Einführung in die Algebra
Blatt 4

Jendrik Stelzner

13. November 2013

Aufgabe 4.1.

Aufgabe 4.2.

(i)

Es ist nach Definition

$$\operatorname{ord}\pi = \min\{n \in \mathbb{N}, n \geq 1 : \pi^n = \mathrm{id}\}. \tag{1}$$

Die x_i paarweise verschieden, und $\pi(x_i) = x_{i+1}$ für $i = 1, \dots, r-1$ und $\pi(x_r) = x_1$. Daher ist für $n = 1, \dots, r-1$

$$\pi^n(x_1) = x_{1+n} \neq x_1,$$

also $\pi^n \neq \mathrm{id}$. Da allerdings für $i = 1, \dots, n$

$$\pi^r(x_i) = x_i$$

ist $\operatorname{ord}\pi = r$ nach (1). Analog ergibt sich, dass $\operatorname{ord}\tau = s$.
Da π und τ fremd sind, kommutieren sie miteinander (aus der Vorlesung bekannt). Es kommutieren daher π^n und τ^m ist daher für alle $n, m \in \mathbb{N}$, da

$$\begin{aligned}\pi^n\tau^m &= \prod_{i=1}^{n} \pi \cdot \prod_{i=1}^{m} \tau = \tau \cdot \prod_{i=1}^{n} \pi \cdot \prod_{i=1}^{m-1} \tau = \tau^2 \cdot \prod_{i=1}^{n} \pi \cdot \prod_{i=1}^{m-2} \tau \\ &= \ldots = \prod_{i=1}^{m-1} \tau \cdot \prod_{i=1}^{n} \pi \cdot \tau = \prod_{i=1}^{m} \tau \cdot \prod_{i=1}^{n} \pi = \tau^m\pi^n.\end{aligned}$$

Auch folgt aus der Fremdheit von π und τ, dass $\langle\pi\rangle \cap \langle\tau\rangle = 1$, wobei 1 die triviale Gruppe bezeichnet: Für $\sigma \in \langle\pi\rangle \cap \langle\tau\rangle$ ist $\pi^n = \sigma = \tau^m$ für passende $n, m \in \mathbb{N}$ mit $0 \leq n \leq r-1$ und $0 \leq m \leq s-1$. Es ist dann für $i = 1, \dots, r$

$$x_i = \pi^r(x_i) = \pi^{r-n}(\pi^n(x_i)) = \pi^{r-n}(\tau^m(x_i)) = \pi^{r-n}(x_i),$$

weshalb $r-n$ ein Teiler von r sein muss; wegen $r - n \leq r$ muss also $r - n = r$ und daher $n = 0$ und $\sigma = \pi^n = \mathrm{id}$.
Für alle $t \in \mathbb{N}, t \geq 1$ mit $(\pi\tau)^t = \mathrm{id}$ ist

$$\pi^t\tau^t = (\pi\tau)^t = \mathrm{id},$$

also $\pi^t = (\tau^t)^{-1} = \tau^{s-t} \in \langle\tau\rangle$. Wie oben bemerkt ist daher $\pi^t = \mathrm{id}$, also t ein Vielfaches von $\operatorname{ord}\pi = r$. Analog ergibt sich, dass t auch ein Vielfaches von $\operatorname{ord}\tau = s$ ist. Also ist $t \geq \mathrm{kgV}(r, s)$. Andererseits ist

$$(\pi\tau)^{\mathrm{kgV}(r,s)} = \pi^{\mathrm{kgV}(r,s)}\tau^{\mathrm{kgV}(r,s)} = \mathrm{id}^2 = \mathrm{id}\,.$$

Also ist $\operatorname{ord}\pi\tau = \mathrm{kgV}(r, s)$.

(ii)

Es ist

$$\begin{aligned}\sigma := &\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11\\ 4 & 1 & 10 & 11 & 8 & 9 & 7 & 2 & 3 & 6 & 5\end{pmatrix}\\ = &\underbrace{\begin{pmatrix}1 & 4 & 11 & 5 & 8 & 2\end{pmatrix}}_{=:\pi}\underbrace{\begin{pmatrix}3 & 10 & 6 & 9\end{pmatrix}}_{=:\tau}.\end{aligned}$$

Nach Aufgabenteil (i) ist $\operatorname{ord}\pi = 6$ und $\operatorname{ord}\tau = 4$. Da π und τ fremde Zykeln sind ist daher

$$\begin{aligned}\sigma^{2013} &= (\pi\tau)^{2013} = \pi^{2013}\,\tau^{2013} = \pi^3\tau\\ &= \begin{pmatrix}1 & 4 & 11 & 5 & 8 & 2\end{pmatrix}^3\begin{pmatrix}3 & 10 & 6 & 9\end{pmatrix}\\ &= \begin{pmatrix}1 & 5\end{pmatrix}\begin{pmatrix}2 & 11\end{pmatrix}\begin{pmatrix}4 & 8\end{pmatrix}\begin{pmatrix}3 & 10 & 6 & 9\end{pmatrix}\\ &= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11\\ 5 & 11 & 10 & 8 & 1 & 9 & 7 & 4 & 3 & 6 & 2\end{pmatrix}.\end{aligned}$$

Aufgabe 4.3.

Aufgabe 4.4.

Sei $n \in \mathbb{N}$ beliebig aber fest. Da $[G, G]$ eine Untergruppe von G ist, ist $1 \in [G, G]$, also $1 \in G_n$, da $1^n = 1 \in [G, G]$. Für alle $g \in G_n$ ist wegen $g^n \in [G, G]$ auch $(g^{-1})^n = (g^n)^{-1} \in [G, G]$, also $g^{-1} \in G_n$. Dass für $g, h \in G_n$ auch $gh \in G_n$ ergibt sich mithilfe der folgenden Bemerkung.

Bemerkung 1. Sei G eine Gruppe und seien $g, h \in G$. Dann ist für alle $n \in \mathbb{N}$

$$(gh)^n = g^n h^n c \text{ mit } c \in [G, G].$$

Beweis. Der Beweis verläuft per Induktion über n.

Induktionsanfang. Sei $n = 0$. Dann ist

$$(gh)^n = (gh)^0 = 1 = 1 \cdot 1 \cdot 1 = g^0 g^0 \cdot 1 = g^n h^n \cdot 1.$$

Induktionsschritt. Sei $n \geq 1$ und gelte die Aussage für $n - 1$. Nach Induktionsvoraussetzung gibt es ein $c \in [G, G]$ mit $(gh)^{n-1} = g^{n-1}h^{n-1}c$. Es ist daher

$$\begin{aligned}(gh)^n &= gh(gh)^{n-1} = ghg^{n-1}h^{n-1}c\\ &= g^n h\left[h^{-1}, g^{1-n}\right]h^{n-1}c = g^n h^n\left[h^{-1}, g^{1-n}\right]\left[\left[h^{-1}, g^{1-n}\right]^{-1}, h^{1-n}\right]c.\end{aligned}$$

Da $[G, G]$ eine Untergruppe von G ist, ist

$$\left[h^{-1}, g^{1-n}\right]\left[\left[h^{-1}, g^{1-n}\right]^{-1}, h^{1-n}\right]c \in [G, G].$$

□

Da $[G, G]$ ein Untergruppe von G ist, und $g^n, h^n \in [G, G]$, ist mit $c \in [G, G]$ mit $(gh)^n = g^n h^n c$ auch $(gh)^n = g^n h^n c \in [G, G]$.
Es gilt noch zu zeigen, dass G_n normal in G ist, dass also für $g \in G_n$ und $h \in G$ auch $hgh^{-1} \in G_n$. Da $g^n \in [G, G]$ und $[G, G]$ normal in G ist, gilt

$$(hgh^{-1})^n = h(g^n)h^{-1} \in [G, G],$$

also auch $hgh^{-1} \in G_n$.

Aufgabe 4.5.

Da $\operatorname{ord}[G, G] = 2$ ist $[G, G] = \{1, \sigma\}$ für ein selbstinverses $\sigma \in G$. G ist nicht abelsch, denn sonst wäre $[G, G] = 1$. G ist insbesondere nichttrivial.
Für alle $g \in G$ ist $g^2 \in Z$, wobei Z das Zentrum von G bezeichnet: Es ist für alle $h \in G$

$$\begin{aligned} g^2 h &= ghg\left[g^{-1}, h^{-1}\right] = hg\left[g^{-1}, h^{-1}\right] g \left[g^{-1}, h^{-1}\right] \\ &= hg\left[g^{-1}, h^{-1}\right]\left[h^{-1}, g\right] g, \end{aligned} \tag{2}$$

da

$$g\left[g^{-1}, h^{-1}\right] = gg^{-1}h^{-1}gh = h^{-1}gh = h^{-1}ghg^{-1}g = \left[h^{-1}, g\right] g.$$

Es ist nun

$$\left[g^{-1}, h^{-1}\right] = 1 \Leftrightarrow g^{-1} \in Z_{\{h^{-1}\}} \Leftrightarrow g \in Z_{\{h^{-1}\}} \Leftrightarrow \left[h^{-1}, g\right] = 1,$$

da $Z_{\{h^{-1}\}}$ eine Untergruppe von G ist. Da $\operatorname{ord}[G, G] = 2$ und $\left[g^{-1}, h^{-1}\right], \left[g, h^{-1}\right] \in [G, G]$ folgt daraus, dass $\left[g^{-1}, h^{-1}\right] = \left[g, h^{-1}\right]$, und da jedes Element in $[G, G]$ selbstinvers ist, auch $\left[g^{-1}, h^{-1}\right]\left[g, h^{-1}\right] = 1$. Aus (2) folgt daher, dass $g^2 h = hg^2$. Aus der Beliebigkeit von h folgt damit $g^2 \in Z$.
Da $Z = \operatorname{Ker} \operatorname{inn}$ folgt daraus, dass $\operatorname{inn}_g^2 = \operatorname{inn}_{g^2} = \operatorname{id}$ für alle $g \in G$, dass also alle $\varphi \in \operatorname{Inn}(G)$ selbstinvers sind. Dies hat zwei wichtige Konsequenzen: Zum einen folgt aus der folgenden Bemerkung, dass $\operatorname{ord} \operatorname{Inn}(G)$ gerade ist.

Bemerkung 2. Sei G eine nichttriviale Gruppe, so dass alle $g \in G$ selbstinvers sind. Dann ist $\operatorname{ord} G$ gerade.

Beweis. Da G nichttrivial ist, gibt es ein $g \in G - 1$. Da $g \neq 1$ selbstinvers ist, ist $\operatorname{ord} g = 2$. Da $\operatorname{ord} g$ ein Teiler von $\operatorname{ord} G$ ist, ist $\operatorname{ord} G$ gerade. □

Dass $\operatorname{Inn}(G)$ nichttrival ist, ergibt sich daraus, dass $\operatorname{Inn}(G) \cong G/Z$. Wäre $\operatorname{Inn}(G)$ trivial, so wäre $G = Z$, also G abelsch.
Zum anderen folgt, da jedes $\varphi \in \operatorname{Inn}(G)$ selbstinvers ist, dass $\operatorname{Inn}(G) \cong G/Z$ abelsch ist. Wegen der entsprechenden Minimalitätseigenschaft von $[G, G]$ folgt daraus, dass $[G, G] \subseteq Z$ eine Untergruppe ist. Da $[G, G]$ normal in G ist, ist $[G, G]$ auch normal Z. (Dies folgt auch aus der Kommutativität von Z.)
Aus dem zweiten Isomorphiesatz folgt nun, dass

$$G/Z \cong (G/[G, G])/(Z/[G, G]).$$

Insbesondere ist

$$\operatorname{ord} G/Z = \frac{\operatorname{ord} G/[G, G]}{\operatorname{ord} Z/[G, G]}.$$

Da $\operatorname{ord} G/Z = \operatorname{ord} \operatorname{Inn}(G)$ gerade ist, ist also auch $(G : [G, G]) = \operatorname{ord} G/[G, G]$ gerade.