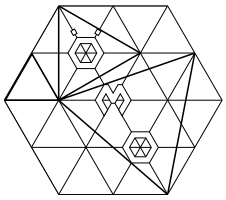

MATHEMATIK macht FREU(N)DE

52. Österreichische Mathematik-Olympiade

Fortgeschrittenen-Kurs „Mathematik macht Freu(n)de“ – Aufgabenblatt für den 18. Juni 2021

Ablauf

Dieses Aufgabenblatt wurde von Josef Greilhuber zusammengestellt.

Wir werden uns am 18. Juni um 16:20 vor dem Mathematik-Institut (Oskar-Morgenstern-Platz 1, 1090 Wien) unter dem roten Dodekaederstern treffen, und uns für die letzte Kurseinheit einen Platz in einem benachbarten Park suchen. Natürlich soll sich niemand gezwungen fühlen, anwesend zu sein, bitte kommt nur, wenn ihr euch damit wohlfühlt! Wenn ihr getestet oder geimpft seid, ist das natürlich besonders gut, wir werden uns aber auf jeden Fall so verhalten, dass alle Anwesenden sicher sein sollten (Abstand und Freiluft). Als Abwechslung wollen wir uns einmal nicht mit der üblichen Olympiademathematik beschäftigen, sondern mit einer der wichtigsten Klassen algebraischer Strukturen, den Gruppen.

Gruppen

Vielleicht die zentrale Idee der höheren Mathematik ist, statt ausschließlich bestimmter Mengen, wie z.B. der Menge der ganzen Zahlen oder der Menge der Polynome mit reellen Koeffizienten, ganz allgemeine Mengen zu betrachten, deren Elemente man so miteinander *verknüpfen* kann, dass bestimmte Spielregeln eingehalten werden. Solche Mengen, zusammen mit der Verknüpfung und den entsprechenden Spielregeln bilden dann eine *algebraische Struktur*.
Eine Menge M zusammen mit einer Verknüpfung "$\cdot$", die zwei beliebigen Elementen a und b aus M jeweils ein eindeutiges Element $a \cdot b$ zuweist, heißt beispielweise *Halbgruppe*, wenn das *Assoziativgesetz* erfüllt ist, also für jede beliebige Wahl dreier Elemente $a, b, c \in M$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

gilt. Es ist also egal, ob ich zuerst a mit b verknüpfe, und dann das Ergebnis mit c, oder ob ich zuerst b mit c verknüpfe, und dann a mit dem Ergebnis *dieser Rechnung* vernküpfe! Wir schreiben $(M, \cdot)$, wenn wir die Menge M zusammen mit dieser Verknüpfung meinen. Je nach Verknüpfung kann man verschiedene Symbole verwenden, z.B. $\times$, $\otimes$, $\circ$, $\wedge$, $\heartsuit$, ...

Beispiel 1. *Die natürlichen Zahlen mit der Addition, geschrieben* $(\mathbb{N}, +)$*, bilden eine Halbgruppe. Aber auch die Menge aller Buchstabenfolgen, die wir aus den* 26 *Buchstaben a,b,c,...,z des Alphabets bilden können, kann auf natürliche Art und Weise zu einer Halbgruppe gemacht werden. Wie? Aber nicht alle Mengen mit Verknüpfung bilden eine Halbgruppe. Zeige, dass* $(\mathbb{Z}, -)$*, also die ganzen Zahlen mit der Subtraktion als Verknüpfung, keine Halbgruppe bilden.*

Wenn es in einer Halbgruppe M ein Element e gibt, welches $e \cdot a = a \cdot e$ für *alle* a aus M erfüllt, dann nennt man M ein *Monoid*, und e das *neutrale Element* oder *Einselement*.

Beispiel 2. *Angenommen, in einer Halbgruppe gibt es ein Element e_l, dass $e_l \cdot a = a$ für alle $a \in M$ erfüllt (aber wir wissen nicht, ob auch $b \cdot e_l = b$ für alle $b \in M$ gilt), und ein Element e_r, welches $a \cdot e_r = a$ für alle $a \in M$ erfüllt. Zeige, dass $e_l = e_r$ gilt, und M somit ein Monoid mit Einselement $e := e_l = e_r$ ist. Kann ein Monoid zwei Einselemente haben?*

Beispiel 3. *Finde eine Halbgruppe, die ein „linksneutrales Element" e_l mit $e_l \cdot a = a$ für alle a besitzt, aber trotzdem kein echtes neutrales Element hat. Kann eine Halbgruppe mehr als ein linksneutrales Element haben?*

Eine Gruppe ist ein Monoid M mit der zusätzlichen Eigenschaft, dass es zu jedem Element a ein Element b gibt, welches $a \cdot b = b \cdot a = e$ erfüllt. Dieses Element heißt das *inverse Element* zu a. Wir schreiben oft G als Bezeichnung für die einer Gruppe zugrundeliegende Menge. Wie vorher bei den Monoiden und den links- bzw. rechtsneutralen Elementen ist es nicht so wichtig, zwischen Links- und Rechtsinversen zu unterscheiden, weil diese ohnehin gleich sein müssen:

Beispiel 4. *Angenommen, in einem Monoid M mit neutralem Element e gibt es zu einem Element $a \in M$ ein Element b_l, sodass $b_l \cdot a = e$ (aber nicht notwendigerweise $a \cdot b_l = e$), und ein Element b_r, sodass $a \cdot b_r = e$. Zeige, dass $b_l = b_r$ gilt, also dass a ein* inverses Element *besitzt. Zeige außerdem, dass a maximal ein inverses Element haben kann.*

Weil das inverse Element eines Gruppenelements a eindeutig ist, können wir es mit a^{-1} bezeichne, und werden das im Folgenden auch tun.
Warum interessiert man sich aber für Gruppen? Der Hauptgrund dafür ist, dass sie uns ein Minimum an Werkzeugen in die Hand geben, um Gleichungen lösen zu können:

Beispiel 5. *Es seien a und b Elemente einer Gruppe G. Zeige, dass es* genau *ein Element $x \in G$ gibt, welches $a \cdot x = b$ erfüllt.*

Es folgen ein paar **Aufgaben** zum Lösen.

Beispiel 6. *Angenommen, in einer Gruppe G gilt für* alle *Gruppenelemente $a \in G$, dass $a \cdot a = e$ ist. Zeige, dass dann für alle Paare von Gruppenelementen $a, b \in G$ gilt, dass $a \cdot b = b \cdot a$.*

Beispiel 7. *Es sei G eine Gruppe mit endlich vielen Elementen (eine „endliche Gruppe"). Man zeige, dass es für jedes Gruppenelement a eine positive ganze Zahl n mit $n \leq |G|$ gibt, sodass*

$$a^n := \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ mal}} = e.$$

Man nennt die kleinstmögliche solche Zahl n die *Ordnung* des Elements a in G.

Beispiel 8. *Es sei G eine Gruppe mit einer endlichen, geraden Anzahl von Elementen. Man zeige, dass es außer e noch mindestens ein weiteres Element $a \in G$ gibt, das $a \cdot a = e$ erfüllt.*

Untergruppen

Eine Teilmenge $U \subseteq G$ einer Gruppe $(G, \cdot)$, die mit der Verknüpfung $\cdot$ selbst zu einer Gruppe wird, heißt eine *Untergruppe* von G. Genauer gesagt ist U dann eine Untergruppe, wenn einerseits für je zwei Elemente $a, b \in U$ auch $a \cdot b$ in U liegt, und andererseits für jedes Element $a \in U$ auch das inverse Element a^{-1} in U liegt.

Beispiel 9. *Zeige, dass die Bedingung „ a liegt in $U \longrightarrow a^{-1}$ liegt in U“ notwendig ist, damit U wieder eine Gruppe ist. Eine Menge U, sodass für alle $a, b \in G$ auch $a \cdot b$ in U liegt, muss nämlich nur eine* Halb*gruppe sein. (Wovon könnte der eigenartige Name dieser Struktur abgeleitet worden sein?)*

Gegeben eine Teilmenge $A \subseteq G$ (muss keine Untergruppe sein), schreiben wir kurzerhand $g \cdot A$ für die Teilmenge $\{g \cdot a : a \in A\}$. Überzeuge dich, dass $g \cdot A$ gleich viele Elemente wie A hat, wenn A eine endliche Menge ist.

Beispiel 10. *Gegeben sei eine Gruppe G und eine Untergruppe $U \subseteq G$. Wir betrachten die Mengen $g \cdot U$ für beliebige Elemente $g \in G$. Zeige, dass $g \cdot U$ und $h \cdot U$ für $g, h \in G$ entweder als Menge gleich sind, oder gar kein Element gemeinsam haben. Zeige außerdem, dass jedes Element der Gruppe in einer solchen Menge enthalten sein muss.*

Das bedeutet, dass die Mengen der Form $g \cdot U, g \in G$ die Gruppe G in lauter gleich große Teile aufteilen, die einander nicht überschneiden. Überzeuge dich davon, dass, wenn G eine endliche Gruppe ist, daraus folgt, dass die Zahl $|G|$ (die „Ordnung“der Gruppe) durch die Zahl $|U|$ teilbar ist. Diese erstaunliche Tatsache wird *Satz von Lagrange* genannt. Der Quotient $\frac{|G|}{|U|}$, der also eine ganze Zahl ist, wird auch der *Index* der Untergruppe U in G genannt. Wir können unsere Aussage über die Ordnung eines Elements $a \in G$ nun präzisieren:

Beispiel 11. *Es sei G eine endliche Gruppe. Zeige, dass für jedes Element a eine positive ganze Zahl n existiert, sodass $a^n = e$ gilt, und dass das kleinstmögliche solche n die Ordnung $|G|$ der Gruppe teilt.*

Eine Anwendung aus der Zahlentheorie ist der Satz von Euler-Fermat

Beispiel 12. *Es sei m eine positive ganze Zahl, und $\phi(m)$ die Anzahl der zu m teilerfremden Zahlen in der Menge $\{0, 1, \ldots, m-1\}$. Zeige, dass für jede zu m teilerfremde Zahl a*

$$a^{\phi(m)} = 1 \mod m$$

gilt.