Musterlösung Blatt 11

Aufgabe 1

a) Eine solche Aussage lässt sich konstruieren, indem man die zuerst die Teilaussagen konstruiert die nur in Zeile 2 bzw. 3 der Tabelle ein W haben und diese mit „∨" verbindet.

X	Y	$X \wedge \neg Y$	$\neg X \wedge Y$	$(X \wedge \neg Y) \vee (\neg X \wedge Y)$	(A)
W	W	F	F	F	F
W	F	W	F	W	W
F	W	F	W	W	W
F	F	F	F	F	F

b) Die Terme können über das Aufstellen einer Wahrheitstabelle aufgelöst werden ~~bis ins~~. Dann kann abgelesen werden ob es eine Tautologie ist. ~~um~~ Oder man formt sie äquivalent um.

- $(X \wedge Y) \vee (\neg X)$

X	Y	$X \wedge Y$	$\neg X$	$(X \wedge Y) \vee (\neg X)$
W	W	W	F	W
W	F	F	F	F ← keine Tautologie
F	W	F	W	W
F	F	F	W	W

- $(X \to \neg Y) \vee \neg X \Leftrightarrow (\neg X \vee \neg Y) \vee (\neg X) = \neg X \vee \neg Y = \neg(X \wedge Y)$
  keine Tautologie
- $(X \to \neg Y) \vee (\neg X \vee Y) \Leftrightarrow (\neg X \vee \neg Y) \vee (\neg X \vee Y) \Leftrightarrow \neg X \vee (\neg Y \vee Y) \Leftrightarrow W$
  Tautologie.

Aufgabe 2

a) Folgende Aussagen sollen äquivalent bewiesen werden. Dazu gibt es mehrere Möglichkeiten:

- $(i) \Leftrightarrow (ii)$, $(ii) \Leftrightarrow (iii)$, $(iii) \Leftrightarrow (iv)$
- $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iii)$, $(iii) \Rightarrow (iv)$, $(iv) \Rightarrow (i)$

$\vdots$

Die zweite erfordert nur vier Implikationen. Im konkreten Fall sähe das so aus:

i) ⇒ ii):

Sei $A \subseteq B$. Nun ist zu zeigen, dass $A \cup B = B$ ist. Die Inklusion $B \subseteq A \cup B$ gilt immer. Für die umgekehrte Inklusion betrachte man:

$$A \cup B \overset{A \subseteq B}{\subseteq} B \cup B = B.$$

ii) ⇒ iii):

Sei $A \cup B = B$, dann soll $A \cap B = A$ gelten. $A \cap B \subseteq A$ gilt immer. Umgekehrt ist

$$A = A \cap A \subseteq A \cap (A \cup B) = A \cap B,$$ was Gleichheit zeigt.

iii) ⇒ iv):

Sei $A \cap B = A$. Dann ist

$$A \setminus B = (A \cap B) \setminus B \subseteq B \setminus B = \emptyset$$ und somit $A \setminus B = \emptyset$.

iv) ⇒ i):

Sei $A \setminus B = \emptyset$. Es gilt $\neg \exists x : x \in \emptyset \Rightarrow \neg \exists x : x \in A \setminus B$

$\Rightarrow \neg \exists x : x \in A \wedge x \notin B \Rightarrow \forall x : x \notin A \vee x \in B$

$\Rightarrow \forall x : x \in A \Rightarrow x \in B \Leftrightarrow A \subseteq B$.

b) Beweis durch Induktion über endl. Mengen.

IA: $A = \emptyset$. Dann ist $A \times B = \emptyset \times B = \emptyset$ und damit endlich.

$A = \{x\}$. Dann ist $A \times B = \{x\} \times B \cong B$ endlich.

Die Bijektion von B und $\{x\} \times B$ ist gegeben durch: $\varphi : B \to \{x\} \times B$

$b \mapsto (x, b)$.

IV: Sei die Aussage für feste endl. Menge A wahr.

IS: Sei x beliebiges Element. Betrachte

$$(A \cup \{x\}) \times B = (A \times B) \cup (\{x\} \times B)$$

Nach Voraussetzung ist $A \times B$ endl. und nach der Berechnung von oben ist auch $\{x\} \times B$ endl. man könnte in einer separaten Induktion nachrechnen, dass die Vereinigung endlicher Mengen endlich ist.

Dies zeigt die Aussage.

Aufgabe 3

a) Sei $j((a,c)) = j((a',c'))$. Also ist $a = a'$. Es bleibt zu zeigen, dass $c = c'$ ist. Da $(a,c), (a',c') \in D$ gilt.

$g(c) = f(a)$, $f(a') = g(c')$. Da $a = a'$ ist $f(a) = f(a')$ und somit $g(c) = g(c')$. ~~Wegen~~ Auf Grund von Injektivität von g gilt $c = c'$. Somit $(a,c) = (a',c')$ und j injektiv.

b) Sei $(a,b) \in D$, dann gilt $2a = 5b$. Somit $5 \mid 2a \Rightarrow 5 \mid a$. Gelte umgekehrt $5 \mid a$, also $a = 5b$, dann ist $(a, 2b) \in D$. Also $j(D) = 5\mathbb{Z} = \{z \in \mathbb{Z} \mid z = 5m \text{ für ein } m \in \mathbb{Z}\}$.

c) $f: \mathbb{Q}_+ \longrightarrow \mathbb{R}_+, \; x \mapsto x^2$.

Sei $f(q) = f(q')$. Da die Quadratfunktion streng monoton wächst auf $\mathbb{Q}_+$ gilt auch Injektivität.
\# Allerdings wird 2 nicht getroffen.

$g: \mathbb{R}_+ \longrightarrow \mathbb{R}_+, \; x \mapsto x^2$

Injektivität gilt aus dem selben Grund wie oben.
Die Wurzelfunktion ist eine Umkehrfunktion.

$h: \mathbb{Q}_+ \longrightarrow \mathbb{Q}_+, \; x \mapsto x^2$.

Siehe f, da $2 \in \mathbb{Q}_+$.

d) Zunächst ist $\varphi: \mathbb{Z} \longrightarrow \mathbb{N}$

$$z \mapsto \begin{cases} -2z, & \text{für } z \leq 0 \\ 2z-1, & \text{für } z > 0 \end{cases}$$

bijektiv.

Stelle dann jedes n 2-adisch dar, dann erhält man eine endliche Folge von Den und 1en.

$$n = \sum_{i=0}^{m} a_i 2^i \longmapsto p = \sum_{i=0}^{m} a_i X^i$$

Ist dann die gewünschte Abbildung zwischen $\mathbb{N}$ und $\mathbb{Z}/2\mathbb{Z}[X]$.

Komposition der Abbildungen ergibt die Gesamtabbildung.

Aufgabe 4 Beweis durch Induktion.

$n=1$: $\Delta_1 = \frac{1(1+1)}{2} = 1 = \prod_{k=1}^{0} \left(1+\frac{1}{k}\right)\left(1+\frac{1}{k+1}\right)$.

Sei die Aussage für $n \in \mathbb{N}$ korrekt.

$n \mapsto n+1$:

$$\prod_{k=1}^{n} \left(1+\frac{1}{k}\right)\left(1+\frac{1}{k+1}\right) = \left(1+\frac{1}{n}\right)\left(1+\frac{1}{n+1}\right)\prod_{k=1}^{n-1} \left(1+\frac{1}{k}\right)\left(1+\frac{1}{k+1}\right)$$

$$= \left(\frac{n+1}{n} \cdot \frac{n+2}{n+1}\right) \Delta_n = \frac{n+1}{n} \cdot \frac{n+2}{n+1} \frac{(n+1)\cdot n}{2} = \frac{n+1\,(n+2)}{2} = \Delta_{n+1}.$$

Aufgabe 5

a) Zu prüfen sind Reflexivität, Symmetrie und Transitivität.

Reflexivität: $\frac{a}{b} \sim_p \frac{a}{b} \Leftrightarrow ab \equiv ab \pmod p \Leftrightarrow p \mid 0$ ✓

Symmetrie: $\frac{a}{b} \sim_p \frac{c}{d} \Leftrightarrow ad \equiv cb \pmod p$

$\Leftrightarrow cb \equiv ad \pmod p \Leftrightarrow \frac{c}{d} \sim_p \frac{a}{b}$

Transitivität: Nach Voraussetzung gelte

$\frac{a}{b} \sim_p \frac{c}{d}$ und $\frac{c}{d} \sim_p \frac{e}{f}$. Außerdem gilt $p \nmid d$.

Dann ist $\frac{a}{b} \sim_p \frac{c}{d} \Leftrightarrow p \mid ad-bc$ und $\frac{c}{d} \sim_p \frac{e}{f} \Leftrightarrow p \mid cf-de$

$\Rightarrow p \mid (ad-bc)f = adf - bcf$ und

$p \mid (cf-de)b = bcf - deb$

$\Rightarrow p \mid adf - bcf + bcf - deb = (af-eb)d$

$\overset{p \nmid d}{\Rightarrow} p \mid af-eb \Rightarrow af \equiv eb \pmod p$

$\Rightarrow \frac{a}{b} \sim_p \frac{e}{f}$.

b) Die Addition und Multiplikation auf $\mathbb{Z}_p$ sollen durch

$$+ : \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \qquad \cdot : \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$$
$$\left(\left[\tfrac{a}{b}\right]_p, \left[\tfrac{c}{d}\right]_p\right) \mapsto \left[\tfrac{ad+bc}{bd}\right]_p, \quad \left(\left[\tfrac{a}{b}\right]_p, \left[\tfrac{c}{d}\right]_p\right) \mapsto \left[\tfrac{ac}{bd}\right]_p$$

definiert werden. Eventuell müssen die entstehenden Brüche erst gekürzt werden. Da $p \nmid b$ und $p \nmid d$ folgt, da p prim ist, das $p \nmid bd$.

Wohldefiniertheit:

„+" Sei $\left[\tfrac{a}{b}\right]_p = \left[\tfrac{a'}{b'}\right]_p$ und $\left[\tfrac{c}{d}\right]_p = \left[\tfrac{c'}{d'}\right]_p$. Zu zeigen: $\left[\tfrac{a}{b}\right] + \left[\tfrac{c}{d}\right] = \left[\tfrac{a'}{b'}\right] + \left[\tfrac{c'}{d'}\right]$

$$\left[\tfrac{a}{b}\right] + \left[\tfrac{c}{d}\right] = \left[\tfrac{ad+bc}{bd}\right], \quad \left[\tfrac{c'}{b'}\right] + \left[\tfrac{c'}{d'}\right] = \left[\tfrac{a'd'+b'c'}{b'd'}\right]$$

$(ad+bc)b'd' \equiv (a'd'+b'c')bd \pmod p$

$\Leftrightarrow ab'dd' + bb'cd' \equiv a'bd'd + b'bc'd \pmod p$

Nach Voraussetzung ist $ab' \equiv a'b$ und $c'd \equiv cd'$, also

$\Leftrightarrow a'bdd' + bb'c'd \equiv a'bdd' + b'bc'd \pmod p$

$\Leftrightarrow p \mid 0$ ✓

„·" Wie oben, $\left[\tfrac{a}{b}\right] \cdot \left[\tfrac{c}{d}\right] = \left[\tfrac{ac}{bd}\right]$, $\left[\tfrac{a'}{b'}\right] \cdot \left[\tfrac{c'}{d'}\right] = \left[\tfrac{a'c'}{b'd'}\right]$

$acb'd' \equiv a'c'bd \pmod p$ gilt, denn $ab' \equiv a'b$ und $cd' \equiv c'd \pmod p$.

Somit ist auch „·" wohldefiniert.

Alle Ringeigenschaften vererben sich nun von $\mathbb{R}$.

c) Sei $\varphi: \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}_p$ ein beliebiger Homomorphismus von Ringen, dann gilt $\varphi([1]_p) = \left[\frac{1}{1}\right]_p$, da $1 \mapsto 1$ gelten muss.

Da $[k]_p = \left[\sum_{i=1}^{k} 1\right]_p = \sum_{i=1}^{k} [1]_p$ gilt für $k \geq 0$ und für $k < 0$ analog mit -1 muss

$$\varphi([k]_p) = \varphi\left(\sum_{i=1}^{k} [1]_p\right) = \sum_{i=1}^{k} \varphi([1]_p) = \sum_{i=1}^{k} \left[\frac{1}{1}\right]_p = \left[\frac{k}{1}\right]_p$$

gelten. Somit kann es höchstens einen Ringhomomorphismus von $\mathbb{Z}/p\mathbb{Z}$ nach $\mathbb{Z}_p$ geben. Es ist also nur zu zeigen, dass die oben genannte Abbildung wohldefiniert ist und bijektiv.

1. Wohldefiniertheit

Sei $[n]_p = [m]_p$, dann gilt ~~$n = m + kp$~~ $n \equiv m \pmod{p}$, somit ist $n \cdot 1 \equiv m \cdot 1 \pmod{p}$ und daher $\frac{n}{1} \sim_p \frac{m}{1}$.

Insgesamt also $\varphi([n]_p) = \varphi([m]_p)$.

2. Bijektivität

Surjektivität: Jedes Element der Form $\left[\frac{n}{1}\right]_p$ in $\mathbb{Z}_p$ wird getroffen, denn $n \equiv r \pmod{p}$ für ein $0 \leq r < p$. Dann ist $[r]_p$ Urbild von $\left[\frac{n}{1}\right]_p$. Nun ist zu zeigen, dass jede Klasse $\left[\frac{a}{b}\right]_p$ in der Form $\left[\frac{n}{1}\right]_p$ geschrieben werden kann.

Sei also $\frac{a}{b}$ beliebiger gekürzter Bruch mit $p \nmid b$. Gesucht ist $n \in \mathbb{Z}$ mit $a \cdot 1 \equiv n \cdot b \pmod{p}$.
Da $p \nmid b$ ist $ggT(p,b) = 1$, somit gibt es $s, t \in \mathbb{Z}$ mit $sp + tb = 1$
Somit $asp + atb = a \Rightarrow atb \equiv a \pmod{p}$ [asp fällt weg!]
at ist das gesuchte n.
$\Rightarrow \varphi$ ist surjektiv.

Injektivität: Sei $\varphi([n]_p) = \varphi([m]_p)$, d.h. $\left[\frac{n}{1}\right]_p = \left[\frac{m}{1}\right]_p$

$\Leftrightarrow \frac{n}{1} \sim_p \frac{m}{1} \Leftrightarrow n \equiv m \pmod p \Leftrightarrow [n]_p = [m]_p$.

Somit ist φ injektiv. Das war zu zeigen.

Aufgabe 6

a) Sei $\varphi: \mathbb{Z}[i] \longrightarrow \mathbb{Z}/7\mathbb{Z}$ Ringhomomorphismus.

Betrachte $\varphi(i)$. Es muss in $\mathbb{Z}/7\mathbb{Z}$ gelten, dass

$[\varphi(i)]^4 = \varphi(i^4) = \varphi(1) = 1$.

Da $[0]^4 = [0]$, $[2]^4 = [16] = [2]$, $[3]^4 = [81] = [4]$,

$[4]^4 = [16]^2 = [2]^2 = [4]$, $[5]^4 = [25]^2 = [4]^2 = [2]$

$[6]^4 = [36]^2 = [1]^2 = [1]$, $[1]^4 = [1]$.

D.h. es kommt nur $\varphi(i) = [6]$ und $\varphi(i) = [1]$ in Frage.

Es gilt aber auch, dass $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1)$

$= -[1] = [6]$.

Aber $\varphi(i) = [1]$ und $\varphi(i) = [6]$ erfüllen das beide nicht. Somit kann φ nicht existieren.

b) Wir haben in 5c) gesehen, dass es für jeden Ring R höchstens einen Ringhomomorphismus von $\mathbb{Z}/n\mathbb{Z}$ nach R gibt, nämlich den, der $[k]_n$ auf $\sum_{i=1}^{k} 1_R$ schickt.

In diesem Fall ist $[1]_{21} = [22]_{21}$, aber

$\sum_{i=1}^{1} [1]_{22} = [1]_{22}$, aber $\sum_{i=1}^{22} [1]_{22} = [22]_{22} = [0]_{22} \neq [1]_{22}$.

Somit gibt es keinen Homomorphismus.

c) Durch den eukl. Algorithmus gibt es $s,t \in \mathbb{Z}$ mit
$ggT(8,33) = 1 = 8s + 33t$.

Somit wäre $[1]_{33} = [8s+33t]_{33} = [8s]_{33} = [\overline{8}]_{33}[s]_{33}$.

Berechne s:

$33 = 4 \cdot 8 + 1 \quad \Rightarrow \quad 1 = 33 + (-4)8$

$\Rightarrow [-4]_{33}$ ist Inverses. $[-4]_{33} = [29]_{33}$.

$\mathbb{Z}/33\mathbb{Z}$ ist kein Körper, da
$[3]_{33} \cdot [11]_{33} = [33]_{33} = [0]_{33}$, aber wede $[3]_{33}$ noch $[11]_{33}$ sind $[0]_{33}$. Somit ist $\mathbb{Z}/33\mathbb{Z}$ nicht nullteilerfrei, was jeder Körper erfüllen muss.

Aufgabe 7

a) Sei R ein Ring und $x \in R$.
$\varphi: R \to R$, $y \mapsto xy$ ist additiv, denn

$\varphi(y+z) = x(y+z) = xy + xz = \varphi(y) + \varphi(z)$.

b) Es gelte die Kürzungsregel und R sei endlich, dann ist R ein Körper.

Alles was R zum Körper fehlt ist die Existenz von Inversen für Elemente, die nicht 0 sind.

Sei $x \in R \setminus \{0\}$ beliebig. Die Abbildung $\varphi_x: R \to R$, $y \mapsto xy$ ist wegen der Kürzungsregel für $x \neq 0$ injektiv, denn $xy = xz \Rightarrow y = z$. Da R endl. ist muss φ_x surjektiv sein. Somit wird die 1 getroffen, d.h.
$\exists y \in R: \varphi_x(y) = 1 \Leftrightarrow \exists y \in R: x \cdot y = 1 \Rightarrow$ es ex. Inverses zu x.

Aufgabe 8

a) Sei e neutral bezüglich der Multiplikation.
D.h. $1 = 1 \circ e = 1^2 + e^2 = 1 + e^2$

$\Rightarrow 0 = e^2 \Rightarrow e = 0.$

Allerdings wäre $2 = 2 \circ e = 2 \circ 0 = 2^2 + 0^2 = 4$ ↯.

→ Keine Gruppe!

b) Die Menge $\{(1-t)x + ty \mid t > 0\} \subseteq \mathbb{C}$ entspricht der offenen Halbgeraden, die in x „beginnt" und durch y geht. Die Multiplikation

$$((1-t)x + ty, (1-s)x + sy) \longmapsto x - st(x-y) = (1-st)x + sty$$

ist assoziativ, denn

$$(((1-t)x + ty, (1-s)x + sy), (1-r)x + ry) = ((1-st)x + sty, (1-r)x + ry)$$
$$= (1-rst)x + rsty$$

$$((1-t)x + ty, ((1-s)x + sy, (1-r)x + ry)) = ((1-t)x + ty, (1-rs)x + rsy)$$
$$= (1-rst)x + rsty.$$

Es gibt ein neutrales Element, denn

$$(1-t)x + ty = (1-st)x + sty$$
$$\Leftrightarrow 0 = y(st-t) + x(1-st-1+t)$$
$$= y(s-1)t + x(1-s)t$$
$$= (y(s-1) + x(1-s))t$$
$$\overset{t \neq 0}{\Rightarrow} y(s-1) - x(s-1) = 0$$
$$\Rightarrow (y-x)(s-1) = 0 \Rightarrow y = x \vee s = 1$$

Der Fall $x = y$ ist uninteressant, da die „Gerade" dann ebenfalls nur aus einem Element besteht und dann offensichtlich eine Gruppe ist.

~~Beh:~~ Das neutrale Element wird beim Parameter $s=1$ angenommen. Das wäre $e=(1-1)x+1y=y$.
Für $s=1$ ist das Element auf jeden Fall neutral bzgl. der Verknüpfung.

Das Inverse zu $\frac{z}{xz}=(1-t)x+ty$ wäre ein $z'=(1-t')x+t'y$ mit $(1-tt')x+tt'y=y$. Setze $t':=t^{-1}$.
t' erfüllt die Gleichung und wegen $t>0$ ist $t'=t^{-1}$ auch größer 0. Das Inverse von z erhält man also durch Invertieren des Parameters von z.

Insgesamt ist die Gerade mit der Verknüpfung eine (abelsche) Gruppe.