D-MATH Algebra I HS 2015
Prof. Richard Pink

Musterlösung: Wiederholungsserie

1. Betrachte die reellen Zahlen $\alpha := \sqrt{2}$ und $\beta := \sqrt{3}$ und setze $\gamma := \alpha + \beta$. Gilt $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$ als Unterringe von $\mathbb{R}$? Gilt $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\gamma]$?

   Lösung: Since $\gamma = \alpha + \beta$, it follows that $\gamma \in \mathbb{Q}[\alpha, \beta]$; hence the inclusion $\mathbb{Q}[\gamma] \subset \mathbb{Q}[\alpha, \beta]$. Direct computation yields $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}$, from which we deduce that $\alpha = (\gamma^3 - 9\gamma)/2$; hence $\alpha \in \mathbb{Q}[\gamma]$. This implies that $\beta = \gamma - \alpha \in \mathbb{Q}[\gamma]$, giving us the reverse inclusion. We conclude that $\mathbb{Q}[\gamma] = \mathbb{Q}[\alpha, \beta]$.

   The inclusion $\mathbb{Z}[\gamma] \subset \mathbb{Z}[\alpha, \beta]$ follows as above. From the equality $\gamma^4 = 10\gamma^2 - 1$, we deduce that every element of $\mathbb{Z}[\gamma]$ can be written in the form $a + b\gamma + c\gamma^2 + d\gamma^3$ for some $a, b, c, d \in \mathbb{Z}$. Using $\gamma^2 = 5 + 2\sqrt{6}$ and the equation for γ^3 above, it follows that every element of $\mathbb{Z}[\gamma]$ can be written as $(a + 5c) + (b + 11d)\sqrt{2} + (b + 9d)\sqrt{3} + 2c\sqrt{6}$. Suppose $\alpha \in \mathbb{Z}[\gamma]$. Writing $\alpha = \sqrt{2}$ in this form and subtracting α from both sides yields $0 = (a + 5c) + (b - 1 + 11d)\sqrt{2} + (b + 9d)\sqrt{3} + 2c\sqrt{6}$. Now $\sqrt{2}$ and $\sqrt{3}$ and $\sqrt{6}$, as well as their pairwise ratios, are irrational. Thus an integral combination of them is zero if and only if each coefficient is zero. But then $b + 11d = 1$ and $b + 9d = 0$, which yields $2d = 1$, contradicting the fact that d is an integer. Thus $\alpha \notin \mathbb{Z}[\gamma]$, and we have $\mathbb{Z}[\gamma] \subsetneq \mathbb{Z}[\alpha, \beta]$.

2. Gibt es einen Integritätsbereich mit 15 Elementen?

   Lösung: Let R be a ring with 15 elements. Then $(R, +)$ is an abelian group of order 15. It follows from the classification theorem for finitely generated abelian groups that $(R, +) \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$. Therefore we may thus choose elements $a, b \in R$ of respective orders 3 and 5. Then $a, b \neq 0$, and $3ab = (3a)b = 0b = 0$ and $5ab = (5b)a = 0a = 0$; hence $ab = 2 \cdot 3ab - 5ab = 0$. Thus R is not an integral domain. Thus the answer is no.

3. Sei K ein Körper. Zeige, dass es unendliche viele irreduzible normierte Polynome in $K[X]$ gibt.

   Lösung: The proof we provide is directly analogous to Euclid's proof that there are infinitely many prime numbers. We know that there exists a monic irreducible polynomial in $K[X]$ (for example $X - 1$). Let $p_1, \ldots, p_n$ be monic irreducible polynomials in $K[X]$. Consider the polynomial

   $$P := p_1 p_2 \cdots p_n + 1.$$

   Then P is monic of degree > 0 and therefore possesses a monic irreducible factor p. We claim that p is distinct from each of the p_i. If $p = p_i$ for some $1 \leqslant i \leqslant n$, then it follows that $p | P$ and $p | P - 1 = \prod_i p_i$, from which it follows that $p | 1$. Thus p is

a unit, a contradiction. Hence for any finite set of monic irreducible elements in $K[X]$, we can find a monic irreducible not contained in that set. It follows that that set of monic irreducible polynomials in $K[X]$ is infinite.

4. Beschreibe den Ring $(\mathbb{Z}/12\mathbb{Z})[X]/(2X-1)$.

   Lösung: Let $R := (\mathbb{Z}/12\mathbb{Z})[X]/(2X-1)$. Then R is isomorphic to the ring $\mathbb{Z}[X]/I$, where I is the ideal generated by 12 and $2X-1$. We show that $I = (3, X-2)$. The inclusion '$\subset$" is immediate since

   $$2X - 1 = 2(X-2) + 3$$

   and 12 is a multiple of 3. We deduce the reverse inclusion from

   $$2X - 1 = 0 \Longrightarrow 12X - 6 = 0 \text{ and together with } 12 = 0 \Longrightarrow 6 = 0 \text{ in } R.$$

   Going through the same procedure again with $6X - 3 = 0$ yields $3 = 0$ in R, which implies that $3 \in I$. Finally, we can write

   $$X - 2 = 4X - 3X - 2 = 2(2X - 1).$$

   Hence, R is isomorphic to $(\mathbb{Z}/3\mathbb{Z})[X]/(X-2) \cong \mathbb{Z}/3\mathbb{Z}$.

5. Bestimme welche der folgenden Polynome irreduzibel sind.

   (a) $X^3 + 9X + 6X - 3 \in \mathbb{Z}[X]$.

   (b) $4X^3 - 15X^2 + 60^X + 180 \in \mathbb{Q}[X]$.

   (c) $X^3 + 3X^2 + 5X + 5 \in \mathbb{Q}[X]$

   (d) $X^7 + 7X^6 + 5X^2 - X + 1 \in \mathbb{R}[X]$.

   Lösung:

   (a) Irreducible. Eisenstein for $p = 3$.

   (b) Irreducible. Eisenstein for $p = 5$.

   (c) Irreducible. Reduction modulo 3 has no roots in $\mathbb{F}_3$.

   (d) Let $f(X) := X^7 + 7X^6 + 5X^2 - X + 1$. The roots of f in $\mathbb{C}$ are either real or occur in complex conjugate pairs. Since the degree of f is odd, there must be a real root. It follows that f factors in $\mathbb{R}[X]$ and is thus reducible.

6. Für welche Ringe R ist der Polynomring $R[X]$ ein Hauptidealring?

   Lösung: We already know that $R[X]$ is a principal ideal domain if R is a field. We claim that this is the only case. So assume that $R[X]$ is a principal ideal domain. Then $R[X]$ is in particular an integral domain; hence so is the subring R. From the natural isomorphism $R \to R[X]/(X)$ it follows that $R[X]/(X)$ is an integral domain, too. Thus the ideal (X) is a non-zero prime ideal. But in a principal ideal domain, every non-zero prime ideal is maximal. Thus (X) is a maximal ideal; hence $R[X]/(X) \cong R$ is a field.

*7. Sei $\mathcal{O}(\mathbb{C})$ der Ring der analytischen Funktionen auf $\mathbb{C}$. Sei $\mathcal{O}_0$ der Ring der Keime analytischer Funktionen an der Stelle $0 \in \mathbb{C}$, definiert wie folgt: Betrachte die Menge

$$F := \left\{ (f, U) \;\middle|\; \begin{array}{l} U \text{ ist eine offene Umgebung von } 0 \text{ und} \\ f\colon U \to \mathbb{C} \text{ ist eine analytische Funktion} \end{array} \right\}$$

mit den beiden Operationen

$$\begin{aligned} (f, U) + (g, V) &:= (f|_{U\cap V} + g|_{U\cap V}, U \cap V), \\ (f, U) \cdot (g, V) &:= (f|_{U\cap V} \cdot g|_{U\cap V}, U \cap V). \end{aligned}$$

Diese sind verträglich mit der Äquivalenzrelation

$$(f, U) \sim (g, V) \;:\Longleftrightarrow\; \exists \text{ offene Umgebung } W \subset U \cap V \text{ von } 0 \text{ mit } f|_W = g|_W$$

auf F und induzieren auf der Menge der Äquivalenzklassen $\mathcal{O}_0 := F/\!\sim$ eine Ringstruktur.

(a) Zeige, dass $\mathcal{O}_0$ und $\mathcal{O}(\mathbb{C})$ Integritätsbereiche sind. Welcher der beiden ist auf natürliche Weise ein Unterring des anderen?

(b) Zeige, dass $\mathcal{O}_0$ ein Hauptidealring ist, der genau ein maximales Ideal besitzt.

(c) Beweise, dass die irreduziblen Elemente in $\mathcal{O}(\mathbb{C})$ genau die Primelemente sind, und bestimme diese. Zeige, dass nicht jedes Element ein Produkt vom Primelementen ist, und schliesse daraus, dass der Ring $\mathcal{O}(\mathbb{C})$ weder faktoriell noch noethersch (siehe §2.4) ist.

(d) Beschreibe die Quotientenkörper von $\mathcal{O}_0$ und $\mathcal{O}(\mathbb{C})$ mit Hilfe von (Keimen von) meromorphen Funktionen. (*Hinweis*: Weierstrass-Produkt-Satz.)

Lösung: Die Abbildung $\mathcal{O}(\mathbb{C}) \to \mathcal{O}_0, f \mapsto [(f, \mathbb{C})]$ definiert einen Ringhomomorphismus, der nach dem Identitätssatz injektiv ist, denn besitzen zwei analytische Funktionen dieselben Keime bei 0, dann stimmen sie per Definition auf einer offenen Umgebung von 0 überein, sind also überhaupt gleich. Wir können daher $\mathcal{O}(\mathbb{C})$ als Unterring von $\mathcal{O}_0$ auffassen. Wir analysieren zuerst die Teilbarkeitsrelation in den Ringen $\mathcal{O}(\mathbb{C})$ und $\mathcal{O}_0$. Zunächst zu $\mathcal{O}(\mathbb{C})$. Wir beginnen mit folgenden Feststellungen:

- Sei $N(f)$ die Menge der Nulstellen einer Funktion $f \in \mathcal{O}(\mathbb{C})$, dann gilt $N(fg) = N(f) \cup N(g)$. Aus dem Identitätssatz folgt ausserdem, dass $N(f)$ diskret in $\mathbb{C}$ ist für $f \neq 0$.
- Für eine analytische Funktion $f : \mathbb{C} \to \mathbb{C}$ und einen Punkt $z \in \mathbb{C}$ sei $\mathrm{ord}_z(f)$ die Nullstellenordnung von f bei z, also das Supremum aller nichtnegativer ganzer Zahlen n, sodass eine analytische Funktion g existiert mit $f(w) = (w - z)^n g(w)$. Gilt dabei $\mathrm{ord}_z(f) = \infty$ für einen Punkt z, dann verschwindet

f nach dem Identitätssatz identisch. Sei $\mathrm{ord}(f) : \mathbb{C} \to \mathbb{Z}_{\geqslant 0} \cup \infty$ die Funktion $z \mapsto \mathrm{ord}_z(f)$, dann ist $\mathrm{ord}(f) \geqslant 0$ und der Träger von $\mathrm{ord}(f)$ ist genau die Menge $N(f)$. Zudem gilt

$$\mathrm{ord}(fg) = \mathrm{ord}(f) + \mathrm{ord}(g) \tag{1}$$

(als Gleichung von Funktionen). Wir behaupten

$$f|g \Leftrightarrow \mathrm{ord}(f) \leqslant \mathrm{ord}(g), \tag{2}$$

insbesondere sind die Einheiten in $\mathcal{O}(\mathbb{C})$ genau die nullstellenfreien Funktionen. Zur Begründung der Implikation „$\Leftarrow$“ können wir $f \neq 0$ annehmen. Definiere die Funktion $h(z) = \frac{g(z)}{f(z)}$ ausserhalb der diskreten Menge $N(f)$. Die Punkte in $N(f)$ sind wegen $\mathrm{ord}(g) \geqslant \mathrm{ord}(h)$ hebbare Singularitäten, wir können h also zu einer analytischen Funktion fortsetzen und es gilt $g = hf$ in $\mathcal{O}(\mathbb{C})$.

Nun zu $\mathcal{O}_0$. Hier ist die Situation wesentlich einfacher. Im folgenden notieren wir Funktionskeime etwas ungenau als $[f]$, wobei f ein Repräsentant dieses Keims ist, der auf einer gewissen Nullumgebung definiert ist. Da Funktionskeime nur das Verhalten einer Funktion in einer „infinitesimalen Umgebung“ von 0 dokumentieren, lässt sich die Funktion ord von oben ersetzen durch die Ordnung ord_0 am einzigen Punkt 0. Wir zeigen zuerst, dass die Ordnung eine wohldefinierte Abbildung $\mathrm{ord}_0 : \mathcal{O}_0 \to \mathbb{Z}_{\geqslant 0} \cup \infty$ induziert. Repräsentieren nämlich zwei Paare (f, U) und (g, V) denselben Keim, dann stimmen f und g in einer Umgebung des Nullpunkts überein, haben dort also dieselbe Nullstellenordnung. Wieder ist $\mathrm{ord}_0([f]) = 1$ nur für den Keim der Nullfunktion. Analog zu oben gilt

$$\mathrm{ord}_0([fg]) = \mathrm{ord}_0([f]) + \mathrm{ord}_0([g])$$

und

$$[f]|[g] \Leftrightarrow \mathrm{ord}_0([f]) \leqslant \mathrm{ord}_0([g]),$$

insbesondere sind die Einheiten in $\mathcal{O}_0$ genau die Keime von Funktionen, die in 0 keine Nullstelle haben.

(a) Seien $f, g \in \mathcal{O}(\mathbb{C}) \setminus \{0\}$, dann ist $N(fg) = N(f) \cup N(g)$ diskret, also gilt $fg \neq 0$. Somit ist $\mathcal{O}(\mathbb{C})$ nullteilerfrei. Dasselbe Argument angewandt auf Repräsentanten von Funktionskeimen zeigt, dass auch $\mathcal{O}_0$ nullteilerfrei ist.

(b) Die Ideale in $\mathcal{O}_0$ der Grösse nach geordnet genau die folgenden sind:

$$([1]), ([z]), ([z^2]), ([z3]), \ldots ([0]).$$

Das einzige maximale Ideal ist $([z])$.

(c) Wir zeigen zuerst, dass die irreduziblen Elemente in $\mathcal{O}(\mathbb{C})$ genau die Funktionen f mit einer einzigen einfachen Nullstelle sind (d.h. $\sum_{z \in \mathbb{C}} \mathrm{ord}_z(f) = 1$) Diese sind

offensichtlich irreduzibel, denn für jede Produktdarstellung $f = gh$ folgt aus (1), dass g oder h keine Nullstelle besitzt, also eine Einheit ist. Besitzt f umgekehrt keine Nullstelle, dann ist f eine Einheit. Gilt $\sum_{z\in\mathbb{C}} \operatorname{ord}_z(f) \geqslant 2$, dann wähle ein $z_0 \in N(f)$ und setze $g(z) = z - z_0$ Nach (2) gilt dann $g|f$, also existiert ein h mit $f = gh$. Nach Definition von g und (1) sind nun g und h keine Einheiten und f somit nicht irreduzibel. Als nächstes zeigen wir, dass jedes irreduzible Element prim ist (die Umkehrung davon gilt immer). Sei also f irreduzibel mit der einzigen Nullstelle z_0 und es gelte $f|gh$. Nach (1) ist z_0 auch eine Nullstelle von g oder h, also teilt f diesen Faktor nach (2). Nach der obigen Diskussion besitzt jedes endliche Produkt von Primelementen nur endlich viele Nullstellen. Die Funktion $\sin \in \mathcal{O}(\mathbb{C})$ zum Beispiel ist also kein Produkt von Primelementen. Damit ist $\mathcal{O}(\mathbb{C})$ weder faktoriell noch noethersch.

(d) Wir behaupten, dass der Körper $\mathcal{M}(\mathbb{C})$ der meromorphen Funktionen auf $\mathbb{C}$ der Quotientenkörper von $\mathcal{O}(\mathbb{C})$ ist. Da $\mathcal{O}(\mathbb{C})$ offensichtlich ein Unterring von $\mathcal{M}(\mathbb{C})$ ist, genügt es zu zeigen, dass jede meromorphe Funktion ein Quotient zweier analytischer Funktionen ist. Dazu werden wir einen nichttrivialen Satz aus der Funktionentheorie verwenden, den *Weierstrass'schen Produktsatz* (Siehe Bermerkungen unten). Sei also $f \neq 0$ eine meromorphe Funktion. Setze

$$D = \{z \in \mathbb{C} \mid \operatorname{ord}_z(f) < 0\}, \quad n : D \to \mathbb{Z}_{\geqslant 0}, z \mapsto \operatorname{ord}_z(f),$$

dann ist D diskret. Nach dem Produktsatz existiert eine analytische Funktion $h \in \mathcal{O}(\mathbb{C})$ mit $N(h) = D$ und $\operatorname{ord}_z(h) = n(z)$ für alle $z \in D$. Die Funktion $g = fh$ ist meromorph und besitzt nur hebbare Singularitäten wegen $\operatorname{ord}(g) = \operatorname{ord}(f) + \operatorname{ord}(h) \geqslant 0$. Sie kann also zu einer analytischen Funktion $g \in \mathcal{O}(\mathbb{C})$ fortgesetzt werden und es gilt dann tatsächlich $f = \frac{g}{h}$ in $\mathcal{M}(\mathbb{C})$. Für $\mathcal{O}_0$ ist die Sache wieder deutlich einfacher. Der Quotientenkörper von $\mathcal{O}_0$ ist der Körper $\mathcal{M}_0$ der Keime meromorpher Funktionen in 0. Das obige Argument funktionert hier genauso, bloss kann man hier für h einfach die Funktion $z^{-\operatorname{ord}_0([f])}$ wählen und hat dann $[f] = \frac{[g]}{[h]}$ in $\mathcal{M}_0$. Man benötigt den Produktsatz also nicht.

Bemerkung: Der Weierstrass'sche Produktsatz lautet:

Sei $D \subset \mathbb{C}$ eine diskrete Teilmenge und $n : D \to \mathbb{Z}_{\geqslant 0}$ eine Funktion. Dann existiert eine analytische Funktion $f : \mathbb{C} \to \mathbb{C}$, welche genau in den Punkten von D Nullstellen besitzt, und so dass $\operatorname{ord}_z(f) = n(z)$ gilt für $z \in D$.

Namensgebend für den Satz ist dabei die Konstruktion von f als Produkt der Form

$$f(z) = \prod_{a\in D} \Big(1 - \frac{z}{a}\Big)^{n(a)} e^{P_a(z)},$$

wobei die Zusatzterme $e^{P_a(z)}$ bei geeigneter Wahl die Konvergenz des Produkts gewährleisten (ohne diese divergiert es in der Regel). Für einen Beweis siehe Freitag, Busam: Funktionentheorie 1, Kap. IV.2.

8. Sei K ein Körper. Berechne die Elementarteiler des $K[X]$-Moduls

$$M := K[X]/((X+1)^2) \oplus K[X]/\big((X-1)(X^2+1)\big) \oplus K[X]/\big((X+1)(X^2-1)\big).$$

Lösung: If K has characteristic 2, then $X^2+1 = X^2-1 = (X+1)^2$. This yields

$$M = K[X]/\big((X+1)^2\big) \oplus K[X]/\big((X+1)^3\big) \oplus K[X]/\big((X+1)^3\big).$$

Since $(X+1)^2 | (X+1)^3 | (X+1)^3$, it follows that the elementary divisors are $e_1 = (X+1)^2$ and $e_2 = e_3 = (X+1)^3$.

Suppose now that $\mathrm{char}(K) \neq 2$. Then $X^2-1 = (X+1)(X-1)$, and the polynomials $X+1$ and $X-1$ and X^2+1 are pairwise relatively prime. The Chinese remainder theorem therefore allows us to separate terms corresponding to their powers. This yields:

$$\begin{aligned} M \cong \;& K[X]/((X+1)^2) \oplus K[X]/\big(X-1\big) \oplus K[X]/\big((X^2+1)\big) \\ & \oplus K[X]/\big((X+1)^2\big) \oplus K[X]/\big(X-1\big). \end{aligned}$$

Again using the Chinese remainder theorem to regroup terms, we obtain:

$$M \cong K[X]/\big((X-1)(X+1)^2\big) \oplus K[X]/\big((X-1)(X+1)^2(X^2+1)\big).$$

We thus obtain for the elementary divisors $e_1 = (X-1)(X+1)^2$ and $e_2 = (X-1)(X+1)^2(X^2+1)$.

9. Bestimme für jede Primzahl p die Ordnung der Automorphismengruppe der Gruppe $(\mathbb{Z}/p^2\mathbb{Z}) \boxplus (\mathbb{Z}/p\mathbb{Z})$.

Lösung: Die Gruppe $G := (\mathbb{Z}/p^2\mathbb{Z}) \boxplus (\mathbb{Z}/p\mathbb{Z})$ ist von den beiden Elementen $(1,0)$ und $(0,1)$ erzeugt. Jeder Automorphismus φ von G ist daher durch die Bilder $(a,b) := \varphi((1,0))$ und $(a',b') := \varphi((0,1))$ bestimmt. Dabei muss jedenfalls (a,b) wie $(1,0)$ ein Element der Ordnung p^2 sein, was äquivalent zu $p \nmid a$ ist. Ausserdem muss (a',b') wie $(0,1)$ ein Element der Ordnung p sein, was äquivalent zu $p|a'$ und $(a',b') \neq (0,0)$ ist. Weiter ist das Element $(0,1)$ nicht in der Untergruppe $\langle (1,0) \rangle$ enthalten, also auch (a',b') nicht in der Untergruppe $\langle (a,b) \rangle = \{(ca, cb) \mid c \in \mathbb{Z}\}$. Wegen $p \nmid a$ und $p|a'$ schliesst dies genau die Elemente $(pda, pdb) = (pda, 0)$ aus für alle $d \in \mathbb{Z}$. Wegen $p \nmid a$ sind dies aber auch genau die Elemente $(pe, 0)$ für alle $e \in \mathbb{Z}$. Insgesamt liefert das die Bedingungen $p \nmid a$ und $p|a'$ und $b' \neq 0$.

Betrachte umgekehrt beliebige (a,b) und $(a',b') \in G$ mit $p \nmid a$ und $p|a'$ und $b' \neq 0$. Dann existiert ein eindeutiger Homomorphismus $\varphi\colon G \to G$ mit $\varphi((1,0)) = (a,b)$ und $\varphi((0,1)) = (a',b')$, nämlich

$$\varphi\colon G \to G,\ (c,d) \mapsto (ca + da', cb + db').$$

Dieser bildet die zyklische Untergruppe $\langle (1,0) \rangle$ der Ordnung p^2 isomorph auf die Untergruppe $\langle (a,b) \rangle$ ab, und die zyklische Untergruppe $\langle (0,1) \rangle$ der Ordnung p

isomorph auf die Untergruppe $\langle (a', b') \rangle$, welche nicht in $\langle (a, b) \rangle$ enthalten ist. Diese beiden Bilder erzeugen daher gemeinsam eine Untergruppe der Ordnung $> p^2$ und folglich (Lagrange) die ganze Gruppe G. Somit ist der Homomorphismus surjektiv, und daher bijektiv, also ein Isomorphismus.

Die Anzahl der Automorphismen von G ist also die Anzahl der Möglichkeiten für (a, b) und $(a', b') \in G$ mit $p \nmid a$ und $p|a'$ und $b' \neq 0$, das heisst gleich

$$\big(|\mathbb{Z}/p^2\mathbb{Z}| - |p\mathbb{Z}/p^2\mathbb{Z}|\big) \cdot |\mathbb{Z}/p\mathbb{Z}| \cdot |p\mathbb{Z}/p^2\mathbb{Z}| \cdot \big(|\mathbb{Z}/p\mathbb{Z}| - 1\big) = (p^2 - p) \cdot p \cdot p \cdot (p-1) = p^3(p-1)^2.$$

10. Eine Gruppe G mit der Eigenschaft $[G, G] = G$ heisst *perfekt*. Zeige für alle $N \triangleleft G$:

    (a) Ist G perfekt, so auch G/N.

    (b) Sind N und G/N perfekt, so auch G.

    (c) Jede endliche Gruppe ist in einer perfekten Gruppe enthalten.

    Lösung: (a) Die Kommutatoren von Elementen in G/N sind genau die Bilder der Kommutatoren von Elementen in G. Ist G perfekt, so erzeugen die letzteren die Gruppe G, also die ersteren die Gruppe G/N; daher ist G/N perfekt.

    (b) Nach Konstruktion gilt $[N, N] < [G, G]$; da N perfekt ist, also $N < [G, G]$. Aus demselben Grund wie in (a) ist nun $[G, G]/N = [G/N, G/N]$. Da G/N perfekt ist, ist dieses gleich G/N. Somit ist $[G, G] = G$, also G perfekt.

    (c) Nach Cayley liefert die Operation von G auf sich durch Linkstranslation eine Einbettung von G in die symmetrische Gruppe $S(G) \cong S_{|G|}$. Nach Serie 11, Aufgabe 3 existiert eine weitere Einbettung $S_{|G|} \hookrightarrow A_{|G|+2}$. Lassen wir die $A_{|G|+2}$ auf den Ziffern $|G| + 3$ bis $|G| + 5$ trivial operieren, so liefert dies eine dritte Einbettung $A_{|G|+2} \hookrightarrow A_{|G|+5}$. Wegen $|G| + 5 \geqslant 5$ ist nun $A_{|G|+5}$ nichtabelsch einfach und somit perfekt. Die Komposition der genannten Einbettungen liefert dann eine Einbettung $G \hookrightarrow A_{|G|+5}$ mit der gesuchten Eigenschaft.

11. Zeige: Jede nilpotente endliche Gruppe der Ordnung n besitzt für jeden Primteiler $p|n$ genau eine p-Sylowgruppe G_p und ist das innere direkte Produkt $\bigtimes_{p|n} G_p$.

    Lösung: We use the following lemma

    Lemma. *Let G be a finite nilpotent group and $H < G$ a proper subgroup. Then H is properly contained in $N_G(H)$.*

    Beweis. By assumption G has an increasing central series $\{1\} = Z_0 \triangleleft Z_1 \triangleleft \ldots \triangleleft Z_n = G$. Let k be the largest integer such that $Z_k \subset H$. Choose $a \in Z_{k+1}$ such that $a \notin H$. Now

    $$H/Z_k \subset G/Z_k \text{ and } Z_{k+1}/Z_k = Z(G/Z_k).$$

    It follows that for every $h \in H$ we have

    $$ahZ_k = (aZ_k)(hZ_k) = (hZ_K)(aZ_k) = haZ_k.$$

Therefore $ha = ahh'$ for some $h' \in Z_k \subset H$. Thus $a^{-1}ha = hh' \in H$. It follows that $a^{-1}Ha = H$, so $a \in N_G(H)$. □

Now let G_p be a p-Sylow subgroup of G. If $N_G(G_p)$ is properly contained in G, then by the lemma, it is properly contained in $N_G(N_G(G_p))$. But Serie 13, Aufgabe 3 implies that $N_G(N_G(G_p)) = N_G(G_p)$, a contradiction. It follows that $N_G(G_p) = G$, so G_p is normal. Any two p-Sylow subgroups are conjugate, so this implies that G_p is the unique p-Sylow subgroup of G. For each pair of distinct primes p and q dividing n, the order of $G_q \cap G_p$ divides $|G_p|$ and $|G_q|$, and so must equal 1. Thus $G_p \cap G_q$ is trivial. We have as well that $|\prod_{p|n} G_p| = \prod_{p|n} |G_p| = n$. All together, it follows that $G = \bigtimes_{p|n} G_p$.

*12. Sei $n \geqslant 3$ ungerade. Finde alle Isomorphieklassen von Gruppen G mit den Eigenschaften

(a) $|G| = 2n$ und

(b) G enthält eine zyklische Untergruppe H der Ordnung n.

Hinweis: Zeige, dass G ein semidirektes Produkt von H mit einer Untergruppe C der Ordnung 2 ist. Beschreibe die möglichen Homomorphismen $C \to \mathrm{Aut}(H)$ und zeige, dass die entsprechenden semidirekten Produkte nicht isomorph sind.

Lösung: Setze $X := \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \mid x^2 = 1\}$. Dann sind die Homomorphismen $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ genau die Abbildungen der Form $a \mapsto x^a$ für alle $x \in X$. Zu jedem solchen x assoziieren wir das semidirekte Produkt

$$G_x := \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

mit der entsprechenden Operation. Dies ist eine Gruppe mit den gewünschten Eigenschaften. Wir behaupten, dass jede Gruppe mit den genannten Eigenschaften isomorph zu G_x ist für ein eindeutiges $x \in X$.

Sei also G eine Gruppe mit den genannten Eigenschaften. Da $|G| = 2n$ ist mit n ungerade, hat G nach dem ersten Sylow-Satz eine Untergruppe C mit $|C| = 2$. Da die Ordnungen von H und C teilerfremd sind, gilt $H \cap C = \{1_G\}$. Die Gruppe H hat Index 2 in G, also ist sie ein Normalteiler von G, und somit ist $HC \subset G$ eine Untergruppe. Deren Ordnung ist durch 2 und durch n teilbar, also ist sie gleich $2n$ und es gilt $HC = G$. Daraus folgt, dass G ein inneres semidirektes Produkt von H mit C ist. Somit ist $G \cong H \rtimes C \cong G_x$ für ein $x \in X$.

Es bleibt zu zeigen, dass $G_x \ncong G_{x'}$ ist für alle $x \neq x'$. Dafür beweisen und verwenden wir den folgenden Satz:

Satz: Ist G eine endliche Gruppe der Ordnung nk mit $\mathrm{ggT}(n, k) = 1$, und ist $N \lhd G$ ein Normalteiler der Ordnung n, so hat G ausser N keine Untergruppe der Ordnung n.

Beweis: Sei $H < G$ eine beliebige Untergruppe der Ordnung n. Nach dem zweiten Isomorphiesatz ist dann HN eine Untergruppe von G mit $HN/N \cong H/(H \cap N)$. Nach Lagrange ist $|H/(H \cap N)|$ ein Teiler von $|H| = n$. Also ist auch $|HN/N|$ ein Teiler von n. Dies ist aber auch ein Teiler von $|G/N| = k$. Die Voraussetzung $\mathrm{ggT}(n, k) = 1$ impliziert also $|HN/N| = 1$. Somit ist $HN = N$ und $H \subset N$, und aus Kardinalitätsgründen deshalb $H = N$. □

Betrachte nun $x, x' \in X$ und einen Isomorphismus $f\colon G_x \xrightarrow{\sim} G_{x'}$. Das Bild der Untergruppe $\mathbb{Z}/n\mathbb{Z} < G_x$ unter f ist dann eine Untergruppe von $G_{x'}$ der Ordnung n, also nach obigem Satz gleich $\mathbb{Z}/n\mathbb{Z} < G_{x'}$. Somit induziert f einen Isomorphismus $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$. Dieser ist gegeben durch $a \mapsto ka$ für ein $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Sei andererseits h das nichttriviale Element von $\mathbb{Z}/2\mathbb{Z}$ als Element von G_x oder $G_{x'}$. Wegen $f(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ gilt dann $f(h) = hu$ für ein $u \in \mathbb{Z}/n\mathbb{Z}$. Für jedes $a \in C_n$ gilt dann ${}^u(ka) = ka$ und somit

$$kxa \overset{\text{in } G_x}{\overset{\downarrow}{=}} f(xa) = f({}^h a) = {}^{f(h)}f(a) = {}^{hu}(ka) = {}^h(ka) \overset{\text{in } G_{x'}}{\overset{\downarrow}{=}} x'ka.$$

Wegen $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, und da $a \in \mathbb{Z}/n\mathbb{Z}$ beliebig ist, folgt daraus $x = x'$. Also ist $G_x \cong G_{x'}$ genau dann, wenn $x = x'$ ist, wie gewünscht.

13. Sei G eine endliche Gruppe, und sei H eine echte Untergruppe, deren Index $p := [G : H]$ gleich dem kleinsten Primteiler von $|G|$ ist. Zeige, dass H ein Normalteiler ist.

Hinweis: Untersuche Kern und Bild des Homomorphismus $G \to S_p$, welcher der Operation von G auf der Menge der Linksnebenklassen G/H entspricht.

Lösung: Die Gruppe G operiert auf G/H vermöge $g(xH) := gxH$. Durch Nummerieren der Nebenklassen entspricht diese Operation einem Homomorphismus $\varphi\colon G \to S_p$. Setze $K := \mathrm{Kern}(\varphi)$.

Der Stabilisator der Nebenklasse H bezüglich dieser Operation von G auf G/H ist gleich H, denn es gilt $gH = H \Leftrightarrow g \in H$. Daher ist K in H enthalten und es gilt

$$[G : K] = [G : H] \cdot [H : K] \geqslant p. \tag{3}$$

Nach dem Homomorphiesatz ist K ein Normalteiler von G und φ induziert einen injektiven Homomorphimus $G/K \hookrightarrow S_p$. Darum kann G/K mit einer Untergruppe von S_p identifiziert werden und nach dem Satz von Lagrange ist $[G : K] = |G/K|$ ein Teiler von $p! = |S_p|$. Da $p! = p \cdot (p-1)!$ gilt, wobei $(p-1)!$ nur Primfaktoren $< p$ hat, kann darum p höchstens mit Exponent 1 in der Primfaktorzerlegung von $[G : K]$ auftreten und Primfaktoren $> p$ können darin gar nicht vorkommen. Der Index $[G : K]$ ist aber auch ein Teiler von $|G|$ und hat daher nur Primteiler $\geqslant p$. Deshalb gibt es für $[G : K]$ nur die Möglichkeiten p und 1. Letztere ist aber wegen (3) ausgeschlossen. Es ist also $[G : K] = p = [G : H]$ und $H = K$ ist normal.

14. Sei $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ die *komplexe obere Halbebene* und betrachte die Abbildungsvorschrift

$$\mathrm{SL}_2(\mathbb{R}) \times \mathbb{H} \to \mathbb{H},\ (\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z) \mapsto \tfrac{az+b}{cz+d}.$$

(a) Zeige, dass dies eine wohldefinierte Linksoperation ist.

(b) Bestimme den Kern des zugehörigen Homomorphismus $\mathrm{SL}_2(\mathbb{R}) \to S(\mathbb{H})$.

(c) Zeige, dass diese Operation transitiv ist.

(d) Berechne den Stabilisator von $i \in \mathbb{H}$.

Lösung: (a) For any matrix $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ we have $(c,d) \in \mathbb{R}^2 \smallsetminus \{(0,0)\}$. For any $z \in \mathbb{H}$ we therefore have $cz + d \neq 0$. Also

$$\begin{aligned} \mathrm{Im}\left(\tfrac{az+b}{cz+d}\right) &= \tfrac{1}{2i} \cdot \left(\tfrac{az+b}{cz+d} - \tfrac{a\bar{z}+b}{c\bar{z}+d}\right) = \tfrac{1}{2i} \cdot \tfrac{(az+b)(c\bar{z}+d)-(a\bar{z}+b)(cz+d)}{(cz+d)(c\bar{z}+d)} = \tfrac{1}{2i} \cdot \tfrac{(ad-bc)(z-\bar{z})}{|cz+d|^2} \\ &= \tfrac{(ad-bc)}{|cz+d|^2} \cdot \mathrm{Im}(z) = \tfrac{\mathrm{Im}(z)}{|cz+d|^2} > 0. \end{aligned}$$

Thus the map is well-defined. That I_2 acts trivially on $\mathbb{H}$ is clear. Let $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ be elements of $\mathrm{SL}_2(\mathbb{R})$. Then $\sigma\tau = \left(\begin{smallmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{smallmatrix}\right)$. Thus for all $z \in \mathbb{H}$ we have

$$(\sigma\tau) \cdot z = \frac{(aa'+bc')z + ab' + bd'}{(ca'+dc')z + cb' + dd'}.$$

Direct computation shows that this is equal to $\sigma \cdot (\tau \cdot z) = \sigma \cdot (\frac{a'z+b'}{c'z+d'})$. Thus the map defines a left action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$.

(b) An element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of $\mathrm{SL}_2(\mathbb{R})$ is in the kernel if and only if $\frac{az+b}{cz+d} = z$ for all $z \in \mathbb{H}$. This is equivalent to $cz^2+(d-a)z+b = 0$. The polynomial $cZ^2+(d-a)Z+b \in \mathbb{C}[Z]$ has infinitely many zeroes if and only if it is the zero polynomial. Thus $b = c = 0$ and $d = a$. This corresponds to the elements $\pm I_2 \in \mathrm{SL}_2(\mathbb{R})$.

(c) Let $z \in \mathbb{H}$, and write $z = x + iy$ for $x, y \in \mathbb{R}$. Define $\sigma = \left(\begin{smallmatrix} y^{-\frac{1}{2}} & -xy^{-\frac{1}{2}} \\ 0 & y^{\frac{1}{2}} \end{smallmatrix}\right)$. Then

$$\sigma \cdot z = \frac{1}{y}(x+iy) - \frac{x}{y} = i.$$

It follows that every element of $\mathbb{H}$ is taken to i by an element of $\mathrm{SL}_2(\mathbb{R})$, from which we deduce the transitivity.

(d) An element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{R})$ fixes i if and only if $\frac{ai+b}{ci+d} = i \Leftrightarrow ai+b = -c+di \Leftrightarrow a = d$ and $b = -c$. Thus $\mathrm{Stab}(i)$ consists of the matrices in $\mathrm{SL}_2(\mathbb{R})$ of the form $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$. This is exactly $\mathrm{SO}_2(\mathbb{R})$.

**15. Bestimme die von allen Grundoperationen mit Rubiks Würfel erzeugte Symmetriegruppe und deren Ordnung. Wenn man den Würfel auseinandernimmt, auf wieviele verschiedene Arten kann man ihn wieder zusammensetzen, so dass die Resultate sich nicht durch eine Folge von Grundoperationen ineinander überführen lassen?

*16. Zeige: Für jeden endlichen Körper K mit $|K| \geqslant 4$ ist die folgende Gruppe einfach:

$$\mathrm{PSL}(2,K) := \mathrm{SL}_2(K)/\{\pm I_2\}.$$

Lösung: Da nicht jede Matrix in $\mathrm{SL}_2(K)$ skalar ist, ist $\mathrm{PSL}(2,K)$ nichttrivial. Es bleibt zu zeigen, dass jeder nichttriviale Normalteiler von $\mathrm{PSL}(2,K)$ gleich $\mathrm{PSL}(2,K)$ ist. Nach dem zweiten Isomorphiesatz ist dies äquivalent dazu, dass jeder Normalteiler $H \triangleleft \mathrm{SL}_2(K)$ mit $\{\pm I_2\} \lneqq H$ gleich $\mathrm{SL}_2(K)$ ist. Sei also H ein solcher.

Schritt 1: In H existiert ein nicht-skalares Element der Form $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$.

Beweis: Falls nicht, so existiert ein $h = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in H$ mit $c \neq 0$. Für jedes $x \in K^\times$ und $y \in K$ ist $g := \left(\begin{smallmatrix} x & y \\ 0 & x^{-1} \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$ und folglich $[h,g] = hgh^{-1}g^{-1} \in H$. Eine explizite Rechnung unter Benutzung von $ad - bc = 1$ liefert

$$[h,g] \;=\; \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}\right] \;=\; \begin{pmatrix} ad - acyx^{-1} - bcx^{-2} & * \\ cd - c^2yx^{-1} - cdx^{-2} & * \end{pmatrix} \;\in\; H.$$

Mit $y := c^{-1}d(x - x^{-1})$ verschwindet der linke untere Eintrag, und der linke obere Eintrag wird x^{-2}. Wegen $\det([h,g]) = 1$ folgt dann

$$[h,g] \;=\; \begin{pmatrix} x^{-2} & * \\ 0 & x^2 \end{pmatrix} \;\in\; H.$$

Falls $x^{-2} \neq x^2$ ist, so ist dies ein nicht-skalares Element der gesuchten Form. Aber die Bedingung $x^{-2} \neq x^2$ ist äquivalent zu $x^4 \neq 1$ und verbietet somit höchstens 4 Elemente von $K^\times$. Im Fall $|K| \geqslant 6$ lässt sich also ein $x \in K^\times$ mit $x^{-2} \neq x^2$ finden, und wir sind fertig. Das Gleiche gilt auch im Fall $|K| = 4$, da dann $K^\times$ die Ordnung 3 hat, also ein Element x der Ordnung 3 besitzt, für welches dann $x^4 = x \neq 1$ ist.

Im Fall $|K| = 5$ ist $K \cong \mathbb{F}_5$, also oBdA $K = \mathbb{F}_5$. Dann gibt es immerhin ein Element $x \in K^\times$ mit $x^2 = -1$, zum Beispiel die Restklasse von 2. Für dieses ergibt sich $[h,g] = \left(\begin{smallmatrix} -1 & -2c^{-1}(a+d) \\ 0 & -1 \end{smallmatrix}\right) \in H$. Ist $a + d \neq 0$, so ist dies ein nicht-skalares Element der gesuchten Form, und wir sind fertig. Ist $a + d = 0$, so hat h das charakteristische Polynom $X^2 + 1$. Über $\mathbb{F}_5$ zerfällt dieses in zwei inäquivalente Linearfaktoren $(X-2)(X-3)$. Somit ist h diagonalisierbar und es existiert ein $g \in \mathrm{GL}_2(K)$ mit $ghg^{-1} = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$. Die Matrix $g' := \left(\begin{smallmatrix} \det(g)^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot g$ liegt dann in $\mathrm{SL}_2(K)$ und erfüllt ebenfalls $g'hg'^{-1} = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$. Wegen $H \triangleleft \mathrm{SL}_2(K)$ ist nun $g'hg'^{-1} \in H$ ein nicht-skalares Element der gesuchten Form, und wir sind ebenfalls fertig. *q.e.d.*

Schritt 2: In H existiert ein Element der Form $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ mit $x \neq 0$.

Beweis: Nach Schritt 1 existiert ein nicht-skalares Element der Form $h = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in H$. Ist $a = d$, so ist $ad = \det(h) = 1$ und folglich $a = d = \pm 1$ und somit

$\pm h = \left(\begin{smallmatrix} 1 & \pm b \\ 0 & 1 \end{smallmatrix}\right) \in H$ mit $\pm b \neq 0$, wie gewünscht. Ist $a \neq d$, so ist der Kommutator $\left[h, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\right] = \left(\begin{smallmatrix} 1 & a/d-1 \\ 0 & 1 \end{smallmatrix}\right) \in H$ mit $a/d - 1 \neq 0$, wie gewünscht. *q.e.d.*

Schritt 3: Es gilt $\left(\begin{smallmatrix} 1 & K \\ 0 & 1 \end{smallmatrix}\right) < H$.

Beweis: Sei x wie in Schritt 2. Für alle $y \in K^\times$ ist $\left(\begin{smallmatrix} y & 0 \\ 0 & y^{-1} \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$ und folglich

$$\begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & y^2 x \\ 0 & 1 \end{pmatrix} \in H.$$

Für zwei Elemente $y, y' \in K^\times$ ist $y^2 x = y'^2 x$ genau dann, wenn $y = \pm y'$ ist. Während y durch $K^\times$ läuft, erhalten wir somit mindestens $|K^\times|/2$ verschiedene nicht-triviale Elemente von $H \cap \left(\begin{smallmatrix} 1 & K \\ 0 & 1 \end{smallmatrix}\right)$. Daher gilt $\left|H \cap \left(\begin{smallmatrix} 1 & K \\ 0 & 1 \end{smallmatrix}\right)\right| \geqslant 1 + |K^\times|/2 > |K|/2$, nach Lagrange also $\left[\left(\begin{smallmatrix} 1 & K \\ 0 & 1 \end{smallmatrix}\right) : H \cap \left(\begin{smallmatrix} 1 & K \\ 0 & 1 \end{smallmatrix}\right)\right] < 2$. Da der Index aber eine ganze Zahl $\geqslant 1$ ist, muss er deshalb gleich 1 sein. Folglich ist $\left(\begin{smallmatrix} 1 & K \\ 0 & 1 \end{smallmatrix}\right) < H$, wie gewünscht. *q.e.d.*

Schritt 4: Es gilt $\left(\begin{smallmatrix} 1 & 0 \\ K & 1 \end{smallmatrix}\right) < H$.

Beweis: Wegen $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$ und

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ K & 1 \end{pmatrix}$$

folgt dies aus Schritt 3. *q.e.d.*

Schritt 5: Es ist $H = \mathrm{SL}_2(K)$.

Beweis: Für alle $x, y, z \in K$ ist

$$A(x,y,z) := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & z \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+xy & x+xyz+z \\ y & 1+yz \end{pmatrix} \in H$$

nach Schritt 3 und 4. Betrachte ein beliebiges Element $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$. Im Fall $c \neq 0$ haben wir $A(c, (a-1)c^{-1}, (d-1)c^{-1}) = \left(\begin{smallmatrix} a & * \\ c & d \end{smallmatrix}\right)$. Da diese Matrix wie g die Determinante 1 hat, ist sie auch insgesamt gleich g und es folgt $g \in H$. Im Fall $c = 0$ ist $a \neq 0$ und $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) g = \left(\begin{smallmatrix} a & b \\ a & a+b \end{smallmatrix}\right) \in H$ wie gerade gezeigt, also auch $g \in H$. *q.e.d.*

Bemerkung: Dass K endlich ist, wurde nur in Schritt 3 benutzt. Für einen unendlichen Körper muss man an dieser Stelle anders argumentieren.

17. Beweise für beliebige Untergruppen $H_1 < G > H_2 > H_2'$ die Ungleichungen

    (a) $[H_1 : H_1 \cap H_2] \leqslant [G : H_2]$.

    (b) $[G : H_1 \cap H_2] \leqslant [G : H_1] \cdot [G : H_2]$.

    (c) $[H_1 \cap H_2 : H_1 \cap H_2'] \leqslant [H_2 : H_2']$.

Lösung: (a) Betrachte die Linksoperation von H_1 auf G/H_2 durch Linkstranslation $(h_1, gH_2) \mapsto h_1 g H_2$. Der Stabilisator der trivialen Nebenklasse H_2 ist die Menge aller $h_1 \in H_1$ mit $h_1 H_2 = H_2$, was äquivalent ist zu $h_1 \in H_2$; der Stabilisator ist also $H_1 \cap H_2$. Die Bahn des Elements $H_2 \in G/H_2$ unter H_1 hat folglich die Länge $[H_1 : H_1 \cap H_2]$, und ist $\leqslant |G/H_2| = [G : H_2]$, woraus (a) folgt.

(b) Mit Lagrange und (a) folgt

$$[G : H_1 \cap H_2] = [G : H_1] \cdot [H_1 : H_1 \cap H_2] \leqslant [G : H_1] \cdot [G : H_2].$$

(c) Wegen $H_1 \cap H_2' = (H_1 \cap H_2) \cap H_2'$ ist (c) genau die Aussage (a) für die Gruppen $H_1 \cap H_2 < H_2 > H_2'$ anstelle von $H_1 < G > H_2$.

*18. *Cohen-Lenstra Heuristik.* Betrachte eine nicht-leere Menge X der Kardinalität n.

(a) Zeige: Die Anzahl der Isomorphieklassen von Gruppen der Ordnung n ist > 0 und $< \infty$.

Seien $G_1, \ldots, G_r$ Repräsentanten dieser Isomorphieklassen. Sei $\mathcal{G}$ die Menge aller Gruppenstrukturen auf X, und für jedes i sei $\mathcal{G}_i$ die Teilmenge der Gruppenstrukturen auf X, so dass die resultierende Gruppe isomorph zu G_i ist. Wir fassen $\mu_i := |\mathcal{G}_i|/|\mathcal{G}|$ auf als die *Wahrscheinlichkeit, dass eine zufällige Gruppe der Ordnung n isomorph zu G_i ist.*

(b) Zeige, dass $\mu_i = c_n / |\operatorname{Aut}(G_i)|$ ist für eine nur von n abhängige Zahl $c_n \in \mathbb{Q}^{>0}$.

(c) Bestimme die Wahrscheinlichkeiten für alle Gruppen der Ordnungen 4, 6, 8. Welche sind jeweils die häufigsten?

Lösung:

(a) Für jede Gruppe G der Ordnung n existiert eine Bijektion $X \to G$, und wenn wir via dieser Bijektion die Gruppenstruktur von G auf X übertragen, wird die Bijektion ein Isomorphismus. Jede Isomorphieklasse von Gruppen der Ordnung n enthält also einen Repräsentanten mit der unterliegenden Menge X. Da es nur endlich viele Abbildungen $X \times X \to X$ gibt, gibt es auch nur endlich viele Gruppenstrukturen auf X. Andererseits gibt es mindestens eine, zum Beispiel für eine zyklische Gruppe der Ordnung n.

(b) Nach der Begründung in (a) ist jedes $\mathcal{G}_i$ nichtleer. Seien $\circ$ und $*$ Gruppenstrukturen in $\mathcal{G}_i$. (Wir können das Einselement weglassen, weil es durch die Gruppenoperation jeweils schon eindeutig bestimmt ist.) Dann existieren Isomorphismen $(X, \circ) \cong G_i \cong (X, *)$. Deren Komposition ist eine Permutation von X, welche die Gruppenstruktur $\circ$ in die Gruppenstruktur $*$ überführt. Umgekehrt überführt jede Permutation von X die Gruppenstruktur $\circ$ in eine weitere Gruppenstruktur in $\mathcal{G}_i$. Also induziert die Operation der symmetrischen Gruppe $S(X)$ auf X eine transitive Operation auf $\mathcal{G}_i$. Der Stabilisator von $\circ$ in $S(X)$ ist die Menge

aller Bijektionen $X \to X$, welche einen Isomorphismus $(X, \circ) \to (X, \circ)$ induzieren, also mit anderen Worten die Automorphismengruppe von $(X, \circ)$. Nach der Bahnengleichung gilt somit

$$n! \;=\; |S(X)| \;=\; |\mathcal{G}_i| \cdot |\operatorname{Stab}_{S(X)}(\circ)| \;=\; |\mathcal{G}_i| \cdot |\operatorname{Aut}((X, \circ))| \;=\; |\mathcal{G}_i| \cdot |\operatorname{Aut}(G_i)|.$$

Folglich ist

$$\mu_i \;:=\; \frac{|\mathcal{G}_i|}{|\mathcal{G}|} \;=\; \frac{n!}{|\mathcal{G}| \cdot |\operatorname{Aut}(G_i)|}$$

und die gesuchte Aussage gilt mit $c_n := n!/|\mathcal{G}|$. Da die Summe der Wahrscheinlichkeiten 1 ergeben muss, kann man c_n auch ausdrücken als

$$c_n \;=\; \left(\textstyle\sum_{i=1}^{r} \frac{1}{|\operatorname{Aut}(G_i)|}\right)^{-1}.$$

(c) Recall the classification of groups of order at most 7 in Serie 9, Aufgabe 4. In each case we compute probabilities using the formula from (b).

- $n = 4$: Here there are two isomorphism classes, represented by $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{F}_2^2$. We have $\operatorname{Aut}(\mathbb{Z}/4\mathbb{Z}) = (\mathbb{Z}/4\mathbb{Z})^\times$, which has order 2. Also $\operatorname{Aut}(\mathbb{F}_2^2) \cong \mathrm{GL}_2(\mathbb{F}_2)$ has order $(2^2 - 1)(2^2 - 2) = 6$. Using the expression above, we obtain $c_4 = (\frac{1}{2} + \frac{1}{6})^{-1} = \frac{3}{2}$. This yields:

G_i	$\lvert\operatorname{Aut}(G_i)\rvert$	μ_i
$\mathbb{Z}/4\mathbb{Z}$	2	$\frac{3}{4}$
$\mathbb{F}_2^2$	6	$\frac{1}{4}$

- $n = 6$: Here again we have two isomorphism classes, represented by $\mathbb{Z}/6\mathbb{Z}$ and $D_3 \cong S_3$. We have $|\operatorname{Aut}(\mathbb{Z}/6\mathbb{Z})| = |(\mathbb{Z}/6\mathbb{Z})^\times| = 2$. Now D_3 is generated by elements S and T with orders 2 and 3 respectively. The elements of order 2 are S, ST, ST^2. Those of order 3 are T and T^2. Any automorphism is determined by the images of S and T. It must furthermore send S to an element of order 2 and T to an element of order 3. Counting we find that there are 6 possibilities for such maps, and one can check that each defines a homomorphism. Therefore $|\operatorname{Aut}(D_3)| = 6$. It follows that $c_6 = (\frac{1}{2} + \frac{1}{6})^{-1} = \frac{3}{2}$. This yields:

G_i	$\lvert\operatorname{Aut}(G_i)\rvert$	μ_i
$\mathbb{Z}/6\mathbb{Z}$	2	$\frac{3}{4}$
D_3	6	$\frac{1}{4}$

- $n = 8$: There are 5 isomorphism classes. We compute $c_8 = \frac{42}{23}$. This yields:

G_i	$\lvert \operatorname{Aut}(G_i) \rvert$	μ_i
C_8	4	$\frac{21}{46}$
$C_2 \times C_4$	8	$\frac{21}{92}$
D_4	8	$\frac{21}{92}$
Q	24	$\frac{7}{92}$
$\mathbb{F}_2^3$	168	$\frac{1}{92}$

In all three cases the cyclic group occurs with the highest probability.