Diskrete Mathematik Übungsstunde Zusammenfassung

Leon Kolmanić

20.11.2023

1 Besprechung Bonusaufgabe

a)

Häufige Fehler waren:

- Verwendet, dass f Homomorphismus ist
- Klammern nicht geschlossen
- Klammern weggelassen
- Assoziativität nicht richtig angewendet

Die Umformung $f(a * b) = f(a) \star f(b)$ kann man nur machen, wenn f ein Homomorphismus ist. Das wird aber erst in einer späteren Teilaufgabe bewiesen. Deshalb konntet ihr das in der Bonusaufgabe noch nicht verwenden.
Achtet darauf, dass jede gesetzte Klammer irgendwann geschlossen wird. In den meisten Fällen ist es nicht schlimm, wenn ihr eine Klammer vergesst, weil klar ist, wie der Ausdruck gemeint ist. In solchen Fällen ziehe ich keine Punkte ab. Aber manchmal hat der Ausdruck durch die fehlende Klammer verschiedene Interpretationen und für die Bewertung ist entscheidend, welche davon ihr meint. Dann kann es Punktabzug geben. In einigen Abgaben habe ich gesehen, dass die Klammern farbig gemacht wurden, um den Überblick zu behalten. Das ist eine gute Idee. Ich würde diese Methode jedem, der mit den Klammern durcheinanderkommt, empfehlen.
Es wurden oft Klammern weggelassen, die man eigentlich noch nicht entfernen durfte. Folgender Fall ist zum Beispiel häufig aufgetreten:

$$f(f^{-1}(f(f^{-1}(a) * f^{-1}(b))) * f^{-1}(c))$$
$$= f(f^{-1}(a) * f^{-1}(b) * f^{-1}(c))$$

In dem unteren Ausdruck ist nicht mehr klar, ob zuerst $f^{-1}(a) * f^{-1}(b)$ oder $f^{-1}(b) * f^{-1}(c)$ ausgewertet wird. Im oberen Ausdruck ist hingegen eindeutig, dass zuerst $f^{-1}(a) * f^{-1}(b)$ ausgewertet wird. Weil $*$ assoziativ ist, ist die

Auswertungsreihenfolge egal. Aber einige von euch haben hier die Assoziativität von $*$ nicht verwendet, aber trotzdem die Klammern weggelassen. Das ist dann ein inkorrekter Beweisschritt. Um solche Fehler zu vermeiden, kann ich euch empfehlen, nach jeder Umformung euren Ausdruck darauf zu prüfen, ob die komplette Auswertungsreihenfolge eindeutig durch Klammern festgelegt ist. Falls nicht, solltet ihr prüfen, ob dies ein Problem darstellt, oder ob durch die Assoziativität der Operatoren die Klammersetzung keine Rolle spielt (aber nehmt diese dann mit in die Begründung auf!).
Einige von euch hatten Mühe, die Assoziativität korrekt anzuwenden. Die Umformung

$$\begin{aligned} & a * (b * c) \\ & = a * b * c \end{aligned}$$

ist keine korrekte Anwendung der Assozitiativität. Wenn wir diese korrekt anwenden wollen, dürfen wir die Klammern nur umsetzen, nicht gänzlich entfernen. Bei Beweisen in der Aussagenlogik und Beweisen in der Gruppentheorie solltet ihr nie Klammern durch die Assoziativität weglassen, sondern nur umsetzen. Um Zeit zu sparen, werden bei Beweisen von Ringeigenschaften/Körpereigenschaften die Klammern weggelassen. Das stellt aber eine Ausnahme dar. Im Zweifel solltet ihr die Klammern nicht weglassen. Ausserdem können wir die Assoziativität nicht "quer durch Funktionen hindurch" anwenden. Die Umformung

$$\begin{aligned} & f(f^{-1}(a) * f^{-1}(b)) * f^{-1}(c) \\ & = f^{-1}(a) * f(f^{-1}(b) * f^{-1}(c)) \end{aligned}$$

lässt sich beispielsweise nicht mit der Assoziativität von $*$ begründen. Denkt am besten über eine Regel wie Assoziativität wie eine Schablone nach: Man legt diese auf einen Ausdruck und schaut, ob sie genau passt. Das bedeutet, dass man a, b und c so wählt, dass $a * (b * c)$ als Teilausdruck vorkommt. Dann ersetzt man diesen Teilausdruck mit $(a * b) * c$. Im obigen Fall kann man a, b und c nicht so wählen, dass die "Schablone" passt.

b)

Diese Aufgabe ist leider sehr binär: Entweder man hat die Idee aus der Musterlösung gehabt, ein Paar von Generatoren[1] aus jeder Menge zu finden und so die Abbildung zu definieren, oder nicht. Falls man diese Idee nicht hatte, blieb einem nichts anderes übrig, als Funktionen aufzustellen und dann durch Berücksichtigung aller Paare von Elementen die Homomorphismus Eigenschaft zu prüfen. Man kann die Menge aller Funktionen, die man als Kandidaten für einen Isomorphismus prüft, dadurch einschränken, dass das neutrale Element auf das neutrale Element und Inverse auf Inverse abgebildet werden (Lemma 5.5 Skript). Ausserdem bildet ein Homomorphismus ein Element von Ordnung

[1] Die Paare von "Generatoren" sind nach der Definition vom Skript eigentlich keine Generatoren, weil ein "richtiger" Generator ganz alleine die ganze Gruppe generieren muss.

k immer auf ein Element von Ordnung k ab. Aber diese Bedingungen reichen nicht aus, um zu prüfen, dass die Funktion tatsächlich ein Homomorphismus ist. Das sind nur notwendige Bedingungen, also Bedingungen, die für jeden Homomorphismus erfüllt sein müssen. Aber sie sind nicht ausreichend. Eine Funktion, die diese Bedingungen erfüllt, ist nicht zwingend ein Homomorphismus.

2 Generatoren finden

Das ist ein Aufgabentyp, der sehr häufig in der Prüfung vorkommt. Glücklicherweise gibt es ein einfaches System, was man üben kann, das immer funktioniert. Wenn man viele solcher Aufgaben geübt hat, sind das einfache Punkte. Wir möchten im Folgendem die Generatoren von $\langle \mathbb{Z}_7^*; \odot \rangle$ finden.

2.1 Theorie am Beispiel

Die Theorie komplett zu verstehen ist nicht nötig, wenn man solche Aufgaben lösen will. Aber es hilft sehr fürs Verständnis, die folgenden Überlegungen zu machen und an einigen Beispielen zu sehen, was die teilweise sehr abstrakten Theoreme aus dem Skript bedeuten.
Im Folgendem gehen wir davon aus, dass die Gruppe G endlich ist. Es gibt auch unendliche zyklische Gruppen, aber es ist untypisch, dass man von diesen Generatoren suchen muss. Es reicht aus sich zu merken, dass 1 und -1 Generatoren von $\langle \mathbb{Z}; +, -, 0 \rangle$ ist, also von den Ganzzahlen unter der Addition.
Ein Generator ist ein Element a von einer Gruppe G, sodass die Menge der Potenzen von a G ist. Das bedeutet, dass wir durch Potenzierung von a jedes Element in G einmal erreichen. Generatoren existieren nur in besonderen Gruppen, den zyklischen Gruppen. Viele Gruppen sind nicht zyklisch und haben somit keine Generatoren. 1 ist zum Beispiel kein Generator von $\langle \mathbb{Z}_7^*; \odot \rangle$, weil 1 potenziert immer nur 1 ergibt.
Um effizient nach Generatoren zu suchen, sind zwei Resultate aus dem Skript wichtig. Zum Einen bilden die Potenzen von $a \in G$ eine Untergruppe von G (im Skript unter Definition 5.14). Ausserdem teilt in einer endlichen Gruppe G die Ordnung jeder Untergruppe H die Gruppenordnung, also $|H| \mid |G|$ (Theorem 5.8). Die Untergruppe der Potenzen von a hat die Ordnung $\text{ord}(a)$. Das ist die kleinste positive Potenz von a, die das Neutralelement ist. Das liegt daran, dass wenn wir Potenzen a grösser als $\text{ord}(a)$ betrachten, wieder die gleichen Elemente

erhalten. Ein Beispiel: $\text{ord}(2) = 3$ in der Gruppe $\langle \mathbb{Z}_7^*; \odot \rangle$, weil:

$$2^0 = 1 \equiv_7 1$$
$$2^1 = 2 \equiv_7 2$$
$$2^2 = 4 \equiv_7 4$$
$$2^3 = 8 \equiv_7 1$$
$$2^4 = 16 \equiv_7 2$$
$$2^5 = 32 \equiv_7 4$$

Wir sehen, dass sich die Folge von Elementen 1, 2, 4, ... bei Potenzen grösser als 2 wiederholt. In einer endlichen Gruppe reicht es aus, die positiven Potenzen von a zu betrachten.
Weil die Potenzen von a eine Untergruppe von G mit Ordnung $\text{ord}(a)$ sind und die Ordnung einer Untergruppe die Gruppenordnung teilt, muss $\text{ord}(a) \mid |G|$ gelten.
Damit wir dieses Resultat konkret anwenden können, müssen wir die Ordnung von $\langle \mathbb{Z}_7^*; \odot \rangle$ rausfinden, also wie viele Elemente $\mathbb{Z}_7^*$ hat. Wir könnten alle Elemente auflisten, aber für den Spezialfall $\mathbb{Z}_n^*$ gibt es eine Formel[2]. Die Phi-Funktion gibt uns genau die Kardinalität von $\mathbb{Z}_n^*$, also die Anzahl teilerfremder Zahlen zu n im Bereich $1 \leq x \leq n-1$. Um diese zu berechnen, müssen wir die Primfaktorenzerlegung von n finden. Betrachte zum Beispiel $n = 72$. Die Primfaktorenzerlegung ist $72 = 2^3 \cdot 3^2$. Nun berechnen wir $\varphi(n)$ wie folgt: Für jede vorkommende Primzahl p in der Primfaktorzerlegung berechnen wir das Produkt von $p-1$ und p^i, wobei i der Exponent von p in der Primfaktorzerlegung Minus 1 ist. In diesem Beispiel erhalten wir für die 2 $(2-1) \cdot 2^{3-1} = 4$ und für die 3 $(3-1) \cdot 3^{2-1} = 6$. $\varphi(n)$ ist dann das Produkt all dieser Zahlen, also in diesem Fall: $\varphi(72) = 4 \cdot 6 = 24$. Die Primfaktorzerlegung von 7 ist 7^1, deshalb $\varphi(7) = (7-1) \cdot 7^{1-1} = 6$.
Jetzt finden wir alle Teiler von der Gruppenordnung 6: Diese sind 1, 2, 3 und 6. Weil die Ordnung von einem Element immer die Gruppenordnung teilt, können die Elemente von $\langle \mathbb{Z}_7^*; \odot \rangle$ nur die Ordnungen 1, 2, 3 und 6 haben. Wenn ein Element die Ordnung 6 hat, ist es ein Generator. Denn dann hat die Untergruppe der Potenzen dieses Elements 6 Elemente, also genau so viele Elemente wie die ganze Gruppe. In allen anderen Fällen ist es kein Generator. Wir prüfen also nun für alle Elemente, ob sie die Ordnung 1, 2 oder 3 haben. Jedes Element, das keine dieser Ordnungen hat, hat die Ordnung 6 und ist damit ein Generator. Die Resultate sind in der Tabelle aufgeführt.

Wir sehen: 1 hat die Ordnung 1, 2 hat die Ordnung 3, 4 hat die Ordnung 3 und 6 hat die Ordnung 2, weil das jeweils die kleinsten Potenzen sind, die das

[2] Wir müssen die Elemente später sowieso auflisten, um deren Potenzen zu berechnen. Die Phi-Funktion könnte uns aber zum Beispiel Arbeit sparen, wenn wir eine Gruppe bekommen und nur für ein konkretes Element prüfen sollen, ob es ein Generator ist. Ausserdem gibt es auch andere Aufgaben, bei denen man die Phi-Funktion berechnen muss.

a	a^1	a^2	a^3
1	1	1	1
2	2	4	1
3	3	2	6
4	4	2	1
5	5	4	6
6	6	1	6

Tabelle 1: Potenzen der Elemente in $\mathbb{Z}_7^*$

Neutralelement ergeben. 3 und 5 müssen nach Ausschlussprinzip die Ordnung 6 haben. Also sind 3 und 5 genau die Generatoren von $\langle \mathbb{Z}_7^*; \odot \rangle$. Das bedeutet, dass wird durch Potenzieren von 3 und 5 alle Gruppenelemente erhalten. Überprüfen wir das noch schnell. Einmal für die 3:

$$
\begin{aligned}
3^0 &= 1 \equiv_7 1 \\
3^1 &= 3 \equiv_7 3 \\
3^2 &= 9 \equiv_7 2 \\
3^3 &= 27 \equiv_7 6 \\
3^4 &\equiv_7 18 \equiv_7 4 \\
3^5 &\equiv_7 12 \equiv_7 5
\end{aligned}
$$

Und für die 5:

$$
\begin{aligned}
5^0 &= 1 \equiv_7 1 \\
5^1 &= 5 \equiv_7 5 \\
5^2 &= 25 \equiv_7 4 \\
5^3 &\equiv_7 20 \equiv_7 6 \\
5^4 &\equiv_7 30 \equiv_7 2 \\
5^5 &\equiv_7 10 \equiv_7 3
\end{aligned}
$$

Hier ist es wichtig, einen Trick der modularen Arithmetik zu verwenden, damit man nicht mit riesigen Zahlen rechnen muss. Anstatt die Potenzen jedes Mal tatsächlich zu berechnen, können wir einfach die vorherige Potenz einmal multiplizieren. Statt 5^5 zu berechnen, rechnen wir $R_7(5 \cdot 2) = 10$, weil $5^4 \equiv_7 2$ ist.

2.2 Rezept

Hier noch einmal das Vorgehen zusammengefasst. Sei G irgendeine endliche Gruppe. Um die Generatoren zu finden, gehen wir wie folgt vor:

1. Finde die Gruppenordnung von G
   - Im Fall der Gruppe $\langle \mathbb{Z}_n; + \rangle$: $|G| = n$
   - Im Fall der Gruppe $\langle \mathbb{Z}_n^*; \cdot \rangle$: $|G| = \varphi(n)$
   - Bei sonstigen Gruppen: Liste alle Elemente auf
2. Finde alle positiven Teiler der Gruppenordnung $t_1, t_2, ...$
3. Für alle Teiler $t_i \neq |G|$: Berechne die t_i-te Potenz aller Gruppenelemente
4. Prüfe für jedes Element, ob eine der Potenzen $t_i \neq |G|$ dieses Elements das Neutralelement ist. Diese Elemente sind keine Generatoren. Alle anderen Elemente sind Generatoren.

Für die Gruppe $\langle \mathbb{Z}_n; + \rangle$ gibt es alternativ einen besonderen Trick: Die Generatoren sind genau die Elemente $a \in \mathbb{Z}_n$ mit $\gcd(a, n) = 1$ (Beispiel 5.27 im Skript). Aber wenn ihr euch diesen nicht merken wollt, lernt die obere Methode. Diese funktioniert immer.

3 Eigenschaften von Ringen

Ringe sind Algebren mit zwei Operationen, häufig Addition und Multiplikation genannt. Sie weisen Eigenschaften auf, die wir so schon von den reellen Zahlen kennen, wie die Assoziativität von Addition und Multiplikation und das Distributivgesetz. Trotzdem gibt es auch einige wichtige Unterschiede: Die Multiplikation ist nicht notwendigerweise kommutativ, Elemente haben nicht unbedingt multiplikative Inverse und Zahlen wie 2 müssen in einem Ring nicht notwendigerweise enthalten sein. Deshalb müssen wir sehr vorsichtig mit elementar aussehenden Eigenschaften, wie zum Beispiel $(-1) \cdot a = -a$ sein. Diese erfordern alle einen Beweis, der nur die Ringaxiome verwendet. Nur weil diese Fakten offensichtlich aussehen, weil wir sie von den reellen Zahlen kennen, müssen sie noch lange nicht für allgemeine Ringe gelten. Die Symbole 1 und 0 werden verwendet, um die Neutralelemente der Multiplikation und Addition in einem Ring zu bezeichnen. Das führt aber oft zum Trugschluss, dass die Elemente von einem Ring Zahlen sind. Tatsächlich können die Elemente von Ringen irgendwelche mathematischen Objekte sein, zum Beispiel Mengen. Deshalb dürfen wir in einem Beweis von Eigenschaften eines Rings nicht $1 + 1 = 2$ schreiben, weil die 2 ja gar nicht in dem Ring enthalten sein muss. Die Algebra $\langle \mathbb{Z}_1; +, -, 0, \cdot, 1 \rangle$ ist ein Ring, weil sie alle Ringaxiome erfüllt, aber $2 \notin \mathbb{Z}_1 = \{0\}$. Für diesen Ring stehen die 1 und 0 beide für das Element 0 des Rings, weil 0 in diesem Ring sowohl das additive als auch das multiplikative Neutralelement ist.

3.1 Beweis von Ringeigenschaften

Im Folgendem sollen wir folgendes Theorem beweisen, dürfen aber nur die Ringaxiome und den Fakt $0 \cdot a = a \cdot 0 = 0$ für alle $a \in R$ verwenden[3]

Theorem. *Sei $\langle R; +, -, 0, \cdot, 1\rangle$ ein Ring. Für alle $a, b \in R$ gilt:*

$$(-a)b = a(-b)$$

Wie auch bei Beweisen in der Gruppentheorie, müssen wir auf Tricks zurückgreifen, wie das Einfügen von unnötigen Neutralelementen. Wenn man einige von solchen Beweisen gesehen hat, gewöhnt man sich an die Tricks und bekommt eine Intuition dafür, wie man sie verwenden kann. Weil ein Ring R dadurch definiert ist, dass $\langle R; +, -, 0\rangle$ eine Gruppe ist und $\langle R; \cdot, 1\rangle$ ein Monoid ist, kommen die Gruppenaxiome/Monoidaxiome sowie die zugehörigen Lemmas in Beweisen über Ringe vor.

Beweis. Seien $a, b \in R$ beliebig.

$$\begin{aligned}
(-a)b &= 0 + (-a)b && (\textbf{G2} \text{ von } \langle R; +, -, 0\rangle)\\
&= a0 + (-a)b && (a0 = 0)\\
&= a(-b + b) + (-a)b && (\textbf{G3} \text{ von } \langle R; +, -, 0\rangle)\\
&= (a(-b) + ab) + (-a)b && (\text{Linkes Distributivgesetz von } R)\\
&= a(-b) + (ab + (-a)b) && (\textbf{G1} \text{ von } \langle R; +, -, 0\rangle)\\
&= a(-b) + (a + -a)b && (\text{Rechtes Distributivgesetz von } R)\\
&= a(-b) + 0b && (\textbf{G3} \text{ von } \langle R; +, -, 0\rangle)\\
&= a(-b) + 0 && (0b = 0)\\
&= a(-b) && (\textbf{G2} \text{ von } \langle R; +, -, 0\rangle)
\end{aligned}$$

□

Ich habe diesen Beweis sehr formell aufgeschrieben. Wenn man Ringeigenschaften beweist ist es in Ordnung, etwas nachlässiger zu sein. Man kann zum Beispiel schreiben "+ ist assoziativ wegen **G1** von $\langle R; +, -, 0\rangle$" und einfach Klammern weglassen (statt sie umzusetzen). Aber meiner Meinung nach ist es ist eine sehr gute Übung zu versuchen, vollständig formal zu bleiben und die Regeln genau in der richtigen Form anzuwenden. Dann macht man keine Fehler bei Beweisen, bei denen ein höherer Grad der Formalität erwartet wird.
Im Folgenden wollen wir eine weitere Eigenschaft beweisen. Es ist zu der Aufgabe noch der Hinweis gegeben, dass man zuerst $a + a = 0$ für alle $a \in R$ zeigen soll. **Generell solltet ihr euch bei solchen Aufgaben immer an den gegebenen Hinweisen orientieren, diese sind sehr hilfreich!**

[3]Dieser Fakt gilt in jedem Ring, ist aber, obwohl es so aussieht, nicht trivial, sondern erfordert einen Beweis. Dieser ist im Skript unter Lemma 5.17.

Theorem. *Sei* $\langle R; +, -, 0, \cdot, 1\rangle$ *ein Ring, sodass für alle* $a \in R$*:*

$$a \cdot a = a$$

$\langle R; +, -, 0, \cdot, 1\rangle$ *ist kommutativ.*

Beweis. Sei $a \in R$ beliebig.

$$\begin{aligned}
a + a &= (a + a) \cdot (a + a) && (a \cdot a = a) \\
&= (a + a)a + (a + a)a && \text{(Linkes Distributivgesetz von } R) \\
&= (aa + aa) + (aa + aa) && \text{(Rechtes Distributivgesetz von } R) \\
&= (a + a) + (a + a) && (a \cdot a = a) \qquad (1)
\end{aligned}$$

Ausserdem

$$a + a = (a + a) + 0 \qquad (\textbf{G2} \text{ von } \langle R; +, -, 0\rangle) \qquad (2)$$

Weil $\langle R; +, -, 0\rangle$ eine Gruppe ist, folgt mit dem Left Cancellation Law, 1 und 2

$$a + a = 0$$

Jedes $a \in R$ ist also Inverses von a bezüglich der Addition. Weil $\langle R; +, -, 0\rangle$ eine Gruppe ist, kann jedes Element nur ein Inverses bezüglich der Addition haben. Nach **G3** von $\langle R; +, -, 0\rangle$ ist $-a$ ein Inverses von a bezüglich der Addition. Also $a = -a$.
Seien nun $a, b \in R$ beliebig.

$$\begin{aligned}
a + 0 + b &= a + b && (\textbf{G2} \text{ von } \langle R; +, -, 0\rangle) \\
&= (a + b) \cdot (a + b) && (a \cdot a = a) \\
&= (a + b)a + (a + b)b && \text{(Linkes Distributivgesetz von } R) \\
&= (aa + ba) + (ab + bb) && \text{(Rechtes Distributivgesetz von } R) \\
&= (a + ba) + (ab + b) && (a \cdot a = a) \\
&= a + ba + ab + b && (\textbf{G1} \text{ von } \langle R; +, -, 0\rangle) \qquad (3)
\end{aligned}$$

Weil $\langle R; +, -, 0\rangle$ eine Gruppe ist, folgt mit den beiden Cancellation Laws und 3

$$\begin{aligned}
0 = ba + ab &\overset{\cdot}{\Longrightarrow} -(ba) + 0 = -(ba) + (ba + ab) && \text{(Addition von } -(ba) \text{ auf beiden Seiten von links)} \\
&\overset{\cdot}{\Longrightarrow} -(ba) = -(ba) + (ba + ab) && (\textbf{G2} \text{ von } \langle R; +, -, 0\rangle) \\
&\overset{\cdot}{\Longrightarrow} -(ba) = (-(ba) + ba) + ab && (\textbf{G1} \text{ von } \langle R; +, -, 0\rangle) \\
&\overset{\cdot}{\Longrightarrow} -(ba) = 0 + ab && (\textbf{G3} \text{ von } \langle R; +, -, 0\rangle) \\
&\overset{\cdot}{\Longrightarrow} -(ba) = ab && (\textbf{G2} \text{ von } \langle R; +, -, 0\rangle) \\
&\overset{\cdot}{\Longrightarrow} ba = ab && (a = -a)
\end{aligned}$$

Also ist $\langle R; +, -, 0, \cdot, 1\rangle$ per Definition kommutativ. □