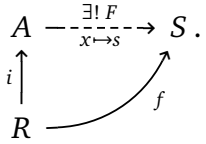
TECHNISCHE UNIVERSITÄT GRAZ
INSTITUT FÜR ANALYSIS UND ZAHLENTHEORIE
Marc Technau & Christian Elsholtz

Sommersemester 2021
Graz, den 21.05.2021

9. Übung zur Einführung in die Algebra

9.1. *(Struktur von $(\mathbb{Z}/n\mathbb{Z})^\times$)* (4 Punkte)
Es sei $G := (\mathbb{Z}/540\mathbb{Z})^\times$. Wegen $540 = 2^2 3^3 5$, Korollar 6.18 und Satz 6.21 ist $(\mathbb{Z}/540\mathbb{Z})^\times \cong C_2 \times C_{18} \times C_4$. Finden Sie Elemente $a, b, c \in G$ mit $\operatorname{ord}(a) = 2$, $\operatorname{ord}(b) = 18$ und $\operatorname{ord}(c) = 4$ und $\{1_G\} = \langle a \rangle \cap \langle b, c \rangle = \langle b \rangle \cap \langle a, c \rangle = \langle c \rangle \cap \langle a, b \rangle$.

9.2. *(Universelle Eigenschaft von $R[X]$)* (4 Punkte)
Es sei $i : R \to A$ ein Homomorphismus zwischen kommutativen Ringen und $x \in A$ sei fixiert. Ferner gelte die folgende Aussage: *für jeden Ringhomomorphismus $f : R \to S$ in einen kommutativen Ring S und jedes $s \in S$ gibt es genau einen Ringhomomorphismuis $F : A \to S$ mit $F(x) = s$, der das folgende Diagramm kommutativ macht:*

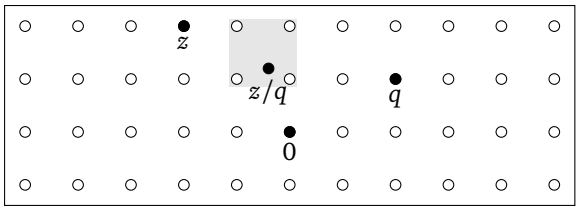


Zeigen Sie, dass A isomorph zum Polynomring $R[X]$ ist.

9.3. *(Die ganzen Gaußsche Zahlen)*
Betrachten Sie $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \in \mathbb{C} : a, b \in \mathbb{Z}\}$ zusammen mit der Funktion $N : \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$, $a + \mathrm{i}b \mapsto (a + \mathrm{i}b)(a - \mathrm{i}b) = a^2 + b^2$ (mit $a, b \in \mathbb{Z}$). Zeigen Sie:

(a) Zu $z, q \in \mathbb{Z}[\mathrm{i}]$ mit $q \neq 0$ existieren $w, r \in \mathbb{Z}[\mathrm{i}]$ mit $z = wq + r$ derart, dass $r = 0$ oder $N(r) < N(q)$ gilt.

$\mathbb{Z}[\mathrm{i}] \subset \mathbb{C}$:



(Bemerkung: dies ist eine Analogon zur Division mit Rest in $\mathbb{Z}$ oder bei Polynomen.)

(b) $(\mathbb{Z}[\mathrm{i}])^\times = \{-1, 1, -\mathrm{i}, \mathrm{i}\}$. Ist $(\mathbb{Z}[\mathrm{i}])^\times \cong C_4$ oder $(\mathbb{Z}[\mathrm{i}])^\times \cong C_2 \times C_2$?

Geben Sie Ihre Lösung bitte digital bis zum 28.05.2021, 10:00 Uhr, im zugehörigen TeachCenter-Kurs ab. Dort und auf der Vorlesungswebseite finden Sie auch weitere Informationen.
`https://tc.tugraz.at/main/course/view.php?id=352`
`https://www.math.tugraz.at/~mtechnau/teaching/2021-s-einf-algebra.html`

9.4. *(Multivariate Polynome)*
Es bezeichne I eine beliebige Indexmenge und $\mathbb{N}_0^{(I)}$ sei die Menge aller Abbildungen $I \to \mathbb{N}_0$, die für alle bis auf höchstens endlich viele Indizes aus I den Wert 0 annehmen, zusammen mit punktweise definierter Addition. Für einen kommutativen Ring R sei $R[\mathbb{N}_0^{(I)}]$ die Menge aller Abbildungen $\mathbb{N}_0^{(I)} \to R$, welche auf allen bis auf höchstens endlich vielen Elementen von $\mathbb{N}_0^{(I)}$ den Wert 0_R annehmen, zusammen mit punktweise definierter Addition und der wie folgt zu definierenden Multiplikation:

$$(f : \mathbb{N}_0^{(I)} \to R) \cdot (g : \mathbb{N}_0^{(I)} \to R) := \left(\mathbb{N}_0^{(I)} \to R,\ c \mapsto \sum_{\substack{a,b \in \mathbb{N}_0^{(I)} \\ a+b=c}} \sum f(a)g(b) \right).$$

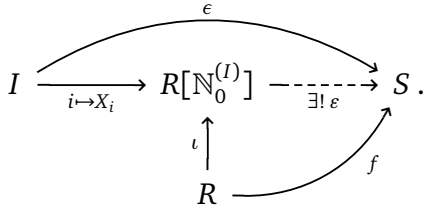
Für $i \in I$ bezeichne $X_i : \mathbb{N}_0^{(I)} \to R$ die Abbildung mit $X_i(i) = 1_R$ und $X_i(j) = 0_R$ für alle $j \in I \setminus \{i\}$. Zeigen Sie die folgenden Aussagen:

(a) Das oben definierte Produkt $f \cdot g$ zweier Elemente $f, g \in R[\mathbb{N}_0^{(I)}]$ ist tatsächlich ein Element von $R[\mathbb{N}_0^{(I)}]$ und $R[\mathbb{N}_0^{(I)}]$ bildet zusammen mit den hier definierten inneren Verknüpfungen einen kommutativen Ring. (Hinweis: alle Ringaxiome zu verifizieren wäre etwas lästig. Besprechen Sie nur eine repräsentative Auswahl nach eigenem Ermessen.)

(b) $\iota : R \to R[\mathbb{N}_0^{(I)}],\ r \mapsto \begin{cases} \mathbb{N}_0^{(I)} \to R, \\ \quad a \mapsto \begin{cases} r & \text{falls } a = (i \mapsto 0), \\ 0_R & \text{sonst,} \end{cases} \end{cases}$
ist ein Ringmonomorphismus.

(c) Jedes $f \in R[\mathbb{N}_0^{(I)}]$ lässt sich als $f = \sum_{a \in \mathbb{N}_0^{(I)}} \iota(f(a)) \prod_{i \in I} X_i^{a(i)}$ schreiben.
(Die auftretenden Produkte haben stets höchstens endlich viele von $1_{R[\mathbb{N}_0^{(I)}]} = X_i^0$ verschiedene Faktoren und die auftretende Summe nur höchstens endlich viele von $0_{R[\mathbb{N}_0^{(I)}]}$ verschiedene Summanden und können somit betrachtet werden, ohne über Konvergenz sprechen zu müssen.)

(d) Ist $f : R \to S$ ein Homomorphismus in einen beliebigen kommutativen Ring S und $\epsilon : I \to S$ eine beliebige Abbildung, so gibt es genau einen Ringhomomorphismus $\varepsilon : R[\mathbb{N}_0^{(I)}] \to S$, welcher das folgende Diagramm kommutativ macht:



Bemerkung: man schreibt auch $R[\boldsymbol{X}]$ statt $R[\mathbb{N}_0^{(I)}]$ mit $\boldsymbol{X} = \{X_i : i \in I\}$ und nennt $R[\boldsymbol{X}]$ den ***Polynomring*** über R in den ***Variablen*** (oder ***Unbestimmten***/***Veränderlichen***) X_i $(i \in I)$. Eigentlich sind die hier diskutierten Objekte sehr konkret: etwa für $I = \{1,2,3,4\}$ und $R = \mathbb{Z}$ ist ein typisches Element von $R[\boldsymbol{X}]$ gleich $10X_1^0 + X_1^{20} + 60X_1^9X_2X_4^7$. Das Bild dieses Elements unter f aus Teil (d) wäre dann $f(10)\epsilon(1)^0 + \epsilon(1)^{20} + f(60)\epsilon(1)^9\epsilon(2)\epsilon(4)^7$.