Kiedy badamy jakąś strukturę matematyczną zawsze pouczające jest badanie także odwzorowań, które tę strukturę zachowują. Odwzorowania zachowujące strukturę mogą wspólną nazwę homomorfizmów. Tego rodzaju odwzorowania spotkaliśmy już na początku semestru badając odwzorowania liniowe i przestrzenie wektorowe. Pamiętamy, że przestrzeń wektorowa jest to zbiór V wyposażony w działanie dodawania wektorów oraz w działanie mnożenia przez liczby. Dodatkowym ważnym elementem struktury jest wektor zerowy. Odwzorowania, które tę strukturę zachowują nazwaliśmy odwzorowaniami liniowymi: (-4)

F - liniowe $\quad F: V \longrightarrow W$

$$F(\underbrace{v_1 + v_2}_{\text{dodawanie w } V}) = F(v_1) \underbrace{+}_{\text{dodawanie w } W} F(v_2)$$

$$F(\underbrace{\lambda v}_{\text{mnożenie przez liczby w } V}) = \underbrace{\lambda F(v)}_{\text{mnożenie przez liczby w } W}$$

Inaczej moglibyśmy powiedzieć, że odwzorowania liniowe są homomorfizmami przestrzeni wektorowych. Przy okazji pracy z grupami również warto badać odwzorowania zachowujące strukturę. Odwzorowania takie nazywają się homomorfizmy grup. Sformułujmy tę definicję bardziej precyzyjnie:

DEFINICJA : Niech $(G, \cdot)$ i $(H, \circ)$ będą grupami. Odwzorowanie $\varphi: G \to H$ jest homomorfizmem grup jeśli dla każdych dwóch elementów grupy zachodzi

$$(*)\ \varphi(\underset{\substack{\uparrow \\ \text{działanie} \\ \text{w } G}}{g_1 \cdot g_2}) = \varphi(g_1) \underset{\substack{\uparrow \\ \text{działanie} \\ \text{w } H}}{\circ} \varphi(g_2)$$

Zanim obejrzymy przykłady homomorfizmów sprawdźmy jakie są bezpośrednie konsekwencje definicji:

1) Niech e_G oznacza element neutralny w grupie G, wtedy

$$g \cdot e_G = g \quad \text{czyli} \quad \varphi(g \cdot e_G) = \varphi(g)$$

ale z drugiej strony $\varphi(g \cdot e_G) = \varphi(g) \cdot \varphi(e_G)$ zgodnie z $(*)$, czyli mamy

$$\varphi(g) = \varphi(g)\varphi(e_G) \to \varphi(e_G) = e_H$$

Homomorfizm zachowuje element neutralny

2) Sprawdźmy teraz co z odwrotnościami:

skoro $g^{-1}g = e_G$ to $\varphi(g^{-1}g) = \varphi(e_G) = e_H$

ale $\varphi(g^{-1}g) = \varphi(g^{-1}) \circ \varphi(g)$

jeśli więc $\varphi(g^{-1}) \circ \varphi(g) = e_H$ to

znaczy że $\varphi(g^{-1})$ i $\varphi(g)$ są wzajemnie odwrotne co można zapisać

$$\varphi(g^{-1}) = \varphi(g)^{-1}$$

Homomorfizm zachowuje także elementy odwrotne

3) Przyjrzyjmy się jeszcze zbiorowi tych elementów grupy G, których obrazem jest e_H

zbiór ten nazywamy jądrem homomorfizmu i oznaczamy $\ker\varphi$ (ma ono wiele wspólnego z jądrem odwzorowania liniowego: $(V,+)$ jest grupą i odwzorowanie liniowe jest w szczególności homomorfizmem grup. Wektor zerowy jest elementem neutralnym w $(V,+)$. Jądro odwzorowania liniowego jest też jądrem w sensie homomorfizmu grup) (-2)

$$\ker\varphi = \{ g \in G : \varphi(g) = e_H \}$$

Jądro homomorfizmu jest podgrupą w G: Istotnie: jeśli $g_1, g_2 \in \ker\varphi$ tzn $\varphi(g_1) = e_H$, $\varphi(g_2) = e_H$ to

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2) = e_H \cdot e_H = e_H$$

oznacza to, że $g_1 \cdot g_2 \in \ker G$. W sposób oczywisty $\ker G$ zawiera e_G (bo $\varphi(e_G) = e_H$) oraz wraz z każdym g zawiera g^{-1} bo

$$e_H = \varphi(g) \to e_H = \varphi(g)^{-1} = \varphi(g^{-1})$$

W grupie skończonej z resztą zbiór zamknięty ze względu na mnożenie jest podgrupą i nie trzeba sprawdzać, czy element neutralny i odwrotności należą. Tak nie jest już jeśli grupa ma nieskończenie wiele elementów.

4) Podgrupą jest także obraz homomorfizmu (podgrupą w H), który oznaczamy $\operatorname{im}\varphi$

$$\operatorname{im}\varphi \subset H$$

$$\operatorname{im}\varphi = \{ h \in H : \exists g \in G : \varphi(g) = h \}$$

-1

Jest więc jasne, że jeśli $h_1 \in \mathrm{im}\,\varphi$ i $h_2 \in \mathrm{im}\,\varphi$ to $h_1 h_2 \in \mathrm{im}\,\varphi$, bo biorąc odpowiednie $g_1 : \varphi(g_1) = h_1$ $g_2 : \varphi(g_2) = h_2$ dostaniemy
$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = h_1 \cdot h_2$$
Podobnie rzecz się ma z odwrotnością i jedynką.

Pora na przykłady: Od razu widać, że skoro jądro homomorfizmu jest zawsze podgrupą, to wybór homomorfizmów dla małych grup jest niewielki. Np jeśli ~~C_3~~ dziedziną homomorfizmu ma być C_3 to mamy do wyboru dwa możliwe jądra: $\{e\}$ lub całe C_3. Jeśli jądrem jest całe C_3 to homomorfizm jest trywialny, bo $\forall g \in C_3$ $\varphi(g) = e$ (i nawet nieważne w jakiej grupie to e jest)

Gdy $\ker\varphi = \{e\}$ to nasze odwzorowanie musi być włożeniem C_3 w jakąś większą grupę (lub izomorfizmem, czyli homomorfizmem odwracalnym) Np istnieje

$$\varphi : C_3 \longrightarrow D_3 \qquad C_3 = \{e, a, a^2\}$$

$$\varphi(e) = id, \quad \varphi(a) = o_1 \quad \varphi(a^2) = o_2$$

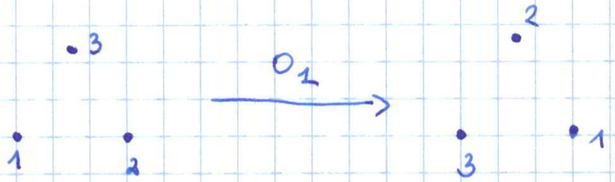
W grupie permutacji S_n jest jeden ważny homomorfizm: $\mathrm{sgn} : S_n \longrightarrow \cancel{\mathbb{Z}_2}\ \{-1, 1\} = \sqrt[2]{1} \cong C_2$

Znak permutacji

Rozważmy teraz następujące odwzorowanie

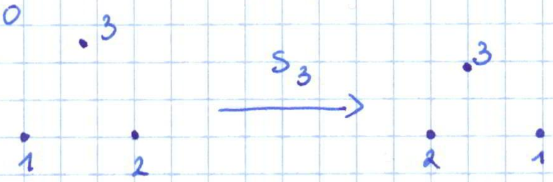
$\varphi: D_3 \longrightarrow S_3$ przyporządkowujące symetrii trójkąta równobocznego permutację odpowiadającą przestawieniu wierzchołków,

np:



$$\varphi(O_1) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

albo



$$\varphi(S_3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Odwzorowanie to zachowuje strukturę grupy, ponadto jest bijekcją, bo $|D_3| = 6 = 3! = |S_3|$, φ jest surjekcją (każda permutacja odpowiada jakiejś symetrii).

Okazuje się więc, że S_3 i D_3 są izomorficzne.

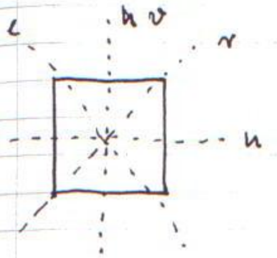
Można powiedzieć, że są to dwie realizacje tej samej grupy.

40. O grupie kwaternionów: reprezentacje, podgrupy, klasy sprzężoności. 1

R34

O grupie D_4. Dobry przykład, różne rzeczy można pokazać na palcach, grupa nie za duża, nie za mała...

D_4 - grupa symetrii kwadratu



$$D_4 = \{e, o_1, o_2, o_3, v, h, r, l\}$$

(1) TABELKA DZIAŁANIA:

	e	o_1	o_2	o_3	v	h	r	l
e	e	o_1	o_2	o_3	v	h	r	l
o_1	o_1	o_2	o_3	e	r	l	h	v
o_2	o_2	o_3	e	o_1	h	v	l	r
o_3	o_3	e	o_1	o_2	l	r	v	h
v	v	l	h	r	e	o_2	o_3	o_1
h	h	r	v	l	o_2	e	o_1	o_3
r	r	v	l	h	o_1	o_3	e	o_2
l	l	h	r	v	o_3	o_1	o_2	e

$$o_1 v \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} = o_1 \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix}$$

$$o_1 r \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} = o_1 \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix}$$

$$v r \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} = v \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$$

$$r v \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = r \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$$

(2) PODGRUPY:

D_4

$\{e\ o_2\ l\ r\}$ $\{e\ o_1\ o_2\ o_3\}$ $\{e\ o_2\ v\ h\}$

$\{e\ l\}$ $\{e\ r\}$ $\{e\ o_2\}$ $\{e\ v\}$ $\{e\ h\}$

$\{e\}$

(a) GENERATORY (R 38) (2)

Weźmy o_3 i h $\quad o_3^4 = e = h^2$ ponadto

$$o_3 h = r = h o_1 = h o_3^3 \qquad \text{Hipoteza: } D_4 \simeq \langle a, b \mid a^4 = b^2 = e,\ ab = ba^3 \rangle$$

$G =$

$$\langle a, b \mid a^4 = b^2 = e\ ;\ ab = ba^3 \rangle =$$
$$= \{ e, a, a^2, a^3, b, ba, ba^2, ba^3 \}$$

$\# G = \# D_4$ czyli na sztuki się zgadza. Niech

$\varphi : G \longrightarrow D_4$ będzie dane:

$\varphi(a) = o_3$ $\qquad$ o_3 i h spełniają te same

$\varphi(b) = h$ $\qquad$ relacje co a i b i ~~ponadto~~

i φ jest homomorfizmem grup.

Szukamy $\ker \varphi$

$$x \in \ker\varphi \iff \varphi(x) = e \qquad x = b^k a^l \qquad k = 0, 1 \quad l = 0, 1, 2, 3$$

$$\varphi(x) = \varphi(b^k)\varphi(a^l) = \varphi(b)^k \varphi(a)^l =$$
$$= \cancel{(o_3} \quad h^k (o_3)^l = e$$
$$\iff k = 0 = l$$

tzn. φ jest injekcyjne. ponieważ $\# G = \# D_4$

to φ jest bijekcją. czyli $G \simeq D_4$.

(b) Automorfizmy: Generatory są wygodnym narzędziem do badania automorfizmów grup: Zauważmy, że o_3, h nie jest jedyną parą generatorów spełniających takie same relacje jak G:

$o_3 \ h \qquad\qquad o_1 \ h$ $\qquad$ jest 8 zestawów generatorów

$o_3 \ v \qquad\qquad o_1 \ v$ $\qquad$ a co za tym idzie

$o_3 \ r \qquad\qquad o_1 \ r$ $\qquad$ osiem automorfizmów

$o_3 \ l \qquad\qquad o_1 \ l$

9

3

$\varphi_0 = id_{D_4}$

$\varphi_1 : \quad \varphi_1(O_3) = O_3 \quad \varphi_1(h) = v$

$\varphi_2 : \quad \varphi_2(O_3) = O_3 \quad \varphi_2(h) = r$

$\vdots$

$\varphi_7 : \quad \varphi_7(O_3) = O_1 \quad \varphi_7(h) = l$

Pytanie: co to za grupa: Aut (D_4) i które są wewnętrzne.
Na to pytanie najlepiej odpowiadać znając klasy sprzężoności

KLASY SPRZĘŻONOŚCI:

w G: $e, a, a^2, a^3, b, ba, ba^2, ba^3$

$[a] = \{a, a^3\} \qquad [e] = \{e\}$

~~dla~~ $bab = bba^3 = a^3$

ogólnie:

$ba^k a (ba^k)^{-1} = ba^k a a^{-k} b = bab = a^3$

$[a^2] = \{a^2\}$ tzn. $Z(G) = \{e, a^2\}$

$ba^k a^2 a^{-k} b = ba^2 b = baba^3 = b^2 a^3 a^3 = a^2$

$aba^3 = ba^3 a^3 = ba^2 \qquad [b] = \{b, ba^2\}$

$a^k b a^{-k} = ba^{3k} a^{-k} = ba^{2k} = \begin{cases} b \\ ba^2 \end{cases}$

$ba^k b (ba^k)^{-1} =$

$= b^2 a^{3k} \cdot a^{-k} b = a^{2k} b = \begin{cases} b \\ a^2 b = ba^6 = ba^2 \end{cases}$

$[ba] = \{ba, ba^3\}$

$a^k ba a^{-k} = ba^{3k} a a^{-k} = ba^{2k+1} = \begin{cases} ba \\ ba^3 \end{cases}$

$bbab = ab = ba^3$

$bba^3 b = a^3 b = ba^9 = ba$

tzn. $G = \{e\} \cup \{a^2\} \cup \{a, a^3\} \cup \{b, ba^2\} \cup \{ba, ba^3\}$ (4)

$D_4 = \{e\} \cup \{o_2\} \cup \{o_1, o_3\} \cup \{h, v\} \cup \{r, l\}$

Wracamy teraz do automorfizmów. Widać, że wewnętrzne mogą być:

$\varphi_0, \varphi_1, \varphi_4, \varphi_5$

Jeśli przyjmiemy oznaczenie $\sigma_g(x) = gxg^{-1}$

wtedy $\sigma_g = \sigma_h \iff$

$\forall x \quad gxg^{-1} = hxh^{-1} \quad / h$

$g^{-1} \setminus \quad gxg^{-1}h = hx$

$g^{-1}gxg^{-1}h = g^{-1}hx$

$x(g^{-1}h) = (g^{-1}h)x$

tzn. $g^{-1}h \in Z(D_4)$

tzn. $\mathrm{InnAut}(D_4) \simeq D_4/Z(D_4)$

ogólnie $\mathrm{InnAut}(G) \simeq D_4/Z(D_4)$

ustaliliśmy wcześniej że $Z(D_4) = \{e, o_2\}$

~~Zauważamy dodatkowo, że jeśli g i h są sprzężone to $g^{-1}h \in Z(G)$~~

~~$g = xhx^{-1}$ $\quad (g^{-1}h)y =$~~

~~$g^{-1} = xh^{-1}x^{-1}$ $\quad xh^{-1}x^{-1}h$~~

~~$\forall y: \; g^{-1}hy = yg^{-1}h \implies y^{-1}g^{-1}hy = g^{-1}h$~~

~~$y^{-1}g^{-1}yy^{-1}hy = g^{-1}h$~~

~~$hy = gyg^{-1}h$~~

5

$$D_4 / Z(D_4) = \{\{e, o_2\}, \{o_3, o_1\}, \{v, h\}, \{r, l\}\}$$

$$\cong$$

$$V_4 = \{E, O, V, R\}$$

$\varphi_{10} = \varphi_E \qquad \varphi_1 = \varphi_O \qquad \varphi_4 = \varphi_V \qquad \varphi_5 = \varphi_R$

tzn. $\operatorname{InnAut}(D_4) \simeq V_4$

ogólnie $\operatorname{Aut}(D_4) \simeq D_4$: dowód:

weźmy φ_7 :

$\varphi_7(o_3) = o_1 \qquad \varphi_7^2: \quad \varphi_7^2(o_3) = \varphi_7(\varphi_7(o_3)) =$

$\varphi_7(h) = l \qquad = \varphi_7(o_1) = \varphi_7(o_3^3) = o_1^3 = o_3$

$\varphi_7^2(h) = \varphi_7(\varphi_7(h)) = \varphi_7(l) = \varphi_7(h o_3) =$

$l \cdot o_1 = h \qquad$ tzn. $\varphi_7^2 = id \quad$ bo $\varphi_7(o_3) = o_3$

$\varphi_7(h) = h$

φ_3:

$\varphi_3^2(o_3) = o_3$

$\varphi_3^2(h) = r$

$\varphi_{3_2}^2$: $\quad \varphi_{3_2}^2(o_3) = o_3$

$\varphi_{3_2}^2(h) = \varphi_{3_2}(\varphi_{3_2}(h)) = \varphi_{3_2}(r) = \varphi_{3_2}(h o_3^3) = \varphi_{3_2}(h)\, \varphi_{3_2}(o_3)^3 =$

$= r o_1 = \cancel{x}\ v$

Iloczyn półprosty:

(1) Zbiór automorfizmów grupy G wyposażony w działanie składania odwzorowań jest grupą

automorfizm jest to odwzorowanie grupy w siebie będące homomorfizmem i bijekcją (czyli odwracalne). Inaczej automorfizm G to izomorfizm G w G.

Weźmy $G = C_3$. Grupa C_3 ma trzy elementy, z których dwa są rzędu 3: $C_3 = \{e, a, a^2\}$ Przykładem konkretnym grupy C_3 jest $\mathbb{Z}_3$ (zbiór reszt modulo 3) lub zbiór zespolonych pierwiastków trzeciego stopnia z 1: $\sqrt[3]{1} = \{1, e^{i\frac{2\pi}{3}}, e^{i\frac{4\pi}{3}}\}$. Zbiór automorfizmów $Aut(C_3)$ składa się z dwóch elementów: odwzorowania identycznościowego:

$$id_{C_3}: \begin{array}{l} e \mapsto e \\ a \mapsto a \\ a^2 \mapsto a^2 \end{array} \quad \text{oraz odwzorowania} \quad \alpha: \begin{array}{l} e \mapsto e \\ a \mapsto a^2 \\ a^2 \mapsto a \end{array}$$

sprawdźmy, że α jest automorfizmem:

-> że jest odwracalne (widać)

-> że jest homomorfizmem grup:

$$\left.\begin{array}{l}\alpha(e\cdot a) = \alpha(a) = a^2 \\ \alpha(e)\alpha(a) = e\cdot a^2 = a^2\end{array}\right\} \qquad \left.\begin{array}{l}\alpha(e\cdot a^2) = \alpha(a^2) = a \\ \alpha(e)\alpha(a^2) = e\cdot\alpha(a^2) = e\cdot a = a\end{array}\right\} \qquad \alpha(e\cdot e)\cdots \text{ trywialne}\ldots$$

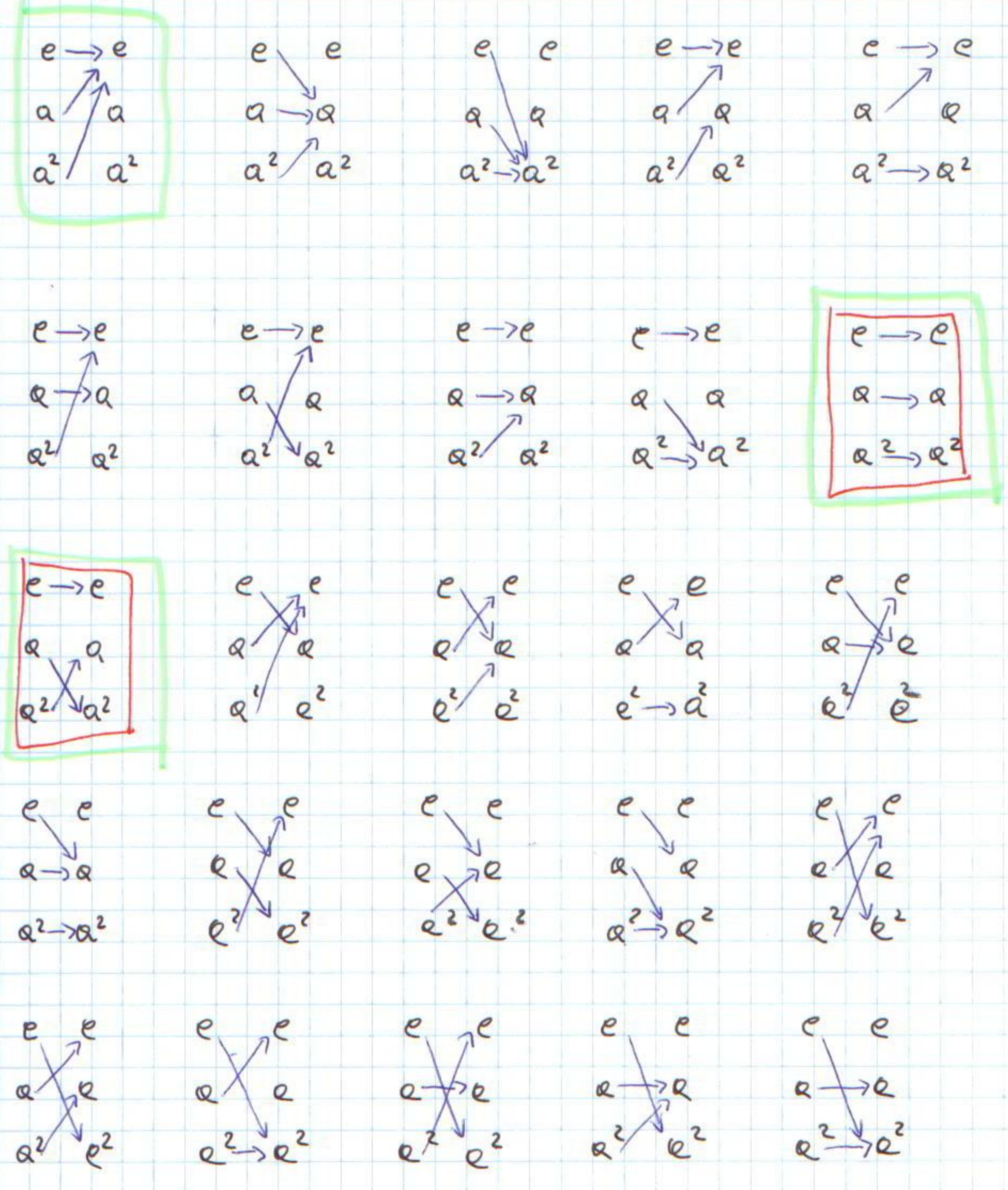
$$\left.\begin{array}{l}\alpha(a\cdot a) = \alpha(a^2) = a \\ \alpha(a)\cdot\alpha(a) = a^2\cdot a^2 = a^3\cdot a = e\cdot a = a\end{array}\right\} \qquad \left.\begin{array}{l}\alpha(a^2\cdot a^2) = \alpha(a) = a^2 \\ \alpha(a^2)\cdot\alpha(a^2) = a\cdot a = a^2\end{array}\right\}$$

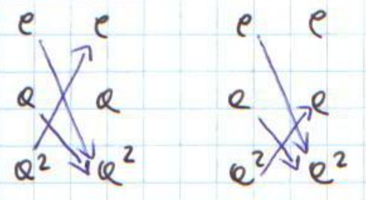
$$\left.\begin{array}{l}\alpha(a\cdot a^2) = \alpha(e) = e \\ \alpha(a)\cdot\alpha(a^2) = a^2\cdot a = e\end{array}\right\}$$

Sprawdziliśmy sześć ze wszystkich dziewięciu możliwych mnożeń. Grupa jest przemienna, pozostałe trzy polegają jedynie na zamianie kolejności.

α jest automorfizmem co sprawdziliśmy bezpośrednim rachunkiem.

Wszystkich odwzorowań C_3 w siebie jest 27 (3^3) 7





$$Aut(C_3) \simeq C_2 \; (\simeq \mathbb{Z}_2)$$

homomorfizmy

automorfizmy

② Niech teraz G, H - dwie grupy

$\rho : G \longrightarrow Aut(H)$ będzie homomorfizmem grup

W zbiorze $G \times H$ wprowadzamy działanie

$$(g_1, h_1) \circ (g_2, h_2) := \left(g_1 \cdot g_2 ,\ h_1 \circ \underbrace{\rho(g_1)}_{\substack{\text{to jest} \\ \text{automorfizm} \\ \text{grupy } H}}(h_2) \right)$$

np: $G = \overset{C_2}{\mathbb{Z}_2}$, $H = C_3$

wiemy już, że automorfizmy C_3 są dwa (id, α)

wprowadzamy $\rho : \mathbb{Z}_2 \to Aut(C_3)$ wzorem

$\rho(0) = id \qquad \rho(1) = \alpha$

$G \times H$ ma sześć elementów: $G \times H = \{(0,e); (0,a); (0,a^2); (1,e); (1,a), (1,a^2)\}$ sprawdzimy jak mnożą się przez siebie np $(1,a) \cdot (0,a^2) =$

$$= \left(1+0,\ a \cdot \rho(1)(a^2)\right) = \left(1,\ a \cdot \underbrace{\alpha(a^2)}_{a}\right) = (1, a^2)$$

	$(0,e)$	$(0,a)$	$(0,a^2)$	$(1,e)$	$(1,a)$	$(1,a^2)$
$(0,e)$	$(0,e)$	$(0,a)$	$(0,a^2)$	$(1,e)$	$(1,a)$	$(1,a^2)$
$(0,a)$	$(0,a)$	$(0,a^2)$	$(0,e)$	$(1,a)$	$(1,a^2)$	$(1,e)$
$(0,a^2)$	$(0,a^2)$	$(0,e)$	$(0,a)$	$(1,a^2)$	$(1,e)$	$(1,a)$
$(1,e)$	$(1,e)$	$(1,a^2)$	$(1,a)$	$(0,e)$	$(0,a^2)$	$(0,a)$
$(1,a)$	$(1,a)$	$(1,e)$	$(1,a^2)$	$(0,a)$	$(0,e)$	$(0,a^2)$
$(1,a^2)$	$(1,a^2)$	$(1,a)$	$(1,e)$	$(0,a^2)$	$(0,a)$	$(0,e)$

$\simeq D_3$

podgrupa

$(1,e)\cdot(1,e) =$
$(1+1,\ e \cdot \rho(1)(e)) =$
$= (0,e)$

$(1,a)(1,a) =$
$= (1+1,\ a\,\alpha(a)) = (0,e)$

$(1,e)(0,a) =$
$= (1,\ e\,\alpha(a)) = (1,a^2)$

$(1,e)(1,a) =$
$(0; e; \alpha(a)) = (0,a^2)$

Taka struktura nazywa się iloczyn półprosty. Trzeba sprawdzić, czy iloczyn półprosty dwóch grup w ogóle jest grupą (9)

jedynka, odwrotność, łączność mnożenia

oznaczenie $G \rtimes H$

1) Sprawdzamy łączność:

$$(g_1,h_1)\cdot\left[(g_2,h_2)\cdot(g_3,h_3)\right] = (g_1,h_1)\cdot\left(g_2\cdot g_3,\ h_2\,\rho(g_2)(h_3)\right) =$$

$$= \left(g_1 g_2 g_3,\ h_1\,\rho(g_1)\left(h_2\cdot\rho(g_2)(h_3)\right)\right) =$$

$$= \left(g_1 g_2 g_3,\ h_1\,\rho(g_1)(h_2)\cdot\rho(g_1)\left(\rho(g_2)(h_3)\right)\right) =$$

$$= \left(g_1 g_2 g_3,\ h_1\cdot\rho(g_1)(h_2)\cdot\rho(g_1 g_2)(h_3)\right)$$

to samo ✓

$$\left[(g_1,h_1)(g_2,h_2)\right]\cdot(g_3,h_3) = \left(g_1 g_2,\ h_1\cdot\rho(g_1)(h_2)\right)(g_3,h_3) =$$

$$= \left(g_1 g_2 g_3,\ h_1\cdot\rho(g_1)(h_2)\cdot\rho(g_1 g_2)(h_3)\right)$$

2) element neutralny to $\cancel{(e_H, e_G)}$ $(e_G, e_H) = E$

$$E(g,h) = (e_G,e_H)(g,h) = \left(e_G g,\ e_H\,\underbrace{\rho(e_G)}_{id}(h)\right) =$$

$$= (g,\ e_H h) = (g,h)\ ✓$$

$$(g,h)\cdot E = (g,h)(e_G,e_H) = \left(g\cdot e_G,\ h\cdot\underbrace{\rho(g)(e_H)}_{e_H}\right) = (g,h)\ ✓$$

3) Czy istnieje element odwrotny:

$$(g,h)^{-1} = (g^{-1}, h') \quad \text{szukamy } h'$$

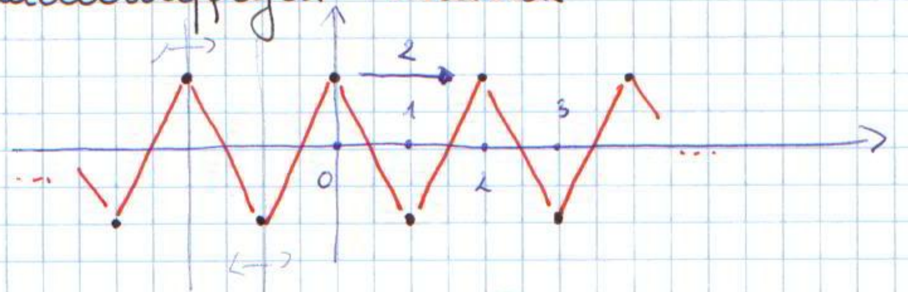
$$(g,h)(g,h)^{-1} = (g,h)(g^{-1},h') = \left(gg^{-1},\ h\rho(g)(h')\right) = \left(\cancel{e_g}\, e_G,\ \underbrace{h\cdot\rho(g)(h')}_{e_H}\right)$$

$$h\cdot\rho(g)(h') = e_H$$

$$\rho(g)(h') = h^{-1} \qquad h' = \rho(g^{-1})(h^{-1})$$

PRZYKŁAD PODSTAWOWY:

Niech G będzie podgrupą izometrii płaszczyzny zachowujących szlaczek



Wykazać, że $G \simeq \mathbb{Z}_2 \ltimes \mathbb{Z}$

Zastanówmy się przede wszystkim jakie odwzorowania zachowują szlaczek: są to przesunięcie w prawo i w lewo o 2 oraz odbicie względem prostych $x = k$ $k \in \mathbb{Z}$. Są to odwzorowania afiniczne, można je więc zapisać jako liniowe + przesunięcie

$$t_k \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + k \begin{bmatrix} 2 \\ 0 \end{bmatrix} \qquad k \in \mathbb{Z}$$

odbicie w prostej $x = k$

$$\begin{bmatrix} x \\ y \end{bmatrix} \longmapsto \begin{bmatrix} 2k-x \\ y \end{bmatrix} \qquad s_k \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 0 \end{bmatrix} k$$

$$t = t_1 \rightsquigarrow t_k = (t_1)^k \qquad s^2 = id$$

$$s = s_0 \qquad s_k = t_k s_0$$

$$sts\ \alpha:\ \begin{bmatrix} x \\ y \end{bmatrix} \xmapsto{s} \begin{bmatrix} -x \\ y \end{bmatrix} \xmapsto{t} \begin{bmatrix} -x+2 \\ y \end{bmatrix} \xmapsto{s} \begin{bmatrix} x-2 \\ y \end{bmatrix}$$

$$t^{-1} = t_{-1}$$

$$\langle s, t \ :\ s^2 = id \quad sts = t^{-1} \rangle$$

te zasady pozwalają sprowadzić każde słowo z liter s, t do postaci $t^k s$. Grupa łowiero więc

$G = \{ id, t, t^{-1}, t^{2}, t^{-2}, \dots, s, ts, t^{2}s, \dots t^{-1}s, t^{-2}s, \dots \}$

s jest rzędu 2 $\quad t$ jest rzędu ∞

Czy G jest $\mathbb{Z}_2 \ltimes \mathbb{Z}$

$$\rho : \mathbb{Z}_2 \longrightarrow \cancel{\#} \operatorname{Aut}(\mathbb{Z})$$

szukamy homomorfizm

$\alpha(1) = id$

$\alpha(-1) =$ mnożenie przez -1.

$$\mathbb{Z}_2 \ltimes \mathbb{Z} = \{ (1, k), (-1, k) \}$$

$k \in \mathbb{Z}$

$$(\varepsilon, k)(\varepsilon', k') = (\varepsilon\varepsilon', k + \varepsilon k')$$

$s \longmapsto (-1, 0) \longrightarrow$ izomorfizm G i $\mathbb{Z}_2 \times \mathbb{Z}$

$t \longmapsto (1, 1) \qquad t^k \longmapsto (1, k)$

$sts = (-1,0)(1,1)(-1,0) = (-1,0)(-1,1) =$

$= (1, 0 + (-1)\cdot 1) = (1,-1) = t^{-1}.$

$s^2 = (-1,0)(-1,0) = (1,0) = id.$