Mathematik für Informatiker 3 - Serie 3

Tobias Reincke
Matrikelnummer 218203884

December 11, 2019

Aufgabe 1

$(a_1, a_2) \oplus (b_1, b_2) := (a_1 + b_1, a_2 + b_2)$
$(a_1, a_2) \odot (b_1, b_2) := (a_1 b_1, a_1 b_2 + a_2 b_1)$
$M := \{(x, y) | x, y \in \mathbb{Q}\}$
Nach Definition ist (M , $\oplus$, $\odot$) ein kommutativer Ring gdw.

- i) (M, $\oplus$) eine abelsche Gruppe.
- ii) (M, $\odot$) eine abelsche Halbgruppe
- iii) Distributivitätgesetz gilt.

i)

Assoziativitätsgesetz:
$((a_1, a_2) \oplus (b_1, b_2)) \oplus (c_1, c_2)$
$= (a_1 + b_1, a_2 + b_2) \oplus (c_1, c_2)$
$= (a_1 + b_1 + c_1, a_2 + b_2 + c_1)$
$= (a_1, a_2) \oplus (b_1 + c_1, b_2 + c_2)$
$= (a_1, a_2) \oplus ((b_1, b_2) \oplus (c_1, c_2))$

Das neutrale Element in (M, $\oplus$) ist (0,0). Es ist auch das einzige, da es die einzige Ergebnis folgender Gleichungen ist:
$a_1 = a_1 + x_1 \rightarrow x_1 = 0$
$a_2 = a_2 + x_2 \rightarrow x_2 = 0$
Jedes Element (a, b) ist invertierbar mit $(-a, -b)$ da: $(a + (-a), b + (-b)) = (0, 0) \rightarrow$ (M, $\oplus$) ist Gruppe. (M, $\oplus$) ist abelsch:
$(a_1, a_2) \oplus (b_1, b_2) = (a_1 + b_1, a_2 + b_2) = (b_1 + a_1, b_2 + a_2) = (b_1, b_2) \oplus (a_1, a_2)$
Das geht eigentlich aus der Assoziativität hervor.

ii)

Assoziativitätsgesetz:
$((a_1, a_2) \odot (b_1, b_2)) \odot (c_1, c_2)$
$= (a_1b_1, a_1b_2 + a_2b_1) \odot (c_1, c_2)$
$= (a_1b_1c_1, a_1b_1c_2 + (a_1b_2 + a_2b_1)c_1)$
$= (a_1b_1c_1, a_1b_1c_2 + a_1b_2c_1 + a_2b_1c_1)$
$= (a_1b_1c_1, a_1(b_1c_2 + b_2c_1) + a_2(b_1c_1))$
Das Erste mal das Zweite plus das Zweite mal das Erste
$= (a_1, a_2) \odot (b_1c_1, b_1c_2 + b_2c_1)$
$= (a_1, a_2) \odot ((b_1, b_2) \odot (c_1, c_2))$
Bewiesen!
$a_1 * b_1 = a_1 \to b_1 = 1$
$a_2 = 1 * a_2 + b_2 * a_1 \to 0 = b_2 * a_1 \to b_2 = 0$

Es gibt genau ein Neutrales Element
$n = (1, 0)$!
n ist invertierbar mit sich selbst! $(M, \odot)$ ist Halbgruppe.
$(M, \odot)$ ist abelsch.
$(a_1, a_2) \odot (b_1, b_2)$
$= (a_1b_1, a_1b_2 + a_2b_1)$
$= (a_1b_1, a_2b_1 + a_1b_2)$
$= (b_1, b_2) \odot (a_1, a_2)$

iii)

Distributivgesetz:
linkes:
$(a_1, a_2) \oplus ((b_1, b_2) \odot (c_1, c_2)) = ((a_1, a_2) \oplus (b_1, b_2)) \odot ((a_{1,2}) \oplus (c_1, c_2))$
$\to (a_1, a_2) \oplus (b_1c_1, c_1b_2 + c_2b_1) = (a_1 + b_1, a_2 + b_2) \odot (a_1 + c_1, a_2 + c_2)$
$\to (a_1 + b_1c_1, a_2 + c_1b_2 + c_2b_1) = (a_1a_1 + a_1b_1 + a_1c_1,)$

hi
$(a_1, a_2) \odot ((b_1, b_2) \oplus (c_1, c_2)) = ((a_1, a_2) \odot (b_1, b_2)) \oplus ((a_{1,2}) \odot (c_1, c_2))$
$\to (a_1, a_2) \odot (b_1 + c_1, b_2 + c_2) = (a_1b_1,)$

Aufgabe 2

Aufgabe 3

Aufgabe 4

RSA-Algorithmus:
geg: Primzahlen $p := 11, q := 17$; private Key $g := 97; n = 11 * 17$ vom Empfänger
g ist teilerfremd zu 160, g ist sogar prim!
$m := \phi(n) = (p-1)(q-1) = 10 * 16 = 160$ Ermitteln von k : 33 (via Code)

```
scary__@archlinux ~/S/Lineare Optimierung> ./choosek
97 160
g = 97, m = 160
97 34 131 68 5 102 39 136 73 10 107 44 141 78 15 112 49 146 83 20 117 54 151 88 25 122 59 156 93 30 127 64 1
3201 mod m == 1! Wähle k =33
98 35 132 69 6 103 40 137 74 11 108 45 142 79 16 113 50 147 84 21 118 55 152 89 26 123 60 157 94 31 128 65 2 99 36 133 70 7
8 85 22 119 56 153 90 27 124 61 158 95 32 129 66 3 100 37 134 71 8 105 42 139 76 13 110 47 144 81 18 115 52 149 86 23 120 5
 135 72 9 106 43 140 77 14 111 48 145 82 19 116 53 150 87 24 121 58 155 92 29 126 63 0
k:
33 ⏎
```

Senden von $k = 33$ und $n = 187$ an Absender (öffentlich)
geg: $a := 20$ Absender verschlüsselt: $e := a^k \mod = 20^{33} \mod 160 = 85899345920000000000000000000000000000000 \mod 160 = 0$
Zur Herleitung: $20^{33} \mod 160 = 2^{33} * 2^{33} * 5^{33} \mod 2*2*2*2*2*5 = 2^{66} * 5^{33} \mod 2^5 * 5 = 0$
Absender verschickt Zahl $e = 0$ Empfänger entschlüsselt $b := e^g \mod n = 0^{97} \mod 187 = 0$
Dabei gilt:
$a = b \leftrightarrow 0 = 20$ Irgendwas ist hier falsch..

```
genius> 20^(33*97) mod (11*17)
= 20
```

Aufgabe 5