Lösungsvorschläge

Die Mathe1-Tutoren

15. März 2012

Aufgabe 1 Mengen und Relationen

a) Gegeben sei die übliche Ordnungsrelation $\leq$ auf der Menge $\{1, 2, 3, 4, 5\}$. Wieso ist diese Relation keine Äquivalenzrelation?

Lösungsvorschlag:

Die übliche Ordnungsrelation $\leq$ hat folgende Eigenschaften:

1. reflexiv: $\forall x \in \{1, 2, 3, 4, 5\} : \ x \leq x$
2. anti-symetrisch: $\forall x, y \in \{1, 2, 3, 4, 5\} : \ (x \leq y \wedge y \leq x) \Rightarrow x = y$
3. transitiv: $\forall x, y, z \in \{1, 2, 3, 4, 5\} : \ (x \leq y \wedge y \leq z) \Rightarrow x \leq z$

Eine Äquivalenzrelation R auf einer Menge M hat (hingegen) folgende Eigenschaften:

1. reflexiv: $\forall x \in M : \ xRx$
2. symmetrisch: $\forall x, y \in M : \ (xRy) \Rightarrow yRx$
3. transitiv: $\forall x, y, z \in M : \ (xRy \wedge yRz) \Rightarrow xRz$

Somit kann der Grund, dass $\leq$ keine Äquivalenzrelation ist, nur die zweite Eigenschaft der Äquivalenzrelation (Symmetrie) sein (die anderen sind gleich, und somit erfüllt die Ordnungsrelation $\leq$ diese a priori).

Als Nachweis, dass die Symmetrie nicht erfüllt ist, reicht folgendes:
$2 \leq 3$, aber $3 \not\leq 2$, da ansonsten wegen der Anti-Symmetrie von $\leq$ folgen würde $2 = 3$, was ein Widerspruch ist.

b) Sei M eine Menge, auf der eine Äquivalenzrelation gegeben ist und seien $x, y \in M$. Zeigen Sie, dass $\overline{x} \neq \overline{y} \Rightarrow \overline{x} \cap \overline{y} = \emptyset$.

Lösungsvorschlag:

Erste Möglichkeit: Beweis via Kontraposition d. h. zu zeigen ist: $\overline{x} \cap \overline{y} \neq \emptyset \Rightarrow \overline{x} = \overline{y}$

Aus $\overline{x} \cap \overline{y} \neq \emptyset$ folgt, dass ein $w \in M$ mit $w \in \overline{x} \cap \overline{y}$ existiert, d h.

$$\begin{aligned} & \exists w \in M : w \in \{z \in M | xRz\} \cap \{z \in M | yRz\} \\ \Rightarrow\ & \exists w \in M : w \in \{z \in M | xRz\} \wedge w \in \{z \in M | yRz\} \\ \Rightarrow\ & \exists w \in M : xRw \wedge yRw \\ \Rightarrow\ & \exists w \in M : xRw \wedge wRy \\ \Rightarrow\ & xRy \text{ (mit Symmetrie: } yRx) \end{aligned}$$

Damit gilt (mit Symmetrie, da R eine Äquivalenzrelation ist):

$$\begin{aligned} & y \in \overline{x} \\ \Rightarrow & \forall z_x \in \overline{x} : xRz_x \wedge yRx \\ \overset{trans.}{\Rightarrow} & \forall z_x \in \overline{x} : yRz_x \\ \Rightarrow & \forall z_x \in \overline{x} : z_x \in \overline{y} \\ \Rightarrow & \overline{x} \subset \overline{y} \end{aligned} \qquad \begin{aligned} & x \in \overline{y} \\ \Rightarrow & \forall z_y \in \overline{y} : yRz_y \wedge xRy \\ \overset{trans.}{\Rightarrow} & \forall z_y \in \overline{y} : xRz_y \\ \Rightarrow & \forall z_y \in \overline{y} : z_y \in \overline{x} \\ \Rightarrow & \overline{y} \subset \overline{x} \end{aligned}$$

Damit: $\overline{x} = \overline{y}$ und somit ist die zu zeigende Aussage bewiesen, und somit auch die Behauptung: $\overline{x} \neq \overline{y} \Rightarrow \overline{x} \cap \overline{y} = \emptyset$ nach den uns bekannten logischen Regeln (Falls p und q Aussagen sind, dann gilt: $(p \rightarrow q) \ \leftrightarrow (\neg q \rightarrow \neg p)$).

Zweite Möglichkeit: Widerspruchsbeweis d. h. zu zeigen ist: Unter Voraussetzung von $\overline{x} \neq \overline{y}$ (d. h. die Aussage $\overline{x} \neq \overline{y}$ ist wahr) ist folgende zusammengesetze Aussage falsch: $(\overline{x} \neq \overline{y}) \wedge (\overline{x} \cap \overline{y} \neq \emptyset)$

Voraussetzung ist: $\overline{x} \neq \overline{y}$

Annahme: $\overline{x} \cap \overline{y} \neq \emptyset$

Somit existiert ein $w \in M$ mit $w \in \overline{x} \cap \overline{y}$, das heisst

$$\begin{aligned} & \exists w \in M : w \in \{z \in M | xRz\} \cap \{z \in M | yRz\} \\ \Rightarrow\ & \exists w \in M : w \in \{z \in M | xRz\} \wedge w \in \{z \in M | yRz\} \\ \Rightarrow\ & \exists w \in M : xRw \wedge yRw \\ \Rightarrow\ & \exists w \in M : xRw \wedge wRy \\ \Rightarrow\ & xRy \text{ (mit Symmetrie: } yRx) \end{aligned}$$

Damit gilt (mit Symmetrie):

$$\begin{aligned} & y \in \overline{x} \\ \Rightarrow\ & \forall z_x \in \overline{x} : xRz_x \wedge yRx \\ \overset{trans.}{\Rightarrow} & \forall z_x \in \overline{x} : yRz_x \\ \Rightarrow\ & \forall z_x \in \overline{x} : z_x \in \overline{y} \\ \Rightarrow\ & \overline{x} \subset \overline{y} \end{aligned} \qquad \begin{aligned} & x \in \overline{y} \\ \Rightarrow\ & \forall z_y \in \overline{y} : yRz_y \wedge xRy \\ \overset{trans.}{\Rightarrow} & \forall z_y \in \overline{y} : xRz_y \\ \Rightarrow\ & \forall z_y \in \overline{y} : z_y \in \overline{x} \\ \Rightarrow\ & \overline{y} \subset \overline{x} \end{aligned}$$

Damit: $\overline{x} = \overline{y}$ im Widerspruch zur Vorraussetzung $\overline{x} \neq \overline{y}$

Somit folgt die Behauptung: $(\overline{x} \neq \overline{y}) \Rightarrow (\overline{x} \cap \overline{y} = \emptyset)$.

Aufgabe 2 Natürliche Zahlen

a) Nennen Sie die Peano Axiome.

Lösungsvorschlag:

Es gibt eine Menge $\mathbb{N}$ mit einem Element $1 \in \mathbb{N}$ und einer Abbildung $S : \mathbb{N} \to \mathbb{N}$, sodass

1. S ist injektiv aber nicht surjektiv, und $1 \notin S(\mathbb{N})$.
2. Ist $M \subset \mathbb{N}$ und gilt
   a) $1 \in M$ und
   b) $n \in M \Rightarrow S(n) \in M$,

   so ist $M = \mathbb{N}$. (Induktionsaxiom)

b) Wie lautet die rekursive Definition der Addition in den natürlichen Zahlen?

Lösungsvorschlag:

Für $m, n \in \mathbb{N}$ setzt man

a) $m + 1 := S(m)$ und

b) $m + S(n) := S(m + n)$.

c) Zeigen Sie durch Induktion: $\forall\, n \in \mathbb{N} :\ n + 1 = 1 + n$. Beim Beweis dürfen Sie das Assoziativgesetz der Addition, aber natürlich nicht das Kommutativgesetz benutzen.

Lösungsvorschlag:

Beweis durch vollständige Induktion:

Induktionsanfang: Die Behauptung soll für $n = 1$ gezeigt werden:

$$1 + 1 = 1 + 1$$

Dies ist offensichtlich eine wahre Aussage.

Induktionsvoraussetzung: $\exists\, n \in \mathbb{N} :\ n + 1 = 1 + n$

Induktionsschritt: $(n \to n+1)$
Die Behauptung soll nun unter der Induktionsvoraussetzung für $n+1$ gezeigt werden. Zu zeigen ist also:

$$(n+1)+1 = 1+(n+1)$$

Beweis für den Induktionsschritt:

$$(n+1)+1 \overset{\text{IV angewandt}}{=} (1+n)+1 \overset{\text{Assoziativgesetz angewandt}}{=} 1+(n+1)$$

Damit wurde die Behauptung bewiesen.

Kommentare:

- In dieser Induktion hatten irgendwelche Summen überhaupt nichts zu suchen!
- Das Assoziativgesetz ist nicht die Induktionsvoraussetzung, es darf einfach so benutzt werden.
- Die Induktionsvoraussetzung kann erst **nach** dem Induktionsanfang gemacht werden, da erst im Induktionsanfang gezeigt wurde, dass tatsächlich mindestens ein solches $n \in \mathbb{N}$ existiert, vorher nicht.
- Es muss in der Induktionsvoraussetzung auf jeden Fall $\exists$-Quantor und **kein** $\forall$-Quantor stehen, da bisher nur bekannt ist, dass die Aussage in mindestens einem Fall gilt, aber es wurde noch nicht gezeigt, dass diese Aussage immer stimmt.
  (Außerdem würde man keinen Induktionsschritt mehr benötigen, wenn der $\forall$-Quantor in der Induktionsvoraussetzung richtig wäre.)
- Im Induktionsschritt soll von n auf $n+1$ geschlossen werden. Dies bedeutet nicht, dass $n = n+1$ ist, denn diese Aussage ist immer falsch, z. B. ist $3 = 4$ eine falsche Aussage.
- Der Beweis im Induktionsschritt konnte auch wie folgt aufgeschrieben werden. (Umformungen jeweils auf der rechten Seite der Gleichung):

$$\begin{aligned} & (n+1)+1 = 1+(n+1) \\ \overset{Asso}{\Leftrightarrow} \quad & (n+1)+1 = (1+n)+1 \\ \overset{IV}{\Leftrightarrow} \quad & (n+1)+1 = (n+1)+1 \qquad \text{(wahre Aussage)} \end{aligned}$$

  Hierbei ist jedoch zu beachten, dass die Äquivalenzumformungen auf jeden Fall auch für die Rückrichtung gelten müssen, da am Anfang der Umformungen die Behauptung und am Ende die wahre Aussage steht.

d) Die Dezimalzahl 1234 soll ins Stellensystem zur Basis 7 umgerechnet werden.
Schreiben Sie diese Zahl im Stellensystem zur Basis 7. Dokumentieren Sie Ihre Rechnung.

Lösungsvorschlag:

Erste Möglichkeit: Es wird jeweils eine Division mit Rest durchgeführt (hier ohne Nebenrechnungen), die Lösung setzt sich dann aus den Resten in umgekehrter Reihenfolge zusammen:

$$\begin{aligned} 1234 \div 7 &= 176 && \text{Rest } 2 \\ 176 \div 7 &= 25 && \text{Rest } 1 \\ 25 \div 7 &= 3 && \text{Rest } 4 \\ 3 \div 7 &= 0 && \text{Rest } 3 \end{aligned}$$

Das Ergebnis ist also folgendes:

$$1234_{10} = 3412_7$$

Zweite Möglichkeit: Es werden die Potenzen von 7 ausgerechnet und (angefangen bei der größten) ermittelt, welche wie oft in die Zahl 1234 „hineinpasst“ und welcher Rest übrig bleibt.

$$7^0 = 1 \qquad 7^1 = 7 \qquad 7^2 = 49 \qquad 7^3 = 343 \qquad 7^4 = 2401 \qquad \ldots$$

Da bereits 7^4 größer als 1234 ist, wird mit 7^3 angefangen:

$$\begin{aligned} 1234 &= 3 \cdot 343 + 205 \\ 205 &= 4 \cdot 49 + 9 \\ 9 &= 1 \cdot 7 + 2 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Es ist also

$$1234_{10} = 3 \cdot 7^3 + 4 \cdot 7^2 + 1 \cdot 7^1 + 2 \cdot 7^0 = 3412_7$$

Aufgabe 3 Gruppentheorie

a) Geben Sie ein Beispiel für eine nicht-kommutative Gruppe und führen Sie dann den Beweis, dass Ihre Gruppe nicht kommutativ ist

Lösungsvorschlag:

Standardbeispiele einer solchen Gruppe $G = (M, \circ)$ sind die symmetrische Gruppe S_n mit $n = 3$ oder $n = 4$, sowie die Matrixmultiplikation der invertierbaren, quadratischen

Matrizen, d. h. $M = \mathrm{GL}_n(\mathbb{K})$. Dabei kann $\mathbb{K}$ ein beliebiger Körper sein. Für diese Standardgruppen muss man auch nicht mehr argumentieren, dass es sich um eine Gruppe handelt.

Nun muss man noch durch Gegenbeispiel beweisen, dass G nicht-kommutativ ist: Seien $A, B \in G$, dann ist G nicht-kommutativ, wenn ein Beispiel mit $A \circ B \neq B \circ A$ existiert.

Gegenbeispiel in der S_3: Für $A = (132) \in S_3$ und $B = (12) \in S_3$ gilt:

- $X_1 = A \circ B : (132) \circ (12) = (23)$ und
- $X_2 = B \circ A : (12) \circ (132) = (13)$.

Da $X_1 \neq X_2$ folgt, dass G nicht-kommutativ ist.

Gegenbeispiel in der $\mathrm{GL}_2(\mathbb{R})$: Für $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ gilt:

- $C = A \cdot B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ und
- $D = B \cdot A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Da $C \neq D$ folgt, dass G nicht-kommutativ ist.

b) Definieren Sie den Begriff „Normalteiler“.

Lösungsvorschlag:

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe von G. Dann ist U einNormalteiler von G, wenn für alle $g \in G$ die Linksnebenklasse gleich der Rechtsnebenklasse ist, d. h. $gU = Ug$ mit $gU = \{gu \mid u \in U\}$.

Eine dazu äquivalente Definition ist:

$$\forall\, g \in G \,\forall\, u \in U : gug^{-1} \in U$$

Es gibt noch weitere Definitionen die äquivalent dazu sind. Die Wikipedia Seite dazu ist sehr gut: `http://de.wikipedia.org/wiki/Normalteiler`.

c) Zeigen Sie, dass in einer kommutativen Gruppe jede Untergruppe Normalteiler ist.

Lösungsvorschlag:

Sei G eine kommutative Gruppe und $U \subseteq G$ eine Untergruppe. Zu zeigen ist, dass für alle $g \in G$ und alle $u \in U$ die Aussage $gug^{-1} \in U$ gilt.

Seien also $g \in G, u \in U$ beliebig, dann gilt:

$$gug^{-1} \overset{\text{da } G \text{ kommutativ}}{=} gg^{-1}u \overset{\text{Def. inv. Elem.}}{=} eu \overset{\text{Def. neutrales Elem.}}{=} u$$

d) Definieren Sie die Ordnung eines Elements $a \in G$ (geschrieben $\mathrm{ord}(a)$ oder $\mathrm{ord}_G(a)$).

Lösungsvorschlag:

Erste Möglichkeit: Die Ordnung eines Elements $a \in G$ einer Gruppe G ist die Anzahl der Elemente der von a erzeugten Untergruppe. Kurz $\mathrm{ord}(a) = |\langle a \rangle|$.

Zweite Möglichkeit: Die Ordnung eines Elements $a \in G$ einer Gruppe G ist die kleinste natürliche Zahl $n \geq 1$, für die $a^n = e$ gilt, wobei $e \in G$ das neutrale Element von G ist. Existiert keine solche, so ist $\mathrm{ord}(a) = \infty$.

e) Sei n eine natürliche Zahl. Beweisen Sie, daß aus der Gleichung $a^n = e$ folgt, dass die Ordnung von a ein Teiler von n ist. (e sei das neutrale Element der Gruppe G.)

Lösungsvorschlag:

Vorbemerkung: Dass die Ordnung von a ein Teiler ist, heißt es gilt $n = \mathrm{ord}(a)$ oder existiert ein $k \in \mathbb{N}$ mit $\mathrm{ord}(a) \cdot k = n$.

Außerdem sei im Folgenden das Gruppenelement $a \in G$ gegeben und fest gewählt.

Man betrachte zunächst die Potenzen von a genauer:

$\langle a \rangle = \{a^1, a^2, \ldots, a^{\mathrm{ord}(a)}\}$ nach Definition der Ordnung von a, d.h. insbesondere $a^j \neq e$ für $j \in \{1, \ldots, \mathrm{ord}(a) - 1\}$

(I) Es gilt:

$$a^j \neq a^i \text{ für } i, j \in \{1, \ldots, \mathrm{ord}(a)\} \text{ und } j \neq i \tag{1}$$

Dies ist entweder direkt (mit kleiner Begründung) ersichtlich aus der Definition der Ordnung ($\mathrm{ord}(a) = \#\langle a \rangle$), besser wäre eine Begründung im Stile von:

Annahme: $a^j = a^i$ für $i, j \in \{1, \ldots, \mathrm{ord}(a)\}$ und $j \neq i$.

Dann gilt: $a^j \cdot a^{-i} = a^{j-i} = e$

Fall 1: $j - i = 0$
$\Rightarrow j = i$ im Widerspruch zur Annahme ($i \neq j$).

Fall 2: $j - i = \mathrm{ord}(a)$
$\Rightarrow i = 0$ oder $j > \mathrm{ord}(a)$ im Widerspruch zur Annahme ($i, j \in \{1, \ldots, \mathrm{ord}(a)\}$).

Fall 3: $j - i = -ord(a)$
$\Rightarrow j = 0$ oder $i > \mathrm{ord}(a)$ im Widerspruch zur Annahme ($i, j \in \{1, \ldots, ord(a)\}$).

(II) Für $m \in \mathbb{N}_0$ mit $m = k \cdot \text{ord}(a) + r$, $k \in \mathbb{Z}, 0 \leq r < \text{ord}(a)$ gilt:

$$a^m = a^{k \cdot \text{ord}(a)+r} = a^{k \cdot \text{ord}(a)} \cdot a^r = (a^{\text{ord}(a)})^k \cdot a^r = e^k \cdot a^r = a^r \qquad (2)$$

Somit kann man Potenzen von a modulo $\text{ord}(a)$ betrachten (d. h. $a^m = a^{m \mod \text{ord}(a)} \in \{a^1, a^2, \ldots, a^{ord(a)}\}$).

(III) **Nutzen der Vorrausetzung:** Nachdem die Vorbetrachtungen abgeschlossen sind, betrachten wir nun die natürliche Zahl n (d. h. $0 < n$) mit der Eigenschaft $a^n = e$:

Fall 1: $n = \text{ord}(a)$

Dann gilt offensichtlich, dass $\text{ord}(a)$ ein Teiler von n ist.

Fall 2: $0 < n < \text{ord}(a)$

Dann gilt: $a^n = e = a^{\text{ord}(a)}$ mit $n \in \{1, \ldots, \text{ord}(a)\}$ und $n \neq \text{ord}(a)$ im Widerspruch zu (1)!

Fall 3: $n > \text{ord}(a)$

Sei $r = n \mod \text{ord}(a)$, dann gilt nach (2): $a^n = a^r = e$ mit $0 \leq r < \text{ord}(a)$. Nach (1) muss also gelten: $r = 0$.

Damit folgt: $n = k \cdot \text{ord}(a) + r = k \cdot \text{ord}(a) + 0 = k \cdot \text{ord}(a)$, d. h. n ist ein Vielfaches von $\text{ord}(a)$ bzw. $\text{ord}(a)$ ist ein Teiler von n.

Wonach wurde gesucht?

Bei der Aufgabe war es wichtig die Punkte (1) und (2) zu erwähnen (am besten zu begründen) und die Erkenntnis auf die „spezielle“ natürliche Zahl n (d. h. die natürliche Zahl n mit der Eigenschaft $a^n = e$), wie zum Beispiel in (III) geschehen, anzuwenden. In keinster Weise musste solch ein detaillierter Beweis geführt werden, aber zumindest die relevanten Kernpunkte mussten erkannt, genannt und angewendet werden.

Häufigste Fehler:

- Es wurde bewiesen, dass $a^{k \cdot \text{ord}(a)} = e$.
  Dieses Ergebnis folgt sofort aus den Potenzgesetzen (siehe 4g):

  $$a^{k \cdot \text{ord}(a)} = (a^{\text{ord}(a)})^k = e^k = e$$

  Des Weiteren ist diese Aussage für den Beweis der Behauptung nicht wichtig!
- Es wurde gezeigt, dass aus „$\text{ord}(a)$ teilt n“ folgt: „$a^n = e$“. Dies ist nicht die zu beweisende Behauptung!
- Es wurde gezeigt: n teilt $\text{ord}(a)$ (n ist eine natürliche Zahl), falls $a^n = e$.
  Dies gilt für $n \in \mathbb{N}$ nur falls $n = \text{ord}(a)$ und dies ist ein trivialer Spezialfall der zu beweisenden Behauptung. Aber bei einer solchen Löosung wurde gezeigt, dass man die Behauptung falsch verstanden hat.

- Es wurde angenommen, dass $n = \text{ord}(a)$. Dies ist im Allgeinen falsch, da in der Aufgabe n eine beliebige natürliche Zahl war mit der Einschränkung, dass die Gleichung $a^n = e$ erfüllt ist.

f) Bestimmen Sie die Ordnung von 2 in $\mathbb{Z}_{257}^*$. (257 ist Primzahl.)

Lösungsvorschlag:

Erste Möglichkeit: Da 257 eine Primzahl ist, besteht die multiplikative Gruppe $\mathbb{Z}_{257}^*$ aus 256 Elementen: $|\mathbb{Z}_{257}^*| = 256$. Oder allgemein und kurz: p prim $\Rightarrow |\mathbb{Z}_p^*| = p - 1$

Da $|\mathbb{Z}_{257}^*| = 256 = 2^8$ und die Ordnung nach dem Satz von LaGrange ein Teiler der Gruppenordnung sein muss, muss man lediglich die kleinste Zweierpotenz finden, für die $2^{(2^k)} = 1$ in $\mathbb{Z}_{257}$ gilt.

Da außerdem für $1 \leq i \leq 8$ die Ungleichung $2^i < 257$ gilt und wie eben bereits erwähnt die Ordnung einer Zweipotenz sein muss, kann man die nächstgrößere Zweierpotenz einfach ausprobieren. In diesem Fall also 16:

$$2^{16} = 2^{8+8} = 2^8 \cdot 2^8 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot (-1) = 1$$

Also gilt $\text{ord}_{\mathbb{Z}_{257}^*}(2) = 16$.

Zweite Möglichkeit: Man berechne für alle $i \leq 16 : 2^i$ in $\mathbb{Z}_{257}^*$: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$, $2^8 = 256 = -1$

An dieser Stelle hätte man mit den Potenzgesetzen argumentieren können, dass für $8 < i < 16$ gilt:

$$2^i = 2^{8+i'} = 2^8 \cdot 2^{i'} = 256 \cdot 2^{i'} = (-1) \cdot 2^{i'} = -2^{i'}$$

(Hierbei gilt $1 \leq i < 8$). D. h. für $8 < i < 16$ sind ebenfalls ungleich 1 und erst für $i = 16$ liegt die Ordnung vor:

$$2^{16} = 2^{8+8} = 2^8 \cdot 2^8 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot (-1) = 1$$

Ansonsten musste man die Potenzen bis $i = 16$ weiter berechnen:

- $2^9 = 2^{8+1} = 2^8 \cdot 2 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot 2 = -2 = 255$
- $2^{10} = 2^{8+2} = 2^8 \cdot 4 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot 4 = -4 = 253$
- $2^{11} = 2^{8+3} = 2^8 \cdot 8 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot 8 = -8 = 249$
- $2^{12} = 2^{8+4} = 2^8 \cdot 16 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot 16 = -16 = 241$
- $2^{13} = 2^{8+4} = 2^8 \cdot 32 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot 32 = -32 = 225$
- $2^{14} = 2^{8+4} = 2^8 \cdot 64 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot 64 = -64 = 193$

- $2^{14} = 2^{8+4} = 2^8 \cdot 128 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot 128 = -128 = 129$
- $2^{16} = 2^{8+8} = 2^8 \cdot 2^8 = 256 \cdot 256 \overset{256=-1 \text{ in } \mathbb{Z}_{257}^*}{=} (-1) \cdot (-1) = 1$

In beiden Fällen gilt also $\text{ord}_{\mathbb{Z}_{257}^*}(2) = 16$.

Wonach wurde gesucht?
Bei der Aufgabe war es wichtig, dass man das bei der zweiten Möglichkeit das Weglassen der Berechnung bestimmter Potenzen entsprechend begründet. Es reichte nicht einfach

$$2^8 = 256 = -1 \Rightarrow 2^{16} = (-1) \cdot (-1) = 1$$

zu schreiben, da hier einfach jedes Argument fehlt. Insbesondere ist bei dieser Variante oder der stumpfen Auflistung der Potenz das Endergebnis noch einmal deutlich zu machen.

Für alle die sich an der ersten Möglichkeit versucht haben, war es wichtig, deutlich zu machen, warum die Voraussetzungen für die entsprechende Sätze aus der Vorlesung gelten.

In beiden Fällen musste man auf jeden Fall begründen, warum man ggf. die Potenzen für $i \leq 8$ weggelassen hat.

Häufigster Fehler:

- Die Behauptung, dass in einer multiplikativen Gruppe mit Primzahlordnung (was 256 im übrigen nicht ist!) jedes Element ein Erzeuger ist und die Ordnung daher die Primzahl selbst sei, ist **falsch**. In allen $\mathbb{Z}_p$ (p prim) erzeugt -1 offensichtlich immer eine zweielementige Untergruppe.

  Der entsprechende Satz aus der Vorlesung besagt, dass in einer **additiven** Gruppe mit Primzahlordnung jedes von 0 verschiedene Element ein Erzeuger ist.

g) Berechnen Sie $2^{100005} \in \mathbb{Z}_{11}^*$. (Geht schnell.)

Lösungsvorschlag:

Wiederholung der Potenzgesetze:
Sei G Gruppe (multiplikativ) und $n, m \in \mathbb{N}_0, a \in G$, dann gilt:

(PG I) $a^{n+m} = a^n \cdot a^m$

(PG II) $a^{n \cdot m} = (a^n)^m = (a^m)^n$

Wir sehen:

$$2^5 = 32 \overset{\text{in } \mathbb{Z}_{11}^*}{=} 10 = -1 \tag{3}$$

Damit folgt in $\mathbb{Z}_{11}^*$:

$$\begin{aligned}
2^{100005} &\overset{(PGI)}{=} 2^{100000} \cdot 2^5 \\
&\overset{(PGII)}{=} (2^{10})^{10000} \cdot 2^5 \\
&\overset{(PGI)}{=} (2^5 \cdot 2^5)^{10000} \cdot 2^5 \\
&\overset{(3)}{=} ((-1) \cdot (-1))^{10000} \cdot (-1) \\
&\overset{\text{da } R \text{ Ring mit } 1}{=} 1^{10000} \cdot (-1) = 1 \cdot (-1) \\
&= -1
\end{aligned}$$

Häufigste Fehler: Potenzgesetze falsch benutzt und somit eine falsche Zerlegung!

h) Berechnen Sie mit dem Erweiterten Euklidischen Algorithmus 86^{-1} in $\mathbb{Z}_{275}^*$. (Geht schnell.)

Lösungsvorschlag:

Ausgangspunkt: Wir betrachten einen Spezialfall (wie in der Aufgabe gestellt), nämlich, dass folgendes gilt: $0 \leq a < b$

Der erweiterete euklidische Algorithmus berechnet den größten gemeinsamen Teiler zweier natürlicher Zahlen a und b, geschrieben $\text{ggT}(a, b)$, und zwei ganze Zahlen s und t, sodass folgende Gleichung erfüllt ist:

$$\text{ggT}(a, b) = s \cdot a + t \cdot b \tag{4}$$

Falls $\text{ggT}(a, b) = 1$, dann gilt $a \in \mathbb{Z}_b^*$ und wir können ein multiplikatives Inverses von a in $\mathbb{Z}_b^*$ berechnen:

$$\begin{aligned}
& s \cdot a + t \cdot b = 1 = \text{ggT}(a.b) \\
\Leftrightarrow \quad & s \cdot a = 1 + (-t) \cdot b \\
\Leftrightarrow \quad & s \cdot a = 1 + (-t) \cdot b \\
\Leftrightarrow \quad & s \text{ ist multiplikatives Inverses von a in } \mathbb{Z}_b^*
\end{aligned}$$

Wie berechnen wir nun den grössten gemeinsamen Teiler von a und b bzw. s und t für gegebene a und b in Gleichung (4)?

(I) ggT berechnen für $0 \leq a < b$

Setze $r_0 = b$ und $r_1 = a$ und rechne:

$$\begin{aligned} r_0 &= q_1 \cdot r_1 + r_2 && 0 \leq r_2 < r_1 \\ r_1 &= q_2 \cdot r_2 + r_3 && 0 \leq r_3 < r_2 \\ &\vdots \\ r_{k-1} &= q_k \cdot r_k + r_{k+1} && 0 \leq r_{k+1} < r_k \\ &\vdots \\ r_{m-1} &= q_m \cdot r_m + r_{m+1} && r_{m+1} = 0 \end{aligned} \tag{5}$$

Dann gilt: $\mathrm{ggT}(a, b) = r_m$.

Dies ist der sogenante euklidische Algorithmus.

(II) Der erweiterte euklidische Algorithmus besteht nun daraus, noch ganze Zahlen s und t zu finden, sodass (4) erfüllt ist.

Man berechne nun s und t (bei der Bestimmung des multiplikativ inversen Elementes von a in $\mathbb{Z}_b^*$ muss nur s berechnet werden!).

1. Variante Ersetze immer r_{k+1} durch $r_{k-1} - q_k \cdot r_k$ bis $k = 0$, d. h. wir erhalten (grob) folgendes Schema (den Wert von m erhalten wir aus dem euklidischen Algorithmus (5)):

$$\begin{aligned} r_m &= r_{m-2} - q_{m-1} \cdot r_{m-1} = r_{m-2} - q_{m-1} \cdot (r_{m-3} - q_{m-2} \cdot r_{m-2}) \\ &= (1 + q_{m-1} \cdot q_{m-2}) \cdot r_{m-2} - q_{m-1} \cdot r_{m-3} = \dots \\ &= s \cdot r_1 + t \cdot r_0 = s \cdot a + t \cdot b \end{aligned}$$

2. Variante

- Ziel: Berechne s. (Wieder erhalten wir den Wert von m aus dem euklidischen Algorithmus (5).)

  Setze $s_0 = 0, s_1 = 1$ und $s_{k+1} = s_{k-1} - q_k \cdot s_k$ und berechne die s_k bis $k = m$, dann gilt $s = s_m$ und (zur Probe geeignet) $b = |s_{m+1}|$
- Ziel: Berechne t. (Wieder erhalten wir den Wert von m aus dem euklidischen Algorithmus (5).)

  Setze $t_0 = 1, t_1 = 0$ und $t_{k+1} = t_{k-1} - q_k \cdot t_k$ und berechne die t_k bis $k = m$, dann gilt $t = t_m$ und (zur Probe geeignet) $a = |t_{m+1}|$

(I)

$$\begin{aligned} 275 &= 3 \cdot 86 + 17 \\ 86 &= 5 \cdot 17 + 1 \\ 17 &= 17 \cdot 1 + 0 \end{aligned}$$

Somit gilt: $\mathrm{ggT}(86, 275) = 1$ und $q_1 = 3,\ q_2 = 5,\ q_3 = 17$ und $m = 3$.

(II) 1. Variante

$$1 = 86 - 5 \cdot 17 = 86 - 5 \cdot (275 - 3 \cdot 86) = \underbrace{16}_{=s} \cdot 86 + \underbrace{(-5)}_{=t} \cdot 275$$

Somit ist 16 das multiplikative Inverse von 86 in $\mathbb{Z}_{275}^*$.

2. Variante $s_0 = 0, s_1 = 1, s_{k+1} = s_{k-1} - q_k \cdot s_k$

$$\begin{aligned} s_2 &= s_0 - q_1 \cdot s_1 = 0 - 3 \cdot 1 &&= -3 \\ s_3 &= s_1 - q_2 \cdot s_2 = 1 - 5 \cdot (-3) &&= 16 \\ s_4 &= s_2 - q_3 \cdot s_3 = (-3) - 17 \cdot 16 &&= -275 \end{aligned}$$

Also gilt: $s = s_3 = 16$ und (zur Probe) $b = 275 = |s_4|$.
Somit ist 16 das multiplikative Inverse von 86 in $\mathbb{Z}_{275}^*$.

Aufgabe 4 Ringtheorie

Sei R ein Ring mit Eins. Wie üblich sei 0 sei das neutrale Element der Addition und 1 das neutrale Element der Multiplikation. Ist $a \in R$, so ist $-a$ das eindeutig bestimme inverse Element von a bezüglich der Addition.

a) Zeigen Sie, dass $-a = (-1)a$

Lösungsvorschlag:

Auf Grund der Kommutativität und der Eindeutigkeit des Inversen bezüglich der Addition in R genügt es zu zeigen, dass

$$a + (-1) \cdot a = 0$$

Also

$$\begin{aligned} a + (-1) \cdot a &\overset{mult.\ Neutr.}{=} 1 \cdot a + (-1) \cdot a \\ &\overset{Distr.}{=} (1 + (-1)) \cdot a \\ &\overset{add.\ Inv.}{=} 0 \cdot a \\ &\overset{add.\ Neutr.}{=} 0 \cdot a + 0 \\ &\overset{add.\ Inv.}{=} 0 \cdot a + (0 \cdot a + (-(0 \cdot a))) \\ &\overset{Assoz.}{=} (0 \cdot a + 0 \cdot a) + (-(0 \cdot a)) \\ &\overset{Distr.}{=} (0 + 0) \cdot a + (-(0 \cdot a)) \\ &\overset{add.\ Neutr.}{=} 0 \cdot a + (-(0 \cdot a)) \\ &\overset{add.\ Inv.}{=} 0 \end{aligned}$$

Kommentare:

- $0 \cdot a = 0$ musste auch gezeigt werden! Diese Aussage wurde im Tutorium erst im Rahmen dieser Aufgabe gezeigt. Ein Verweis auf das Tutorium war hier nicht genug, sonst hätte man genauso gut gleich auf den kompletten Beweis im Tutorium verweisen können. Stillschweigendes Voraussetzen war ein noch schwerwiegenderer Fehler, da mit dem Verweis wenigstens die Notwendigkeit die Aussage zu begründen erkannt wurde.
- $(-1) \cdot a = -(1 \cdot a)$ ist keine gültige Anwendung der Assoziativität! '$-$' ist kein Element von R und dass ein vorgestelltes '$-$' wie Multiplikation mit (-1) behandelt werden kann, soll gerade erst bewiesen werden.

b) Zeigen Sie, dass $(-1)(-1) = 1$

Lösungsvorschlag:

Die linke Seite der Gleichung legt nahe, die Aussage aus 4a) anzuwenden. Aus der Eindeutigkeit des Inversen und $1 + (-1) = (-1) + 1 = 0$ folgt darüber hinaus, dass $-(-1) = 1$. Also

$$(-1) \cdot (-1) \overset{4a)}{=} -(-1) \overset{Eind.\ d.\ Inv.}{=} 1$$

Kommentare:

- Hier wurden weitestgehend dieselben Fehler wie in 4a) gemacht.
- Ein weiterer häufiger Fehler war das Anwenden der alten Schulmerkregel '*Negative Zahl mal negative Zahl ergibt positive Zahl*'. Die Begriffe '*positiv*' und '*negativ*' machen erst im Kontext von (totalen) Ordnungsrelationen wirklich Sinn, die auf einem Ring nicht sinnvoll definiert sein müssen, siehe z.B. Restklassen- oder Matrizenringe.
  Zusätzlich trifft diese Merkregel keine Aussage über den konkreten Wert des Produkts, sondern nur über dessen Relation zur 0.

c) Sei R ein kommutativer Ring. Für Elemente $a, b \in R$ definiert man: $a/b :\Leftrightarrow \exists c \in R : ac = b$. Man zeige: Wenn $\langle b \rangle \subset \langle a \rangle$, dann a/b.

Im Folgenden bezeichne zum besseren Verständnis $0_R, 1_R$ die neutralen Elemente bezüglich Addition bzw. Multiplikation in R, sowie $0_{\mathbb{Z}}$ das additiv Neutrale in $\mathbb{Z}$.

Lösungsvorschlag:

Zeige: $\exists c \in R : \ ac = b$

Aus $\langle b \rangle \subset \langle a \rangle$ folgt $b \in \langle a \rangle$, also

$$\exists z \in \mathbb{Z} : \ z \cdot a = b$$

Fallunterscheidung über $z \in Z$
Fall 1: $z < 0_{\mathbb{Z}}$

$$\begin{aligned} z \cdot a &= \sum_{i=1}^{|z|}(-a) \\ &\overset{4a),\ Komm.}{=} \sum_{i=1}^{|z|}(a \cdot (-1_R)) \\ &\overset{Assoz.,\ Distr.}{=} a \cdot \sum_{i=1}^{|z|}(-1_R) \end{aligned}$$

Setze $c := \sum_{i=1}^{|z|}(-1_R) \in R$.

Fall 2: $z = 0_{\mathbb{Z}}$

$$\begin{aligned} 0_{\mathbb{Z}} \cdot a &= 0_R \\ &\overset{vgl.\ 4a)}{=} 0_R \cdot a \\ &\overset{Komm.}{=} a \cdot 0_R \end{aligned}$$

Setze $c := 0_R \in R$.

Fall 3: $z > 0_{\mathbb{Z}}$

$$\begin{aligned} z \cdot a &= \sum_{i=1}^{z} a \\ &\overset{mult.\ Neutr.}{=} \sum_{i=1}^{z}(a \cdot 1_R) \\ &\overset{Assoz.,\ Distr.}{=} a \cdot \sum_{i=1}^{z} 1_R \end{aligned}$$

Setze $c := \sum_{i=1}^{z} 1_R \in R$.

Kommentare

- Im Kontext von Ringen sind zyklische Untergruppen $\langle a \rangle$ falls nicht weiter spezifiziert additive Untergruppen, da im Allgemeinen die Existenz multiplikativ inverser Elemente in Ringen nicht gegeben ist.

- Ideale sind zwar immer additive Untergruppen, aber umgekehrt stimmt das nicht! Als Notation für Ideale werden runde Klammern statt spitze Klammern wie bei Untergruppen verwendet.
- Es war zu zeigen a/b, nicht $|\langle b\rangle|/|\langle a\rangle|$!
- Im Rahmen dieser Aufgabe bezeichnet a/b wie aus der Aufgabenstellung ersichtlich keinen Bruch bzw. kein Element aus R, sondern eine Aussage!

Aufgabe 5 Polynome

Betrachten Sie die als Strings von Elementen von $\mathbb{Z}_{11}$ gegebenen Polynome $a = 765431, b = 432$. Damit sind also $a, b \in \mathbb{Z}_{11}[X]$, und $\text{grad}(a) = 5$ und $\text{grad}(b) = 2$.

a) Berechnen Sie das Polynomprodukt $a \cdot b$.

Lösungsvorschlag:

$$
\begin{aligned}
&(7X^5 + 6X^4 + 5X^3 + 4X^2 + 3X^1 + 1) \cdot (4X^2 + 3X^1 + 2) \\
&= (7X^5 + 6X^4 + 5X^3 + 4X^2 + 3X^1 + 1) \cdot 4X^2 \\
&+ (7X^5 + 6X^4 + 5X^3 + 4X^2 + 3X^1 + 1) \cdot 3X^1 \\
&+ (7X^5 + 6X^4 + 5X^3 + 4X^2 + 3X^1 + 1) \cdot 2 \\
&= (28X^7 + 24X^6 + 20X^5 + 16X^4 + 12X^3 + 4X^2) \\
&+ (21X^6 + 18X^5 + 15X^4 + 12X^3 + 9X^2 + 3X^1) \\
&+ (14X^5 + 12X^4 + 10X^3 + 8X^2 + 6X^1 + 2) \\
&= 28X^7 + 45X^6 + 52X^5 + 43X^4 + 34X^3 + 21X^2 + 9X^1 + 2 \\
&\overset{\text{in } \mathbb{Z}_{11}^*}{=} 6X^7 + 1X^6 + 8X^5 + 10X^4 + 1X^3 + 10X^2 + 9X^1 + 2
\end{aligned}
$$

Für die Lösung dieser Aufgabe können die Polynome auch als Strings aufgefasst werden und dann mit der normalen schriftlichen Multiplikation multipliziert werden. Hierbei muss nur darauf geachtet werden, dass das Ergebnis 10 ein Koeffizient ist und keine Zahl - das heißt unter anderem darf hieraus kein Übertrag entstehen. Hilfreich hierfür ist es, entweder die 10 mit einem Buchstaben zu kodieren oder sich an $10 = -1 \mod 11$ zu erinnern. Allgemein dürfen beim Addieren der Teilstrings keine Überträge verwendet werden - schließlich geht es hier um Koeffizienten! Die Addition von $5X^2$ und $6X^2$ ergibt nicht $1X^3 + 1X^2$! Dies würde ein Beibehalten der Überträge jedoch bewirken.

Alternative: Bei Nutzung der Stringnotation ergibt sich die folgenden Rechnung:

7	6	5	4	3	1	·	4	3	2
		6	2	9	5	1	4		
			10	7	4	1	9	3	
				3	1	10	8	6	2
		6	1	8	10	1	10	9	2

b) Führen Sie die Division mit Rest von a durch b durch, d. h. berechnen Sie explizit Polynome $q, r \in \mathbb{Z}_{11}[X]$ mit $a = qb + r$ und $\text{grad}(r) < 2$.

Lösungsvorschlag:

Hier ist eine Polynomdivision mit Rest durchzuführen, hier werden nur die einzelnen Schritte gezeigt.

1. $(7X^5 + 6X^4 + 5X^3 + 4X^2 + 3X^1 + 1) : (4X^2 + 3X^1 + 2)$:
   Für den ersten Koeffizienten von q müssen wir $7 : 4$ in $\mathbb{Z}_{11}^*$ berechnen. Dies ergibt 10 bzw. -1, denn $(-1) \cdot 4 = -4 = 7$. Also erhalten wir $10X^3$ als ersten Teil des Polynoms.
   Führt man die Rückmultiplikation durch, erhält man: $10X^3 \cdot (4X^2 + 3X^1 + 2) = 7X^5 + 8X^4 + 9X^3$. Die Subtraktion ergibt: $9X^4 + 7^3 + 4X^2 + 3X^1 + 1$
2. Nun wiederholen wir den Schritt mit der erhaltenen Differenz:
   $(9X^4 + 7^X 3 + 4X^2 + 3X^1 + 1) : (4X^2 + 3X^1 + 2)$:
   Hier ergibt sich als erster Koeffizient $9 : 4 = 5$ in $\mathbb{Z}_{11}^*$. Damit ist $5X^2$ der zweite Teil des Polynoms.
   Führt man die Rückmultiplikation durch, erhält man: $5X^2 \cdot (4X^2 + 3X^1 + 2) = 9X^4 + 4X^3 + 10X^2$. Subtraktion ergibt dann: $3X^3 + 5X^2 + 3X^1 + 1$
3. Erneut wiederholung des letzten Schrittes mit der neuen Differenz:
   $(3X^3 + 5X^2 + 3X^1 + 1) : (4X^2 + 3X^1 + 2)$:
   Der erste Koeffizient hier ist $9 = 3 : 4$ in $\mathbb{Z}_{11}^*$, damit ist der dritte Teil des Polynoms $9X^1$.
   Führ man die Rückmultiplikation durch, erhält man: $9X^1 \cdot (4X^2 + 3X^1 + 2) = 3X^3 + 5X^2 + 7X^1$. Subtraktion ergibt dann: $7X^1 + 1$. Dieses Polynom hat einen Grad kleiner als 2. Also gilt:

$(7X^5+6X^4+5X^3+4X^2+3X^1+1) = (10X^3+5X^2+9X^1)\cdot(4X^2+3X^1+2)+(7X^1+1)$, damit ist die Aufgabe gelöst.

Alternative: Bei Nutzung der Stringnotation ergibt sich die folgenden Rechnung:

7	6	5	4	3	1	÷	4	3	2	=	10	5	9	REST	7	1
7	8	9														
	9	7	4													
	9	4	10													
		3	5	3												
		3	5	7												
				7	1											

Aufgabe 6 Eisensteinsche Zahlen

Der Ring der Eisensteinschen Zahlen $\mathbb{Z}[\omega] = E$ besteht aus der Menge $\{a + b\omega | a, b \in \mathbb{Z}\}$, wobei $\omega := \frac{-1}{2} + i\frac{\sqrt{3}}{2}$, Addition und Multiplikation in diesem Ring sind gegeben durch die Addition und Multiplikation in $\mathbb{C}$.

a) Man zeige, dass ω und $\omega + 1$ Einheiten im Ring $\mathbb{Z}[\omega]$sind.

Lösungsvorschlag:

Erste Möglichkeit: Man erinnere sich an Übungsblatt 11 Aufgabe 4a, hier galt es die sogenante „Multiplikativität“ der Norm in den Gaußschen Zahlen zu zeigen. Außerdem wurde in Aufgaben 4b) noch gezeigt, dass die Einheiten in den Gaußschen Zahlen immer gleich 1 ist. Weiter ist $N(z) = a^2+b^2$ komplexe Zahlen und aufgrund der Darstellungsform der Gaußschen gilt dies insbesondere auch für die Gaußschen Zahlen.

Man konnte diese Ergebnisse einfach auf die Eisensteinschen Zahlen übertragen: Die Norm von Einheiten in den Eisensteinschen Zahlen ist ebenfalls immer gleich 1, außerdem wurde bewiesen, dass für die Norm der Eisensteinschen Zahlen $N(z) = a^2 + b^2 - ab$ gilt. Mit diesen Vorbemerkungen kann man nun einfach die Normen von ω und $\omega + 1$ ausrechnen:

$$N(\omega) = N(0 + 1 \cdot \omega) = 0^2 + 1^2 - 0 \cdot 1 = 1$$
$$N(\omega + 1) = N(1 + 1 \cdot \omega) = 1^2 + 1^2 - 1 \cdot 1 = 1$$

Damit sind ω und $\omega + 1$ Einheiten.

Zweite Möglichkeit: Man betrachte ω und $\omega + 1$ als komplexe Zahlen und berechne die Inversen Elemente und zeige dann, dass die Inverse Eisensteinsche Zahlen sind.

Zunächst das Inverse von ω:

$$\begin{aligned}
\omega^{-1} = \frac{1}{\omega} = \frac{1}{\frac{-1}{2} + i\frac{\sqrt{3}}{2}} &= \frac{1}{\frac{-1}{2} + i\frac{\sqrt{3}}{2}} \cdot \frac{\frac{-1}{2} - i\frac{\sqrt{3}}{2}}{\frac{-1}{2} - i\frac{\sqrt{3}}{2}} \\
&= \frac{\frac{-1}{2} - i\frac{\sqrt{3}}{2}}{\left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right) \cdot \left(\frac{-1}{2} - i\frac{\sqrt{3}}{2}\right)} \\
&= \frac{\frac{-1}{2} - i\frac{\sqrt{3}}{2}}{\left(\frac{-1}{2}\right)^2 + i \cdot \frac{-1}{2} \cdot \frac{\sqrt{3}}{2} - i \cdot \frac{-1}{2} \cdot \frac{\sqrt{3}}{2} - i^2 \cdot \left(\frac{\sqrt{3}}{2}\right)^2} \\
&= \frac{\frac{-1}{2} - i\frac{\sqrt{3}}{2}}{\frac{1}{4} + \frac{3}{4}} = \frac{\frac{-1}{2} - i\frac{\sqrt{3}}{2}}{1} \\
&= -\frac{1}{2} - i\frac{\sqrt{3}}{2} \quad \left(= \omega^{-1}\right) \\
&= -\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \\
&= -1 - \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \\
&= -1 - \omega \quad (\in \mathbb{Z}[\omega])
\end{aligned}$$

Bei einer Reinschrift hätte man auch behaupten können, dass $-1 - \omega$ das Inverse von ω ist und dies durch nachrechnen beweisen. Offensichtlich ist $-1 - \omega \in \mathbb{Z}[\omega]$ und da die Inversen in den komplexen Zahlen eindeutig sind, sind die Inversen in den Eisensteinschen Zahlen ebenfalls eindeutig, sofern sie denn in den Eisensteinschen Zahlen existieren:

$$\omega \cdot (-1 - \omega) = -\omega - \omega^2 \overset{-\omega^2 - \omega = 1}{=} 1 \tag{6}$$

Wenn man sich die Gleichungskette (6) genau anschaut sieht man schnell, dass das Inverse von $\omega + 1$ nur $-\omega$ sein:

$$(1 + \omega) \cdot (-\omega) = -\omega - \omega^2 \overset{-\omega^2 - \omega = 1}{=} 1$$

Falls man dies nicht gesehen hat, berechnet man das Inverse von $\omega + 1$:

$$\begin{aligned}
(\omega+1)^{-1} = \frac{1}{\omega+1} &= \frac{1}{1+\left(\frac{-1}{2}+i\frac{\sqrt{3}}{2}\right)} = \frac{1}{\frac{1}{2}+i\frac{\sqrt{3}}{2}} \\
&= \frac{1}{\frac{1}{2}+i\frac{\sqrt{3}}{2}} \cdot \frac{\frac{1}{2}-i\frac{\sqrt{3}}{2}}{\frac{1}{2}-i\frac{\sqrt{3}}{2}} \\
&= \frac{\frac{1}{2}-i\frac{\sqrt{3}}{2}}{\left(\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)\cdot\left(\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)} \\
&= \frac{\frac{1}{2}-i\frac{\sqrt{3}}{2}}{\left(\frac{1}{2}\right)^2 + i\cdot\frac{1}{2}\cdot\frac{\sqrt{3}}{2} - i\cdot\frac{1}{2}\cdot\frac{\sqrt{3}}{2} - i^2\cdot\left(\frac{\sqrt{3}}{2}\right)^2} \\
&= \frac{\frac{1}{2}-i\frac{\sqrt{3}}{2}}{\frac{1}{4}+\frac{3}{4}} = \frac{\frac{1}{2}-i\frac{\sqrt{3}}{2}}{1} \\
&= \frac{1}{2}-i\frac{\sqrt{3}}{2} \quad \left(= (\omega+1)^{-1}\right) \\
&= -\left(\frac{-1}{2}+i\frac{\sqrt{3}}{2}\right) \\
&= -\omega \quad (\in \mathbb{Z}[\omega])
\end{aligned}$$

Häufigste Fehler:

- Man kann nicht einfach behaupten, dass irgendwelche Elemente die Inversen sind ohne die entsprechenden Argumente zu nennen und zumindestens nachzurechnen, dass das Produkt von Element und Inversem wirklich gleich 1 ist.
- Verweise auf den komplexen Einheitskreis sind zwar ein guter Ansatzpunkt, aber eine bloße Zeichnung und weitere Argumente zeigt leider nichts. Ebensowenig durfte man die Behauptung „Einheiten liegen auf dem Einheitskreis“ verwenden und daraus sofort schließen. Meistens wurde nicht einmal gezeigt, dass das ω und $\omega+1$ überhaupt auf diesem Einheitskreis liegen.
- Es gab auffällig viele Rechenfehler bei (doppelten) Brüchen. Des Weiteren waren vielen scheinbar die binomischen Formeln unbekannt:
  - $(a+b)^2 = a^2 + 2ab + b^2$, erste Binomische Formel (Plus-Formel)
  - $(a-b)^2 = a^2 - 2ab + b^2$, zweite Binomische Formel (Minus-Formel)
  - $(a+b)\cdot(a-b) = a^2 - b^2$, dritte Binomische Formel (Plus-Minus-Formel)

b) Für $z \in \mathbb{C}$ setzt man $N(z) = z\overline{z}$. Sind $a, b \in \mathbb{Z}$, so ist $z = a + b\omega$ eine Eisensteinsche Zahl.
Man berechne $N(a + b\omega)$ so, dass das Ergebnis ein Ausdruck ist, in dem zwar a und b vorkommen, ω aber nicht mehr.

Lösungsvorschlag:

Es sei $z = a + b\omega \in \mathbb{Z}[\omega]$.

Erste Möglichkeit: Nachrechnen ohne Einsetzen von ω liefert die folgende Rechnung:

$$\begin{aligned}
N(z) &= N(a + b\omega) \\
&= (a + b\omega) \cdot \overline{(a + b\omega)} \\
&= (a + b\omega) \cdot (a + b\overline{\omega}) \\
&= a^2 + b^2\omega\overline{\omega} + ab\omega + ab\overline{\omega}) \\
&\overset{\omega^2=\overline{\omega}}{=} a^2 + b^2\omega^3 + ab(\omega + \omega^2) \\
&\overset{\omega^3=1}{=} a^2 + b^2 + ab(\omega + \omega^2) \\
&\overset{\omega^2+\omega=-1}{=} a^2 + b^2 - ab
\end{aligned}$$

Zweite Möglichkeit: Nachrechnen mit Einsetzen von ω liefert die folgende Rechnung:

$$\begin{aligned}
N(z) &= N(a + b\omega) \\
&= (a + b\omega) \cdot \overline{(a + b\omega)} \\
&= \left(a + b \cdot \left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right)\right) \cdot \overline{\left(a + b \cdot \left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right)\right)} \\
&= \left(\left(a + \frac{-b}{2}\right) + i \cdot b \cdot \frac{\sqrt{3}}{2}\right) \cdot \left(\left(a + \frac{-b}{2}\right) - i \cdot b \cdot \frac{\sqrt{3}}{2}\right) \\
&= \left(a + \frac{-b}{2}\right)^2 + \left(i \cdot b \cdot \frac{\sqrt{3}}{2}\right) \cdot \left(-i \cdot b \cdot \frac{\sqrt{3}}{2}\right) \\
&= a^2 + 2 \cdot a \cdot \frac{-b}{2} + \frac{1}{4} \cdot b^2 - i^2 \cdot b^2 \cdot \left(\frac{\sqrt{3}}{2}\right)^2 \\
&= a^2 - ab + \frac{1}{4} \cdot b^2 + \frac{3}{4} \cdot b^2 \\
&= a^2 + b^2 - ab
\end{aligned}$$

In beiden Fällen gilt also für $z = a + b\omega \in \mathbb{Z}[\omega] : N(z) = a^2 + b^2 - ab$.