Algebraische Zahlentheorie

Wir beschäftigen uns vor allem mit den ganzen algebraischen Zahlen. Dabei schränken wir uns folgendermaßen ein: Gegeben sei ein Körper K der Charakteristik 0, also ein Körper, der $\mathbb{Q}$ als Unterkörper enthält, und der als $\mathbb{Q}$-Vektorraum endliche Dimension besitzt (es ist also $K\colon \mathbb{Q}$ eine endliche Körper-Erweiterung), man nennt einen solchen Körper K einen *Zahlkörper.* Für einige allgemeine Begriffsbildungen werden wir davon ausgehen, dass ein Unterring R eines Körpers Ω gegeben ist (R ist notwendigerweise kommutativ und nullteilerfrei, also ein *Bereich*).

Teil I. Grundlagen

Das Hauptziel von Teil I ist folgender Satz:

Satz. (a) *Ist K ein Zahlkörper, so ist der Ring $\mathcal{O}_K$ der ganzen Zahlen in K ein Dedekind-Ring.* (b) *In einem Dedekind-Ring lässt sich jedes von Null verschiedene Ideal eindeutig als Produkt von maximalen Idealen schreiben.*

Einzuführen ist, was man unter "ganzen Zahlen" in K versteht. Zu zeigen ist, dass die Menge der ganzen Zahlen in K immer ein Ring ist. Und natürlich ist zu definieren, was man unter einem Dedekind-Ring versteht. Dedekind-Ringe spielen nicht nur in der Zahlentheorie, sondern auch in der algebraischen Geometrie eine grundlegende Rolle: dort beschreiben sie singularitätenfreie affine Kurven. Im Zentrum der Beweise steht der Satz von Krull-Akizuki.

1. Ganzheit. Ganzer Abschluss. Normalität.

Sei R ein Unterring des Körpers Ω. Man nennt $x \in \Omega$ *ganz über* R, falls es ein normiertes Polynom $f \in R[X]$ gibt mit $f(x) = 0$. *Ganze* (oder ganz-algebraische) Zahlen nennt man die komplexen Zahlen, die ganz über $\mathbb{Z}$ sind. (Warnung: Wenn wir hier von "ganzen Zahlen" sprechen, so muss man zur Unterscheidung die Elemente aus $\mathbb{Z}$ "ganze rationale Zahlen" nennen; dies macht Sinn, wie wir gleich sehen werden.)

Beispiele ganzer Zahlen:

- $\sqrt{2}, \sqrt{3}$ usw — denn zum Beispiel ist $\sqrt{2}$ Nullstelle von $X^2 - 2.$.
- Die Einheitswurzeln in $\mathbb{C}$: ist ζ n-te Einheitswurzel, so ist ζ Nullstelle des Polynoms $X^n - 1$.
- $x = \frac{1}{2}(1 + \sqrt{5})$ und $x' = \frac{1}{2}(1 - \sqrt{5})$ sind die beiden Nullstellen des Polynoms $X^2 - X - 1$ (denn $x + x' = 1, xx' = \frac{1}{4}(1 - 5) = -1$), also sind dies ganze Elemente.
- Allgemeiner: Ist $d \equiv 1 \mod 4$, so ist $x = \frac{1}{2}(1 + \sqrt{d})$ ganz. Beweis: Sei $x' = \frac{1}{2}(1 - \sqrt{d})$. Es ist $xx' = \frac{1}{2}(1 + \sqrt{d})\frac{1}{2}(1 - \sqrt{d}) = \frac{1}{4}(1 - d) \in \mathbb{Z}$ und natürlich auch $x + x' \in \mathbb{Z}$.
- *Ist α algebraische Zahl* (als Nullstelle eines normierten Polynoms f mit Koeffizienten in $\mathbb{Q}$), *so gibt es $c \in \mathbb{N}_1$, sodass $c\alpha$ ganz ist.* Beweis: Sei $f(X) = X^n +$

$\sum_{i=0}^{n-1} \frac{a_i}{c} X^i$, mit $a_i \in \mathbb{Z}$ und $c \in \mathbb{N}_1$. Multipliziere $f(X)$ mit c^n, dann erhalten wir $c^n X^n + \sum_{i=0}^{n-1} a_i c^{n-i} c^i X^i$. Da α Nullstelle von $f(X)$ ist, ist α auch Nullstelle von $c^n f(X)$ und demnach $c\alpha$ Nullstelle des Polynoms $g(X) = X^n + \sum_{i=0}^{n-1} a_i c^{n-i} X^i$. Das Polynom $g(X)$ ist normiert und hat Koeffizienten in $\mathbb{Z}$.

Sind $R \subseteq S$ Bereiche, so sagt man, dass S *ganz über* R ist, falls jedes Element von S ganz über R ist. Der Bereich R ist *ganz-abgeschlossen* (oder auch *normal*), falls gilt: Ist $x \in \mathrm{Quot}(R)$ ganz über R, so ist $x \in R$.

1.1. *Seien $x, y \in R$ und $\frac{x}{y}$ ganz über R. Dann gibt es ein n mit $y | x^n$.*

Beweis: Sei $f \in R[X]$ normiert mit $f(\frac{x}{y}) = 0$, etwa $f = \sum_{i=0}^{n} r_i X^i$ mit $r_n = 1$. Es ist $0 = f(\frac{x}{y}) = \sum_{i=0}^{n} r_i \frac{x^i}{y^i}$, also $x^n = -\sum_{i=0}^{n-1} r_i x^i y^{n-i}$ und die rechte Seite ist ein Vielkfaches von y.

Folgerung. *Ist R faktoriell (also ein Ring mit eindeutiger Primfaktorzerlegung), so ist R normal.*

Beweis: Seien $x, y \in R$ und $\frac{x}{y}$ ganz über R. Schreibe $y = \epsilon y_1 \cdots y_t$ mit einer Einheit ϵ und Primelementen y_i. Aus $y | x^n$ folgt $y_t | y | x^n$, also $y_t | x$ (weil y_t Primelement ist). wir können also y_t wegkürzen. Induktiv können wir alle Faktoren y_i wegkürzen. Es folgt, dass y ein Teiler von x, also $\frac{x}{y} \in R$.

Insbesondere: *Jeder Hauptidealbereich ist normal* (also zum Beispiel: der Ring $\mathbb{Z}$ der ganzen Zahlen, wie auch der Polynomring $k[X]$ in einer Variablen X über dem Körper k). Das heißt aber: *Die ganzen Elemente in $\mathbb{Q}$ sind die ganzen Zahlen.*

1.2. Äquivalente Beschreibung der Ganzheit. Sei R Unterring des Körpers Ω. Wir brauchen den Begriff eines R-Untermoduls M von Ω: Dies ist eine Untergruppe $M \subseteq \Omega$ mit $rM \subseteq M$ für alle $r \in R$. Ein Unterring S von Ω, der R enthält, ist natürlich ein R-Untermodul. Ein R-Modul M heißt *endlich erzeugt,* wenn es Elemente $y_1, \ldots, y_n \in M$ mit $M = \sum_i Ry_i$ gibt (ist $n = 1$, so nennt man M einen *zyklischen* Modul).

Lemma. *Sei R Unterring des Körpers Ω. Sei $x \in \Omega$. Dann sind die folgenden Aussagen äquivalent:*

(1) *Das Element x ist ganz über R.*
(2) *Der Unterring $R[x]$ ist endlich erzeugter R-Modul.*
(3) *Es gibt einen Unterring S von Ω der x enthält und endlich erzeugt als R-Modul ist.*
(4) *Es gibt einen von Null verschiedenen endlich erzeugten R-Untermodul M von Ω mit $xM \subseteq M$.*

Beweis: (1) impliziert (2): Ist x ganz, etwa $f(x) = 0$ mit $f = \sum_{i=0}^{n} r_i X^i$ mit $r_i \in R$ und $r_n = 1$, so nimmt man $t = n$ und $y_i = x^{i-1}$ für $1 \leq i < n$. Es ist $xy_i = y_{i+1}$ für $1 \leq i \leq n-1$, und $xy_n = xx^{n-1} = x^n = \sum_{i=0}^{n-1}(-r_i)x^i = \sum_{j=1}^{n}(-r_{j-1})y_j$.

(4) impliziert (1): Sei $M \neq 0$ der von den Elemente $y_1, \ldots, y_t \in \Omega$ erzeugte R-Untermodul, und es gelte $xM \subseteq M$. Es ist also $xy_i = \sum_j a_{ij} y_j$ für $1 \leq i \leq n$, daher gilt die Matrizengleichung

$$x \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = A \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}, \qquad \text{also} \quad (xI_n - A) \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = 0.$$

Da der Spaltenvektor der y_i nicht der Nullvektor ist, ist die linke Matrix singulär, also ist $\det(xI_n - A) = 0$. Sei χ_A das charakteristische Polynom der Matrix A. Es ist normiert, hat Koeffizienten in R und es ist $\chi_A(x) = 0$.

1.3. Anwendung 1. *Sind x, x' ganz über R, so auch $-x$, $x + x', xx'$. Die über R ganzen Elemente in Ω bilden demnach einen Unterring.*

Beweis: Zu x gibt es $y_1, \ldots, y_n$ mit $xM \subseteq M$ für $M = \sum_i Ry_i$. Zu x' gibt es $y'_1, \ldots, y'_m$ mit $x'M' \subseteq M'$ für $M' = \sum_j Ry'_j$. Setze $M'' = \sum_{i,j} Ry_i y'_j$. Es ist $xM'' \subseteq M''$ und $x'M'' \subseteq M''$, also auch $(x + x')M'' \subseteq M''$ und $(xx')M'' \subseteq M''$. Der zweite Satz folgt unmittelbar. Und natürlich ist schon $(-x)M \subseteq M$.

Die Beweise von 1.2 und 1.3 liefern ein effektives Verfahren, um normierte Polynome f mit $f(x) = 0$ zu finden. Beispiel: $\sqrt{2} + \sqrt{3}$. Nimm $y_1 = 1, y_2 = \sqrt{2}$, $y'_1 = 1, y'_2 = \sqrt{3}$, also für $\sqrt{2} + \sqrt{3}$ nimm den von $y_i y'_j$ mit $1 \leq i, j \leq 2$ erzeugten $\mathbb{Z}$-Untermodul von $\mathbb{C}$. Wir erhalten eine 4×4 Matrix.

1.4. Lemma. *Seien $R \subset S \subset T$ Ringe. Ist S endlich erzeugter R-Modul, T endlich erzeugter S-Modul, so ist T endlich erzeugter R-Modul.*

Beweis: $S = \sum_i Rs_i$, $T = \sum_j St_j$. Dann ist $T = \sum_j St_j = \sum_j (\sum_i Rs_i)t_j = \sum_{i,j} Rs_i t_j$.

Daraus folgt: **Anwendung 2.** *Sei R Unterring des Körpers Ω. Seien $s_1, \ldots, s_t \in \Omega$ ganz über R. Dann ist der von R und den Elementen $s_1, \ldots, s_t$ erzeugte Unterring ein endlich erzeugter R-Modul.*

Beweis: Sei $R_i = R[s_1, \ldots, s_i]$ für $0 \leq i \leq n$. Für $1 \leq i \leq n$ ist $R_i = R_{i-1}[s]$ ein endlich-erzeugter R_{i-1}-Modul, denn s_i ist ganz über R, also ganz über R_{i-1}. Wende induktiv Lemma 1.4 auf die folgende Kette von Ring-Erweiterungen an:

$$R = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_n.$$

1.5. Anwendung 3. *Seien $R \subseteq S$ Unterringe des Körpers Ω. Sei S ganz über R. Ist dann $x \in \Omega$ ganz über S, so ist x ganz über R.*

Beweis. Sei x Nullstelle des normierten Polynoms $f = \sum_{i=0}^{n} s_i X^i$. Da $s_0, \ldots, s_{n-1}$ ganz über R sind, ist der von R und $s_0, \ldots, s_{n-1}$ ereugte Unterring S' endlich erzeugter R-Modul, siehe 1.4. Da x ganz über S' ist, ist $S'[x]$ endlich erzeugter S'-Modul, also endlich erzeugter R-Modul.

Sei also R ein Unterring des Körpers Ω. Nach 1.4 ist die Menge R' der Elemente von Ω, die über R ganz sind, ein Unterring. Nach 1.5 ist dieser Unterring ganz abgeschlossen. Man nennt R' den *ganzen Abschluss* von R in Ω. Allgemeiner seien $R \subseteq S$ Unterringe eines Körpers Ω. Die Menge der Elemente von S, die ganz über R sind, bilden einen Unterring von S, der R enthält: man nennt ihn den *ganzen Abschluss von R in S*. Den ganzen Abschluss eines Bereichs R in seinem Quatientenkörper $\mathrm{Quot}(R)$ nennt man die *Normalisierung von R*.

Der Ring $\mathcal{O}_K$. Ist K ein Zahlkörper, so interessieren wir uns für den ganzen Abschluss $\mathcal{O}_K$ von $\mathbb{Z}$ in K, also den Ring der ganzen algebraischen Zahlen in K. Aus 1.5 folgt: *$\mathcal{O}_K$ ist normal.*

2. Ganze Bereichs-Erweiterungen.

Wir betrachten hier Bereiche $R \subseteq S$ und setzen voraus, dass S ganz über R ist.

2.1. *Sei $R \subseteq S$ ganze Bereichs-Erweiterung. Ist $0 \neq J \neq S$ ein Ideal von S, so ist $0 \neq J \cap R \neq R$ ein Ideal von R.*

Beweis: Natürlich ist $J \cap R$ ein Ideal. Wäre $J \cap R = R$, so wäre $1 \in J$, also $J = S$. Es bleibt zu zeigen $J \cap R \neq 0$. Sei $x \neq 0$ in J. Da x ganz über R ist, gibt es ein normiertes Polynom mit Koeffizienten in R, sodass x Nullstelle ist, etwa $0 = x^n + \sum_{i=0}^{n-1} r_i x^i$. Nimm ein solches Polynom mit kleinstmöglichem Grad. Dann ist $a_0 \neq 0$ und einerseits ist $a_0 \in R$, andererseits ist $a_0 = x(-x^{n-1} - \sum_{i=1}^{n-1} r_i x^{i-1})$ ein Vielfaches von x, also in J. Wir sehen: $J \cap R \neq 0$.

Zusatz. *Sei $\mathbb{Z} \subseteq S$ ganze Bereichserweiterung. Ist $0 \neq J$ ein Primideal von S, so gibt es eine Primzahl $p \in J \cap \mathbb{Z}$.* (Ist nämlich $0 \neq z \in J \cap \mathbb{Z}$, so ist $z \neq \pm 1$. Schreiben wir $\pm z$ als Produkt von Primzahlen, so muss mindestens ein Faktor in J liegegn, weil J Primideal ist.)

2.2. *Sei $R \subseteq S$ ganze Bereichs-Erweiterung. Genau dann ist R ein Körper, wenn S ein Körper ist.*

Beweis: Sei R ein Körper. Wäre S kein Körper, so gäbe es in S ein Ideal $0 \neq J \neq S$. Dann wäre aber $0 \neq J \cap R \neq R$ ein Ideal in R, also R kein Körper.

Umgekehrt sein nun S Körper. Sei $0 \neq r \in R$. In S ist r invertierbar und $\frac{1}{r}$ ist ganz über R. Wähle ein normiertes Polynom f kleinsten Grads n in $R[X]$ mit $f(r) = 0$, etwa $f = \sum a_i r^i$ mit $a_i \in R$. Multipliziere $0 = f(\frac{1}{r}) = \frac{1}{r^n} + \sum_{i=0}^{n-1} a_i \frac{1}{r^i}$ mit r^n. Wir erhalten $0 = 1 + \sum_{i=0}^{n-1} a_i r^{n-i}$; die Summanden rechts haben alle einen Faktor r, also ist $1 = r(-\sum_{i=0}^{n-1} a_i r^{n-i-1})$. Dies zeigt, dass r schon in R invertierbar ist.

2.3. *Sei $R \subseteq S$ ganze Bereichs-Erweiterung. Ist jedes von Null verschiedene Primideal von R maximal, so ist jedes von Null verschiedene Primideal von S maximal.*

Beweis: Sei $J \neq 0$ ein Primideal von S. Der Ring-Homomorphismus $R \to S \to S/J$ hat als Kern $J \cap R$, also erhalten wir einen injektiven Ring-Homorphismus $R/(J \cap R) \to S/J$, demnach ist $J \cap R$ ein Primideal (denn $R/(J \cap R)$ ist nullteilerfrei). Wegen 2.1 ist $J \cap R \neq 0$, also ein maximales Ideal und demnach ist $R/J \cap R)$ ein Körper. Nun ist aber die Bereichs-Erweiterung $R/(J \cap R) \to S/J$ ganz (denn ist $\overline{s}$ die Restklasse eines Elements in S/J, so ist s Nullstelle eines normierten Polynoms $f \in R[X]$; modulo $J \cap R$ erhalten wir ein normiertes Polynom in $(R/J \cap R)[X]$ mit Nullstelle $\overline{s}$. Nach 2.2 ist S/J Körper, also J maximales Ideal.

Bemerkung: Es gilt auch die Umkehrung. Und ganz allgemein gilt: Sei $R \subseteq S$ ganze Bereichs-Erweiterung, dann stimmt die Krull-Dimension von S und von R überein (Kaplansky, Satz 48). Dabei versteht man unter der *Krull-Dimension* die maximale Länge von Primidealketten (oder besser: das Supremum); eine Primidealkette der Länge n hat die Form

$$P_0 \subset P_1 \subset \cdots \subset P_n$$

mit Primidealen P_i und (echten!) Inklusionen $P_{i-1} \subset P_i$.

Der Ring $\mathcal{O}_K$ für einen Zahlkörper K. Wir betrachten $\mathbb{Z} \subseteq \mathcal{O}_K$, dies ist eine ganze Bereichs-Erweiterung ist. Da $\mathbb{Z}$ die krull-Dimension 1 hat, hat auch $\mathcal{O}_K$ die Krull-Dimension 1. Es gilt also: $\mathcal{O}_K$ ist ein Bereich, kein Körper, und jedes von Null verschiedene Primideal von $\mathcal{O}_K$ ist maximal.

3. Noethersche Ringe.

Ein kommutativer Ring R heißt *noethersch*, wenn jedes Ideal I von R endlich erzeugt ist (also $I = \sum_{i=1}^{n} Rr_i$ mit Elementen $r_1, \ldots, r_n \in I$).

Beispiele: Hauptidealring sind offensichtlich noethersch. Dagegen ist der Polynomring in abzählbar vielen Variablen $X_1, X_2, \ldots$ nicht noethersch - das von den Variablen erzeugte Ideal ist offensichtlich nicht endlich erzeugt.

In noetherschen Ringen gilt die Maximalbedingung für Ideale: *In jeder nichtleeren Menge $\mathcal{S}$ von Idealen gibt es ein maximales Element* (also $I \in \mathcal{S}$ mit der Eigenschaft: Ist $I \subseteq I' \in \mathcal{S}$, so ist $I = I'$). Beweis: Ansonsten gäbe es eine unendliche Folge $I_1 \subset I_2 \subset \cdots$ von Idealen in $\mathcal{S}$. Bilde $I = \bigcup_i I_i$, dies ist ein Ideal von R, also endlich erzeugt, etwa durch $r_1, \ldots, r_n$. Es sei $r_i \in I_{t(i)}$ und $t = \max_i t(i)$. Dann ist $I \subseteq I_t \subset I_{t+1} \subseteq I$, ein Widerspruch. (Es gilt auch die Umkehrung: gilt die Maximalbedingung für Ideale, so ist R noethersch.)

Allgemeiner definiert man: Ein Modul heißt *noethersch,* wenn alle Untermoduln endlich erzeugt sind. Ist R noetherscher Ring und M endlich-erzeugter R-Modul, so ist M noethersch.