Zadanie 29

Udowodnię przez indukcję, że $a_1a_2a_3\dots a_na_1^{-1}a_2^{-1}a_3{}^{-1}1\dots a_n^{-1}cdc^{-1}d^{-1} = b_1b_2\dots b_mb_1^{-1}b_2^{-1}\dots b_m^{-1}$.

Dla $n = 0$ nie ma co dowodzić, dla większego n: jeżeli jest ono nieparzyste, to dopisujemy $a_{n+1} = 1$, uzyskując n parzyste, który to przypadek dowodzimy, kładąc:

$$\begin{aligned} b_1 &= d^{-1} \\ b_{k+1} &= da_kc && \text{dla } k \text{ nieparzystego, } 1 \leqslant k \leqslant n \\ b_{k+1} &= c^{-1}a_k^{-1}d^{-1} && \text{dla } k \text{ parzystego, } 1 \leqslant k \leqslant n \\ b_{n+2} &= dcd^{-1} \end{aligned}$$

Uzyskujemy wtedy, że iloczyn $b_1b_2\dots b_{n+2}b_1^{-1}b_2^{-1}\dots b_{n+2}^{-1}$ jest równy

$$d^{-1}\cdot da_1c\cdot c^{-1}a_2d^{-1}\cdot da_3c\cdots c^{-1}a_nd^{-1}\cdot dcd^{-1}\cdot d\cdot c^{-1}a_1^{-1}d^{-1}\cdot da_2^{-1}c\cdots c^{-1}a_{n-1}^{-1}d^{-1}\cdot da_n^{-1}c\cdot dc^{-1}d^{-1}$$

co upraszcza się łatwo do $a_1a_2\dots a_na_1^{-1}\dots a_n^{-1}cdc^{-1}d^{-1}$.

Zadanie 41

Fakt, że $H \trianglelefteq K$ jest oczywisty: skoro sprzęganie przez elementy G zachowuje H, to sprzęganie przez elementy K tym bardziej.

Zdefiniujmy przekształcenie zbiorów: $\phi : G/H \to G/K$ jako $\phi(gH) = gK$. Jest to dobrze zdefiniowane, gdyż jeżeli $gH = \hat{g}H$, to znaczy, że $g^{-1}\hat{g} \in H \leqslant K$, zatem także $gK = \hat{g}K$. Zauważmy teraz, że jeżeli $\hat{g}H$ oraz gH leżą w tej samej warstwie $(G/H)/(K/H)$, tj. $\hat{g}H = gH\cdot kH = gk\cdot H$ (z normaności $H \trianglelefteq K$), to $\phi(\hat{g}H) = gkK = gK = \phi(\hat{g})$, zatem ϕ na każdej warstwie $(G/H)/(K/H)$ jest stałe, zatem ma sens morfizm zbiorów $\xi : (G/H)/(K/H) \to G/K$ indukowany przez ϕ.

Mamy, że $\xi(gH(K/H)) = gK$. Oczywiście jest to epimorfizm w Set, dla każdego gK mamy $\xi(gH(K/H)) = gK$. Jeżeli ponadto $\xi(gH(K/H)) = \xi(\hat{g}H(K/H))$, to $gK = \hat{g}K$, zatem $\hat{g} = gk$ dla pewnego $k \in K$. Teraz widzimy, $hatgH)(K/H) = ((gH)(kH))(K/H) = ((gH)(K/H))((kH)(K/H))$. Jednakże $kH \in K/H$, zatem $(\hat{g}H)(K/H) = (gH)(K/H)$, stąd ξ jest monomorfizmem w Set.

Z własności kategorii Set wnioskujemy, że ξ jest izomorfizmem zbiorów.

Załóżmy teraz $K/H \trianglelefteq G/H$. Mamy wtedy, że istnieje morfizm $\sigma : G/H \to Z$ w pewne $Z \in \mathrm{Ob}(\mathrm{Grp})$, że $\ker\sigma = K/H$. Niech $\pi : G \to G/H$ będzie kanoniczną injekcją. Wtedy $\ker(\sigma\circ\pi) = K$, gdyż $\pi^{-1}(K/H) = K$, a $\ker\pi = H \trianglelefteq K$. Zatem $K \trianglelefteq G$.

Teraz jednak widzimy, że oczywiście $\phi(1H) = 1K$ oraz $\phi(aH)\cdot\phi(bH) = aK\cdot bK = (a\cdot b)K = \phi((a\cdot b)H) = \phi(aH\cdot bH)$, zatem ϕ jest także morfizmem, gdy G/H i G/K potraktujemy w Grp. Dowód epimorficzności pozostaje bez zmian, dowód monomorficzności ξ staje się natychmiastowo dowodem, że $K/H = \ker\phi$, zatem $(G/H)/(K/H) \simeq G/K$.

Zadanie 42

Część a

Rozpatrzmy

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in GL(5) \right\}$$

z operacją mnożenia macierzy. Łatwo widać, że jest to grupa, $I \in G$, iloczyn dwóch macierzy z G też jest tej postaci, oraz macierz odwrotna do macierzy z G należy do G. Jest to więc grupa rzędu 125. Ponadto

$$\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$$
$$\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$$

Zatem jest to grupa nieabelowa.

Jednakże dla $A = \begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}$ mamy wymnażając: $A^2 = \begin{pmatrix}1&2a&ac+2b\\0&1&2c\\0&0&1\end{pmatrix}$, skąd dalej mamy, że $A^4 = \begin{pmatrix}1&4a&ac+4b\\0&1&4c\\0&0&1\end{pmatrix}$, skąd $A^5 = I$, zatem każdy element jest rzędu 5.

Teraz wskażmy drugą grupę. Na potrzeby tego opisu przyjmę, że $\mathbb{Z}_k$ będzie miało notację addytywną. Określmy $\phi : \mathbb{Z}_5 \to \mathrm{Aut}(\mathbb{Z}_{25})$ jako $\phi(a)(b) = (1+5a)b$. Oczywiście $b \mapsto (1+5a)b$ jest automorfizmem, gdyż $0 \mapsto (1+5a)9 = 0$, $b+c \mapsto (1+5a)b + (1+5a)c$. Tak samo widać, że ϕ jest homomorfizmem, gdyż $\phi(0)(b) = (1+5\cdot 0)b$, zatem $\phi(0) = \mathrm{id}$, zaś $(\phi(a)\circ\phi(\hat{a}))(b) = (1+5a)(1+5\hat{a})b = (1+5a+5\hat{a}+25a\hat{a})b = (1+5(a+\hat{a}))b = \phi(a+\hat{a})(b)$. Zatem ma sens rozważanie $H = \mathbb{Z}_{25} \rtimes_\phi \mathbb{Z}_5$. Jest to oczywiście grupa o rzędzie 125, przy czym $(1,0)\cdot(0,1) = (1+(1+5\cdot 0)\cdot 0, 0+1) = (1,1)$, zaś $(0,1)\cdot(1,0) = (0+(1+5\cdot 1)\cdot 1, 1) = (6,1)$, więc jest to grupa nieabelowa. Ponadto $(1,1)\cdot(1,1) = (1+(1+5\cdot 1)\cdot 1, 1+1) = (7,2)$, $(7,2)\cdot(7,2) = (7+(1+5\cdot 2)\cdot 7, 2+2) = (9,4)$, $(9,4)\cdot(1,1) = (9+(1+5\cdot 4)\cdot 1, 4+1) = (5,0)$, zatem $5\cdot(1,1) \neq (0,0)$, czyli $(1,1)$ jest rzędu większego niż 5, zatem $G \not\simeq H$.

Część b

Wstępne rozważania

Niech K będzie grupą nieabelową rzędu 125. Mamy możliwości: $|Z(K)| \in \{1,5,25,125\}$. Jednak $Z(K)$ jest nietrywialne, gdyż K jest p-grupą. Oczywiście $K \neq Z(K)$, bo K jest nieabelowa. Ponadto gdyby $|Z(K)| = 25$, to $|K/K(Z)| = 5$, zatem $K/K(Z)$ byłoby cykliczne, a jak dowodziliśmy, implikowałoby to, że K byłaby abelowa. Zatem $Z(K) \simeq \mathbb{Z}_5$.

Jednak $|K/Z(K)| = 25$. Jednakże wszystkie grupy rzędu 25 są abelowe (W – nieabelowa rzędu 25 ma oczywiście $Z(W) \neq 1, W$, lecz to daje $|Z(W)| = 5$, czyli $|W/Z(W)| = 5$, czyli $W/Z(W)$ jest cykliczna, zatem W jest abelowa wbrew założeniu). Jeżeli w $K/Z(K)$ istniałby element rzędu 25, to byłaby to grupa cykliczna, więc k byłaby abelowa. Zatem $K/Z(K)$ ma wszystkie nietrywialne elementy rzędu 5. biorąc $x \in K$, $x \notin Z(K)$, a następnie $y \in K$, $yZ(K) \notin \langle xZ(K)\rangle$, łatwo widzimy, że $K/Z(K) = \langle xZ(K), yZ(K)\rangle$.

Mamy teraz, że $[K,K] \subseteq Z(K)$, gdyż biorąc kanoniczne $\pi : K \to K/Z(K)$ widzimy, że $\pi([a,b]) = 1$, gdyz $K/Z(K)$ jest abelowe, zatem $[a,b] \in \ker\pi = K$.

Niech teraz $Z(K) = \langle z\rangle$. Wtedy mamy, że każdy element z K jest postaci $x^a y^b z^c$, gdyż $K/Z(K) = \{x^a y^b Z(K)\}$. Jednakże z komutuje z x oraz y. Gdyby więc x i y komutowały, to K byłaby abelowa, wbrew założeniu. Zatem $[x,y] \neq 1$, możemy więc przyjąć dla uproszczenia $z = [x,y]$.

Morfizm ψ

Mamy teraz, że $[a,b] = aba^{-1}b^{-1}$, zatem $[a,b]ba = ab$, czyli zamiana a z b powoduje powstanie dodatkowego $[a,b] \in [K,K] \leqslant Z(K)$, więc stąd $a^n b^m = b^m a^n [a,b]^{nm}$ – gdyż dokładnie nm razy będę musiał przerzucać ab na ba. Analogicznie możemy stwierdzić, że $a^n b^n = (ab)^n [a,b]^{\frac{n(n-1)}{2}}$.

W szczególności, przekształcenie analogiczne do endomorfizmu Frobeniusa, tj. $\psi : K \to K$ dane jako $\psi(v) = v^5$ jest homomorfizmem, gdyż $\psi(ab) = (ab)^5 = a^5b^5([a,b]^5)^{-4} = a^5b^5 = \psi(a)\psi(b)$, gdyż $[a,b]^5 \in [K,K] \subseteq Z(K)$, lecz $|Z(K)| = 5$, skąd tw. Lagrange'a daje $[a,b]^5 = 1$.

Widzimy w szczególności, że $\ker\psi$ to dokładnie te elementy K, których rząd to 5 lub 1. Mamy także, że $\psi(v) \in Z(K)$, gdyż $\pi(\psi(v)) = \pi(v^5) = (\pi(v))^5 = (vZ(K))^5 = Z(K)$, gdyż $Z(K)$ jest rzędu 5, skąd mamy, że $\psi(v) \in \ker\pi = Z(K)$.

Zatem $\psi : K \to Z(K)$. Rząd przeciwdziedziny wynosi 5, zatem $|\operatorname{im}\psi| \in \{1, 5\}$.

Przypadek $|\operatorname{im}\psi| = 1$

Wtedy mamy, że podnoszenie do piątej potęgi przerzuca całe K na jedynkę, zatem wszystkie elementy K mają rząd conajwyżej 5. W szczególności, $x^5 = y^5 = [x, y]^5 = 1$.

Określmy przekształcenie $\kappa : G \to K$ jako $\kappa\left(\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}\right) = x^c y^a [y, x]^b = x^c y^a [x, y]^{-b}$. Zauważmy, że

$$\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & \hat{a} & \hat{b}\\ 0 & 1 & \hat{c}\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \hat{a} + a & a\hat{c} + \hat{b} + b\\ 0 & 1 & \hat{c} + c\\ 0 & 0 & 1\end{pmatrix}$$

A także

$$x^c y^a [y, x]^b x^{\hat{c}} y^{\hat{a}} [y, x]^{\hat{b}} = x^c \left(y^a x^{\hat{c}}\right) y^{\hat{a}} [y, x]^{b+\hat{b}} = x^c \left(x^{\hat{c}} y^a [y, x]^{\hat{c}a}\right) y^{\hat{c}} [y, x]^{b+\hat{b}} = x^{c+\hat{c}} y^{a+\hat{a}} [y, x]^{b+\hat{b}+a\hat{c}}$$

zatem κ jest morfizmem grup, gdyż zarówno w G jak i w K liczby a, b, c pochodzą z $GF(5)$. Jest to oczywiście epimorfizm, gdyż każdy element z K zapisuje się jako $x^c y^a [y, x]^b$, więc jest obrazem odpowiedniej macierzy. Jednak $|K| = |G| = 125$, zatem to jest izomorfizm, więc $K \simeq G$.

Przypadek $|\operatorname{im}\psi| = 5$

Wtedy mamy, że $|\ker\psi| = 25$, a ponadto nie każdy element K ma rząd $\leqslant 5$, zatem istnieje element o rzędzie 25 (125 nie jest możliwe, bo K nie jest cykliczna). Niech w będzie rzędu 25. Wtedy jednak widzimy, że $\langle w\rangle$ oraz $\ker\psi$ są różnymi podgrupami K o rzędzie 25 – w $\ker\psi$ nie istnieje element o rzędzie 25, w $\langle w\rangle$ – tak. Weźmy teraz $u \in \ker\psi$ takie, żeby $u \notin \langle w\rangle$. Wtedy $|\langle u\rangle| = 5$ oraz $\langle u\rangle \cap \langle w\rangle = 1$. Oznaczmy więc $W = \langle w\rangle, U = \langle u\rangle$.

Normalność W Teraz przedstawię standardowy dowód, że w dowolnej grupie A, której rząd jest skończony i jej najmniejszy dzielnik pierwszy to p, każda podgrupa indeksu p jest normalna. Rozważmy bowiem podgrupę indeksu p, oznaczmy ją B. Wtedy A działa na A/B przez lewe przesunięcia. Działanie to indukuje homomorfizm $\tau : A \to \Sigma_p$ (warstw A/B jest p). Mamy wtedy, że $\operatorname{im}\tau \leqslant \Sigma_p$, zatem $|\operatorname{im}\tau| \mid p!$, jednakże $\operatorname{im}\tau \simeq A/\ker\tau$, zatem $|\operatorname{im}\tau| \mid |A|$. Zatem $|\operatorname{im}\tau| \mid \gcd(p!, |A|)$. Jednak założyliśmy, że p jest najmniejszym dzielnikiem pierwszym A, zatem mamy $\gcd(p!, |A|) = p$. Stąd $(A : \ker\tau) = |\operatorname{im}\tau| \mid p$.

Niech $r \in \ker\tau$. Wtedy mamy, że lewe przesuwanie przez r nie rusza żadnej warstwy A/B. Zatem w szczególności nie rusza B, zatem $r \in B$. Stąd $\ker\tau \leqslant B$. Jednakże $(A : B) = p$, $\ker\tau \leqslant B < A$, $(A : \ker\tau) \mid p$ implikuje, że $B = \ker\tau$, zatem B jest podgrupą normalną.

W naszym zadaniu stosujemy powyższe rozumowanie dla $A = K$, $B = W$, $p = 5$.

Wewnętrzny produkt półprosty Mamy teraz, że $W \trianglelefteq G$, $U \leqslant G$, $U \cap W = 1$. Mamy więc $\rho : U \to \operatorname{Aut}(W)$ dane przez $\rho(u)(w) = uwu^{-1} \in W$ z normalności. Zatem ma sens rozważanie $W \rtimes_\rho U$.

Mamy teraz $\xi : W \rtimes_\rho U \to K$ dane jako $\xi((w, u)) = wu$. Łatwo widać, że jest to homomorfizm, gdyż braliśmy jako automorfizmy automorfizmy wewnętrzne. Ponadto zauważmy, że $\xi((w, u)) = \xi((\hat{w}, \hat{u})) \implies wu = \hat{w}\hat{u} \implies W \ni \hat{w}^{-1}w = \hat{u}u^{-1} \in U$, zatem $\hat{u}u^{-1} = \hat{w}^{-1}w = 1$, czyli $u = \hat{u}$, $w = \hat{w}$. Zatem ξ jest monomorfizmem, a ponieważ prowadzi między grupami o tej samej mocy 125, to jest to izomorfizm.

Zatem wiemy, że K jest produktem półprostym: $\mathbb{Z}_{25} \rtimes \mathbb{Z}_5$, gdyż $W \simeq \mathbb{Z}_{25}$.

Automorfirzm grupy $\mathbb{Z}_{25}$ jest zadany przez wartość na generatorze. Obrazem jedynki może być dowolny inny element rzędu 25, a ich jest jak łatwo widać $\phi(25) = 5\cdot 4 = 20$. Zatem $\operatorname{Aut}(\mathbb{Z}_{25}) \simeq \mathbb{Z}_{20}$. Jest tam dokładnie jedna grupa 5-elementowa (na mocy twierdzenia Sylowa istnieje, oraz liczba tych podgrup przystaje do 1 modulo 5 oraz dzieli 4).

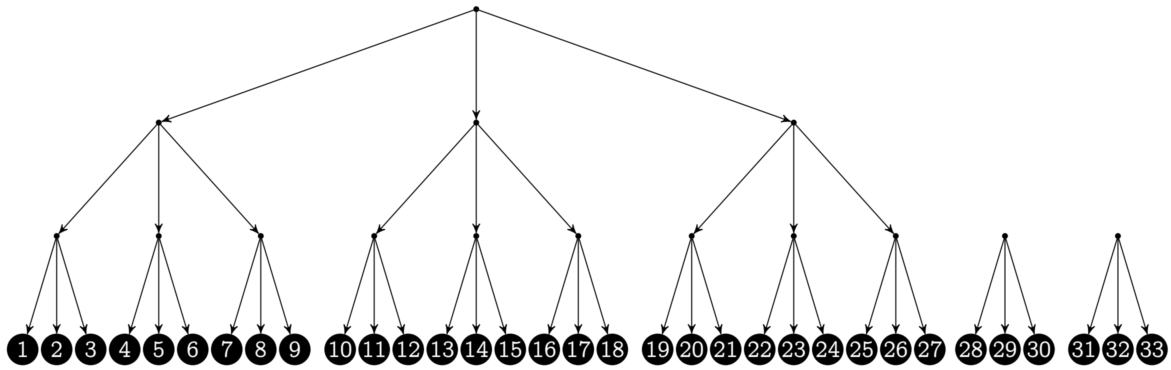
Mamy, że $\omega : \mathbb{Z}_5 \to \operatorname{Aut}(\mathbb{Z}_{25})$, zatem albo $\operatorname{im}\omega = 1$ albo $\operatorname{im}\omega$ jest tą jedną grupą 5-elementową. W pierwszym przypadku widzimy, ze rozważany produkt półprosty się degeneruje do produktu prostego, zatem mielibyśmy, że K jest abelowa, wbrew założeniu. Zatem $|\operatorname{im}\omega| = 5$. Uzyskujemy wtedy, że z dokładnością do przenumerowania elementów $\mathbb{Z}_5$ istnieje dokładnie jedno ω, zatem jest dokładnie jeden produkt półprosty $\mathbb{Z}_{25} \rtimes \mathbb{Z}_5$ i jest on jak łatwo widać izomorficzny z grupą H z podpunktu a.

Zadanie 43

Część a

Mamy, że $G = \langle(1\,2\,3\,4\,5), (6\,7\,8\,9\,10), (11\,12\,13\,14\,15)\rangle \leqslant \Sigma_{25}$ oraz G jest abelowa rzędu 125.

Część b



Rysunek 1: Las dla $n = 33$, $p = 3$

Rozważmy najpierw $n = p^k$. Ustawmy liczby $1, 2, \dots, n$ w ciągu i zbudujmy nad tym ciągiem drzewo p-arne w następujący sposób: grupujemy elementy w paczki po p, na nad każdą paczką rysujemy wierzchołek, uzyskamy wtedy p^{k-1} wierzchołków, następnie paczki te grupujemy w paczki paczek, liczące po p paczek itp. (por. rys. 1).

Operacją nazwę cykliczne przesunięcie cykliczne synów dowolnego wierzchołka. Oczywiście każda operacja indukuje pewną permutację liści, tj. element z Σ_n. Niech G będzie grupą generowaną przez operacje. Mamy wtedy oczywiste $\phi : G \to \Sigma_n$. Niech m będzie liczbą wierzchołków (nie licząc liści) w rozważanym drzewie.

Każdy element G mogę przedstawić w kanonicznej postaci jako złożenie pewnej liczby operacji na korzeniu, a następnie operacji na synach korzenia, wnukach korzenia, etc., gdyż wykonanie operacji na synu, a następnie na ojcu, to to samo, co wykonanie operacji na ojcu, a następnie operacji na następnym synu. Zatem łatwo widać, że $|G| = p^m$, gdyż w każdym wierzchołku decyduję, o ile przesunąć cyklicznie jego synów.

Ponadto permutacja liści jednoznacznie wyznacza całe drzewo. Bardziej formalnie: Niech $f \in \ker\phi$, tj. $\phi(f) = \mathrm{id}$. Wtedy wiemy, że liczba operacji na ojcu jest podzielna przez p, gdyż w przeciwnym wypadku np. liść z numerem 1 znalazłby się w złym poddrzewie. Schodząc indukcyjnie wgłąb drzewa uzyskujemy, że w każdym wierzchołku wykonaliśmy cykliczne przesunięcie o wielokrotność p, zatem widzimy, że f jest elementem neutralnym G.

Teraz dla dowolnego n bierzemy znów ciąg $1, 2, \dots, n$ i znajdujemy największe p^k mieszczące się w n, następnie nad elementami $1, 2, \dots, p^k$ budujemy drzewo jak wyżej, zostajemy z $n - p^k$ elementami, tam znowu znajdujemy największą potęgę p mieszczącą się w $n - p^k$ i rysujemy drzewo, etc. W wyniku uzyskamy las drzew p-arnych zbudowanych nad ciągiem n-elementowym. Łatwo widać, że wierzchołków na wysokości i nad ciągiem będzie $\lfloor \frac{n}{p^i} \rfloor$, zatem łącznie wierzchołków będzie $m := \sum_{i=1}^{n} \lfloor \frac{n}{p^i} \rfloor$, czyli tyle, że $p^m \mid n!$, zaś $p^{m+1} \nmid n!$.

Zauważmy, że teraz więc grupa operacji na tym lesie ma znów p^m elementów: jest ona iloczynem prostym grup operacji na poszczególnych zbiorach. Ponadto mamy znów wierne odwzorowanie drzew w permutacje liści, zatem mamy $\phi : G \to \Sigma_n$ będące monomorfizmem. Zatem $\operatorname{im}\phi$ jest p-podgrupą Sylowa w Σ_n.