Lösungshinweise zu Blatt # 5
Lineare Algebra und Analytische Geometrie 1

WS 2014/15 Dozent: Ingo Runkel

Zu den kurzen Fragen (4 P)

1. [1P] Nein, betrachte z.B. die Untergruppen $(2\mathbb{Z}, +)$ und $(3\mathbb{Z}, +)$ von $(\mathbb{Z}, +)$. Die Vereinigung enthält zwar die Elemente 2 und 3, aber nicht $2 + 3$.
2. [1P] Die Injektivität impliziert, dass jeder Bildwert höhstens einmal getroffen wird. Aus Satz 1.4.9 wissen wir, dass für eine Abbildung $f\colon A \to B$ die Identität $f(e_A) = e_B$ gilt.
3. [1P] Mit Bemerkung 1.5.3 a) gilt für alle $r \in R$, dass $r = 1 \cdot r = 0 \cdot r = 0$.
4. [1P] $(\mathbb{Z}, \tilde{+})$ ist keine Gruppe.

Zu Aufgabe 18 (2 P)
Wir zeigen, dass für alle $n \geq 0$ gilt

$$A(n) := \left(\sum_{i=0}^{n} f_i = f_{n+2} - 1 \right).$$

Die ersten Folgenglieder sind gegeben durch

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ \dots\ .$$

<u>(IA)</u>

Behauptung. $A(0)$ ist wahr.

Beweis. Es gilt

$$f_0 = 0 \quad \text{und} \quad f_2 - 1 = 1 - 1 = 0.$$

$\square$

<u>(IS)</u>

Behauptung. $\forall n \geq 0\colon A(n) \implies A(n+1)$.

Beweis.

$$\sum_{i=0}^{n+1} f_i = \sum_{i=0}^{n} f_i + f_{n+1} \overset{A(n)}{=} (f_{n+2} - 1) + f_{n+1} \overset{\text{Def.}}{=} f_{n+3} - 1.$$

$\square$

Zu Aufgabe 19 (5 P)

1. [2P] $a) \Rightarrow b)$: Man überzeugt sich leicht, dass L_a ein Gruppenhomomorphismus von $(R, +)$ in sich selbst ist. Da R nullteilerfrei ist und $a \neq 0$, gilt $0 = L_a(b) = ab \Rightarrow b = 0$. Die Aussagen folgt nun aus Satz 1.4.13.

   $b) \Rightarrow a)$: Klar.

2. [2P] Wir müssen zeigen, dass für jedes $r \in R\backslash\{0\}$ ein $r^{-1} \in R$ existiert: Nach 1. und dem Hinweis ist für jedes $r \in R\backslash\{0\}$ die Abbildung L_r surjektiv. Insbesondere gibt es ein $b \in R$, so dass mit der Kommutativität von R die Identität $1 = L_r(b) = rb = br$ gilt. Also ist $r^{-1} = b$.

3. [1P] Nein, z.B. ist $(\mathbb{Z}, +, \cdot)$ ein kommutativer, nullteilerfreier Ring mit Eins, aber kein Körper.

Zu Aufgabe 20 (7 P)
(Diese Lösung ist vollständig ausformuliert. D.h. in etwa diesem Umfang erwarten wir Ihre Abgaben.)

1. [2P] Wir zeigen, dass die Abbildung wohldefiniert (d.h. repräsentantenunabhängig) ist:

   Behauptung. Seien $x, y \in \mathbb{Z}/m\mathbb{Z}$. Wähle $a, b \in \mathbb{Z}$ mit $x = [a]$, $y = [b]$. Setze $z := [a \cdot b]$. Für alle $a', b' \in R$ mit $x = [a']$, $y = [b']$ gilt

   $$z = [a' \cdot b'].$$

   Beweis. Wegen $[a] = [a'] \Leftrightarrow a' - a \in m\mathbb{Z}$ gibt es $u, v \in \mathbb{Z}$, so dass $a' - a = um$ und $b' - b = vm$ gilt. Es folgt

   $$\begin{aligned} a'b' &= (a + um)(b + vm) \\ &= ab + m(av + bu + uvm) \\ \Longrightarrow \quad [a'b'] &= [ab]. \end{aligned}$$

   □

2. [2P] (R1) folgt aus Satz 1.4.14.

   (R2) ($\cdot$ ist assoziativ): Für alle $a, b, c \in R$ gilt

   $$[a] \cdot ([b] \cdot [c]) = [a] \cdot [bc] = [a(bc)] = [(ab)c] = [ab] \cdot [c] = ([a] \cdot [b]) \cdot [c].$$

   (R3) (Distributivgesetz): Für alle $a, b, c \in R$ gilt

   $$([a] + [b]) \cdot [c] = [a + b] \cdot [c] = [(a + b)c] = [ac + bc] = [ac] + [bc] = [a] \cdot [c] + [b] \cdot [c],$$
   $$[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a] \cdot [b] + [a] \cdot [c].$$

3. [2P] Die Multiplikation in R ist kommutativ, denn $[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a]$. Wegen $1 \notin p\mathbb{Z}$ gilt $[0] \neq [1]$. Nach Aufgabe 19 bleibt daher nur noch zu zeigen, dass R nullteilerfrei ist: Seien $[a], [b] \in \mathbb{Z}/p\mathbb{Z}$. Dann gilt

$$0 = [a] \cdot [b] = [ab] \iff ab = up \quad \text{für ein } u \in \mathbb{Z}.$$

Da p eine Primzahl ist, muss daher a oder b durch p teilbar sein.[1] Sei dies ohne Beschränkung der Allgemeinheit für a der Fall. Dann gibt es ein $v \in \mathbb{Z}$, so dass gilt

$$a = vp \implies [a] = [0].$$

Also ist R nullteilerfrei.

4. [1P] Es gilt $[4]^{-1} = [13]$, denn $[13] \cdot [4] = [52]$ und $52 = 1 + 3 \cdot 17 \Leftrightarrow [52] = [1]$.

Zu Aufgabe 21 (2 P)

$x + y$:

$x \backslash y$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$x \cdot y$:

$x \backslash y$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Zu Aufgabe 22 (4 P)
(K2) Durch direktes Nachrechnen weist man nach, dass $(\mathbb{C}\backslash\{0\}, \cdot)$ eine abelsche Gruppe (und insbesondere abgeschlossen) ist. Das neutrale Element ist $(1, 0)$ und für $(a, b) \in \mathbb{C}\backslash\{0\}$ ist das Inverse durch $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ gegeben.
(K3) Das Distributivgesetz gilt:

$$\begin{aligned}(a_1, b_1) \cdot [(a_2, b_2) + (a_3, b_3)] &= (a_1, b_1) \cdot (a_2 + a_3, b_2 + b_3) \\ &= (a_1(a_2 + b_2) - b_1(b_2 + b_3), a_1(b_2 + b_3) + b_1(a_2 + a_3)) \\ &= (a_1, b_1)(a_2, b_2) + (a_1, b_1)(a_3, b_3).\end{aligned}$$

Die Beziehung $[(a_1, b_1) + (a_2, b_2)] \cdot (a_3, b_3) = (a_1, b_1)(a_3, b_3) + (a_2, b_2)(a_3, b_3)$ zeigt man analog.

[1] Dies ist eine bekannte Aussage über Primzahlen, die wir hier ohne Beweis benutzt haben.