Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Vorlesung 16

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

$$\mathbb{Z}_{(3)}/((ab^2)^3 - ab^2) = \mathbb{Z}_{(3)}/((ab^2)^2 - 1)$$

$$= \mathbb{Z}_{(3)}/((ab^2+1)(ab^2-1)),$$

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 $\operatorname{Spur}(z) = 1$, $\frac{1}{9}(3-3aab^2) = \frac{1}{3}(1-a^2b^2)$ 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

$$1-a^2b^2 = \begin{cases} 0 \text{ bei } t=1\,, \\ -15 \text{ bei } t=4\,, \\ -48 \text{ bei } t=7 \end{cases} \mod 9,$$

also stets ein Vielfaches von 3. Ferner ist

$$\begin{aligned} & 1+a^2b^2(a^2+b^2-3) \\ = \;& 1+\big(81mn+9(m+n)r+r^2\big)\big(9(m+n)+2r-3\big) \end{aligned}$$

$$\begin{aligned} &= 1 + 81A + 18(m+n)r^2 - 27(m+n)r + 9(m+n)r^2 + 2r^3 - 3r^2 \\ &= 81A + 1 + 27(m+n)r^2 - 27(m+n)r + 2r^3 - 3r^2 \\ &= 81A + 1 + 27(m+n)(r^2 - r) + 2r^3 - 3r^2 \\ &= 81A' + 1 + 2r^3 - 3r^2. \end{aligned}$$

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

$$\operatorname{ord}_{(3)}(mn) \geq -1,$$

also $\operatorname{ord}_{(3)}(m) \geq 0$ oder $\operatorname{ord}_{(3)}(n) \geq 0$, und

$$\operatorname{ord}_{(3)}(m^3 + n^3q) \geq 0.$$

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 $\frac{1}{9}$. □

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. 9

Lizenzerklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 9