12.1.2015 MONTAG

LuDS

BLATT 10

Aufgabe 1

$\mathbb{Q} = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \} \subseteq \mathbb{R}$

$(\mathbb{Q}, +, \cdot)$ Körper?

$(\mathbb{Q}, +)$ abelsche Gruppe

$(\mathbb{Q} \setminus \{0\}, \cdot)$ abelsche Gruppe

Distributivgesetze

$a + b\sqrt{2},\ c + d\sqrt{2} \in \mathbb{Q}$

$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}$

$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = a \cdot c + a \cdot d\sqrt{2} + cb\sqrt{2} + bd(\sqrt{2})^2$

$= (ac + 2b \cdot d) + (a \cdot d + b \cdot c)\sqrt{2} \in \mathbb{Q}$

Kommutativität und Assoziativität gilt, da auch auf $\mathbb{R}$ gilt:

Neutrales Element bzgl Addition ist 0

—— " —— Multiplikation ist 1

Distributivgesetze gelten, da sie in $\mathbb{R}$ auch gelten

Für $a+b\sqrt{2} \in \mathbb{Q}$ ist

$-(a+b\sqrt{2})$ das additive Inverse

und

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

ist multiplikatives Inverses, denn $a^2-2b^2 \neq 0$, ~~da~~

, da sonst $a^2=2b^2$

$$\Rightarrow a=\sqrt{2}\,b \notin \mathbb{Q} \quad \lightning$$

$\Longrightarrow (\mathbb{Q}, +, \cdot)$ ist ein Körper

Abgeschlossenheit

$a \in N$

$b \in N$

$a+b \in N$

wenn z.B.

$a-b \notin N$

möglich

Aufgabe 3)

a) $(R_1, +_1, \cdot_1), (R_2, +_2, \cdot_2)$ Ringe

$(R_1 \times R_2, +, \cdot)$ Ring 2

Abgeschlossenheit offensichtlich

$(R_1 \times R_2, +)$ abelsche Gruppe

$(R_1 \times R_2, \cdot)$ Halbgruppe

Distributivgesetze

Seien $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in R_1 \times R_2$

Assoziativität $((a_1, a_2) + (b_1, b_2)) + (c_1, c_2)$

$= (a_1 +_1 b_1, a_2 +_2 b_2) + (c_1, c_2)$

$= ((a_1 +_1 b_1) +c_1, (a_2 +_2 b_2) +_2 c_2)$

$= (a_1, a_2) + ((b_1, b_2) + (c_1, c_2))$

Kommutativität $(a_1, a_2) + (b_1, b_2)$

$= (a_1 +_1 b_1, a_2 +_2 b_2)$

$= (b_1 +_1 a_1, b_2 +_2 a_2)$

$= (b_1, b_2) + (a_1, a_2)$

Neutr. Element θ_1, θ_2 neutrale Elemente des jeweiligen Ringes

$$(a_1, a_2) + (a_1, a_2) = (a_1 +_1 a_1 , a_2 +_2 a_2) = (a_1, a_2)$$

Inv. Elemente $-a_1, -a_2$ inv. Ele. im jeweiligen Ring

$$(a_1, a_2) + (-a_1, -a_2) = a_1 +_1 (-a_1), a_2 + (-a_2)) = (\theta_1, \theta_2)$$ ✓

Assoziativität $((a_1, a_2) \cdot (b_1, b_2)) (c_1, c_2)$

$$= ((a_1 \cdot b_1) \cdot c_1, (a_2 \cdot_2 b_2) \cdot c_2)$$
$$= (a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2))$$

Distributivgesetz $(a_1, a_2)) \cdot ((b_1, b_2) + (c_1, c_2))$

$$(a_1, a_2) \cdot ((b_1, b_2) + (c_1, c_2))$$
$$= (a_1, a_2) \cdot (b_1 +_1 c_1, b_2 +_2 c_2)$$
$$= (a_1 \cdot (b_1 +_1 c_1), a_2 \cdot_2 (b_2 +_2 c_2))$$
$$= ((a_1 \cdot_1 b_1) + (a_1 \cdot_1 c_1), (a_2 \cdot_2 b_2) +_2 (a_2 \cdot_2 c_2))$$
$$= (a_1, a_2) \cdot (b_1, b_2) + (a_1, a_2) \cdot (c_1, c_2)$$
$$= (a_1, a_2) + ((b_1, b_2) \cdot (c_1, c_2))$$

analog $\Rightarrow (R_1 \times R_2 +, \cdot)$ Ring

$x \equiv 6 \mod 17$

$x \equiv 4 \mod 13$

$17 = 1 \cdot 13 + 4$

$13 = 3 \cdot 4 + 1$

$4 = 4 \cdot 1 + 0$

$1 = 13 - 3 \cdot 4 = 13 - 3(17 - 13) = 4 \cdot 13 - 3 \cdot 17$

Es ergibt sich insgesamt

$x = 6 \cdot (4 \cdot 13) + 4((-3) 17) = 108$

① RSA Verschlüsselung

$p = 5$, $q = 7$

$n = 35$ $\varphi(n) = \varphi(p) \cdot \varphi(q) = 4 \cdot 6 = 24$

Sei $e \in \{5, 7, 11, 13, 17, 19, 23\}$

$E(x) = mod(x^e, n)$

$\mathbb{Z}/n\mathbb{Z}$ $d = e^{-1}$, in unseren Fall $d = e$

a) $(x_1 \rightarrow \neg x_2) \land \neg (x_3 \leftrightarrow x_1)$

x_1	x_2	x_3	
0	0	0	1
0	0	1	1
0	1	0	0
			0
			1
			1
			0
			0

DNF $(\neg x_1 \land \neg x_2 \land x_3) \lor (\neg x_1 \land x_2 \land x_3) \lor$

$(x_1 \land \neg x_2 \land \neg x_3)$

b) $(x_1 \to \neg x_2) \wedge \neg(x_3 \leftrightarrow x_1)$

$\equiv (x_1 \to \neg x_2) \wedge \neg((x_3 \to x_1) \wedge (x_1 \to x_3))$

$\equiv (\neg x_1 \vee \neg x_2) \wedge \neg((\neg x_3 \vee x_1) \wedge (\neg x_1 \vee x_3))$

$\equiv (\neg x_1 \vee \neg x_2) \wedge (\neg(\neg x_3 \vee x_1) \vee \neg(\neg x_1 \vee x_3))$

$\equiv (\neg x_1 \vee \neg x_2) \wedge (\neg\neg x_3 \wedge x_1) \vee (\neg\neg x_1 \wedge \neg x_3))$

$\equiv (\neg x_1 \vee \neg x_2) \wedge (((x_3 \wedge \neg x_1) \vee x_1) \wedge ((x_3 \wedge \neg x_1) \vee \neg x_3))$

$\equiv (\neg x_1 \vee \neg x_2) \wedge ((x_3 \vee x_1) \wedge (\neg x_1 \vee x_1)$

$\equiv (\neg x_1 \vee \neg x_2) \wedge ((x_3 \vee x_1) \wedge (\neg x_1 \vee x_1) \wedge (x_3 \vee \neg x_3) \wedge (\neg x_1 \vee \neg x_3)$

4) $(M, \circ)$ eine Halbgruppe

Gegeben:

Komplette Defi- 1 $\boxed{x \circ e = x = e \circ x}$

Komplette Definition 2 $\boxed{x \circ y = e = y \circ x}$

$z \circ x = e$

$$y \circ x = e \circ (y \circ x) = (z \circ x) \circ (y \circ x)$$

$$= z \circ (x \circ y) \circ x$$

$$= (z \circ e \circ x)$$

$$= z \circ x = e$$

$$x \circ e = x \circ (y \circ x) = (x \circ y) \circ x = e \circ x = x$$

$K = \{x \in \mathbb{R} \mid \forall q \in \mathbb{Q} : x\, q \notin \{\pi, \frac{1}{\pi}\}\} \subseteq \mathbb{R}$

Es gilt: $a = \sqrt{2} \in K$ und $b = \frac{\pi}{\sqrt{2}}$, aber

$$a \cdot b = \sqrt{2}\, \frac{\pi}{\sqrt{2}} = \pi \notin K$$