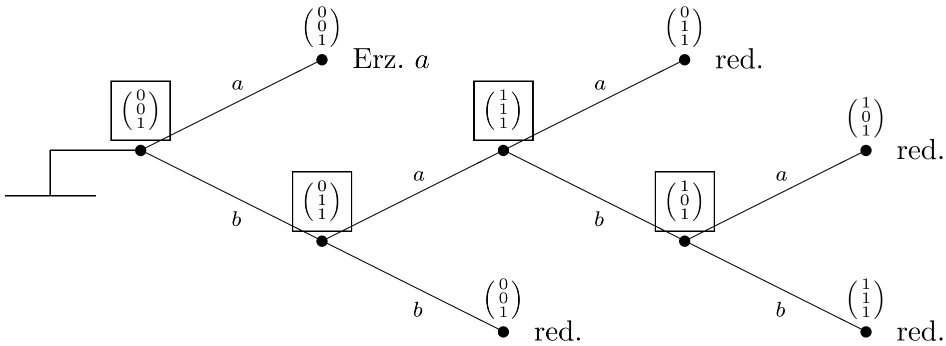
G. Nebe, M. Künzer 02.12.2004

Algebra I, WS 04/05

Lösung Probeklausur I

Aufgabe 1.

(1) Verwenden wir die treue Operation von G auf $\mathbf{F}_2^3$, und wählen wir z.B. $\begin{pmatrix}0\\0\\1\end{pmatrix}$ als erstes Element der base, so erhalten wir folgenden Baum.



Daraus ergeben sich folgende strong generators.

$$
\begin{aligned}
w_{\begin{pmatrix}0\\0\\1\end{pmatrix}}\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right) &= 1 &= \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\\
w_{\begin{pmatrix}0\\0\\1\end{pmatrix}}\left(\begin{pmatrix}0\\1\\1\end{pmatrix}\right) &= b &= \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\\
w_{\begin{pmatrix}0\\0\\1\end{pmatrix}}\left(\begin{pmatrix}1\\1\\1\end{pmatrix}\right) &= ab &= \begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}\\
w_{\begin{pmatrix}0\\0\\1\end{pmatrix}}\left(\begin{pmatrix}1\\0\\1\end{pmatrix}\right) &= bab &= \begin{pmatrix}1&1&1\\0&1&0\\0&0&1\end{pmatrix}
\end{aligned}
$$

Es ist $\mathrm{Stab}_G\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right) = \langle a\rangle$.

Wählen wir z.B. $\begin{pmatrix}0\\1\\0\end{pmatrix}$ als zweites Element der base, so ergeben sich direkt folgende strong generators.

$$
\begin{aligned}
w_{\begin{pmatrix}0\\1\\0\end{pmatrix}}\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right) &= 1 &= \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\\
w_{\begin{pmatrix}0\\1\\0\end{pmatrix}}\left(\begin{pmatrix}1\\1\\0\end{pmatrix}\right) &= a &= \begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}
\end{aligned}
$$

Es ist nun $\mathrm{Stab}_G\left(\begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}\right) = 1$.

(2) Es ist $\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}1\\0\\1\end{pmatrix}$. Somit ist $\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix} \in G$ genau dann, wenn $w_{\begin{pmatrix}0\\0\\1\end{pmatrix}}\left(\begin{pmatrix}1\\0\\1\end{pmatrix}\right)^{-1}\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix} = \begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix} \in \mathrm{Stab}_G\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right)$.

Falls man es an dieser Stelle noch nicht direkt erkennt, argumentiert man wie folgt. Es ist $\begin{pmatrix} 1&1&0\\0&1&0\\0&0&1 \end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}1\\1\\0\end{pmatrix}$. Somit ist $\begin{pmatrix} 1&1&0\\0&1&0\\0&0&1 \end{pmatrix} \in \mathrm{Stab}_G(\begin{pmatrix}0\\0\\1\end{pmatrix})$ genau dann, wenn $w_{\left(\begin{smallmatrix}0\\1\\0\end{smallmatrix}\right)}(\begin{pmatrix}1\\1\\0\end{pmatrix})^{-1}\begin{pmatrix} 1&1&0\\0&1&0\\0&0&1 \end{pmatrix} = \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1 \end{pmatrix} \in \mathrm{Stab}_G(\begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix})$.

Dies ist der Fall.

Setzen wir zusammen. Es ist

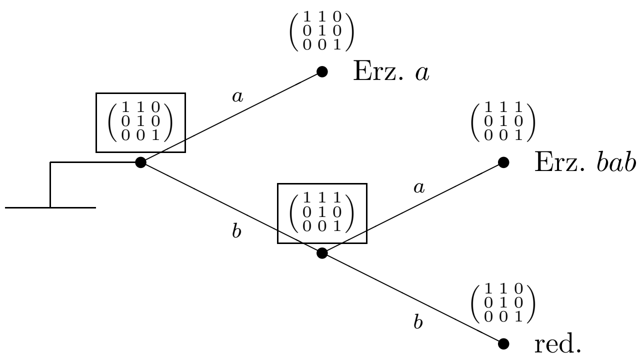
$$\begin{aligned} \begin{pmatrix} 1&0&1\\0&1&0\\0&0&1 \end{pmatrix} &= w_{\left(\begin{smallmatrix}0\\0\\1\end{smallmatrix}\right)}(\begin{pmatrix}1\\0\\1\end{pmatrix})\begin{pmatrix} 1&1&0\\0&1&0\\0&0&1 \end{pmatrix} \\ &= bab \cdot w_{\left(\begin{smallmatrix}0\\1\\0\end{smallmatrix}\right)}(\begin{pmatrix}1\\1\\0\end{pmatrix}) \\ &= baba\,. \end{aligned}$$

An dieser Stelle empfiehlt sich eine Probe.

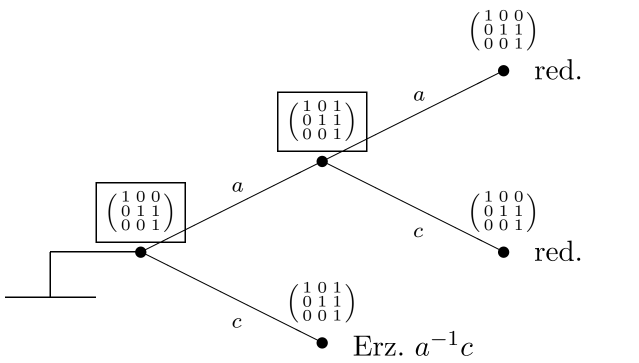
(3) Hier gibt es einen theoretischen und einen rechnerischen Lösungsweg.

Theoretisch. Wegen $ab \neq ba$ ist G nicht abelsch. Also ist $|\mathrm{Z}(G)| \neq 8$. Ferner ist daher auch $|\mathrm{Z}(G)| \neq 4$, da sonst $G/\mathrm{Z}(G)$ zyklisch und wiederum G abelsch wäre. Schließlich ist $|\mathrm{Z}(G)| \neq 1$, da G eine 2-Gruppe ist. Bleibt nur die Möglichkeit $|\mathrm{Z}(G)| = 2$.

Rechnerisch. Wir wenden den Bahnenalgorithmus auf die Operation von G auf sich via Konjugation an und bestimmen den Stabilisator $\mathrm{Stab}_G(a, b)$. Das liefert zunächst den folgenden Baum.



Mit $c := bab = \begin{pmatrix} 1&1&1\\0&1&0\\0&0&1 \end{pmatrix}$ wird also $\mathrm{Stab}_G(a) = \langle a, c\rangle$. Damit erhalten wir folgenden Baum.



Somit wird $\mathrm{Z}(G) = \mathrm{Stab}_G(a, b) = \langle ac\rangle = \langle\begin{pmatrix} 1&0&1\\0&1&0\\0&0&1 \end{pmatrix}\rangle$, und also $|\mathrm{Z}(G)| = 2$.

Die Rechnung liefert nun etwas genauer als die Theorie auch die Elemente von $\mathrm{Z}(G)$ – die Mühe war also nicht ganz umsonst.

Aufgabe 2.

Um die Anzahl der Bahnen zu bestimmen, bestimmen wir für je einen Vertreter σ der Konjugiertenklassen die Anzahl der Fixpunkte auf A, d.h. die Kardinalität von $\mathrm{Fix}_A(\sigma) = \{f \in A \ :\ \sigma\}$. Es ergibt sich unter Berücksichtigung von Einerzykeln folgende Tabelle.

σ	$\lvert\,\mathrm{Fix}_A(\sigma)\rvert$	$\lvert\,{}^{\mathcal{S}_5}\sigma\rvert$
$(1,2,3,4,5)$	4^1	24
$(1,2,3,4)(4)$	4^2	30
$(1,2,3)(3,4)$	4^2	20
$(1,2,3)(3)(4)$	4^3	20
$(1,2)(3,4)(5)$	4^3	15
$(1,2)(3)(4)(5)$	4^4	10
$(1)(2)(3)(4)(5)$	4^5	1

Mit Burnside erhalten wir

$$\frac{1}{5!}\left(24\cdot 4^1 + 30\cdot 4^2 + 20\cdot 4^2 + 20\cdot 4^3 + 15\cdot 4^3 + 10\cdot 4^4 + 1\cdot 4^5\right) \ \ (= \ \ 56)$$

Bahnen von $\mathcal{S}_5$ auf A.

Aufgabe 3.

Es genügt zu zeigen, daß G/G' unendlich ist, da eine endliche Gruppe keinen unendlichen Quotienten haben kann.

Für G/G' berechnen wir die Elementarteilerform der Matrix $\left(\begin{smallmatrix} 2 & 1 & 1 \\ -2 & 5 & 1 \\ -2 & -1 & -1 \end{smallmatrix}\right)$ zu $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$. Also ist $G/G' \simeq C_4 \times \mathbf{Z}$, und somit keine endliche Gruppe.

Aufgabe 4.

(1) Wir behaupten, daß G keine Untergruppe von Index 4 enthält. Wäre $U \le G$ von Index 4, so gäbe es in G einen Normalteiler N, welcher zum einen in U enthalten ist, und welcher zum anderen einen Index in G hat, welcher $4! = 24$ teilt (cf. 18 (2)). Also wäre $4 \le [G:N] \le 24$, und N insbesondere $N \not\in \{1, G\}$. Da G einfach ist, ist dies nicht möglich.

(2) Es ist $\lvert\,\mathrm{Syl}_5(G)\rvert \in \{6, 36\}$, da diese Anzahl ein Teiler von 72 und $\equiv_5 1$ sein sollte, sowie ungleich 1 sein muß wegen G einfach. Wäre $\lvert\,\mathrm{Syl}_5(G)\rvert = 36$, so gäbe es in G genau $36 \cdot 4 = 144$ Elemente der Ordnung 5, im Widerspruch zur Voraussetzung.

Damit gibt es einen nichttrivialen Gruppenmorphismus $G \longrightarrow \mathcal{S}_{\mathrm{Syl}_5(G)} \simeq \mathcal{S}_6$. Dessen Kern kann nicht gleich G sein, und muß somit gleich 1 sein wegen G einfach. Also ist er injektiv, und G isomorph zu seinem Bild, welches eine Untergruppe von $\mathcal{S}_6$ darstellt, wie behauptet.

(3) Sei $U \le \mathcal{S}_6$ die in (2) gefundene Untergruppe isomorph zu G. Wäre $U \not\le \mathcal{A}_6$, so wäre $U \xrightarrow{\mathrm{sgn}} \{-1, +1\}$ surjektiv, hätte also einen Kern von Ordnung 180, im Widerspruch zur Einfachheit von U. Also ist $U \le \mathcal{A}_6$. Wegen $|U| = |\mathcal{A}_6|$ ist insgesamt $G \simeq U = \mathcal{A}_6$.

Aufgabe 5.

Sei $C_2 \times C_2 = \langle x, y \mid x^2, y^2, [x,y]\rangle$ geschrieben. Ein Endomorphismus von $C_2 \times C_2$ schickt $x \longmapsto x^a y^c$ und $y \longmapsto x^b y^d$ für gewisse $a, b, c, d \in \mathbf{F}_2$. Weisen wir einem solchen Endomorphismus die Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ zu, so entspricht die Komposition der Matrixmultiplikation. Invertierbare Endomorphismen, i.e. Automorphismen, entsprechen also invertierbaren Matrizen. So erhalten wir einen Isomorphismus $\mathrm{Aut}(C_2 \times C_2) \xrightarrow{\sim} \mathrm{GL}_2(\mathbf{F}_2)$.

Es ist z.B. $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_2)$ ein Element der Ordnung 3, wie man entweder durch Ausprobieren, oder aber als Begleitmatrix des Polynoms $X^2 + X + 1 \in \mathbf{F}_2[X]$, einem Teiler von $X^3 - 1$, findet.

Dies liefert den Automorphismus

$$\begin{array}{rcl} C_2 \times C_2 & \xrightarrow{\sim} & C_2 \times C_2 \\ x & \longmapsto & y \\ y & \longmapsto & xy \end{array}$$

von Ordnung 3.

Aufgabe 6.

Sei G eine Gruppe von Ordnung $|G| = 55$. Es ist $|\operatorname{Syl}_{11}(G)| = 1$. Sei N die normale 11-Sylowgruppe, und sei U eine 5-Sylowgruppe. Es ist $N \cap U = 1$ und $|N||U| = 11 \cdot 5 = 55$, und somit $G \simeq N \rtimes U$.

Da N und U abelsch sind, ist dieses semidirekte Produkt ist genau dann abelsch, wenn es sich um ein direktes Produkt handelt.

Nehmen wir nun für U eine zyklische Gruppe von Ordnung 5, erzeugt von u, und für N eine zyklische Gruppe der Ordnung 11, erzeugt von n. Es bleibt zu klären, wieviele paarweise nichtisomorphe Gruppen der Form $N \rtimes U$ man ausgehend von einem nichttrivialen Morphismus

$$(*) \qquad U \longrightarrow \operatorname{Aut} N$$

erhält. Ein solcher ist gegeben durch ein Bild von u in $\operatorname{Aut} N$, welches Ordnung 5 besitzt (und nicht Ordnung 1).

Ein Automorphismus von N ist gegeben durch $n \longmapsto n^a$ mit $a \in (\mathbf{Z}/11\mathbf{Z}) \smallsetminus \{0\}$. Für $a = 2$ erhält man wegen $2^2 \not\equiv_{11} 1$ und $2^5 \not\equiv_{11} 1$ einen Automorphismus der Ordnung 10. Damit erhält man für $a \in \{2^1, 2^3, 2^{-1}, 2^{-3}\}$ sämtliche Elemente der Ordnung 10 in $\operatorname{Aut} N$, und folglich für $a \in \{2^2, 2^6, 2^{-2}, 2^{-6}\} = \{4, -2, 3, 5\}$ sämtliche Elemente der Ordnung 5 in $\operatorname{Aut} N$. Schreiben wir die aus letzteren hervorgehenden Gruppen der Form $N \rtimes U$ einmal G_4, G_{-2}, G_3 resp. G_5.

Mit G_{-2} haben wir eine nichtabelsche Gruppe von Ordnung 55 konstruiert.

Wenn wir $u' = u^2$ setzen in G_{-2}, so erzeugt auch u' die Untergruppe U, und es kommt u' unter $(*)$ auf $n \longmapsto n^{(-2)^2} = n^4$. Also ist $G_4 \xrightarrow{\sim} G_{-2}$ via $n \longmapsto n$, $u \longmapsto u'$.

Wenn wir $u' = u^3$ setzen in G_{-2}, so erzeugt auch u' die Untergruppe U, und es kommt u' unter $(*)$ auf $n \longmapsto n^{(-2)^3} = n^3$. Also ist $G_3 \xrightarrow{\sim} G_{-2}$ via $n \longmapsto n$, $u \longmapsto u'$.

Wenn wir $u' = u^4$ setzen in G_{-2}, so erzeugt auch u' die Untergruppe U, und es kommt u' unter $(*)$ auf $n \longmapsto n^{(-2)^4} = n^5$. Also ist $G_5 \xrightarrow{\sim} G_{-2}$ via $n \longmapsto n$, $u \longmapsto u'$.

Somit repräsentiert G_{-2} den einzigen Isomorphietyp nichtabelscher Gruppen der Ordnung 55.

Bemerkung. Man unterscheide die beiden Schritte. Im ersten Schritt wurde untersucht, wie eine nichtabelsche Gruppe von Ordnung 55 aussehen *muß* – sie muß von der Form $C_{11} \rtimes C_5$ sein. Im zweiten Schritt wurden *alle* solche Gruppen *konstruiert* und ihr Verhältnis zueinander untersucht.

Aufgabe 7.

(1) Es ist

$$\begin{array}{rcl} R/(5) & \simeq & \mathbf{Z}[X]/(X^3 - 2, 5) \\ & \simeq & \mathbf{F}_5[X]/(X^3 - 2) \\ & = & \mathbf{F}_5[X]/((X+2)(X^2 - 2X - 1)) \\ & \simeq & \mathbf{F}_5[X]/(X+2) \times \mathbf{F}_5[X]/(X^2 - 2X - 1) \end{array}$$

nach dem Chinesischen Restsatz. Da sowohl $X + 2$ als auch $X^2 - 2X - 1$ in $\mathbf{F}_5[X]$ irreduzibel sind, ist R in ein ringdirektes Produkt von Körpern zerlegt.

(2) Es ist

$$\begin{aligned} R/(3) &\simeq \mathbf{Z}[X]/(X^3-2,3) \\ &\simeq \mathbf{F}_3[X]/(X^3-2) \\ &= \mathbf{F}_3[X]/((X+1)^3)\ . \end{aligned}$$

Letzterer Ring enthält als nichtverschwindendes nilpotentes Element z.B. die Restklasse von $X+1$. Verfolgt man die Isomorphismen zurück, so erkennt man, daß die Restklasse von $X+1$ auch in $R/(3)$ nilpotent und ungleich Null ist.

Aufgabe 8.

(1) Die Aussage ist falsch. Zum Beispiel enthält $C_2 \times C_2 = \langle a, b \mid a^2,\, b^2,\, [a,b]\rangle$ für $p = 2$ die Untergruppen $\langle a\rangle$, $\langle b\rangle$ und $\langle ab\rangle$ von Ordnung 2, welche in verschiedenen Bahnen unter der Konjugationsoperation liegen, da in abelschen Gruppen diese Bahnen samt und sonders Länge 1 haben.

(2) Die Aussage ist richtig. Ist $\alpha \in \operatorname{Aut} G$, so ist wegen $|\alpha(P)| = |P|$ auch $\alpha(P)$ eine p-Sylowgruppe von G. Da P aber die einzige P-Sylowgruppe von G ist, folgt $\alpha(P) = P$.

(3) Die Aussage ist richtig. Bezeichne $G \xrightarrow{\varphi} G/G'$, $g \longmapsto gG'$ die Restklassenabbildung. Es ist $U/G' \leq G/G'$. Da G/G' abelsch ist, ist sogar $U/G' \trianglelefteq G/G'$. Daher ist auch $U = \varphi^{-1}(U/G') \trianglelefteq G$ als Urbild eines Normalteilers unter einem Gruppenmorphismus selbst ein Normalteiler.