

Darstellungen von Gruppen in der  
Algebraischen Zahlentheorie:  
eine Einführung

Boas Erez

11. September 2003

## Zusammenfassung

In diesem Bericht werden eine Reihe von Ergebnissen vorgestellt, die im Laufe der Zeit zur Formulierung von Problemen geführt haben, für welche ich mich interessiere. Die Darstellung ist nicht chronologisch, sondern nimmt Rücksicht auf die zum jeweiligen Zeitpunkt bereits eingeführten Begriffe.

Eine Möglichkeit, eine Frage zu motivieren, besteht darin, den Weg einer Idee nochmals zu durchlaufen. Da es sich hier letztlich um ein Problem der algebraischen Zahlentheorie handelt, werde ich damit beginnen, verschiedene Probleme und Begriffe dieser Theorie einzuführen; diese scheinen – zu Anfang – nur wenig miteinander zu tun zu haben. Ich hoffe aber, daß es mir gelungen ist zu zeigen, daß diese dennoch untereinander verbunden sind, wenn dieses Band auch zugegebenermaßen etwas 'mysteriös' erscheinen mag. Die Anführungszeichen sind an dieser Stelle unerlässlich, weil dieses Band, um das es sich handelt, in Wirklichkeit ein bewiesener Satz ist. Nach meiner Meinung handelt es sich bei fraglichen 'Mysterium' um etwas, das zum Inhalt und zur Schönheit der Mathematik wesentlich beiträgt; ich hoffe, daß es mir gelungen ist, dies und die dahinterstehenden Ideen zu erklären.

# Kapitel 1

## Zahlkörper und algebraische Zahlen

In diesem ersten Kapitel soll gezeigt werden, wie einige moderne Konzepte der algebraischen Zahlentheorie entwickelt wurden, um die Lösung gewisser Probleme der klassischen Zahlentheorie zu verstehen.

### 1.1 Primzahlen

Die algebraische Zahlentheorie beschäftigt sich mit ... Zahlen. Aber was für welchen? Die Zahlen, die einem am wenigsten Probleme zu bereiten scheinen, sind die natürlichen Zahlen: die Menge  $\mathbb{N}$ , die aus  $1, 2, 3, \dots$  etc. besteht. Wir wollen uns nicht mit einer Diskussion der negativen Zahlen aufhalten und betrachten auch die Menge  $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$  der ganzen rationalen Zahlen als bekannt.

Man stellt nun fest, daß es in diesen ganzen Zahlen die Relation der *Teilbarkeit* gibt; einige dieser Zahlen haben dabei die Eigenschaft, daß ihre Teiler ziemlich trivial sind, nämlich die Zahlen  $\pm 1, \pm 2, \pm 3, \pm 5, \dots, \pm 163, \dots$ . Die ganze Zahl 163 ist beispielsweise genau durch die vier Zahlen  $\pm 1$  und  $\pm 163$  teilbar. Solche Zahlen mit genau vier Teilern (man beachte, daß die Zahlen  $\pm 1$  nicht dazu gehören) nennt man *prim*. Die Primzahlen spielen in der Mathematik eine wichtige Rolle; so gilt z.B. der

**Satz 1.1. Fundamentalsatz der Arithmetik** *Jede ganze Zahl  $n \in \mathbb{Z}$  läßt sich eindeutig als Produkt von Primzahlen schreiben; genauer: für jedes  $n \in \mathbb{Z}$*

existieren endlich viele eindeutig bestimmte Primzahlen  $p_1 < p_2 < \dots < p_r$  und natürliche Zahlen  $n_0, n_1, \dots, n_r \in \mathbb{N}$  mit

$$n = (-1)^{n_0} \cdot p_1^{n_1} \dots p_r^{n_r}. \quad (1.1)$$

Dabei sind auch die  $n_i \in \mathbb{N}$  eindeutig bestimmt, wenn man  $n_0 \in \{1, 2\}$  wählt.

Dieser Fundamentalsatz ist derart grundlegend, daß es scheinen könnte, er sei offensichtlich wahr und bedürfe keines Beweises. Wir werden weiter unten aber sehen, daß dieser Schein trügt. Bleiben wir noch ein bißchen beim Fundamentalsatz: er besagt, daß sich die unendlich vielen ganzen Zahlen als Produkt von Primzahlen und einem Vorzeichen schreiben lassen. Wenn die Anzahl dieser Primzahlen endlich wäre, würde es genügen, die Eigenschaften dieser endlich vielen Primzahlen zu untersuchen, um fast alle Eigenschaften der ganzen Zahlen zu verstehen. Leider – oder glücklicherweise – hat schon Euklid zeigen können, daß es unendlich viele Primzahlen gibt. Andererseits scheint es, daß die chinesischen Mathematikern, die – wie die Griechen – ebenfalls die Arithmetik auf konkrete Probleme angewandt haben, den Begriff der Primzahl nicht verwendet haben. Die Primzahlen sind also keine logische Notwendigkeit: jedenfalls sind sie aber nützlich, eben weil sie im Fundamentalsatz der Arithmetik auftauchen.

## 1.2 Summen von Quadraten

Vermutlich wegen ihrer geometrischen Bedeutung hat man sich schon früh für die Quadratzahlen interessiert, also diejenigen natürlichen Zahlen, die man durch die Multiplikation einer Zahl mit sich selbst erhält. Es ist klar, daß nicht jede natürliche Zahl ein Quadrat ist; vielleicht läßt sich aber jede natürliche Zahl als Summe zweier Quadrate schreiben? Nun ist  $1 = 1^2 + 0^2$ ,  $2 = 1^2 + 1^2$ ,  $4 = 2^2 + 0^2$  und  $5 = 1^2 + 2^2$ , aber 3 ist nicht Summe zweier Quadrate. Wir wollen beiläufig erwähnen, daß Lagrange 1770 bewiesen hat, daß sich jede natürliche Zahl als Summe von höchstens vier Quadraten schreiben läßt.

Aber bleiben wir beim Problem von zwei Quadraten.

Wir bemerken zuerst, daß das Produkt von Summen zweier Quadrate wieder eine Summe zweier Quadrate ist:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \quad (1.2)$$

Diese Beobachtung von Fibonacci erlaubt es dank des Fundamentalsatzes der Arithmetik, unser Problem auf ein Problem über Primzahlen zurückzuführen:

denn wenn wir wissen, welche Primzahlen Summen zweier Quadrate sind, dann können wir mittels des Fundamentalsatzes auch die Bedingungen angeben, die eine beliebige Zahl genügen muß, um Summe zweier Quadrate zu sein. Man kann nun zeigen, daß eine ungerade Primzahl  $p$  genau dann Summe zweier Quadrate ist, wenn 4 Teiler von  $p - 1$  ist. Ist weiter  $n$  die Summe der beiden Quadrate  $a^2$  und  $b^2$ , so können zwei Fälle auftreten: entweder teilt  $p$  sowohl  $a$  als auch  $b$  (in diesem Fall ist  $n$  durch  $p^2$  teilbar), oder  $p$  teilt weder  $a$  noch  $b$ . Im zweiten Fall kann man zeigen, daß dann  $p - 1$  durch 4 teilbar oder  $p = 2$  sein muß. Zusammenfassend haben wir das folgende Resultat, das die Summen zweier Quadrate vollständig charakterisiert:

**Satz 1.2. Fermat** *Ist  $n$  eine natürliche Zahl mit Primfaktorzerlegung wie in (1.1): dann ist  $n$  Summe zweier Quadrate genau dann, wenn die Primzahlen  $p_i$  in (1.1), für die  $p_i + 1$  durch 4 teilbar ist, mit geradem Exponenten  $n_i$  auftreten.*

**Beispiel.** Die Zahl  $n = 15 = 3 \cdot 5$  ist keine Summe zweier Quadrate,  $n = 45 = 3^2 \cdot 5$  dagegen schon.

Um diese Eigenschaft auf andere Weise beschreiben zu können, führen wir die Gaußschen Zahlen ein.

### 1.3 Die Gaußschen Zahlen

In diesem Abschnitt ist eine Kenntnis der komplexen Zahlen hilfreich. Wir betrachten ein Symbol  $i$ , und allgemeiner Ausdrücke der Form  $a + bi$ , wo  $a$  und  $b$  ganze Zahlen sind: es ist dann  $i = 0 + 1 \cdot i$ . Die Gesamtheit dieser Symbole wird mit  $\mathbb{Z}[i]$  (lies:  $\mathbb{Z}$  adjungiert  $i$ ) bezeichnet, und heißt *Ring ganzer Gaußscher Zahlen*.

Wir können uns die ganzen Zahlen  $\mathbb{Z}$  als in  $\mathbb{Z}[i]$  eingebettet vorstellen: ist  $n \in \mathbb{Z}$ , so identifizieren wir  $n$  mit dem Element  $n + 0 \cdot i$  von  $\mathbb{Z}[i]$ . Wir definieren die Summe, bzw. das Produkt von  $a + bi$  und  $c + di$  in  $\mathbb{Z}[i]$  durch  $(a+c) + (b+d)i$ , bzw.  $(ac-bd) + (ad+bc)i$ . Insbesondere sind diese Operationen mit Addition und Multiplikation in  $\mathbb{Z}$  verträglich, sowie mit  $i^2 = -1$ .

Stellen wir  $a + bi$  in einem kartesischen Koordinatensystem dar als Punkt mit der Abszisse  $a$  und Ordinate  $b$ , so sehen wir, daß die ganze Zahl  $a^2 + b^2$  das Quadrat des Abstands von  $a + bi$  zum Ursprung ist. Wir nennen diese Zahl die *Norm* von  $a + bi$  und bezeichnen sie mit

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$

Man sieht leicht, daß  $N(u)N(v) = N(uv)$  für alle  $u, v \in \mathbb{Z}[i]$  gilt (vgl. dies mit der Identität (1.2) von Fibonacci).

Wir können an dieser Stelle bereits erraten, daß es zwischen den Gaußschen Zahlen und den Summen zweier Quadrate einen Zusammenhang gibt. Um diesen zu finden, untersuchen wir die Arithmetik von  $\mathbb{Z}[i]$ . Genauer wollen wir uns fragen, ob der Fundamentalsatz der Arithmetik auch für  $\mathbb{Z}[i]$  gilt.

Die wesentliche Eigenschaft, die  $\mathbb{Z}[i]$  und  $\mathbb{Z}$  gemeinsam haben, ist die Existenz einer 'Division mit Rest'. Erinnern wir uns daran, daß dies in  $\mathbb{Z}$  bedeutet, daß es zu zwei ganzen Zahlen  $m, n \in \mathbb{Z}$  mit  $n \neq 0$  immer zwei ganze Zahlen  $q$  und  $r$  gibt derart, daß  $m = qn + r$  gilt und der Betrag von  $r$  echt kleiner ist als derjenige von  $n$ , in Zeichen:  $|r| < |n|$ . Man kann nun zeigen, daß es zu  $u, v \in \mathbb{Z}[i]$  mit  $v \neq 0$  immer  $q, r \in \mathbb{Z}[i]$  gibt derart, daß  $u = qv + r$  gilt und die Norm von  $r$  echt kleiner ist als diejenige von  $v$ , in Zeichen:  $N(r) < N(v)$ .

Der Beweis ist einfach und hübsch. Wir beginnen mit der Beobachtung, daß ein Quotient zweier Elemente  $a + bi$  und  $c + di$  sich in der Form  $s + ti$  mit  $s, t \in \mathbb{Q}$  schreiben läßt: mit den oben eingeführten Operationen gilt nämlich

$$\frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.$$

Ein einfaches elementargeometrisches Argument zeigt – man beachte wieder die Darstellung im kartesischen Koordinatensystem – daß es zu jedem  $s + ti$  mit  $s, t \in \mathbb{Q}$  ein Element  $q \in \mathbb{Z}[i]$  gibt mit  $N(s + ti - q) < 1$ . Wenden wir diese Beobachtung auf den Quotienten der beiden Zahlen  $u$  und  $v$  an. Wir sehen dann, daß es ein  $q \in \mathbb{Z}[i]$  gibt mit  $N(u/v - q) < 1$ ; setzen wir  $r := u - qv$ , so haben wir angesichts von  $N(u/v - q) = N(u - qv)/N(v) < 1$  das gewünschte Resultat  $N(r) < N(v)$ .

Jetzt, wo wir wissen, daß es in  $\mathbb{Z}[i]$  eine Division mit Rest gibt, können wir wie in  $\mathbb{Z}$  verfahren und das Analogon des Fundamentalsatzes für  $\mathbb{Z}[i]$  beweisen (sh. [IR], 1.4). Wir sollten vielleicht auch die Rolle der invertierbaren Elemente in  $\mathbb{Z}[i]$  erwähnen, die sich wie  $\pm 1$  in  $\mathbb{Z}$  verhalten.

Daher sind auch in  $\mathbb{Z}[i]$  die Primelemente wichtig, und man muß sie kennen, um die Arithmetik in  $\mathbb{Z}[i]$  zu verstehen. Es wäre denkbar, daß die Primelemente von  $\mathbb{Z}$  auch in  $\mathbb{Z}[i]$  prim sind; aber schon die Zahl 2 ist ein Gegenbeispiel, wie man an  $2 = (1 + i)(1 - i) = N(1 + i)$  sieht. Allgemeiner gilt, daß eine Primzahl  $p$  genau dann in  $\mathbb{Z}[i]$  prim bleibt, wenn sie nicht Norm einer

Zahl aus  $\mathbb{Z}[i]$  ist, mit anderen Worten: wenn  $p$  nicht Summe zweier Quadrate ist!

Es ist klar, daß  $p$  nicht prim in  $\mathbb{Z}[i]$  ist, wenn  $p = (a + bi)(a - bi) = N(a + bi)$  gilt. Ist umgekehrt  $p$  nicht prim in  $\mathbb{Z}[i]$ , so zerfällt  $p$  in ein Produkt  $p = (a + bi)(c + di)$ , wobei  $a + bi$  und  $c + di$  nicht gleich  $\pm 1, \pm i$  sind (dies sind die einzigen invertierbaren Elemente in  $\mathbb{Z}[i]$ ). Bilden der Norm liefert  $p^2 = (a^2 + b^2)(c^2 + d^2)$  und somit, da  $p$  prim in  $\mathbb{Z}$  ist,  $p = a^2 + b^2 = c^2 + d^2$ .

Nun, da wir die Verbindung zwischen den Gaußschen Zahlen und dem klassischen Problem der Summen zweier Quadrate gefunden haben, können wir darangehen, diese Gaußschen Zahlen mit berechtigtem Interesse zu studieren.

## 1.4 Zahlkörper

Einen Körper  $K$ , welcher die rationalen Zahlen  $\mathbb{Q}$  enthält, kann man als  $\mathbb{Q}$ -Vektorraum auffassen. Ist die Dimension von  $K$  als  $\mathbb{Q}$ -Vektorraum endlich, so nennt man  $K$  einen Zahlkörper. Man kann zeigen, daß es in jedem Zahlkörper  $K$  ein Element  $\alpha$  gibt, sodaß sich jedes  $\beta \in K$  in der Form  $\beta = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$  mit Koeffizienten  $a_j \in \mathbb{Q}$  schreiben läßt, d.h. daß es eine  $\mathbb{Q}$ -Basis von  $K$  gibt, die aus lauter Potenzen eines einzigen Elements  $\alpha$  besteht. Um diese Eigenschaft auszudrücken, verwendet man die Schreibweise  $K = \mathbb{Q}(\alpha)$ . Für eine Wiederholung der Begriffe der linearen Algebra sh. [L2].

**Beispiel.** Sei  $d$  eine ganze quadratfreie Zahl, also z.B.  $d = -1$  oder  $d = 2$ , und sei  $\sqrt{d}$  eine (komplexe) Zahl mit  $\sqrt{d}^2 = d$ . Dann bildet die Menge aller Ausdrücke  $s + t\sqrt{d}$  mit  $s, t \in \mathbb{Q}$  einen Körper  $\mathbb{Q}(\sqrt{d})$  der Dimension 2 über  $\mathbb{Q}$  (in der Tat ist z.B.  $\{1, \sqrt{d}\}$  eine  $\mathbb{Q}$ -Basis von  $K$ ). Zahlkörper der Form  $\mathbb{Q}(\sqrt{d})$  nennt man *quadratische Zahlkörper*.

## 1.5 Ganze Algebraische Zahlen

Ein weiterer fundamentaler Begriff in der algebraischen Zahlentheorie ist derjenige einer ganzen algebraischen Zahl. Dieser Begriff ist das Resultat der Suche nach einer guten Verallgemeinerung des Begriffs der ganzen Zahlen innerhalb von  $\mathbb{Q}$ , sowie der Gaußschen Zahlen.

Wir suchen nach der Definition einer Familie von (komplexen) Zahlen, für die mit zwei Elementen auch deren Summe und Produkt wieder dazugehört,

und welche darüberhinaus mit  $\mathbb{Q}$  genau die ganzen Zahlen  $\mathbb{Z}$  gemeinsam hat (diese Formulierung des Problems stammt aus dem Buch [He]).

Die Lösung dieses Problems ist überraschend einfach ... es ist im wesentlichen eine Frage des Vokabulars. Sei  $K$  ein Zahlkörper; ein Element  $\alpha \in K$  heißt eine *ganze algebraische Zahl*, wenn es Zahlen  $a_0, a_1, \dots, a_n - 1$  aus  $\mathbb{Z}$  gibt mit  $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$ . Insbesondere ist  $i$  eine ganze algebraische Zahl wegen  $i^2 + 1 = 0$ ,  $\frac{1}{2}$  dagegen nicht. Die Menge  $\mathbb{Z}_K$  aller ganzen algebraischen Zahlen eines Zahlkörpers  $K$  nennt man seinen *Ganzheitsring*.

Man kann zeigen, daß  $\mathbb{Z}[i]$  die Menge aller ganzen Zahlen von  $\mathbb{Q}(i)$  ist. Man beachte aber: im allgemeinen ist  $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$  *nicht* der Ganzheitsring des quadratischen Zahlkörpers  $\mathbb{Q}(\sqrt{d})$ . Der Leser möge als Übung untersuchen, unter welchen Bedingungen  $\frac{1}{2}(a + b\sqrt{d})$  eine ganze algebraische Zahl ist (Lösung: sh. [Sa]).

## 1.6 Ideale

Wir haben gesehen, daß die Gaußschen Zahlen Eigenschaften besitzen, die denjenigen von  $\mathbb{Z}$  völlig analog sind. Aber schon für Ganzheitsringe anderer quadratischer Zahlkörper ist dies falsch. Beispielsweise hat die Zahl 6 in  $\mathbb{Z}[\sqrt{-5}]$  die beiden wesentlich verschiedenen Faktorisierungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = N(1 + \sqrt{-5}). \quad (1.3)$$

Die beiden Zahlen 3 und  $(1 + \sqrt{-5})$  haben in  $\mathbb{Z}[\sqrt{-5}]$  keine nichttrivialen Teiler. In der Tat, wäre z. B.  $(1 + \sqrt{-5})$  durch  $a + b\sqrt{-5}$  teilbar, so wäre  $6 = N(1 + \sqrt{-5})$  durch die Norm  $a^2 + 5b^2 = N(a + b\sqrt{-5})$  teilbar, d.h. es müßte  $a^2 + 5b^2 = 2$  oder  $a^2 + 5b^2 = 3$  gelten. Diese beiden Gleichungen besitzen aber keine Lösungen in  $\mathbb{Z}$ . Dem Leser sei der diesbezügliche Kommentar Kummers zur Lektüre empfohlen (sh. [W2], p. 381).

Wenn wir also lediglich die Operationen zwischen *Elementen* (d.h. Zahlen) eines Zahlkörpers betrachten, so dürfen wir nicht hoffen, ein Fundamentalsatz der Arithmetik für den Ganzheitsring von Zahlkörpern beweisen zu können. Der richtige Weg, den Fundamentalsatz zu verallgemeinern, erfordert die Einführung von Objekten, die ursprünglich 'ideale Zahlen' genannt wurden. Heute heißen sie einfach *Ideale*, und dieser Begriff hat inzwischen – dank der Algebra – weite Teile der gesamten Mathematik durchdrungen.

Es ist lohnend, sich die Arbeiten von Kummer (ab 1845) anzusehen; dieser hat in seiner Attacke auf das Fermatproblem ( $x^n + y^n = z^n$ ) und seiner

Erforschung der Kreisteilungskörper die Basislager für die Entwicklung der algebraischen Zahlentheorie errichtet, indem er unter anderem die Grundlagen für die Idealtheorie und die  $p$ -adische Analysis gelegt hat. Für eine Würdigung der Leistungen Kummers sh. z. B. die Einführung zu seinen gesammelten Werken, die A. Weil [W1] verfaßt hat.

Vor der Einführung der Ideale erinnern wir an die Definition eines Rings. Ein (kommutativer) Ring ist eine Menge, versehen mit zwei Verknüpfungen  $+$  und  $\cdot$ , und zwei Elementen  $0$  und  $1$ , welche die üblichen Eigenschaften wie Assoziativität und Distributivität besitzen (sh. [L2] für eine formale Definition).

$\mathbb{Z}$ , und allgemeiner die Menge  $\mathbb{Z}_K$  aller ganzalgebraischen Elemente eines Zahlkörpers  $K$  (mit den Operationen aus  $K$ ) sind Beispiele von Ringen (daher auch der Name Ganzheitsring’); sh. [Sa] oder [He].

Sei ab nun  $A$  ein kommutativer Ring. Ein Ideal  $I$  in  $A$  ist eine Teilmenge von  $A$ , sodaß die Summe zweier Elemente aus  $I$ , sowie das Produkt von Elementen aus  $A$  mit solchen aus  $I$  wieder in  $I$  liegen; in Zeichen:  $I + I \subseteq I$  und  $A \cdot I \subseteq I$ .

**Beispiel 1.5.1** Die geraden Zahlen bilden ein Ideal in  $\mathbb{Z}$ , welches mit  $2\mathbb{Z}$  oder mit  $(2)$  bezeichnet wird. Ebenso bilden die Vielfachen von  $4$  ein Ideal  $4\mathbb{Z} = (4)$ , und es gilt  $(4) \subset (2)$ .

Allgemeiner bilden die endlichen Summen von Vielfachen endlich vieler Elemente  $a_1, \dots, a_r$  eines Ringes  $A$  ein Ideal, das mit  $(a_1, \dots, a_r)A$  oder einfach mit  $(a_1, \dots, a_r)$  bezeichnet wird. Ein Ideal der Form  $aA$  heißt *Hauptideal*. Ein Element  $b \in A$  ist genau dann ein Vielfaches von  $a \in A$ , wenn die Inklusion  $(b) \subseteq (a)$  gilt.

An dieser Stelle ist es angebracht, auf die Bedeutung der invertierbaren Elemente hinzuweisen: ist  $u$  invertierbar in  $A$ , dann erzeugen  $a$  und  $au$  dasselbe Ideal in  $A$ ; z.B. ist  $2\mathbb{Z} = (-2)\mathbb{Z}$  und  $2\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i]$ ; allgemeiner ist  $I = uI$  für jedes Ideal  $I$  in  $A$ .

In  $\mathbb{Z}$  sind Ideale und Zahlen fast dasselbe in dem Sinn, daß jedes Ideal  $I$  in  $\mathbb{Z}$  Hauptideal ist, daß also ein  $n \in \mathbb{Z}$  existiert mit  $I = n\mathbb{Z}$  (sh. [IR], 1.3). Dieselbe Aussage gilt für  $\mathbb{Z}[i]$ , nicht aber für  $\mathbb{Z}[\sqrt{-5}]$ .

Um die Verallgemeinerung des Fundamentalsatzes zu formulieren, müssen wir definieren, wann ein Ideal durch ein anderes teilbar sein soll, was wir unter dem Produkt zweier Ideale verstehen wollen, und wann Ideale prim sind. Sei also  $A$  kommutativer Ring und seien  $I$  und  $J$  Ideale in  $A$ .

- Man sagt,  $I$  teile  $J$ , wenn  $J$  Teilmenge von  $I$  ist ('teilen bedeutet enthalten').
- Das Produkt  $IJ$  ist die Menge der endlichen Summen von Produkten der Form  $ij$  mit  $i$  aus  $I$  und  $j$  aus  $J$ ; man zeigt leicht, daß  $IJ$  ein Ideal in  $A$  ist.
- Ein Ideal  $P \neq A$  heißt *prim*, wenn gilt: ist  $P$  Teiler von  $IJ$ , dann ist  $I$  oder  $J$  durch  $P$  teilbar.

Dem Leser sei es als Übung überlassen zu zeigen, daß eine Zahl  $p$  genau dann prim ist, wenn es das Ideal  $p\mathbb{Z}$  ist.

**Beispiel.** Betrachten wir noch einmal die Faktorisierung (1.4); wir werden nun sehen, daß sich das Ideal  $6\mathbb{Z}[\sqrt{-5}]$  auf eindeutige Art und Weise als Produkt von Idealen schreiben läßt: in der Tat ist

$$\begin{aligned} 3\mathbb{Z}[\sqrt{-5}] &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) \\ 2\mathbb{Z}[\sqrt{-5}] &= (2, 1 + \sqrt{-5})^2 \end{aligned}$$

**Satz 1.3. (Dedekind)** Sei  $\mathbb{Z}_K$  der Ganzheitsring eines Zahlkörpers  $K$ . Jedes Ideal  $\mathfrak{a}$  in  $\mathbb{Z}_K$  läßt sich eindeutig als Produkt von Primidealen schreiben, d.h. es existieren Primideale  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  und natürliche Zahlen  $n_1, \dots, n_r$  mit

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}. \quad (1.4)$$

Es ist zu bemerken, daß diese Art mit unendlichen Mengen zu rechnen niemanden überfordern wird, der z.B. die Konstruktion der reellen Zahlen als unendliche Folge rationaler Zahlen studiert hat.

## 1.7 Zerlegung von Primzahlen und Summen zweier Quadrate

Sei  $\mathbb{Z}_K$  der Ganzheitsring eines Zahlkörpers  $K$  und  $p$  eine Primzahl in  $\mathbb{Z}$ . Als Element von  $\mathbb{Z}_K$  erzeugt  $p$  ein Ideal  $p\mathbb{Z}_K$  und zerfällt gemäß Satz 1.3. Es gibt also Primideale  $\mathfrak{p}_1, \dots, \mathfrak{p}_g$  und natürliche Zahlen  $e_1, \dots, e_g$  mit

$$p\mathbb{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \quad (1.5)$$

Wir wollen uns diese Zerlegung von  $p$  in  $\mathbb{Z}_K$  genauer ansehen, und zwar hinsichtlich der Verzweigung von  $p$  in  $K/\mathbb{Q}$ . Die Zahl  $e_i$  in (1.5) nennt man den *Verzweigungsindex* von  $\mathfrak{p}_i$  in  $K/\mathbb{Q}$ .

**Beispiel.** Ist  $K$  ein quadratischer Zahlkörper, so gibt es drei verschiedene Möglichkeiten, wie  $p$  sich in  $K$  verhalten kann: entweder ist  $p\mathbb{Z}_K = \mathfrak{p}^2$ ,  $p\mathbb{Z}_K = \mathfrak{p}$ , oder  $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ ; man sagt dann,  $p$  sei in  $K/\mathbb{Q}$  *verzweigt*, *träge*, oder *zerlegt*.

In dieser Sprache läßt sich ein Teil von Satz 1.2 so formulieren:

Eine ungerade Primzahl  $p$  ist Summe zweier Quadrate genau dann, wenn  $p$  in  $\mathbb{Q}(i)$  zerlegt ist.

Allgemeiner sagt man, eine Primzahl  $p$  sei in  $K$  *verzweigt*, wenn für mindestens eines der  $\mathfrak{p}_i$  in (1.5)  $e_i \geq 2$  gilt. Man kann zeigen, daß es in einem gegebenen Zahlkörper  $K$  nur endlich viele Primzahlen  $p$  geben kann, die in  $K/\mathbb{Q}$  verzweigen, und daß diese alle Teiler einer ganzen Zahl  $d_K$  sind (eine Invariante von  $K$ ), die man Diskriminante von  $K$  nennt.

## 1.8 Kreisteilungskörper

Ich beende dieses erste Kapitel mit einem kurzen Abschnitt über eine wichtige Familie von Zahlkörpern: den Kreisteilungskörpern. Ich stelle diese Körper mit der Absicht vor, ein Beispiel zu geben, dessen wir uns im folgenden oft bedienen werden, sowie um damit eine Reihe von Definitionen zu erläutern, die sonst vielleicht ein wenig zu formal wären, um interessant zu sein (Um die ursprünglichen Probleme zu lösen, hat man neue Konzepte eingeführt, und diese haben dann neue Probleme geschaffen! Trotzdem haben sie bei der Klärung der ursprünglichen Probleme geholfen).

'Kreisteilung' rührt natürlich von der Teilung des Kreises her. Kreisteilungskörper sind Zahlkörper, die von Lösungen (Wurzeln) von Gleichungen der Form  $x^m = 1$  erzeugt werden. Die Lösungen dieser Gleichung (in den komplexen Zahlen) haben Betrag 1, befinden sich daher auf dem Einheitskreis und teilen diesen in  $m$  gleiche Teile. Wir werden im folgenden nur den Fall betrachten, in dem  $m$  eine Primzahl ist.

Sei also  $p$  prim. Der Körper der  $p$ -ten Einheitswurzeln ist der Körper  $\mathbb{Q}(\zeta_p)$ , der definiert ist als der kleinste Zahlkörper, der  $\mathbb{Q}$  und alle Lösungen der Gleichung  $x^p = 1$  enthält.

Nun gilt  $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + 1)$ . Sei  $\zeta$  eine komplexe Lösung der Gleichung  $x^{p-1} + x^{p-2} + \dots + 1 = 0$ , z. B.  $\zeta = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$ . Dann ist  $\mathbb{Q}(\zeta_p)$  die Menge aller komplexen Zahlen der Form

$$a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}, \quad a_0, \dots, a_{p-2} \in \mathbb{Q}. \quad (1.6)$$

Die Dimension dieses  $\mathbb{Q}$ -Vektorraums ist  $p - 1$ . Der Ganzheitsring von  $K = \mathbb{Q}(\zeta_p)$  besteht aus allen Zahlen der Form (1.6), für welche die  $a_i \in \mathbb{Z}$  sind. Das Hauptideal  $(1 - \zeta)\mathbb{Z}_K$  in  $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$  ist prim, und es gilt

$$p\mathbb{Z}[\zeta_p] = (1 - \zeta)^{p-1}\mathbb{Z}[\zeta_p].$$

Die Kreisteilungskörper  $\mathbb{Q}(\zeta_p)$  tauchen auf natürliche Art und Weise beim Fermatschen Problem auf, bei dem es um den Nachweis geht, daß die Gleichung

$$x^p + y^p = z^p \quad (1.7)$$

keine Lösung in von 0 verschiedenen ganzen Zahlen  $x, y, z$  besitzt. Um dies einzusehen, schreiben wir (1.7) in der Form

$$(x + y)(x + y\zeta)(x + y\zeta^2) \cdots (x + y\zeta^{p-1}) = z^p. \quad (1.8)$$

Indem er (1.8) als Gleichung von Idealen interpretierte, hat Kummer eine Antwort auf das Fermatsche Problem in einer Vielzahl von Fällen geben können (sh. [Wa] für eine moderne Darstellung des Kummerschen Beweises).

Analog können wir die Kreisteilungskörper  $\mathbb{Q}(\zeta_m)$  für alle natürlichen Zahlen  $m$  definieren, und zwar mittels der Kreisteilungspolynome, also der über  $\mathbb{Q}$  irreduziblen Faktoren von Polynomen der Form  $x^m - 1$  (sh. [Wa]).

# Kapitel 2

## Galoisgruppen

In diesem Kapitel geht es um die Elemente der Galoistheorie und ihrer Anwendung auf Zahlkörper. Eines unserer Ziele wird es sein, die Beziehungen zu beschreiben, die zwischen der Operation der Galoisgruppe auf dem Ganzheitsring eines Zahlkörpers einerseits und der Arithmetik in diesem Zahlkörper andererseits bestehen.

Wir beginnen mit der Betrachtung quadratischer Zahlkörper  $\mathbb{Q}(\sqrt{d})$ , sowie von Kreisteilungskörpern  $\mathbb{Q}(\zeta_p)$ , die wir oben eingeführt haben. In beiden Fällen gibt es eine Menge von (natürlichen) Transformationen dieser Körper, und diese bilden eine Gruppe (sh. [L2]).

- Im Falle von  $\mathbb{Q}(\sqrt{d})$  bildet die Transformation  $\sigma$ , welche  $a + b\sqrt{d}$  auf  $a - b\sqrt{d}$  abbildet, zusammen mit der Identität (die jedes Element auf sich abbildet) eine Gruppe mit zwei Elementen.
- Im Falle von  $\mathbb{Q}(\zeta_p)$  betrachte man die Abbildungen  $\sigma_a$ , wo  $a$  eine natürliche Zahl zwischen 1 und  $p - 1$  ist, und die ein Element der Form (1.6) auf

$$a_0 + a_1\zeta^a + a_2\zeta^{2a} + \dots + a_{p-2}\zeta^{(p-2)a}$$

abbildet.

Als Übung möge man diese Transformationen geometrisch interpretieren, indem man die Körper als Teilkörper der komplexen Zahlen auffaßt.

In beiden Fällen ist die Anzahl der Elemente der Gruppe gleich der Dimension des Zahlkörpers über  $\mathbb{Q}$ . Die Transformationen  $\sigma$ , die wir betrachtet haben, sind die sogenannten  $\mathbb{Q}$ -Automorphismen der betreffenden

Zahlkörper; das bedeutet, daß diese Transformationen Summen und Produkte respektieren, daß sie die Elemente von  $\mathbb{Q}$  fest lassen, und daß sie invertierbar sind; in Zeichen: ein  $\mathbb{Q}$ -Automorphismus  $\sigma$  hat die folgenden Eigenschaften:

- $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ ;
- $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ ;
- ist  $a \in \mathbb{Q}$ , so gilt  $\sigma(a) = a$ ;
- es gibt einen  $\mathbb{Q}$ -Automorphismus  $\tau$ , sodaß  $\sigma(\tau(\alpha)) = \tau(\sigma(\alpha)) = \alpha$  für alle  $\alpha \in K$  gilt.

Man beachte, daß es in jedem Zahlkörper mindestens einen  $\mathbb{Q}$ -Automorphismus gibt, nämlich die Identität, die jedes Element auf sich abbildet! Man kann zeigen, daß allgemein die Anzahl der  $\mathbb{Q}$ -Automorphismen eines Zahlkörpers  $K$  nicht größer sein kann als dessen Dimension über  $\mathbb{Q}$  (sh. z.B. [L2]); daher interessiert man sich natürlich für den Spezialfall, in dem beide Zahlen gleich sind. Man sagt, ein Zahlkörper sei *galoissch* über  $\mathbb{Q}$ , wenn er ebensoviele  $\mathbb{Q}$ -Automorphismen besitzt wie seine Dimension über  $\mathbb{Q}$  angibt. Die Gruppe aller  $\mathbb{Q}$ -Automorphismen eines galoisschen Zahlkörpers  $K$  heißt seine *Galoisgruppe* und wird mit  $\text{Gal}(K/\mathbb{Q})$  bezeichnet.

Eine andere Möglichkeit, galoissche Körper zu definieren, besteht darin,  $K$  in der Form  $K = \mathbb{Q}(\alpha)$  zu schreiben und zu verlangen, daß das irreduzible Polynom minimalen Grades, von welchem  $\alpha$  eine Nullstelle ist, nicht nur die Nullstelle  $\alpha$  in  $K$  besitzt, sondern daß vielmehr sämtliche Nullstellen dieses Polynoms in  $K$  liegen; in diesem Fall bildet die Galoisgruppe Wurzeln dieses Polynoms auf andere Wurzeln ab.

**Satz 2.1.** *Sei  $K$  ein galoisscher Zahlkörper (über  $\mathbb{Q}$ ) und  $G = \text{Gal}(K/\mathbb{Q})$ . Dann gibt es eine bijektive Korrespondenz zwischen den Untergruppen von  $G$  und den Teilkörpern von  $K/\mathbb{Q}$ ; dazu ordnet man jeder Untergruppe  $H$  von  $G$  die Teilmenge  $K^H$  von  $K$  zu, deren Elemente von  $H$  fest gelassen werden. Dabei ist  $H$  ein Normalteiler von  $G$  genau dann, wenn der Körper  $K^H$  ebenfalls galoissch über  $\mathbb{Q}$  ist; in diesem Fall ist  $\text{Gal}(K^H/\mathbb{Q})$  isomorph zur Faktorgruppe  $G/H$ . Schließlich gilt noch  $K^G = \mathbb{Q}$ .*

Wir haben nicht definiert, was ein Normalteiler einer Gruppe  $G$  ist, erinnern aber daran, daß in abelschen Gruppen  $G$  jede Untergruppe Normalteiler ist (sh. [L2]).

**Satz 2.2.** *Jeder  $\mathbb{Q}$ -Automorphismus eines Zahlkörpers  $K$  bildet eine Zahl (bzw. ein Ideal) aus  $\mathbb{Z}_K$  wieder auf eine Zahl (bzw. ein Ideal) aus  $\mathbb{Z}_K$  ab.*

**Definition** Ein Zahlkörper  $K$  heißt *abelsch*, wenn seine Galoisgruppe abelsch (also kommutativ) ist.

Es ist leicht nachzuvollziehen, daß die Existenz einer Gruppe, die auf allen betrachteten Objekten operiert, für die Physik und die Geometrie von nicht zu unterschätzender Bedeutung sind, insbesondere wegen der Symmetrie, die von der Operation einer Gruppe herrührt. Analog kann man beim Studium der galoisschen Zahlkörper von der Operation einer Galoisgruppe profitieren, und auch hier bringt sie eine Symmetrie ins Spiel. Diese läßt sich am leichtesten bei der Zerlegung einer rationalen Primzahl in Primideale beobachten: ist nämlich  $K$  ein galoisscher Zahlkörper, so kann man die Zerlegung (1.5) in der Form  $p\mathbb{Z}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$  schreiben.

# Kapitel 3

## Anwendung von Galoisgruppen

### 3.1 Der Satz von Stickelberger (1890)

Wir haben gesehen, wie jedes Element  $a$  eines Ringes  $A$  ein Ideal  $aA$  in  $A$  bestimmt – genauer ein Hauptideal. Obwohl wir Beispiele von Ringen kennengelernt haben, in denen – wie in  $\mathbb{Z}$  – alle Ideale Hauptideale sind, wissen wir, daß dies im allgemeinen nicht richtig ist. Es ist dieser Unterschied zwischen Zahlen und Idealen in gewissen Zahlringen algebraischer Zahlkörper, der bei der Entwicklung der Idealtheorie Pate gestanden hat. Für diese Zahlringe kann man jedoch einen Satz beweisen, der im wesentlichen besagt, daß man messen kann, wie weit Ideale in solchen Ringen davon entfernt sind, Hauptideale zu sein. Genauer kann man für jeden Zahlring  $\mathbb{Z}_K$  die Existenz einer ganzen, nur von  $\mathbb{Z}_K$  abhängigen Zahl  $h_K$  nachweisen, sodaß die  $h_K$ -te Potenz eines beliebigen Ideals ein Hauptideal ist.

Eine vollständige Formulierung lautet wie folgt: sei  $\mathbb{Z}_K$  der Ring ganzer Zahlen in einem algebraischen Zahlkörper  $K$ . Man kann das Inverse eines Ideals in  $\mathbb{Z}_K$  als ein verallgemeinertes (*gebrochenes*) Ideal in  $K$  definieren, und zwar so, daß die Menge der von  $(0)$  verschiedenen gebrochenen Ideale  $I_K$  zusammen mit ihren Inversen eine abelsche Gruppe bezüglich der Idealmultiplikation erzeugen. Die gebrochenen Hauptideale bilden eine Untergruppe, und die Faktorgruppe  $\text{Cl}(K) = I_K/H_K$  heißt die Idealklassengruppe von  $\mathbb{Z}_K$ . Es stellt sich heraus, daß diese Faktorgruppe eine (abelsche) Gruppe *endlicher* Ordnung  $h_K$  ist. [Sa]

Leider kennt man diese Zahl  $h_K$  im allgemeinen nicht explizit; die explizite Kenntnis von  $h_K$  ist wichtig, wie schon die Arbeiten von Kummer über das

Fermatsche Problem zeigen.

Der Satz von Stickelberger gibt nun explizite Elemente  $S$ , sodaß für jedes Ideal  $I$  eines Kreisteilungskörpers  $\mathbb{Q}(\zeta_p)$  die Potenz  $I^S$  ein Hauptideal ist. Diese Elemente  $S$  sind aber keine Zahlen.

Wir haben oben gesehen, daß die Galoisgruppe  $G$  von  $\mathbb{Q}(\zeta_p)/\mathbb{Q}$  aus  $p-1$  Elementen  $\sigma_a$  ( $1 \leq a \leq p-1$ ) besteht, die dadurch charakterisiert sind, daß sie  $\zeta$  auf  $\zeta^a$  abbilden. Außerdem haben wir in Satz 2.2. festgestellt, daß diese Automorphismen Ideale in Ideale überführen.

Sei  $\sigma_a(I)$  das Ideal, welches man durch Anwendung von  $\sigma_a$  auf das Ideal  $I$  in  $\mathbb{Z}[\zeta_p]$  erhält. Wir betrachten nun die Menge aller Summen von Elementen aus  $G$  mit Koeffizienten aus  $\mathbb{Z}$  (bzw.  $\mathbb{Q}$ ), die wir mit  $\mathbb{Z}G$  (bzw.  $\mathbb{Q}G$ ) bezeichnen. Ein Element  $T$  von  $\mathbb{Z}G$  hat daher die Gestalt

$$T = t_1\sigma_1 + t_2\sigma_2 + \dots + t_{p-1}\sigma_{p-1}, \quad t_j \in \mathbb{Z}.$$

$\mathbb{Z}G$  und  $\mathbb{Q}G$  sind Ringe. Ist  $I$  ein Ideal in  $\mathbb{Z}[\zeta_p]$ , so definieren wir

$$I^T = \sigma_1(I^{t_1}) \cdot \dots \cdot \sigma_{p-1}(I^{t_{p-1}}).$$

Jetzt können wir den Satz von Stickelberger formulieren.

**Satz 3.1.** *Sei  $R \in \mathbb{Q}G$  definiert durch*

$$R = \frac{1}{p}(\sigma_1 + 2\sigma_2^{-1} + \dots + (p-1)\sigma_{p-1}^{-1}).$$

*Dann hat jedes Vielfache  $S$  von  $R$ , welches in  $\mathbb{Z}G$  liegt, die Eigenschaft, daß  $I^S$  für jedes Ideal  $I \neq (0)$  ein Hauptideal ist.*

Fenster mit Aussicht: Dieses Ergebnis kann als ein Satz betrachtet werden, der explizite Relationen in der Idealklassengruppe von  $\mathbb{Q}(\zeta_p)$  angibt. Er wurde auf beliebige abelsche Erweiterungen von  $\mathbb{Q}$  ausgedehnt und ist der Prototyp neuerer Resultate über Annihilatoren anderer Gruppen, wie z. B. projektive Klassengruppen von Gruppenalgebren, oder von  $K_2$ -Gruppen in der algebraischen  $K$ -Theorie.

## 3.2 Charaktere

Wer ein wenig mit der Gruppentheorie vertraut ist, weiß um die Bedeutung der Darstellungen einer Gruppe und ihrer dazugehörigen Charaktere.

Da wir der Einfachheit halber nur abelsche Gruppen behandeln, werden wir Charaktere auch nur für solche Gruppen definieren.

**Def. 3.2.1.** Sei  $G$  eine abelsche Gruppe. Ein Charakter  $\chi$  von  $G$  ist ein Homomorphismus von  $G$  in die multiplikative Gruppe  $\mathbb{C}^\times$  der komplexen Zahlen, also:

$$\chi : G \longrightarrow \mathbb{C}^\times, \quad \chi(gh) = \chi(g)\chi(h).$$

**Beispiel.** Das Legendre-Symbol. Sei  $p$  eine ungerade Primzahl. Die Reste bezüglich der Division durch  $p$  bilden einen Ring (sogar einen Körper, da  $p$  prim ist), der mit  $\mathbb{Z}/p\mathbb{Z}$  bezeichnet wird. Für  $p = 5$  sind die möglichen Reste  $0, 1, 2, 3, 4$ . Die Summe zweier Reste wird definiert als der Rest der Summe in  $\mathbb{N}$  bei Division durch  $p$ ; so gilt in  $\mathbb{Z}/5\mathbb{Z}$  z. B.  $2 + 4 = 1$ . Analog wird das Produkt definiert, und in  $\mathbb{Z}/5\mathbb{Z}$  hat man  $2 \cdot 3 = 1$ .

Ist ein  $x \neq 0$  in  $\mathbb{Z}/p\mathbb{Z}$  ein Quadrat in  $\mathbb{Z}/p\mathbb{Z}$ , so schreiben wir  $(x/p) = 1$ , und  $(x/p) = -1$  andernfalls. Dadurch ist ein Charakter  $(\cdot/p)$  mit Werten  $\pm 1$  auf der Gruppe  $U_p$  der invertierbaren (das sind hier alle von 0 verschiedenen) Elemente definiert. In der Tat gilt  $(xy/p) = (x/p)(y/p)$ . Dieser Charakter heißt Legendre-Symbol [Se].

Indem man jeder ganzen Zahl  $n$  ihren Rest  $r(n)$  bei Division durch  $p$  zuordnet, erhält man eine surjektive Abbildung  $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ . Auf diese Weise kann man jeder nicht durch  $p$  teilbaren Zahl den Wert  $-1$  oder  $+1$  zuordnen, indem man  $(n/p) := (r(n)/p)$  setzt.

Mit Hilfe des Legendre-Symbols können wir das Zerlegungsgesetz für quadratische Zahlkörper genauer formulieren. Ist z. B.  $d - 1$  ein Vielfaches von 4, so verzweigt eine Primzahl  $p$  (bzw. zerfällt oder ist träge), je nachdem  $p$  ein Teiler von  $d$  ist (bzw.  $(d/p) = +1$  oder  $(d/p) = -1$ ).

Sei nun  $m$  eine ganze Zahl und  $U_m$  die Gruppe der invertierbaren Elemente im Ring  $\mathbb{Z}/m\mathbb{Z}$  der Reste bei Division durch  $m$ . Ist  $m$  eine Primzahl  $p$ , so ist  $U_p$  eine zyklische Gruppe mit  $p - 1$  Elementen: daher existiert ein  $r \in U_p$ , sodaß  $U_p$  gleich der Menge aller Potenzen von  $r$  ist (Tatsächlich ist  $U_p$  die multiplikative Gruppe eines endlichen Körpers; der Leser möge als Übung Erzeugende  $r$  in den Fällen  $p = 3, 5, 7$  finden). Durch  $\chi(r) = \zeta$  wird ein Charakter  $\chi$  von  $U_p$  definiert.

Wir haben bereits erwähnt, daß man  $U_p$  mit der Galoisgruppe von  $\mathbb{Q}(\zeta_p)/\mathbb{Q}$  identifizieren kann. Allgemeiner ist die Gruppe  $U_m$  der Galoisgruppe von  $\mathbb{Q}(\zeta_m)/\mathbb{Q}$  isomorph. Ein tiefer Satz von Kronecker und Weber (1853/1886) besagt, daß jeder über  $\mathbb{Q}$  abelsche Zahlkörper Teilkörper eines Kreisteilungskörpers  $\mathbb{Q}(\zeta_m)$  ist. Genau aus diesem Grunde sind die Charaktere der Gruppen  $U_m$  für uns so wichtig.

**Beispiel.** Sei  $p$  eine ungerade Primzahl. Ist  $p - 1$  ein Vielfaches von 4, dann

ist  $\mathbb{Q}(\sqrt{p})$  in  $\mathbb{Q}(\zeta_p)$  enthalten; ist  $p + 1$  ein Vielfaches von 4, so ist  $\mathbb{Q}(\sqrt{p})$  in  $\mathbb{Q}(\zeta_{4p})$  enthalten.

Der Satz von Kronecker und Weber macht keine näheren Angaben über die Zahl  $m$ , deren Existenz er garantiert; mittels Charaktertheorie können wir bei gegebenem Körper  $K$  die kleinste natürliche Zahl  $f$  bestimmen, für die  $K$  in  $\mathbb{Q}(\zeta_f)$  enthalten ist; diese Zahl  $f$  heißt der *Führer* des Zahlkörpers und wird mit  $f_K$  bezeichnet. Ist  $m$  irgendeine Zahl mit  $K \subseteq \mathbb{Q}(\zeta_m)$ , so wissen wir dank Satz 2.1. daß  $G = \text{Gal}(K/\mathbb{Q})$  einer Faktorgruppe von  $U_m$  isomorph ist. Folglich können wir die Charaktere von  $G$  als Charaktere von  $U_m$  auffassen. Jedem Charakter  $\chi$  von  $U_m$  ordnen wir eine Zahl  $f_\chi$  zu, die Führer von  $\chi$  genannt wird.

Ist  $n$  ein Teiler von  $m$ , so gibt es eine Projektion  $\pi_{m,n}$  von  $U_m$  auf  $U_n$ . Es kann daher vorkommen, daß ein Charakter  $\chi$  von  $U_m$  über  $U_n$  faktorisiert, d.h. daß es einen Charakter  $\psi$  von  $U_n$  gibt, sodaß  $\chi$  die Komposition  $\psi \circ \pi_{m,n}$  ist. Die kleinste Zahl  $n$ , für die  $\chi$  über  $U_n$  faktorisiert, wird der Führer  $f_\chi$  des Charakters  $\chi$  genannt.

**Satz 3.2.** *Der Führer  $f_K$  eines abelschen Zahlkörpers ist das kleinste gemeinsame Vielfache der Führer  $f_\chi$ , wo  $\chi$  die Charaktere von  $\text{Gal}(K/\mathbb{Q})$  durchläuft.*

Die Führer von Charakteren liefern so eine Faktorisierung der Diskriminante eines abelschen Zahlkörpers  $K$ : es gilt  $d_K = \prod_\chi \chi(-1) f_\chi$ , wo das Produkt sich über alle Charaktere der Galoisgruppe von  $K$  erstreckt (sh. z.B. [Ha], Sätze 16 und 17, oder [Wa], S. 27 und 36).

### 3.3 Gaußsche Summen

Um zu beweisen, daß es möglich ist, mit Zirkel und Lineal ein regelmäßiges 17-Eck zu konstruieren, hat Gauß gewisse Summen von Einheitswurzeln eingeführt, die sich in einer leicht modifizierten Form als unglaublich nützlich erwiesen haben. Verwandt mit diesen Summen sind die Lagrangeschen Resolventen, die dieser benutzt hatte, um die Auflösung der Gleichungen vierten Grades zu erklären.

Es gibt *Gaußsche Summen* zu jedem Charakter  $\chi$  von  $U_f$ ,  $f$  prim: man setzt nämlich

$$\tau(\chi) = \sum_{a=1}^{f-1} \chi(a) \exp\left(\frac{2a\pi i}{f}\right).$$

Wir wollen eine kleine Anwendung Gaußscher Summen auf die Zahlentheorie geben. Sei  $f = p$  eine ungerade Primzahl und  $\chi$  der durch das Legendresymbol definierte Charakter von  $U_p$ ; in diesem Fall ist die Summe  $\tau$  von Gauß in seinem sechsten (!) Beweis des quadratischen Reziprozitätsgesetzes verwendet worden. Dieses Gesetz besagt, daß für zwei verschiedene ungerade Primzahlen immer  $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$  gilt. Der Leser ist eingeladen, diese Gleichung direkt aus der Definition des Legendresymbols herzuleiten: er wird sich wundern! Ist beispielsweise 4 ein Teiler von  $p - 1$ , so ist  $p$  genau dann ein Quadrat in  $\mathbb{Z}/q\mathbb{Z}$ , wenn  $q$  ein Quadrat in  $\mathbb{Z}/p\mathbb{Z}$  ist.

Hier nun der Beweis des quadratischen Reziprozitätsgesetzes: sei also  $\tau = \sum_a (a/p) \exp(2a\pi i/p)$ . Dann ist  $\tau^2 = (-1)^{(p-1)/2} p$  und daher

$$\tau^{q-1} = (\tau^2)^{(q-1)/2} = (-1)^{(p-1)(q-1)/4} p^{(q-1)/2},$$

sowie  $p^{(q-1)/2} = (p/q)$  in  $\mathbb{Z}/q\mathbb{Z}$ . Andererseits folgt aus der Binomialentwicklung von  $\tau^q$ , daß  $\tau^q = (q/p)\tau$  in  $\mathbb{Z}/q\mathbb{Z}$  gilt. Daraus folgt dann die Behauptung (für Details sh. [L1], IV.4).

Die Gaußschen Summen sind wichtig, weil sie in der Funktionalgleichung der  $L$ -Funktionen auftreten.

## 3.4 L-Funktionen

Ein erstaunliches Phänomen in der algebraischen Zahlentheorie ist die Verwendung analytischer Methoden, um algebraische Information zu erhalten. Das klassische Beispiel hierfür ist der Gebrauch der  $L$ -Funktionen zu einem Charakter  $\chi$  von  $U_f$ .

Sei  $\chi$  ein Charakter von  $U_f$  mit Führer  $f_\chi = f$ . Die  $L$ -Funktion zu  $\chi$  ist die Funktion einer komplexen Veränderlichen, die für alle komplexen  $s$  mit positivem Realteil durch  $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$  definiert ist.

### 3.4.1 Analytische Bestimmung der Klassenzahl

Hier geht es um eine Formel, die die Berechnung der Klassenzahl eines abelschen Zahlkörpers aus dem Wert an der Stelle  $s = 1$  derjenigen  $L$ -Funktionen erlaubt, die zu den Charakteren der Galoisgruppe von  $K/\mathbb{Q}$  gehören.

Sei also  $K$  ein abelscher Zahlkörper mit Klassenzahl  $h_K$ . Dann existiert

eine Konstante  $C$  (die von  $K$  abhängt und leicht berechnet werden kann) mit

$$hR = C \prod_{\chi} L(1, \chi),$$

wo  $\chi$  über alle Charaktere der Galoisgruppe  $\text{Gal}(K/\mathbb{Q})$  läuft, die nicht nur den Wert 1 annehmen, und wo  $R$  eine reelle Zahl ist, die man ausrechnen kann, wenn man eine explizite Basis für die invertierbaren Elemente in  $\mathbb{Z}_K$  besitzt.

Leider ist es nicht immer möglich, eine solche Basis zu finden, um  $R$  zu bestimmen. Es ist daher nicht nur eine Frage des Prinzips, weshalb man nach einer *algebraischen* Methode zur Berechnung der Klassenzahl sucht. Der Satz von Stickelberger ist ein Schritt in diese Richtung.

### 3.4.2 Funktionalgleichung der $L$ -Funktionen

Multipliziert man die Funktion  $L(s, \chi)$  mit einer geschickt gewählten (und nur vom Charakter  $\chi$  abhängigen) Funktion, so erhält man eine Funktion  $\Lambda(s, \chi)$ , welche der *Funktionalgleichung*

$$\Lambda(s, \chi) = W_{\chi} \Lambda(1 - s, \bar{\chi}) \quad (3.1)$$

genügt, wo  $\bar{\chi}$  der konjugiert-komplexe Charakter zu  $\chi$  ist, und wo  $W_{\chi}$  eine durch die Gleichung

$$W_{\chi} = \tau(\chi) f_{\chi}^{-\delta/2} \quad (3.2)$$

definierte komplexe Zahl vom Betrag 1 ist. Weiter ist  $\delta = 0$  oder  $= 1$ , in Abhängigkeit von  $\chi$ .

Die Funktionalgleichung (3.1) ist grundlegend für viele Beziehungen zwischen den Relationen unter den Invarianten von  $K$ ; außerdem kommt sie wegen (3.2) im Studium der Gaußschen Summen vor.

Wir werden sehen, daß die Konstante  $W_{\chi}$  in der Theorie der Galoismoduln wieder auftaucht.

# Kapitel 4

## Galoismoduln

In diesem Kapitel werden wir zur Besprechung jüngerer Resultate übergehen. Aus diesem Grunde läßt es sich nicht vermeiden, einige etwas fortgeschrittene Konzepte zu verwenden.

### 4.1 Normalbasen

Es ist ein Resultat von Deuring, daß jeder über  $\mathbb{Q}$  normale Zahlkörper ein Element  $\alpha$  enthält mit der Eigenschaft, daß die Menge aller  $\sigma(\alpha)$ , wo  $\sigma$  die Gruppe  $\text{Gal}(K/\mathbb{Q})$  durchläuft, eine  $\mathbb{Q}$ -Basis von  $K$  bildet. Eine solche Basis nennt man eine *Normalbasis* von  $K/\mathbb{Q}$ . Jetzt stellt sich ein analoges Problem für den Ganzheitsring  $\mathbb{Z}_K$  eines Zahlkörpers  $K$ :

**Problem.** Sei  $K$  ein Zahlkörper, galoisch über  $\mathbb{Q}$ . Existiert ein Element  $\beta \in \mathbb{Z}_K$  mit der Eigenschaft, daß die Menge der  $\sigma(\beta)$ , wo  $\sigma$  die Galoisgruppe von  $K/\mathbb{Q}$  durchläuft, eine  $\mathbb{Z}$ -Basis von  $\mathbb{Z}_K$  bildet? Wenn es ein solches  $\beta$  gibt, so nennt man  $\{\sigma(\beta) \mid \sigma \in \text{Gal}(K/\mathbb{Q})\}$  eine Normalbasis von  $K/\mathbb{Q}$ .

Eine Antwort auf diese Frage zu geben bedeutet, die Struktur des Ringes  $\mathbb{Z}_K$  als Modul der Gruppenalgebra  $\mathbb{Z}[\text{Gal}(K/\mathbb{Q})]$  zu untersuchen, also kurz,  $\mathbb{Z}_K$  als Galoismodul zu betrachten.

**Beispiel 4.1.** Falls  $d \equiv 1 \pmod{4}$  ist, so ist der Ganzheitsring  $\mathbb{Z}_K$  von  $K = \mathbb{Q}(\sqrt{d})$  gegeben durch  $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ . Die Galoisgruppe von  $K/\mathbb{Q}$  enthält die Identität und die Transformation  $\sigma$ , welche  $\sqrt{d}$  auf  $-\sqrt{d}$  abbildet. Man prüft nach, daß  $\beta = \frac{1+\sqrt{d}}{2}$  und  $\sigma(\beta) = \frac{1-\sqrt{d}}{2}$  eine Normalbasis bilden.

**Beispiel 4.2.** Sei  $p$  eine Primzahl. Der Ring ganzer Zahlen in  $K = \mathbb{Q}(\zeta_p)$  ist

$\mathbb{Z}[\zeta_p]$ . Die Menge  $\{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$  bildet eine Normalbasis von  $\mathbb{Z}_K$ .

Hilbert ([Hi], Satz 136) hat gezeigt, daß die Existenz einer Normalbasis eines Zahlkörpers  $K/\mathbb{Q}$ , dessen Galoisgruppe zyklisch der Ordnung  $p$  ist, und in dem  $p$  nicht verzweigt, zum Satz von Stickelberger in  $\mathbb{Q}(\zeta_p)$  äquivalent ist. Indem er diese Äquivalenz ausnutzte, konnte Hilbert den Satz von Stickelberger beweisen, indem er für jeden Körper  $K$  mit obigen Eigenschaften eine Normalbasis konstruierte.

Allgemeiner hat Hilbert eine Normalbasis für jede abelsche Erweiterung konstruiert, welche folgende Eigenschaft hat:

(H) Die Primteiler von  $(K : \mathbb{Q})$  sind in  $K/\mathbb{Q}$  nicht verzweigt.

Hilberts Idee war, den Satz von Kronecker und Weber zu benutzen, um das Problem auf den kleinsten Kreisteilungskörper  $\mathbb{Q}(\zeta_f)$  zurückzuführen, welcher  $K$  umfaßt. Wenn  $K$  der Bedingung (H) genügt, so ist  $\mathbb{Q}(\zeta_f)$  Kompositum von Kreisteilungskörpern mit Normalbasis; daher hat auch  $\mathbb{Q}(\zeta_f)$  eine solche. Durch Bildung der Spur erhält man schließlich aus der Normalbasis von  $\mathbb{Q}(\zeta_f)$  eine solche von  $K$ .

Speiser hat bemerkt, daß die Bedingung (H) nicht notwendig für die Existenz einer Normalbasis ist und hat eine solche notwendige Bedingung angegebene. Er hat nämlich gezeigt, daß eine Normalbasis von  $K/\mathbb{Q}$  nur dann existiert, wenn gilt:

(S) Der Verzweigungsindex (sh. Abschnitt 1.7) einer Primzahl  $p$  ist nicht durch  $p$  teilbar.

Diese notwendige Bedingung an die Verzweigung zeigt, daß nicht alle Zahlkörper eine Normalbasis besitzen. Beispielsweise hat  $\mathbb{Q}(\sqrt{-5})$  keine.

Speiser hat darüberhinaus gezeigt – unter Verwendung der Hilbertschen Methoden – daß jeder über  $\mathbb{Q}$  abelsche Körper  $K$ , der (S) genügt, eine Normalbasis besitzt.

E. Noether hat dieses Problem wieder aufgegriffen und die Bedingung (S) 1932 neu interpretiert. Sie zeigte, daß (S) äquivalent ist zur Existenz einer lokalen Normalbasis für jede Primzahl  $p$ . Dies bedeutet, daß für jede rationale Primzahl  $p$  und jedes Primideal  $\mathfrak{p}$ , welches  $p$  in  $K$  teilt, die lokale Erweiterung  $K_{\mathfrak{p}}$  des Körpers  $\mathbb{Q}_p$  der  $p$ -adischen Zahlen (mit  $K/\mathbb{Q}$  ist auch immer  $K_{\mathfrak{p}}/\mathbb{Q}_p$  galoissch) eine Normalbasis besitzt.

**Bemerkung.** Die Bedingung (S) ist auch gleichbedeutend damit, daß  $\mathbb{Z}_K$  ein projektiver  $\mathbb{Z}\text{Gal}(K/\mathbb{Q})$ -Modul ist.

Man mußte bis zum Jahre 1968 auf ein Beispiel einer Galoiserweiterung  $K/\mathbb{Q}$  warten, für welche die Bedingung (S) nicht hinreichend für die Existenz einer Normalbasis von  $K$  ist. In diesem Beispiel – konstruiert von J. Martinet – ist die Galoisgruppe von  $K/\mathbb{Q}$  isomorph zur Quaternionengruppe der Ordnung 8.

Mit anderen Worten zeigt das Beispiel von Martinet, daß die Existenz einer lokalen Normalbasis für jedes  $p$  nicht die Existenz einer globalen Normalbasis für  $K$  nach sich zieht. Diese Formulierung ist typisches Merkmal einer Methode, die darin besteht, ein Problem über einem Zahlkörper  $K$  (den man einen globalen Körper nennt) auf zwei andere Probleme zurückzuführen: der eine ist das analoge Problem über den  $p$ -adischen Körpern, die zu  $K$  assoziiert sind (und die lokale Körper heißen), das andere besteht darin, die 'lokalen Lösungen' zu einer 'globalen Lösung' zusammenzusetzen. Diese Sprache rührt von einer Analogie her, die zwischen der Zahlentheorie und der algebraischen Geometrie besteht.

Nach 1968 haben sich die Forschungen auf diesem Gebiet darauf konzentriert, hinreichende Bedingungen für die Existenz einer Normalbasis in solchen Körpern  $K$  zu formulieren, die der Bedingung (S) genügen. Es waren diese Forschungen, die schließlich Unerwartetes ans Licht gebracht haben.

## 4.2 Das mysteriöse Band

Sei  $p$  eine ungerade Primzahl. Wir betrachten einen galoisschen Zahlkörper  $K$  vom Grad  $p$  über  $\mathbb{Q}$ , in welchem  $p$  nicht verzweigt (insbesondere genügt  $K$  der Bedingung (S)). Wir wissen, daß  $K/\mathbb{Q}$  eine Normalbasis besitzt. Wenn wir von der Äquivalenz von Hilbert (sh. oben) Gebrauch machen, können wir dies auch dadurch beweisen, daß wir die Gültigkeit des Satzes von Stickelberger nachweisen. Wenn wir untersuchen, wie Stickelberger seinen Satz bewiesen hat, so finden wir, daß er die Zerlegung einer Gaußschen Summe benutzt hat. Wir halten fest

**Tatsache 1.** Die Gaußsche Summe sollte in der Bestimmung der Normalbasis auftauchen.

Wo?

Man stellt fest, daß die von Hilbert gefundene Äquivalenz die Galoiserweiterungen vom Grad  $p$  über  $\mathbb{Q}$  mit dem Kreisteilungskörper  $\mathbb{Q}(\zeta_p)$  verbindet und auf der Konstruktion einer Abbildung beruht, die mit Hilfe von Charakteren der Galoisgruppe definiert wird.

**Tatsache 2.** Es scheint, daß man Charaktere der Galoisgruppe dazu verwenden kann, die Hilbertsche Äquivalenz auf Körper zu verallgemeinern, die nicht notwendig abelsch sind.

Wie?

**Tatsache 3.** Das Auftreten der Quaternionengruppe in Martinet's Gegenbeispiel gibt zu der Vermutung Anlaß, daß die sogenannten *symplektischen Charaktere* eine spezielle Rolle spielen.

Wer? Es war A. Fröhlich, der einen großen Teil dazu beigetragen hat, die Lage aufzuklären, und der die wirklich wichtigen Elemente für einen eventuellen Beweis eines allgemeinen Satzes isoliert hat (Dem Leser sei die Lektüre der Einführung von [Fr] nahegelegt, wo Fröhlich auf unterhaltsame Weise die Entwicklung seiner Entdeckungen beschreibt). Unter diesen Elementen kommen – O Wunder – auch die Konstanten  $W_\chi$  vor ...

Der folgende Satz wurde von Fröhlich 1976 vermutet und 1981 in größter Allgemeinheit von seinem Schüler M. J. Taylor bewiesen. Die Konstanten  $W_\chi$ , die im Satz auftauchen, hängen mit den Artinschen  $L$ -Funktionen zusammen, welche die  $L$ -Funktionen aus 3.4 verallgemeinern. Diese wiederum haben etwas mit den Charakteren einer – nicht notwendig abelschen – Galoisgruppe zu tun. Man kann zeigen, daß auch diese  $L$ -Funktionen einer Funktionalgleichung genügen.

**Satz 4.1.** *Sei  $K/\mathbb{Q}$  eine Galoiserweiterung, die der Bedingung (S) genügt. Damit  $K/\mathbb{Q}$  eine Normalbasis besitzt, genügt es, daß die Konstanten  $W_\chi$ , die in der Funktionalgleichung der zu den irreduziblen symplektischen Charakteren  $\chi$  von  $\text{Gal}(K/\mathbb{Q})$  gehörigen Artinschen  $L$ -Funktionen auftauchen, positives Vorzeichen haben.*

Ist  $K/\mathbb{Q}$  insbesondere abelsch, so erhalten wir den Satz von Hilbert-Speiser zurück, da abelsche Gruppen keine symplektischen Charaktere besitzen und folglich keine Bedingung zu erfüllen ist! So wird der Satz von Hilbert-Speiser heute formuliert.

### 4.3 Andere Resultate

Die Theorie der Galoismoduln wurde im wesentlichen in den letzten 20 Jahren entwickelt, und ihre Hauptergebnisse sind in Fröhlich's Buch [Fr] enthalten. Die größte Lücke in diesem Buch betrifft die Ergebnisse, die ihren Ursprung

in den Arbeiten von Leopoldt [Le] haben; allerdings kann man diese ebenfalls in der Bibliographie in [Fr] finden.

# Literaturverzeichnis

- [Fr] A. Fröhlich, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik(3) **1**, Springer 1983 23, 24
- [Ha] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Physica 1965 17
- [He] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Math. **77**, Springer 1981 6, 7
- [Hi] D. Hilbert *Die Theorie der algebraischen Zahlkörper*, Gesammelte Abh. **I**, 63–363, Springer Verlag 1970 21
- [IR] K. Ireland, M. Rosen, *A Classical introduction to modern number theory*, Graduate Texts in Math. **84**, Springer 1972 4, 7
- [L1] S. Lang, *Algebraic number theory*, Graduate Texts in Math. **110**, Springer 1986 18
- [L2] S. Lang, *Algebra*, Addison-Wesley 1971 5, 7, 11, 12
- [Le] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149 24
- [Sa] P. Samuel, *Théorie algébrique des Nombres*, 2ème Ed., Hermann, Paris 1971 6, 7, 14
- [Se] J.-P. Serre, *Cours d'Arithmétique*, Presse Univ. France, Paris, 1970 16
- [Wa] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer 1979 10, 17

- [W1] A. Weil, *Introduction to 'Collected Papers by E. E. Kummer'* Œuvres Scientifiques, vol. III, Springer 1979 7
- [W2] A. Weil, *La cyclotomie jadis et naguère*, Œuvres Scientifiques, vol. III, Springer 1979 6

Dem Original nachempfunden (übersetzt wage ich nicht zu sagen) von Franz Lemmermeyer