7, 11$.

Aufgabe 29.11.*

Beschreibe die logarithmische Ableitung

$$R^\times \longrightarrow \Omega_{R|\mathbb{Z}},\ f \longmapsto \frac{df}{f},$$

für $R = \mathbb{Z}[\sqrt{2}]$ mit Hilfe einer Fundamentaleinheit von R. Was ist die Ordnung des Bildes einer Fundamentaleinheit?

Aufgabe 29.12.*

Beschreibe die logarithmische Ableitung

$$R^\times \longrightarrow \Omega_{R|\mathbb{Z}},\ f \longmapsto \frac{df}{f},$$

für $R = \mathbb{Z}[\sqrt{7}]$ mit Hilfe einer Fundamentaleinheit von R. Was ist die Ordnung des Bildes einer Fundamentaleinheit?

Aufgabe 29.13.*

Zeige, dass im 15. Kreisteilungsring $R_{15} = \mathbb{Q}[X]/(\Phi_{15})$ mit

$$\Phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$$

das Element $X - 1$ eine Einheit ist.

Aufgabe 29.14.*

(1) Bestimme für den 15. Kreisteilungskörper $R_{15} = \mathbb{Q}[X]/(\Phi_{15})$ mit

$$\Phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$$

das Minimalpolynom für $Y = X + X^{-1} = X + X^{14}$.

(2) Es sei $S = \mathbb{Z}[Y] \subseteq R_{15}$ der von Y erzeugte Unterring. Bestimme die Ringautomorphismen von S.

(3) Ist Y eine Einheit in S?

(4) Beschreibe die Einheitengruppe von S.

Aufgabe 29.15.*

Es sei

$$\begin{aligned} S &= \mathbb{Z}[Y]/\big(Y^4 - Y^3 - 4Y^2 + 4Y + 1\big) \\ &\subseteq R_{15} \\ &= \mathbb{Z}[X]/\big(X^8 - X^7 + X^5 - X^4 + X^3 - X + 1\big), \end{aligned}$$

wobei $Y = X + X^{-1}$ ist.

(1) Zeige, dass das Element

$$Z \;=\; \frac{1+\sqrt{5}}{2}$$

zu S gehört.
(2) Schreibe Z als polynomialen Ausdruck in Y.
(3) Beschreibe S als quadratische Erweiterung von $\mathbb{Z}[Z]$.

Aufgabe 29.16.*

Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen und es sei $u_1, \ldots, u_{r+s-1}$ ein System von Fundamentaleinheiten von R. Es sei Λ das von $L(u_1), \ldots, L(u_{r+s-1})$ im Untervektorraum $H \;=\; \left\{(v_1, \ldots, v_{r+s}) \mid \sum_{j=1}^{r+s} v_j = 0\right\} \;\subset\; \mathbb{R}^{r+s}$ erzeugte Gitter. Zeige, dass zwischen dem Regulator und dem Volumen einer Grundmasche $\mathfrak{M}$ von Λ der Zusammenhang

$$\sqrt{r+s} \cdot \operatorname{Reg}(R) \;=\; \operatorname{vol}(\mathfrak{M})$$

besteht.

Abbildungsverzeichnis