Introduction to Topological Algebra

Przepisał: Ricko

15 listopada 2021

Spis treści

Rozdział 1

Wstęp

Poniższy skrypt ma na celu usystematyzowanie wiedzy poznanej na kursie *Introduction to Topological Algebra* czyli Wstęp do Algebry Topologicznej. Autorem wykładów jest znany matematyk rosyjski prof.dr.hab. Mikhail Tkachenko wykładający na Metropolitan Autonomous University w Mexico City i specjalizujący się w takich dziedzinach matematyki jak algebra, geometria czy topologia. Skrypt jest tłumaczeniem informacji podawanych nam na wykładzie w języku angielskim na język polski. Zawarty jest też w nim słowniczek z najważniejszymi wyrażeniami poznanymi na kursie w języku angielskim. Dodatkowo dołączone są skany orginalnego wykładu, a także pierwszy 3 rozdziały z książki profesora, na bazie której stworzony był wykład. Całość uzupełniają ćwiczenia zadane na wykładzie do zrobienia w domu oraz te robione na konwersatorium.

Rozdział 2

Wykłady

2.1 22.02.16

Def 1.
Półgrupą *nazywamy parę $(S, \cdot)$, gdzie S jest zbiorem niepostym, $a \cdot : S \times S \to S$ jest łącznym działaniem dwuargumentowym:*

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Def 2.
Monoidem *nazywamy półgrupę posiadającą element neutralny:*

$$e \in S \qquad e \cdot s = s \cdot e = s \underset{s \in S}{\forall}$$

Def 3.
Niech S będzie półgrupą oraz $a \in S$.
Akcją lewostronną *nazywamy odwzorowanie $\lambda_a \colon S \to S$ dane wzorem $\lambda_a(x) = a \cdot x \underset{x \in S}{\forall}$*
Akcją prawostronną *nazywamy odwzorowanie $g_a \colon S \to S$ dane wzorem $g_a(x) = x \cdot a \underset{x \in S}{\forall}$*
Jeśli S jest grupą to odwzorowania λ_g oraz g_a nazywamy ***translacjami***

Przykład 1.
Półgrupy:

1. $(\mathbb{Z}, \cdot)$ - *monoid, element neutralny: 1*
2. $(\mathbb{Q}, \cdot)$ - *monoid, element neutralny: 1*
3. $(\mathbb{R}, \cdot)$ - *monoid, element neutralny: 1*
4. $(\mathbb{R}_+, +)$ - *półgrupa przemienna, brak elementu neutralnego,*
5. $(\mathbb{N}, *)$, *gdzie* $m * n = \max\{n, m\}$ - *monoid przemienny, element neutralny:* 1
6. $(\mathbb{N}, \square)$, *gdzie* $m \square n = \min\{n, m\}$ - *półgrupa przemienna*
7. $(S, *)$, *gdzie* $x * y = y$ - *monoid dla zbioru* S $1-$*elementowego (wtedy ten element jest neutralny), półgrupa nieprzemienna dla* $|S| \geqslant 2$

8. $(S, *)$, *gdzie* $x * y = x$ *- monoid dla zbioru* S $1-$*elementowego (wtedy ten element jest neutralny), półgrupa nieprzemienna dla* $|S| \geqslant 2$

9. $(S(X,X), \circ)$, *gdzie* $S(X,X) = \{f : f : X \to X\}$ *- zbiór wszystkich odwzorowań z* X *do* X, $a \circ$ *jest działaniem składania funkcji - monoid, element neutralny:* id_x, *przemienny dla* $|X| \leqslant 2$

Def 4.
Grupą *nazywamy monoid, w którym każdy element ma element przeciwny.*

$$x \cdot y = y \cdot x = e \Longrightarrow y = x^{-1}$$

Fakt 1.
Jeśli G *jest grupą to* λ_a, g_a *są translacjami (bijekcjami grupy* G *dla każdego* $a \in G$*)*

Dowód.
Niech $\lambda_a : G \to G$ będzie odwzorowaniem danym wzorem $\lambda_a(x) = a \cdot x \ \ \forall_{x \in G}$
Pokażemy, że λ_a jest "na"
Niech $y \in G$. Załóżmy, że y jest wartością funkcji λ_a, spróbujemy wyliczyć postać x
$\lambda_a(x) = y \Longrightarrow ax = y \Longrightarrow x = a^{-1}y$ jest elementem, którego obrazem jest y
Pokażemy, że λ_a jest "1-1"
Niech $x_1, x_2 \in G$
$\lambda_a(x_1) = \lambda_a(x_2) \Longrightarrow ax_1 = ax_2 \ / \cdot a^{-1} \Longrightarrow x_1 = x_2$ - zatem mamy różnowartościowość.
Nasza funkcja jest suriekcją i iniekcją zatem także bijekcją. □

Przykład 2.
Grupy:

1. $(\mathbb{Z}, +)$

2. $(\mathbb{Q} \setminus \{0\}, \cdot)$

3. $(\mathbb{R}^*, \cdot)$

4. $(\mathbb{R}_+, \cdot)$

5. $(\mathbb{Z}_2, +)$ *- grupa boolowska*

6. $(\mathbb{Z}_n, +)$ *- działaniem jest dodawanie modulo* n*.*

7. $(\mathbb{T}, \cdot)$, *gdzie* $\mathbb{T} = \{z \in \mathbb{C} \colon |z| = 1\}$ *(okrąg jednostkowy), działaniem jest mnożenie elementów (w praktyce jest to dodawanie kątów modulo* π*:* $z_1, z_2 \in \mathbb{T}$*, wtedy* $z_1 = e^{i\varphi_1}, z_2 = e^{i\varphi_2}$*, a działanie wygląda nastepujaco:* $z_1 \cdot z_2 = e^{i\varphi_1} \cdot e^{i\varphi_2} \ e^{i(\varphi_1 + \varphi_2)}$*)*

8. $(Gl(n, \mathbb{R}), \cdot)$

9. $(S_X, \circ)$ *gdzie* S_X *jest zbiorem wszystkich bijekcji zbioru* X*, jest to grupa przemienna dla* $|X| \leqslant 2$ *Jeśli* $|X| = n$ *to* S_X *oznaczamy także* S_n *i nazywamy grupą permutacyjną* n*-elementową*

Def 5.
Zbiór $A \subset G$*, gdzie* G *jest grupą nazywamy symetrycznym jeśli* $A^{-1} = A$

Def 6.
Zbiór niepusty $H \subset S$, gdzie S jest półgrupą nazywamy ***podpółgrupą*** *półgrupy S jeśli $H \cdot H \subset H$ albo równoważnie*

$$xy \in H \quad \underset{x,y \in H}{\forall}$$

Def 7.
Zbiór niepusty $H \subset G$, gdzie G jest grupą nazywamy ***podgrupą*** *grupy G jeśli $H \cdot H^{-1} \subset H$, gdzie $H^{-1} = \{h^{-1} \colon h \in H\}$ albo równoważnie*

$$H \cdot H \subset H \ \wedge H^{-1} \subset H$$

Fakt 2.
Grupy mogą zawierać podpółgrupy.

Fakt 3.
Półgrupy mogą zawierać podgrupy.

Def 8.
Zbiór niepusty $H \subset G$ jest ***podgrupą normalną*** *grupy G (oznaczamy $H \leqslant G$ lub $H \triangleleft G$), jeśli*

$$xHx^{-1} \subset H \quad \underset{x \in G}{\forall}$$

Uwaga: zamiast $\subset$ można użyć znaku równości, ponieważ $H \subset x^{-1}Hx$

Def 9.
Niech $H \subset G$ będzie podgrupą normalną grupy G. Zbiór $\{x \cdot H \colon x \in G\}$ nazywamy rodziną ***warstw lewostronnych*** *podgrupy H*

Def 10.
Niech $H \subset G$ będzie podgrupą normalną grupy G. Zbiór $\{H \cdot x \colon x \in G\}$ nazywamy rodziną ***warstw prawostronnych*** *podgrupy H*

Fakt 4.
Dwie warstwy podgrupy $H \subset G$ są albo identyczne albo są rozłączne. Identyczność warstw opisuje warunek:

$$x_1, x_2 \in G \qquad x_1 H = x_2 H \iff x_1^{-1} x_2 \in H$$

Def 11.
Niech $H \subset G$ będzie podgrupą normalną grupy G oraz niech $x, y \in G$. Definiujemy działanie $*$ następująco:

$$(xH) * (yH) = (xy)H$$

Zbiór wszystkich warstw podgrupy normalnej H względem grupy G z działaniem $*$, elementem neutralnym H nazywamy ***grupa ilorazową*** *i oznaczamy G/H.*
Ponadto dla każdego elementu xH element przeciwny ma postać $x^{-1}H$.

Dowód. Poprawność działania $*$
Niech $H \subset G$ będzie podgrupą normalną oraz $x_1, x_2, y_1, y_2 \in G$
Wiemy, że $x_1H = x_2H \iff x_1^{-1}x_2 \in H$ oraz $y_1H = y_2H \iff y_1^{-1}y_2 \in H$
$(x_1H) * (y_1H) = (x_1y_1)H$
$(x_2H) * (y_2H) = (x_2y_2)H$
Pytamy czy $x_1y_1H = x_2x_2H$ czyli będziemy sprawdzali warunek:

$$x_1y_1H = x_2y_2H \iff (x_1y_1)^{-1}x_2y_2 \in H$$

Rozpiszmy prawa część równoważności:
$(x_1y_1)^{-1}x_2y_2 = y_1^{-1}\underbrace{x_1^{-1}x_2}_{\in H}y_2 = y_1^{-1}\underbrace{h}_{x_1^{-1}x_2}y_1y_1^{-1}y_2 = \underbrace{y_1^{-1}hy_1}_{\in H}\underbrace{y_1^{-1}y_2}_{\in H} \in H$ □

Fakt 5.
W podgrupie normalnej $xH = Hx \ \forall_{x\in G}$

Twierdzenie 1. *(Lagrange'a)*
$|G| = |H| \cdot |G/H|$ *(równoważnie* $|G| = |H| \cdot [G : H]$*)*

Def 12.
Niech S będzie półgrupą i $a \in S$. Mówimy, że element a jest ***elementem idempotentnym*** *jeśli*

$$a^2 = a$$

Łatwo zauważyć, że $a^3 = a^2 * a = a * a = a$. Zatem $a^n = a \ \forall_{n\geqslant 1}$.
Ponadto jeśli S jest grupą, $a \in S$ to $< a >= \{a^n : n \in \mathbb{Z}\}$

Przykład 3.
Weźmy $S(X, X)$ - zbiór wszystkich odwzorowań z X do X. Jakie mamy tutaj elementy idempotentne?

$$f^2 = f$$

Szukamy takich funkcji, że $(f \circ f)(x) = f(x)$
Przykładowo taką funkcją jest identyczność: id_X
Funkcje spełniające tę zależność nazywamy ***retrakcjami****, są to odwzorowania postaci $f : X \to A \subset X$, gdzie $f\big|_A = id_A$*
Zatem łatwo zauważyć, że funkcje te przenoszą raz dowolny element z X do A, a następnie pozostawiają go w A na miejscu, przez co są one idempotentne.

Def 13.
Niech $(G, \cdot), (H, *)$ będa grupami. ***Homomorfizmem grup*** *nazywamy odwzorowanie $f : G \to H$ takie, że*

$$f(a \cdot b) = f(a) * f(b) \underset{a,b\in G}{\forall}$$

Def 14.
Jądrem *homomorfizmu $f : G \to H$ nazywamy zbiór postaci:*

$$\{x \in G : f(x) = e_H\}$$

Fakt 6.
Jądro homomorfizmu jest podgrupą normalną.

Dowód.
Oznaczmy $N = Kerf$. Niech $x \in G$ oraz $h \in N$.
Pokażemy, że $xhx^{-1} \in N$
$f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x) \cdot e_H \cdot (f(x))^{-1} = e_H$
Co pokazuje, że N jest podgrupą normalną. □

Def 15.
Homomorfizm, który jest "na" i "1-1" nazywamy ***izomorfizmem****.*

Def 16.
Izomorfizm działający z grupy w nią samą nazywamy ***automorfizmem****.*
Grupę wszystkich automorfizmów grupy G oznaczamy $Aut(G)$

Def 17.
Niech G będzie grupą i $a \in G$. ***Automorfizmem wewnętrznym*** *nazywamy odwzorowanie postaci:*

$$\varphi_a(x) = axa^{-1} \underset{x \in G}{\forall}$$

Fakt 7.
φ_a jest automorfizmem $\forall_{a \in G}$

Dowód.
Ustalmy $x, y \in G$
Pokażemy, że φ_a jest homomorfizmem.
$\varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x) \cdot \varphi_a(y)$
Teraz pokażemy, że φ_a jest $1-1$
Niech $\varphi_a(x) = \varphi_a(y) \Longrightarrow axa^{-1} = aya^{-1} / : a^{-1} \Longrightarrow ax = ay / : a \Longrightarrow x = y$
Pozostało pokazać, że φ_a jest "na"
Ustalmy $y \in G$ takie, że $\varphi_a(x) = y$. Spróbujemy wyliczyć x
$axa^{-1} = y \Longrightarrow x = a^{-1}a$ - zatem φ_a jest suriekcją.
Stąd φ_a jest automorfizmem. □

2.2 23.02.16

Lem 1. *Niech H będzie podgrupą grupy abelowej G oraz niech $f\colon H \to F$ (gdzie F tez jest grupą abelową) będzie homomorfizmem grup. Niech ponadto $x \in G, y \in F$.*
Wtedy istnieje homomorfizm $h\colon \langle H \cup \{x\}\rangle \to F$ taki, że $h(x) = y$ wtedy i tylko wtedy, gdy $m = \min\{n \in \mathbb{N}^*\colon nx \in H\} = \infty$ lub $m \in \mathbb{N}$ i $f(mx) = my$, gdzie $\mathbb{N}^* = \mathbb{N} \cup \{\infty\}$.

Dowód.
$\Longleftarrow$
Przypadek 1:
$m = \infty \Rightarrow nx \notin H \ \forall_{n \in \mathbb{N}}$. Wtedy też $\langle x\rangle \cap H = \{\emptyset\}$.
Niech $H_0 = \langle H \cup \{x\}\rangle$. Wtedy każdy element $z \in H_0$ posiada jednoznaczną reprezentację w postaci

$z = kx + a$, gdzie $k \in \mathbb{Z}$ i $a \in H$
Sprawdzimy, że odwzorowanie h dane wzorem $h(z) = h(kx + a) = ky + f(a)$ jest homomorfizmem.
Niech $z_1 = kx + a$o raz $z_2 = lx + b$
$z_1 + z_2 = kx + a + lx + b = (k + l)x + (a + b)$
$h(z_1 + z_2) = (k + l)y + f(a + b) = ky + ly + f(a) + f(b)$ (bo f jest homomorfizmem).
$ky + ly + f(a) + f(b) = (ky + f(a)) + (ly + f(b)) = h(z_1) + h(z_2)$ - zatem h jest homomorfizmem.
Ponadto $h\Big|_H = f$

Przypadek 2:
Teraz zakładamy, że $m \in \mathbb{N}$ oraz $f(mx) = my$
Niech $h(x) = y$. Ponadto niech $z \in H_0$ (gdzie H_0 jest tak samo zdefiniowane jak w poprzednim przypadku). Teraz jednak przedstawienie z nie będzie jednoznaczne, ponieważ $\langle x\rangle \cap H \neq \{\emptyset\}$. Zatem $z = kx+a$, gdzie $k \in \mathbb{Z}$ i $a \in H$. Ponownie zdefiniujemy odwzorowanie $h(z) = h(kx + a) = ky + f(a)$ i ponownie pokażemy, że taka definicja jest poprawna.
Dokładnie rzecz biorąc, dowiedziemy, że przy podanych założeniach dwa różne przedstawienia $h(z)$ są tym samym (ich różnica będzie wynosiła wtedy 0).
Zatem niech $z = kx + a$ oraz $z = lx + b$
Wtedy $h(z) = ky + f(a)$ oraz $h(z) = ly + b$.
Ich różnica wynosi $(l - k)y + f(b - a)$ (f-homomorfizm).
Wróćmy jeszcze do postaci przed $kx + a = lx + b$. Zauważmy, że $(l - k)x = \underbrace{a - b}_{\in H}$. Stąd $l - k$ jest wielokrotnością elementu m
Wtedy $l - k = mp$ dla $p \in \mathbb{Z}$ czyli $(l - k)x = mpx = a - b$
Wracając do postaci różnicy wartości homomorfizmu $h(z)$ mamy $(l-k)y+f(b-a) = mpy+f(b-a) = mpx - f(a - b) = mpy - f(mpx) = p(my - f(mx)) = p(my - my) = 0$.
Zatem różnica wynosi 0, stąd nasz homomorfizm h jest poprawnie zdefiniowany.
$\Longrightarrow$
Wiemy, że $h(x) = y, mx \in H$ i że h jest homomorfizmem. Wtedy $my = mh(x) = h(mx) = f(mx)$.
Komentarz: ta część dowodu była bardzo szybko przedstawiana i może być niekompletna. □

Def 18.
*Mówimy, że grupa G jest **podzielna** jeśli $\forall_{b\in G}$ równanie $x^n = b$ ma rozwiązanie w grupie G dla każdego elementu $n \in \mathbb{N}$*

Przykład 4.
Grupy podzielne

1. $(\mathbb{R}, +)$ $nx = b \Rightarrow x = \frac{b}{n}$ - *podzielna*
2. $(\mathbb{T}, \cdot)$ $z \in \mathbb{T}, z = e^{i\varphi}, z = t^n \Rightarrow t = e^{i\frac{\varphi}{n}}$ - *podzielna*
3. $(\mathbb{C}, +)$ - *podzielna*
4. $(\mathbb{Z}_2, +)$ - *niepodzielna, ponieważ np.* $2 \cdot x = 1$ *nie ma rozwiązania.*

Def 19.
*Mówimy, że para $(\mathcal{P}, \leqslant)$ jest **zbiorem częściowo uporządkowanym**, gdy relacja $\leqslant$ częściowo porządkowuje zbiór $\mathcal{P}$ (niektóre elementy mogą być nieporównywalne).*

Przykład 5.
Zbiór $(\mathbb{C}, <)$ jest zbiorem częściowo uporządkowanym, gdyż $z < w \Leftrightarrow |z| < |w|$, zatem nie wszystkie elementy sa porównywane (np. liczb o takich samych modułach nie da się porównać).

Def 20.
*Mówimy, że zbiór $\mathcal{C}$ jest **łańcuchem**, gdy jest liniowo uporządkowany przez relację $\leqslant$*

Def 21.
*Mówimy, że x jest **ograniczeniem górnym** zbioru $\mathcal{C}$ jeśli $c \leqslant x$ dla każdego $c \in \mathcal{C}$*

Lem 2. *(Kuratowskiego - Zorna)*
Niech $(\mathcal{P}, \leqslant)$ będzie zbiorem częściowo uporządkowanym tak, że każdy łańcuch $\mathcal{C} \subset \mathcal{P}$ na ograniczenie górne w $\mathcal{P}$. Wtedy $\mathcal{P}$ ma element maksymalny czyli $\exists_{x_0 \in \mathcal{P}}$ taki, że żaden element $x \in \mathcal{P}$ nie spełnia warunku $x_0 < x$

Twierdzenie 2. *Niech H będzie podgrupą grupy abelowej G. Wtedy każdy homomorfizm $f\colon H \to F$ idący w podzielną i abelową grupę F można rozszerzyć do homomorfizmu $h\colon G \to F$.*

Dowód.
Niech $(\mathcal{P}, \leqslant)$ będzie takim zbiorem częściowo uporzadkowanym, że zbiór $\mathcal{P}$ zawiera pary (K, g), gdzie K jest podgrupą grupy G zawierającą podgrupę H, a g będzie homomorfizmem z K do F rozszerzającym f, a relacja $\leqslant$ działa następująco: dla dwóch par (K, g) i (K_1, g_1) mamy $(K, g) \leqslant (K_1, g_1)$ jeśli $K \subset K_1$ i g_1 rozszerza g. Mamy pewność, że $\mathcal{P}$ jest niepusty, bo na pewno jest w nim para (H, f).
Niech ponadto $\mathcal{C}$ będzie niepustym łańcuchem w $(\mathcal{P}, \leqslant)$. (H, f) jest najmniejszym elementem $(\mathcal{P}, \leqslant)$ zatem (H, f) jest w $\mathcal{C}$.
Zdefiniujemy teraz zbiór $P^* = \bigcup\{K : (K, g) \in \mathcal{C} \text{ dla wszystkich } g\colon K \to F\}$
Claim 1.
P^* jest podgrupą grupy G.
Jest tak, ponieważ w $\mathcal{C}$ mamy liniowy porządek, zatem zbiory zawierają się jeden w drugim.
Teraz definiujemy $g^*\colon P^* \to F$. Ponadto bierzemy $x \in P^*$. Wtedy $\exists_{(K,g)\in\mathcal{C}}$ taki, że $x \subset K$. Wtedy definicja $g^*(x) = g(x)$ jest poprawna (bo mamy łańcuch).
Claim 2.
g^* jest homomorfizmem.
Pokazać, że $g^*(x + y) = g^*(x) + g^*(y)$ - Ćwiczenie
Zauważmy też, że $H \subset P^*$ oraz g^* rozszerza f.
Claim 3.
(P^*, g^*) jest ograniczeniem górnym łańcucha $\mathcal{C}$. Stosujemy lemat Kuratowskiego-Zorna i mamy element maksymalny $(K, h) \in \mathcal{P}$.
Claim 4.
Pokażemy, że $K = G$
Przeprowadzimy dowód nie wprost. Załóżmy, że istnieje element $x \in G \setminus K$. Zdefiniujemy $H_0 = \langle K \cup \{x\}\rangle$ istotnie większy od K
Ponadto $h\colon K \to F$ niech będzie homomorfizmem. Stosujemy wcześniej udowodniony lemat. Wtedy $h^*(x) = y$ i $h(mx) = my \ / : m$ (można, bo F jest podzielna). Wtedy $h^*\colon H_0 \to F$ jest rozszerzeniem h. Mamy zatem $(H_0, h^*) \in \mathcal{P}$ oraz $(K, h) < (H_0, h^*)$ co jest sprzecznością, ponieważ (K, h) był elementem maksymalnym. Zatem $K = G$ i $(K, h) = (G, h)$ (rozszerzenie f) co kończy dowód. □

Def 22.
Kwaterniony - $\mathbb{Q}$
$\mathbb{Q} = \{a + bi + cj + dk \colon a, b, c, d \in \mathbb{R},\ i^2 = j^2 = k^2 = -1\}$
Ponadto:

$$i \cdot j = -j \cdot i = k \qquad j \cdot k = -k \cdot j = i \qquad i \cdot k = -k \cdot i = j$$

W zbiorze kwaternionów definiujemy działanie dodawania:
Niech $q = a + bi + cj + dk \qquad q' = a' + b'i + c'j + d'k$. *Wtedy:*

$$q + q' = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

Ponadto w zbiorze kwaternionów definiujemy działanie mnożenią

$$q \cdot q' = (a + bi + cj + dk) \cdot (a' + b'i + c'j + d'k) =$$

$$= (aa' - bb' - cc' - dd') + (ab' + ba' + cd - dc')i + (ac' + ca' + bd' - db')j + (ad' + da' + bc' - cd')k$$

Do najważniejszych własności kwaternionów należą:

1. $(\mathbb{Q}, +)$ *jest grupą przemienną*
2. $(\mathbb{Q} \setminus \{0\}, \cdot)$ *jest nieprzemienną grupą z elementem neutralnym* $e = 1 + 0 \cdot i + 0 \cdot j + 0 \cdot k$
3. $x(y + z) = xy + xz$
   $(y + z)x = yx + zx$ - *Ćwiczenie*
4. $(\mathbb{Q}, +, \cdot)$ - *ciało nieprzemienne (pierscień z dzieleniem)*

Claim 1.
Każdy element niezerowy z $\mathbb{Q}$ *jest odwracalny.*
$q = a + bi + cj + dk \qquad \overline{q} = a - bi - cj - dk$ - *element sprzężony*
$q \cdot \overline{q} = a^2 + b^2 + c^2 + d^2$ - *Ćwiczenie*
$||q|| = \sqrt{a^2 + b^2 + c^2 + d^2}$
$q^{-1} = \frac{\overline{q}}{(a^2+b^2+c^2+d^2)} = \frac{\overline{q}}{||q||^2}$

2.3 29.02.16

Grupa liczb (r)-adycznych
Dla $r \leqslant 2$ grupę liczb (r)-adycznych oznaczać będziemy Ω_r. Przejdźmy do ich konstrukcji. Niech $A = \{0, 1, ..., r - 1\}$ - zbiór reszt z dzielenia przez r. Wtedy poprzez $A^{\mathbb{Z}}$ rozumiemy funkcję idące z A do $\mathbb{Z}$. Element tego zbioru przedstawimy w postaci ciągu nieskończonego z obydwu stron:

$$x = (..., x_{-2}, x_{-1}, x_0, x_1, x_2, ...)$$

Rodzinę Ω_r definiujemy następująco:

$$\Omega_r = \{x \in A^{\mathbb{Z}} \colon \underset{n}{\exists} \text{ takie, że } x_k = 0 \underset{k<n}{\forall}\}$$

W niej definiujemy operację (działanie) dodawania. Potrzebujmy w tym celu dwóch elementów dodatnich oznaczmy je jako N i M:

$$N = x_0 + x_1 r + x_2 r^2 + ... + x_m r^m \ x_i \in A \underset{i}{\forall}, \ x_m \neq 0$$

$$M = y_0 + y_1 r + y_2 r^2 + ... + y_n r^n \ y_i \in A \underset{i}{\forall}, \ y_n \neq 0$$

Ich sumę na razie oznaczymy jako:

$$M + N = z_0 + z_1 r + z_2 r^2 + ... + z_k r^k \ z_i \in A \underset{i}{\forall}, \ z_k \neq 0$$

Wstawiając otrzymujemy (załóżmy, że $m < n$):

$$\begin{aligned} M + N &= x_0 + y_0 + (x_1 + y_1)r + (x_2 + y_2)r^2 + ... + (x_m + y_m)r^m + ... \\ &= z_0 + z_1 r + z_2 r^2 + ... + z_k r^k \text{ gdzie } k \leqslant \max\{m, n\} + 1 \end{aligned}$$

Zestawiając ze sobą współczynniki (używając operacji modulo) otrzymujemy

$$x_0 + y_0 \equiv z_0 (\text{mod } r)$$

Stąd:

$$x_0 + y_0 = z_0 + t_0 r \text{ gdzie } t_0 \in \{0, 1\}$$

Wstawiając te wyliczenia do wzoru na sumę mamy:

$$\begin{aligned} M + N &= z_0 + t_0 r + (x_1 + y_1)r + (x_2 + y_2)r^2 + ... + (x_m + y_m)r^m + ... \\ &= z_0 + z_1 r + z_2 r^2 + ... + z_k r^k \text{ gdzie } k \leqslant \max\{m, n\} + 1 \end{aligned}$$

Zatem

$$t_0 + x_1 + y_1 \equiv z_1$$

Wiemy, że $0 \leqslant t_0 + x_1 + y_1 \leqslant 1 + r - 1 + r - 1 < 2r$ i wykonując analogiczny krok jak dla z_0 mamy:

$$t_0 + x_1 + y_1 = z_1 + t_1 r \text{ gdzie } t_1 \in \{0, 1\}$$

Powtarzając naszą procedurę k razy otrzymujemy

$$t_k + x_{k+1} + y_{k+1} = z_{k+1} + t_{k+1} r \text{ gdzie } t_k \in \{0, 1\}$$

Takie działanie wyznaczone jest dla ciagów skończonych, my potrzebujemy dla nieskończonych. W tym celu zdefiniujmy element neutralny:

$$\overline{0} = (..., 0, 0, 0, ...)$$

oraz weźmy $x, y \in \Omega_r$ dane następująco:

$$x = (..., 0, 0, x_m, x_{m+1}, ...)$$

$$y = (..., 0, 0, y_n, y_{n+1}, ...)$$

Ponadto zdefiniujmy $k = \min\{m, n\}$. Wtedy $z_k = 0 \underset{k<k_0}{\forall}$ i nasz wzór

$$\underset{k>k_0}{\forall} z_k + t_k r = t_{k-1} + x_k + y_k \text{ gdzie } t_k, t_{k-1} \in \{0, 1\}$$

jest poprawny i $z = (..., 0, 0, z_k, z_{k+1}, ...) = x + y$, ponadto wyznaczony element neutralny $\overline{0}$ jest poprawny i zachodzi $\overline{0} + x = x + \overline{0} = x$.

Przykład 6.
$x = ...00020168721...$
$y = ...00053954109...$
$z = ...000730239201...$

Dodawanie w Ω_r jest przemienne (ponieważ przemienne jest dodawanie w liczbach całkowitych). Teraz pokażemy, że działanie to jest łączne.
Weźmy $x, y, z \in \Omega_r$. Chcemy pokazać, że $(x + y) + z = x + (y + z)$ (oczywiście jeśli każdy jest różny od 0). Ustalmy k_0 takie, że x, y, z nie mają zerowego współczynnika na pozycji k_0.
Zdefiniujmy zbiór

$$\sum_{k_0} = \{x \in \Omega_r \colon x_k = 0 \underset{k<k_0}{\forall} \text{ oraz } x \text{ ma skończoną ilość niezerowych współczynników}\}$$

Ponadto określmy odwzorowanie z $\sum_{k_0}$ do $\mathbb{N} \cup \{0\}$

$$f(x) = \underbrace{x_{k_0} + x_{k_0+1} r + x_{k_0+2} r^2 + ...}_{\text{skończona ilość}} \in \mathbb{N} \cup \{0\}$$

Rozdział 3

Ćwiczenia

3.1 Zadane na wykładzie 23.02.16

Uwaga: *Ćwiczenia zadane do domu są niesprawdzone, zatem mogą być błednie rozwiązane.*

3.1.1 Pokazanie, że g^* z twierdzenia jest homomorfizmem

Mamy dane odwzorowanie $g^*\colon P^* \to F$, gdzie $P^* = \bigcup\{K\colon (K,g) \in \mathcal{C}$ dla wszystkich $g\colon K \to F\}$
Wiemy ponadto, że $\mathcal{C}$ jest łańcuchem. Mamy pokazać:

$$g^*(x+y) = g^*(x) + g^*(y)$$

Weźmy

$$x \in P^* \Longrightarrow \underset{(K_1,g_1)\in\mathcal{C}}{\exists} x \subset K_1 \ \wedge g^*(x) = g_1(x)$$

$$y \in P^* \Longrightarrow \underset{(K_2,g_2)\in\mathcal{C}}{\exists} y \subset K_2 \ \wedge g^*(y) = g_2(y)$$

Z tego, że $\mathcal{C}$ jest łańcuchem wiemy, że $(K_1,g_1) \leqslant (K_2,g_2)$ czyli $K_1 \subset K_2$ i g_2 rozszerza g_1 albo mamy doczynienia z symetryczną sytuacją odwrotną (gdy $(K_2,g_2) \leqslant (K_1,g_1)$), przyjmijmy pierwszy przypadek. Wtedy (pamiętając, że g_1, g_2 są homomorfizmami):

$$g_2(x+y) = g^*(x+y) = g^*(x) + g^*(y) = g_1(x) + g_2(y) = g_2(x) + g_2(y) = g_2(x+y)$$

3.1.2 Kwaterniony Hamiltona - rodzielność dodawania względem mnożenia

Mamy pokazać, że $x(y+z) = xy + xz$ oraz $(y+z)x = yz + zx$. Niech

$$x = a + bi + cj + dk \qquad y = e + fi + gj + hk \qquad z = t + ui + vj + wk$$

$\boldsymbol{x(y+z)} = (a+bi+cj+dk)[(e+t)+(f+u)i+(g+v)j+(h+w)k] = (ae+at)+(af+au)i+(ag+av)j+(ah+aw)k+(be+bt)i-(bf+bu)+(bg+bv)k+(bh+bw)j+(cd+ct)j-(cf+cu)k-(cg+cv)+(ch+cw)i+(de+dt)k-(df+du)j-(dg+dv)i-(dh+dw) = (ae-bf-cg-dh)+(af+be+ch-dg)i+(ag+bh+ce-df)j+(ah+bg-cf+de)k+(at-bu-cv-dw)+(au+bt+cw-dw)i+(av+bw+ct-du)j+(aw+bv-cu+dt)k = \boldsymbol{xy+xz}$
Drugi przypadek dowodzimy analogicznie.

3.1.3 Iloczyn kwaternionu z elementem do niego sprzężonym

Niech $q = a + bi + cj + dk$. Wtedy elementem sprzężonym do q nazywamy $\overline{q} = a - bi - cj - dk$
Licząc ich iloczyn mamy:

$$\begin{aligned} q \cdot \overline{q} &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= a^2 - abi - acj - adk + abi + b^2 - bck - bdj + acj + bck + c^2 - cdi + adk + bdj + cdi + d^2 \\ &= a^2 + b^2 + c^2 + d^2 \end{aligned}$$

Rozdział 4

Słowniczek

4.1 Wykład 22.02.16

semigroup - półgrupa
non-empty - niepusty
associativity - łączność
communativity - łączność
composition - złożenie
bijection - bijekcja
theorem - twierdzenie
definition - definicja
coefficient - współczynnik
subgroup - podgrupa
permutation - permutacja
idempotent - idempotentny
retraction - retrakcja
quotient group - grupa ilorazowa
assume - załóżmy
identity - identyczność
multiplication - mnożenie
translation - translacja
mapping - odwzorowanie
inverse - odwrotność
example - przykład
lemma - lemat
non-degenerable - nieosobliwe
matrices - macierze
equivalently - równoważnie
coset - warstwa
invariant subgroup - podgrupa normalna
homomorphism - homomorfizm
kernel - jądro
inner automorphism - automorfizm wewnętrzny

4.2 Wykład 23.02.16

abelian - abelowa
unique - unikalny
solution - rozwiązanie
chain - łańcuch
upper bound - ograniczenie górne
stricly bigger - istotnie większy
skew field - ciało nieprzemienne
extend - rozszerzać
divisible - podzielna
partially ordered set - zbiór częściowo uporządkowany
linearly ordered ser - zbiór liniowo uporządkowany
maximal element - element maksymalny
contraddition - sprzeczność