Jak zdefiniować homomorfizm, konkretnie?

Wstęp Wiemy, co to znaczy że funkcja $f : G \to H$ między grupami jest homomorfizmem, ale jak zdefiniować homomorfizm w konkretnym przypadku? Oczywiście, moglibyśmy najpierw zdefiniować funkcję, i potem sprawdzić warunek homomorfizmu na wszystkich produktach. Ale jak rząd G rośnie, to liczba takich produktów rośnie do kwadratu, więc to się szybko robi ciężko.

W przestrzeniach liniowych mamy takie rzeczy jak bazy, które w tym pomagają. Jeśli chcę zdefiniować przekształcenie liniowe $f : V \to W$, to nie muszę go zdefiniować na każdym elemencie: przyporządkowanie każdemu wektorowi z pewnej bazy V jakiegoś wektora w W rozszerza się do dokładnie jednego homomorfizmu z całego V. Dlaczego? Dlatego, że każdy wektor w V pisze się *jednoznacznie* jako kombinacja liniowa elementów z bazy.

Czy możemy coś podobnego zrobić w grupach? Moglibyśmy pomyśleć, że jeśli mam generatory grupy G, to żeby zdefiniować homomorfizm $G \to H$ to wystarczy przyporządkować każdemu generatorowi jakiś element w H. Otóż to nie działa. Dlaczego? Ponieważ teraz to ogólnie nie jest prawda, że każdy element z G pisze się *jednoznacznie* jako produkt generatorów i ich odwrotności! Więc już nie wiadomo, jak rozszerzać taką funkcję na generatorach do homomorfizmu jednoznacznie... łatwy przykład: $G = D_8$. Chcemy zdefiniować homomorfizm $G \to \mathbb{Z}$. Jakbyśmy mogli to zdefiniować na generatorach, to wystarczyłoby powiedzieć na przykład: niech $r \mapsto 2$ i $s \mapsto 0$. Wtedy skoro f jest homomorfizmem, mamy $rs \mapsto f(r) + f(s) = 2$, oraz $sr^3 \mapsto f(s) + 3f(r) = 6$, ale $rs = sr^3$! Jest problem: jeden element ma dwa obrazy... To nie jest dobrze zdefiniowana funkcja.

Grupy cykliczne Zdefiniowanie na generatorach ogólnie nie działa, ale może coś innego zadziała? Zacznijmy od prostych przykładów, czyli od grup cyklicznych.

Jeśli $G = \langle a \rangle$ i a ma nieskończony rząd (więc $G \cong \mathbb{Z}$) to łatwo sprawdzić, że aby zdefiniować $f : G \to H$ wystarczy wyznaczyć $f(a) := b$. Wtedy $f(a^n) = b^n$ dla wszystkich $n \in \mathbb{Z}$. W tym bardzo prostym przypadku, wystarczy zadać f na generatorze a!

Jeśli $G = \langle a \rangle$ i a ma rząd $n < \infty$ (więc $G \cong \mathbb{Z}_n$), to homomorfizmy $G \to H$ są w bijekcji z elementami w H rzędu dzielnik n: to są nasze możliwe obrazy a. Rzeczywiście, z pierwszego twierdzenia o izomorfizmie wiemy, że homomorfizmy $\mathbb{Z}_n \to H$ to to samo co homomorfizmy $f : \mathbb{Z} \to H$ takie, że $\ker(f) = n\mathbb{Z}$. Ale $f(n) = f(1)^n = 0$ co znaczy, że rząd $f(1)$ dzieli n, i już wiemy, że $f(1)$ wyznacza f. Udowodniliśmy, że $\mathrm{Hom}(\mathbb{Z}_n, H) \cong H[n]$ gdzie $H[n]$ oznacza elementy w H rzędu dzielącego n.

W poprzednim przypadku widzimy, że wystarczy się upewnić, że przyporządkowaliśmy generatorowi $1 \in \mathbb{Z}_n$ jakiś element który nie łamie zasady że rząd $f(1)$ musi dzielić rząd 1, czyli n. Czy ogólnie to wystarczy? Czyli, jeśli mam generatory G i chcę zdefiniować homomorfizm $f : G \to H$, czy wystarczy wyznaczyć dla każdego generatora $g \in G$ jakiś element w H taki, że jego rząd dzieli rząd g?

Otóż też nie. Na przykład $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$. Spróbujmy zdefiniować homomorfizm $f : S_3 \to S_3$ tak jak powyżej, więc niech f przesyła wszystkie 3-cykle na zero, i niech przesyła 2-cykle na same siebie. Wtedy rząd $f(\sigma)$ dzieli rząd σ dla wszystkich $\sigma \in S_3$, ale czy to wyznacza homomorfizm? Nie, ponieważ dla $\sigma = (1\ 2)$ i $\tau = (1\ 2\ 3)$ mamy $f(\sigma\tau) = f((2\ 3)) = (2\ 3)$, ale $f(\sigma)f(\tau) = (1\ 2\ 3)$.

Żeby zdefiniować homomorfizm, często łatwiej jest to zrobić inaczej, na przykład za pomocą pierwszego twierdzenia o izomorfizmie: homomorfizmy $G \to H$ są w bijekcji z homomorfizmami

$G/\ker(f) \to H$, i tę bijekcję rozumiemy. Więc jeśli $G/\ker(f)$ jest łatwiejszy, na przykład cykliczny, to możemy z niego zdefiniować morfizm ręcznie bez błędu. Zróbmy przykład.

Zadanie. Opisać wszystkie homomorfizmy $f : A_4 \to \mathbb{Z}_{12}$.

Pierwsze rozwiązanie Taki homomorfizm ma jądro, które jest podgrupą normalną A_4. Wiemy, jak wyglądają podgrupy normalne A_4: to zrobiliśmy na ćwiczeniach. To są id, A_4 i

$$H \coloneqq \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

Przypominam jak to zrobiliśmy: wystarczy opisać klasy sprzężoności w A_4 (klasa identyczności, klasa permutacji typu $(2,2)$ i dwie klasy mocy 4 składające się z 3-cyklów), bo podgrupa jest normalna wtedy i tylko wtedy, gdy jest sumą klas sprzężoności.

Teraz, jeśli jądro jest wszystkim, to dostajemy tylko homomorfizm zerowy. Jądro nie może być $\{\mathrm{id}\}$, bo wtedy f byłby izomorfizmem, co jest nie możliwe bo jedna grupa jest abelowa a druga nie. Zostaje badać co, jeśli jądro to H.

Alternatywny dowód tego, że jeśli f jest nietrywialny to $\ker(f) = H$. Permutacje typu $(2,2)$ przechodzą na elementy rzędu dzielącego 2, czyli na 0 lub na 6 w $\mathbb{Z}_{12}$. Udowadniamy, że nie mogą przejść na 6. Załóżmy niewprost, że $f((a\ c)(b\ d)) = 6$. Wiemy, że 3-cykle muszą przejść na elementy rzędu dzielącego 3, czyli $0, 4, 8$. A teraz zauważmy, że $(a\ c)(b\ d) = (a\ b\ c)(a\ b\ d)$. Aplikując f i licząc rzędy dostajemy rozkład 6 jako sumy dwóch z 0, 4, 8, co jest niemożliwe.

Wtedy pierwsze twierdzenie o izomorfizmie mówi, że wystarczy zdefiniować homomorfizm $\tilde{f} : A_4/H \to \mathbb{Z}_{12}$. Ale A_4/H ma trzy elementy, więc jest cykliczna: możemy łatwo z niej zdefiniować homomorfizm. Możemy konkretnie opisać warstwy tak: warstwa H, warstwa σH i warstwa $\sigma^2 H$ dla dowolnego 3-cyklu σ ($\sigma H \neq \sigma^2 H$, bo inaczej mielibyśmy $\sigma \in H$). Weźmy dla ustalenia uwagi $\sigma = (1\,2\,3)$.

Elementy rzędu dzielącego 3 w $\mathbb{Z}_{12}$ to $0, 4, 8$. Więc w sumie mamy 3 homomorfizmy $\tilde{f}$, w czym 2 nietrywialne, wyznaczone poprzez $\tilde{f}(\sigma H) = 4$ lub $\tilde{f}(\sigma H) = 8$. W pierwszym przypadku $\tilde{f}(\sigma^2 H) = 8$ a w drugim $\tilde{f}(\sigma^2 H) = 4$. Weźmy pierwszy dla ustalenia uwagi, i opiszmy odpowiedny homomorfizm $f : A_4 \to \mathbb{Z}_{12}$.

To jest $f = \tilde{f} \circ \pi$, gdzie $\pi : A_4 \to A_4/H$ przesyła permutację na swoją warstwę. Więc wystarczy powiedzieć do której warstwy należy każda permutacja, innymi słowy, opisać warstwy. To jest prosty rachunek: 4 mnożenia nam dają

$$\sigma H = \{(1\,2\,3), (1\,3\,4), (1\,4\,2), (2\,4\,3)\},$$

i wtedy $\sigma^2 H = (1\,3\,2)H$ się składa z reszty 3-cyklów, czyli:

$$\sigma^2 H = \{(1\,3\,2), (1\,4\,3), (1\,2\,4), (2\,3\,4)\}.$$

Więc nasze żądane f wygląda tak: elementy w H przechodzą na 0, elementy w σH przechodzą na 4, i elementy w $\sigma^2 H$ przechodzą na 8. Ten drugi homomorfizm niezerowy po prostu przesyła elementy w σH na 8 i elementy w $\sigma^2 H$ na 4.

Drugie rozwiązanie Skoro $\mathbb{Z}_{12}$ jest abelowa, to żeby zdefiniować homomorfizm $A_4 \to \mathbb{Z}_{12}$ wystarczy zdefiniować homomorfizm $A_4' \to \mathbb{Z}_{12}$, gdzie A_4' to abelianizacja A_4. Trzeba więc policzyć komutant A_4.

Niech H będzie tą samą podgrupą co w pierwszym rozwiązaniu. Wiemy, że $A_4/H \cong \mathbb{Z}_3$ jest abelowa, więc $[A_4, A_4] \leq H$. Wiemy też, że $[A_4, A_4] \neq \{\mathrm{id}\}$, ponieważ A_4 nie jest abelowa. Zawsze komutant jest podgrupą normalną: $[A_4, A_4] \triangleleft A_4$, z czego wynika, że $[A_4, A_4] = H$. Albo dlatego, że znamy podgrupy normalne A_4 (jak w pierwszym rozwiązaniu), albo na palcach: jakby $[A_4, A_4]$ była podgrupą rzędu 2, to byłaby generowana przez jakąś $(a\ b)(c\ d)$, ale to nie jest podgrupa normalna, ponieważ $(a\ b\ c)(a\ b)(c\ d)(a\ c\ b) = (a\ d)(b\ c)$. Teraz postępujemy tak samo jak w pierwszym rozwiązaniu.

Trzecie rozwiązanie Załóżmy, że $f : A_4 \to \mathbb{Z}_{12}$ jest homomorfizmem nietrywialnym. Wtedy:

f ma jądro H: jak w pierwszym rozwiązaniu.

f przesyła $(1\ 2\ 3)$ na 4 lub 8 z powodu rzędu. Załóżmy, że $f((1\ 2\ 3)) = 4$. Mamy, że $(1\ 2\ 3)\sigma$ jest typu $(2,2)$ dla $\sigma \in \{(1\ 2\ 4), (1\ 4\ 3), (2\ 3\ 4)\}$, więc aplikując f widzimy, że one wszystkie przechodzą na 8. Mamy też $(1\ 2\ 3)(1\ 3\ 2) = \mathrm{id}$, więc $f((1\ 3\ 2)) = 8$ także.

Również widzimy, że $(1\ 3\ 2)\tau$ jest typu $(2,2)$ dla $\tau \in \{(1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\}$, więc skoro $f((1\ 3\ 2)) = 8$, one wszystkie przechodzą na 4.

Co udowodniliśmy? Że jeśli f jest homomorfizmem i $f((1\ 2\ 3) = 4$, to $f(H) = 0$ oraz $f(\{(1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 3), (2\ 3\ 4)\}) = \{8\}$ i $f(\{(1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\}) = \{4\}$.

To nie wystarczy. Znaleźliśmy jakiegoś kandydata na homomorfizm, ale to, że nasze rozumowania nas do tego doprowadziły, nie znaczy że nie ma jakiejś sprzeczności gdzieś. Na przykład, mogłoby *a priori* być tak, że żaden homomorfizm nie przeprowadza $(1\ 2\ 3)$ na 4. To nie jest sprzeczne z naszym rozumowaniem: jego hipoteza (że f jest homomorfizmem i $f((1\ 2\ 3)) = 4$) wtedy nigdy nie jest spełniona, więc z niej wszystko wynika!

Jak z tego wyjść? Zdefiniowaliśmy *funkcję* $f : A_4 \to \mathbb{Z}_{12}$ i teraz trzeba sprawdzić, że $f(\sigma\tau) = f(\sigma)f(\tau)$ dla wszystkich $\sigma, \tau \in A_4$. To 144 rachunki, albo 121 usuwając te z identycznością. Wykonalne, ale niewygodne. Lepiej użyć trochę technologii jak w rozwiązaniach pierwszym i drugim.

Inne podejście wykraczające poza przedmiot Pytanie filozoficzne: *dlaczego* homomorfizmy $\mathbb{Z} \cong \langle a \rangle \to G$ są zdeterminowane przez to co robią z generatorem a ? Ponieważ w grupie cyklicznej nieskończonej ten generator nie spełnia żadnej relacji, to jest, wszystkie potęgi a^n są różne.

Dlaczego homomorfizmy $\mathbb{Z}_n \cong \langle a \rangle \to G$ są zdeterminowane przez to co robią z generatorem a, jeśli tylko prześlimy go na jakiś element rzędu dzielnik n? Ponieważ w grupie cyklicznej skończonej ten generator a spełnia relację $a^n = e$, i wszystkie inne relacje z tego wynikają, na przykład jeśli $n = 7$ to $a^2 = a^9$ ale to wynika z tego, że $a^7 = e$. Więc żeby funkcja f była homomorfizmem wystarczy, aby ją wyznaczyć w generatorze i się upewnić, że relacja $a^n = e$ jest zachowana przez f, to jest, że $f(a)^n = e$, i.e. $f(a)$ ma rząd dzielnik n.

Co jeśli mamy więcej niż jeden generator? To też jest prawda! Tylko, że nie mamy technologii która pozwala nam powiedzieć co to znaczy, że wyznaczamy grupę poprzez generatory i relacje (z których wszystkie inne relacje w grupie wynikają)... Ale możemy dać prosty przykład który nie powinien zaskoczyć: $D_n = \langle r, s \rangle$, to wiemy, i wiemy, że $r^n = e$, $s^2 = e$, ale to nie wszystko, bo z tych dwóch relacji nie wynika, że $rsr = s$, a jednak to jest prawda w grupie dihedralnej! A może te trzy relacje starczą? Tak, to jest prawda. Notacja jest taka:

$$D_n = \langle r, s | r^n = e, s^2 = e, rsr = s \rangle.$$

Możecie spróbować się przekonać, że rzeczywiście inne relacje w D_n wynikają z tych, ale żeby to udowodnić formalnie, trzeba by zdefiniować pojęcie *prezentacji* grupy, i to się pojawi dopiero w Algebrze II, niestety...

Jak to pomaga w zdefiniowaniu homomorfizmów? Otóż jeśli G jest dana generatorami g_i i relacjami, to żeby zdefiniować $f : G \to H$ wystarczy wyznaczyć $f(g_i)$ i się upewnić, że zachodzą te same relacje, np. jeśli $g_1 g_2^3 = g_2 g_1^2$, to $f(g_1)f(g_2)^3 = f(g_2)f(g_1)^2$. To nie jest trudne twierdzenie jeśli już mamy definicję formalną. (Oczywiście w drugą stronę też działa, czyli jeśli f jest homomorfizmem, to zachowuje relacje.)

A więc jakbyśmy mieli prezentację A_4, to moglibyśmy z tego skorzystać, na przykład żeby dokończyć trzecie rozwiązanie, nie robiąc 121 rachunków! Jest prawdą, ale nie oczywistą, że:

$$A_4 = \langle x, y | x^2 = y^3 = (xy)^3 = e \rangle$$

oraz

$$A_4 = \langle a, b, c | a^2 = b^2 = c^3 = e, cac^{-1} = ab = ba, cbc^{-1} = a \rangle$$

Jak widzicie, prezentacje mogą być bardzo różne, i jest to bardzo trudny problem ustalić ogólnie, czy dwie grupy dane różnymi prezentacjami są izomorficznie czy nie.

W pierwszej prezentacji możemy wziąć $x = (1\,2)(3\,4)$ oraz $y = (1\,2\,3)$. W rozwiązaniu trzecim, jak już mamy kandydata na homomorfizm, wystarczy sprawdzić więc, czy $2f(x) = 0$, $3f(y) = 0$, oraz $3f(x)f(y) = 0$. Tamten f to spełnia, więc jest homomorfizmem!

Widzimy też, że przyporządkowanie $s \mapsto 0, r \mapsto 2$ we wstępie nie definiuje homomorfizmu $D_8 \to \mathbb{Z}$ dlatego, że nie zachowuje relacji $rs = sr^3$.