Hausaufgaben zu Algebraische Strukturen / Linearen Algebra 2

Prof. Dr. P. Pickl
Kajetan Söhnen

Lösungsvorschlag zu Blatt 6

Aufgabe 1 *(2 Punkte)*: Zeigen Sie, dass $\leq$ ("Untergruppe sein") transitiv ist.
Zeigen Sie weiter, dass $\trianglelefteq$("Normalteiler sein") im allgemeinen nicht transitiv ist.

Tipp: Nutzen Sie den Normalteiler $U \trianglelefteq A_4$ vom Tutoriumsblatt.

Lösungsvorschlag. Sei U eine Untergruppe von V die eine Untergruppe von G ist. Als Untergruppe von V ist U nicht leer. Außerdem muss für alle $a, b \in U$ gelten, dass $a \circ b^{-1} \in U$. Wir sehen, dass in der Definition die Obermenge V gar nicht vorkommt. Damit ist auch klar, dass U eine Untergruppe von G ist. Wenn man ganz exakt sein will, sollte man sich überlegen, dass V die gleiche Verknüpfung nutzt wie G und U die gleiche wie V und damit auch U die gleiche Verknüpfung wie G nutzt.

Um zu zeigen, dass Normalteiler sein nicht transitiv ist, betrachten wir

$$U = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq A_4$$

vom Tutoriumsblatt. Wir müssen nun ein Untergruppe $V \leq U$ angeben, sodass $V \trianglelefteq U$ aber $V \not\trianglelefteq A_4$.

Wir betrachten $V = \{(1), (1\ 2)(3\ 4)\}$. Zunächst zeigen wir, dass $V \not\trianglelefteq A_4$. Wir betrachten den Zyklus $(1\ 2\ 3) = (1\ 2)(2\ 3) \in A_4$.

Mit der Aufgabe 1 vom Tutoriumsblatt erhalten wir

$$(1\ 2\ 3)(1\ 2)(3\ 4)(3\ 2\ 1) = (2\ 3)(1\ 4) \notin V.$$

Damit ist V kein Normalteiler von A_4.

Es bleibt zu zeigen, dass V ein Normalteiler in U ist.

Auf dem Tutoriumsblatt haben wir bereits gesehen, dass U kommutativ ist, (U hat nur 4 Elemente) und somit sind alle Untergruppen Normalteiler. Damit haben wir $V \trianglelefteq U$ und $U \trianglelefteq A_4$ aber nicht $V \trianglelefteq A_4$ was die Transitivität widerlegt. □

Aufgabe 2 *(2 Punkte)*: Sei K ein endlicher Körper mit Charakteristik ungleich 2. Zeigen sie, dass genau die Hälfte der Elemente von $K\backslash\{0\}$ Quadratzahlen sind. Wie verhält es

sich mit Körpern der Charakteristik 2? Hinweis: Betrachten Sie die Abbildung f, die jedes Element aus K auf dessen Quadratzahl abbildet ($f(x) = x^2$).

Lösungsvorschlag. Sei f die Abbildung $x \mapsto x^2$. Die Abbildung ist ein Gruppenhomomorphismus, da $xy \mapsto (xy)^2 = x^2y^2$ und $x^{-1} \mapsto x^{-2} = (x^2)^{-1}$. Der Kern der Abbildung enthält zwei Elemente, nämlich 1 und -1, da bei Zahlen beim Quadrieren auf dem neutralen Element in $K \setminus \{0\}$ landen, nämlich bei 1. Hier nutzen wir das $\operatorname{char} K \neq 2$. Ansonsten wäre $-1 = 1$ und der Kern hätte nur ein Element. Sei $Q \subseteq K$ die Menge der Quadratzahlen ungleich 0. Dann ist

$$f : K \setminus \{0\} \to Q$$

surjektiv und wir erhalten nach Homomorphiesatz, dass $Q \simeq (K \setminus \{0\})/\{-1, 1\}$.

Der Quotient rechts hat nach Vorlesung genau halb so viele Elemente wie $K \setminus \{0\}$ und wegen der Isomorphie hat auch Q genau halb so viele Elemente wie $K \setminus \{0\}$.

Im Fall von $\operatorname{char} K = 2$ ist die Abbildung f injektiv und entsprechend gibt es gleich viele Quadratzahlen wie Elemente in K, also muss jede Zahl eine Quadratzahl sein. Da die Abbildung x^2 also bijektiv ist, kann man auf $\operatorname{char} K = 2$ wunderbar eine Wurzelfunktion definieren. □

Aufgabe 3 *(2 Punkte)***:** Zeigen Sie, dass sich in endlichen Körpern jede Zahl als Summe zweier Quadratzahlen schreiben lässt. Hinweis: Betrachten Sie die Menge aller Quadrate $Q \subset K$ sowie für beliebiges $g \in K$ die Menge $g - Q$. Aufgabe 2 wird hier hilfreich sein.

Lösungsvorschlag. Für $\operatorname{char} K = 2$ sind alle Zahlen Quadratzahlen und die Aussage ist trivial. Sei nun $\operatorname{char} K \neq 2$. Sei n die Anzahl der Elemente in K. Nach Aufgabe 3 sind $(n+1)/2$ (von den $n-1$ ohne 0 die Hälfte und dazu noch die 0) Zahlen Quadratzahlen.

Sei nun $g \in K$ und Q wie in der Aufgabenstellung die Menge aller Quadratzahlen. Wir betrachten die Mengen $g - Q = \{g - q \mid q \in Q\}$ und $Q = \{q \mid q \in Q\}$. Beide Mengen sind Teilmengen von K die gleichmächtig sind wie Q, also $(n+1)/2$ Elemente enthalten. Die beiden Mengen können nicht disjunkt sein, da die Vereinigung dann $n+1$ Elemente enthalten müsste, was in $|K| = n$ nicht möglich ist. Also finden wir $q_1, q_2 \in Q$ sodass $g - q_1 = q_2$, also $g = q_1 + q_2$ was die Aussage beweist. □

Aufgabe 4 *(2 Punkte)***:** Gegeben Seien die Ziffern $0, 1, \ldots, 9, X$. Geben Sie ein Verfahren zur Prüfziffernkodierung an, dass zu einer neunstelligen Zahl aus diesen Ziffern, eine Prüfziffer erzeugt. Mit der Prüfziffer soll man sowohl Tippfehler an einer Stelle sowie das Vertauschen benachbarter Ziffern erkennen können. Beweisen sie, dass ihr System beide Fehler mit Sicherheit erkennen wird.

Lösungsvorschlag. Sei $M = \{0, 1, \ldots, 9, X\}$. Die Menge aller möglichen neunstelligen Zahlen ist $M^9 = M \times M \times \ldots \times M$.

Wir definieren die Prüfziffer als $P : M^9 \to M$ mit

$$P(x_1, \ldots, x_9) = x_1 + 2 \cdot x_2 + \ldots + 9 \cdot x_9 \mod 11.$$

Hierbei rechnen wir mit X wie mit der 10.

Hängen wir die Prüfziffer an die ursprüngliche Zahl an, erhalten wir ein 10stellige Zahl.

Angenommen beim übertragen dieser Zahl unterläuft uns an einer Stelle ein Fehler. Wenn wir die Prüfziffer falsch abschreiben, fällt das sofort auf. Wir berechnen aus den übrigen Stellen die richtige Prüfziffer und sehen sofort, dass etwas nicht stimmt.

Was passiert, wenn sich ein Fehler an einer der anderen Stellen einschleicht. Sei $k \in \{1, \ldots, 9\}$ beliebig. $x_1, \ldots, x_9, \tilde{x}_k \in M$. Dann gilt

$$\begin{aligned} P(x_1, \ldots, x_9) - P(x_1, \ldots, \tilde{x}_k, \ldots x_9) &= kx_k - k\tilde{x}_k \mod 11 \\ &= k(x_k - \tilde{x}_k) \mod 11 \end{aligned}$$

Wären beide Prüfziffern gleich, müsste das Ergebnis Null sein. Da $\mathbb{Z}/11\mathbb{Z}$ ein Körper ist, folgt, dass $k = 0 \mod 11$ oder $x_k - \tilde{x}_k = 0 \mod 11$. Da $k \in 1, \ldots 9$ kann ersteres nicht zu treffen und es folgt $x_k = \tilde{x}_k$. Im Umkehrschluss, führt ein Fehler in einer Stelle also zu einer Änderung der errechneten Prüfziffer. Solange wir in diesem Fall also die Prüfziffer richtig übertragen haben, fällt der Fehler also auf.

Was passiert wenn wir zwei Ziffern vertauschen. Zunächst betrachten wir was passiert, wenn wir die Prüfziffer mit ihrem Vorgänger, also der neunten regulären Ziffer vertauscht haben.

Die Prüfziffer der ursprünglichen Zahl, ist

$$P = P(x_1, \ldots, x_9) = x_1 + 2 \cdot x_2 + \ldots + 9 \cdot x_9 \mod 11.$$

Die neue Zahl ist also $x_1 x_2 \ldots x_8 P x_9$.

Wir möchten sicher stellen, dass x_9 nicht die Prüfziffer dieser Zahl ist und der Fehler somit auffällt. Die Prüfziffer errechnet sich (Wenn wir den Wert von P einsetzen) als

$$\begin{aligned} & x_1 + 2x_2 + \ldots + 8x_8 + 9(x_1 + 2x_2 + \ldots + 8x_8 + 9x_9) \mod 11 \\ =& x_1 + 2x_2 + \ldots + 8x_8 - 2(x_1 + 2x_2 + \ldots + 8x_8 + 9x_9) \mod 11 \\ =& -(x_1 + 2x_2 + 3x_3 + \ldots 8x_8 + 9x_9) - 9x_9 \mod 11 \\ =& -P - 9x_9. \end{aligned}$$

Angenommen das Ergebnis wäre x_9. Dann müsste $x_9 = -P - 9x_9 \mod 11$ also $P = x_9 \mod 11$ gelten. Da P und x_9 beides Zahlen zwischen 0 und $X = 10$ sind, müssten sie also gleich sein. Das heißt die letzte Ziffer der ursprünglichen Zahl und ihre Prüfziffer waren gleich. Dann war aber auch das "vertauschen"kein echter Fehler.

Was passiert wenn wir an einer anderen Stelle zwei Zahlen vertauschen? Sei hierzu $k \in 1, \ldots 8$. Wir betrachten

$$\begin{aligned} P(x_1, \ldots, x_9) - P(x_1, \ldots, x_{k+1}, x_k \ldots x_9) &= kx_k + (k+1)x_{k+1} - kx_{k+1} - (k+1)x_k \mod 11 \\ &= x_{k+1} - x_k \mod 11. \end{aligned}$$

Angenommen die Prüfziffer würde diesen Fehler nicht erkennen, dann wären beide Prüfziffern gleich und es folgt $x_{k+1} - x_k = 0 \mod 11$. Da (mit $X = 10$) beide Ziffern zwischen 0 und 10 liegen, $-10 \leq x_{k+1} - x_k \leq 10$. Die einzige Möglichkeit wie das Ergebnis durch 11 teilbar sein kann, ist also wenn es gleich Null ist und beide Ziffern gleich waren. Dann ist es aber auch kein Fehler beide Ziffern zu vertauschen. □