Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 5

Es bestehen viele und weitreichende Parallelen zwischen dem Ring $\mathbb{Z}$ der ganzen Zahlen und einem Polynomring in einer Variablen über einem Körper. Grundlegend ist, dass man in beiden Situation eine *Division mit Rest* durchführen kann.

Division mit Rest in $\mathbb{Z}$

Zu einer ganzen Zahl d ist die Menge

$$\mathbb{Z}d = \{kd | \, k \in \mathbb{Z}\}$$

aller Vielfachen von d eine Untergruppe von $\mathbb{Z}$. Wir wollen zeigen, dass jede Untergruppe der ganzen Zahlen $\mathbb{Z}$ diese Gestalt besitzt, also von einem Element erzeugt wird.

Satz 5.1. *Sei d eine fixierte positive natürliche Zahl. Dann gibt es zu jeder ganzen Zahl n eine eindeutig bestimmte ganze Zahl q und eine eindeutig bestimmte natürliche Zahl r, $0 \leq r \leq d-1$, mit*

$$n = qd + r \, .$$

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

In der Notation des vorstehenden Satzes soll q an *Quotient* und r an *Rest* erinnern. Die Division mit Rest kann man auch so verstehen, dass man jede rationale Zahl n/d als

$$\frac{n}{d} = \lfloor \frac{n}{d} \rfloor + \frac{r}{d}$$

schreiben kann, wobei $\lfloor s \rfloor$ die größte ganze Zahl $\leq s$ bedeutet und der rationale Rest r/d die Bedingungen $0 \leq r/d < 1$ erfüllt. In dieser Form kann man auch eine Division mit Rest für jede reelle Zahl aus den Axiomen der reellen Zahlen beweisen.

Satz 5.2. *Die Untergruppen von $\mathbb{Z}$ sind genau die Teilmengen der Form*

$$\mathbb{Z}d = \{kd | \, k \in \mathbb{Z}\}$$

mit einer eindeutig bestimmten nicht-negativen Zahl d.

Beweis. Eine Teilmenge der Form $\mathbb{Z}d$ ist aufgrund der Distributivgesetze eine Untergruppe. Sei umgekehrt $H \subseteq \mathbb{Z}$ eine Untergruppe. Bei $H = 0$ kann man $d = 0$ nehmen, so dass wir voraussetzen dürfen, dass H neben 0 noch mindestens ein weiteres Element x enthält. Wenn x negativ ist, so muss die

Untergruppe H auch das Negative davon, also $-x$ enthalten, welches positiv ist. D.h. H enthält auch positive Zahlen. Sei nun d die kleinste positive Zahl aus H. Wir behaupten $H = \mathbb{Z}d$. Dabei ist die Inklusion $\mathbb{Z}d \subseteq H$ klar, da mit d alle (positiven und negativen) Vielfache von d dazugehören müssen. Für die umgekehrte Inklusion sei $h \in H$ beliebig. Nach Satz 5.1 gilt

$$h = qd + r \text{ mit } 0 \leq r < d\,.$$

Wegen $h \in H$ und $qd \in H$ ist auch $r = h - qd \in H$. Nach der Wahl von d muss wegen $r < d$ gelten: $r = 0$. Dies bedeutet $h = qd$ und damit $h \in \mathbb{Z}d$, also $H \subseteq \mathbb{Z}d$. □

Division mit Rest in $K[X]$

Satz 5.3. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es seien $P, T \in K[X]$ zwei Polynome mit $T \neq 0$. Dann gibt es eindeutig bestimmte Polynome $Q, R \in K[X]$ mit*

$$P = TQ + R \text{ und mit } \operatorname{grad}(R) < \operatorname{grad}(T) \text{ oder } R = 0\,.$$

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

Die Berechnung der Polynome Q und R heißt *Polynomdivision*. Wir geben dazu ein Beispiel über den komplexen Zahlen.

Beispiel 5.4. Wir führen die Polynomdivision

$$P = 6X^3 + X + 1 \text{ durch } T = 3X^2 + 2X - 4$$

durch. Es wird also ein Polynom vom Grad 3 durch ein Polynom vom Grad 2 dividiert, d.h. dass der Quotient und auch der Rest (maximal) vom Grad 1 sind. Im ersten Schritt überlegt man, mit welchem Term man T multiplizieren muss, damit das Produkt mit P im Leitterm übereinstimmt. Das ist offenbar $2X$. Das Produkt ist

$$2X\left(3X^2 + 2X - 4\right) = 6X^3 + 4X^2 - 8X.$$

Die Differenz von P zu diesem Produkt ist

$$6X^3 + X + 1 - \left(6X^3 + 4X^2 - 8X\right) = -4X^2 + 9X + 1.$$

Mit diesem Polynom, nennen wir es P', setzen wir die Division durch T fort. Um Übereinstimmung im Leitkoeffizienten zu erhalten, muss man T mit $\frac{-4}{3}$ multiplizieren. Dies ergibt

$$-\frac{4}{3}T = -\frac{4}{3}\left(3X^2 + 2X - 4\right) = -4X^2 - \frac{8}{3}X + \frac{16}{3}.$$

Die Differenz zu P' ist somit

$$-4X^2 + 9X + 1 - \left(-4X^2 - \frac{8}{3}X + \frac{16}{3}\right) = \frac{35}{3}X - \frac{13}{3}.$$

Dies ist das Restpolynom und somit ist insgesamt

$$6X^3+X+1 \;=\; \left(3X^2+2X-4\right)\left(2X-\frac{4}{3}\right)+\frac{35}{3}X-\frac{13}{3}.$$

LEMMA 5.5. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom und $a \in K$. Dann ist a genau dann eine Nullstelle von P, wenn P ein Vielfaches des linearen Polynoms $X-a$ ist.*

Beweis. Wenn P ein Vielfaches von $X-a$ ist, so kann man

$$P=(X-a)Q$$

mit einem weiteren Polynom Q schreiben. Einsetzen ergibt

$$P(a)=(a-a)Q(a)=0\,.$$

Im Allgemeinen gibt es aufgrund der Division mit Rest eine Darstellung

$$P=(X-a)Q+R\,,$$

wobei $R=0$ oder aber den Grad null besitzt, also eine Konstante ist. Einsetzen ergibt

$$P(a)=R\,.$$

Wenn also $P(a)=0$ ist, so muss der Rest $R=0$ sein, und das bedeutet, dass $P=(X-a)Q$ ist. □

KOROLLAR 5.6. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom ($\neq 0$) vom Grad d. Dann besitzt P maximal d Nullstellen.*

Beweis. Wir beweisen die Aussage durch Induktion über d. Für $d=0,1$ ist die Aussage offensichtlich richtig. Sei also $d \geq 2$ und die Aussage sei für kleinere Grade bereits bewiesen. Sei a eine Nullstelle von P. Dann ist $P=Q(X-a)$ nach Lemma 5.5 und Q hat den Grad $d-1$, so dass wir auf Q die Induktionsvoraussetzung anwenden können. Das Polynom Q hat also maximal $d-1$ Nullstellen. Für $b \in K$ gilt $P(b)=Q(b)(b-a)$. Dies kann nur dann 0 sein, wenn einer der Faktoren 0 ist, so dass eine Nullstelle von P gleich a ist oder aber eine Nullstelle von Q ist. Es gibt also maximal d Nullstellen von P. □

KOROLLAR 5.7. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Dann besitzt jedes $P \in K[X]$, $P \neq 0$, eine Produktzerlegung*

$$P=(X-\lambda_1)^{\mu_1}\cdots(X-\lambda_k)^{\mu_k}\cdot Q$$

mit $\mu_j \geq 1$ und einem nullstellenfreien Polynom Q. Dabei sind die auftretenden verschiedenen Zahlen $\lambda_1,\ldots,\lambda_k$ und die zugehörigen Exponenten $\mu_1,\ldots,\mu_k$ (bis auf die Reihenfolge) eindeutig bestimmt.

Beweis. Siehe Aufgabe 5.8. □

Es gilt allgemeiner, dass die Zerlegung eines Polynoms in irreduzible Faktoren im Wesentlichen eindeutig ist. Das werden wir später behandeln.

Der Fundamentalsatz der Algebra

Es gilt der folgende *Fundamentalsatz der Algebra*, den wir hier ohne Beweis erwähnen.

Satz 5.8. *Jedes nichtkonstante Polynom $P \in \mathbb{C}[X]$ über den komplexen Zahlen besitzt eine Nullstelle.*

Aus dem Fundamentalsatz der Algebra folgt, dass jedes von 0 verschiedene Polynom $P \in \mathbb{C}[X]$ in Linearfaktoren zerfällt, d.h. man kann schreiben

$$P = c(X - z_1)(X - z_2) \cdot (X - z_n)$$

mit eindeutig bestimmten komplexen Zahlen $z_1, \ldots, z_n$ (wobei Wiederholungen erlaubt sind).

Euklidische Bereiche

Ringe, in denen man eine Division mit Rest sinnvoll durchführen kann, bekommen einen eigenen Namen.

Definition 5.9. Ein *euklidischer Bereich* (oder *euklidischer Ring*) ist ein Integritätsbereich R, für den eine Abbildung $\delta : R \setminus \{0\} \to \mathbb{N}$ existiert, die die folgende Eigenschaft erfüllt:

Für Elemente a, b mit $b \neq 0$ gibt es $q, r \in R$ mit

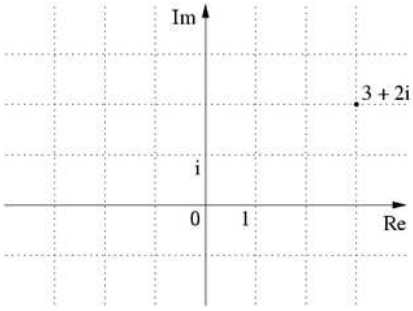
$$a = qb + r \text{ und } r = 0 \text{ oder } \delta(r) < \delta(b)\,.$$

Die in der Definition auftauchende Abbildung δ nennt man auch *euklidische Funktion*. Die ganzen Zahlen $\mathbb{Z}$ bilden also einen euklidischen Ring mit dem Betrag als euklidischer Funktion.

Beispiel 5.10. Für einen Körper K ist der Polynomring $K[X]$ in einer Variablen ein euklidischer Bereich, wobei die euklidische Funktion δ durch die Gradfunktion gegeben ist. Viele Parallelen zwischen dem Polynomring $K[X]$ und $\mathbb{Z}$ beruhen auf dieser Eigenschaft. Die Gradfunktion hat die Eigenschaft

$$\delta(fg) = \delta(f) + \delta(g)\,.$$

Beispiel 5.11. Eine Gaußsche Zahl z ist durch $z = a + b\mathrm{i}$ gegeben, wobei a und b ganze Zahlen sind. Die Menge dieser Zahlen wird mit $\mathbb{Z}[\mathrm{i}]$ bezeichnet. Die Gaußschen Zahlen sind die Gitterpunkte, d.h. die Punkte mit ganzzahligen Koordinaten, in der komplexen Ebene. Sie bilden mit komponentenweiser Addition und mit der induzierten komplexen Multiplikation einen kommutativen Ring.



Gaußsche Zahlen als Gitterpunkte in der komplexen Zahlenebene

Eine euklidische Funktion ist durch die Norm N gegeben, die durch $N(a + b\mathrm{i}) := a^2 + b^2$ definiert ist. Man kann auch schreiben $N(z) = z \cdot \bar{z}$, wobei $\bar{z}$ die komplexe Konjugation bezeichnet. Die Norm ist das Quadrat des komplexen Absolutbetrages und wie dieser multiplikativ, also $N(zw) = N(z)N(w)$.

Mit der Norm lassen sich auch leicht die Einheiten von $\mathbb{Z}[\mathrm{i}]$ bestimmen: ist $wz = 1$, so ist auch $N(zw) = N(z)N(w) = 1$, also $N(z) = 1$. Damit sind genau die Elemente $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ diejenigen Gaußschen Zahlen, die Einheiten sind.

LEMMA 5.12. *Der Ring der Gaußschen Zahlen ist mit der Normfunktion ein euklidischer Bereich.*

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □

Abbildungsverzeichnis