Gruppentheorie

FSU Jena - SS 2009

Übungsserie 08 - Lösungen

Stilianos Louca

July 9, 2009

Aufgabe 30

(i) Die Fälle $n = 0$ und $n = 1$ sind klar. Sei nun $[a^n, b] = [a, b]^n$ für ein $n \in \mathbb{N}$. Dann

$$[a^{n+1}, b] = [aa^n, b] = a \underbrace{[a^n, b]}_{[a,b]^n} a^{-1}[a, b] = [a, b]^n aa^{-1}[a, b] = [a, b]^{n+1}$$

Wegen

$$1 = [a^{-n}a^n, b] = a^{-n} \underbrace{[a^n, b]}_{[a,b]^n} a^n [a^{-n}, b] = [a, b]^n [a^{-n}, b] \quad , \quad n \in \mathbb{N}$$

ist dann auch $[a^{-n}, b] = [a, b]^{-n}$.

(ii) Induktionsanfang $n = 1$ ist klar. Wegen $[a, b]b = b[a, b]$, bzw. $b^{-1} \underbrace{[b, a]}_{[a,b]^{-1}} = [b, a]b^{-1}$ ist

$$[b, a]b = b \underbrace{b^{-1}[b, a]}_{[b,a]b^{-1}} b = b[b, a]$$

(analog für a) das heißt $[b, a]$ vertauscht mit a, a^{-1}, b und b^{-1}. Ferner gilt

$$ab^n = abb^{n-1} = [a, b]bab^{n-1} = bab^{n-1}[a, b] = b^2a[a, b]b^{n-2}[a, b] = b^2ab^{n-2}[a, b]^2 = (..) = b^n a[a, b]^n \tag{1}$$

Es gelte nun die Behauptung für irgendein $n \in \mathbb{N}$, dann ist

$$(ab)^{n+1} = (ab)^n(ab) \overset{\text{I.V.}}{=} a^n b^n [b, a]^{\binom{n}{2}} ab = a^n b^n \overbrace{[a, b]^n aa^{-1}[b, a]^n}^{1} [b, a]^{\binom{n}{2}} ab$$

$$= a^n \underbrace{b^n a[a, b]^n}_{\substack{ab^n \\ (1)}} \underbrace{[b, a]^n [b, a]^{\binom{n}{2}}}_{[b,a]^{\binom{n+1}{2}}} \underbrace{a^{-1}a}_{1} b = a^{n+1}b^n \underbrace{[b, a]^{\binom{n+1}{2}} b}_{b[b,a]^{\binom{n+1}{2}}} = a^{n+1}b^{n+1}[b, a]^{\binom{n+1}{2}}$$

□

Aufgabe 31

Nennen $\mathfrak{B}(n, \mathbb{K})$ die Gruppe aller oberen Dreiecksmatrizen aus $\mathrm{GL}(n, \mathbb{K})$ (vgl. Übungsaufgabe 10) und $\mathfrak{D}(n, \mathbb{K})$ die Menge aller Matrizen aus $\mathfrak{B}(n, \mathbb{K})$ mit 1-Diagonale. Ferner sei $\mathfrak{G}(n, \mathbb{K})$ die Menge aller oberen Dreiecksmatrizen.

Beachte dass für $A, B \in \mathfrak{G}(m, \mathbb{K})$ stets $AB \in \mathfrak{G}(m, \mathbb{K})$ ist. Ist ferner die Diagonale von B gleich 0, so ist auch die Diagonale von AB und BA gleich 0.

(i)

- **Behauptung:** Für beliebiges $0 \le m \le n-1$ ist

$$G_m := \left\{ \underbrace{1_n + \begin{pmatrix} 0 & \dots & A \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}}_{M^A} : A \in \mathfrak{G}(m, \mathbb{K}) \right\} \tag{2}$$

  eine Untergruppe von $G := \mathfrak{D}(n, \mathbb{K})$.
  Beweis: Für $M \in \mathfrak{G}(n, \mathbb{K})$ und $A \in \mathfrak{G}(m, \mathbb{K}),\ m \le n-1$ gilt

$$M \cdot M^A = M + M \cdot \begin{pmatrix} 0 & \dots & A \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} = M + \begin{pmatrix} 0 & \dots & M_{m\times m} \cdot A \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \tag{3}$$

  und

$$M^A \cdot M = M + \begin{pmatrix} 0 & \dots & A \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \cdot M = M + \begin{pmatrix} 0 & \dots & A \cdot M^{m\times m} \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \tag{4}$$

  wobei

$$\underbrace{\begin{pmatrix} M_{11} & \dots & M_{1m} \\ \vdots & \ddots & \vdots \\ 0 & \dots & M_{mm} \end{pmatrix}}_{=:M_{m\times m} \in \mathfrak{D}(m,\mathbb{K})} \cdot A \in \mathfrak{G}(m, \mathbb{K}) \quad , \quad A \cdot \underbrace{\begin{pmatrix} M_{n-m+1,n-m+1} & \dots & M_{n-m+1,n} \\ \vdots & \ddots & \vdots \\ 0 & \dots & M_{nn} \end{pmatrix}}_{=:M^{m\times m} \in \mathfrak{D}(m,\mathbb{K})} \in \mathfrak{G}(m, \mathbb{K})$$

  Nun zum Beweis der Behauptung. Der Fall $m = 0$ ist klar, ebenso der Fall $m = 1$ (da $G_1 = Z(\mathfrak{D}(n, \mathbb{K}))$ nach Übungsaufgabe (16)). Sei nun $G_{m-1} \le G$ für irgendein $1 \le m \le n-1$. Dann ist G_m nicht leer und für $M^A, M^B \in G_m$ gilt

$$\underbrace{M^A}_{\in \mathfrak{G}(n,\mathbb{K})} \cdot M^B = \begin{pmatrix} 1 & \dots & A \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} + \begin{pmatrix} 0 & \dots & M^A_{m\times m} B \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \in G_m \quad \text{denn} \quad A + M^A_{m\times m} B \in \mathfrak{G}(m, \mathbb{K})$$

$$\text{Insbesondere:} \quad \begin{pmatrix} 1 & \dots & -M^A_{m\times m} A \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} 1 & \dots & A \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}^{-1}$$

- **Behauptung:** Es ist $G_m \trianglelefteq G$.
  Beweis: $G_m \le G$ ist klar. Seien nun $M \in G$ und $M^A \in G_m$ beliebig, dann ist

$$MM^A = M + \begin{pmatrix} 0 & \dots & M_{m\times m} \cdot A \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} = \underbrace{M + \begin{pmatrix} 0 & \dots & \widetilde{A} M^{m\times m} \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}}_{MM^{\widetilde{A}}}$$

  mit

$$\widetilde{A} := \underbrace{M_{m\times m}}_{\in \mathfrak{D}(m,\mathbb{K})} A \underbrace{(M^{m\times m})^{-1}}_{\in \mathfrak{D}(m,\mathbb{K})} \in \mathfrak{G}(m, \mathbb{K})$$

  Somit ist

$$G = G_{n-1} \trianglerighteq G_{n-2} \trianglerighteq \dots \trianglerighteq G_1 \trianglerighteq G_0 = \{1\}$$

  eine Normalreihe.

- **Behauptung:** Für $m \leq n-1$ ist

$$G_m/G_{m-1} \subseteq Z(G/G_{m-1})$$

Beweis: Zu zeigen wäre: Für $M^A \in G_m$ und beliebiges $M \in \overbrace{\mathfrak{D}(n,\mathbb{K})}^{G}$ ist

$$(M^A G_{m-1})(MG_{m-1}) = (MG_{m-1})(M^A G_{m-1})$$

das heißt

$$M^A M = MM^A \cdot M^C$$

für geeignetes $M^C \in G_{m-1}$. Gesucht ist also ein $C \in \mathfrak{G}(m-1,\mathbb{K})$ mit

$$M^A M - MM^A = MM^A \cdot \begin{pmatrix} 0 & \dots & C \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

das heißt nach (3) und (4):

$$AM^{m\times m} - M_{m\times m}A \overset{!}{=} (MM^A)_{(m-1)\times(m-1)}C$$

Tatsächlich ist

$$\widetilde{C} := AM^{m\times m} - M_{m\times m}A = \cancel{A} + A\underbrace{\begin{pmatrix} 0 & * & \dots & * \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & * \\ 0 & 0 & \dots & 0 \end{pmatrix}}_{\in\mathfrak{G}(m-1,\mathbb{K})} - \cancel{A} - \underbrace{\begin{pmatrix} 0 & \star & \dots & \star \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \star \\ 0 & 0 & \dots & 0 \end{pmatrix}}_{\in\mathfrak{G}(m-1,\mathbb{K})} A \in \mathfrak{G}(m-1,\mathbb{K})$$

so dass

$$C := \underbrace{\underbrace{[(\underbrace{MM^A}_{\in\mathfrak{D}(n,\mathbb{K})})_{(m-1)\times(m-1)}]^{-1}}_{\in\mathfrak{D}(m-1,\mathbb{K})} \cdot \underbrace{\widetilde{C}}_{\in\mathfrak{G}(m-1,\mathbb{K})}}_{\in\mathfrak{G}(m-1,\mathbb{K})}$$

genau die Bedingung erfüllt.

- Somit ist

$$G = G_{n-1} \trianglerighteq G_{n-2} \trianglerighteq \dots \trianglerighteq G_1 \trianglerighteq G_0 = \{1\}$$

sogar eine Zentralreihe und G nilpotent mit Klasse höchstens $n-1$.

Alternative für Teil (i): Wir zeigen (durch Induktion über m) dass

$$Z_m(G) = G_m \quad , \quad \forall\ 0 \leq m \leq n-1$$

(siehe Def. 2). Insbesondere hat dann $G = G_{n-1}$ die Nilpotenzklasse $n-1$.
Der Fall $m = 0$ ist klar, denn $G_0 = \{1\} = Z_0(G)$. Es gelte nun die Behauptung für ein $m \leq n-2$.

- Aus Darstellung (3) ist ersichtlich: Für $M, N \in G$ gilt

$$NZ_m(G) = M\underbrace{Z_m(G)}_{G_m} \ \Leftrightarrow\ \exists\ M^A \in G_m : N = M \cdot M^A \ \Rightarrow\ M_{kl} = N_{kl} \ \ \forall\ k < l < n+k-m$$

Aber auch die Umkehrung gilt: Sind $M_{kl} = N_{kl}\ \forall\ k < l < n+k-m$ (sprich M und N gleich, bis auf rechts-oberes $m \times m$ - Dreieck), so erfüllt

$$A := \underbrace{\overbrace{(M_{m\times m})^{-1}}^{\in\mathfrak{D}(m,\mathbb{K})} \cdot \begin{pmatrix} N_{1,n-m+1} & \dots & N_{1,n} \\ \vdots & \ddots & \vdots \\ 0 & \dots & N_{m,n} \end{pmatrix}}_{\in\mathfrak{G}(m,\mathbb{K})}$$

genau die Bedingung $N = M \cdot M^A$.

- Sei nun $H_{kl} := (\delta_{ik} \cdot \delta_{jl})_{i,j=1}^{n}$, dann ist $1 + H_{kl} \in G$ für $k < l$. Da jede $M \in G$ dargestellt werden kann als
$$M = 1 + \sum_{k<l} \underbrace{M_{kl}}_{\in \mathbb{K}} \underbrace{H_{kl}}_{\in \mathbb{K}^{n \times n}}$$
gilt die Äquivalenz:
$$CZ_m(G) \in \underbrace{Z\left(G/Z_m(G)\right)}_{Z_{m+1}(G)/Z_m(G)} \quad \Leftrightarrow \quad CH_{kl} = H_{kl}C(\mathrm{mod} Z_m(G)) \quad \forall\ k < l$$
das heißt nach obigen Überlegungen
$$\underbrace{\begin{array}{cc} & \begin{array}{cccccccccc} &&& l \\ &&& \downarrow &&&&&& \end{array} \\ \begin{array}{c} \\ \\ \\ k \rightarrow \\ \\ \end{array} & \begin{pmatrix} 0 & \dots & 0 & C_{1k} & 0 & \dots & * & * & \dots & * \\ 0 & \dots & 0 & C_{2k} & 0 & \dots & 0 & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & & & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 & \dots & * \\ \vdots & & & & & & & & & \vdots \end{pmatrix} \end{array}}_{CH_{kl}} = \underbrace{\begin{array}{cc} & \begin{array}{cccccccc} &&& l \\ &&& \downarrow &&&& \end{array} \\ \begin{array}{c} \\ \\ \\ k \rightarrow \\ \\ \\ \end{array} & \begin{pmatrix} 0 & 0 & \dots & 0 & \dots & * & \dots & * \\ \vdots & \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & & 0 & \dots & 0 & \dots & * \\ C_{l1} & C_{l2} & \dots & 1 & \dots & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & & & & & & \vdots \end{pmatrix} \end{array}}_{H_{kl}C}$$
sprich
$$C_{jk} = 0 \ \ \forall\ j < l < n + j - 1 \quad , \quad C_{lj} = 0 \ \ \forall\ k < j < n + k - i$$
für $k < l$. Somit ist $CZ_m(G) \in Z(G/Z_m(G))$ (also $C \in Z_{m+1}(G)$) äquivalent zu $C_{kl} = 0\ \forall\ k < l < n + k - m - 1$, das heißt $C \in G_{m+1}$.

Somit ist dann auch $Z_{m+1}(G) = G_{m+1}$.

(ii) Zu $\mathbb{K}_+ := \mathbb{K} \setminus \{0\}$ betrachte die Abbildung
$$f : \mathfrak{B}(n, \mathbb{K}) \rightarrow (\mathbb{K}_+, \cdot)^n \quad , \quad \begin{pmatrix} a_1 & * & \dots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ 0 & & & a_n \end{pmatrix} \overset{f}{\mapsto} \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix}$$
Offenbar ist f ein Epimorphismus, mit $\ker(f) = G$. Nach Holomorphiesatz ist dann $\mathfrak{B}(n, \mathbb{K})/G \cong (\mathbb{K}_+, \cdot)^n$, und da $(\mathbb{K}_+, \cdot)^n$ als abelsche Gruppe auflösbar ist, ist auch $\mathfrak{B}(n, \mathbb{K})/G$ auflösbar. Als nilpotente Gruppe (vgl. (i)) ist auch G auflösbar. Demnach muss auch $\mathfrak{B}(n, \mathbb{K})$ auflösbar sein.

□

Aufgabe 32

(i) O.B.d.A sei G nicht-abelsch (ansonsten siehe 5). Sei $x \in G$ mit <u>maximaler</u> Ordnung, dann muss $|\langle x \rangle| \in \{2, 4, 8\}$. Die Fälle $|\langle x \rangle| \in \{2, 8\}$ sind jedoch ausgeschlossen, da sonst G abelsch wäre, also $|\langle x \rangle| = 4$. Insbesondere ist $\langle x \rangle$ wegen $|G : \langle x \rangle| = 2$ ein Normalteiler in G. Wähle ein Element $y \in G \setminus \langle x \rangle$, dann ist:
$$G = \langle x \rangle \overset{+}{\cup} (\langle x \rangle\, y) = \left\langle 1, x, x^2, x^3, y, xy, x^2y, x^3y \right\rangle$$
(Vereinigung aller Restklassen). Außerdem muss $yxy^{-1} \in x^n$ sein für irgendein $n \in \{0, .., 3\}$. Der Fall $n = 0$ ist ausgeschlossen (da sonst $x = 1$), ebenso der Fall $n = 1$ (da sonst $xy = yx$ also G abelsch) und $n = 2$ (da sonst $yx^2y^{-2} = (yxy^{-1})^2 = x^4 = 1 \rightarrow x^2 = 1$). Demzufolge ist $yxy^{-1} = x^3$ also
$$yx = x^3y$$
das heißt jede Verknüpfungskette $x^{i_1}y^{j_1} \dots x^{i_n}y^{j_n}$ kann geschrieben werden als $x^k y^l$ und die Verknüpfungstabelle ist festgelegt (nach Festlegung der Ordnung von y).

Dabei existieren nach Lagrange 2 Möglichkeiten: $|\langle y\rangle| = 2$ (also $G \cong D_8$ in Übungsaufgabe 09) und $|\langle y\rangle| = 4$ (also $G \cong Q_8$ in Übungsaufgabe 25).

Alternative: Sei G eine Gruppe der Ordnung 8.

- Fall: G abelsch. Bekanntlich existieren genau 3 abelsche Gruppen der Ordnung 8, nämlich

$$\underbrace{\mathbb{Z}/8\mathbb{Z}}_{\text{zyklisch}}\ ,\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\ ,\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \tag{5}$$

- Alternative Fall. Sei $1 \neq x \in G$ mit maximaler Ordnung. Nach Lagrange $|\langle x\rangle| \in \{2,4\}$ (da G nicht zyklisch). Ist $|\langle x\rangle| = 2$, so müssen alle Elemente in G der Ordnung ≤ 2 sein, das heißt nach Aufgabe (6) G ist abelsch (erster Fall).

  Sei also $|\langle x\rangle| = 4$, dazu wählen $1 \neq y \notin \langle x\rangle$. Dann ist $\langle x\rangle < |\langle x,y\rangle|$ also nach Lagrange $\langle x,y\rangle = G$.

  - Fall: $\langle x\rangle \cap \langle y\rangle = \{1\}$, dann ist

$$\underbrace{|\langle x\rangle\langle y\rangle|}_{\leq 8} = \frac{|\langle x\rangle|\cdot|\langle y\rangle|}{|\langle x\rangle\cap\langle y\rangle|} = 4\cdot\underbrace{|\langle y\rangle|}_{\in\{2,4\}} \ \Rightarrow\ |\langle y\rangle| = 2 \ \Rightarrow\ \langle x\rangle\langle y\rangle = G$$

    Folglich
$$G = \left\{1, x, x^2, x^3, y, xy, x^2y, x^3y\right\}$$
    Wollen nun die Verknüpfungstabelle angeben. Beachte dass $yx \neq xy$ da sonst $\langle x\rangle, \langle y\rangle$ Normalteiler wären, was implizieren würde $G = \langle x\rangle \oplus \langle y\rangle \cong \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (1. Fall). Wegen $yx \notin \langle x\rangle, \langle y\rangle$ (da sonst $y \in \langle x\rangle$ oder $x \in \langle y\rangle$) (analog auch für xy) muss $yx \in \left\{x^2y, x^3y\right\}$ sein. Im ersten Fall wäre aber
$$\langle (yx)\rangle = \{1, yx, \underbrace{(yx)^2}_{x^3}, \underbrace{(yx)^3}_{y}, \underbrace{(yx)^4}_{x}, \dots\}$$
    ein Widerspruch zur maximalen Ordnung von x, also $yx = x^3y$. Folglich
$$yx^3y = \underbrace{y^2}_{1} x = x \underbrace{y^2}_{1} \ \Rightarrow\ yx^3 = xy$$
$$\Rightarrow\ yx^3 = xy = x^2x^3y = x^2yx \ \Rightarrow\ yx^2 = x^2y$$
    Mit diesen Regeln ergibt sich schnell die Verknüpfungstabelle (1).

	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x	x	x^2	x^3	1	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x^3	x^3	1	x	x^2	x^3y	y	xy	x^2y
y	y	x^3y	x^2y	xy	1	x^3	x^2	x
xy	xy	y	x^3y	x^2y	x	1	x^3	x^2
x^2y	x^2y	xy	y	x^3y	x^2	x	1	x^3
x^3y	x^3y	x^2y	xy	y	x^3	x^2	x	1

Table 1: Verknüpfungstabelle für $|G| = 8$ im 1. nicht-abelschen Fall.

  - Alternative Fall: $\langle x\rangle \cap \langle y\rangle \neq \{1\}$. Dann muss auch $|\langle y\rangle| > 2$ (also $|\langle y\rangle| = 4$) sein, denn sonst wäre $y \in \langle x\rangle$ (wegen $\langle y\rangle \cap \langle x\rangle \neq \{1\}$) ein Widerspruch zur Wahl von y!

    Nach Lagrange muss anderseits $|\langle x\rangle \cap \langle y\rangle| \in \{2,4\}$ sein, das heißt $|\langle x\rangle \cap \langle y\rangle| = 2$ (da sonst $\langle x\rangle = \langle y\rangle \ \rightsquigarrow\ y \in \langle x\rangle$). Wegen $y \neq x^k\ \forall\ k = 0,..,3$ (da sonst $y \in \langle x\rangle$), $y^2 \neq x$ (da sonst $x^2 = y^4 = 1$), $y^2 \neq x^3$ (da sonst $x^2 = y^4 = 1$), $y^3 \neq x$ (da sonst $y = y^9 = x^3 \in \langle x\rangle$), $y^3 \neq x^2$ (da sonst $y^2 = x^4 = 1$), $y^3 \neq x^3$ (da sonst $x^2 = x^6 = y^6 = y^2$ ein Widerspruch zu $|\langle x\rangle \cap \langle y\rangle| = 2$) muss $x^2 = y^2$:
$$\langle x\rangle \cap \langle y\rangle = \{1, \underbrace{x^2}_{y^2}\}$$

Da ferner $xy \neq yx$ (sonst $G = \langle x, y \rangle$ abelsch) und $xy \notin \langle x \rangle, \langle y \rangle$ (da sonst $y \in \langle x \rangle$ oder $x \in \langle y \rangle$) (analog auch für yx) ergibt sich

$$G = \langle 1, x, x^2, x^3, y, y^3, xy, yx \rangle$$

Wollen nun die Verknüpfungstabelle angeben. Wegen $xyx \neq 1$ (da sonst $yx = x^3 \to y = x^2$), $xyx \neq x$ (sonst $y = x^3$), $xyx \neq x^2$ (sonst $y = 1$), $xyx \neq x^3$ (sonst $y = x$), $xyx \neq y^3$ (sonst $yx = xy$), $xyx \neq xy$ (sonst $x = 1$), $xyx \neq yx$ (sonst $x = 1$) muss $xyx = y$ sein. Wegen $xy^3 \notin \{1, x, x^2, x^3, y, y^3, xy\}$ (da sonst $x^3 = y^3$ oder $y^3 = 1$ oder $y^3 = x$ oder $y^3 = x^2$ oder $1 = xy^2 = x^3$ oder $x = 1$ oder $x^3 = x$) muss $xy^3 = yx$ sein. Da x, y vollkommen *gleichberechtigt* sind, muss auch $yxy = x$ und $yx^3 = xy$.
Mit diesen Regeln ergibt sich schnell die Verknüpfungstabelle (2).

	1	x	x^2	x^3	y	y^3	xy	yx
1	1	x	x^2	x^3	y	y^3	xy	yx
x	x	x^2	x^3	1	xy	yx	y^3	y
x^2	x^2	x^3	1	x	y^3	y	yx	xy
x^3	x^3	1	x	x^2	yx	xy	y	y^3
y	y	yx	y^3	xy	x^2	1	x	x^3
y^3	y^3	xy	y	yx	1	x^2	x^3	x
xy	xy	y	yx	y^3	x^3	x	x^2	1
yx	yx	y^3	xy	y	x	x^3	1	x^2

Table 2: Verknüpfungstabelle für $|G| = 8$ im 2. nicht-abelschen Fall.

Beide Verknüpfungstabellen definieren tatsächlich eine Gruppe (jeweils D_8 und Q_8). Sie sind ferner nicht Isomorph, denn erstere hat 5 Elemente der Ordnung 2, letztere nur eins.

(ii) Sei G eine Gruppe der Ordnung 10.

- Der eine Fall ist $G = \langle x \rangle$ zyklisch, z.B. $G = \mathbb{Z}/10\mathbb{Z}$.
- Alternative Fall. Wählen $1 \neq x \in G$ mit maximaler Ordnung. Nach Lagrange muss $|\langle x \rangle| \in \{2, 5\}$.
  - Fall $|\langle x \rangle| = 2$, dann haben alle $y \in G$ Ordnung ≤ 2, das heißt nach Aufgabe (6) G ist abelsch. Für weiteres Element $1 \neq y \notin \langle x \rangle$ (also $\langle y \rangle \cap \langle x \rangle = \{1\}$) wäre dann $\langle x \rangle \langle y \rangle \leq G$, und weiterhin

    $$|\langle x \rangle \langle y \rangle| = \frac{|\langle x \rangle| \cdot |\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} = 4$$

    ein Widerspruch zu Lagrange! Demnach muss $|\langle x \rangle| = 5$ sein.
  - Sei also $|\langle x \rangle| = 5$, dazu $1 \neq y \notin \langle x \rangle$. Dann ist $\langle y \rangle \cap \langle x \rangle = \{1\}$, denn sonst müsse nach Lagrange (angewandt auf $\langle x \rangle$) $|\underbrace{\langle x \rangle \cap \langle y \rangle}_{\leq \langle x \rangle}| = 5 = \langle x \rangle$ sein, also $\langle x \rangle \overset{y \notin \langle x \rangle}{\subsetneq} \langle y \rangle$ ein Widerspruch zur Maximalität von $|\langle x \rangle|$. Demnach

    $$\underbrace{|\langle x \rangle \langle y \rangle|}_{\leq 10} = \frac{|\langle x \rangle| \cdot |\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} = 5 \cdot \underbrace{|\langle y \rangle|}_{\in \{2,5\}} \quad \Rightarrow \quad |\langle y \rangle| = 2$$

    und insbesondere $\langle x \rangle \langle y \rangle = G$, also

    $$G = \{1, x, x^2, x^3, x^4, y, xy, x^2y, x^3y, x^4y\}$$

    Da $\langle x \rangle \trianglelefteq G$ (da $|G : \langle x \rangle| = 2$) muss $yxy^{-1} = x^n$ sein für irgendein $n \in \{0, .., 4\}$. Insbesondere

    $$x = \underbrace{y^2}_{1} x \underbrace{y^{-2}}_{1} = yx^n y^{-1} = (\underbrace{yxy^{-1}}_{x^n})^n = x^{n^2}$$

    muss $n^2 = 1(\text{mod}5)$ sein, also $n = 4$. Demzufolge ist

    $$yx = x^4 y$$

das heißt jede beliebige Verknüpfung $x^{i_1}y^{j_1}\dots x^{i_n}y^{j_n}$ kann auf die Form $x^k y^l$ gebracht werden, und die Verknüpfungen der Gruppe sind eindeutig bestimmt.

- **Bemerke:** G ist nicht-abelsch, denn sonst wäre $G = \langle x\rangle \oplus \langle y\rangle \cong \mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}$ zyklisch.

Existenz: Zu $\langle x\rangle \cong \mathbb{Z}/5\mathbb{Z}$, $\langle y\rangle \cong \mathbb{Z}/2\mathbb{Z}$ und $\varphi : \langle y\rangle \to \mathrm{Aut}(\langle x\rangle)$, $y \mapsto (x \mapsto x^{-1})$ (beachte dass $(x \mapsto x^{-1}) \in \mathrm{Aut}(\langle x\rangle))$ ist

$$\langle x\rangle \rtimes_\varphi \langle y\rangle =: D_{10}$$

eine nicht-abelsche Gruppe der Ordnung 10. Bezeichnung: Diedergruppe der Ordnung 10.

Aufgabe 33

Sei $G = \langle x\rangle$ der Ordnung n und $d \mid n$, o.B.d.A $d > 1$ (der Fall $d = 1$ ist klar). Dann ist

$$|\underbrace{\langle x^{n/d}\rangle}_{\leq G}| = d$$

denn $(x^{n/d})^m = 1 \;\Leftrightarrow\; n \mid \frac{mn}{d} \;\Leftrightarrow\; \frac{m}{d} \in \mathbb{N} \;\Rightarrow\; m \geq d.$

Sei nun $m \in \{1, .., n\}$ so dass $|\langle x^m\rangle| = d$ (jede Untergruppe von G ist zyklisch also durch irgendein x^m erzeugt). Dann ist insbesondere $x^{md} = 1$ das heißt

$$n \mid md \;\Rightarrow\; \underbrace{\frac{md}{n}}_{\frac{m}{\frac{n}{d}}} \in \mathbb{N} \;\Rightarrow\; \frac{n}{d} \mid m \;\Rightarrow\; x^m \in \left\langle x^{n/d}\right\rangle \;\Rightarrow\; \langle x^m\rangle \subseteq \left\langle x^{n/d}\right\rangle$$

Da $|\langle x^m\rangle| = \left|\left\langle x^{n/d}\right\rangle\right|$ folgt $\langle x^m\rangle = \left\langle x^{n/d}\right\rangle$.
$\square$