Technische Universität Graz
Institut für Analysis und Zahlentheorie
Marc Technau

Sommersemester 2023
Graz, den 17.05.2023

10. Übung zur Einführung in die Algebra

10.1. *(Ringe in der Topologie, II)* (4 Punkte)
In Fortsetzung von Aufgabe 9.4 betrachten wir den Ring R der stetigen Funktionen $f : \mathbb{R} \to \mathbb{R}$. (Notiz: Im Vergleich zu Aufgabe 9.4 ist der Definitionsbereich hier nicht kompakt.) Zeigen Sie, dass es ein maximales Ideal $\mathfrak{m}$ von R gibt, welches nicht von der Form $\mathfrak{m}_x = \{ f \in R : f(x) = 0 \}$ für $x \in \mathbb{R}$ ist. (Hinweis: Satz 6.12.)

10.2. *(Primideale, Teil I)*
Ein Ideal $\mathfrak{p} \subsetneq R$ eines Ringes R heißt ***Primideal*** (oder ***prim***), falls für alle Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von R aus $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ schon $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$ folgt. Im Folgenden sei R zusätzlich als *kommutativ* vorausgesetzt. Zeigen Sie dann die folgenden Aussagen:

(a) Für jedes Ideal $\mathfrak{p} \subseteq R$ von R sind die folgenden Aussagen äquivalent:
   (1) $\mathfrak{p}$ ist prim;
   (2) $\mathfrak{p} \neq R$ und $\forall a, b \in R \colon ab \in \mathfrak{p} \Rightarrow (a \in \mathfrak{p}$ oder $b \in \mathfrak{p})$;
   (3) $R/\mathfrak{p}$ ist ein Integritätsbereich.

(b) Jedes maximale Ideal $\mathfrak{m}$ von R ist prim.

(c) Alle Primideale $\mathfrak{p} \neq \{0\}$ von $\mathbb{Z}$ sind maximal.

10.3. *(Zum Chinesischen Restsatz)* (4 Punkte)
Finden Sie einen Ring R mit Idealen $\mathfrak{a}_1$, $\mathfrak{a}_2$ und $\mathfrak{a}_3$ derart, dass $\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 = R$ gilt, aber $R/\bigcap_i \mathfrak{a}_i$ *nicht* isomorph zu $\prod_i (R/\mathfrak{a}_i)$ ist.

10.4. *(Einheitengruppe von $\mathbb{Z}/p^\nu\mathbb{Z}$)*
Es sei p eine ungerade Primzahl und $\nu \geq 2$. Wir setzen $\lfloor \varrho \rfloor := \max\{ r \in \mathbb{Z} : r \leq \varrho \}$. Beweisen Sie die folgenden Aussagen:

(a) Es gilt $(1+p)^{p^{\nu-2}} \equiv 1 + p^{\nu-1} \bmod p^\nu$. (Hinweis: Induktion & Binomischer Lehrsatz.)

(b) $1 + p \bmod p^\nu$ hat Ordnung $p^{\nu-1}$ in $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$.

(c) Sind x und y Elemente einer endlichen abelschen Gruppe $(G, \cdot)$ mit teilerfremden Ordnungen, so ist $\operatorname{ord}(xy) = \operatorname{ord}(x)\operatorname{ord}(y)$.

(d) Hat $g \bmod p$ Ordnung $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, so hat $g^{p^{\nu-1}}(1+p) \bmod p^\nu$ Ordnung $p^\nu - p^{\nu-1}$ in $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$.

Hinweis: Bis zum 13.06.2023 läuft die Vorlesungs- und Übungsevaluierung für die *Einführung in die Algebra* (VO+UE). Bitte ziehen Sie in Erwägung, an dieser teilzunehmen.

Geben Sie Ihre Lösung bitte am 25.05.2023 vor der Vorlesung ab.
`https://www.math.tugraz.at/~mtechnau/teaching/2023-s-einf-algebra.html`