Dr. Reimund Albers, Arithmetik als Prozess, WiSe 08/09

6. Übung, Lösungsskizzen

1a) R_5

$\cdot$ mod 5	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

R_6

$\cdot$ mod 6	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

b) R_5: Alle Restklassen tauchen in jeder Zeile auf außer in der Zeile für $\bar{0}$

R_6: Alle Restklassen tauchen nur in den Zeilen für $\bar{1}$ und $\bar{5}$ auf

c) in R_5 $\quad \bar{a} \cdot \bar{b} = \bar{0} \iff \bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$

in R_6 $\quad \bar{a} \cdot \bar{b} = \bar{0}$ gilt für $\bar{a} = 0$ u. $\bar{b}$ beliebig, $\bar{b} = \bar{0}$ und $\bar{a}$ beliebig, $\bar{2} \cdot \bar{3} = 0$, $\bar{3} \cdot \bar{2} = 0$, $\bar{3} \cdot \bar{4} = \bar{0}$, $\bar{4} \cdot \bar{3} = \bar{0}$

d) R_5 hat keine Nullteiler

R_6 hat $\bar{2}$, $\bar{3}$ und $\bar{4}$ als Nullteiler

e) R_7 hat auch keine Nullteiler

f) R_5 u. R_7 keine Nullteiler: Vermutung ist, dass keine Nullteiler bei ungeraden Modulu auftauchen.

R_9

$\cdot$ mod 9	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$					

also ist $\bar{3}$ Nullteiler in R_9

Die Vermutung mit den ungeraden Modulu ist falsch!

...... Ergebnis $\bar{a} \neq \bar{0}$ ist Nullteiler in R_n

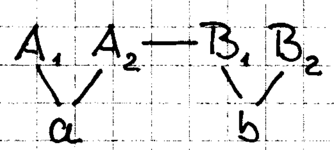
$\Leftrightarrow$ a und n haben einen gemeinsamen Teiler größer als 1

HAUSÜBUNGEN

2a. Reflexivität

Jeder Mensch hat mit sich selbst die gleichen Eltern, die zu sich selbst Geschwister sind

Symmetrie

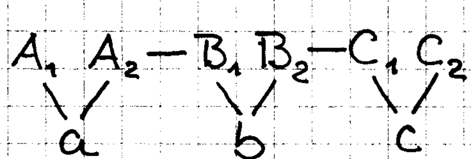


A_1, A_2 Eltern von a

B_1, B_2 " " b

Cousin/Cousine ist symmetrisch, da „Geschwister sein" symmetrisch ist.

Transitivität



In diesem Diagramm sieht man deutlich, dass sich „Cousin/-sine sein" <u>nicht</u> transitiv überträgt.

2b) Reflexivität

a AGP a Jeder Studi gibt mit sich selbst die Übungsaufgaben ab

Symmetrie

a AGP $b \Rightarrow b$ AGP a Wenn a mit b die Übungen in einer Gruppe abgibt, so auch b mit a

Transitivität

a AGP b und b AGP $c \Rightarrow a$ AGP c

Wenn a mit b und b mit c abgibt, dann auch a mit c.

Die Grundmenge für diese Relation ist die Menge aller Studierenden dieser Vorlesung. Die Menge zerfällt in die Übungsgruppen, die die Äquivalenzklassen darstellen.

3a) Annahme: $n \in \mathbb{N}$ ist in zwei verschiedenen Restklassen von R_{10}, also $n \in \overline{a}$ und $n \in \overline{b}$ mit $\overline{a} \neq \overline{b}$. Es seien a und b jeweis die kleinsten Repräsentanten von $\overline{a}$ und $\overline{b}$

$\Rightarrow \overline{a} = \{ k \mid k = t \cdot 10 + a,\ t \in \mathbb{N}_0 \}$

$\overline{b} = \{ i \mid i = t \cdot 10 + b,\ t \in \mathbb{N}_0 \}$

$$\left.\begin{array}{l} n \in \overline{a} \Rightarrow \exists\, t_a \in \mathbb{N} \text{ mit } n = t_a \cdot 10 + a \\ n \in \overline{b} \Rightarrow \exists\, t_b \in \mathbb{N} \text{ mit } n = t_b \cdot 10 + b \end{array}\right\} \text{gleichsetzen}$$

$t_a \cdot 10 + a = t_b \cdot 10 + b \Rightarrow a - b = 10(t_b - t_a)$

$a-b$ ist ein Vielfaches von 10, dann kann wegen $0 \leq a,b < 10$ nur $a - b = 0$ sein.

Dann gilt aber $\overline{a} = \overline{b}$ Widerspruch!

Nach der Definition der Äquivalenzklassen gilt $\overline{a} = \{ n \in M \mid n \otimes a \}$ und $\overline{b} = \{ m \in M \mid m \otimes b \}$

Dann bedeutet

$c \in \overline{a}$, dass $c \otimes a$ und $c \in \overline{b}$ bedeutet $c \otimes b$

Wegen der Transitivität von $\otimes$ folgt

$a \otimes b$. D.h. $a \in \overline{b}$ und $b \in \overline{a}$

Ist n ein beliebiges Element aus $\overline{a}$, so gilt $n \otimes a$. Mit $a \otimes b$ folgt $n \otimes b$, also $n \in \overline{b}$

Jedes Element von $\overline{a}$ ist also Element von $\overline{b}$ (*)

Ist m ein beliebiges Element aus $\overline{b}$, so gilt $m \otimes b$. Mit $a \otimes b$ folgt $m \otimes a$, also $m \in \overline{a}$

Jedes Element von $\overline{b}$ ist auch Element von $\overline{a}$ (**)

(*) und (**) besagen, dass $\overline{a} = \overline{b}$ $\square$

4. $3 \equiv 3 \mod 11 \qquad 3^2 \equiv 9 \mod 11 \qquad 3^3 \equiv 5 \mod 11$

$3^4 = 3^3 \cdot 3 \equiv 4 \mod 11 \qquad 3^5 \equiv 3^4 \cdot 3 \equiv 1 \mod 11$

also $3^{10} = 3^5 \cdot 3^5 \equiv 1 \mod 11$

Ist der Exponent von 3 durch 5 teilbar, so ist die Potenz $\equiv 1 \mod 11$

Also

$$3^{132} = 3^{130} \cdot 3^2 \equiv 1 \cdot 9 = 9 \mod 11$$

$$3^{132} \equiv 9 \mod 11$$

5. (2) Substitution $x^2 = z \quad x^4 = z^2$

(3) Einsetzen der Substitution

(3) → (4) a^2 nach rechts, quadratische Ergänzung

(4) → (5) links vollständiges Binom, rechts ausgerechnet

(5) → (6) Wurzel ziehen, + und − vor der Wurzel

(6) → (7) $(a+1)$ subtrahieren, damit nach z aufgelöst

(7) → (8) Rücksubstitution $z = x^2$

(8) → (9) Wurzel ziehen, + und − vor der Wurzel