Tutorium 5

Michael Walter

1 Der chinesische Restsatz

1 Satz (Chinesischer Restsatz)**.** *Es sei R ein kommutativer Ring und I, $J \subseteq R$ Ideale, und $i_0 \in I$ mit $1 - i_0 \in J$. Dann ist*

$$\Phi : R \to R/I \times R/J, x \mapsto (x + I, x + J)$$

ein surjektiver Homomorphismus mit Kern $I \cap J$.

Ein Urbild von $(r + I, s + J)$ ist dabei gegeben durch $(1 - i_0)r + i_0 s$.

Insbesondere gilt: $R/(I \cap J) \cong R/I \times R/J$.

2 Aufgabe. Sei R ein kommutativer Ring sowie a, $b \in R$ mit

$$ar + br' = 1$$

für bestimmte r, $r' \in R$. Dann gilt:

$$aR \cap bR = abR$$

Beweis. ($\supseteq$) ist klar. ($\subseteq$) Sei $x = as = bs' \in aR \cap bR$. Dann gilt:

$$x = 1x = arx + br'x = abrs' + abr's \in abR$$

□

3 Bemerkung. Zwei Zahlen a, $b \in \mathbb{Z}$ sind teilerfremd gdw. es r, $r' \in \mathbb{Z}$ gibt mit $ar + br' = 1$, also gdw. es $i_0 \in a\mathbb{Z}$ gibt mit $1 - i_0 \in b\mathbb{Z}$.

4 Satz (Chinesischer Restsatz für $\mathbb{Z}$)**.** *Seien $a_1, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremd. Dann hat das System von Kongruenzen*

$$\begin{aligned} x &\equiv r_1 \mod a_1 \\ &\vdots \\ x &\equiv r_n \mod a_n \end{aligned}$$

eine Lösung (für beliebige aber feste $r_1, \ldots, r_n \in \mathbb{Z}$). Sie ist eindeutig bis auf Vielfache von $\prod a_k$.

Beweis. Wir beweisen: Es gibt ein t, so dass das System äquivalent ist zu

$$x \equiv t \mod \prod a_k$$

Deshalb genügt es den Fall $n = 2$ zu betrachten (dann kombiniert man nacheinander zwei Kongruenzen, bis nur noch eine übrig bleibt).

Wir suchen also ein Urbild von $(r_1 + a_1\mathbb{Z}, r_2 + a_2\mathbb{Z})$ unter dem Homomorphismus

$$\Phi : \mathbb{Z} \to a_1\mathbb{Z} \times a_2\mathbb{Z}, x \mapsto (x + a_1\mathbb{Z}, x + a_2\mathbb{Z})$$

Der chinesische Restsatz liefert so eines, und es ist eindeutig bis auf ein Element aus $a_1\mathbb{Z} \cap a_2\mathbb{Z} = a_1a_2\mathbb{Z}$, d.h. bis auf Vielfache von a_1a_2 (vgl. Aufgabe 2). □

5 Aufgabe. Finde $x \in \mathbb{Z}$ so dass gilt:

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 4 \mod 7 \\ x &\equiv 5 \mod 9 \end{aligned}$$

Lösung. (1) Wir suchen ein Urbild t von

$$(2 + 5\mathbb{Z}, 4 + 7\mathbb{Z})$$

Wegen $3 \cdot 5 + (-2) \cdot 7 = 1$ können wir $i_0 := 3 \cdot 5 = 15$ wählen und erhalten die äquivalente Kongruenz

$$t \equiv (1 - 15) \cdot 2 + 15 \cdot 4 \equiv 32 \equiv -3 \mod 35$$

(2) Nun suchen wir ein Urbild t von

$$(-3 + 35\mathbb{Z}, 5 + 9\mathbb{Z})$$

Es gilt $(-1) \cdot 35 + 4 \cdot 9 = 1$, also wählen wir $i_1 := -35$ und erhalten

$$t \equiv (1 - (-35)) \cdot (-3) + (-35) \cdot 5 \equiv -283 \equiv 32 \mod 315$$

Man hätte allerdings schon am Ende von Schritt 1 sehen können, dass 32 eine Lösung ist... □

2 Moduln

6 Definition. Sei R ein Ring. Eine *R-Modul* ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Skalarmultiplikation $\cdot : R \times M \to M$ so dass gelten:

$$\begin{aligned}(rs)\cdot m &= r\cdot(s\cdot m)\\ 1\cdot m &= m\\ (r+s)\cdot(a+b) &= r\cdot a + r\cdot b + s\cdot a + s\cdot b\end{aligned}$$

7 Beispiel. Ist k ein Körper, so sind die k-Moduln genau die k-Vektorräume.

8 Beispiel. R ist selbst R-Modul mit der Ringmultiplikation.

9 Beispiel. Sei M eine beliebige Menge. Dann ist $\mathrm{Abb}(M,R)$ ein R-Modul mit

$$(r\cdot f)(m) := rf(m)$$

10 Beispiel. R ist S-Modul für jeden Teilring $S \subseteq R$.

11 Beispiel. Jede abelsche Gruppe M hat eine eindeutige $\mathbb{Z}$-Modulstruktur.

12 Bemerkung. R-Moduln entsprechen abelschen Gruppen mit Homomorphismen $\Phi : R \to \mathrm{End}((M,+))$ in deren Endomorphismenring.

13 Definition. Ein *Untermodul* U ist eine Untergruppe $U \subseteq (M,+)$ mit $RU \subseteq U$.

14 Beispiel. Jedes Ideal $I \subseteq R$ ist ein Untermodul des R-Moduls R, insbesondere also selbst R-Modul.

15 Beispiel. Die Abbildungen mit endlichem Träger $\mathrm{Abb}_0(M,R)$ bilden einen Untermodul von $\mathrm{Abb}(M,R)$.

16 Definition. Das *Modulerzeugnis* von $X \subseteq M$ ist definiert als

$$\langle X\rangle_{R\text{-mod}} := \bigcap\{U : U \subseteq M \text{ Untermodul}, X \subseteq U\}$$

17 Bemerkung. $\langle X\rangle_{R\text{-mod}}$ ist der kleinste Untermodul von M, der X enthält.

18 Definition. Ein R-Modulhomomorphismus $\Phi : M \to N$ erfüllt

$$\begin{aligned}\Phi(m+n) &= \Phi(m)+\Phi(n)\\ \Phi(rm) &= r\Phi(m)\end{aligned}$$

19 Definition. Der *Annihilator* des R-Moduls M in R ist definiert durch

$$\mathrm{Ann}_R(M) := \{r \in R : rm = 0\ (\forall m \in M)\}$$

20 Aufgabe. $\mathrm{Ann}_R(M) \subseteq R$ ist ein Ideal.

Beweis. (1) $\mathrm{Ann}_R(M)$ ist Untergruppe, denn: $0 \in \mathrm{Ann}_R(M)$ und für $r, s \in \mathrm{Ann}_R(M)$ gilt

$$(r-s)m = rm - sm = 0 \quad (\forall m \in M)$$

(2) Für $s \in R$, $r \in \mathrm{Ann}_R(M)$ gilt

$$(sr)m = s(rm) = s0 = 0 \quad (\forall m \in M)$$

Also ist $\mathrm{Ann}_R(M)$ sogar ein Ideal. □

21 Aufgabe. Sei $I \subseteq R$ ein Ideal. Dann ist R/I ein R-Modul, und es gilt

$$\mathrm{Ann}_R(R/I) = I$$

Beweis. (1) Offensichtlich definiert

$$\cdot : R \times R/I \to R/I, (r, s+I) \mapsto rs+I$$

eine R-Modulstruktur auf R/I.

(2) Es gilt:

$$\begin{aligned}&\mathrm{Ann}_R(R/I) = \{r \in R : rs + I = 0 + I \ \ (\forall s \in R)\}\\ =\ &\{r \in R : rs \in I \ \ (\forall s \in R)\} = I\end{aligned}$$

(betrachte $s = 1$). □

3 Algebren

22 Definition. Sei R ein kommutativer Ring. Eine *R-Algebra* A ist sowohl Ring als auch R-Modul, so dass gelten:

$$r \cdot (ab) = (r \cdot a)b = a(r \cdot b) \qquad (\forall r \in R, a, b \in A)$$

(d.h. die Ringmultiplikation ist R-bilinear).

23 Bemerkung. Äquivalent: Eine R-Algebra A ist ein Ring zusammen mit einem Ringhomomorphismus $\sigma : R \to A$ (sog. *Strukturhomomorphismus*) mit

$$\sigma(r)a = a\ \sigma(r) \qquad (\forall r \in R, a \in A)$$

Gegeben eine R-Modulstruktur nimmt man einfach $\sigma : r \mapsto r \cdot 1$. Und ausgehend von σ erhält man eine R-Modulstruktur via $r \cdot a := \sigma(r)a$.

24 Beispiel. $R^{n\times n}$ ist eine R-Algebra.

25 Definition. Das *Zentrum* eines Rings A ist definiert als

$$Z(A) := \{a \in A : ab = ba \quad (\forall b \in A)\}$$

26 Bemerkung. Ist der Strukturhomomorphismus injektiv, dann kann man R als Teilring des Zentrums $Z(A)$ ansehen, und also auch als Teilring von A selbst.

Andersrum ist $Z(A)$ der größte Teilring $R \subseteq A$ bzgl. dem A noch R-Algebra ist (mit der Inklusion als Strukturhomomorphismus).

27 Definition. Eine *Unteralgebra* U von A ist Teilring und Untermodul.

28 Definition. Das *Algebrenerzeugnis* von $X \subseteq A$ ist definiert als

$$A[X] := \langle X \rangle_{R\text{-Alg}} := \bigcap \{U : U \subseteq A \text{ Unteralgebra}, X \subseteq U\}$$

29 Bemerkung. $A[X]$ ist die kleinste Unteralgebra von A, die X enthält.

30 Definition. Ein R-Algebrenhomomorphismus $\Phi : A \to B$ erfüllt

$$\begin{aligned} \Phi(a+b) &= \Phi(a) + \Phi(b) \\ \Phi(a \cdot b) &= \Phi(a) \cdot \Phi(b) \\ \Phi(1) &= 1 \\ \Phi(ra) &= r\Phi(a) \end{aligned}$$

31 Notation. $\mathrm{Hom}_{R\text{-Alg}}(A, B)$ bezeichnet die Menge aller R-Algebrenhomomorphismen, und $\mathrm{Aut}(A|R) := \mathrm{Aut}_{R\text{-Alg}}(A, B)$ die Gruppe der R-Algebren-automorphismen.

4 Monoidringe

32 Definition. Ist R ein kommutativer Ring und $(M, \cdot)$ ein Monoid, so wird der *Monoidring* $(R[M], +, \star)$ definiert durch

$$\begin{aligned} R[M] &:= \mathrm{Abb}(M, R)_0 \\ (f \star g)(m) &:= \sum_{xy=m} f(x)g(y) \end{aligned}$$

Ist M sogar Gruppe, dann heißt $R[M]$ *Gruppenring*.

33 Bemerkung. Für $m \in M$ definiere $\delta_m \in R[M], n \mapsto \delta_{m,n}$. Dann lässt sich jedes $f \in R[M]$ als R-Linearkombination schreiben:

$$f = \sum_m f(m)\delta_m$$

Und mit $\delta_m \star \delta_n = \delta_{mn}$ ergibt sich recht natürlich

$$f \star g = (\sum_m f(m)\delta_m) \star (\sum_n g(n)\delta_n) = \sum_{m,n} f(m)g(n)\delta_{mn}$$

was im Nachhinein die Multiplikationsvorschrift motiviert. Man erkennt nun auch leicht, dass δ_1 das neutrale Element des Monoidrings ist.

34 Bemerkung. Der Monoidring $R[M]$ ist sogar eine R-Algebra via

$$(r \cdot f)(m) := rf(m)$$

(vgl. Beispiel 15).

35 Beispiel. $R[(\mathbb{N}_0, +)]$ ist der Polynomring in einer Variablen!

Die übliche Notation erhält man, wenn man $R[X] := R[\mathbb{N}_0]$ und $X := \delta_1$ setzt, dann gilt nämlich $X^n \star X^m = X^{n+m}$, und die Elemente in $\mathbb{R}[X]$ sind gerade die endlichen Linearkombinationen

$$\sum_n a_n\delta_n = \sum_n a_n X^n$$

36 Aufgabe. R ist Teilring von $(R[M], +, \star)$ und M ist Untermonoid von $(R[M], \star)$.

Ist M Gruppe, dann ist M Untergruppe von $(R[M]^x, \star)$.

Beweis. (1) Der Ringhomomorphismus

$$\iota : R \to R[M], r \mapsto r\delta_1$$

ist injektiv.

(2) Der Monoidhomomorphismus

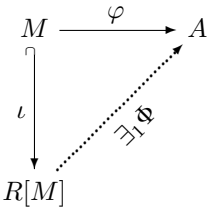
$$M \to R[M], m \mapsto \delta_m$$

ist injektiv. □

37 Satz (UAE des Monoidrings)**.** *Für jede R-Algebra A und jeden Monoidhomomorphismus $\varphi : (M, \cdot) \to (A, \cdot)$ existiert genau ein R-Algebrenhomomorphismus $\Phi : R[M] \to A$ mit*

$$\Phi(\delta_m) = \varphi(m)$$

Als Bild:



38 Aufgabe. Finde einen surjektiven R-Algebrenhomomorphismus $\mathbb{R}[S_3] \to \mathbb{R}^{2\times 2}$.

Lösung. (1) Wir konstruieren einen Monoidhomomorphismus $\varphi : S_3 \to \mathbb{R}^{2\times 2}$, der die gesuchte Abbildung induzieren soll. Diese wird wohl injektiv sein, d.h. wir suchen eine Untergruppe von $\mathrm{GL}(2, \mathbb{R})$ isomorph zur S_3. Spontan denkt man vielleicht an die Symmetriegruppe eines Dreieck: Setzt man

$$\tau := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$$
$$\pi := \left(\begin{smallmatrix} \cos(\frac{2\pi}{3}) & -\sin(\frac{2\pi}{3}) \\ \sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{smallmatrix}\right)$$

Dann gilt $\mathrm{ord}(\tau) = 2$, $\mathrm{ord}(\pi) = 3$, und an

$$\begin{aligned} \tau\pi\tau^{-1} &= \left(\begin{smallmatrix} \cos(\frac{2\pi}{3}) & \sin(\frac{2\pi}{3}) \\ -\sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} \cos(\frac{4\pi}{3}) & -\sin(\frac{4\pi}{3}) \\ \sin(\frac{4\pi}{3}) & \cos(\frac{4\pi}{3}) \end{smallmatrix}\right) = \pi^2 \end{aligned}$$

erkennt man, dass die von τ und π erzeugte Untergruppe G Ordnung 6 hat und nichtabelsch ist, d.h. isomorph zur S_3. Der Isomorphismus gibt uns das gesucht φ.

(2) Noch zu zeigen ist die Surjektivität, d.h. dass wir durch $\mathbb{R}$-Linearkombinationen von Elementen aus G ganz $\mathbb{R}^{2\times 2}$ erzeugen können.

Via $\pi + \pi^2$ erhalten wir $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ und damit $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ sowie $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Damit ergibt sich auch $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ aus π.

Und via $\pi - \pi^2$ erhält man $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ und damit die restlichen Basiselemente $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ sowie $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. □