Aufgabe 1 (Frühjahr 1999)**.** Seien U und V Untergruppen einer endlichen Gruppe G mit $U \cap V = \{e\}$. Es bezeichne $\langle U \cup V \rangle$ die von $U \cup V$ erzeugte Untergruppe von G. Man zeige:

(a) $|U| \cdot |V| \leqslant |\langle U \cup V \rangle|$. *(Wurde bereits letzte Woche besprochen.)*

(b) In (a) gilt Gleichheit, wenn U Normalteiler in G ist.

(c) Man gebe eine Gruppe G mit zwei Untergruppen U und V mit $U \cap V = \{e\}$ an, so daß in (a) nicht Gleichheit besteht. *(Wurde bereits letzte Woche besprochen.)*

Lösung. **(b)** Wir zeigen, daß jedes Element in $\langle U \cup V \rangle$ eine Darstellung der Form uv hat mit $u \in U$ und $v \in V$. Ein Element $x \in \langle U \cup V \rangle$ kann nach Definition geschrieben werden als endliches Produkt $x = x_1 \cdots x_n$ mit $x_i \in U \cup V$, dh. $x_i \in U$ oder $x_i \in V$. Wir werden nun Induktion nach n anwenden.
Sei $n = 1$, dann ist $x = x_1 \in U$ oder $x = x_1 \in V$, Im ersten Fall ist unsere gewünschte Darstellung xe und im zweiten Fall ex.
Sei $n = 2$, dann ist $x = x_1 x_2$. Die Fälle $x_1, x_2 \in U$, oder $x_1, x_2 \in V$, oder $x_1 \in U$ und $x_2 \in V$ sind trivial. Sei also $x_1 \in V$ und $x_2 \in U$. Da U Normalteiler ist, gilt $x_1 U = U x_1$. Insbesondere gibt es $x_2' \in U$ mit $x = x_1 x_2 = x_2' x_1$. Wir setzen also $u := x_2'$ und $v := x_1$ und sind fertig.
Für den Induktionsschritt nehmen wir an, daß wir für $n \geqslant 1$ bereits gezeigt haben, daß jedes Produkt $x = x_1 \cdots x_n$ wie oben aus n Elementen eine Darstellung hat der Form uv. Sei nun $x = x_1 \cdots x_{n+1}$ ein Produkt aus $n+1$ Elementen. MIt dem Assoziativgesetz gilt $x = (x_1 \cdots x_n) x_{n+1}$ und nach Induktionsannahme können wir $x_1 \cdot x_n$ schreiben als uv. Ist $x_{n+1} \in V$, so ist $x = (uv)x_{n+1} = u(vx_{n+1})$ bereits in der gewünschten Form. Ist $x_{n+1} \in U$, so gibt es, da U Normalteiler ist ein $x_{n+1}' \in U$ mit $vx_{n+1} = x_{n+1}' v$, also $x = u(vx_{n+1}) = (ux_{n+1}')v$, und damit ist x in der gewünschten Form.

Aufgabe 2. Sei p prim, G Gruppe der Ordnung p^2. Man zeige, daß entweder $G \cong \mathbb{Z}/\mathbb{Z}p^2$, oder $\mathbb{Z} \cong \mathbb{Z}/\mathbb{Z}p \times \mathbb{Z}/\mathbb{Z}p$.

Lösung. Wir wissen, daß G abelsch ist. Falls für alle $e \neq x \in G$ gilt $\operatorname{ord}(x) = p$: sei $e \neq x, y \in G$ mit $y \in G \backslash \langle x \rangle$. Da $\langle x \rangle$ und $\langle y \rangle$ die Ordnung p haben, gilt

$$\langle x \rangle \cap \langle y \rangle = \{e\}.$$

Wir zeigen: die Abbildung

$$h : \mathbb{Z}/\mathbb{Z}p \times \mathbb{Z}/\mathbb{Z}p \to G, (\overline{a}, \overline{b}) \mapsto x^a y^b$$

ist Isomorphismus, dabei ist $\overline{a} = a + \mathbb{Z}p$ und $\overline{b} = b + \mathbb{Z}p$.

$$\begin{aligned} h((\overline{a}_1, \overline{b}_1) + (\overline{a}_2, \overline{b}_2)) &= h(\overline{a}_1 + \overline{a}_2, \overline{b}_1 + \overline{b}_2) \\ &= h(\overline{a_1 + a_2}, \overline{b_1 + b_2}) \\ &= x^{a_1 + a_2} y^{b_1 + b_2} \\ &= x^{a_1} x^{a_2} y^{b_1} y^{b_2} \\ &= x^{a_1} y^{b_1} x^{a_2} y^{b_2} = h(\overline{a}_1 \overline{b}_1) h(\overline{a}_2, \overline{b}_2). \end{aligned}$$

h ist injektiv: Aus $h(\overline{a}, \overline{b}) = e$ folgt $x^a y^b = e$ also $x^a = y^{-b} \in \langle x \rangle \cap \langle y \rangle = \{e\}$, das heißt $x^a = y^b = e$ und es muß gelten $p|a, b$ in anderen Worten $a, b \in \mathbb{Z}p$ oder $a = \overline{b} = \overline{0}$. Also $(\overline{a}, \overline{b}) = (\overline{0}, \overline{0})$.
Da beide Seiten p^2 Elemente haben, ist h Isomorphismus.
Gibt es $x \in G$ der Ordnung p^2, dann ist $G = \langle x \rangle$ und es gibt einen Ismorphismus

$$\mathbb{Z}/\mathbb{Z}p^2 \to \langle x \rangle.$$

Aufgabe 3 (Frühjahr 1991)**.** Sei $\alpha : G \to H$ ein Gruppenhomomorphismus, wobei H abelsch sei. Man zeige: α ist genau dann surjektiv, wenn für je zwei Gruppenhomomorphismen $\beta, \gamma : H \to K$ mit $\beta \circ \alpha = \gamma \circ \alpha$ gilt $\beta = \gamma$.

Lösung. Wir nehmen zuerst an, daß α surjektiv ist. Seien $\beta, \gamma : H \to K$ beliebige Homomorphismen mit $\beta \circ \alpha = \gamma \circ \alpha$. Wir müssen zeigen, daß $\beta = \gamma$. Dazu genügt es zu zeigen, daß für alle $h \in H$ gilt $\beta(h) = \gamma(h)$. Aber da α surjektiv ist, gibt es für jedes $h \in H$ ein $g \in G$ mit $h = \alpha(g)$ und es gilt

$$\beta(h) = \beta(\alpha(g)) = \beta \circ \alpha(g) = \gamma \circ \alpha(g) = \gamma(\alpha(g)) = \gamma(h).$$

Und wir sind fertig.
Nehmen wir andererseits an, daß für je zwei Homomorphismen $\beta, \gamma : H \to K$ mit $\beta\circ\alpha = \gamma\circ\alpha$ gilt $\beta = \gamma$. Da H abelsch ist, ist $\alpha(G) \subset H$ als Untergruppe Normalteiler und der Quotient $H/\alpha(G)$ eine Faktorgruppe. Sei $\beta : H \to H/\alpha(G), h \mapsto \overline{0}$, die triviale Abbildung. Sei andererseits $\gamma : H \to H/\alpha(G), h \mapsto \overline{h}$ die kanonische Abbildung. Für $g \in G$ gilt $\beta \circ \alpha(g) = \overline{0} = \gamma \circ \alpha(g)$, das heißt

$$\beta \circ \alpha = \overline{0} = \gamma \circ \alpha$$

und damit nach Voraussetzung $\beta = \gamma$. Da γ surjektiv ist, ist also $H/\alpha(G) = \{\overline{0}\}$ und damit $\alpha(G) = H$. Also ist α surjektiv.

Aufgabe 4 (Herbst 1977)**.** G sei eine endliche Gruppe und φ ein Automorphismus von G, für den $\varphi(x) = x$ nur für $x = e$ gilt. Man zeige:

(a) Die Abbildung $y \mapsto y^{-1}\varphi(y)$ von G in sich ist injektiv.

(b) Zu jedem $x \in G$ gibt es ein $y \in G$ mit $x = y^{-1}\varphi(y)$.

(c) Wenn zusätzlich $\varphi^2 = \mathrm{id}$ gilt, dann folgt

  (i) $\varphi(x) = x^{-1}$ für alle $x \in G$,

  (ii) G ist abelsch.

Lösung. **(a)** Sei für $x, y \in G$

$$x^{-1}\varphi(x) = y^{-1}\varphi(y).$$

Wir multiplizieren von links mit y und von rechts mit $\varphi(x)^{-1} = \varphi(x^{-1}$

$$yx^{-1} = \varphi(y)\varphi(x)^{-1} = \varphi(y)\varphi(x^{-1}) = \varphi(yx^{-1}).$$

Dann gilt nach Voraussetzung $yx^{-1} = e$, also $y = x$. Dies zeigt, daß die Abbildung injektiv ist.

(b) Da G endliche Gruppe, also insbesondere endliche Menge ist, und eine injektive Selbstabbildung einer endlichen Menge automatisch surjektiv ist, ist die Abbildung aus **(a)** surjektiv und es gibt für jedes $x \in G$ ein $y \in G$ mit $x = y^{-1}\varphi(y)$ wie gewünscht.

(c.i) Sei $x \in G$. Nach **(b)** gibt es $y \in G$ mit $x = y^{-1}\varphi(y)$. Dann ist $\varphi(x) = \varphi(y^{-1})\varphi^2(y) = \varphi(y)^{-1}y$. Also

$$x\varphi(x) = y^{-1}\varphi(y)\varphi(y)^{-1}y = e.$$

Das heitßt $\varphi(x)$ ist Inverses von x.

(c.ii) Sei $x, y \in G$. Setze $a = xy$. Wir üssen zeigen, daß $xy = yx$, oder äquivalent dazu $xyx^{-1}y^{-1} = e$. Nach **(c.i)** gilt

$$xyx^{-1}y^{-1} = xy\varphi(x)\varphi(y) = xy\varphi(xy) = a\varphi(a) = e.$$

Aufgabe 5 (Herbst 1993)**.** Es bezeichne $M(2 \times 2, S)$ den RIng aller 2-reihigen atrizen mit Koeffizienten in eine Ring S. Sei

$$O(2) := \{A \in M(2 \times 2, \mathbb{R}) : A^tA = 1\}$$

die Gruppe der reellen orthogonalen 2-reihigen Matrizen.

(a) Man zeige:

$$G := 0(2) \cap M(2 \times 2, \mathbb{Z})$$

is eine Gruppe der Ordnung 8.

(b) G besitzt genau eine zyklische Untergruppe G_0 der Ordnung 4.

(c) Für alle $d \in G_0$ und $s \in G \backslash G_0$ gilt

$$sd = d^{-1}s.$$

Lösung. **(a)** Die Gruppe $O(2)$ sind die reellen orthogonalen Matrizen und stellen Drehspiegelungen dar. Sie haben Determinante 1 (für Drehungen) oder -1 (für Spiegelungen). Sei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{dann ist} \qquad A^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Und die Gleichung $A^t A = 1$ liefert die Gleichungen

$$\begin{aligned} a^2 + c^2 &= 1 \\ b^2 + d^2 &= 1 \\ ab + cd &= 0 \end{aligned}$$

Über $\mathbb{R}$ erhält man damit

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} = D(\alpha) \qquad \text{oder} \qquad A = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} = S(\alpha),$$

mit $0 \leqslant \alpha \leqslant 2\pi$. Ersteres ist eine Drehung um den Winkel α mit Drehzentrum im Ursprung, und letzteres eine Spiegelung an der Achse $\mathbb{R}\begin{pmatrix} \cos\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} \end{pmatrix}$.

Über $\mathbb{Z}$ ergeben die obigen Gleichungen:

$$\left\{ \begin{matrix} a = \pm 1 \\ d = \pm 1 \\ b = c = 0 \end{matrix} \right\} \text{ oder } \left\{ \begin{matrix} b = \pm 1 \\ c = \pm 1 \\ a = d = 0 \end{matrix} \right\}.$$

Die Menge G enthält also die acht Matrizen

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$$

Es gilt

$$\begin{aligned} 1 &= \det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \det\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \det\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \det\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ -1 &= \det\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \det\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \det\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \det\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \end{aligned}$$

Die Menge G ist eine Gruppe, da

- $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in O(2) \cap M(2 \times 2, \mathbb{Z})$,
- für $A, B \in O(2) \cap M(2 \times 2, \mathbb{Z})$ gilt $AB \in O(2)$, da $O(2)$ Gruppe ist, und $AB \in M(2 \times 2, \mathbb{Z})$ wegen der Definition der Matrixmultiplikation,
- für $A \in O(2)$ gilt $A^{-1} \in O(2)$, da $O(2)$ eine Gruppe ist, und $A^{-1} \in M(2 \times 2, \mathbb{Z})$, da $A = A^t$.

(b) Für die Elemente gilt

$$\begin{aligned} 1 &= \operatorname{ord}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ 2 &= \operatorname{ord}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \operatorname{ord}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \operatorname{ord}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \operatorname{ord}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \operatorname{ord}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \\ 4 &= \operatorname{ord}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \operatorname{ord}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

Und

$$G_0 := \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

ist die einzige Untergruppe der Ordnung 4.

(c) Sie Elemente in $G \setminus G_0$ sind genau die Elemente der Ordnung 2, die nicht in G_0 enthalten sind, also

$$G \setminus G_0 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Für $d = e$ gilt die Gleichung trivialerweise für alls $s \in G \setminus G_0$.
Für $d = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1e$ ist $d^{-1} = d$ und die Gleichung $sd = ds$ gilt ebenso trivialerweise da d ein Vielfaches der Einheitsmatrix ist.
Für $d = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ist $d^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und die Gleichungen

$$sd = d^{-1}s \quad \text{und} \quad sd^{-1} = ds$$

sind äquivalent. Dies kann man leicht nachrechnen:

$$\begin{aligned}
s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}: &\quad sd = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = d^{-1}s \\
s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}: &\quad sd = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = d^{-1}s \\
s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}: &\quad sd = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = d^{-1}s \\
s = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}: &\quad sd = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = d^{-1}s
\end{aligned}$$