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

Sommersemester 2021
Graz, den 07.05.2021

8. Übung zur Einführung in die Algebra

8.1. *(Primideale, Teil I)* (4 Punkte)
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 $\mathfrak{p} \subsetneq R$ von R sind die folgenden Aussagen äquivalent:
  (1) $\mathfrak{p}$ ist prim;
  (2) $\forall a, b \in R\colon ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ 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.

8.2. *(Primideale, Teil II)*
Es sei $f : R \to S$ Homomorphismus zwischen kommutativen Ringen R und S.

(a) Zeigen Sie: ist $\mathfrak{p}$ ein Primideal von S, so ist das Urbild $f^{-1}(\mathfrak{p})$ ein Primideal von R.

(b) Belegen Sie durch ein Beispiel, dass das Urbild $f^{-1}(\mathfrak{m})$ eines maximalen Ideals $\mathfrak{m}$ von S nicht maximal in R zu sein braucht.

8.3. *(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.

8.4. *(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 $\mathrm{ord}(xy) = \mathrm{ord}(x)\,\mathrm{ord}(y)$.

Geben Sie Ihre Lösung bitte digital bis zum 14.05.2021, 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`

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

Ankündigung: die *Evaluierungen* für die Vorlesung und Übungen sind vom 07.05. bis zum 30.05.2021 in TUGRAZonline freigeschaltet. Bitte nehmen Sie sich Zeit, diese auszufüllen.