Mathematisches Institut
der Universität München
Helmut Schwichtenberg

Sommersemester 2008
Blatt 6

Übungen zur Vorlesung „Diskrete Strukturen“

Auf diesem Blatt sind A, B kommutative Ringe mit 1.

Aufgabe 21. Sei $f\colon A \to B$ Ringhomomorphismus. Man zeige
(a) Wenn $\mathfrak{b} \subseteq B$ Ideal von B ist, so ist auch $f^{-1}(\mathfrak{b})$ Ideal von A.
(b) Ist $\mathfrak{a} \subseteq A$ Ideal von A und f surjektiv, so ist auch $f(\mathfrak{a})$ Ideal von B.

Aufgabe 22. Ein Ideal $\mathfrak{p} \subseteq A$ mit $\mathfrak{p} \neq A$ heißt *Primideal*, wenn für alle $x, y \in A$ gilt

Aus $xy \in \mathfrak{p}$ folgt $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$.

(a) Sei $\mathfrak{p} \subseteq A$ ein Ideal mit $\mathfrak{p} \neq A$. Man zeige:

$\mathfrak{p}$ ist Primideal genau dann, wenn $A/\mathfrak{p}$ ein Integritätsring ist.

(b) Sei $A = \mathbf{Z}$, $\mathfrak{p} = p\mathbf{Z}$ mit $p \in \mathbf{N}$, $p \geq 2$. Man zeige, daß $p\mathbf{Z}$ genau dann ein Primideal ist, wenn p Primzahl ist.

Aufgabe 23. Für Ideale $\mathfrak{a}, \mathfrak{b} \subseteq A$ und Teilmengen $M \subseteq A$ definiert man

$$\mathfrak{a} + \mathfrak{b} := \{\, x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b} \,\}, \quad \mathfrak{a} \cap \mathfrak{b} := \{\, x \mid x \in \mathfrak{a}, x \in \mathfrak{b} \,\},$$
$$(M) := \{\, x_1 a_1 + \cdots + x_n a_n \mid n \geq 0, a_1, \dots, a_n \in M, x_1, \dots, x_n \in A \,\}.$$

Wir schreiben $(a_1, \dots, a_n)$ für$(\{a_1, \dots, a_n\})$. Man zeige
(a) $\mathfrak{a} + \mathfrak{b}$ und $\mathfrak{a} \cap \mathfrak{b}$ sind Ideale von A.
(b) (M) ist das kleinste M umfassende Ideal von A, d.h. es gilt
  (i) (M) ist ein Ideal.
  (ii) $(M) \supseteq M$.
  (iii) Ist $\mathfrak{a} \supseteq M$ Ideal von A, so ist $\mathfrak{a} \supseteq (M)$.
(c) Für $a, b \in A$ ist $(a) + (b) = (a, b)$.

Aufgabe 24. Man zeige
(a) Für $a, b \in \mathbf{Z}$ und $m \in \mathbf{N}$, $m > 0$ sind äquivalent
  (i) a und b haben denselben Rest bei der Division durch m.
  (ii) $m \mid a - b$.
  Bezeichnung: $a \equiv b \mod m$; „a ist kongruent zu b modulo m“.
(b) Für $a, b, c, d \in \mathbf{Z}$ und $m \in \mathbf{N}$, $m > 0$ gelte $a \equiv b \mod m$ und $c \equiv d \mod m$. Man zeige
  (i) $a + c \equiv b + d \mod m$,
  (ii) $-a \equiv -b \mod m$,
  (iii) $ac \equiv bd \mod m$.

Abgabe. Dienstag, 10. Juni 2008, 14:15 Uhr, Briefkasten im 1. Stock