Diskrete Mathematik Übungsstunde Zusammenfassung

Leon Kolmanić

13.11.2023

1 Besprechung Bonusaufgabe

Häufige Fehler waren:

- Produktzeichen $\prod$ falsch interpretiert
- Notationsprobleme
  - keine Doppelpfeile/Pfeile in die falsche Richtung
  - Umformungen ohne Pfeile/Gleichheitszeichen
- Fälle in der Fallunterscheidung vergessen
- $\min(x, \max(y, z)) = \max(\min(x, y), \min(x, z))$ nicht bewiesen
- Fallunterscheidung nicht für jedes i einzeln gemacht

Das Zeichen $\prod$ ist das Äquivalent von $\sum$ für Produkte. Es wird verwendet, um regelmässige Produkte zu notieren. In dem Kontext der Zahlentheorie kann man zum Beispiel

$$a = \prod_i {p_i}^{e_i}$$

schreiben, um a in der Primfaktorzerlegung zu schreiben. p_i steht hier für die i-te Primzahl und e_i für den Exponent der i-ten Primzahl in der Primfaktorzerlegung von a. Eine andere mögliche Notation wäre

$${p_1}^{e_1} \cdot {p_2}^{e_2} \cdot (...)$$

Wenn man sich im Umgang mit $\prod$ nicht so sicher fühlt, kann ich empfehlen, den Ausdruck auf diese Weise umzuschreiben.
Einige von euch haben ihren Beweis folgendermassen strukturiert:

$$\begin{aligned} &\gcd(a, \operatorname{lcm}(b, c)) = \operatorname{lcm}(\gcd(a, b), \gcd(a, c)) \\ \dot{\Longrightarrow} &\gcd(a, \prod_i {p_i}^{\max(f_i, g_i)}) = \operatorname{lcm}(\prod_i {p_i}^{\min(e_i, f_i)}, \prod_i {p_i}^{\min(e_i, g_i)}) \\ \dot{\Longrightarrow} &\prod_i {p_i}^{\min(e_i, \max(f_i, g_i))} = \prod_i {p_i}^{\max(\min(e_i, f_i), \min(e_i, g_i))} \end{aligned} \tag{1}$$

Dann wurde ein Beweis für Gleichung 1 gegeben. So ist der Beweis aber formal nicht korrekt. Es wurde hier mit der Aussage, die man zeigen soll, angefangen und daraus eine wahre Aussage hergeleitet. In einem Beweis müssen wir aber durch unsere Argumentation von wahren Aussagen (zum Beispiel den Annahmen) beginnen und bei der zu zeigenden Aussage ankommen. Um diesen formalen Fehler zu korrigieren, kann man alle $\dot{\Longrightarrow}$ zu $\dot{\Longleftarrow}$ ändern.
Einige von euch haben Umformungen und Beweisschritte gemacht, ohne $=$ oder $\dot{\Longrightarrow}$ zu verwenden. Das macht euren Beweis weniger verständlich und kann für Abzug sorgen.
Wenn man eine Fallunterscheidung macht, ist es entscheidend, dass man alle möglichen Fälle berücksichtigt. Wenn a und b zum Beispiel zwei Ganzzahlen sind, reicht es nicht aus, die Fälle $a < b$ und $b < a$ zu betrachten. Dann ist nämlich $a = b$ nicht abgedeckt. Man kann die Fallunterscheidung korrigieren, indem man die Fälle $a \leq b$ und $b \leq a$ betrachtet. Bei einer Fallunterscheidung ist es in Ordnung, wenn sich Fälle überschneiden.
Die Gleichung $\min(x, \max(y, z) = \max(\min(x, y), \min(x, z))$ zu beweisen, war der wichtigste Teil des Beweises. Wenn man sie als trivial vorausgesetzt hat, hat man sehr viele Punkte verloren. Wenn ihr euch bei einer Bonusaufgabe nicht sicher seid, ob ihr etwas verwenden dürft, könnt ihr gerne mich fragen.
Einige Leute haben den Fehler gemacht, dass sie die Fallunterscheidung auf alle i gleichzeitig bezogen haben. Also es wurde z.B. $e_i \leq f_i \leq g_i$ *für alle* i angenommen und damit Gleichung 1 von oben bewiesen. Aber das ist so nicht ganz sauber, denn für jedes i könnte ein anderer Fall eintreten, also es könnte zum Beispiel $e_1 < f_1 < g_1$, aber $g_2 < f_2 < e_2$ gelten. Dann muss man für $i = 1$ und $i = 2$ verschiedene Fälle betrachten. Der formal korrekte Weg war es, *für ein* beliebiges i die Fallunterscheidung zu machen und aus dieser die Gleichheit der i-ten Faktoren der beiden Produkte zu folgern.

2 Beweis von Gruppenaxiomen

Wir wollen folgendes Theorem zeigen:

Theorem. *Sei* $S = (\mathbb{Q} \setminus \{0\}) \times \mathbb{Q}$. *Betrachte die Algebra* $\langle S; * \rangle$, *wobei* $*$ *für alle* $(a, b), (c, d) \in S$ *definiert ist durch*

$$(a, b) * (c, d) = (ac, ad + b)$$

$\langle S; * \rangle$ *ist eine Gruppe.*[1]

Um zu zeigen, dass eine bestimmte Algebra eine Gruppe ist, müssen wir die drei Gruppenaxiome zeigen. Wir müssen also zeigen, dass $*$ assoziativ ist, dass es ein neutrales Element e gibt und dass es für jedes Element $a \in S$ ein inverses Element $\hat{a} \in S$ gibt sodass $a * \hat{a} = \hat{a} * a = e$.

[1] Für eine Gruppe braucht es natürlich noch eine nulläre Operation e, die das Neutralelement zurückgibt, und eine unäre Operation $\hat{}$, die zu einem Element das Inverse zurückgibt. Diese werden aber oft bei der Notation einer Gruppe weggelassen, so auch hier.

Für den Beweis der Assoziativität von $*$ wählen wir $(a,b),(c,d),(e,f) \in S$ beliebig und zeigen $((a,b)*(c,d))*(e,f) = (a,b)*((c,d)*(e,f))$. Bei dem Beweis von Gleichheiten ist es oft sinnvoll, sich zu überlegen, was das Ziel ist und wo man anfängt. Wir fangen mit $((a,b)*(c,d))*(e,f)$ an. Wir formen zunächst diesen Ausdruck mit der Definition von $*$ um:

$$\begin{aligned}((a,b)*(c,d))*(e,f) &= (ac, ad+b)*(e,f) \\ &= ((ac)e, (ac)f + (ad+b)) \end{aligned} \tag{2}$$

Das Ziel der Umformung ist $(a,b)*((c,d)*(e,f))$. Jetzt formen wir diesen Ausdruck um:

$$\begin{aligned}(a,b)*((c,d)*(e,f)) &= (a,b)*(ce, cf+d) \\ &= (a(ce), a(cf+d)+b) \end{aligned} \tag{3}$$

Nun müssen wir im Beweis nur noch die "Lücke" zwischen 2 und 3 schliessen. Für das neutrale Element überlegen wir uns welches Paar $(e_1,e_2) \in (\mathbb{Q}\setminus\{0\})\times\mathbb{Q}$ andere Paare "unverändert" lässt:

$$(a,b)*(e_1,e_2) = (ae_1, ae_2+b) \overset{!}{=} (a,b)$$

Wenn wir $e_1 = 1$ und $e_2 = 0$ wählen, gilt die Gleichung für beliebige $(a,b) \in S$. Jetzt haben wir aber nur überprüft, dass (e_1,e_2) ein rechtes Neutralelement ist. Im Beweis müssen wir noch zeigen, dass es auch ein linkes Neutralelement ist. Ein neutrales Element ist nach Definition nämlich ein rechtes Neutralelement und ein linkes Neutralelement.
Für die inversen Elemente überlegen wir uns, wie wir für jedes $(a,b) \in S$ $(c,d) \in S$ wählen können, sodass folgendes gilt:

$$(a,b)*(c,d) = (ac, ad+b) \overset{!}{=} \underbrace{(1,0)}_{\text{unser gefundenes Neutralelement}}$$

Wir sehen, dass für die Wahl $c = \frac{1}{a}$ und $d = \frac{-b}{a}$ die Gleichung erfüllt ist. Im Beweis müssen wir auch hier beide Seiten überprüfen[2]. Hier sollte man beachten, dass wir nur durch a teilen dürfen, weil $S = (\mathbb{Q}\setminus\{0\})\times\mathbb{Q}$ gilt, also die linken Elemente von Paaren aus S sind nicht 0.
Diese Überlegungen kann man folgendermassen formal umsetzen:

Beweis. Wir zeigen, dass alle drei Gruppenaxiome für $\langle S; * \rangle$ erfüllt sind.

[2]Im Skript wird bewiesen, dass die Gruppenaxiome nicht minimal sind, also dass man sie relaxieren kann, ohne die Bedeutung zu verändern. Deshalb muss man hier nicht zeigen, dass $(1,0)$ auch ein rechtes Inverses ist, wenn man auf den entsprechenden Beweis im Skript verweist.

G1 Seien $(a,b),(c,d),(e,f) \in S$ beliebig.

$$\begin{aligned}((a,b)*(c,d))*(e,f) &= (ac, ad+b)*(e,f) \text{ (Def. } *) \\ &= ((ac)e, (ac)f + (ad+b)) \text{ (Def. } *) \\ &= (ace, acf + ad + b) \text{ ($\mathbb{Q}$ Arithmetik)} \\ &= (a(ce), a(cf+d) + b) \text{ ($\mathbb{Q}$ Arithmetik)} \\ &= (a,b)*(ce, cf+d) \text{ (Def. } *) \\ &= (a,b)*((c,d)*(e,f)) \text{ (Def. } *)\end{aligned}$$

G2 Sei $(a,b) \in S$ beliebig. Betrachte $(1,0) \in S$. Es gilt:

$$\begin{aligned}(a,b)*(1,0) &= (a \cdot 1, a \cdot 0 + b) \text{ (Def. } *) \\ &= (a,b) \text{ ($\mathbb{Q}$ Arithmetik)}\end{aligned}$$

Ausserdem:

$$\begin{aligned}(1,0)*(a,b) &= (1 \cdot a, 1 \cdot b + 0) \text{ (Def. } *) \\ &= (a,b) \text{ ($\mathbb{Q}$ Arithmetik)}\end{aligned}$$

Also ist $(1,0)$ per Definition ein neutrales Element von $\langle S; * \rangle$.

G3 Sei $(a,b) \in S$ beliebig. Nach der Definition von S: $a \neq 0$. Also ist $\frac{1}{a}$ wohldefiniert und $\frac{1}{a} \neq 0$. Betrachte nun $(\frac{1}{a}, \frac{-b}{a}) \in S$. Wir haben:

$$\begin{aligned}(a,b)*(\frac{1}{a}, \frac{-b}{a}) &= (a \cdot \frac{1}{a}, a \cdot \frac{-b}{a} + b) \text{ (Def. } *) \\ &= (1,0) \text{ ($\mathbb{Q}$ Arithmetik)}\end{aligned}$$

Weiter:

$$\begin{aligned}(\frac{1}{a}, \frac{-b}{a})*(a,b) &= (\frac{1}{a} \cdot a, \frac{1}{a} \cdot b + \frac{-b}{a}) \text{ (Def. } *) \\ &= (1,0) \text{ ($\mathbb{Q}$ Arithmetik)}\end{aligned}$$

□

3 Eigenschaften von Homomorphismen

Wir möchten im Folgendem Lemma 5.5 aus dem Skript beweisen. Dieses macht zwei Aussagen über einen Homomorphismus $\psi : G \to H$ von einer Gruppe $\langle G; *, \hat{}, e \rangle$ zu einer Gruppe $\langle H; \star, \tilde{}, e' \rangle$.

Lemma. *Für ψ gilt:*

i) $\psi(e) = e'$

ii) $\psi(\hat{a}) = \widetilde{\psi(a)}$

Um den ersten Teil des Lemmas zu beweisen, nutzen wir einen Trick, der bei solchen Beweisen häufig nützlich ist. Wir fügen "unnötige" Neutralelemente ein. Es ist wichtig zu beachten, welche Gruppenaxiome wir verwenden, also ob wir die von G oder H verwenden. $e \in G$, deshalb verwenden wir für die Umformung $e = e * e$ das Gruppenaxiom 2 von G. Für die Umformung $\psi(e) = \psi(e) \star e'$ verwenden wir das Gruppenaxiom 2 von H, weil $\psi(e)$ ein Element von H ist.

Beweis.

$$\begin{aligned} \psi(e) &= \psi(e * e) \text{ (**G2** von } G) \\ &= \psi(e) \star \psi(e) \text{ (ψ ist ein Homomorphismus)} \end{aligned} \tag{4}$$

Weiter:

$$\psi(e) = \psi(e) \star e' \text{ (**G2** von } H) \tag{5}$$

Zusammen mit 4 und 5 erhalten wir:

$$\psi(e) \star \psi(e) = \psi(e) \star e' \tag{6}$$

Mit 6 und dem "Left cancellation law" (Lemma 5.3 (iii)) folgt:

$$\psi(e) = e'$$

□

Die Tricks bei solchen Beweisen sind immer ähnlich. Wenn man viele von solchen Aufgaben löst, bekommt man eine Intuition dafür, wie man vorgehen kann.
Um die zweite Eigenschaft zu beweisen, überlegen wir uns, wie wir die Gleichung in Worten ausdrücken können. Dann ist der Beweis auch einfacher. Wenn wir $\tilde{a}$ für ein $a \in H$ schreiben, meinen wir das inverse Element von a. $\tilde{a} = b$ bedeutet zum Beispiel: Das inverse Element von a ist b. Das Lemma sagt also aus: Das inverse Element von $\psi(a)$ ist $\psi(\hat{a})$. Es ist einfach zu prüfen, ob ein Element b ein inverses Element von a ist. Wir schauen, ob bei $a \star b$ und $b \star a$ e' rauskommt.

Beweis.

$$\begin{aligned} \psi(a) \star \psi(\hat{a}) &= \psi(a * \hat{a}) \text{ (ψ ist ein Homomorphismus)} \\ &= \psi(e) \text{ (**G3** von G)} \\ &= e' \text{ (Lemma (i))} \end{aligned}$$

$\psi(\hat{a})$ ist also ein rechtes Inverses von $\psi(a)$. Wir zeigen noch, dass es ein linkes Inverses ist:

$$\begin{aligned} \psi(\hat{a}) \star \psi(a) &= \psi(\hat{a} * a) \text{ (ψ ist ein Homomorphismus)} \\ &= \psi(e) \text{ (**G3** von G)} \\ &= e' \text{ (Lemma (i))} \end{aligned}$$

$\psi(\hat{a})$ ist also ein inverses Element von $\psi(a)$. Weil $\widetilde{\psi(a)}$ auch ein inverses Element von $\psi(a)$ ist (**G2** von H) und es nach Lemma 5.2 nur ein inverses Element von einem Element geben kann, folgt

$$\psi(\hat{a}) = \widetilde{\psi(a)}$$

wie gewünscht. □

4 Isomorphie

Ein Isomorphismus ist ein bijektiver Homomorphismus. Wenn wir zwischen zwei Gruppen G und H einen Isomorphismus finden, nennen wir sie isomorph und schreiben $G \simeq H$. Dass zwei Gruppen isomorph sind bedeutet intuitiv, dass die Gruppen sich gleich verhalten, aber die Elemente andere Namen haben. Im Allgemeinen ist es schwierig, einen Isomorphismus zwischen zwei Gruppen zu finden. Oft erfordert das ein tieferes Verständnis über die Struktur der beiden Gruppen. Im Folgendem wollen wir beispielhaft die Isomorphie der folgenden Gruppen informell zeigen:

Theorem. $\mathbb{Z}_3^* \simeq \mathbb{Z}_4^*$

Für den Beweis müssen wir eine Funktion von $\mathbb{Z}_3^*$ nach $\mathbb{Z}_4^*$ angeben. Diese soll die "Umbenennung" der Elemente repräsentieren, also sie soll uns für jedes $a \in \mathbb{Z}_3^*$ sagen, welches $f(a) \in \mathbb{Z}_4^*$ diesem "entspricht". Wir schauen uns zunächst die Multiplikationstabellen der beiden Gruppen an:

	1	2
1	1	2
2	2	1

Tabelle 1: Multiplikationstabelle $\mathbb{Z}_3^*$

	1	3
1	1	3
3	3	1

Tabelle 2: Multiplikationstabelle $\mathbb{Z}_4^*$

Die Tabellen haben eine grosse Ähnlichkeit miteinander, diese Ähnlichkeit ist die Isomorphie. Diese ist farblich noch mal hervorgehoben. Wegen dem Lemma von oben wissen wir, dass jeder Isomorphismus dem Neutralelement das Neutralelement zuweist. In beiden Gruppen ist das Neutralelement 1, also wird unser Isomorphismus 1 auf 1 abbilden. Durch die Multiplikationstabellen wird klar, dass 2 die gleiche Rolle in $\mathbb{Z}_3^*$ spielt, wie 3 in $\mathbb{Z}_4^*$. Eine Gemeinsamkeit ist zum Beispiel: Beide Elemente ergeben mit sich selbst multipliziert das Neutralelement 1. Wir können also $\psi : \mathbb{Z}_3^* \to \mathbb{Z}_4^*$ definieren durch $\psi(1) = 1$ und

$\psi(2) = 3$. Diese Funktion ist offensichtlich bijektiv und durch die Multiplikationstabellen können wir sehen, dass ψ auch ein Homomorphismus ist. Wir können dies aber auch manuell überprüfen, indem wir für alle $a, b \in \mathbb{Z}_3^*$ prüfen, ob $\psi(a \odot_3 b) = \psi(a) \odot_4 \psi(b)$ gilt. $\odot_n$ steht hier für die Multiplikation modulo n.
Hinweis: Dieses sehr kleine Beispiel sollte veranschaulichen, was Isomorphie bedeutet und zeigen, wie man sich über die Multiplikationstabellen einen Isomorphismus erschliessen kann. Das war aber kein formaler Beweis. In einem Beweis müsste man zum Beispiel zeigen, dass ψ ein Homomorphismus ist. Um nicht zu viel für die Bonusaufgabe diese Woche vorwegzunehmen, lasse ich den formalen Beweis an dieser Stelle aber aus.