

## Algebraische Zahlentheorie

### Vorlesung 6

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.

### 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

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

wobei die Koeffizienten  $r_i$ ,  $i = 0, \dots, n-1$ , 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  $\mathbb{Z} \subseteq \mathbb{Z}[i]$  ist  $i$  ganz über  $\mathbb{Z}$ , wie die Ganzheitsgleichung

$$i^2 = -1$$

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

$$(a + bi)^2 - 2a(a + bi) + a^2 + b^2 = 0.$$

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  $R$ -Untermodule  $M$  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

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

ergibt sich

$$x^n = -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \cdots - r_1x - r_0.$$

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  $x^0 = 1, x^1, x^2, \dots, x^{n-1}$  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  $y_1, \dots, y_n$  erzeugende Elemente von  $M$ . Dann ist insbesondere  $xy_i$  für jedes  $i$  eine  $R$ -Linearkombination der  $y_j$ ,  $j = 1, \dots, n$ . Dies bedeutet

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

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

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

Dies schreiben wir als

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

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

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

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.  $\square$

**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  $y_1, \dots, y_n$  ein  $R$ -Erzeugendensystem von  $T_1$  und  $z_1, \dots, z_m$  ein  $R$ -Erzeugendensystem von  $T_2$ . Wir können annehmen, dass  $y_1 = z_1 = 1$  ist. Betrachte den endlich erzeugten  $R$ -Modul

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

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

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

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.  $\square$

## 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

$$q^n + r_{n-1}q^{n-1} + r_{n-2}q^{n-2} + \dots + r_1q + r_0 = 0$$

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  $R$

$$a^n + (r_{n-1}b)a^{n-1} + (r_{n-2}b^2)a^{n-2} + \cdots + (r_1b^{n-1})a + (r_0b^n) = 0.$$

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.  $\square$

**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.  $\square$

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  $\alpha_i$  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.  $\square$

**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.  $\square$

### 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

$$f^n + q_{n-1}f^{n-1} + \cdots + q_1f + q_0 = 0$$

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

$$(rf)^n + q_{n-1}r(rf)^{n-1} + \cdots + q_1r^{n-1}(rf) + q_0r^n = 0.$$

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.  $\square$

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.

## Abbildungsverzeichnis

- Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von <http://commons.wikimedia.org>) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren Dateinamen auf Commons angeführt zusammen mit ihrem Autor bzw. Hochlader und der Lizenz. 7
- Lizenzklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 7