A.1.10.1 (a) Gibt es eine Gruppe mit genau einem Element? Gibt es einen Körper mit genau einem Element?

(b) Stelle die Verknüpfungstafeln der Restklassenkörper $\mathbb{Z}_2$, $\mathbb{Z}_3$ und $\mathbb{Z}_5$ auf.

(c) Löse durch probieren die quadratische Gleichung $x^2 + x + \bar{1} = \bar{0}$ in $\mathbb{Z}_2$, $\mathbb{Z}_3$ und $\mathbb{Z}_5$. In welchen Fällen lässt sich die aus der Schule geläufige Lösungsformel für quadratische Gleichungen anwenden?

(a) Ja, es gibt eine Gruppe mit genau einem Element. Diese Gruppe lautet $(\{e\}, \cdot)$, wobei e das neutrale Element ist. Das gilt jedoch nicht für Körper, da der kleinste mögliche Körper bloß die Elemente 0 und 1 enthält.

(b) Die Elemente dieser Körper sind Äquivalenzklassen.

- $\mathbb{Z}_2$:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $\mathbb{Z}_3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- $\mathbb{Z}_5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(c) Keine Lösung

$x = \bar{1} \Rightarrow \bar{1}^2 + \bar{1} + \bar{1}$
$= \bar{3} = \bar{0}$

(genau) eine Lösung

Keine Lösung

A1.10.2 (a) Sei $n \in \mathbb{N}$ und $\sqrt{n} \in \mathbb{R}^+ \cup \{0\}$. Beweise: $\mathbb{Q}(\sqrt{n}) := \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{R}$.

Beweis: Um zu zeigen, dass $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{R}$, gehen wir in 4 Schritten vor:

- $(\mathbb{Q}(\sqrt{n}), +)$ ist eine abel'sche Gruppe:

$((a + b\sqrt{n}) + (c + d\sqrt{n})) + (e + f\sqrt{n}) =$
$(a + b\sqrt{n}) + ((c + d\sqrt{n}) + (e + f\sqrt{n}))$, also gilt Assoziativität.
$(0 + 0\sqrt{n}) = 0 \in \mathbb{Q}(\sqrt{n})$, also ist 0 das neutrale Element, weil
$a + b\sqrt{n} + 0 = a + b\sqrt{n}$.
$(a + b\sqrt{n}) - (a + b\sqrt{n}) = 0$ und daher ist $-a - b\sqrt{n}$ das inverse Element von $a + b\sqrt{n}$.
$(a + b\sqrt{n}) + (c + d\sqrt{n}) = (c + d\sqrt{n}) + (a + b\sqrt{n})$ zeigt die Kommutativität.

- $(\mathbb{Q}(\sqrt{n}) \setminus \{0\}, \cdot)$ ist eine abel'sche Gruppe:

$((a + b\sqrt{n}) \cdot (c + d\sqrt{n})) \cdot (e + f\sqrt{n}) = (a + b\sqrt{n}) \cdot ((c + d\sqrt{n}) \cdot (e + f\sqrt{n}))$, also gilt Assoziativität.
$(1 + 0\sqrt{n}) = 1 \in \mathbb{Q}(\sqrt{n}) \setminus \{0\}$, also ist 1 das neutrale Element, weil
$(a + b\sqrt{n}) \cdot 1 = (a + \sqrt{n})$.
$(a + b\sqrt{n}) \cdot (a + b\sqrt{n})^{-1} = 1$ und daher ist $(a + b\sqrt{n})^{-1}$ das inverse Element von $a + b\sqrt{n}$ (, wobei $a + b\sqrt{n} = 0 \notin \mathbb{Q}(\sqrt{n}) \setminus \{0\}$).
$(a + b\sqrt{n}) \cdot (c + d\sqrt{n}) = (c + d\sqrt{n}) \cdot (a + b\sqrt{n})$ zeigt die Kommutativität.

- Das Distributivgesetz gilt zwischen $\cdot$ und $+$:

$(a + b\sqrt{n}) \cdot ((c + d\sqrt{n}) + (e + f\sqrt{n})) =$
$(a + b\sqrt{n})(c + d\sqrt{n}) + (a + b\sqrt{n})(e + f\sqrt{n})$

- $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{R}$:

Nachdem $\mathbb{Q} \subseteq \mathbb{R}$ folgt $a, b \in \mathbb{Q} \Rightarrow a, b \in \mathbb{R}$. Weiters ist $\mathbb{R}^+ \subseteq \mathbb{R}$, also $\sqrt{n} \in \mathbb{R}^+ \Rightarrow \sqrt{n} \in \mathbb{R}$. Weil der Körper $\mathbb{R}$ durch die Operationen $+$ und $\cdot$ abgeschlossen ist, gilt also $a + b\sqrt{n} \in \mathbb{Q}(\sqrt{n}) \Rightarrow a + b\sqrt{n} \in \mathbb{R}$

Anhang: $+$ und $\cdot$ sind im Körper $\mathbb{Q}(n)$ auch abgeschlossen, da $(a + b\sqrt{n}) + (c + d\sqrt{n}) = (a + b) + ((b + d)\sqrt{n}) \in \mathbb{Q}(\sqrt{n})$ und $(a + b\sqrt{n})(c + d\sqrt{n}) = ac + ad\sqrt{n} + b\sqrt{n}c + b\sqrt{n}d\sqrt{n} =$ $(ac + bdn) + ((ad + bc)\sqrt{n}) \in \mathbb{Q}(\sqrt{n})$, weil $n \in \mathbb{N} \subseteq \mathbb{Q}$. □

A 1.10.9 Gegeben sei die komplexen Zahl

$$v = \frac{1}{2}(1 + \sqrt{3}\,i).$$

(a) Berechne $|v|$, v^2 und v^3. Gib dann für alle $n \in \mathbb{Z}$ die komplexen Zahlen v^n an. (Alle gesuchten komplexen Zahlen sollen so wie v durch ihren Real- und Imaginärteil festgelegt werden.)

(b) Zeige $|v^n| = 1$ für alle $n \in \mathbb{Z}$.

Hinweis: In der Gaußschen Zahlenebene bilden die Zahlen $1, v, v^2, \ldots, v^5$ ein regelmäßiges Sechseck mit der Seitenlänge 1 (Abbildung 1.8). Das darf nicht zur Herleitung der Ergebnisse verwendet werden, wohl aber zur anschaulichen Kontrolle der Rechnungen.

(a) $v = 1/2 + \sqrt{3}\,i/2$ und daher $|v| = \sqrt{(1/2)^2 + \left(\frac{\sqrt{3}}{2}\right)^2}$
$= \sqrt{1/4 + 3/4} = \sqrt{1} = 1.$

Weiters ist $v^2 = (1/2 + \sqrt{3}\,i/2)^2 = 1/4 + 2 \cdot 1/2 \cdot \sqrt{3}\,i/2 + \left(\frac{\sqrt{3}\,i}{2}\right)^2$
$= 1/4 + \sqrt{3}\,i/2 + {}^{-3}/_{4} = -1/2 + \sqrt{3}\,i/2$ und
$v^3 = v^2 \cdot v = (-1/2 + \sqrt{3}\,i/2)(1/2 + \sqrt{3}\,i/2) = -1/4 - 1/2 \cdot \frac{\sqrt{3}\,i}{2} +$
$\sqrt{3}\,i/2 \cdot 1/2 + (\sqrt{3}\,i/2)^2 = -1/4 - 3/4 = -1$. Aber
$v^4 = v^3 \cdot v = -1 \cdot v$ und $v^5 = v^3 \cdot v^2 = -1 \cdot v^3$ und
$v^6 = v^3 \cdot v^3 = (-1) \cdot (-1) = 1$ ... und $v^7 = v^6 \cdot v = 1 \cdot v$
$= v$. Daher ist $v^n = v^{n \bmod 6}$.

(b) Um $|v^n| = 1$ für alle $n \in \mathbb{Z}$ zu zeigen, genügt es, zu sehen, dass $|v| = 1$ und $|v^{n+1}| = |v^n| \cdot |v| = |v^n| \cdot 1 = |v^n|$.

A I.II.1 Beweise: Die Abbildung $\Psi: \mathbb{C}^+ \to \mathbb{R}^+ : z \to |z|$ ist ein surjektiver Gruppenhomomorphismus von $(\mathbb{C}^\times, \cdot)$ auf $(\mathbb{R}^\times, \cdot)$. Bestimme ferner $\ker \Psi$, die Nebenklassen des Kerns in $\mathbb{C}^\times$ und veranschauliche die Ergebnisse in der Gaußschen Zahlenebene.

Beweis: Die Multiplikation muss durch Ψ in $\mathbb{R}^\times$ erhalten bleiben, also $\Psi(x \cdot y) = \Psi(x) \cdot \Psi(y)$, wenn $x := a + bi$ und $y := c + di$.

$\Psi(x \cdot y) = \Psi((a+bi)(c+di)) = \Psi(ac + adi + bic - bd)$

$= \Psi((ac - bd) + (ad + bc)i) = \sqrt{(ac - bd)^2 + (ad + bc)^2} =$

$= \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2}$ und

$\Psi(x) \cdot \Psi(y) = \sqrt{a^2 + b^2} \cdot \sqrt{c^2 + d^2} = \sqrt{(a^2+b^2)(c^2+d^2)} =$

$= \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2}$ und somit gilt tatsächlich

$\Psi(x \cdot y) = \Psi(x) \cdot \Psi(y)$.

Ψ ist surjektiv, weil $\mathbb{R}^+ \subseteq \mathbb{C}^+$, siehe $x \in \mathbb{R}^\times$ und $x = x + 0i \subseteq \mathbb{C}^+$. Also $|x + 0i| = x$, weil $x > 0$. □

$\ker \Psi$ ist die Menge jener Elemente aus $\mathbb{C}^+$, die auf das neutrale Element $1 \in (\mathbb{R}^\times, \cdot)$ abgebildet werden, d.h.

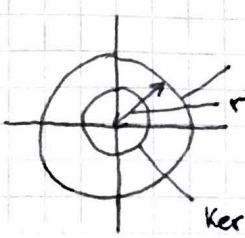
$\ker \Psi = \{z \in \mathbb{C}^\times : |z| = 1\}$, genauer $z = a + bi$ und

$|a + bi| = 1 \Rightarrow \sqrt{a^2 + b^2} = 1 \Rightarrow a^2 + b^2 = 1 \Rightarrow a^2 = 1 - b^2$

$\Rightarrow a = \pm\sqrt{1 - b^2}$, wobei $b \in [-1, 1]$, also

$\ker \Psi = \{a + bi \in \mathbb{C}^\times : b \in [-1, 1] \wedge a = \pm\sqrt{1 - b^2}\}$.

Eine beliebige Nebenrestklasse von $\ker \Psi$ lautet $r \cdot \ker \Psi = \{z \in \mathbb{C}^\times : |z| = |r|\}$. Der Betrag von r wird verwendet, weil $r \in \mathbb{C}^\times$ möglich ist



A 1.11.6 Es seien G eine Gruppe und $U \subset G$ eine Untergruppe. Nach 1.11.10 ist die Relation $\sim_U$ mit $a \sim_U b$ genau für $ab^{-1} \in U$ eine Äquivalenzrelation auf G.

(a) Beweise, dass alle Äquivalenzklassen von $\sim_U$ gleichmächtig sind.

(b) Leite aus (a) den folgenden Satz von Lagrange[5] ab: Ist U eine Untergruppe einer endlichen Gruppe G, so ist $\#U$ ein Teiler von $\#G$.

Beweis: Um zu zeigen, dass alle Äquivalenzklassen gleichmächtig sind, müssen wir eine Bijektion zwischen zwei beliebigen Äquivalenzklassen finden. Sollten zwei $[a]_{\sim_U} \cap [b]_{\sim_U} \neq \emptyset$, dann ist diese Bijektion bloß die Identität. Sind diese aber disjunkt, so gehen wir wie folgt vor

$$[a]_{\sim_U} = \{x : x \sim_U a\} = \{x : xa^{-1} \in U\}$$

Aufgrund der Definition einer Nebenklasse Ua, die Menge aller Elemente $u \in U$, punktweise multipliziert mit a, folgt $xa^{-1} \in U \Leftrightarrow (xa^{-1})a \in Ua \Leftrightarrow x \in Ua$. Deswegen ist $[a]_{\sim_U} = Ua$. Weiters ist $Ue = U$.
Wir stellen also eine Bijektion $Ua \xrightarrow{\Psi} Ub = Ua \xrightarrow{f_1} Ue \xrightarrow{f_2} Ub$ auf, wobei $f_1 : x \mapsto x \cdot a^{-1}$ und $f_2 : x \mapsto x \cdot b$, sowie $f_1^{-1} : x \mapsto x \cdot a$ und $f_2^{-1} : x \mapsto x \cdot b^{-1}$. Also ist Ψ tatsächlich bijektiv und Ua und Ub bzw. $[a]_{\sim_U}$ und $[b]_{\sim_U}$ gleichmächtig.

Es ist uns, nach dem Auswahlaxiom, möglich, aus jeder Äquivalenzklasse genau eine Repräsentante auszuwählen, und diese in der Menge R zusammenzufassen. Die Anzahl der Äquivalenzklassen entspricht also $\#R \in \mathbb{N}$. Weil $[e]_{\sim_U} = Ue = U$, besitzt die Äquivalenzklasse $[e]_{\sim_U}$ die Mächtigkeit $\#U$, also auch alle anderen Äquivalenzklassen.

$$\bigcup_{a \in G} [a]_{\sim_U} = G$$

Daher gilt $\#R \cdot \#U = \#G$ und $\#U$ teilt $\#G$. $\square$

A 1.11.9 Es seien G, G', G'' Gruppen und $\Psi: G \to G'$ sowie $\Psi': G' \to G''$ Homomorphismen. Beweise:

(a) Für die neutralen Elemente e, e' von G bzw. G' gilt $\Psi(e) = e'$.

(b) $\Psi(a^{-1}) = (\Psi(a))^{-1}$ für alle $a \in G$.

(c) Ist Ψ ein Isomorphismus, so ist Ψ^{-1} ebenfalls ein Isomorphismus.

(d) Die zusammengesetzte Abbildung $\Psi' \circ \Psi: G \to G''$ ist ein Homomorphismus.

Beweis: $\Psi(a+b) = \Psi(a) \cdot \Psi(b) \Leftrightarrow \Psi(e+e) = \Psi(e) \cdot \Psi(e)$
$\Leftrightarrow \Psi(e) = \Psi(e) \cdot \Psi(e) \Leftrightarrow \Psi(e) = \Psi(e) \cdot e' \Leftrightarrow \Psi(e) = e'$
und $\Psi(a-a) = \Psi(a) \cdot \Psi(-a) = e' \Leftrightarrow \Psi(-a) = (\Psi(a))^{-1}$,
wodurch (a) und (b) gelten.
Damit (c) gilt, muss Ψ^{-1} bijektiv sein und mit den Rechenoperationen verträglich sein. Da Ψ bijektiv ist, ist Ψ^{-1} ebenfalls bijektiv. $\Psi^{-1}(\Psi(a) \cdot \Psi(b)) = \Psi^{-1}(\Psi(a+b)) =$
$a + b = \Psi^{-1}(\Psi(a)) + \Psi^{-1}(\Psi(b))$, weil Ψ und Ψ^{-1} bijektiv sind, also $\Psi \circ \Psi^{-1} = id_{G'}$ und $\Psi^{-1} \circ \Psi = id_G$.
Damit (d) gilt, muss $\Psi' \circ \Psi$ verträglich mit den jeweiligen Rechenoperationen sein: $(\Psi' \circ \Psi)(a+b) = \Psi'(\Psi(a+b)) =$
$\Psi'(\Psi(a) \cdot \Psi(b)) = \Psi'(\Psi(a)) * \Psi'(\Psi(b)) =$
$(\Psi' \circ \Psi)(a) * (\Psi' \circ \Psi)(b)$

□

1.11. x Entscheiden Sie, welche folgenden Aussagen a, 6, c, d für alle Gruppen G gelten. Finden Sie für jede der Aussagen, die NICHT für alle Gruppen gilt, ein Gegenbeispiel (also eine Gruppe und einen Homomorphismus, für die die Aussage nicht gilt)

a. Jeder Homomorphismus $f: G \to G$ ist surjektiv.

6. Jeder Homomorphismus $f: G \to G$ ist injektiv.

c. Für alle Homomorphismen $f: G \to G$ gilt: wenn f surjektiv ist, dann ist $\ker(f)$ leer.

d. Für alle Homomorphismen $f: G \to G$ gilt: wenn f surjektiv ist, dann ist $\ker(f)$ nicht leer.

Betrachte den Homomorphismus $f: G \to G: x \mapsto e$, wobei e das neutrale Element von G ist.

a. f ist nicht notwendigerweise surjektiv, da $\{e\} \subsetneq G$ möglich ist.

6. —"— injektiv —"—

c. Angenommen, $f: G \to G$ ist ein Automorphismus, dann ist $\ker(f) = \{x\}$, mit $x \in G$, also nichtleer.

d. Wenn der Homomorphismus $f: G \to G$ surjektiv ist, dann gilt $f(G) = G$ und somit Injektivität (und Bijektivität). Daher ist f ein Automorphismus und $\ker(f)$ ist nichtleer.