Blatt #3, 31. Okt. 2002

Aufgabe 9.

(1) Zu (R 1): $(\mathfrak{P}(M), +)$ ist abelsche Gruppe (mit neutralem Element 0) nach Aufgabe 7.(3).
Zu (R 2a): $(\mathfrak{P}(M), \cap)$ ist abelsches Monoid mit 1. Seien dazu $A, B, C \in \mathfrak{P}(M)$, dann gilt:
(G 1) $A \cap (B \cap C) = (A \cap B) \cap C$;
(G 2) Mit $1 := M \in \mathfrak{P}(M)$ gilt $A \cap 1 = 1 \cap A = A$;
(G 4) $A \cap B = B \cap A$.
Zu (R 3): Da $(\cap)$ kommutativ ist, genügt $(A + A') \cap B = \big((A \setminus A') \cup (A' \setminus A)\big) \cap B = \Big(\big((A \cap B) \setminus (A' \cap B)\big) \cup \big((A' \cap B) \setminus (A \cap B)\big)\Big) = (A \cap B) + (A' \cap B)$ für $A, A', B \in \mathfrak{P}(M)$.

(2) Nach Vorlesung gilt: $(\mathfrak{P}(M), +, \cap)$ Körper $\Leftrightarrow 1 \neq 0$ (d.h. $M \neq \emptyset$) und $\forall A \in \mathfrak{P}(M) \setminus \{\emptyset\} \quad \exists B \in \mathfrak{P}(M) : A \cap B = M = 1$.
$\#M = 0$. Kein Körper, da $M = \emptyset$.
$\#M = 1$. Da $\mathfrak{P}(M) \setminus \{\emptyset\} = \{M\}$ und $M \cap M = 1$, ist $(\mathfrak{P}(M), +, \cap)$ ein Körper.
$\#M \geq 2$. Sei $A \in \mathfrak{P}(M) \setminus \{\emptyset, M\}$. Dann gilt $\forall B \in \mathfrak{P}(M) : A \cap B \subseteq A \subsetneq M = 1$, also existiert zu A kein Inverses, und folglich ist $(\mathfrak{P}(M), +, \cap)$ kein Körper.

(3) Es ist $\mathfrak{P}(N) \leqslant \mathfrak{P}(M)$ bzgl. $(+)$ nach Aufgabe 7.(4); da $\forall A \in \mathfrak{P}(N) \quad \forall B \in \mathfrak{P}(M) : A \cap B \subseteq A \in \mathfrak{P}(N)$, ist $\mathfrak{P}(N)$ Ideal.

(4) Nach Definition ist $\mathfrak{P}(M)/\mathfrak{P}(N) = \{\bar{A} \mid A \in \mathfrak{P}(M)\}$ mit $\bar{A} = \{A + B \mid B \in \mathfrak{P}(N)\}$. Damit ist $\mathfrak{P}(M)/\mathfrak{P}(N) = \{\overline{\emptyset}, \overline{\{b\}}\}$ mit $\overline{\emptyset} = \{\emptyset, \{a\}\}$ und $\overline{\{b\}} = \{\{b\}, \{a, b\}\}$. Repräsentantenweise Ausführung der Operationen ergibt:

$+$	$\overline{\emptyset}$	$\overline{\{b\}}$
$\overline{\emptyset}$	$\overline{\emptyset}$	$\overline{\{b\}}$
$\overline{\{b\}}$	$\overline{\{b\}}$	$\overline{\emptyset}$

$\cap$	$\overline{\emptyset}$	$\overline{\{b\}}$
$\overline{\emptyset}$	$\overline{\emptyset}$	$\overline{\emptyset}$
$\overline{\{b\}}$	$\overline{\emptyset}$	$\overline{\{b\}}$

(5) Für $a, b \in R$ ist $0 = (a+b)^2 - (a+b) = (a^2 + ab + ba + b^2) - (a+b) = ab + ba$. Mit $c = a = b$ folgt $0 = c^2 + c^2 = c + c$, d.h. stets $c = -c$ und damit auch $ab = -ba = ba$.

Aufgabe 10.

(1)

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(2)

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(3) Es ist $x \equiv_7 3$ oder $x \equiv_7 5$.

(4) $\mathbf{F}_p$ ist Körper, d.h. $(\mathbf{F}_p \setminus \{0\}, \cdot)$ ist abelsche Gruppe mit $p-1$ Elementen. Sei $x \in \mathbf{F}_p \setminus \{0\}$. Dann ist $G_x := \{x^m \mid m \in \mathbf{Z}\} \leqslant \mathbf{F}_p \setminus \{0\}$ Untergruppe. Da $\#G_x =$ (Ordnung von x), gibt es nach Aufgabe 4.(1) ein $k \in \mathbf{Z}$ mit (Ordnung von x) $\cdot\, k = p - 1$. Also $x^{p-1} \equiv_p (x^{(\text{Ordnung von } x)})^k \equiv_p$

$1^k \equiv_p 1$ und damit $x^{p-1} - 1 \equiv_p 0$. Also gilt $x^p - x \equiv_p x(x^{p-1} - 1) \equiv_p 0$ sowohl für $x \in \mathbf{F}_p \setminus \{0\}$ als auch für $x \equiv_p 0$.

Aufgabe 11.

(1) Alle Potenzen sind bereits gegeben durch $\{3^i \mid i \in \mathbf{Z}\} = \{1, 3, 9, 11\}$.

(2) E ist $\{x \in \mathbf{Z}/16\mathbf{Z} \mid 6 \cdot x \equiv_{16} 0\} = \{0, 8\}$.

(3) Invertierbar sind:

x	1	3	5	7	9	11	13	15
x^{-1}	1	11	13	7	9	3	5	15

(4) Einsetzen aller 16 Werte ergibt $\{x \in \mathbf{Z}/16\mathbf{Z} \mid x^3 + x + 2 \equiv_{16} 0\} = \{3, 6, 7, 11, 15\}$.

(5) Nach (3) gilt $\{x \in \mathbf{Z}/16\mathbf{Z} \mid 5 \cdot x \equiv_{16} 1\} = \{13\}$. Mit dem Ansatz $x = 13 + 16k$ mit $k \in \mathbf{Z}$ ergibt sich $\{(x, y) \in \mathbf{Z} \times \mathbf{Z} \mid 5 \cdot x + 16 \cdot y = 1\} = \{(x, y) \in \mathbf{Z} \times \mathbf{Z} \mid x = 13 + 16k, y = -4 - 5k, k \in \mathbf{Z}\}$.

(6) Für $x \in \mathbf{Z}/16\mathbf{Z}$ errechnet man $x^4 \equiv_{16} 0$ oder $x^4 \equiv_{16} 1$. Also ist die Restklasse der Summe von 14 Biquadratzahlen enthalten in $\{0, 1, \ldots, 14\}$. Eine solche Summe kann demnach nicht von der Form $16k + 15$ sein.

Aufgabe 12.

(1) Es ist

$$\begin{aligned} 0 \cdot x &= 0 \cdot x + (0 \cdot x - 0 \cdot x) && \text{nach (R 1)} \\ &= (0 + 0) \cdot x - 0 \cdot x && \text{nach (R 3)} \\ &= 0 \cdot x - 0 \cdot x && \text{nach (R 1)} \\ &= 0 && \text{nach (R 1)} \end{aligned}$$

und genauso folgt $x \cdot 0 = 0$.

(2) Seien $a, b, c \in R$. Falls alle beteiligten Elemente aus $R \setminus \{0\}$ stammen, gilt die jeweilige Aussage aus (G 1, 2, 4) nach (R 4). Bleiben folgende Fälle zu betrachten:
Zu (G 1): Ist (mind.) eines der Elemente a, b, c gleich null, so folgt mit (1):
$0 = (a \cdot b) \cdot c = a \cdot (b \cdot c) = 0$.
Zu (G 2): Nach (1) ist $1 \cdot 0 = 0 \cdot 1 = 0$.
Zu (G 4): Ist (mind.) eines der Elemente a, b gleich null, so folgt mit (1): $0 = a \cdot b = b \cdot a = 0$.