Prof. Dr. H. Maier
Dipl.-Math. D. Haase
daniel.haase@uni-ulm.de

08.11.2007
WS 2007/2008

Lineare Algebra für Informatiker - Lösungsblatt 3

Zur Übungsstunde vom 08.11.2007

Aufgabe 12 (Die Restklassen modulo n) — 3 Punkte

Diese und die folgende Aufgabe werden auf zukünftigen Blättern fortgeführt!
Es sei n eine feste natürliche Zahl und $\bar{a} = \{a + kn \;:\; k \in \mathbb{Z}\}$ für $a \in \mathbb{Z}$ die „Gerade" vom letzten Übungsblatt. Das Mengensystem aller dieser Mengen bezeichnen wir mit $\mathbb{Z}_n = \{\bar{a} \;:\; a \in \mathbb{Z}\}$, man nennt es den *Restklassenring modulo n* und $\bar{a}$ die *Restklasse* von a modulo n. Zeigen Sie die folgenden Aussagen:

(a) Die Mengen $\bar{a}$ und $\bar{b}$ sind genau dann gleich, wenn $a - b$ durch n ohne Rest teilbar ist.
(b) Der Restklassenring $\mathbb{Z}_n$ enthält genau n Mengen.

Lösung

Zu a):
Richtung $\Rightarrow$:
Angenommen die Mengen $\bar{a}$ und $\bar{b}$ sind gleich, also $\{a + kn \;:\; k \in \mathbb{Z}\} = \{b + kn \;:\; k \in \mathbb{Z}\}$. Dann ist insbesondere $a \in \bar{a} = \bar{b}$, also gibt es $k \in \mathbb{Z}$ mit $a = b + kn$, somit ist $a - b = kn$ glatt durch n teilbar.

Richtung $\Leftarrow$:
Angenommen $a-b$ ist ohne Rest durch n Teilbar, dann ist $a-b = kn$ für ein $k \in \mathbb{Z}$. Wir müssen jetzt zeigen, dass $\bar{a} \subseteq \bar{b}$ und $\bar{b} \subseteq \bar{a}$ gilt. Ist $x \in \bar{a}$ beliebig, also $x = a+ln$ für irgend ein $l \in \mathbb{Z}$, so ist $x = a+ln = a+(b-a)+(l+k)n = b+(l+k)n \in \bar{b}$, also $\bar{a} \subseteq \bar{b}$. Ist dagegen $y \in \bar{b}$, also $y = b + dn$, dann ist $y = b + dn = b + (a - b) + (d - k)n = a + (d - k)n \in \bar{a}$, also auch $\bar{b} \subseteq \bar{a}$, und die beiden Mengen sind gleich.

Zu b):
Nach der vorigen Rechnung ist $\bar{a} = \bar{b}$ genau dann, wenn $a - b$ ohne Rest durch n teilbar ist. Damit sind die Mengen $\bar{0}, \bar{1}, \dots, \overline{n-1}$ alle paarweise verschieden, weil keine Differenz aus den Zahlen $0, 1, \dots, n-1$ glatt durch n teilbar ist. Andererseits ist $\bar{0} = \bar{n} = \overline{2n} = \cdots$. Damit ist

$$\mathbb{Z}_n \;=\; \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

ein Mengensystem mit genau n Mengen.

Aufgabe 13 (Rechnen mit Restklassen) — 4 Punkte

Wieder sei $n \in \mathbb{Z}$ fest. Wir definieren die Summe von Teilmengen aus $\mathbb{Z}$ über

$$R + S \;=\; \{r + s \;:\; r \in R\,,\; s \in S\}\,.$$

Zeigen Sie zunächst die Regel $\overline{a+b} = \bar{a} + \bar{b}$, wobei $\bar{a} = \{a + kn \;:\; k \in \mathbb{Z}\}$ die Restklasse von a modulo n ist. Zeigen Sie nun ausführlich durch Nachrechnung aller Axiome, dass $(\mathbb{Z}_n, +)$ eine abelsche Gruppe bildet.

Achtung: In diesen beiden Aufgaben bezeichnet $\bar{a}$ eine der Zahl a zugeordnete Menge. In den folgenden Aufgaben ist $\bar{z}$ die konjugierte komplexe Zahl von z. Beide Schreibweisen haben sich in der Mathematik eingebürgert, wir unterscheiden Sie, indem wir ganze Zahlen mit niedrigen Buchstaben $a, b, c, \dots$ und komplexe Zahlen mit höheren Buchstaben $z, w, s, \dots$ bezeichnen.

Lösung

Zu a): Nach Definition ist

$$\overline{a+b} \;=\; \{(a+b) + kn \;:\; k \in \mathbb{Z}\} \;\underset{(*)}{=}\; \{(a + l_1 n) + (b + l_2 n) \;:\; k, l \in \mathbb{Z}\} \;=\; \bar{a} + \bar{b}\,,$$

wobei der Schritt $(*)$ gilt, weil jedes $k \in \mathbb{Z}$ als Summe $k = l_1 + l_2$ von zwei ganzen Zahlen geschrieben werden kann (dass mehrere verschiedene Summen das gleiche k geben ist unwichtig, das innerhalb einer Mengenklammer jedes Objekt nur einmal gezählt wird).

Zu b): Wir rechnen alle Axiome nach:

Axiom G1 (Assoziativgesetz):
Es seien $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ beliebig, dann gilt

$$(\bar{a}+\bar{b})+\bar{c} \underset{\text{(a)}}{=} \overline{(a+b)}+\bar{c} \underset{\text{(a)}}{=} \overline{(a+b)+c)} \underset{\text{G1 in } \mathbb{Z}}{=} \overline{a+(b+c)} \underset{\text{(a)}}{=} \bar{a}+\overline{(b+c)} \underset{\text{(a)}}{=} \bar{a}+(\bar{b}+\bar{c})\,.$$

Axiom G2 (Neutrales Element):
Das neutrale Element von $\mathbb{Z}_n$ ist die Nullrestklasse $\bar{0}$, also die Menge $\{0+kn \ : \ k \in \mathbb{Z}\}$ aller ganzen Zahlen, die durch n teilbar sind. Beweis: Für jedes $\bar{a} \in \mathbb{Z}_n$ gilt

$$\bar{0}+\bar{a} \underset{\text{(a)}}{=} \overline{0+a} = \bar{a} \ , \ \bar{a}+\bar{0} \underset{\text{(a)}}{=} \overline{a+0} = \bar{a}\,.$$

Axiom G3 (Inverses Element):
Das inverse zu $\bar{a}$ in $\mathbb{Z}_n$ ist $\overline{n-a}$, denn es gilt

$$\bar{a}+\overline{n-a} \underset{\text{(a)}}{=} \overline{a+n-a} = \bar{n} = \bar{0}\,.$$

Axiom G4 (Kommutativgesetz):
Es gilt

$$\bar{a}+\bar{b} \underset{\text{(a)}}{=} \overline{a+b} \underset{\text{G4 in } \mathbb{Z}}{=} \overline{b+a} \underset{\text{(a)}}{=} \bar{b}+\bar{a}\,.$$

Aufgabe 14 (Die Polardarstellung) 3 Punkte

Betrachten Sie die Abbildung $\Phi : \ (0,\infty) \times [0,2\pi) \to \mathbb{C}-\{0\} \ , \ (r,\phi) \mapsto r \cdot (\cos(\phi)+i\sin(\phi))$. Zeigen Sie, dass diese Abbildung eine Bijektion ist, d. h. jede komplexe Zahl $z \in \mathbb{C}$ (mit der Ausnahme $z=0$) kann mit einem Paar (r,ϕ) identifiziert werden.

Lösung

Injektivität von Φ: Erstmal ist $|\Phi(r,\phi)| = r$ für alle $r > 0$ und $\phi \in [0,2\pi)$, aus $\Phi(r,\phi) = \Phi(r',\phi')$ folgt somit $r = r'$, und wir müssen nur noch zeigen, dass die zweite Komponente gleich ist. Aus $\Phi(r,\phi) = \Phi(r,\phi')$ folgt, dass $\sin(\phi) = \sin(\phi')$ und gleichzeitig $\cos(\phi) = \cos(\phi')$ gelten, das ist nur für $\phi = \phi' + 2\pi k$ und ein $k \in \mathbb{Z}$ möglich, da $\phi, \phi' \in [0,2\pi)$ aber niemals einen Abstand $\geq 2\pi$ haben können bleibt nur $\phi = \phi'$, also ist Φ injektiv.

Surjektivität von Φ: Jedes $z \neq 0$ hat das Urbild $\Phi^{-1}(z) = (r,\phi)$ mit $r = |z|$ und dem Winkel $\phi \in [0,2\pi)$, den die Verbindungsstrecke von 0 zu z mit der reellen Achse bildet.

Aufgabe 15 (Rechnen mit komplexen Zahlen) 2 Punkte

Berechnen Sie die folgenden komplexen Zahlen in der Darstellung $z = x + iy$:

$$z = \frac{2i}{1-i} \ , \ \omega = \frac{1+i}{\sqrt{2}} \ , \ \omega^4 \ , \ n = \sum_{k=0}^{7} \omega^k\,.$$

Tipp zur letzten Summe: die Real- und Imaginärteile auszurechnen und aufzuaddieren ist nicht die beste Lösung. Teilen Sie die Summe in zwei gleichgroße Teile und vergleichen Sie beide unter Verwendung des Ergebnisses für ω^4.

Lösung

Es gilt durch Erweitern:

$$z = \frac{2i}{1-i} = \frac{2i(1+i)}{(1-i)(1+i)} = \frac{2i(1+i)}{1^2-i^2} = \frac{2i(1+i)}{2} = i(1+i) = i-1\,.$$

Trivialerweise ist

$$\omega = \frac{1}{\sqrt{2}} \cdot 1 + \frac{1}{\sqrt{2}} \cdot i\,.$$

Das Quadrat von ω ist

$$\omega^2 = \left(\frac{1+i}{\sqrt{2}}\right)^2 = \frac{(1+i)^2}{2} = \frac{1+2i+i^2}{2} = \frac{2i}{2} = i\,.$$

Die vierte Potenz ist also $\omega^4 = i^2 = -1$. Die Summe ist schließlich

$$\sum_{k=0}^{7} \omega^k \;=\; \sum_{k=0}^{3} \omega^k + \sum_{k=4}^{7} \omega^k \;=\; \sum_{k=0}^{3} \omega^k + \sum_{k=0}^{3} \omega^{4+k} \;=\; \sum_{k=0}^{3} \omega^k - \sum_{k=0}^{3} \omega^k \;=\; 0\,.$$

Aufgabe 16 (Rechnen mit der Konjugation) — 4 Punkte

Beweisen Sie Satz 2.4.5 der Vorlesung durch direkte Rechnung:

(a) Es ist $\overline{z+w} = \bar{z} + \bar{w}$ (hat nichts mit Aufgabe 13 zu tun).
(b) Es ist $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$, sowie $\overline{w^{-1}} = (\bar{w})^{-1}$.
(c) $\mathrm{Re}(z) = \frac{1}{2}(z + \bar{z})$ und $\mathrm{Im}(z) = \frac{1}{2i}(z - \bar{z})$. Insbesondere gilt $\bar{z} = z \Leftrightarrow z \in \mathbb{R}$.

Lösung

Zu a): Es seien $z = x + iy$ und $w = r + is$ mit $x, y, r, s \in \mathbb{R}$ vorgegeben, dann gilt

$$\overline{z+w} \;=\; \overline{(x+iy)+(r+is)} \;=\; \overline{(x+r)+i(y+s)} \;=\; (x+r) - i(y+s) \;=\; (x-iy)+(r-is) \;=\; \bar{z}+\bar{w}\,.$$

Zu b): Für das Produkt gilt

$$\begin{aligned} \overline{z \cdot w} \;&=\; \overline{(x+iy)(r+is)} \;=\; \overline{xr + iyr + ixs + i^2 ys} \;=\; \overline{(xr-ys)+i(yr+xs)} \\ &=\; (xr-ys) - i(yr+xs) \;=\; (x-iy)(r-is) \;=\; \bar{z}\cdot\bar{w}\,. \end{aligned}$$

Wir müssen jetzt zeigen, dass das Inverse von $\bar{w}$ durch $\overline{w^{-1}}$ gegeben ist. Es gilt nach der Regel für das Produkt

$$\bar{w} \cdot \overline{w^{-1}} \;=\; \overline{w \cdot w^{-1}} \;=\; \bar{1} \;=\; 1\,.$$

Nach G3 ist also $\overline{w^{-1}}$ das Inverse von $\bar{w}$, aber auch $(\bar{w})^{-1}$ ist das Inverse, also sind beide Werte gleich. Die Regel für den Quotienten folgt nun aus

$$\overline{\left(\frac{z}{w}\right)} \;=\; \overline{z \cdot w^{-1}} \;=\; \bar{z} \cdot \overline{w^{-1}} \;=\; \bar{z} \cdot (\bar{w})^{-1} \;=\; \frac{\bar{z}}{\bar{w}}\,.$$

Zu c): Es gilt $z + \bar{z} = (x+iy) + (x-iy) = 2x = 2\mathrm{Re}(x)$, sowie $z - \bar{z} = (x+iy) - (x-iy) = 2iy = 2i\mathrm{Im}(z)$.