Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, hhu
K. Halupczok

Z3: Zahlkörper und Zahlringe

Stichworte: Ganze Elemente in Komm. Ringen, ganzer Abschluss von A in B, B ganz über A, ganz abgeschlossen, ganz algebraisch, Zahlkörper/Zahlring

---

3.1. **Einleitung:** Der Begriff der "Ganzheit", d.h. was ganze Zahlen $z \in \mathbb{Z}$ ausmacht, (nämlich Nst. eines normierten Polynoms vom Grad 1 zu sein: $f(z)=0$ für $f(T)=T-z \in \mathbb{Z}[T]$), wird verallgemeinert zu ganzen Elementen $x \in B$ eines Oberringes B von A (nämlich Nst. eines normierten Polynoms vom Grad ≥ 1 zu sein: $f(x)=0$ für $f(T) \in A[T]$, wo f normiert).

In einem Zahlkörper bildet die Teilmenge der ganzen Elemente den zugehörigen Zahlring.
Das Mipo einer ganzen (algebraischen) Zahl liegt in $\mathbb{Z}[T]$.

3.2. **Bezeichnung:** Seien A, B kommutative Ringe, $A \subseteq B$, $x_1, \dots, x_n \in B$.
Dann bezeichnet $A[x_1, \dots, x_n]$ den von $A \cup \{x_1, \dots, x_n\}$ in B erzeugte Ring, d.h. $A[x_1, \dots, x_n] = \{ \sum_{\substack{i \text{ endl.} \\ (i=(i_1,\dots,i_m))}} a_{i_1,\dots,i_m} x_1^{i_1} \cdots x_m^{i_m} ; a_i \in A \}$,

für $x \in B$ also $A[x] = \{ \sum_{i=0}^{n} a_i x^i ; n \in \mathbb{N}, a_0, \dots, a_n \in A \}$.

3.3. Erinnerung: • $A[x_1, \dots, x_m]$ bzw. $A[x]$ sind A-Module, vgl. Algebra A16.2.
Der Begriff "A-Modul" wird in 3.6 wichtig.

• Def. "algebraisch" aus Algebra A18.2: In $L|K$ heißt $x \in L$ algebraisch über K, falls $\exists f \in K[T]: f \neq 0 \wedge f(x)=0$.

• Eine algebraische Zahl α ist ein $\alpha \in \mathbb{C}$, das algebraisch über $\mathbb{Q}$ ist.
Gängige Bezeichnung: $\overline{\mathbb{Q}} := \{ \alpha \in \mathbb{C} ; \exists f \in \mathbb{Q}[T], f \neq 0 : f(\alpha)=0 \}$,
der Körper der algebraischen Zahlen (ist Körper).
Dieser bildet den algebraischen Abschluss von $\mathbb{Q}$ in $\mathbb{C}$,
d.h. jedes $f \in \mathbb{Q}[T]$, $f \neq 0$, hat darin eine Nullstelle. Der algebraische Abschluss von $\mathbb{R}$ ist $\mathbb{C}$.

Nun die zentrale Def. dieses Kapitels:

3.4. **Def.:** Seien $A \subseteq B$ kommutative Ringe (mit 1). Ein Element $x \in B$ heißt **ganz über** A, falls es ein **normiertes** Polynom $f(T) \in A[T]$ gibt mit $f(x) = 0$. ("**Ganze Gleichung**" für x)

3.5. **Bsp.:** (1) Alle Elemente $x \in A$ sind ganz über A: $T - x \in A[T]$ tut's.
(2) $\mathbb{Z} \subseteq \mathbb{C}$: $\sqrt{2}$, $\sqrt{5}$, $\sqrt{-5}$, $e^{2\pi i/n}$ sind ganz über $\mathbb{Z}$,
da Wurzeln (=Nullstellen) von T^2-2, T^2-5, T^2+5, T^n-1.
(3) $A \subseteq C \subseteq B$, $x \in B$, x ganz über $A \Rightarrow x$ ganz über C.
(4) $K \subseteq L$ Körper, $x \in L$. Dann: x ganz über $K \Leftrightarrow x$ algebraisch über K.
(5) $\frac{1}{2}$ ist nicht ganz über $\mathbb{Z}$.

3.6. **Satz:** Seien $A \subseteq B$ Integritätsbereiche. Für $x \in B$ sind äquivalent:
(i) x ist ganz über A, (ii) $A[x]$ ist endlich erzeugter A-Modul,
(iii) Es existiert ein Zwischenring C, $A \subseteq C \subseteq B$, mit $x \in C$,
der als A-Modul endl. erz. ist.

Bew.: (i) $\Rightarrow$ (ii): Sei $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ eine ganze Glg. für x über A.
Dann ist $A[x] = \sum_{i=0}^{\infty} Ax^i = \sum_{i=0}^{n-1} Ax^i$ endl. erz. A-Modul.
(ii) $\Rightarrow$ (iii): $C := A[x]$ tut's.
(iii) $\Rightarrow$ (i):
Es ist $A \subseteq A[x] \subseteq C \subseteq B$ mit $C = \sum_{i=1}^{n} Ay_i$ für gewisse $y_1, \dots, y_n \in C$.
Schreiben $C \ni xy_i := \sum_{j=1}^{n} a_{ij} y_j$, die $a_{ij} \in A$.
Dann ist $(x I_n - (a_{ij})) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$,
da B ein Integritätsbereich, folgt also $\det(x I_n - (a_{ij})) = 0$,
d.h. x ist ganz über A [Laplace-Entwicklung von det]. □

Bem.: Der Satz 3.6 gilt auch allgemeiner für kommutative Ringe, die nicht notwendig IBe sind, vgl. [Brüske/Ischebeck/Vogel: Kommutative Algebra, Satz 7.2].

3.7. **Kor.:** Seien $x_1, \dots, x_m \in B$ ganz über A. Dann ist $A[x_1, \dots, x_m]$ endl. erz. A-Modul.

Bew.: Vollst. Ind. nach m: $m=0$: ✓, $m>0$: Nach Ind.vor. ist $A[x_1, \dots, x_{m-1}]$ endl. erz. A-Modul, etwa $A[x_1, \dots, x_{m-1}] = \sum_{i=1}^{s} A y_i =: C$.
Nun ist x_m ganz über C, also $A[x_1, \dots, x_{m-1}, x_m] = \sum_{j=1}^{t} C z_j$ für gewisse $z_1, \dots, z_t \in B$. Also ist $A[x_1, \dots, x_m] = \sum_{j=1}^{t} C z_j$
$= \sum_{j=1}^{t} \left(\sum_{i=1}^{s} A y_i \right) z_j = \sum_{\substack{i \le s \\ j \le t}} A (y_i z_j)$, d.h. $A[x_1, \dots, x_m]$ ist endl. erz. A-Modul. □

3.8. **Kor. und Def.:** $A' := \{x \in B;\ x \text{ ganz über } A\}$ ist Unterring von B, der ganze Abschluss von A in B.

Bew.: z.z.: x, y ganz über $A \Rightarrow x \pm y,\ x \cdot y$ ganz über A.
$x, y \in A' \overset{3.7}{\Rightarrow} A[x,y]$ endl. erz. A-Modul mit $x \pm y,\ x \cdot y \in A[x,y]$.
Also ist $A \subseteq A[x \pm y] \subseteq A[x,y] = C \subseteq B$, mit 3.6. folgt $x \pm y \in A'$. □

3.9. **Def.:** B heißt ganz über A, falls alle $x \in B$ ganz über A sind.

3.10. **Kor.:** $A \subseteq B \subseteq C$ Kommutative Ringe, C ganz über B, B ganz über A. Dann ist C ganz über A.

Bew.: Sei $x \in C$, $x^m + \underbrace{b_{m-1}}_{\in B_0} x^{m-1} + \dots + \underbrace{b_0}_{\in B_0} = 0$ ganze G/g. für x über B.

Dann ist $B_0 := A[b_0, \dots, b_{m-1}]$ endl. erz. A-Modul nach 3.7, da $b_0, \dots, b_{m-1}$ nach Vor. ganz über A sind. Nun ist x auch ganz über B_0 ($b_i \in B_0$), also ist nach 3.6 dann $B_0[x]$ endl. erz. B_0-Modul, also auch endl. erz. A-Modul. Nach 3.6 wiederum folgt, dass x ganz über A ist. □

3.11. **Def.:** Ein Integritätsbereich A heißt ganzabgeschlossen, falls er in seinem Quotientenkörper $K = \mathrm{Quot}(A)$ ganz abgeschlossen ist, d.h. jedes über A ganze Element aus K liegt bereits in A.

3.12. **Erinnerung:** $\mathrm{Quot}(A) := \{\frac{a}{b};\ a, b \in A,\ b \neq 0\}$ heißt Quotientenkörper von A, vgl. Algebra A 12.29.

3.13. **Bsp.:** $\mathbb{Z}$ (allg.: jeder faktorielle Ring) ist ganz abgeschlossen.
⌈Sei $(\frac{u}{v})^n + a_{n-1}(\frac{u}{v})^{n-1} + \dots + a_0 = 0$ eine ganze G/g. über $\mathbb{Z}$ für $\frac{u}{v} \in \mathbb{Q}$, die $a_i \in \mathbb{Z}$, $(u,v)=1$. Dann ist $u^n + a_{n-1}vu^{n-1} + \dots + a_0 v^n = 0$, d.h. also: $v \mid u^n$. Da $(u,v)=1$, folgt $v = \pm 1$, d.h. $\frac{u}{v} \in \mathbb{Z}$.⌋

3.14. **Kor.:** Sei A Unterring eines Körpers K. Dann ist der ganze Abschluss von A in K ganz abgeschlossen.
Bew.: Sei $A \subseteq A' \subseteq K$, A' ganzer Abschluss von A in K. Sei $x \in K$ ganz über A', da A' über A ganz, ist also auch x ganz über A. Also ist $x \in A'$, d.h. A' ist ganz abgeschlossen. □

3.15. **Def.:** Eine komplexe Zahl heißt ganz (algebraisch), falls sie ganz über $\mathbb{Z}$ ist.

3.16. **Bsp.:** $A := \{x \in \mathbb{C};\ x \text{ ganz (algebraisch)}\}$ ist Ring.

3.17. **Def.:** Ein Zahlkörper (vom Grad n) ist eine endliche Erweiterung $K \subseteq \mathbb{C}$ von $\mathbb{Q}$ vom Grad n. Der Ring $A_K := A \cap K$ heißt Zahlring von K bzw. Ring der ganzen Zahlen von K bzw. Ganzheitsring (auch: $\mathcal{O}_K$).
$\rightsquigarrow A = \mathcal{O}_{\mathbb{Q}}$

3.18. **Bsp.:**
$$\begin{array}{ccc} A_K & \subseteq & K \\ \cup & & \cup \\ \mathbb{Z} & \subseteq & \mathbb{Q} \end{array}$$
- K ist der Quotientenkörper von A_K.

⌈Sei $x \in K$, $f(T) = T^n + b_{n-1}T^{n-1} + \dots + b_0 \in \mathbb{Q}[T]$ das Mipo von x über $\mathbb{Q}$. Schreiben $b_i = \frac{u_i}{v_i}$ mit $u_i, v_i \in \mathbb{Z}$, setze $v := \prod_{i=0}^{n-1} v_i$. Betrachte $v^n f(T)$, sowie $g(T) := T^n + vb_{n-1}T^{n-1} + \dots + v^n b_0 \in \mathbb{Z}[T]$. Dann ist $g(vx) = v^n f(x) = 0$, d.h. $y := vx \in A_K$. Also ist $x = \frac{y}{v}$.⌋

3.19. **Gaußsches Lemma:** $f, h \in A[T]$, f, h primitiv $\Rightarrow f \cdot h$ primitiv, falls A faktoriell. Dabei heißt f primitiv, falls der ggT der Koeff. von f gleich 1 ist.
⌈Bew. s. Algebra A15.5.⌋

3.20. **Lemma:** $x \in \mathbb{C}$ ist ganz (algebraisch) $\Leftrightarrow$ Das Mipo f von x über $\mathbb{Q}$ liegt in $\mathbb{Z}[T]$.

Bew.: „$\Leftarrow$": Klar, „$\Rightarrow$": Sei $x \in \mathbb{C}$, ganz (alg.), $g(T) \in \mathbb{Z}[T]$ normiert mit $g(x) = 0$. Sei $f(T) \in \mathbb{Q}[T]$ das Mipo von x über $\mathbb{Q}$, dieses teilt $g(T)$ in $\mathbb{Q}[T]$, d.h. $\exists\, h \in \mathbb{Q}[T]$ mit $g = f \cdot h$. Seien $u, v \in \mathbb{N}$ minimal mit $uf, vh \in \mathbb{Z}[T]$. Dann sind uf, vh primitiv, nach dem Lemma von Gauß 3.19 ist dann auch $uvg = (uf)(vh)$ primitiv. Es folgt: $u = 1 = v$, d.h. insb. ist $f(T) \in \mathbb{Z}[T]$. □

3.21. **Kor.:** Sei $x \in \mathbb{C}$ ganz (alg.) vom Grad n. Dann ist $\mathbb{Z}[x] = \sum_{i=0}^{n-1} \mathbb{Z} x^i$.

Bew.: Es ist $x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$ für gewisse $a_i \in \mathbb{Z}$. □