Grupy: torus i odometr

Na podstawie wykładu prof. T. Downarowicza

Mateusz Kwaśnicki

2 lipca 2008

Rozdział ten ma na celu przypomnienie pojęcia grupy i jej podstawowych własności oraz omówienie dwóch ważnych przykładów: torusa i odometru.

1 Definicje

Definicja 1. Trójkę $\langle G, e, m\rangle$, gdzie G jest niepustym zbiorem, $e \in G$ oraz $m : G \times G \to G$ (najczęściej zamiast $m(a, b)$ piszemy $a \cdot b$ lub po prostu ab) nazywamy *grupą*, jeśli spełnione są następujące warunki:

$$a(bc) = (ab)c \quad \text{dla wszystkich } a, b, c \in G, \tag{1a}$$

$$ea = a \quad \text{dla wszystkich } a \in G, \tag{1b}$$

$$\text{dla każdego } a \in G \text{ istnieje } a^{-1} \in G \text{ takie, że } a^{-1}a = e. \tag{1c}$$

Element a^{-1} nazywamy *odwrotnością* elementu a. Jeśli dodatkowo spełniony jest warunek:

$$ab = ba \quad \text{dla wszystkich } a, b \in G, \tag{1d}$$

to grupę nazywamy *przemienną* lub *abelową*.

Gdy z kontekstu wynika, jakie działanie mamy na myśli, mówimy po prostu „G jest grupą”. Jeśli mamy do czynienia z wieloma grupami, czasem dla jasności element neutralny grupy G oznaczamy e_G. W przypadku grup przemiennych najczęściej stosujemy notację addytywną: zamiast $m(a, b)$ oraz a^{-1} piszemy $a + b$ oraz $-a$.

Przykład 2. Grupami przemiennymi są:

- Zbiory $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ liczb całkowitych, wymiernych, rzeczywistych i zespolonych z dodawaniem jako działaniem grupowym. Elementem neutralnym jest 0.

- Przestrzeń $\mathbb{R}^n$ wektorów n-wymiarowych z dodawaniem wektorów jako działaniem.

- Zbiory $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ (względnie $\mathbb{Q}_+$, $\mathbb{R}_+$) liczb wymiernych, rzeczywistych i zespolonych różnych od zera (względnie dodatnich) z działaniem mnożenia i elementem neutralnym 1.

Gdy a, b, p są liczbami całkowitymi i $p > 0$, to oznaczmy przez $a +_p b$ resztę z dzielenia $a+b$ przez p oraz przez $a \cdot_p b$ resztę z dzielenia $a \cdot b$ przez p. Działania $+_p$ oraz $\cdot_p$ nazywamy dodawaniem i mnożeniem modulo p. Wówczas:

- Zbiór $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ z dodawaniem modulo p i elementem neutralnym 0 jest grupą przemienną.

- Zbiór $\mathbb{Z}_p^* = \{k \in \mathbb{Z}_p : \mathrm{NWD}(k, p) = 1\}$ z mnożeniem modulo p i elementem neutralnym 1 jest grupą przemienną.

Grupami nieprzemiennymi są:

- Zbiór S_A permutacji zbioru A (tj. różnowartościowych odwzorowań zbioru A na zbiór A) z operacją składania i odwzorowaniem identycznościowym jako elementem neutralnym. Grupa ta jest nieprzemienna jeśli tylko A ma co najmniej trzy elementy. Gdy $A = \{0, 1, 2, \ldots, n-1\}$, to piszemy $S_A = S_n$. Oczywiście A może być zbiorem nieskończonym (np. odcinkiem $[0, 1]$).

- Zbiór $GL_n(\mathbb{R})$ macierzy rzeczywistych $n \times n$ nieosobliwych z mnożeniem macierzy (ang. general linear group).

- Zbiór $SL_n(\mathbb{R})$ macierzy rzeczywistych $n \times n$ o wyznaczniku 1 z mnożeniem macierzy (ang. special linear group).

Zwykle zakłada się nieco mocniejsze wersje aksjomatów grupy (1). Nasza definicja jest jednak tylko pozornie uboższa od tej powszechnie stosowanej. Dowód tego faktu pozostawiamy jako ćwiczenie.

Ćwiczenie 3. Udowodnić, że jeśli G jest grupą, zaś $a \in G$, to:

$$\begin{gathered} \text{Jeśli } aa = a, \text{ to } a = e, \\ a^{-1}a = aa^{-1} = e, \\ ea = ae = a, \\ \left(a^{-1}\right)^{-1} = a. \end{gathered} \tag{2}$$

Wykazać również, że e jest jedynym elementem mającym własność (1b), zaś a^{-1} jest jedynym elementem mającym własność (1c).

Definicja 4. Niech G będzie grupą, $a \in G$. Definiujemy:

$$\begin{aligned} a^0 &= e, \\ a^{n+1} &= aa^n \quad \text{dla } n \geq 0, \\ a^{-n} &= (a^n)^{-1} \quad \text{dla } n > 0. \end{aligned}$$

Warto zauważyć, że a^{-1} ma teraz dwa znaczenia: element odwrotny dany przez (1c) oraz (-1)-sza potęga zdefiniowana w powyższym ćwiczeniu; obie definicje są jednak zgodne.

Ćwiczenie 5. Sprawdzić (metodą indukcji matematycznej), że zachodzą wzory:

$$\begin{gathered} a^{m+n} = a^m a^n, \\ a^{mn} = (a^m)^n, \\ \text{jeśli } G \text{ jest przemienna, to } (ab)^n = a^n b^n \end{gathered}$$

dla wszystkich $a, b \in G$, $m, n \in Z$.

Gdy grupa jest przemienna i stosujemy notację addytywną, piszemy na zamiast a^n. Może to prowadzić do dwuznaczności, gdy elementami grupy są liczby: $2a$ może wtedy oznaczać bądź zwykły iloczyn liczb, bądź drugą potęgę a w grupie, czyli $a +_G a$. Będziemy unikać stosowania takiego zapisu w drugim przypadku.

Definicja 6. Podzbiór H grupy G nazywamy *podgrupą*, co zapisujemy $H < G$, jeśli H z działaniem odziedziczonym z G jest grupą.

Formalnie powinniśmy napisać: trójkę $\langle H, e_H, m_H\rangle$ nazywamy podgrupą grupy $\langle G, e_G, m_G\rangle$, jeśli $H \subset G$ oraz $m_H(a,b) = m_G(a,b)$ dla wszystkich $a, b \in H$.

Ćwiczenie 7. Udowodnić, że jeśli $\langle H, e_H, m_H\rangle$ jest podgrupą $\langle G, e_G, m_G\rangle$, to $e_H = e_G$.
Wskazówka: Skorzystać ze wzoru (2).

Przykład 8. Niektóre grupy z przykładu 2 są podgrupami innych:

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C},$$
$$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*,$$
$$\mathbb{Q}_+ < \mathbb{R}_+,$$
$$\mathbb{Q}_+ < \mathbb{Q}^*, \quad \mathbb{R}_+ < \mathbb{R}^*,$$
$$SL_n(\mathbb{R}) < GL_n(\mathbb{R}).$$

Ćwiczenie 9. Udowodnić, że niepusty pozdbiór H grupy G jest podgrupą wtedy i tylko wtedy, gdy $ab^{-1} \in G$ dla wszystkich $a, b \in H$.

Jeśli zatem mamy udowodnić, że jakiś podzbiór znanej nam grupy (liczb, macierzy etc.) jest podgrupą, to wystarczy sprawdzić jeden warunek z powyższego ćwiczenia.

Ćwiczenie 10. Niech $\{H_\alpha : \alpha \in A\}$ będzie niepustą rodziną podgrup grupy G. Wykazać, że $\bigcap_{\alpha\in A} H_\alpha$ jest podgrupą grupy G. Wywnioskować stąd, że dla dowolnego podzbioru $A \subset G$ istnieje najmniejsza (w sensie relacji zawierania) podgrupa G zawierająca A.

Taką podgrupę nazywamy *podgrupą generowaną* przez A i oznaczamy (A). Jeśli $G = (A)$, to zbiór A nazywamy *zbiorem generatorów* grupy G. Jeśli A jest zbiorem jednoelementowym, to G nazywamy *grupą cykliczną*.

Ćwiczenie 11. Udowodnić, że jeżeli A jest niepustym zbiorem generatorów G, to:

$$G = \left\{a_1 a_2 \dots a_n : n \in \mathbb{Z}_+, a_i \in A \text{ lub } a_i^{-1} \in A \text{ dla } i = 1, 2, \dots, n\right\}.$$

W szczególności gdy $G = (\{a\})$ jest grupą cykliczną, to:

$$G = \{a^n : n \in \mathbb{Z}\}.$$

Ostatnie stwierdzenie często przyjmuje się za definicję grupy cyklicznej. Nieskończoną grupę cykliczną nazywamy *grupą wolną*.

Definicja 12. *Rzędem grupy* G nazywamy liczbę elementów G i oznaczamy go $|G|$. *Rzędem elementu* $a \in G$ nazywamy rząd podgrupy cyklicznej generowanej przez a. Jeśli jest to grupa wolna, to element a także nazywamy wolnym.

Wprowadzimy teraz wiele ważnych typów odwzorowań grupy w grupę.

Definicja 13. Niech G, H będą grupami. Odwzorowanie $\varphi : G \to H$ nazywamy *homomorfizmem*, jeśli

$$\varphi(ab) = \varphi(a)\varphi(b) \tag{3}$$

dla wszystkich $a, b \in G$. Wyróżniamy wiele typów homomorfizmów:

- Jeśli $\varphi(G) = H$, to φ nazywamy *faktoryzacją*, grupę H *faktorem* grupy G, a grupę G *rozszerzeniem* grupy H.
- Różnowartościowy homomorfizm nazywamy *zanurzeniem*.
- Odwracalny homomorfizm nazywamy *izomorfizmem*, a dwie grupy, między którymi istnieje izomorfizm – *grupami izomorficznymi*.
- Homomorfizm $\varphi : G \to G$ nazywamy *endomorfizmem* grupy G, zaś izomorfizm $\varphi : G \to G$ nazywamy *automorfizmem* grupy G.

Zbiór $\ker \varphi = \{a \in G : \varphi(a) = e\}$ nazywamy *jądrem* homomorfizmu φ.

Jeśli dla wszystkich faktoryzacji $\varphi, \psi : G \to H$ zachodzi $\ker \varphi = \ker \psi$, to grupę H nazywamy *faktorem kanonicznym* grupy G.

Zbiór wszystkich endomorfizmów grupy G wraz z operacją składania jest grupą oznaczaną $\operatorname{End} G$. Podobnie automorfizmy tworzą grupę ze składaniem, oznaczaną $\operatorname{Aut} G$; jest to oczywiście podgrupa grupy endomorfizmów.

Dodajmy, że w równości (3) pierwsze mnożenie jest działaniem w G, a drugie w H. Równanie to można by też zapisać w formalnie poprawniejszej, lecz dużo mniej czytelnej postaci:

$$\varphi(m_G(a, b)) = m_H(\varphi(a), \varphi(b)).$$

Przykład 14. Homomorfizmami są następujące odwzorowania:

- $\varphi : \mathbb{Z} \to \mathbb{Z}_p$, gdzie $\varphi(n)$ jest resztą z dzielenia n przez p. Jest to faktoryzacja kanoniczna o jądrze $\ker\varphi = \{pn : n \in \mathbb{Z}\} = p\mathbb{Z}$.
- $\varphi : \mathbb{R}^2 \to \mathbb{R}$ dany wzorem $\varphi(x, y) = x$. Nie jest to faktoryzacja kanoniczna, ponieważ $\psi : \mathbb{R}^2 \to \mathbb{R}$ określony przez $\psi(x, y) = y$ jest również faktoryzacją, ale $\ker\varphi \neq \ker\psi$.
- $\varphi : SL_n(\mathbb{R}) \to GL_n(\mathbb{R})$ dany wzorem $\varphi(M) = M$; φ jest zanurzeniem.
- $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ dany wzorem $\varphi(x) = |x|$; tak określony φ nie jest ani faktoryzacją, ani zanurzeniem, ani automorfizmem, ale jest endomorfizmem; $\ker\varphi = \{x \in R : |x| = 1\} = \{-1, 1\}$.

Ćwiczenie 15. Niech $\varphi : G \to H$ będzie homomorfizmem. Wykazać, że:

1. $f(e)$ jest jednością w H oraz $f(a^{-1}) = (f(a))^{-1}$.

   Wskazówka: Porównaj z zadaniem 7.

2. φ jest różnowartościowy (tzn. jest zanurzeniem) wtedy i tylko wtedy, gdy $\ker\varphi = \{e\}$.

3. $\ker\varphi$ jest podgrupą grupy G, a $\varphi(G)$ jest podgrupą grupy H.

Poniższe ćwiczenie zawiera charakteryzację grup cyklicznych.

Ćwiczenie 16. Załóżmy, że G jest grupą cykliczną generowaną przez $\{a\}$. Udowodnić, że:

- G jest izomorficzne z jedną z grup $\mathbb{Z}$, $\mathbb{Z}_p$ $(p = 1, 2, 3, \dots)$.
- Jeśli grupa H jest faktorem grupy G, to H jest cykliczna. Jeśli G jest grupą skończoną, to rząd grupy H jest dzielnikiem rzędu grupy G.
- Każda podgrupa H grupy G jest cykliczna. Jeśli G jest grupą skończoną, to rząd grupy H jest dzielnikiem rzędu grupy G. Jeśli G jest grupą wolną (ma rząd nieskończony), to także H jest grupą wolną.

Faktoryzacje kanoniczne w grupę cykliczną skończoną mają ciekawą i ważną charakteryzację:

Ćwiczenie 17. Niech p będzie liczbą naturalną oraz niech $\varphi : G \to \mathbb{Z}_p$ będzie homomorfizmem. Udowodnić, że:

1. $\ker\varphi \supset \{a^p : a \in G\}$.

2. Jeśli φ jest faktoryzacją oraz $\ker\varphi \subset \{a^p : a \in G\}$, to φ jest faktoryzacją kanoniczną.

Przyjmijmy następujące oznaczenie: jeśli G jest grupą, $g \in G$ oraz $A, B \subset G$, to $gA = \{ga : a \in A\}$, $Ag = \{ag : a \in A\}$, $AB = \{ab : a \in A, b \in B\}$.

Definicja 18. Niech H będzie podgrupą G oraz niech $g \in G$. Zbiór gH nazywamy *warstwą lewostronną* elementu g; podobnie Hg nazywamy *warstwą prawostronną* g.

Liczbę różnych warstw lewostronnych gH ($g \in G$) nazywamy *indeksem* podgrupy H w grupie G i oznaczamy $(G : H)$.

Jeśli dla każdego $g \in G$ zachodzi $gH = Hg$, to podgrupę H nazywamy *podgrupą normalną* lub *dzielnikiem normalnym*, co zapisujemy $H \triangleleft G$.

Oczywiście każda podgrupa grupy przemiennej jest podgrupą normalną. Kilka innych podstawowych własności wyżej wprowadzonych pojęć zawartych jest w następującym ćwiczeniu.

Ćwiczenie 19. Niech $H < G$. Pokazać, że:

1. Jeśli $g_1, g_2 \in G$, to warstwy g_1H oraz g_2H są albo rozłączne, albo równe. Podobnie warstwy Hg_1 i Hg_2 jeśli są różne, to są rozłączne.

2. Liczba warstw lewostronnych jest równa liczbie liczbie warstw prawostronnych.

3. Zachodzi *twierdzenie Lagrange'a*: $|G| = |H| \cdot (G : H)$ (porównaj z ćwiczeniem 16).

4. Jeśli G jest rzędu skończonego, to rząd każdej podgrupy grupy G oraz rząd każdego elementu $g \in G$ są dzielnikami $|G|$.

5. Jeśli rząd elementu $g \in G$ jest skończony, to jest to najmniejsza liczba naturalna n taka, że $g^n = e$.

6. Podgrupa H jest normalna wtedy i tylko wtedy, gdy dla każdego $g \in G$ zachodzi $gHg^{-1} \subset H$.

7. Jądro każdego homomorfizmu jest podgrupą normalną (porównaj z ćwiczeniem 15).

Przykład 20. Pokażemy, że nie wszystkie podgrupy są normalne. W tym celu rozważmy grupę S_3 permutacji zbioru $\{0,1,2\}$. Przez $\langle k_0, k_1, k_2\rangle$ rozumiemy przekształcenie przyporządkowujące liczbie i liczbę k_i. Niech $H = \{\langle 0,1,2\rangle, \langle 0,2,1\rangle\}$. Wówczas H jest podgrupą S_3. Sa trzy warstwy lewostronne względem H: H, $\{\langle 1,2,0\rangle, \langle 1,0,2\rangle\}$ oraz $\{\langle 2,0,1\rangle, \langle 2,1,0\rangle\}$; są też trzy warstwy prawostronne: H, $\{\langle 1,2,0\rangle, \langle 2,1,0\rangle\}$ i $\{\langle 2,0,1\rangle, \langle 1,0,2\rangle\}$. Jak widać, H nie jest podgrupą normalną G.

Twierdzenie 22 ukazuje kluczową własność podgrup normalnych i zarazem wyjaśnia pochodzenie nazwy *dzielnik normalny*.

Iloczyn kartezjański jest w wielu teoriach narzędziem do tworzenia bardziej złożonych i bogatszych struktur. Tak jest również w teorii grup.

Ćwiczenie 21. Załóżmy, że H_1, H_2 są podgrupami normalnymi grupy G. Mówimy, że G jest *produktem prostym* podgrup H_1, H_2, jeśli $H_1H_2 = G$ oraz $H_1 \cap H_2 = \{e\}$.

Niech G_1, G_2 będą dowolnymi grupami. Definiujemy *produkt prosty* grup G_1, G_2 jako grupę $G_1 \times G_2$ z działaniem $\langle h_1, h_2\rangle \cdot \langle h_1', h_2'\rangle = \langle h_1h_1', h_2h_2'\rangle$.

Jaki jest związek między tymi definicjami?
Wskazówka: Udowodnić, że jeśli $g_1 \in G_1$, $g_2 \in G_2$, to $g_1g_2 = g_2g_1$.

2 Podstawowe twierdzenia

Twierdzenie 22. Niech H będzie podgrupą normalną grupy G. Wówczas zbiór warstw $\{aH : a \in G\}$ z działaniem określonym wzorem:

$$(aH)\cdot(bH) = (ab)H \tag{4}$$

jest grupą.

Definicja 23. Jeśli H jest dzielnikiem normalnym grupy G, to grupę warstw elementów G względem H z działaniem określonym wzorem (4) nazywamy *grupą ilorazową* i oznaczamy symbolem G/H.

Dowód twierdzenia: Musimy udowodnić, że wzór (4) prawidłowo określa działanie i że jest to działanie grupowe.

Weźmy $a' \in aH$, $b' \in bH$. Zatem $a' = ah_1$, $b' = bh_2$ dla pewnych $h_1, h_2 \in H$. Ze względu na to, że H jest podgrupą normalną, zachodzi $Hb = bH$, a więc $h_1b = bh_3$ dla pewnego $h_3 \in H$. Zatem:

$$(a'b')H = (ah_1bh_2)H = (abh_3h_2)H = (ab)(h_3h_2H) = (ab)H.$$

Oznacza to, że jeśli $aH = a'H$ i $bH = b'H$, to $(aH) \cdot (bH) = (a'H) \cdot (b'H)$.

Ponadto działanie określone wzorem (4) spełnia aksjomaty (1), bowiem:

$$(aH)((bH)(cH)) = (a(bc))H = ((ab)c)H = ((aH)(bH))(cH),$$
$$(eH)(aH) = (ea)H = aH,$$
$$(a^{-1}H)(aH) = (a^{-1}a)H = eH, \text{ a więc } (aH)^{-1} = a^{-1}H.$$

Śledząc uważniej powyższy dowód można zauważyć, że gdy podgrupa H nie jest normalna, to wzór (4) nie określa jednoznacznie mnożenia na warstwach.

Jeśli określimy relację R na G poprzez: $aRb \Leftrightarrow a^{-1}b \in H$, to warstwa aH elementu $a \in G$ jest klasą równoważności $[a]$ elementu a względem relacji R. Pokazaliśmy, że jeśli aRa' oraz bRb' (czyli $aH = a'H$ oraz $bH = b'H$), to $abRa'b'$. Tę własność nazywa się zgodnością relacji R z mnożeniem. Wynika z niej, że $[a]\,[b] = [ab]$ dla wszystkich $a, b \in G$. W związku z tym często zamiast aH pisze się $[a]$.

Przyporządkowanie elementowi $a \in G$ jego warstwy $[a] \in G/H$ nazywane jest kanonicznym homomorfizmem grupy G w grupę ilorazową G/H. Będziemy je oznaczali literą κ.

Twierdzenie 24. O IZOMORFIZMIE. Niech G, H będą grupami, zaś $\varphi : G \to H$ homomorfizmem. Oznaczmy $K = \ker\varphi$. Wówczas grupa ilorazowa G/K jest izomorficzna z $\varphi(G)$. Ponadto izomorfizm może zostać wybrany kanonicznie w następującym sensie: istnieje izomorfizm $\psi : G/K \to H$ taki, że $\psi \circ \kappa = \varphi$.

Dowód: Określamy $\psi([a]) = \varphi(a)$. Musimy pokazać, że ψ jest poprawnie określone, tzn. wartość φ na wszystkich elementach warstwy jest taka sama, oraz że ψ jest izomorfizmem.

Jeśli $[a] = [b]$, to $a = bk$ dla pewnego $k \in K = \ker\varphi$ i $\varphi(a) = \varphi(a)\varphi(k) = \varphi(ak) = \varphi(b)$. To dowodzi poprawności określenia ψ.

Odwzorowanie ψ jest homomorfizmem, bo $\psi([a]\,[b]) = \psi([ab]) = \varphi(ab) = \varphi(a)\varphi(b) = \psi([a])\psi([b])$. Ponadto $\psi(G/K) = \varphi(G)$, więc ψ jest „na”. Jeśli $\psi([a]) = \psi([b])$, to $\varphi(a) = \varphi(b)$, czyli $\varphi(a^{-1}b) = e$. Stąd $a^{-1}b \in K$, a więc $b \in aK$, czyli $[a] = [b]$, co dowodzi różnowartościowości ψ. Zatem ψ jest izomorfizmem.

Przykład 25. Niech p będzie dodatnią liczbą całkowitą. Dla $n \in \mathbb{Z}$ niech $\varphi(n)$ będzie resztą z dzielenia n przez p. Wówczas $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ jest jest

faktoryzacją o jądrze $\ker\varphi = \{pn : n \in \mathbb{Z}\} = pZ$. Na mocy twierdzenia o izomorfizmie grupy $\mathbb{Z}/p\mathbb{Z}$ oraz $\mathbb{Z}_p$ są izomorficzne.

Ćwiczenie 26. Z twierdzenia Lagrange'a (cwiczenie 19) oraz twierdzenia o izomorfizmie wywnioskować, że jeśli grupa H jest faktorem grupy G rzędu skończonego, to rząd H jest dzielnikiem rzędu G (porównaj z ćwiczeniem 16).

3 Grupa torusa

Definicja 27. Grupę ilorazową $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ nazywamy *torusem* lub *grupą torusa*.

Torus jest izomorficzny z grupą $G = [0, 1)$ z dodawaniem modulo 1 (tzn. $a +_1 b = a + b - \lfloor a + b \rfloor$). Izomorfizmem jest przyporządkowanie $G \ni x \mapsto [x] \in \mathbb{R}/\mathbb{Z}$.

Grupa torusa jest także izomorficzna z podgrupą $H = \{z \in \mathbb{C}^* : |z| = 1\}$ grupy $\mathbb{C}^*$ niezerowych liczb zespolonych z mnożeniem. Istotnie, izomorfizm między G i H jest ustalony przez przyporządkowanie $G \ni x \mapsto e^{2\pi ix} \in H$. Zbiór H jest okręgiem jednostkowym na płaszczyźnie zespolonej, a okrąg czasem nazywa się jednowymiarowym torusem – stąd pochodzi nazwa.

W praktyce będziemy utożsamiać trzy wyżej wprowadzonye grupy i określali je wspólnie mianem torusa $\mathbb{T}$. W szczególności będziemy mówili $x \in \mathbb{T}$ oraz $z \in \mathbb{T}$, gdy $x \in [0, 1)$ oraz $z \in \mathbb{C}$, $|z| = 1$.

Ćwiczenie 28. Pokazać, że torus posiada podgrupy izomorficzne z $\mathbb{Z}_p$ ($p \geq 2$), $\mathbb{Z}$, $\mathbb{Q}$.

Ćwiczenie 29. Udowodnić, że grupa $\mathbb{Z}$ nie jest faktorem torusa. Podobnie, żadna z grup $\mathbb{Z}_p$ ($p \geq 2$) nie jest faktorem torusa.
Wskazówka: Dla wszystkich $a \in \mathbb{Z}$ zachodzi $a + a \neq 1$. Znaleźć analogiczną własność $\mathbb{Z}_p$.

Ćwiczenie 30. Sklasyfikować skończone podgrupy torusa.

4 Granica wsteczna i odometr

Pojęcie granicy wstecznej ciągu grup posłuży nam do zdefiniowania odometru.

Przyjmijmy następującą umowę: $\langle a_n \rangle$ oznacza ciąg $\langle a_1, a_2, \ldots \rangle$. Gdy φ jest odwzorowaniem określonym na zbiorze ciągów, to zamiast $\varphi(\langle a_n \rangle)$ będziemy pisać $\varphi \langle a_n \rangle$, by uniknąć zbędnego zagnieżdżania nawiasów.

Definicja 31. Niech $\langle G_n \rangle$ będzie ciągiem grup, a $\varphi_n : G_{n+1} \to G_n$ $(n = 1, 2, 3, \ldots)$ ciągiem homomorfizmów. Niech $G = G_1 \times G_2 \times \ldots$. W zbiorze G definiujemy działanie „po osiach", tzn. dla $\langle a_n \rangle, \langle b_n \rangle \in G$ określamy $\langle a_n \rangle \cdot \langle b_n \rangle = \langle a_n b_n \rangle$. Wówczas G jest grupą. Niech:

$$H = \{\langle a_n \rangle \in G : \varphi_n(a_{n+1}) = a_n \text{ dla } n = 1, 2, \ldots\}.$$

Wówczas H jest podgrupą G. Grupę H nazywamy *granicą wsteczną* ciągu $\langle G_n \rangle$, co oznaczamy $H = \varprojlim G_n$.

Ćwiczenie 32. Sprawdzić, że powyższa definicja jest poprawna, tzn. że faktycznie G jest grupą, a H jej podgrupą. Jaki jest element neutralny grupy H? Jak wygląda element odwrotny w H?

Należy dodać, że granica wsteczna zależy nie tylko od grup G_n, lecz także od homomorfizmów φ_n, co nie jest uwidocznione w notacji $\varprojlim G_n$.

Granica wsteczna podciągu ciągu grup jest izomorficzna z granicą wsteczną wyjściowego ciągu. Należy jednak sprecyzować, jakie homomorfizmy łączą kolejne wyrazy podciągu grup.

Ćwiczenie 33. Niech $\langle G_1 \rangle$ będzie ciągiem grup, $\langle \varphi_n \rangle$ odpowiednim ciągiem homomorfizmów. Niech $\langle k_n \rangle$ będzie ściśle rosnącym ciągiem indeksów. Określmy $\psi_n : G_{k_{n+1}} \to G_{k_n}$ poprzez $\psi_n = \varphi_{k_n} \circ \varphi_{k_n+1} \circ \cdots \circ \varphi_{k_{n+1}-1}$. Wskazać izomorfizm między granicą wsteczną $\varprojlim G_n$ względem φ_n oraz granicą wsteczną $\varprojlim G_{k_n}$ względem ψ_n.

Definicja 34. Niech $\langle p_n \rangle$ będzie ściśle rosnącym ciągiem liczb spełniającym warunek $p_n | p_{n+1}$. Niech $G_n = \mathbb{Z}_{p_n}$. Niech $\varphi_n(a)$ oznacza resztę z dzielenia a przez p_n. *Odometrem* o bazie $\langle p_n \rangle$ nazywamy granicę wsteczną ciągu $\langle G_n \rangle$ i oznaczamy $\Delta_{\langle p_n \rangle} = \varprojlim G_n$; ciąg $\langle p_n \rangle$ spełniający warunek $p_n | p_{n+1}$ dla wszystkich n nazywamy *bazą odometru*.

Zatem odometr o bazie $\langle p_n \rangle$ to zbiór ciągów $\langle a_n \rangle$ liczb naturalnych takich, że $0 \leq a_n < p_n$ oraz $a_{n+1} \equiv a_n \pmod{p_n}$ (tzn. $a_{n+1} - a_n$ jest wielokrotnością

p_n). Działaniem jest dodawanie „po osiach", przy czym na n-tej osi (lub n-tej współrzędnej) jet to dodawanie modulo p_n.

Ćwiczenie 35. Niech ciąg $\langle p_n \rangle$ będzie bazą odometru $\Delta_{\langle p_n \rangle}$. Określmy $q_n = \frac{p_n}{p_{n-1}}$ dla $n = 1, 2, \ldots$, przyjmując dla wygody $p_0 = 1$. Niech $\Delta'_{\langle p_n \rangle}$ będzie zbiorem ciągów $\langle a_n \rangle$ liczb naturalnych takich, że $0 \leq a_n < q_n$. W $\Delta'_{\langle p_n \rangle}$ wprowadzamy działanie w następujący sposób. Niech $\langle a_n \rangle, \langle b_n \rangle \in \Delta'_{\langle p_n \rangle}$. Określmy indukcyjnie:

$$\begin{aligned} t_0 &= 0, \\ s_n &= a_n + b_n + t_{n-1}, \\ t_n &= \left\lfloor \frac{s_n}{q_n} \right\rfloor, \\ c_n &= s_n - t_n q_n \end{aligned}$$

dla $n = 1, 2, \ldots$. Piszemy $\langle a_n \rangle + \langle b_n \rangle = \langle c_n \rangle$. Pokazać, że tak określone dodawanie jest działaniem grupowym oraz że $\Delta_{\langle p_n \rangle}$ oraz $\Delta'_{\langle p_n \rangle}$ są izomorficzne. Wywnioskować stąd, że odometr jest grupą nieprzeliczalną, mocy continuum.

Dodawanie w $\Delta'_{\langle p_n \rangle}$ ma bardzo prostą interpretację. Przyjmijmy na początek, że $q_n = 10$ dla każdego n. Wypiszmy wyrazy ciągów $\langle a_n \rangle, \langle b_n \rangle \in \Delta'_{\langle p_n \rangle}$ w następujący sposób:

$$\begin{array}{ccccc} \ldots & a_4 & a_3 & a_2 & a_1 \\ \ldots & b_4 & b_3 & b_2 & b_1. \end{array}$$

Aby uzyskać ciąg $\langle c_n \rangle = \langle a_n \rangle + \langle b_n \rangle$ musimy dodać powyższe ciągi tak, jak dodajemy liczby; t_n jest przeniesieniem (tym, co mamy w pamięci), a c_n cyfrą jedności sumy a_n, b_n i przeniesienia. Gdy q_n jest dowolne, postępujemy podobnie, w n-tym kroku przyjmując, że liczby są zapisane w systemie o podstawie q_n.

Ze wzlgędu na izomorfizm między $\Delta_{\langle p_n \rangle}$i $\Delta'_{\langle p_n \rangle}$ odometr nazywa się czasem *grupą $\langle p_n \rangle$-adyczną*. Będziemy mówili, że ciąg $\langle a_n \rangle \in \Delta_{\langle p_n \rangle}$ jest elementem odometru zapisanym klasycznie, a ciąg $\langle a_n \rangle \in \Delta'_{\langle p_n \rangle}$ jest elementem odometru zapisanym adycznie.

Przykład 36. Niech $p_n = 2^n$. Wówczas $q_n = 2$.

- W notacji klasycznej:

$$\langle 1, 3, 3, 11, 27, 59, \ldots \rangle + \langle 0, 2, 6, 6, 22, 22, \ldots \rangle = \langle 1, 1, 1, 1, 17, 17, \ldots \rangle .$$

- To samo działanie w notacji adycznej:

$$\langle 1,1,0,1,1,1,\ldots\rangle + \langle 0,1,1,0,1,0,\ldots\rangle = \langle 1,0,0,0,1,0,\ldots\rangle\,.$$

Choć notacja adyczna jest bardziej intuicyjna, w dowodach wygodniejsza jest klasyczna, ze względu na prostotę działania.

Zauważmy jeszcze, że odometr jest pewnym uogólnieniem grup cyklicznych skończonych $\mathbb{Z}_p$. Odrzućmy bowiem w definicji odometru warunek ścisłej monotoniczności ciągu $\langle p_n\rangle$, żądając jedynie, by $p_n|p_{n+1}$. Otrzymany twór nazywać będziemy odometrem uogólnionym. Jeśli $\lim p_n = \infty$, to nie otrzymamy niczego nowego: z ciągu $\langle p_n\rangle$ można wybrać ściśle rosnący podciąg $\langle p_{k_n}\rangle$ i na mocy ćwiczenia 33 uogólniony odometr $\Delta_{\langle p_n\rangle}$jest izomorficzny z odometrem $\Delta_{\langle p_{k_n}\rangle}$. Jeśli jednak $p = \lim p_n$ jest skończone, to od pewnego momentu p_n jest stale równe p i wówczas $\Delta_{\langle p_n\rangle}$jest izomorficzne z $\mathbb{Z}_p$. W następnym rozdziale zobaczymy, że wiele własności grup $\mathbb{Z}_p$ przenosi się na odometry. Często dla wygody będziemy je formułować dla odometrów uogólnionych.

5* Własności odometru

W tym rozdziale udowodnimy szereg twierdzeń o faktoryzacjach odometru w grupy cykliczne i odometry oraz podgrupach odometru. Niestety wiele twierdzeń ma dość skomplikowane i długie dowody. Potrzebne nam będą pewne fakty z elementarnej teorii liczb, których udowodnienie pozostawiamy jako ćwiczenie. Wcześniej jednak ustalmy pewne oznaczenia.

Niech $p > 0$. Zdanie $p|a$ oznacza, że p jest dzielnikiem a. Piszemy $a \equiv b \pmod p$ jeśli a i b dają te same reszty modulo p, czyli $p|a-b$. Największy wspólny dzielnik liczb a, b oznaczamy $\mathrm{NWD}(a,b)$. Mówimy, że dwie liczby są względnie pierwsze, jeśli ich największym wspólnym dzielnikiem jest 1 lub, równoważnie, nie mają wspólnego czynnika pierwszego.

Ćwiczenie 37. Udowodnić, że jeśli $p, q > 0$, $a, b, a', b' \in \mathbb{Z}$, to:

$$\begin{array}{l} a \equiv b,\ a' \equiv b' \quad\Rightarrow\quad a + a' \equiv b + b',\ aa' \equiv bb' \pmod p, \\ a \equiv b \pmod{pq} \quad\Rightarrow\quad a \equiv b \pmod p, \\ aq \equiv bq \pmod{pq} \quad\Leftrightarrow\quad a \equiv b \pmod p, \\ c \text{ i } p \text{ są względnie pierwsze} \quad\Rightarrow\quad \exists_{c^{-1}\in\mathbb{Z}_p}\ cc^{-1} \equiv 1, \\ c \text{ i } p \text{ są względnie pierwsze}, \quad ac \equiv bc \quad\Rightarrow\quad a \equiv c \end{array} \tag{5}$$

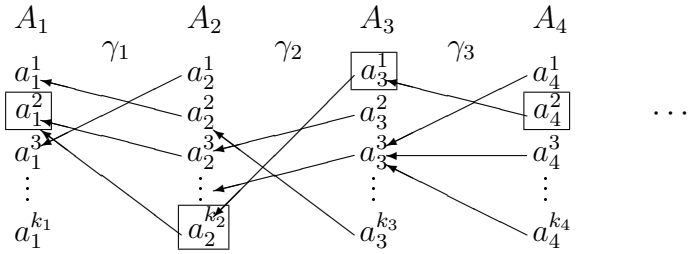
Ponadto c^{-1} w czwartym wzorze jest wyznaczony jednoznacznie. Liczba c^{-1} jest nazywana *odwrotnością c modulo p*.

Ze wzorów (5) będziemy korzystać bez dodatkowego komentarza.

W badaniu własności odometru pomocny będzie lemat o strzałkach, z pozoru odległy od algebry.

Lemat 38. O STRZAŁKACH. Niech $\langle A_n \rangle$ będzie ciągiem niepustych zbiorów skończonych. Niech $\gamma_n : A_{n+1} \to A_n$ będzie dowolnym ciągiem odwzorowań. Wówczas istnieje ciąg $\langle b_n \rangle$ taki, że $b_n \in A_n$ oraz $\gamma_n(b_{n+1}) = b_n$ dla $n = 1, 2, \ldots$.

Niech $A_n = \left\{a_n^1, a_n^2, \ldots, a_n^{k_n}\right\}$. Lemat mówi, że jeśli narysujemy tablicę liczb a_n^i i połączymy strzałką każdy element $(n+1)$-szej kolumny z dokładnie jednym elementem z n-tej kolumny (dokładniej, łączymy a_{n+1}^i z $\gamma_n(a_{n+1}^i)$), to będziemy mogli wybrać nieskończony ciąg strzałek takich, że następna kończy się tam, gdzie poprzednia się zaczyna.



Dowód polega na wskazaniu sposobu wyboru kolejnych strzałek.

Dowód lematu: Aby uprościć zapis dowodu, zdefiniujmy dodatkowo zbiór $A_0 = \{a_0\}$ jako dowolny zbiór jednoelementowy oraz funkcję $\gamma_0 : A_1 \to A_0$ w jedyny możliwy sposób, tzn. $\gamma_0(a) = a_0$ dla wszystkich $a \in A_1$.

Dla $0 \leq n < m$ określmy $\Gamma_{n,m} : A_m \to A_n$ jako złożenie $\Gamma_{n,m} = \gamma_n \circ \gamma_{n+1} \circ \cdots \circ \gamma_{m-1}$. Oczywiście teraz $\Gamma_{n,k} \circ \Gamma_{k,m} = \Gamma_{n,m}$, o ile $0 \leq n < k < m$, oraz $\Gamma_{n-1,m} = \gamma_{n-1} \circ \Gamma_{n,m}$ dla $0 < n < m$.

Określmy indukcyjnie ciąg b_n oraz pomocnicze zbiory B_n poprzez:

$$b_0 = a_0,$$
$$B_n = \left\{b \in A_n : \gamma_{n-1}(b) = b_{n-1}, \forall_{m>n}\ \exists_{a \in A_m}\ b = \Gamma_{n,m}(a)\right\},$$
$$b_n \in B_n \quad \text{– dowolny element}$$

dla $n > 0$. Zbiór B_n zawiera wszystkie te elementy zbioru A_n, które są połączone strzałką z b_{n-1} oraz gwarantują możliwość dalszego wyboru strzałek. Tak określony ciąg $\langle b_n \rangle$ ma oczywiście żądaną własność, pozostaje zatem

tylko udowodnić poprawność tej definicji. Wystarczy pokazać, że w każdym kroku zbiór B_n jest niepusty, dzięki czemu możliwy jest wybór b_n.

Załóżmy zatem przeciwnie, że B_n jest zbiorem pustym. To oznacza, że dla każdego $b \in \gamma_{n-1}^{-1}(\{b_{n-1}\})$ istnieje indeks m_b taki, że $b \notin \Gamma_{n,m_b}(A_{m_b})$. Ale b przebiega zbiór skończony, więc istnieje takie m, że $m \geq m_b$ dla wszystkich rozważanych b. Wówczas dla każdego $b \in \gamma_{n-1}^{-1}(\{b_{n-1}\})$:

$$b \notin \Gamma_{n,m_b}(A_{m_b}) \supset \Gamma_{n,m_b} \circ \Gamma_{m_b,m}(A_m) = \Gamma_{n,m}(A_m).$$

Oznacza to, że:

$$\gamma_{n-1}^{-1}(\{b_{n-1}\}) \cap \Gamma_{n,m}(A_m) = \emptyset,$$

czyli:

$$b_{n-1} \notin \gamma_{n-1} \circ \Gamma_{n,m}(A_m) = \Gamma_{n-1,m}(A_m).$$

Jeśli $n = 1$ jest to niemożliwe, bo $\Gamma_{n-1,m}(A_m) = \{a_0\} = \{b_{n-1}\}$. Gdy $n > 1$, to jest to sprzeczne z definicją b_{n-1} oraz B_{n-1}. Zatem założenie $B_n = \emptyset$ musiało być fałszywe, co kończy dowód.

Do końca tego rozdziału zakładamy, że $\langle p_n \rangle$ jest ustaloną bazą odometru $\Delta_{\langle p_n \rangle}$.

Lemat 39. Niech dane będą liczby a_n oraz $q > 0$. Jeśli dla wszystkich $n > 0$ zachodzi:

$$qa_{n+1} \equiv qa_n \pmod{p_n},$$

to istnieje ciąg $\langle b_n \rangle \in \Delta_{\langle p_n \rangle}$ taki, że $qb_n \equiv qa_n \pmod{p_n}$.

Inaczej tezę lematu można sformułować następująco. Niech c_n będzie resztą z dzielenia qa_n przez p_n. Jeśli $\langle c_n \rangle \in \Delta_{\langle p_n \rangle}$, to istnieje $\langle b_n \rangle \in \Delta_{\langle p_n \rangle}$ taki, że $q \langle b_n \rangle = \langle c_n \rangle$. Należy dodać, że ogólnie $\langle b_n \rangle \neq \langle a_n \rangle$, o czym świadczy następujący przykład.

Przykład 40. Niech $p_n = 2^n$, $a_1 = 0$, $a_n = 1$ dla $n > 1$, $q = 2$. Wówczas:

$$\langle c_n \rangle = \langle qa_n \rangle = \langle 0, 2, 2, \ldots \rangle \in \Delta_{\langle p_n \rangle},$$

lecz:

$$\langle a_n \rangle = \langle 0, 1, 1, \ldots \rangle \notin \Delta_{\langle p_n \rangle}.$$

Właściwym ciągiem $\langle b_n \rangle$ jest tutaj ciąg jedynek.

Dowód lematu: Niech $A_n = \{a \in \mathbb{Z}_{p_n} : qa \equiv qa_n \pmod{p_n}\}$. Zbiory A_n są skończone i niepuste (bo reszta z dzielenia a_n przez p_n jest elementem A_n).

Niech $\gamma_n(a)$ oznacza resztę z dzielenia a przez p_n. Zauważmy, że $\gamma_n : A_{n+1} \to A_n$. Istotnie, jeśli $a \in A_{n+1}$, to:

$$qa \equiv qa_{n+1} \pmod{p_{n+1}},$$

a więc również:

$$q\gamma_n(a) \equiv qa \equiv qa_{n+1} \equiv qa_n \pmod{p_n},$$

czyli $\gamma_n(a) \in A_n$.

Możemy więc skorzystać z lematu o strzałkach. W efekcie otrzymujemy ciąg $\langle b_n \rangle \in \Delta_{\langle p_n \rangle}$ taki, że $b_n \in A_n$, czyli:

$$qb_n \equiv qa_n \pmod{p_n}$$

tak, jak żądaliśmy.

Wniosek 41. Jeśli p jest liczbą względnie pierwszą z p_n dla każdego n, to dzielenie przez p jest wykonalne w odometrze $\Delta_{\langle p_n \rangle}$.

Dowód: Niech i_n będzie odwrotnością p modulo p_n (a więc taką liczbą, że $pi_n \equiv 1 \pmod{p_n}$). Weźmy dowolny $\langle c_n \rangle \in \Delta_{\langle p_n \rangle}$. Oznaczmy $a_n = i_n c_n$. Wówczas $pa_n = pi_n c_n \equiv c_n \pmod{p_n}$, czyli na mocy udowodnionego lematu istnieje ciąg $\langle b_n \rangle \in \Delta_{\langle p_n \rangle}$ taki, że $pb_n \equiv pa_n \equiv c_n \pmod{p_n}$, co kończy dowód.

Teraz zbadamy się faktoryzacje odometru w grupy cykliczne.

Twierdzenie 42. Niech $\varphi : \Delta_{\langle p_n \rangle} \to \mathbb{Z}_p$ będzie faktoryzacją. Wówczas dla pewnego n zachodzi $p | p_n$.

Dowód: Rozumowanie podzielimy na cztery części.

1. Niech $q_n = \mathrm{NWD}(p, p_n)$ oraz $q = \lim q_n$. Granica istnieje, ponieważ ciąg q_n jest niemalejący (nawet $q_n | q_{n+1}$) i ograniczony przez p. Jest to ciąg liczb całkowitych, więc od pewnego miejsca jest stały. Niech więc k będzie tak duże, że $q = q_k = \mathrm{NWD}(p, p_k)$. Pokażemy, że $q = p$. Wówczas $p | p_k$ tak, jak chcieliśmy.

2. Ustalmy n. Liczby $\frac{p}{q_n}$ i $\frac{p_n}{q_n}$ są całkowite i względnie pierwsze, więc istnieje odwrotność pierwszej modulo druga, tzn. liczba i_n taka, że:

$$\frac{p}{q_n} i_n \equiv 1 \pmod{\frac{p_n}{q_n}}.$$

Stąd:

$$pi_n \equiv q_n \pmod{p_n}.$$

Zauważmy, że $q_n|q$. Niech $j_n = \frac{q}{q_n} i_n$. Wówczas:

$$pj_n \equiv q \pmod{p_n}.$$

Wobec tego, że $p_n|p_{n+1}$, zachodzi:

$$qj_{n+1} \equiv (pj_n)j_{n+1} = (pj_{n+1})j_n \equiv qj_n \pmod{p_n}.$$

3. Ustalmy dowolny ciąg $\langle a_n \rangle \in \Delta_{\langle p_n \rangle}$. Niech $\widetilde{a}_n = j_n a_n$. Wówczas:

$$q\widetilde{a}_{n+1} = (qj_{n+1})a_{n+1} \equiv (qj_n)a_n \equiv q\widetilde{a}_n \pmod{p_n},$$

zatem możemy zastosować lemat 39 dla ciągu $\langle \widetilde{a}_n \rangle$ i q. Otrzymamy ciąg $\langle b_n \rangle \in \Delta_{\langle p_n \rangle}$ taki, że $qb_n \equiv q\widetilde{a}_n \pmod{p_n}$. Stąd:

$$pb_n = \frac{p}{q} qb_n \equiv \frac{p}{q} q\widetilde{a}_n \equiv pj_n a_n \equiv qa_n \pmod{p_n},$$

co oznacza, że $p \cdot \langle b_n \rangle = q \cdot \langle a_n \rangle$.

4. Wybierzmy w poprzednim kroku $\langle a_n \rangle \in \Delta_{\langle p_n \rangle}$ tak, by $\varphi \langle a_n \rangle = 1$. Wówczas:

$$0 \equiv p \cdot \varphi \langle b_n \rangle \equiv q \cdot \varphi \langle a_n \rangle \equiv q \pmod{p}.$$

Oznacza to, że $p|q$. Ale $q = \mathrm{NWD}(p, p_k)$, więc również $q|p$. Stąd $p = q$, co kończy dowód.

Twierdzenie 43. Niech p będzie dzielnikiem p_k dla pewnego k. Niech $\varphi \langle a_n \rangle$ będzie resztą z dzielenia a_k przez p. Wówczas $\varphi : \Delta_{\langle p_n \rangle} \to \mathbb{Z}_p$ jest kanoniczną faktoryzacją o jądrze:

$$\ker \varphi = \left\{ \langle a_n \rangle \in \Delta_{\langle p_n \rangle} : p|a_k \right\}. \tag{6}$$

Dowód: Sprawdzenie, że φ jest faktoryzacją pozostawiamy jako ćwiczenie. Pozostaje pokazać kanoniczność φ. Zgodnie z ćwiczeniem 17 wystarczy pokazać, że jeśli $\langle a_n \rangle \in \ker \varphi$, to istnieje $\langle b_n \rangle \in \Delta_{\langle p_n \rangle}$ taki, że $p_k \cdot \langle b_n \rangle = \langle a_n \rangle$.

Weźmy zatem $\langle a_n \rangle \in \ker \varphi$. Wówczas $p|a_k$. Dla $n > k$ zachodzi $a_k \equiv a_n \pmod{p_k}$, więc również $p|a_n$. Niech $a_n = p\widetilde{a}_n$ dla $n \geq k$. Określmy dodatkowo $\widetilde{a}_n = \widetilde{a}_k$ dla $n < k$. Zachodzi:

$$p\widetilde{a}_n \equiv a_n \pmod{p_n}$$

dla wszystkich n. Istotnie, dla $n \geq k$ powyższe przystawanie jest równością, a dla $n < k$ wynika z następującego rachunku:

$$p\widetilde{a}_n = p\widetilde{a}_k = a_k \equiv a_n \pmod{p_n}.$$

Zatem:

$$p\widetilde{a}_{n+1} \equiv a_{n+1} \equiv a_n \equiv p\widetilde{a}_n \pmod{p_n}.$$

Możemy zatem zastosować lemat 39 do ciągu $\langle \widetilde{a}_n \rangle$ i liczby p. Otrzymujemy ciąg $\langle b_n \rangle \in \Delta_{\langle p_n \rangle}$ taki, że: $pb_n \equiv p\widetilde{a}_n = a_n \pmod{p_n}$, tzn. $p \cdot \langle b_n \rangle = \langle a_n \rangle$.

Wniosek 44. Dla każdego n grupa $\mathbb{Z}_{p_n}$ jest faktorem kanonicznym odometru $\Delta_{\langle p_n \rangle}$. Jądrem każdej faktoryzacji $\Delta_{\langle p_n \rangle}$ w $\mathbb{Z}_{p_n}$ jest zbiór tych ciągów $\langle a_n \rangle \in \Delta_{\langle p_n \rangle}$, że $a_1 = a_2 = \cdots = a_n = 0$.

Twierdzenie 45. Grupa $\mathbb{Z}$ nie jest faktorem odometru $\Delta_{\langle p_n \rangle}$.

Dowód: Załóżmy wbrew tezie, że $\varphi : \Delta_{\langle p_n \rangle} \to \mathbb{Z}$ jest faktoryzacją. Ustalmy k. Niech $\kappa_k : \mathbb{Z} \to \mathbb{Z}_{p_k}$ będzie faktoryzacją (na przykład niech $\kappa_k(a)$ będzie resztą z dzielenia a przez p_k). Określmy $\varphi_k = \kappa_k \circ \varphi$. Wówczas $\varphi_k : \Delta_{\langle p_n \rangle} \to \mathbb{Z}_{p_k}$ jest faktoryzacją $\Delta_{\langle p_n \rangle}$w $\mathbb{Z}_{p_k}$. Na mocy wniosku 44 φ_k jest faktoryzacją kanoniczną i ma jądro:

$$\ker \varphi_k = \left\{ \langle a_n \rangle \in \Delta_{\langle p_n \rangle} : a_1 = a_2 = \cdots = a_k = 0 \right\}.$$

Jeśli $\varphi \langle a_n \rangle = 0$, to także $\varphi_k \langle a_n \rangle = \kappa_k(0) = 0$, więc $\ker \varphi \subset \ker \varphi_k$. Tak jest dla każdego k, więc:

$$\ker \varphi \subset \bigcap_{k=1}^{\infty} \ker \varphi_k = \{ \langle 0, 0, \ldots \rangle \}.$$

Oznacza to, że φ jest izomorfizmem. Jest to niemożliwe, bo zbiór $\mathbb{Z}$ jest przeliczalny, a $\Delta_{\langle p_n \rangle}$nie.

Analogiczne wyniki są prawdziwe także dla faktoryzacji odometru $\Delta_{\langle p_n \rangle}$w odometr $\Delta_{\langle q_n \rangle}$.

Twierdzenie 46. Jeśli odometr $\Delta_{\langle q_n \rangle}$ jest faktorem odometru $\Delta_{\langle p_n \rangle}$, to spełniony jest następujący warunek:

$$\text{dla każdego } n \text{ istnieje } m \text{ takie, że } q_n | p_m. \tag{7}$$

Dowód: Załóżmy, że $\varphi : \Delta_{\langle p_n \rangle} \to \Delta_{\langle q_n \rangle}$ jest faktoryzacją. Ustalmy k. Niech $\psi_k : \Delta_{\langle q_n \rangle} \to \mathbb{Z}_{q_k}$ będzie faktoryzacją daną wzorem $\psi_k \langle b_n \rangle = b_k$. Niech $\varphi_k = \psi_k \circ \varphi$. Wówczas φ_k jest faktoryzacją $\Delta_{\langle p_n \rangle}$w $\mathbb{Z}_{q_k}$, więc, na mocy twierdzenia 42, dla pewnego m zachodzi $q_k | p_m$. Wobec dowolności k, zachodzi warunek (7).

Twierdzenie 47. Jeśli warunek (7) jest spełniony, to $\Delta_{\langle q_n \rangle}$ jest faktorem kanonicznym odometru $\Delta_{\langle p_n \rangle}$ i jądrem każdej faktoryzacji jest:

$$\left\{ \langle a_n \rangle \in \Delta_{\langle p_n \rangle} : \text{ dla każdego } n \text{ istnieje } m \text{ takie, że } q_n | a_m \right\}. \tag{8}$$

Dowód: Załóżmy, że warunek (7) jest spełniony. Skonstruujemy faktoryzację w kilku krokach.

1. Dla każdego n dobierzmy m_n tak, by $q_n | p_{m_n}$, żądając dodatkowo, by m_n był ciągiem ściśle rosnącym (możemy tak zrobić, bo $\langle p_n \rangle$ jest bazą odometru). Niech $p'_n = p_{m_n}$. Określimy faktoryzację $\varphi : \Delta_{\langle p_n \rangle} \to \Delta_{\langle q_n \rangle}$ jako złożenie dwóch faktoryzacji: $\sigma : \Delta_{\langle p_n \rangle} \to \Delta_{\langle p'_n \rangle}$ oraz $\tau : \Delta_{\langle p'_n \rangle} \to \Delta_{\langle q_n \rangle}$.

2. Niech $\sigma \langle a_n \rangle = \langle a_{m_n} \rangle$; σ jest izomorfizmem (porównaj z ćwiczeniem 33). W szczególności σ jest faktoryzacją.

3. Niech $\tau_k : \Delta_{\langle p'_n \rangle} \to \mathbb{Z}_{q_k}$ będzie kanoniczną faktoryzacją taką, jak w twierdzeniu 43, tzn. niech $\tau_k \langle a_n \rangle$ będzie resztą z dzielenia a_k przez q_k. Definiujemy $\tau : \Delta_{\langle p'_n \rangle} \to \Delta_{\langle q_n \rangle}$ wzorem:

   $$\tau \langle a_n \rangle = \langle \tau_n \langle a_n \rangle \rangle = \langle \tau_1 \langle a_n \rangle, \tau_2 \langle a_n \rangle, \ldots \rangle.$$

   Ze względu na $q_k | q_{k+1}$ oraz $q_k | p'_k$ zachodzi:

   $$\tau_{k+1} \langle a_n \rangle \equiv a_{k+1} \equiv a_k \equiv \tau_k \langle a_n \rangle \pmod{q_k},$$

   więc istotnie $\tau \langle a_n \rangle \in \Delta_{\langle q_n \rangle}$. Ponieważ każde τ_k jest homomorfizmem, więc również τ jest homomorfizmem. Trzeba wykazać, że τ jest „na”. Skorzystamy z lematu o strzałkach.

4. Niech $\langle a_n \rangle \in \Delta_{\langle q_n \rangle}$. Określmy:

$$A_n = \left\{ a \in \mathbb{Z}_{p'_n} : a \equiv a_n \pmod{q_n} \right\}$$

i niech $\gamma_n(a)$ oznacza resztę z dzielenia a przez p'_n. Weźmy $a \in A_{n+1}$. Ponieważ $q_n | q_{n+1}$, więc $a \equiv a_{n+1} \pmod{q_n}$. Wobec $q_n | p'_n$ otrzymujemy $\gamma_n(a) \equiv a \pmod{q_n}$. Ponadto $\langle a_n \rangle \in \Delta_{\langle q_n \rangle}$, więc $a_{n+1} \equiv a_n \pmod{q_n}$. Zatem:

$$\gamma_n(a) \equiv a \equiv a_{n+1} \equiv a_n \pmod{q_n},$$

czyli $\gamma_n : A_{n+1} \to A_n$.

5. Możemy zatem zastosować lemat o strzałkach dla zbiorów A_n i funkcji γ_n. Otrzymamy ciąg $\langle b_n \rangle$ taki, że $b_k \in A_k$ i $\gamma_k(b_{k+1}) = b_k$. Drugi warunek oznacza, że $b_{k+1} \equiv b_k \pmod{p'_k}$, czyli $\langle b_n \rangle \in \Delta_{\langle p'_n \rangle}$. Z pierwszy wynika, że $b_k \equiv a_k \pmod{q_k}$, a więc $\tau_k \langle b_n \rangle = a_k$, czyli $\tau \langle b_n \rangle = \langle a_n \rangle$. Zatem τ jest „na". Wynika stąd, że $\varphi = \tau \circ \sigma$ jest szukaną faktoryzacją.

Pozostaje uzasadnić, że skonstruowana faktoryzacja jest kanoniczna. Grupy $\Delta_{\langle p_n \rangle}$i $\Delta_{\langle p'_n \rangle}$ są izomorficzne, więc $\Delta_{\langle q_n \rangle}$ jest faktorem kanonicznym $\Delta_{\langle p_n \rangle}$wtedy i tylko wtedy, gdy jest faktorem kanonicznym $\Delta_{\langle p'_n \rangle}$. Wystarczy zatem udodwonić, τ jest faktoryzacją kanoniczną. Rozumowanie znów podzielimy na kilka części.

1. Jądro τ ma postać:

$$\ker \tau = \left\{ \langle b_n \rangle \in \Delta_{\langle p'_n \rangle} : \tau_k \langle b_n \rangle = 0 \text{ dla wszystkich } k \right\} = \bigcap_{k=1}^{\infty} \ker \tau_k.$$

2. Określmy $\psi_k : \Delta_{\langle q_n \rangle} \to \mathbb{Z}_{q_k}$ wzorem $\psi_k \langle b_n \rangle = b_k$. Wówczas:

$$\ker \psi_k = \left\{ \langle b_n \rangle \in \Delta_{\langle q_n \rangle} : b_1 = b_2 = \cdots = b_k = 0 \right\},$$

$$\bigcap_{k=1}^{\infty} \ker \psi_k = \left\{ \langle 0, 0, \ldots \rangle \right\}.$$

3. Niech teraz $\widetilde{\tau} : \Delta_{\langle p'_n \rangle} \to \Delta_{\langle q_n \rangle}$ będzie dowolną faktoryzacją. Określmy $\widetilde{\tau}_k = \psi_k \circ \widetilde{\tau}$. Jeśli $\widetilde{\tau} \langle a_n \rangle = 0$, to $\widetilde{\tau}_k \langle a_n \rangle = 0$, więc $\ker \widetilde{\tau} \subset \ker \widetilde{\tau}_k$. Zatem:

$$\ker \widetilde{\tau} \subset \bigcap_{k=1}^{\infty} \ker \widetilde{\tau}_k.$$

Z drugiej strony załóżmy, że $\langle a_n \rangle \in \ker \widetilde{\tau}_k$ dla wszystkich k. Oznaczmy $\langle b_n \rangle = \widetilde{\tau} \langle a_n \rangle$. Wówczas $\psi_k \langle b_n \rangle = \widetilde{\tau}_k \langle a_n \rangle = 0$, czyli:

$$\langle b_n \rangle \in \bigcap_{k=1}^{\infty} \ker \psi_k = \{\langle 0, 0, \ldots \rangle\},$$

a więc $\langle a_n \rangle \in \ker \widetilde{\tau}$. Pokazaliśmy zatem, że:

$$\ker \widetilde{\tau} = \bigcap_{k=1}^{\infty} \ker \widetilde{\tau}_k.$$

4. Faktoryzacje τ_k i $\widetilde{\tau}_k$ są kanoniczne na mocy twierdzenia 43, a więc $\ker \tau_k = \ker \psi_k$ dla wszystkich k. Stąd:

$$\ker \tau = \bigcap_{k=1}^{\infty} \ker \tau_k = \bigcap_{k=1}^{\infty} \ker \widetilde{\tau}_k = \ker \widetilde{\tau}.$$

To oznacza, że τ jest faktoryzacją kanoniczną.

Własność (7) można interpretować jako swego rodzaju podzielność ciągu $\langle p_n \rangle$ przez ciąg $\langle q_n \rangle$. Pokazaliśmy, że odometr o bazie $\langle q_n \rangle$ jest faktorem odometru o bazie $\langle p_n \rangle$ wtedy i tylko wtedy, gdy $\langle q_n \rangle$ „dzieli" $\langle p_n \rangle$ (porównaj z ćwiczeniem 16).

Powyższe twierdzenie ma trzy bardzo interesujące konsekwencje, podane poniżej w formie ćwiczeń.

Ćwiczenie 48. Wskazać odometr będący wspólnym rozszerzeniem wszystkich odometrów.

Ćwiczenie 49. Pokazać, że każda faktoryzacja odometru $\Delta_{\langle p_n \rangle}$w siebie jest izomorfizmem, tzn. jeśli homomorfizm $\Delta_{\langle p_n \rangle}$ w $\Delta_{\langle p_n \rangle}$ jest „na", to jest różnowartościowy. Wskazać przykład, że przeciwna implikacja nie zawsze jest prawdziwa, tj. znaleźć odometr $\Delta_{\langle p_n \rangle}$ oraz różnowartościowy homomorfizm $\Delta_{\langle p_n \rangle}$ w $\Delta_{\langle p_n \rangle}$, który nie jest „na".

Definicja 50. Niech $\mathbb{P}$ oznacza zbiór liczb pierwszych. Jeśli $\langle p_n \rangle$ jest bazą odometru uogólnionego, to dla każdej liczby $p \in \mathbb{P}$ określamy:

$$\alpha(p) = \sup \left\langle k : p^k | p_n \text{ dla pewnego } n \right\rangle$$

(dopuszczamy oczywiście $\alpha_p = \infty$). Funkcję $\alpha : \mathbb{P} \to \mathbb{N}$ nazywamy *funkcją charakterystyczną* odometru $\Delta_{\langle p_n \rangle}$. W przypadku, gdy $\Delta_{\langle p_n \rangle}$ redukuje się do grupy cyklicznej $\mathbb{Z}_p$, mówimy także, że α jest funkcją charakterystyczną grupy $\mathbb{Z}_p$.

Ćwiczenie 51. Niech α, β będą funkcjami charakterystycznymi odometrów $\Delta_{\langle p_n \rangle}$ i $\Delta_{\langle q_n \rangle}$. Udowodnić, że:

1. odometr $\Delta_{\langle q_n \rangle}$ jest faktorem odometru $\Delta_{\langle p_n \rangle}$ wtedy i tylko wtedy, gdy $\alpha_p \geq \beta_p$ dla każdego $p \in \mathbb{P}$,

2. odometry $\Delta_{\langle p_n \rangle}$ i $\Delta_{\langle q_n \rangle}$ są izomorficzne wtedy i tylko wtedy, gdy $\alpha_p = \beta_p$ dla każdego $p \in \mathbb{P}$.

Zatem odometr jest w pełni charakteryzowany przez maksymalne wykładniki, w jakich liczby pierwsze dzielą elementy jego bazy.

Dla kompletu dodajmy, że nie wszystkie faktoryzacje odometru są odometrami uogólnionymi (tzn. odometrami lub skończonymi grupami cyklicznymi), co wynika z dalszych twierdzeń tego rozdziału (dokładniej ćwiczenia 52 i twierdzenia 55), nie ma więc pełnej analogii z grupami cyklicznymi.

W dalszej części zbadamy podgrupy odometru.

Ćwiczenie 52. Pokazać, że odometr (zakładamy ścisłą monotoniczność ciągu $\langle p_n \rangle$!) posiada podgrupę cykliczną wolną, tzn. izomorficzną z $\mathbb{Z}$.

Twierdzenie 53. Jeśli odometr $\Delta_{\langle p_n \rangle}$posiada podgrupę cykliczną rzędu p to spełniony jest następujący warunek:

$$\text{Istnieje } m \text{ takie, że } p | p_m \text{ oraz } \operatorname{NWD}\left(p, \frac{p_{n+1}}{p_n}\right) = 1 \text{ gdy } n \geq m. \qquad (9)$$

Dowód: Załóżmy, że $G < \Delta_{\langle p_n \rangle}$ jest podgrupą cykliczną rzędu p generowaną przez $\langle a_n \rangle$. Jeśli $p = 1$, to warunek (9) jest spełniony; przyjmijmy więc, że $p > 1$. Wiemy, że $G = \{k \cdot \langle a_n \rangle : k = 0, 1, \ldots, p-1\}$. Rozumowanie podzielimy na kilka kroków.

1. Niech m będzie tak duże, że liczby ka_m dają różne reszty modulo p_m dla $k = 0, 1, \ldots, p-1$. Taki wybór jest możliwy; załóżmy bowiem przeciwnie, że dla każdego n istnieje k_n takie, że $0 < k_n < p$ oraz $k_n a_n \equiv$

$0 \pmod{p_n}$. Ciąg $\langle k_n \rangle$ przyjmuje pewną wartość k nieskończenie wiele razy, a więc dla nieskończenie wielu n zachodzi $ka_n \equiv 0 \pmod{p_n}$, przez co $k \cdot \langle a_n \rangle = \langle 0, 0, \ldots \rangle$, wbrew założeniu.

2. Dla każdego $n \geq m$ liczby ka_n $(k = 0, 1, \ldots, p-1)$ dają różne reszty modulo p_n, bo $ka_n \equiv la_n \pmod{p_n}$ implikuje $ka_m \equiv la_m \pmod{p_m}$, czyli $k = l$ na mocy poprzedniego punktu.

3. Ponieważ $pa_n \equiv 0 \pmod{p_n}$, więc $pa_n = c_n p_n$ dla pewnych liczb c_n. Ponadto:

$$\frac{p}{\mathrm{NWD}(c_n, p)} a_n = \frac{c_n}{\mathrm{NWD}(c_n, p)} p_n \equiv 0 \pmod{p_n},$$

więc na mocy poprzedniego punktu $\frac{p}{\mathrm{NWD}(c_n,p)}$ jest wielokrotnością p, czyli $\mathrm{NWD}(c_n, p) = 1$.

4. Ponieważ $p_n \mid (a_{n+1} - a_n)$, więc:

$$pp_n \Big| (pa_{n+1} - pa_n) = c_{n+1}p_{n+1} - c_n p_n = \left(c_{n+1} - c_n \frac{p_{n+1}}{p_n} \right) p_n,$$

skąd $p \Big| \left(c_{n+1} - c_n \frac{p_{n+1}}{p_n} \right)$. Zatem:

$$c_{n+1} \equiv c_n \frac{p_{n+1}}{p_n} \pmod{p}.$$

Lewa strona jest względnie pierwsza z p (poprzedni punkt), więc prawa strona również. W szczególności $\mathrm{NWD}\left(p, \frac{p_{n+1}}{p_n}\right) = 1$, czyli (9).

Twierdzenie 54. Jeśli warunek (9) zachodzi, to $\Delta_{\langle p_n \rangle}$posiada jedyną podgrupę cykliczną rzędu p.

Dowód: Niech m będzie takie, jak w warunku (9). Znów teza jest oczywiście spełniona, gdy $p = 1$, rozważmy więc przypadek $p > 1$. Rozumowanie podzielimy na kilka kroków. Wyznaczymy wszystkie elementy rzędu p i pokażemy, że wszystkie generują tę samą podgrupę cykliczną.

1. Niech $A = \{a \in \mathbb{Z}_p : \mathrm{NWD}(a, p) = 1\}$. Wybierzmy $a \in A$.

2. Niech m będzie takie, jak we wzorze (9). Zdefiniujemy ciąg $\langle a_n \rangle$ tak, by $a_m = \frac{ap_m}{p}$ oraz dla wszystkich n:

$$0 \leq a_n < p_n, \quad a_{n+1} \equiv a_n \pmod{p_n}, \quad pa_n \equiv 0 \pmod{p_n}.$$

3. Określmy $a_m = \frac{ap_m}{p}$ oraz niech a_n będzie resztą z dzielenia a_m przez p_n dla $n = 1, 2, \ldots, m-1$. Zauważmy, że warunek z punktu 2 jest spełniony dla właśnie zdefiniowanych wyrazów ciągu. Pozostałą część ciągu określimy indukcyjnie.

4. Załóżmy, że określone są już $a_1, a_2, \ldots, a_n$, gdzie $n \geq m$ i spełniają one warunek z punktu 2. Rozważmy liczby:

$$a_n + kp_n \quad \text{dla } k = 0, 1, \ldots, \frac{p_{n+1}}{p_n} - 1.$$

   Wszystkie są elementami $\mathbb{Z}_{p_{n+1}}$ i wszystkie dają resztę a_n przy dzieleniu przez p_n.

   Skoro $pa_n \equiv 0 \pmod{p_n}$, więc $pa_n = c_n p_n$ dla pewnego c_n. Zatem dla $k = 0, 1, \ldots, \left(\frac{p_{n+1}}{p_n} - 1\right)$ zachodzi:

$$p(a_n + kp_n) = pa_n + kpp_n = c_n p_n + kpp_n = (c_n + kp)p_n.$$

   Ale NWD $\left(p, \frac{p_{n+1}}{p_n}\right) = 1$, więc dla $k = 0, 1, \ldots, \left(\frac{p_{n+1}}{p_n} - 1\right)$ liczby $(c_n + kp)$ dają różne reszty modulo $\frac{p_{n+1}}{p_n}$. Zatem dokładnie jedna z nich daje resztę zero. Niech więc:

$$0 \equiv c_n + k_n p \pmod{\frac{p_{n+1}}{p_n}}.$$

   Zatem:

$$0 \equiv p_n (c_n + k_n p) = p (a_n + k_n p_n) \pmod{p_{n+1}}.$$

   Zdefiniujemy $a_{n+1} = a_n + k_n p_n$. Na mocy powyższego przystawania, warunek z punktu 2 pozostaje spełniony.

5. Dla każdego $a \in A$ określiliśmy więc ciąg $\langle a_n \rangle \in \Delta_{\langle p_n \rangle}$ taki, że $p \cdot \langle a_n \rangle = \langle 0, 0, \ldots \rangle$. Ponadto dla $0 < k < p$ liczba p nie jest dzielnikiem ka, więc p_m nie jest dzielnikiem $\frac{kap_m}{p} = ka_m$, czyli $k \cdot \langle a_n \rangle \neq \langle 0, 0, \ldots \rangle$. Oznacza to, że $\langle a_n \rangle$ jest elementem rzędu p.

6. Warunek z punktu 2 jest konieczny na to, by $\langle a_n \rangle$ był elementem rzędu p. Ponieważ jednak wybór k_n był jednoznaczny, więc $\langle a_n \rangle$ jest zdeterminowany przez wartość m-tego wyrazu.

7. W punkcie 3. dowodu twierdzenia 53 wykazaliśmy, że jeśli $\langle b_n \rangle$ jest elementem rzędu p, to $pb_m = c_m p_m$ dla pewnego $c_m \in A$. Zatem skonstruowaliśmy wszystkie elementy rzędu p odometru $\Delta_{\langle p_n \rangle}$.

8. Liczba elementów rzędu p w każdej grupie cyklicznej rzędu p jest równa mocy zbioru A, zatem rozważany odometr może posiadać tylko jedną podgrupę cykliczną rzędu p. To kończy dowód twierdzenia.

Warunek (9) można dużo prościej wyrazić w języku funkcji charakterystycznych. Jeśli α, γ oznaczają funkcje charakterystyczne $\Delta_{\langle p_n \rangle}$ i $\mathbb{Z}_p$, to $\Delta_{\langle p_n \rangle}$ posiada podgrupę izomorficzną z $\mathbb{Z}_p$ wtedy i tylko wtedy, gdy:

$$\begin{gathered} \gamma(p) \leq \alpha(p) \quad \text{dla każdego } p \in \mathbb{P}, \\ \alpha(p) = \infty \quad \Rightarrow \quad \gamma(p) = 0. \end{gathered}$$

Można pokazać, że skonstruowana powyżej podgrupa cykliczna jest jądrem (kanonicznej) faktoryzacji odometru $\Delta_{\langle p_n \rangle}$w odometr $\Delta_{\langle q_{m+n} \rangle}$, gdzie $q_n = \frac{p_n}{p}$ dla $n \geq m$. W istocie można pokazać dużo więcej.

Przypomnijmy, że grupę cykliczną $\mathbb{Z}_p$ możemy utożsamiać z odometrem uogólnionym o bazie $\langle p_n \rangle$, gdzie $p_n = p$.

Twierdzenie 55. Załóżmy, że odometr uogólniony $\Delta_{\langle q_n \rangle}$, jest faktorem $\Delta_{\langle p_n \rangle}$. Wówczas jądro każdej faktoryzacji $\Delta_{\langle p_n \rangle}$ w $\Delta_{\langle q_n \rangle}$ (dane wzorem (8)) jest izomorficzne z pewnym odometrem uogólnionym.

Dokładniej, faktoryzacja odometru $\Delta_{\langle p_n \rangle}$ w odometr uogólniony o bazie $\langle q_n \rangle$ ma jądro izomorficzne z odometrem uogólnionym o bazie $\langle s_n \rangle$, gdzie:

$$s_k = \frac{p_k}{\lim_{n \to \infty} \mathrm{NWD}(p_k, q_n)}.$$

Dowód: Znów podzielimy rozumowanie na pewną liczbę części.

1. Faktoryzacja $\Delta_{\langle p_n \rangle}$ w $\Delta_{\langle q_n \rangle}$ jest kanoniczna na mocy twierdzeń 43 oraz 47. Ponadto dla każdego n istnieje m_n taki, że $q_n | p_{m_n}$; bez straty ogólności możemy przyjąć, że $\langle m_n \rangle$ jest ściśle rosnący. Niech $p'_n = p_{m_n}$;

a więc $q_n | p'_n$. Ponadto p'_n jest właściwym dzielnikiem p'_{n+1}, czyli $\langle p'_n \rangle$ jest bazą odometru, izomorficznego na mocy cwiczenia 33 z odometrem $\Delta_{\langle p_n \rangle}$.

2. Ustalmy k. Ciąg $\mathrm{NWD}(p'_k, q_n)$ jest niemalejący i ograniczony przez p'_k, więc jest stały od pewnego miejsca. Niech więc N_k będzie najmniejszą taką liczbą, że dla $n \geq N_k$ będzie $\mathrm{NWD}(p'_k, q_n) = \mathrm{NWD}(p'_k, q_{N_k})$ i oznaczmy $\mathrm{NWD}(p'_k, q_{N_k}) = q'_k$. Ciąg N_k jest niemalejący (bo $p'_k | p'_{k+1}$).

3. Oczywiście $q'_k | p'_k$, więc $p'_k = q'_k r_k$ dla pewnego r_k. Niech $n \geq N_{k+1}$. Zachodzi:
$$q'_k = \mathrm{NWD}(p'_k, q_n) | \, \mathrm{NWD}(p'_{k+1}, q_n) = q'_{k+1},$$
więc $\langle q'_n \rangle$ jest bazą odometru uogólnionego. Ponadto:
$$\frac{r_{k+1}}{r_k} = \frac{p'_{k+1} q'_k}{p'_k q'_{k+1}} = \frac{p'_{k+1} \, \mathrm{NWD}(p'_k, q_n)}{p'_k \, \mathrm{NWD}(p'_{k+1}, q_n)} = \frac{\mathrm{NWD}(p'_k p'_{k+1}, q_n p'_{k+1})}{\mathrm{NWD}(p'_k p'_{k+1}, q_n p'_k)}$$
jest liczbą całkowitą, więc $r_k | r_{k+1}$, czyli również $\langle r_n \rangle$ jest bazą odometru uogólnionego.

4. Z definicji $q'_k | q_{N_k}$. Ponadto:
$$q_k | \, \mathrm{NWD}(p'_k, q_{N_k}) = q'_k.$$
Stąd wynika, że odometry $\Delta_{\langle q_n \rangle}$ i $\Delta_{\langle q'_n \rangle}$ są izomorficzne.

5. W dalszym ciągu przyda nam się następująca równość. Jeśli $n \geq N_{k+1}$, to:
$$\begin{aligned} \mathrm{NWD}(p'_k, q'_{k+1}) &= \mathrm{NWD}(p'_k, \mathrm{NWD}(p'_{k+1}, q_n)) = \\ &= \mathrm{NWD}(p'_k, p'_{k+1}, q_n) = \mathrm{NWD}(p'_k, q_n) = q'_k. \end{aligned}$$

6. Odometry $\Delta_{\langle p_n \rangle}$ i $\Delta_{\langle p'_n \rangle}$ są izomorficzne oraz odometry $\Delta_{\langle q_n \rangle}$ i $\Delta_{\langle q'_n \rangle}$ są izomorficzne. Zatem jądro kanonicznej faktoryzacji $\Delta_{\langle p_n \rangle}$ w $\Delta_{\langle q_n \rangle}$ jest izomorficzne z jądrem kanonicznej faktoryzacji $\Delta_{\langle p'_n \rangle}$ w $\Delta_{\langle q'_n \rangle}$. Niech ψ będzie faktoryzacją $\Delta_{\langle p'_n \rangle}$ w $\Delta_{\langle q'_n \rangle}$; wystarczy więc pokazać, że $\ker \psi$ jest izomorficzne z pewnym odometrem uogólnionym. Pokażemy, że $\ker \psi$ jest izomorficzne z $\Delta_{\langle r_n \rangle}$.

7. Wobec $q'_n | p'_n$, wzory (6) i (8) mówią, że:

$$\ker \psi = \left\{ \langle a_n \rangle \in \Delta_{\langle p'_n \rangle} : q'_n | a_n \text{ dla wszystkich } n \right\}.$$

Niech $\langle u_n \rangle$ będzie ustalonym ciągiem liczb całkowitych. Dla $\langle a_n \rangle \in \ker \psi$ niech b_n oznacza resztę z dzielenia liczby $\frac{u_n a_n}{q'_n}$ przez r_n. Określmy φ wzorem $\varphi \langle a_n \rangle = \langle b_n \rangle$. Dobierzemy liczby u_n tak, by φ było izomorfizmem $\ker \psi$ oraz $\Delta_{\langle r_n \rangle}$.

8. Żądamy, by $\langle b_n \rangle \in \Delta_{\langle r_n \rangle}$, tzn. dla każdego k:

$$\frac{a_k}{q'_k} u_k \equiv b_k \equiv b_{k+1} = \frac{a_{k+1}}{q'_{k+1}} u_{k+1} \pmod{r_k}.$$

Ustalmy k. Ponieważ $a_{k+1} = a_k + cp'_k = a_k + cq'_k r_k$ dla pewnego c, więc:

$$\frac{a_k}{q'_k} u_k = \frac{a_{k+1}}{q'_k} u_k - c r_k u_k \equiv \frac{a_{k+1}}{q'_{k+1}} \cdot \frac{q'_{k+1}}{q'_k} u_k \pmod{r_k}.$$

Zatem aby $\langle b_n \rangle \in \Delta_{\langle r_n \rangle}$, potrzeba i wystarcza:

$$u_{k+1} \equiv \frac{q'_{k+1}}{q'_k} u_k \pmod{r_k}.$$

Skunstruujemy indukcyjnie ciąg $\langle u_n \rangle$ tak, by zachodził powyższy warunek i ponadto $\mathrm{NWD}(u_n, r_n) = 1$ (będzie to potrzebne do pokazania, że φ jest bijekcją).

9. Gdy $k = 1$, to przyjmujemy $u_1 = 1$; oczywiście $\mathrm{NWD}(u_1, r_1) = 1$. Przyjmijmy, że dla pewnego k określiliśmy tak, jak żądaliśmy, liczby $u_1, u_2, \ldots, u_k$.

Oznaczmy przez M największy dzielnik r_{k+1} względnie pierwszy z r_k. Niech t będzie odwrotnością r_k modulo M i przyjmijmy:

$$d = -t \left(\frac{q'_{k+1}}{q'_k} u_k - 1 \right).$$

Określmy:

$$u_{k+1} = \frac{q'_{k+1}}{q'_k} u_k + d r_k$$

Zachodzi:

$$u_{k+1} = \frac{q'_{k+1}}{q'_k}u_k + dr_k = \frac{q'_{k+1}}{q'_k}u_k - tr_k\left(\frac{q'_{k+1}}{q'_k}u_k - 1\right) \equiv$$
$$\equiv \frac{q'_{k+1}}{q'_k}u_k - \frac{q'_{k+1}}{q'_k}u_k + 1 = 1 \pmod{M}.$$

W szczególności u_{k+1} nie ma wspólnego czynnika pierwszego z M. Zgodnie z punktem 5.:

$$\mathrm{NWD}(u_{k+1}, r_k) = \mathrm{NWD}\left(\frac{q'_{k+1}}{q'_k}u_k + dr_k, r_k\right) =$$
$$= \mathrm{NWD}\left(\frac{q'_{k+1}}{q'_k}u_k, r_k\right) = \mathrm{NWD}\left(\frac{q'_{k+1}}{q'_k}, r_k\right) =$$
$$= \frac{1}{q'_k}\mathrm{NWD}(q'_{k+1}, q'_k r_k) = \frac{1}{q'_k}\mathrm{NWD}(q'_{k+1}, p'_k) = \frac{1}{q'_k}\cdot q'_k = 1.$$

Zatem u_{k+1} nie ma również wspólnego czynnika pierwszego z r_k. Ale każdy czynnik pierwszy r_{k+1} jest czynnikiem pierwszym M albo r_k, więc $\mathrm{NWD}(u_{k+1}, r_{k+1}) = 1$.

Oczywiście zachodzi $u_{k+1} \equiv \frac{q'_{k+1}}{q'_k}u_k \pmod{r_k}$, zatem tak określone u_{k+1} spełnia żądane warunki. Na mocy poprzedniego punktu, φ odwzorowuje $\ker\psi$ w $\Delta_{\langle r_n\rangle}$.

10. Udowodnimy teraz, że przekształcenie φ jest homomorfizmem. Niech $\langle a'_n\rangle, \langle a''_n\rangle \in \ker\psi$. Oznaczmy:

$$\langle b'_n\rangle = \varphi\langle a'_n\rangle, \quad \langle b''_n\rangle = \varphi\langle a''_n\rangle, \quad \langle b_n\rangle = \varphi\left(\langle a_n\rangle + \langle b_n\rangle\right).$$

Zgodnie z definicją φ, oznacza to:

$$b'_n \equiv \frac{u_n a'_n}{q'_n}, \quad b''_n \equiv \frac{u_n a''_n}{q'_n}, \quad b_n \equiv \frac{u_n(a'_n + a''_n)}{q'_n} \pmod{r_n}.$$

Stąd łatwo:

$$b_n \equiv \frac{u_n(a'_n + a''_n)}{q'_n} = \frac{u_n a'_n}{q'_n} + \frac{u_n a'_n}{q'_n} \equiv b'_n + b''_n \pmod{r_n},$$

czyli $\langle b_n\rangle = \langle b'_n\rangle + \langle b''_n\rangle$, jak chcieliśmy.

11. Niech $\varphi\langle a_n\rangle = \varphi\langle a'_n\rangle$, $\langle a_n\rangle, \langle a'_n\rangle \in \ker\psi$. Oznacza to, że dla każdego n:
$$\frac{a_n}{q'_n}u_n \equiv \frac{\widetilde{a}_n}{q'_n}u_n \pmod{r_n}.$$
Ale dobraliśmy u_n tak, by $\mathrm{NWD}(u_n, r_n) = 1$, zatem:
$$\frac{a_n}{q'_n} \equiv \frac{\widetilde{a}_n}{q'_n} \pmod{r_n},$$
czyli $a_n \equiv \widetilde{a}_n \pmod{p'_n}$, lub inaczej $\langle a_n\rangle = \langle\widetilde{a}_n\rangle$. Zatem homomorfizm φ jest różnowartościowy.

12. Weźmy teraz$\langle b_n\rangle \in \Delta_{\langle r_n\rangle}$. Ponieważ $\mathrm{NWD}(u_n, r_n) = 1$, więc istnieje odwrotność u_n modulo r_n. Niech $u_n v_n \equiv 1 \pmod{r_n}$. Zdefiniujmy a_n jako resztę z dzielenia $q'_n v_n b_n$ przez p'_n. Ponieważ q'_n jest dzielnikiem liczb $q'_n v_n b_n$ oraz p'_n, więc $q'_n | a_n$. Zgodnie z definicją u_{n+1}:
$$v_n \equiv u_{n+1}v_{n+1}v_n \equiv \frac{q'_{n+1}}{q'_n}u_n v_n v_{n+1} \equiv \frac{q'_{n+1}}{q'_n}v_{n+1} \pmod{r_n},$$
skąd:
$$q'_n v_n \equiv q'_{n+1}v_{n+1} \pmod{p'_n}.$$
Ponadto $b_{n+1} \equiv b_n \pmod{r_n}$, czyli $q'_n b_{n+1} \equiv q'_n b_n \pmod{p'_n}$. Stąd:
$$a_{n+1} \equiv q'_{n+1}v_{n+1}b_{n+1} \equiv q'_n v_n b_{n+1} \equiv q'_n v_n b_n \equiv a_n \pmod{p'_n},$$
czyli $\langle a_n\rangle \in \Delta_{\langle p_n\rangle}$. Wobec $q'_n | a_n$ otrzymujemy $\langle a_n\rangle \in \ker\psi$. Niech $\langle b'_n\rangle = \varphi\langle a_n\rangle$. Wówczas:
$$q'_n b'_n \equiv u_n a_n \equiv q'_n b_n u_n v_n \pmod{p'_n},$$
czyli:
$$b'_n \equiv b_n u_n v_n \equiv b_n \pmod{r_n}.$$
Oznacza to, że $\varphi\langle a_n\rangle = \langle b_n\rangle$. Wobec dowolności $\langle b_n\rangle \in \Delta_{\langle r_n\rangle}$, homomorfizm φ jest „na”.

13. Pokazaliśmy, że φ izomorfizmem między $\ker\psi$ i odometrem uogólnionym $\Delta_{\langle r_n\rangle}$. Aby zakończyć dowód twierdzenia, zauważmy, że $\langle r_n\rangle$ jest podciągiem ciągu $\langle s_n\rangle$ zdefiniowanego w tezie twierdzenia, a więc odometry $\Delta_{\langle r_n\rangle}$ i $\Delta_{\langle s_n\rangle}$ są izomorficzne.

Otrzymany wynik można sformułować w języku funkcji charakterystycznych. Jeśli odometr $\Delta_{\langle p_n \rangle}$ o funkcji charakterystycznej α ma faktor $\Delta_{\langle q_n \rangle}$ o funkcji charakterystycznej β, to (cwiczenie 51) $\beta \leq \alpha$. Właśnie udowodniliśmy, że jądro faktoryzacji $\Delta_{\langle p_n \rangle}$ w $\Delta_{\langle q_n \rangle}$ jest izomorficzne z odometrem uogólnionym $\Delta_{\langle s_n \rangle}$ o funkcji charakterystycznej γ określonej równaniem $\gamma(p) = \alpha(p) - \beta(p)$, z dodatkową umową $\infty - \infty = 0$.

W szczególności odometr $\Delta_{\langle p_n \rangle}$ posiada podgrupy izomorficzne z odometrami $\Delta_{\langle s_n \rangle}$ o funkcjach charakterystycznych γ takich, że:

$$\begin{aligned} &\gamma(p) \leq \alpha(p) \quad \text{dla każdego } p \in \mathbb{P}, \\ &\alpha(p) = \infty \quad \Rightarrow \quad \gamma(p) \in \{0, \infty\}. \end{aligned}$$