17. Drei Anwendungen der Gruppentheorie

Das 14-15-Puzzle: Auf 4×4 Feldern liegen Steine mit den Nummern 1 bis 15. Das letzte Feld ist frei und wird benützt, um Steine zu verschieben:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

$(*)$

Die Aufgabe besteht normalerweise darin, die Steine durch verschieben gut zu mischen und dann den oben dargestellten Ausgangszustand $(*)$ wieder herzustellen. Ein klassisches Rätsel aus dem 19. Jahrhundert ist es, den Urzustand $(*)$ ausgehend von der folgenden Anordnung aus wieder herzustellen, bei dem nur die Steine mit den Nummern 14 und 15 vertauscht worden sind:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

$(**)$

Dieses Problem war damals sehr populär, ist aber unlösbar.

Jede Anordnung der 15 Steine und des leeren Felds kann als Element der Gruppe S_{16} aufgefasst werden bzw. jede Anordnung mit leerem Feld rechts unten als Element der Gruppe S_{15}. Jede Verschiebung eines Steins kann als Transposition (in S_{16}) aufgefasst werden. Eine Anordnung mit leerem Feld rechts unten, die man, ausgehend von $(*)$, auf (legale) Weise erreichen kann, muss eine gerade Permutation (d.h. Element von A_{15}) sein, da das leere Feld sich bei ihrer Herstellung genauso oft nach oben (bzw. rechts) wie nach unten (bzw. links) bewegt haben muss. D.h. die Permutation muss durch eine gerade Anzahl von Transpositionen entstanden sein.

Tatsächlich kann man zeigen, dass die von $(*)$ aus erreichbaren Anordnungen mit leerem Feld rechts unten genau den geraden Permutationen, d.h. der Gruppe A_{15}, entsprechen.

Das kann z.B. geschehen, indem man zeigt, dass alle Elemente eines geeigneten Erzeugendensystems von A_{15}, ausgehend von $(*)$, durch Verschieben hergestellt werden können.

Ähnlich haben auch Rubik's Cube und verwandte Spielzeuge die Struktur einer Gruppe.

Diffie – Hellman – Schlüsselaustausch: Alice und Bob wollen geheime Informationen über ein unsicheres Medium (z.B. eine Funk- oder Datenleitung, die abgehört werden kann) übertragen. Sie haben sich auf ein Verschlüsselungsverfahren geeinigt, stehen aber vor dem Problem, den dazugehörigen Schlüssel auszutauschen. Sie gehen folgendermaßen vor:

1. Sie wählen eine (möglichst komplizierte) zyklische Gruppe G und einen Erzeuger g (d.h. $G = \langle g \rangle$). Beides braucht nicht geheim gehalten zu werden und kann auch über ein unsicheres Medium übertragen werden.

2. Alice wählt eine (zufällige) Zahl $a \in \{2, 3, \dots, |G| - 1\}$, die sie geheimhält. Ebenso wählt Bob ein (geheimes) $b \in \{2, 3, \dots, |G| - 1\}$.

3. Alice berechnet $A := g^a \in G$ und Bob berechnet $B := g^b \in G$.

4. Alice teilt Bob A über das unsichere Medium mit und Bob informiert Alice über B.

5. Beide berechnen $K := g^{ab} \in G$. (Alice kann das, da $K = (g^b)^a = B^a$. Bob kann das, da $K = (g^a)^b = A^b$.)

6. Der Wert K kann für die Verschlüsselung ihrer weiteren Kommunikation verwendet werden.

Wer die Kommunikation von Alice und Bob belauscht, kennt zwar möglicherweise G, g, A und B – aber nicht a, b und K.

Eine mögliche Wahl für die zyklische Gruppe G ist die prime Restklassengruppe $(\mathbb{Z}_p^*, \cdot)$ für eine (große) Primzahl p. In diesem Fall ist g eine Primitivwurzel (d.h. $\langle g \rangle = \mathbb{Z}_p^*$) und $a, b \in \{2, 3, \dots, p-2\}$. Die Berechnung von A und B erfolgt mittels Kongruenzen, d.h. $A \equiv g^a \pmod{p}$ (wobei $0 \leq A < p$) und $B \equiv g^b \pmod{p}$ (wobei $0 \leq B < p$). Ebenso ist $K \equiv A^b \equiv B^a \pmod{p}$ mit $0 \leq K < p$.

Prüfziffern: Prüfsummen bzw. Prüfziffern werden verwendet, um die Korrektheit bestimmter Daten zu gewährleisten (z.B. von Kontonummern, Kreditkartennummern, Sozialversicherungsnummern, ISBN, Seriennummern von Geldscheinen). Eine einfache Möglichkeit dafür ist die Ziffern- bzw. Quersumme. Z.B. kann man der Zahl 2347 mit Ziffernsumme $2+3+4+7 = 16$ die Prüfziffer 4 hinzufügen. Die so entstandene Zahl hat eine Ziffernsumme die durch 10 teilbar ist, denn $2 + 3 + 4 + 7 + 4 = 20 \equiv 0 \pmod{10}$.

Abstrakt kann man das so formulieren: Bezeichnen $a_1, a_2, \dots, a_{n-1}, a_n \in \{0, 1, \dots, 9\}$ Ziffern, so fügt man der Zahlenfolge $a_1 a_2 \dots a_{n-1} a_n$ eine Ziffer a_{n+1} hinzu, derart dass $a_1 + a_2 + \cdots + a_{n-1} + a_n + a_{n+1} \equiv 0 \pmod{10}$, oder, wenn man zu Restklassen übergeht, derart dass die Gleichung

$$\overline{a_1} + \overline{a_2} + \cdots + \overline{a_{n-1}} + \overline{a_n} + \overline{a_{n+1}} = \overline{0}$$

in der Gruppe $\mathbb{Z}_{10}$ erfüllt ist.

Auf diese Weise kann man einzelne falsche Ziffern erkennen. Schreibt man im obigen Beispiel etwa versehentlich 5 statt 3 (also 25474 statt 23474), so ist die Ziffernsumme $2 + 5 + 4 + 7 + 4 = 22 \equiv 2 \pmod{10}$. Trotzdem ist diese Methode für die Praxis nicht gut geeignet, da z.B. das Vertauschen zweier benachbarter Ziffern nicht erkannt wird. (Vertauscht man z.B. in unserem Beispiel 2 und 3, so hat die entstandene Zahl 32474 die selbe Ziffernsumme wie die korrekte Zahl 23474.) Eine mögliche Lösung für dieses Problem ist es, die einzelnen Summanden in der Ziffernsumme mit verschiedenen Gewichten zu versehen. So besteht die aktuelle Version der Internationalen Standardbuchnummer ISBN aus 13 Ziffern, von denen die letzte die Prüfziffer ist. Bei der Bildung der Quersumme wird jede zweite Ziffer mit 3 multipliziert. Ist also $a_1 a_2 \dots a_{12} a_{13}$ ISBN eines Buchs (wieder mit Ziffern $a_1, a_2, \dots, a_{12}, a_{13} \in \{0, 1, \dots, 9\}$), so muss

$$a_1 + 3a_2 + a_3 + 3a_4 + \cdots + a_{11} + 3a_{12} + a_{13} \equiv 0 \pmod{10}$$

gelten. Dadurch ist es möglich, nicht nur einzelne falsche Ziffern zu erkennen, sondern auch viele Vertauschungen benachbarter Ziffern. Genauer wird eine derartige Vertauschung genau dann nicht erkannt, wenn sich die beiden vertauschten Ziffern um 5 unterscheiden, da für $a, b \in \{0, 1, \dots, 9\}$ gilt, dass

$$3a + b \equiv a + 3b \pmod{10} \Leftrightarrow 2a \equiv 2b \pmod{10} \Leftrightarrow a \equiv b \pmod{5} \Leftrightarrow |a - b| = 5.$$

Ein anderer Vorschlag für die Berechnung von Prüfziffern stammt von Jacobus Verhoeff. Er beruht auf der Tatsache, dass es außer $\mathbb{Z}_{10}$ (bis auf Isomorphie) ja noch eine zweite (nicht-abelsche) Gruppe mit 10 Elementen gibt, nämlich D_5. Dafür identifiziert man jede Ziffer $k \in \{0, 1, \dots, 9\}$ mit einem $\sigma_k \in D_5$. Analog zu oben kann man nun zu einer gegebenen Zahlenfolge $a_1, a_2, \dots, a_{n-1}, a_n \in \{0, 1, \dots, 9\}$ eine Ziffer a_{n+1} hinzufügen, derart dass

$$\sigma_{a_1} \circ \sigma_{a_2} \circ \cdots \circ \sigma_{a_n} \circ \sigma_{a_{n+1}} = \varepsilon.$$

Ähnlich wie bei den gewichteten Ziffernsummen ist es auch hier sinnvoll, die σ_{a_i} vor dem Verknüpfen geeignet zu modifizieren, um möglichst viele Arten von Fehlern zu erkennen. Diese Art von Prüfziffern wurde bei den Seriennummern von D-Mark Scheinen verwendet.