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.

Beweis. (a). Nach einem Lemma über Gruppenhomomorphismen ist $f^{-1}(\mathfrak{b})$ Untergruppe von $(A, +)$. Noch zu zeigen ist $Af^{-1}(\mathfrak{b}) \subseteq f^{-1}(\mathfrak{b})$. Seien dazu $y \in A$ und $x \in A$ mit $f(x) \in \mathfrak{b}$. Dann gilt $f(yx) = f(y)f(x) \in \mathfrak{b}$, da $f(x) \in \mathfrak{b}$ und $\mathfrak{b}$ ein Ideal ist. Damit folgt $yx \in f^{-1}(\mathfrak{b})$. (b). Nach dem Lemma über Gruppenhomomorphismen ist $f(\mathfrak{a})$ Untergruppe von $(B, +)$. Noch zu zeigen ist $Bf(\mathfrak{a}) \subseteq f(\mathfrak{a})$. Seien dazu $x \in \mathfrak{a}$ und $y \in B$. Da f surjektiv ist, existiert ein $z \in A$ mit $f(z) = y$. Dann gilt $yf(x) = f(z)f(x) = f(zx) \in f(\mathfrak{a})$, da $zx \in \mathfrak{a}$. □

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.

Beweis. (a). Folgende Aussagen sind äquivalent.

$\mathfrak{p}$ Primideal

$\forall_{x,y \in A}(xy \in \mathfrak{p} \to x \in \mathfrak{p}$ oder $y \in \mathfrak{p})$

$\forall_{x,y \in A}(xy \sim_{\mathfrak{p}} 0 \to x \sim_{\mathfrak{p}} 0$ oder $y \sim_{\mathfrak{p}} 0)$

$A/\mathfrak{p}$ Integritätsring

(b). Folgende Aussagen sind äquivalent.

$p\mathbf{Z}$ Primideal

$\forall_{x,y \in \mathbf{Z}}(p \mid xy \to p \mid x$ oder $p \mid y)$

p Primzahl

□

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

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

Wir schreiben $(a_1, \ldots, a_n)$ für$(\{a_1, \ldots, a_n\})$. 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 $(a) + (b) = (a, b)$.

Beweis. (a). Unter Benützung des Untergruppenkriteriums läßt sich leicht zeigen, daß $\mathfrak{a} + \mathfrak{b}$ und $\mathfrak{a} \cap \mathfrak{b}$ Untergruppen von $(A, +)$ sind. Seien nun $a \in A$, $w \in \mathfrak{a} + \mathfrak{b}$, $z \in \mathfrak{a} \cap \mathfrak{b}$. Dann existieren $x \in \mathfrak{a}$ und $y \in \mathfrak{b}$ so, daß $w = x + y$ und es gilt $aw = a(x + y) = ax + ay \in \mathfrak{a} + \mathfrak{b}$, da $ax \in \mathfrak{a}$ und $ay \in \mathfrak{b}$ ($\mathfrak{a}$ und $\mathfrak{b}$ sind Ideale), sowie $az \in \mathfrak{a} \cap \mathfrak{b}$, da $az \in \mathfrak{a}$ und $az \in \mathfrak{b}$. Damit folgt, daß $\mathfrak{a} + \mathfrak{b}$ und $\mathfrak{a} \cap \mathfrak{b}$ Ideale von A sind.

(b). Wieder folgt nach dem Untergruppenkriterium sofort, daß (M) Untergruppe von $(A, +)$ ist. Seien $a \in A$ und $x = x_1 a_1 + \cdots + x_n a_n \in (M)$. Dann folgt $ax = (ax_1)a_1 + \cdots + (ax_n)a_n \in (M)$, da $ax_i \in A$ für alle i, also ist (M) ein Ideal. $(M) \supseteq M$ ist klar. Sei $\mathfrak{a} \supseteq M$ Ideal von A. Dann folgt $\mathfrak{a} \supseteq AM (:= \{\, yx \mid y \in A, x \in M \,\})$, da $\mathfrak{a}$ Ideal ist, und damit $\mathfrak{a} \supseteq (M)$, da $\mathfrak{a}$ Untergruppe von $(A, +)$ ist.

(c). Seien $a, b \in A$. Es gilt $(a) \subseteq (a, b)$ und $(b) \subseteq (a, b)$, also $(a) + (b) \subseteq (a, b)$, da (a, b) Untergruppe von $(A, +)$ ist. Nach (a) ist $(a) + (b)$ ein Ideal und damit $(a) + (b) \supseteq (a, b)$ nach (b). Also gilt $(a) + (b) = (a, b)$. $\square$

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) $ac \equiv bd \mod m$.

Beweis. (a). Seien $a = mp + r$ und $b = mq + s$ mit $p, q \in \mathbf{Z}$ und $r, s \in \mathbf{N}$, $r, s < m$. $\rightarrow$. Gelte $r = s$. Dann ist $a - b = m(p - q)$, also $m \mid a - b$. $\leftarrow$. Es ist $a - b = m(p - q) + (r - s)$. Aus $m \mid a - b$ folgt also $m \mid r - s$. Wegen $0 \leq r, s < m$ folgt $r = s$.

(b). Gelte $m \mid (a - b)$ und $m \mid (c - d)$. Dann folgt (i) $m \mid ((a - b) + (c - d))$, also $m \mid ((a + c) - (b + d))$. (ii). Klar. (iii). Es folgt $m \mid (a(c - d) + (a - b)d)$, also $m \mid (ac - bd)$. $\square$

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