TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Prof. Dr. Ulrich Thiel
Laura Voggesberger, M. Sc.

Mathematik für Informatik: Algebraische Strukturen

Sommersemester 2022 - Übungsblatt 8

Abgabetermin: 24.06.2022, 10:00 Uhr, Briefkästen Gebäude 48 Erdgeschoss oder als eine PDF mit dem Button im OLAT hochladen. Die Programmieraufgaben dürfen als extra Datei (zum Beispiel txt) hochgeladen werden.

Aufgabe 1 (4 Punkte)**.** Ein Integritätsring ist ein kommutativer Ring mit $1 \neq 0$, der außer 0 keine Nullteiler hat. Zeigen Sie, dass in einem Integritätsring R die Kürzungsregel gilt: Sind $a, b, c \in R$ und $c \neq 0$, dann

$$a \cdot c = b \cdot c \quad \Rightarrow \quad a = b.$$

Aufgabe 2 (4 Punkte)**.** Bestimmen Sie in $\mathbb{Q}[x]$ einen größten gemeinsamen Teiler $\mathrm{ggT}(f, g)$ von

$$f = x^2 + 2x + 1,$$
$$g = x^2 - 2x + 1$$

und $a, b \in \mathbb{Q}[x]$ mit $\mathrm{ggT}(f, g) = a \cdot f + b \cdot g$.

Aufgabe 3 (4 Punkte)**.** Bestimmen Sie unter Verwendung des erweiterten Euklidischen Algorithmus die Menge $L \subset \mathbb{R}[x]$ aller Lösungen f der simultanen Kongruenzen

$$f \equiv 2 + 3(x-1) \bmod (x-1)^2$$
$$f \equiv 1 + 2(x+1) \bmod (x+1)^2.$$

Finden Sie die eindeutige Lösung $f \in L$ minimalen Grades.
Hinweis: Sie können das Ergebnis aus Aufgabe 2 hier verwenden.

Aufgabe 4. Welche der folgenden Ringe sind Hauptidealringe? Bitte begründen Sie Ihre Antwort.

(a) $\mathbb{R}[x]$.

(b) $\mathbb{Z}/_m$ mit $m \in \mathbb{N}$.

(c) $\mathbb{Z}[x]$. *Hinweis: Betrachten Sie $I = (2, x)$.*

Zusatzaufgabe 5 (4 Punkte)**.** Der Fermatsche Primzahltest: Eine Zahl $n \in \mathbb{N}$ heißt Fermatsche Pseudoprimzahl zur Basis $a \in \mathbb{N}$, wenn n nicht prim ist, aber dennoch wie im kleinen Satz von Fermat

$$a^{n-1} \equiv 1 \bmod n$$

gilt. Bestimmen Sie mit Computerhilfe jeweils alle Pseudoprimzahlen $n \leq 1000$ zur Basis a mit $a = 2, 3, 5$ und vergleichen Sie deren Anzahl mit der Anzahl der Primzahlen.
Hinweis: Wenn Sie Maple verwenden, können Sie die Maple-Funktionen `nextprime` *und* `mod` *verwenden.*
Wenn Sie mit Julia arbeiten wollen, so können Sie die Funktion `mod` *verwenden, wobei* $a \bmod b$ *dann berechnet wird als* `mod(a,b)`*. Um die echten Primzahlen* ≤ 1000 *zu bestimmen, verwenden Sie in Julia die Funktion* `nextprime`*, siehe auch* `https://juliamath.github.io/Primes.jl/v0.3/api.html#Primes.nextprime`.