Spis treści

Rozdział 1

Grupy nilpotentne i rozwiązalne

1.1 Grupy nilpotentne

Skończone p – grupy mają szereg własności podobnych do grup przemiennych. U ich źródła leży stwierdzenie o nietrywialności centrum. Odnotujmy wlasność p – grup, która posłuży nam do zdefiniowania grup nilpotentnych.

Twierdzenie 1. *Jeżeli G jest p-grupą i $|G| = p^m$, to istnieje ciąg podgrup*

$$\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{m-1} \leqslant H_m = G,$$

taki że $H_i \trianglelefteq G$ i $H_{i+1}/H_i \leqslant Z(G/H_i)$

Dowód. Ciąg H_i definiujemy indukcyjnie. $H_0 = \{1\}$, $H_1 = Z(G)$, $H_{i+1} = \pi_i^{-1}(Z(G/H_i))$, gdzie $\pi_i : G \to G/H_i$. Ponieważ centrum p – grupy jest nietrywialne, to $|H_{i+1}| > |H_i|$ i dla pewnego n, $H_n = G$. □

W dalszym ciągu będziemy posługiwali się ciągami podgrup, więc od razu wprowadzimy definicje:

Definicja 1. *Niech $J \leqslant G$ będzie podgrupą. Ciągiem długości n od J do G nazywamy ciąg podgrup:*

$$J = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G.$$

Jeżeli $J = \{1\}$, to mówimy o ciągu grupy G.

a) Ciąg nazywa się **subnormalny** *jeżeli dla każdego i, $H_i \trianglelefteq H_{i+1}$.*

b) Ciąg nazywa się **normalny** *jeżeli dla każdego i, $H_i \trianglelefteq G$.*

c) *Ciąg normalny* $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$ *nazywa się* **centralny** *jeżeli dla każdego* i, $H_{i+1}/H_i \leqslant Z(G/H_i)$

d) *Jeżeli ciąg jest subnormalny, to grupy* H_{i+1}/H_i *nazywają się* **ilorazami** *ciągu.*

Poprzednie twierdzenie możemy więc sformułować tak: Skończona p – grupa posiada ciąg centralny.

Odnotujmy następujący lemat:

Lemat 1. *Ciąg normalny*

$$\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$$

jest centralny wtedy i tylko wtedy, gdy dla każdego $0 \leq i \leq n-1$

$$[H_{i+1}, G] \leqslant H_i.$$

Dowód. Warunek $H_{i+1}/H_i \leqslant Z(G/H_i)$ oznacza, że dla każdego $g \in G$ i każdego $x \in H_{i+1}$ komutator $[g, x] \in H_i$. □

Zdefiniujemy teraz rekurencyjnie dwa ciągi centralne dla dowolnej grupy G (niekoniecznie skończonej).

Definicja 2. *Niech* G *będzie grupą,*

- *Niech* $\Gamma_0(G) = G$ *i niech* $\Gamma_n(G) = [G, \Gamma_{n-1}(G)]$ *dla każdego* $n > 1$. *Otrzymujemy* ***dolny ciąg centralny:***

$$G = \Gamma_0(G) \geqslant \Gamma_1(G) \geqslant \Gamma_2(G) \geqslant \ldots$$

- *Niech* $Z_0(G) = \{1\}$ *i niech* $Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$ *dla każdego* $n > 0$. *Otrzymujemy* ***górny ciąg centralny:***

$$\{1\} = Z_0(G) \leqslant Z_1(G) \leqslant Z_2(G) \leqslant \ldots$$

Oczywiście istnieją grupy, dla których rekurencja nie prowadzi do właściwych ciągów – przykładem mogą być grupy doskonałe i grupy o trywialnym centrum. Jednak, jeżeli grupa posiada ciąg centralny, to nazwy górny i dolny wyjaśnia następujące stwierdzenie.

Stwierdzenie 1. *Dla dowolnej grupy* G *jeżeli*

$$\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$$

jest ciągiem centralnym, to dla każdego $i \geq 0$

$$\Gamma_{n-i}(G) \leqslant H_i \leqslant Z_i(G).$$

Jego dowód poprzedzimy lematem.

Lemat 2. *Niech H, K, L będą normalnymi podgrupami grupy G, $H \leqslant K$ i niech $K/H \leqslant Z(G/H)$. Wówczas $KL/HL \leqslant Z(G/HL)$*

Dowód. Rozważmy dla dowolnych $g \in G$, $k \in K$, $l \in L$ element $gklg^{-1}$. Mamy $gklg^{-1} = gkg^{-1}glg^{-1}$. Element $gkg^{-1} \in H$ gdyż $K/H \leqslant Z(G/H)$, zaś $glg^{-1} \in L$ z normalności $L \trianglelefteq G$. Zatem $gklg^{-1} \in HL$, co dowodzi tezy. □

Możemy teraz udowodnić stwierdzenie 1.

Dowód. Stwierdzenie $H_i \leqslant Z_i(G)$ dowodzimy przez indukcję ze względu na i. Dla $i = 0$ jest ono oczywiste. Z założenia indukcyjnego $H_{i-1} \leqslant Z_{i-1}(G)$, a zatem

$$H_{i-1}Z_{i-1}(G) = Z_{i-1}(G).$$

Korzystając z tej równości, założenia $H_i/H_{i-1} \leqslant Z(G/H_{i-1})$ i lematu mamy

$$\begin{aligned} H_iZ_{i-1}(G)/Z_{i-1}(G) &= H_iZ_{i-1}(G)/H_{i-1}Z_{i-1}(G) \leqslant Z(G/H_{i-1}Z_{i-1}(G)) = \\ &= Z(G/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G). \end{aligned}$$

Wynika z tego, że $H_iZ_{i-1}(G) \leqslant Z_i(G)$, co wobec $Z_{i-1}(G) \leqslant Z_i(G)$ oznacza, że $H_i \leqslant Z_i(G)$. Podobnie, pokażemy, że $\Gamma_j(G) \leqslant H_{n-j}$. Jest to oczywiste dla $j = 0$. Załóżmy, że $\Gamma_j(G) \leqslant H_{n-j}$. Ciąg jest centralny więc z Lematu 1,

$$[H_{n-j}, G] \leqslant H_{n-j-1},$$

a więc

$$\Gamma_{j+1}(G) = [\Gamma_j(G), G] \leqslant [H_{n-j}, G] \leqslant H_{n-j-1}.$$

□

Wniosek 1. *Dla grupy G, n jest najmniejszą liczbą dla której $Z_n(G) = G$ wtedy i tylko wtedy, gdy n jest najmniejszą liczba dla której $\Gamma_n(G) = \{1\}$.*

Definicja 3. *Grupa G nazywa się* ***nilpotentna klasy n****, jeżeli n jest najmniejszą liczbą naturalną dla której $Z_n(G) = G$. Grupa nazywa się* ***nilpotentna****, jeżeli jest nilpotentna klasy n dla pewnego n.*

Oczywiście jeżeli grupa ma ciąg centralny długosci n, to jest nilpotentna klasy co najwyżej n.Odnotujmy następujące własności grup nilpotentnych:

Twierdzenie 2. *a) Grupy abelowe są nilpotentne klasy* 1*.*

b) Podgrupa grupy nilpotentnej klasy n jest nilpotentna klasy co najwyżej n.

c) Grupa ilorazowa grupy nilpotentnej klasy n jest nilpotentna klasy co najwyżej n.

d) Jeżeli G jest nilpotentna klasy n a H nilpotentna klasy m, to $G \times H$ jest nilpotentna klasy $max(n, m)$.

e) Jeżeli $|G| = p^n$, to G jest nilpotentna klasy co najwyżej n.

Dowód. Punkt a) jest oczywisty, a punkt e) wynika z dowodu Twierdzenia 1.

Ad b) Jeżeli $H \leqslant G$, to $\Gamma_i(H) \leqslant \Gamma_i(G)$ i stąd teza.

Ad c) Niech $H \trianglelefteq G$ i niech $\pi : G \to G/H$ będzie epimorfizmem na grupę ilorazową. Wówczas $\Gamma_i(G/H) \leqslant \pi(\Gamma_i(G))$ i stąd teza.

Ad d) Wynika natychmiast z równości $\Gamma_i(G \times H) = \Gamma_i(G) \times \Gamma_i(H)$. □

Uwaga 1. *Zauważmy, że punktu d) powyższego twierdzenia nie można uogólnić na rozszerzenia - nie jest prawdą, że rozszerzenie grupy nilpotentnej przez nilpotentną jest grupa nilpotentną. Przykładem są np. grupy dihedralne D_{2n}, $\mathbb{Z}_n \trianglelefteq D_{2n} \to \mathbb{Z}_2$, gdzie n jest nieparzyste.*

1.2 Skończone grupy nilpotentne

Definicja nilpotentności i twierdzenie poprzedniego paragrafu dotyczą dowolnych grup, także nieskończonych.

Definicja 4. *Podgrupa $H \leqslant G$ nazywa się subnormalna w G, jeżeli istnieje ciąg subnormalny $H = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$*

Stwierdzenie 2. *Jeżeli G jest grupą nilpotentną i $H \leqslant G$ dowolną podgrupą, to H jest subnormalna w G.*

Dowód. Niech $Z_i(G)$ będzie górnym ciągiem centralnym dla grupy G. Wówczas $H_i = HZ_i(G)$ jest szukanym ciągiem subnormalnym. □

Następne twierdzenie charakteryzuje skończone grupy była nilpotentne.

Twierdzenie 3. *Skończona grupa G jest grupą nilpotentną wtedy i tylko wtedy, gdy jest produktem swoich podgrup Sylowa.*

Dowód. Oczywiście, jeżeli G jest produktem swoich podgrup Sylowa, które jako p – grupy są nilpotentne, to G jest nilpotentna. Wystarczy pokazać, że jeżeli G jest nilpotentna a P jest jej podgrupa Sylowa, to $P \trianglelefteq G$. Niech $P = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$ będzie subnormalnym ciągiem od P do G. Zauważmy, że dla każdego i, P jest podgrupą Sylowa w H_i. Z subnormalności $P \trianglelefteq H_1$ i jako normalna podgrupa Sylowa jest charakterystyczna. Ponieważ $H_1 \trianglelefteq H_2$, to $P \trianglelefteq H_2$, a zatem ponownie $P \blacktriangleleft H_2$. Rozumując indukcyjnie $P \trianglelefteq G$. □

1.3 Grupy rozwiązalne

Zdefiniujemy teraz najmniejszą klasę grup, która zawiera grupy abelowe i jest zamknięta ze względu na rozszerzenia.

Definicja 5. *Grupa nazywa się* **rozwiązalna** *jeżeli posiada ciąg subnormalny o abelowych ilorazach.*

Stwierdzenie 3. *Niech $H \trianglelefteq G \to G/H$ będzie rozszerzeniem. Wówczas G jest rozwiązalna wtedy i tylko wtedy, gdy grupy H i G/H są rozwiązalne.*

Dowód. Niech $\pi : G \to G/H$ i niech

$$\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$$

będzie subnormalnym ciągiem rozwiązującym dla G. Nietrudno sprawdzic, że wówczas

$$\{1\} = H_0 \cap H \leqslant H_1 \cap H \leqslant \cdots \leqslant H_{n-1} \cap H \leqslant H_n \cap H = H$$

oraz

$$\pi(H_0) \leqslant \pi(H_1) \leqslant \cdots \leqslant \pi(H_{n-1}) \leqslant \pi(H_n) = G$$

są subnormalnymi ciągami o ilorazach abelowych dla H i G/H odpowiednio.

Jeżeli zaś

$$\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = H$$

i

$$\{1\} = K_0 \leqslant K_1 \leqslant \cdots \leqslant K_{m-1} \leqslant K_m = G/H$$

są ciągami rozwiązującymi dla H i G/H, to

$$\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_n = H = \pi^{-1}(K_0) \leqslant \pi^{-1}(K_1) \leqslant \cdots \leqslant \pi^{-1}(K_m) = G$$

jest subnormalnym ciągiem o ilorazach abelowych dla G. □

Definicja 6. *Długością pochodną (derived length) grupy rozwiązalnej nazywamy długość najkrótszego ciągu rozwiązującego G.*

Liczbę tę możemy wyznaczyć algorytmicznie.

Definicja 7. *Definiujemy rekurencyjnie ciąg pochodny grupy G: NIech $G^{(0)} = G$, $G^{(1)} = [G, G]$ zaś $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$.*

Zachodzi następujace

Stwierdzenie 4. *Jeżeli $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$ jest subnormalnym ciągiem o ilorazach abelowych, to $G^{(i)} \leqslant H_{n-i}$.*

Dowód. Dowód jest przez indukcję i przypadek $i = 0$ jest oczywisty. Załóżmy, że $G^{(i)} \leqslant H_{n-i}$. Grupa H_{i+1}/H_i jest abelowa, więc $[H_i, H_i] \leqslant H_{i+1}$, co przy założeniu indukcyjnym daje tezę. □

Zatem jeżeli grupa G jest rozwiązalna, to istnieje n dla którego $G^{(n)} = \{1\}$. Jest także jasne, że najmniejsze n, dla którego $G^{(n)} = \{1\}$ jest długoscią pochodną grupy G. Zauważmy, że ciąg $G \geq G^{(1)} \geq \cdots \geq G^{(n-1)} \geq G^{(n)} = \{1\}$ jest ciągiem normalnym o abelowych ilorazach, a nawet składa się z podgrup charakterystycznych grupy G. Wynika z tego, że tym istotnym warunkiem dla którego grupy nilpotentne nie są zamknięte ze względu na rozszerzenia jest warunek centralności. Korzystając z charakteryzacji grup rozwiązalnych bardzo łatwo jest uzasadnić, że podgrupa i grupa ilorazowa grupy rozwiązalnej jest rozwiązalna. Dla $H \leqslant G$, $H^{(i)} \leqslant G^{(i)}$ i $G/H^{(i)} = \pi(G/H)^{(i)}$, gdzie $\pi : G \to G/H$. Odnotujmy jeszcze następujące twierdzenie.

Twierdzenie 4. *Jeżeli G jest skończoną grupą rozwiązalną, to G posiada ciąg subnormalny o ilorazach cyklicznych, a nawet o ilorazach cyklicznych rzędu pierwszego.*

Dowód. Ciąg subnormalny o skończonych abelowych ilorazach można zagęścić do pożądanego korzystając z postaci skończonych grup abelowych. □

Skończone rozwiązalne grupy abelowe mają następującą własność:

Twierdzenie 5. *Jeżeli G jest skończoną grupą rozwiązalną, zaś $V \trianglelefteq G$ minimalną podgrupą normalną, to V jest elementarną grupą abelową.*

Dowód. Rozważmy $[V, V] \blacktriangleleft V$. Z minimalności V, $[V, V] = V$ lub $[V, V] = \{1\}$. V jest rozwiązalna, jako podgrupa więc pierwsza mmożliwość odpada i V jest grupą przemienną. Niech P będzie p – podgrupą Sylowa w V. Z abelowości V, $P \blacktriangleleft V$ a więc $P \trianglelefteq G$ i z minimalności $P = V$. Podobnie $\{x \in P\colon x^p = 1\} \blacktriangleleft V$, więc $\{x \in P\colon x^p = 1\} \trianglelefteq G$ i $\{x \in P\colon x^p = 1\} = V$. □

Mamy dwa słynne twierdzenia charakteryzujące skończone grupy rozwiązalne.

Twierdzenie 6. (Burnside'a) *Każda grupa rzędu $p^m q^n$, gdzie p i q sa liczbami pierwszymi jest rozwiązalna.*

Twierdzenie 7. (Feita - Thompsona) *Każda grupa rzędu nieparzystego jest rozwiązalna.*

1.4 Klasyfikacja rozszerzeń z abelowym jądrem

Będziemy rozważać sytuację, gdy grupa G jest rozszerzeniem grupy H przez grupę K, czyli mamy diagram:

$$K \trianglelefteq G \xrightarrow{p} \!\!\!\!\rightarrow H\ .$$

Jeżeli dla homomorfizmu $p : G \to H$ istnieje homomorfizm nazywany *przekrojem* $s : H \to G$, $ps = id_H$, to G jest produktem półprostym K i H, przekrój s definiuje działanie $\varphi : H \to \mathrm{Aut}(K)$ wzorem $\varphi(h)(k) = s(h)ks(h)^{-1}$ i wówczas G jest izomorficzna z $K \rtimes_\varphi H$.

Rozważmy teraz przypadek, w którym K jest grupą przemienną. Wówczas nawet gdy nie istnieje przekrój, to rozszerzenia zadaje działanie grupy H na grupie K. Dla g, g' takich, że $p(g) = p(g') = h$ mamy: $g' = gk$ dla pewnego $k \in K$. Z przemienności grupy K automorfizmy wewnętrzne $g \cdot g^{-1}, g' \cdot g'^{-1} \colon K \to K$ są równe. Możemy więc zdefiniować działanie H na K wzorem

$$\varphi : H \to \mathrm{Aut}(K), \qquad \varphi(h)(k) = gkg^{-1}, \text{ gdzie } p(g) = h.$$

Działanie grupowe w K będziemy zapisywać addytywnie. Jeśli zadane jest działanie $\varphi : H \to \mathrm{Aut}(K)$ i K jest grupą przemienną, to będziemy mówili, że K jest H modułem i będziemy pisać xa zamiast $\varphi(x)(a)$.

Naszym zadaniem będzie sklasyfikowanie rozszerzeń grupy H przez przemienną grupę K odpowiadających zadanej strukturze H modułu na K. Sprecyzujemy słowo "sklasyfikować".

Definicja 8. *Niech K będzie H modułem. Powiemy, że rozszerzenia $K \xrightarrow{i} G \xrightarrow{p} H$ i $K \xrightarrow{i'} G' \xrightarrow{p'} H$ odpowiadających zadanej strukturze H modułu na K są równoważne wtedy i tylko wtedy, gdy istnieje izomorfizm $\psi : G \to G'$ dla którego przemienny jest diagram:*

$$\begin{array}{ccccc} K & \xrightarrow{i} & G & \xrightarrow{p} & H \\ {\scriptstyle id_K}\downarrow & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle id_H} \\ K & \xrightarrow{i'} & G' & \xrightarrow{p'} & H \end{array}.$$

Niech

$$K \xrightarrow{i} G \xrightarrow{p} H$$

będzie rozszerzeniem odpowiadającym H modułowi K. Funkcję $l : H \to G$ będziemy nazywać podniesieniem, jeżeli $pl = id_H$. Mówimy, że podniesienie jest *znormalizowane* jeżeli $l(1) = 0 \in K$ i w dalszym ciągu rozpatrywać będziemy tylko znormalizowane podniesienia.

Definicja 9. *Jeżeli $l : H \to K$ jest znormalizowanym podniesieniem, to funkcję $f : H \times H \to K$ zdefiniowaną wzorem*

$$f(x, y) = l(x)l(y)l(xy)^{-1}$$

nazywamy zbiorem ilorazowym lub znormalizowanym kocyklem.

Tak więc funkcja f "mierzy" odstępstwo podniesienia l od bycia homomorfizmem, czyli przekrojem. Jeżeli G jest produktem półprostym a l przekrojem, to $f = 0$

Stwierdzenie 5. *Niech H będzie grupą a K – H modułem. Jeżeli*

$$K \xrightarrow{i} G \xrightarrow{p} H$$

jest rozszerzeniem odpowiadającym temu modułowi, l znormalizowanym podniesieniem, zaś $f : H \times H \to K$ wyznaczonym przezeń kocyklem, to:

a) dla dowolnych $x, y \in H$, $f(x, 1) = f(1, y) = 0$;

b) dla dowolnych $x, y, z \in H$ spełniona jest równość zwana tożsamością kocyklu:

$$f(x, y) + f(xy, z) = xf(y, z) + f(x, yz).$$

Dowód. Punkt a) jest oczywisty. Ad b): pamiętając, że oznaczne symbolem $+$ działanie w K jest tak na prawdę mnożeniem w G mamy:

$$f(x,y)+f(xy,z) = l(x)l(y)l(xy)^{-1}l(xy)l(z)l(xyz)^{-1} = l(x)l(y)l(z)l(xyz)^{-1} =$$

$$= \underbrace{l(x)l(y)l(z)l(yz)l(x)^{-1}}\,\underbrace{l(x)l(yz)l(xyz)^{-1}} = l(x)f(y,z)l(x)^{-1}f(x,yz) =$$

$$= xf(y,z) + f(x,yz)$$

□

Stwierdzenie 6. *Niech H będzie grupą a K – H modułem. Niech $f : H \times H \to K$ spełnia warunki a) i b) poprzedniego stwierdzenia. Wówczas istnieje rozszerzenie*

$$K \xrightarrow{i} G \xrightarrow{p} H$$

odpowiadającym H modułowi K oraz znormalizowane podniesienie tego rozszerzenia, takie że f jest odpowiadającym znormalizowanym zbiorem iloczynowym.

Dowód. Zdefiniujemy strukturę grupy na zbiorze $K \times H$. Grupę tę będziemy oznaczać symbolem $G(K, H, f)$. Działania grupowe definiujemy następująco:

- elementem neutralnym jest $(0, 1)$;
- $(a, x)(b, y) = (a + xb + f(x, y), xy)$;
- $(a, x)^{-1} = (-x^{-1}a - x^{-1}f(x, x^{-1}), x^{-1})$.

Własność a) gwarantuje, że $(0,1)$ jest elementem neutralnym, zaś tożsamość kocyklu sprawia, że działanie jest łączne. Tak skonstruowana grupa $G(K,H,f)$ jest rozszerzeniem H przez K, bowiem $i_f : K \to G(K,H,f)$, $i(a) = (a,1)$ jest włożeniem na podgrupę izomorficzną z K, która jest normalna. Mamy epimorfizm $p_f : G(K,H,f) \to H$, $p_f(a,x) = x$, którego jądrem jest K. Tak więc $G(K,H,f)$ jest rozszerzeniem H przez K. Musimy jeszcze sprawdzić, czy to rozszerzenie zadaje wyjściową strukturę H modułu na K. W tym celu liczymy:

$$(a',x)(a,1)(a',x)^{-1} = (a' + xa + f(x,1), x)(-x^{-1}a' - x^{-1}f(x,x^{-1}), x^{-1}) =$$

$$= ((a' + xa, x)(-x^{-1}a' - x^{-1}f(x,x^{-1}), x^{-1}) =$$

$$= (a' + xa + x(-x^{-1}a' - x^{-1}f(x,x^{-1}) + f(x,x^{-1}), 1) =$$

$$= (a' + xa - a' - f(x,x^{-1}) + f(x,x^{-1}, 1) = (xa, 1).$$

Niech teraz $l_f : H \to G(K,H,f)$ będzie podniesieniem $l_f(x) = (0,x)$. Jest to podniesienie znormalizowane i kocykl przez l_f wyznaczony jest równy:

$$l_f(x)l_f(y)l_f(xy)^{-1} = (0,x)(0,y)(0,xy)^{-1} = (f(x,y), xy)(-(xy)^{-1}f(xy,(xy)^{-1}), (xy)^{-1}) =$$

$$= (f(x,y) + xy(-(xy)^{-1}f(xy,(xy)^{-1})) + f(xy,(xy)^{-1}), 1) =$$

$$= (f(x,y) - f(xy,(xy)^{-1}) + f(xy,(xy)^{-1}), 1) = (f(x,y), 1).$$

□

Jeżeli kocykl f pochodzi od pewnego rozszerzenia wraz ze znormalizowanym podniesieniem l, $K \xrightarrow{i} G \underset{p}{\overset{l}{\leftrightarrows}} H$, to skonstruowana grupa $G(K,H,f)$ jest izomorficzna z wyjściową grupą G. Dokładniej:

Stwierdzenie 7. *Jeżeli K jest H modułem, $K \xrightarrow{i} G \xrightarrow{p} H$ jest rozszerzeniem odpowiadającym strukturze modułu, l podniesieniem a f kocyklem wyznaczonym przez l, to istnieje izomorfizm $\psi : G(K,H,f) \to G$, dla którego przemienny jest diagram:*

$$\begin{array}{ccccc} K & \xrightarrow{i_f} & G(K,H,f) & \underset{p_f}{\overset{l_f}{\leftrightarrows}} & H \\ {\scriptstyle id_K}\downarrow & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle id_H} \\ K & \xrightarrow{i} & G & \underset{p}{\overset{l}{\leftrightarrows}} & H \end{array} .$$

Dowód. Definiujemy $\psi(a,x) = al(x)$. Czytelnikowi pozostawiamy sprawdzenie, że ψ jest izomorfizmem spełniającym zadane warunki. □

Mamy zatem bijekcję klas izomorfizmów rozszerzeń ze znormalizowanym podniesieniem ze zbiorem znormalizowanych kocykli.

Chcemy klasyfikować dla danego H modułu K rozszerzenia na podstawie kocykli przypisując kocyklowi f rozszerzenie $G(K,H,f)$ i pozbyć się niejednoznaczności związanej z wyborem podniesienia.

Rozważmy dwa podniesienia l, l' rozszerzenia $K \to G \to H$ i wyznaczone przez nie kocykle f, f'. Niech $h : H \to K$ będzie zdefiniowane wzorem $l'(x) = h(x)l(x)$ (warstwy prawostronne są równe lewostronnym). Mamy:

$$\begin{aligned} f'(x,y)f(x,y)^{-1} =& l'(x)l'(y)l'(xy)^{-1}l(xy)l(y)^{-1}l(x)^{-1} = \\ =& h(x)l(x)h(y)l(y)l(xy)^{-1}h(xy)^{-1}l(xy)l(y)^{-1}l(x)^{-1} = \\ =& h(x)\underbrace{l(x)h(y)l(x)^{-1}}\underbrace{l(x)l(y)l(xy)^{-1}}h(xy)^{-1}\underbrace{l(xy)l(y)^{-1}l(x)^{-1}} = \\ =& h(x)\underbrace{l(x)h(y)l(x)^{-1}}h(xy)h(xy)^{-1}h(xy)^{-1} = \\ =& h(x)\underbrace{l(x)h(y)l(x)^{-1}}h(xy)^{-1} \end{aligned}.$$

Przechodząc do addytywnego zapisy K jako H modułu mamy:

$$f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x).$$

Definicja 10. *Niech K będzie H modułem. Funkcję $g : H \times H \to K$ nazywamy* **kobrzegiem** *wtedy i tylko wtedy, gdy istnieje funkcja $h : H \to K$, dla której*

$$h(1) = 0 \quad oraz \quad g(x,y) = xh(y) - h(xy) + h(x).$$

Z powyższego rachunku wynika następujacy wniosek:

Wniosek 2. *Kocykle wyznaczone przez to samo rozszerzenie $K \to G \to H$ różnią się o kobrzeg.*

Stwierdzenie 8. *Niech K będzie H modułem. Jeżeli $g : H \times H \to K$ jest kobrzegiem, to jest (znormalizowanym) kocyklem.*

Dowód. Jest to proste sprawdzenie. □

Podobnie prosty rachunek pokazuje, że :

Stwierdzenie 9. *Zbiór (znormalizowanych) kocykli jest abelową grupą, a zbiór kobrzegów jej podgrupą.*

Grupę znormalizowanych kocykli oznaczać będziemy symbolem $Z^2(H,K)$, zaś jej podgrupę kobrzegów symbolem $B^2(H,K)$.

Definicja 11. *Niech K będzie H modułem. Drugą grupą kohomologii nazywamy grupę ilorazową :*

$$H^2(H,K) = Z^2(H,K)/B^2(H,K).$$

Twierdzenie 8. Schreira *Niech K będzie H modułem. Niech $e(K,H)$ oznacza klasę izomorfizmów rozszerzeń H przez K. Wówczas*

$$\Psi : H^2(H,K) \to e(K,H) \qquad \Psi(f + B^2(H,K)) = [G(K,H,f)]$$

jest bijekcją. Ponadto $\Psi(0)$ jest produktem półprostym.

Dowód. Musimy pokazać, że

a) Ψ jest dobrze określone;

b) Ψ jest różnowartościowe;

c) Ψ jest "na".

Punkt d) został udowodniony. Dla dowodu a) załóżmy, że $K \xrightarrow{i} G \underset{p}{\overset{l}{\leftrightarrows}} H$ i $K \xrightarrow{i'} G' \underset{p'}{\overset{l'}{\leftrightarrows}} H$ są rozszerzeniami odpowiadającymi kocyklom f i f'. (Wiemy, że $G(K,H,f)$ i $G(K,H,f')$ takie są, ale piszemy G i G' dla prostoty oznaczeń.) Załóżmy, że f i f' różnią się o kobrzeg $f - f' = h$, to znaczy

$$f(x,y) - f'(x,y) = xh(y) - h(xy) + h(x).$$

Rozważmy diagram:

$$\begin{array}{ccccc} K & \xrightarrow{i} & G & \underset{p}{\overset{l}{\leftrightarrows}} & H \\ {\scriptstyle id_K}\downarrow & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle id_H} \\ K & \xrightarrow{i'} & G' & \underset{p'}{\overset{l'}{\leftrightarrows}} & H \end{array}$$

gdzie $\gamma(al(x)) = h(x)al'(x)$ Musimy sprawdzić, że γ jest homomorfizmem i izomorfizmem i że diagram (litych strzałek) jest przemienny, co pozostawiamy czytelnikowi. Jeśli natomiast istnieje izomorfizm γ, dla którego diagram (litych strzałek) jest przemienny, to definiujemy $\gamma l : H \to G'$. Ponieważ γ jest izomorfizmem to γl jest podniesieniem wyznaczającym kocykl f. Z wniosku 1 wynika, że $f - f$ jest kobrzegiem.

□

1.5 Zadania

1.5.1. Niech $f : H \to H'$ będzie homomorfizmem. Pokazać, że indukuje on przekształcenie $f^{\#} : e(H',K) \longrightarrow e(H,K)$ oraz homomorfizm $f^* : H^2(H',K) \to H^2(H,K)$ dla którego przemienny jest diagram:

$$\begin{array}{ccc} H^2(H',K) & \xrightarrow{\Psi} & e(H',K)\,. \\ {\scriptstyle f^*}\downarrow & & \downarrow{\scriptstyle f^{\#}} \\ H^2(H,K) & \xrightarrow{\Psi} & e(H,K) \end{array}$$

1.5.2. Niech $f : K \to K'$ będzie homomorfizmem. Pokazać, że indukuje on przekształcenie $f_{\#} : e(H,K) \longrightarrow e(H,K')$ oraz homomorfizm $f_* : H^2(H,K) \to H^2(H,K')$ dla którego przemienny jest diagram:

$$\begin{array}{ccc} H^2(H,K) & \xrightarrow{\Psi} & e(H,K) \\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_{\#}} \\ H^2(H,K') & \xrightarrow{\Psi} & e(H,K') \end{array} .$$

1.5.3. Opisać "sumę" rozszerzeń wyznaczoną przez sume kocykli i izomorfizm $\Psi : H^2(H,K) \to e(K,H)$.

Rozdział 2

Teoria Galois

2.1 Ciało rozkładu wielomianu

2.1.1 Definicja i podstawowe własności

Niech K będzie ciałem i niech $f \in K[X]$ będzie wielomianem nierozkładalnym. Ciało $K[X]/(f)$ jest rozszerzeniem generowanym przez warstwę $X+(f)$ i element $X + (f)$ jest pierwiastkiem wielomianu f w $K[X]/(f)$.

Definicja 12. *Mówimy, że rozszerzenie $K \subset L$ jest rozszerzeniem o pierwiastek wielomianu $f \in K[X]$, jeżeli $L = K(u)$ i u jest pierwiastkiem wielomianu f.*

Rozszerzenie o pierwiastek wielomianu nierozkładalnego jest wyznaczone jednoznacznie.

Twierdzenie 9. *Niech $\varphi : K \to L$ będzie izomorfizmem, zaś $f \in K[X]$ wielomianem nierozkładalnym. Niech $\varphi_* : K[X] \to L[X]$ będzie indukowanym przez φ izomorfizmem pierścieni wielomianów. Niech $K(u)$ będzie rozszerzeniem o pierwiastek wielomianu f a $L(\tilde{u})$ rozszerzeniem o pierwiastek $\varphi_*(f) = \tilde{f}$. Wówczas istnieje izomorfizm $\tilde{\varphi} : K(u) \to L(\tilde{u})$, dla którego $\tilde{\varphi}_{|_K} = \varphi$ i $\tilde{\varphi}(u) = \tilde{u}$.*

Dowód. Szukany izomorfizm jest złożeniem następujących izomorfizmów nad K:

$$K(u) \xleftarrow{\cong} K[X]/(f) \xrightarrow{\cong} L[X]/(\tilde{f}) \xrightarrow{\cong} L(\tilde{u})$$

□

Definicja 13. *Niech K będzie ciałem i niech $f \in K[X]$. Mówimy, że rozszerzenie $K \subset M$ jest ciałem rozkładu wielomianu f jeżeli:*

- *wielomian $f \in M[X]$ jest iloczynem wielomianów liniowych;*
- *$M = K(u_1, \ldots, u_k)$, gdzie $u_1, \ldots, u_k$ są wszystkimi pierwiastkami wielomianu f w M.*

Twierdzenie 10. *Dla dowolnego wielomianu $f \in K[X]$ istnieje jego ciało rozkładu.*

Dowód. Indukcja ze względu na $\deg(f)$. Jeżeli $\deg(f) = 1$, to ciałem rozkładu f jest K. Dla $\deg(f) > 1$, niech g będzie wielomianem nierozkładalnym, $g \mid f$. Niech $K \subset K(u)$ będzie rozszerzeniem o pierwiastek g. W pierścieniu $K(u)[X]$ mamy $f = (X - u)h$. Z założenia indukcyjnego istnieje ciało rozkładu $K(u) \subset M$ wielomianu $h \in K(u)$. Jest jasne, że $K \subset M$ jest ciałem rozkładu f nad K. □

Jest jasne, że ciało rozkładu wielomianu f jest rozszerzeniem skończonym stopnia co najwyżej $n!$, $n = \deg(f)$.
Ciało rozkładu jest wyznaczone jednoznacznie w następującym sensie:

Twierdzenie 11. *Niech $\varphi : K \to L$ będzie izomorfizmem ciał. Niech $\varphi_* : K[X] \to L[X]$. Niech $K \subset M$ będzie ciałem rozkładu wielomianu f, a $L \subset N$ ciałem rozkładu wielomianu $\varphi_*(f)$. Wówczas istnieje izomorfizm $\tilde{\varphi} : M \to N$, dla którego $\tilde{\varphi}_{|_K} = \varphi$.*

$$\begin{array}{ccc} M & \overset{\tilde{\varphi}}{\rightarrowtail} & N \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi} & L \end{array}$$

Dowód. Dowód ze względu na stopień rozszerzenia $[M : K]$.
Jeżeli $[M : K] = 1$, czyli $M = K$, to f jest iloczynem czynników liniowych w $K[X]$, a zatem $\varphi_*(f)$ jest iloczynem czynników liniowych w $L[X]$ i $L = N$ oraz $\tilde{\varphi} = \varphi$.
Niech g będzie nierozkładalnym dzielnikiem f stopnia co najmniej 2. Niech $u \in M$ będzie pierwiastkiem wielomianu g w M, zaś $\tilde{u} \in N$ będzie pierwiastkiem wielomianu $\varphi_*(g)$. Rozpatrzmy diagram:

$$\begin{array}{ccc} M & \overset{\tilde{\varphi}}{\rightarrowtail} & N \\ \uparrow & & \uparrow \\ K(u) & \xrightarrow{\bar{\varphi}} & L(\tilde{u}) \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi} & L \end{array}$$

Izomorfizm $\bar{\varphi}$ wynika z Twierdzenia 9. Ponieważ $[M : K(u)] < [M : K]$, to teza wynika z założenia indukcyjnego. □

Możemy spytać, kiedy rozszerzenie skończone jest ciałem rozkładu pewnego wielomianu.

Twierdzenie 12. *Niech $K \subset M$ będzie rozszerzeniem skończonym. Wówczas następujące warunki są równoważne:*

a) M jest ciałem rozkładu nad K pewnego wielomianu z $K[X]$;

b) każdy nierozkładalny wielomian z $K[X]$, który ma pierwiastek w ciele M rozkłada się w ciele M na czynniki liniowe.

Dowód. $a) \Rightarrow b)$ Niech M będzie ciałem rozkładu wielomianu $f \in K[X]$. Niech $g \in K[X]$ będzie wielomianem nierozkładalnym i niech $u \in M$ będzie jego pierwiastkiem. Przypuśćmy, że g nie rozkłada się w M na czynniki liniowe. Zatem istnieje nierozkładalny wielomian $h \in M[X]$, $\deg(h) > 1$ i $h|g$ w $M[X]$. Niech $M(v)$ będzie rozszerzeniem M o pierwiastek wielomianu h. Oczywiście zarówno $K(u)$ jak i $M(v)$ są rozszerzeniami K o pierwiastek nierozkładalnego wielomianu $g \in K[X]$. Zatem $K(u)$ jak i $M(v)$ są izomorficzne nad K – jest to niemożliwe, gdyż $[M(v) : K] > [M : K] \geq [K(u) : K]$.

$b) \Rightarrow a)$ Niech $v_1, \dots v_n \in M$ będzie bazą M jako przestrzeni liniowej nad K. Niech $f_i \in K[X]$ będzie wielomianem minimalnym dla v_i. Rozpatrzmy wielomian $f = f_1 \dots f_n$. Z założenia wielomian f rozkłada się w M na czynniki liniowe. Ponieważ M jest generowane przez pierwiastki f, to M jest ciałem rozkładu wielomianu f nd K.

□

2.1.2 Istnienie i jednoznaczność ciał skończonych.

Niech K będzie ciałem skończonym charakterystyki p. Wiemy, że K jako przestrzeń liniowa nad $\mathbb{Z}_p$ ma p^m elementów. Pokażemy, że dla każdego $m \in \mathbb{N}$ istnieje ciało p^m elementowe i jest ono wyznaczone jednoznacznie z dokładnością do izomorfizmu.

Zaczniemy od ogólnej obserwacji.

Definicja 14. *Jeżeli $f = a_n X^n + \dots + a_1 X + a_0 \in K[X]$, to jego pochodną nazywamy wielomian $f' = n a_n X^{n-1} + \dots 2a_2 X + a_1$.*

Uwaga 2. *Niech $a \in K$ będzie pierwiastkiem wielomianu $f \in K[X]$, czyli równoważnie $x - a \mid f$ w $K[X]$. Wówczas $(X - a)^2 \mid f$ w $K[X]$ wtedy i tylko wtedy, gdy $X - a \mid f'$.*

Twierdzenie 13. (Galois) *Niech p będzie liczbą pierwszą . Wówczas*

a) dla każdego $m \in \mathbb{N}$ istnieje ciało p^m elementowe;

b) każde dwa ciała p^m elementowe są izomorficzne.

Dowód. Niech $q = p^m$.

a) Niech K będzie ciałem rozkładu wielomianu $f = X^q - X \in \mathbb{Z}_p[X]$. Pokażemy, że $|K| = q$. Niech $D = \{a \in K \colon a^q - a = 0\}$. $(X^q - X)' = qX^{q-1} - 1 = -1$, więc f i f' nie maja wspolnego dzielnika i wielomian f ma w K, q pierwiastków różnych, czyli $|D| = q$. Zauważmy, że D jest podciałem K, a ponieważ K jest generowane przez pierwiastki f, to $D = K$;

b) z jednoznaczności ciała rozkładu wielomianu wynika, że wystarczy pokazać, że każde ciało q elementowe jest ciałem rozkładu wielomianu $f = X^q - X \in \mathbb{Z}_p[X]$. Dla każdego $a \in K$, $a \neq 0$, $a^{q-1} = 1$, więc a jest pierwiastkiem wielomianu $X^{q-1} - 1$. Jeżeli rozpatrzymy wielomian f, to dodajemy 0 i widzimy, że wszystkie elementy K są pierwiastkami f, czyli K jest ciałem rozkładu.

□

2.1.3 Zadania

2.1.1. Udowodnić, że jeżeli $K \subset L$ jest ciałem rozkładu wielomianu $f \in K[X]$ stopnia n, to $[L : K] \mid n!$. Pokazać, że jeżeli $[L : K] = n!$, to f jest wielomianem nierozkładalnym.

2.1.2. Niech $K \subset L \subset M$ będą rozszerzeniami. Niech ciało L będzie generowane przez pewne pierwiastki wielomianu $f \in K[X]$. Udowodnić, że M jest ciałem rozkładu wielomianu f nad K wtedy i tylko wtedy gdy M jest ciałem rozkładu wielomianu f nad L.

2.1.3. Niech $f \in K[X]$ będzie wielomianem stopnia $f = X^n + a_{n-1}X \cdots + a_1X + a_0$, $n \geq 1$.. Niech $f|X^m - b$. Korzystając z ciała rozkładu wielomianu f, pokazać że $b^n = (-1)^{mn}a_0^m$.

2.1.4. Niech K będzie ciałem skończonym charakterystyki p. Pokazać, że istnieje element $a \in K$ dla którego $K = \mathbb{Z}_p(a)$.

Wskazówka: Licząc elementy pokazać, że suma mnogościowa właściwych podciał K jest różna od K.

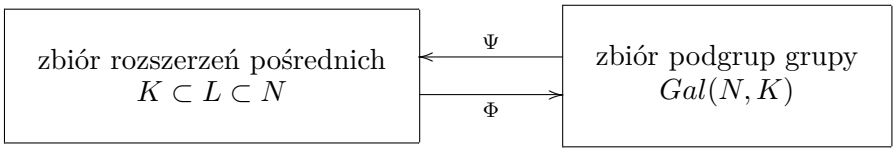
2.2 Podstawy teorii Galois.

2.2.1 Odpowiedniość Galois

Dla rozważań w tym paragrafie ustalamy rozszerzenie $K \subset N$.

Definicja 15. *Grupą Galois rozszerzenia $K \subset N$ nazywamy grupę tych automorfizmów $N \to N$, które są identycznością na ciele K. Grupę tę będziemy oznaczać symbolem $Gal(N, K)$.*

Teoria Galois to badanie związków między zbiorem ciał pośrednich między K a N z jednej strony a zbiorem podgrup grupy Galois z drugiej. Rozpatrzmy następujące przekształcenia:



$$\Phi(L) = \{\varphi \in Gal(N, K) \colon \forall_{x \in L}\ \varphi(x) = x\}$$

$$\Psi(H) = N^H$$

Twierdzenie 14. *Przekształcenia Phi i Ψ mają następujące własności:*

(1) Φ oraz Ψ odwracają inkluzje;

(2) $L \subset \Psi\Phi(L)$ dla każdego ciała pośredniego L;

(3) $H \leqslant \Phi\Psi(H)$ dla każdej podgrupy $H \leqslant Gal(N, K)$;

(4) $\Phi\Psi\Phi = \Phi$ i $\Psi\Phi\Psi = \Psi$

Dowód. Jedynie punkt 4) wymaga uzasadnienia - jest on prostą konsekwencja poprzednich zawierań: $L \subset \Psi\Phi(L)$, więc z punktu 1) mamy : $\Phi\Psi\Phi(L) \leqslant \Phi(L)$. Dla dowolnej podgrupy H, $H \leqslant \Phi\Psi(H)$ i podstawiając $H = \Phi(L)$ otrzymujemy $\Phi(L) \leqslant \Phi\Psi\Phi(L)$. Drugą równość dowodzimy analogicznie. □

Definicja 16. *Ciało $\Psi\Phi(L)$ nazywamy domknięciem ciała L i oznaczamy symbolem $\overline{L}$. Ciało pośrednie $K \subset L \subset N$ nazywa się domknięte jeżeli $L = \overline{L}$.*

Z punktu (4) powyżej wynika, że $\overline{\overline{L}} = \overline{L}$.

Definicja 17. *Podgrupę $\Phi\Psi(H)$ nazywamy domknięciem podgrupy $H \leqslant Gal(N, K)$ i oznaczamy $\overline{H}$. Podgrupa H nazywa się domknięta jeżeli $\overline{\overline{H}} = \overline{H}$.*

Z punktu (4) powyżej wynika, że $\overline{\overline{H}} = \overline{H}$.

Przykład 1. *Niech $K \subset N$ będzie rozszerzeniem.*

a) $\Phi(N) = \{1\}$, $\overline{N} = N$;

b) $\Psi(Gal(N,K)) = K$, $\overline{Gal(N,K)} = Gal(N,K)$;

c) $\Psi(\{1\}) = N$, $\overline{\{1\}} = \{1\}$;

d) $Gal(\mathbb{Q}(\sqrt[3]{5}), \mathbb{Q}) = \{1\}$, $\overline{\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{5})$;

Definicja 18. *Rozszerzenie $K \subset N$ nazywa się rozszerzeniem Galois, jeżeli $\overline{K} = K$.*

Zauważmy, że $\Phi(L) = Gal(N, L)$ oraz że ciało pośrednie L jest domknięte wtedy i tylko wtedy, gdy rozszerzenie $L \subset N$ jest Galois.
Z Twierdzenia 14 wynika, że obrazem domkniętego ciała pośredniego jest domknięta podgrupa i podobnie dla przekształcenia Ψ. Mamy więc następujące:

Stwierdzenie 10. *Niech $K \subset N$ będzie rozszerzeniem. Przekształcenia Φ i Ψ ustalają wzajemnie jednoznaczną odpowiedniość między domkniętymi ciałami pośrednimi a domkniętymi podgrupami.*

Musimy teraz ustalić, co to znaczy, że ciało pośrednie jest domknięte i podgrupa jest domknięta. Zacznijmy od następującej przydatnej obserwacji:

Uwaga 3. *Niech $K \subset L \subset M \subset N$ będzie ciągiem rozszerzeń, zaś $\{1\} \leqslant \Phi(M) \leqslant \Phi(L) \leqslant Gal(N,K)$ odpowiadającym mu ciągiem podgrup. Wówczas istnieje różnowartościowe przekształcenie ze zbioru warstw $\Phi(L)/\Phi(M)$ w zbiór $\{\varphi_{|_M} : M \to N \mid \varphi \in Gal(N,K)\}$.*

Dowód. Każde dwa elementy warstwy $\Phi(L)/\Phi(M)$ różnią się o identyczność na M, więc przekształcenie jest dobrze określone. Natomiast jeśli $\varphi_{|_M} = \varphi'_{|_M}$, to $\varphi_{|_M}\varphi'^{-1}_{|_M} = id_{|_M}$, więc $\varphi_{|_M}$ i $\varphi'_{|_M}$ należą do tej samej warstwy. □

Twierdzenie 15. *Niech $K \subset L \subset M \subset N$ będzie ciągiem rozszerzeń. Jeżeli rozszerzenie $L \subset M$ skończone, to $|\Phi(L) : \Phi(M)| \leq |M : L|$.*

Dowód. Dowód przez indukcję ze względu na $|M : L|$. Jeżeli $|M : L| = 1$, to teza jest oczywista.
W kroku indukcyjnym rozpatrujemy wpierw przypadek, gdy istnieje ciało L_0, $L \subsetneq L_0 \subsetneq M$. Z założenia indukcyjnego

$$|\Phi(L) : \Phi(L_0)||\Phi(L_0) : \Phi(M)| \leq |M : L_0||L_0 : L| = |M : L|,$$

ale $|\Phi(L) : \Phi(L_0)||\Phi(L_0) : \Phi(M)| = |\Phi(L) : \Phi(M)|$.
Jeżeli ciała pośredniego między L a M nie ma, to $M = L(u)$ dla pewnego $u \in M$. Niech $f \in L[X]$ będzie wielomianem minimalnym dla u. Zgodnie z uwagą

3 każdy element warstwy $\Phi(L)/\Phi(M)$ wyznacza inny obraz elementu u. Ponieważ rozpatrywane automorfizmy są identycznością na L, to obraz u musi być także pierwiastkiem wielomianu f, a tych różnych jest co najwyżej $\deg(f) = |M : L|$. □

Analogiczne twierdzenie jest prawdziwe po stronie podgrup grupy Galois.

Twierdzenie 16. *Jeżeli $H \leqslant J \leqslant Gal(N, K)$ jest ciągiem podgrup i $|J : H| < \infty$, to $|\Psi(H) : \Psi(J)| \leq |J : H|$.*

Dowód. Podobnie jak w uwadze 3 mamy dobrze zdefiniowane przekształcenie $J/H \to \{\varphi_{|_{\Psi(H)}} : \Psi(H) \to N, |\ \varphi \in Gal(N, K)\}$. Niech $|J : H| = n$ i przypuśćmy nie wprost, że $|\Psi(H) : \Psi(J)| > n$. Niech $u_1, \dots u_{n+1}$ będą liniowo niezależnymi nad $\Psi(J)$ elementami $\Psi(H)$. Niech $\varphi_1 = id, \varphi_2, \dots, \varphi_n$ będą reprezentantami warstw J/H. Możemy założyć, że $\varphi_1 = id$. Rozpatrzmy $n+1$ wektorów w przestrzeni liniowej N^n nad $\Psi(J)$: $\alpha_1 = (\varphi_1(u_1), \varphi_2(u_1), \dots, \varphi_n(u_1)), \alpha_2 = (\varphi_1(u_2), \varphi_2(u_2), \dots, \alpha_{n+1} = \varphi_n(u_2)), \dots (\varphi_1(u_{n+1}), \varphi_2(u_{n+1}), \dots, \varphi_n(u_{n+1}))$. Układ ten liniowo zależny więc podprzestrzeń $A = \{(a_1, \dots, a_{n+1}) \colon \sum_{i=1}^{n+1} a_i\alpha_i = 0\} \leqslant N^{n+1}$ jest nietrywialna i ma następujące własności:

- dla dowolnego niezerowego elementu A nie wszystkie jego współrzędne należą do $\Psi(J)$. Wynika to z tego, że założyliśmy, iż elementy u_i są liniowo niezależne a $\varphi_1 = id$.
- zbiór A jest H niezmieniczy, bowiem dla $\eta \in H$, $\eta(\sum_{i=1}^{n+1} a_i\alpha_i) =$

Wybierzmy w A element o największej liczbie zerowych współrzędnych. Dokonując ewentualnego przenumerowania możemy założyć, że ciąg wygląda następująco: $(a_1, a_2, \dots, a_r, 0, \dots 0)$ i że $a_2 \notin \Psi(J)$. □

Oba twierdzenia złożone razem prowadzą do następującego.

Twierdzenie 17. *Niech $K \subset N$ będzie rozszerzeniem i $Gal(N, K)$ jego grupą Galois.*

a) Niech $K \subset L \subset M \subset N$ będzie ciągiem rozszerzeń. Jeżeli ciało L jest domknięte w N oraz $|M : L| < \infty$, to ciało M jest domknięte w N i $|\Phi(L) : \Phi(M)| = |M : L|$.

b) Niech $H \leqslant J \leqslant Gal(N.K)$ będzie ciągiem podgrup oraz $|J : H| < \infty$. Jeżeli podgrupa H jest domknięta w $Gal(N.K)$, to podgrupa J jest domknięta w $Gal(N.K)$ i $|\Psi(H) : \Psi(J)| = |J : H|$.

Dowód.

a) Mamy

$$|\overline{M} : \overline{L}| = |\Psi\Phi(M) : \Psi\Phi(L)| \leq |\Phi(L) : \Phi(M)| \leq |M : L|.$$

Z założenia $\overline{L} = L$ i $M \subset \overline{M}$, zatem $M = \overline{M}$.

b) Mamy

$$|\overline{J} : \overline{H}| = |\Phi\Psi(J) : \Phi\Psi(H)| \leq |\Psi(H) : \Psi(J)| \leq |J : H|.$$

Z założenia $\overline{H} = H$ i $J \subset \overline{J}$, zatem $J = \overline{J}$.

□

Podgrupa trywialna grupy Galois jest domknięta z definicji. Wynika z tego, że zawsze domknięte są wszystkie podgrupy skończone. Podobnie, jeżeli $K \subset N$ jest rozszerzeniem Galois, to domknięte w N są wszystkie skończone rozszerzenia K. Mamy więc **twierdzenie Galois:**

Twierdzenie 18. *Jeżeli $K \subset N$ jest skończonym rozszerzeniem Galois, to przekształcenia Φ i Ψ zadają wzajemnie jednoznaczną odpowiedniość między podgrupami grupy Galois $Gal(N, K)$, a ciałami pośrednimi $K \subset L \subset N$. Ponadto $|L : K| = |Gal(N, K) : \Phi(L)|$. W szczególności $|N : K| = |Gal(N, K)|$.*

2.2.2 Normalne podgrupy grupy Galois

Zacznijmy od oczywistej uwagi dotyczącej działań grup.

Uwaga 4. *Niech grupa G działa na zbiorze X. Wówczas:*

1. *Jeżeli $Y \subset X$ jest podzbiorem niezmienniczym, to podgrupa*

$$H = \{g \in G \colon \forall_{y \in Y} g(y) = y\}$$

jest normalną podgrupą grupy G;

2. *Jeżeli $H \trianglelefteq G$, to zbiór punktów stałych X^H jest podzbiorem niezmienniczym.*

Mamy zatem:

Twierdzenie 19. *Niech $K \subset N$ będzie rozszerzeniem i $Gal(N, K)$ jego grupą Galois. Wówczas:*

a) jeżeli $K \subset L \subset N$ jest $Gal(N, K)$ niezmienniczym ciałem pośrednim, to $\Phi(L) \trianglelefteq Gal(N, K)$;

b) jeżeli $H \trianglelefteq Gal(N, K)$, to $\Psi(H)$ jest $Gal(N, K)$ niezmienniczym ciałem pośrednim.

Wniosek 3. *a) Jeżeli $H \trianglelefteq Gal(N, K)$, to $\overline{H} \trianglelefteq Gal(N, K)$;*

b) Jeżeli $K \subset L \subset N$ jest $Gal(N, K)$ niezmienniczym ciałem pośrednim, to $\overline{L}$ jest także jest $Gal(N, K)$ niezmienniczym ciałem pośrednim.

Twierdzenie 20. *Niech $K \subset N$ będzie rozszerzeniem Galois i niech L będzie $Gal(N, K)$ niezmienniczym ciałem pośrednim. Wówczas rozszerzenie $K \subset L$ jest Galois.*

Dowód. Niech $u \in L \setminus K$. Istnieje $\varphi \in Gal(N, K)$, $\varphi(u) \neq u$. Z niezmienniczości L, $\varphi_{|_L} \in Gal(L, K)$. □

Czy fakt, że rozszerzenie $K \subset L$ jest Galois, odpowiada niezmienniczości L? W tym celu rozpatrzmy lemat.

Lemat 3. *Niech $K \subset N$ będzie rozszerzeniem Galois i niech $f \in K[X]$ będzie wielomianem nierozkładalnym, który ma w N pierwiastek. Wówczas w ciele N wielomian f jest iloczynem czynników liniowych parami różnych.*

Dowód. Niech $u \in N$ i $f(u) = 0$. Niech $u = u_1, \ldots, u_k$, $k \leq n$ wszystkie, parami różne pierwiastki f w N. Niech $g = (X - u_1) \ldots (X - u_k) \in N[X]$. Każdy automorfizm N nad K zachowuje f a więc permutuje pierwiastki $u_i, \ldots, u_k$, czyli zachowuje wielomian g, a zatem jest stały na jego współczynnikach. Rozszerzenie jest Galois więc, $g \in K[X]$. Wielomian f jest minimalny dla u zatem $f \mid g$, co ze względu na $\deg g \leq \deg f$ oznacza $f = g$. □

Twierdzenie 21. *Niech $K \subset N$ będzie rozszerzeniem, $K \subset L \subset N$ ciałem pośrednim, takim że rozszerzenie $K \subset L$ jest Galois i algebraiczne. Wówczas podciało L jest $Gal(N, K)$ niezmiennicze.*

Dowód. Niech $u \in L$ i niech f wielomian minimalny dla u. Z poprzedniego twierdzenia wszystkie pierwiastki f należą do L. Dla $\sigma \in Gal(N, K)$, $\sigma(u)$ jest pierwiastkiem f, a zatem należy do L. □

Twierdzenie 22. *Niech $K \subset N$ będzie rozszerzeniem, a $Gal(N, K)$ jego grupą Galois. Niech $K \subset L \subset N$ będzie $Gal(N, K)$ niezmienniczym ciałem pośrednim. Wówczas grupa ilorazowa $Gal(N, K)/\Phi(L)$ jest izomorficzna z podgrupą tych automorfizmów rozszerzenia $K \subset L$, które są obcięciem automorfizmu rozszerzenia $K \subset N$.*

Dowód. Ponieważ L jest podciałem niezmienniczym, to mamy dobrze zdefiniowany homomorfizm $Gal(N, K) \to Gal(L, K)$ przyporządkowujący automorfizmowi jego obcięcie. Jądrem tego homomorfizmu jest oczywiście $\Phi(L)$. □

Niech teraz $K \subset N$ będzie skończonym rozszerzeniem Galois. Dla rozszerzenia pośredniego $K \subset L \subset N$ niezmienniczość L odpowiada temu, że rozszerzenie $K \subset L$ jest Galois. Ponadto $Gal(N, K)/Gal(N, L) = Gal(L, K)$. To ostatnie stwierdzenie wymaga wyjaśnienia. Można pokazać, że każdy automorfizm L nad K rozszerza się do N lub zauważyć, że zgodnie z twierdzeniem 17 $|Gal(N, K) : Gal(N, L)| = |L : K|$. Ponieważ rozszerzenie $K \subset L$ jest Galois, to $|L : K| = |Gal(L, K)|$. Możemy więc uzupełnić zasadnicze twierdzenie Galois.

Twierdzenie 23. *Niech $K \subset N$ będzie skończonym rozszerzeniem Galois, a $Gal(N, K)$ jego grupą Galois.. Wówczas:*

(1) Przyporządkowanie $H \rightsquigarrow N^H$ zadaje bijekcję między podgrupami grupy $Gal(N, K)$ a ciałami pośrednimi rozszerzenia $K \subset N$. Przy tym włożenie $H \to Gal(N, N^H)$jest izomorfizmem.

(2) Przyporządkowanie $H \rightsquigarrow N^H$ zadaje bijekcję między normalnymi podgrupami grupy $Gal(N, K)$ a ciałami pośrednimi $K \subset L \subset N$, takimi że rozszerzenie $K \subset L$ jest Galois. Ponadto N^H jest $Gal(N, K)$ niezmiennicze i homomorfizm $Gal(N, K) \to Gal(N^H, K)$ zadaje izomorfizm $Gal(N, K)/H \cong Gal(N^H, K)$.

.

2.2.3 Skończone rozszerzenia Galois.

Twierdzenie 24. *Niech $f \in K[X]$ będzie wielomianem nierozkładalnym. Następujące warunki są równoważne:*

1. *f nie ma pierwiastków wielokrotnych w pewnym ciele rozkładu f nad K;*
2. *f nie ma pierwiastków wielokrotnych w każdym ciele rozkładu f nad K;*
3. *$f' \neq 0$.*

Definicja 19. *Nierozkładalny wielomian $f \in K[X]$ nazywa się rozdzielczy (separable) nad K jeżeli spełniony jest jeden z warunków powyżej.*

Definicja 20. *Niech $K \subset M$ będzie rozszerzeniem. Element $u \in M$ nazywa się rozdzielczy nad K, jeżeli jest algebraiczny nad K i jego wielomian minimalny jest rozdzielczy. Rozszerzenie $K \subset M$ nazywa się rozdzielcze, jeżeli każdy element $u \in M$ jest rozdzielczy nad K.*

Zauważmy, że w ciele charakterystyki 0 każde rozszerzenie algebraiczne jest rozdzielcze. W ciele charakterystyki p wielomiany, które nie są rozdzielcze, to wielomiany zmiennej x^p.

Twierdzenie 25. *Niech $K \subset M$ będzie rozszerzeniem skończonym. Następujące warunki są równoważne:*

a) $K \subset M$ jest rozszerzeniem Galois;

b) $K \subset M$ jest rozszerzeniem rozdzielczym i M jest ciałem rozkładu;

c) $K \subset M$ jest ciałem rozkładu wielomianu, którego czynniki nierozkładalne są wielomianami rozdzielczymi.

Dowód. a)⇒ b) - wynika z twierdzenia 12 i lematu 3. b)⇒ c) łatwo c)⇒ a) Wystarczy pokazać, że rząd grupy Galois jest równy stopniu rozszerzenia. Dalej przez indukcję. Niech M ciało rozkładu f. Jeżeli f rozkłada się w K na czynniki liniowe, to $M = K$ i teza jest prawdziwa. Niech g nierozkładalny czynnik wielomianu f stopnia >1. Niech $g(u) = 0$. Niech $L = K(u)$. Wówczas z uwagi 3 wynika, że jest $|G : \Phi(L)|$ różnych obrazów u przy automorfizmach G. Z jednoznaczności z dokładnością do izomorfizmu rozszerzenia o pierwiastek i jednoznaczności ciała rozkładu g wynika, że każdy pierwiastek wielomianu g jest takim obrazem, więc $|L : K| = |G : \Phi(L)| = \deg(g)$. Zauważmy, że M jest ciałem rozkładu f nad L i nierozkładalne czynniki wielomianu f są rozdzielcze nad L, bo są dzielnikami nierozkładalnych czynników f nad K. Dalej przez indukcję.

□

Co zrobić, jeżeli rozszerzenie $K \subset L$ nie jest Galois? Zawsze można wziąć $\overline{K}$, ale to zmienia ciało wyjściowe. Jest drugi sposób - polega na powiększeniu ciała L a zatem i powiększeniu grupy Galois, dzięki czemu K już będzie domknięte - można to zrobić dla rozszerzeń skończonych.

Twierdzenie 26. *Niech $K \subset L$ będzie rozszerzeniem skończonym. Wówczas istnieje rozszerzenie $K \subset L \subset M$, takie że*

a) M jest ciałem rozkładu pewnego wielomianu o współczynnikach w ciele K;

b) nie istnieje ciało M', takie że $K \subset L \subset M' \subset M$ i M' jest ciałem rozkładu nad ciałem K;

c) jeżeli $K \subset L \subset N$ spełnia warunki a) i b), to istnieje izomorfizm $\varphi : M \to N$. taki że $\varphi_{|_L} = id_L$;

d) jeżeli rozszerzenie $K \subset L$ jest rozdzielcze, to rozszerzenie $K \subset M$ jest Galois i nazywamy je **domknięciem Galois L nad K.**

Dowód.

a) Konstrukcja M: niech $v_1, \ldots, v_k$ baza L nad K i niech $f_1, \ldots, f_k \in K[X]$ odpowiadające tym elementom wielomiany minimalne. Niech $f = f_1 f_2 \ldots f_k$ i niech M będzie ciałem rozkładu f.

b) W każdym ciele rozkładu nad K zawierającym L i zawartym w M, każdy z wielomianów f_i rozkłada się na czynniki liniowe, a więc ciało to zawiera M.

c) Ciało N musi być ciałem rozkładu wielomianu f i teza wynika z jednoznaczności ciała rozkładu.

d) Wynika z twierdzenia 25 punkt c) □

Ciało M z poprzedniego twierdzenia nazywa się **rozkładowym domknięciem** ciała L nad K.

Sumą ciał $N \cup P$ nazywamy ciało zawierające P i L i generowane przez ich sumę mnogościową.

Stwierdzenie 11. *Niech $K \subset L$ będzie rozszerzeniem skończonym. Niech M, $K \subset L \subset M$ będzie rozkładowym domknięciem ciała L nad K. Wówczas M jest sumą ciał $L \cup L_1 \cup \cdots \cup L_r$ ciał, z których każde jest izomorficzne z ciałem L.*

Dowód. Używając oznaczeń z dowodu poprzedniego twierdzenia, niech $v_i^1, \ldots, v_i^{m_i}$, $m_i = \deg f_i$ będą wszystkimi pierwiastkami nierozkładalnego wielomianu f_i i przyjmijmy, że $v_i = v_i^1$. Dla $1 \leq i \leq k$, $2 \leq j \leq m_i$ rozpatrzmy ciało $L_i^j = K(v_1, \ldots, v_{i-1}, v_i^j, v_{i+1}, \ldots, v_k)$. Z jednoznaczności ciała powstającego przez dołączenie pierwiastka wielomianu nierozkładalnego wynika, że każde z ciał L_i^j jest izomorficzne z ciałem L oraz M jest sumą ciała L oraz ciał L_i^j. □

2.2.4 Zadania

2.2.1. Udowodnić, że $Gal(\mathbb{R}, \mathbb{Q}) = \{1\}$. Wskazówka: Pokazać, że każdy automorfizm nad $\mathbb{Q}$ zachowuje porządek.

2.2.2. Niech $K \subset L$ będzie rozszerzeniem Galois i ciałem rozkładu wielomianu f stopnia n. Niech $a_1, \ldots . a_n$ będą wszystkimi pierwiastkami wielomianu f. Pokazać, że jeżeli działanie grupy $Gal(L, K)$ na zbiorze pierwiastków ma k orbit, to wielomian f jest iloczynem k wielomianów nierozkładalnych.

2.2.3. Niech $K \subset L$ i $L \subset M$ bedą rozszerzeniami Galois. Czy wynika z tego, że $K \subset M$ jest rozszerzeniem Galois?

2.2.4. Niech $K \subset M$ będzie rozszerzeniem Galois. Niech $K \subset L \subset M$ będzie ciałem pośrednim. Pokazać, że

$$\{\sigma \in Gal(M, K) \colon \sigma(L) = L\} = N_{Gal(M,K)}(Gal(M, L)).$$

2.2.5. Skonstruować rozszerzenie Galois, którego grupa Galois jest równa $\mathbb{Z}_2 \times \mathbb{Z}_4$.

2.2.6. Niech $K \subset L$ będzie rozszerzeniem i niech K,L będą ciałami skończonymi. Czy rozszerzenie to jest Galois?

2.2.7. Niech $K \subset L$ będzie rozszerzeniem i niech K,L będą ciałami skończonymi. Pokazać, że $Gal(L, K)$ jest grupą cykliczną.

2.3 Rozszerzenia pierwiastnikowe

Jesteśmy u źródeł teorii Galois, czyli odpowiedzi na pytanie kiedy dla danego wielomianu istnieją wzory na jego pierwiastki, które oprócz zwykłych działań arytmetycznych dopuszczają pierwiastkowanie.

Definicja 21. *Rozszerzenie $K \subset L$ nazywa się pierwiastnikowe wtedy i tylko wtedy, gdy $L = K(a_1, \ldots, a_n)$ oraz $a_i^{k_i} \in K(a_1, \ldots, a_{i-1})$ dla pewnego $k_i \in \mathbb{N}$ i każdego $1 \leq i \leq n$.*

Zauważmy, że możemy założyć, że k_i są liczbami pierwszymi ew. zwiększając liczbę generatorów. Jeżeli $f \in K[X]$ jest wielomianem, to istnieją wzory na jego pierwiastki, które oprócz zwykłych działań arytmetycznych dopuszczają pierwiastkowanie wtedy i tylko wtedy, gdy ciało rozkładu tego wielomianu jest zawarte w rozszerzeniu pierwiastnikowym. Będziemy więc badać grupy Galois rozszerzeń zawartych w rozszerzeniu pierwiastnikowym.

Zauważmy następujące własności rozszerzeń pierwiastnikowych:

Lemat 4. *Suma pierwiastnikowych rozszerzeń ciała K jest pierwiastnikowym rozszerzeniem ciała K*

Dowód. Jeżeli $L = K(a_1, \ldots, a_n)$ a $M = K(b_1, \ldots, b_m)$ pierwiastnikowe, to $L \cup M = K(a_1, \ldots, a_n, b_1, \ldots, b_m)$ i oczywiście jest pierwiastnikowe. □

Lemat 5. *Niech $K \subset L$ będzie rozszerzeniem pierwiastnikowym, zaś $K \subset L \subset M$ jego rozkładowym domknięciem. Wówczas $K \subset M$ jest rozszerzeniem pierwiastnikowym.*

Dowód. M jest sumą rozszerzeń izomorficznych z L. □

Przypomnijmy, że skończona podgrupa grupy multyplikatywnej ciała jest cykliczna. Wynika z tego, że cykliczna jest podgrupa pierwiastków wielomianu $X^n - 1$.

Lemat 6. *Niech p będzie liczbą pierwszą, a L ciałem rozkładu $X^p - 1 \in K[X]$. Wówczas grupa $Gal(L, K)$ jest przemienna (a nawet cykliczna)*

Dowód. Jeżeli $\chi(K) = p$, to $X^p - 1 = (X - 1)^p$ i $K = L$. W przeciwnym przypadku $X^p - 1$ ma p pierwiastków różnych i $L = K(\epsilon)$. Ponieważ p jest liczbą pierwszą, to każdy automorfizm jest postaci $\epsilon \to \epsilon^i$. □

Lemat 7. *Niech wielomian $X^n - 1$ rozkłada się w K na czynniki liniowe. Dla $a \in K$ niech L będzie ciałem rozkładu wielomianu $X^n - a$. Wówczas grupa $Gal(L, K)$ jest przemienna (a nawet cykliczna).*

Dowód. Niech $u \in L$ będzie pewnym pierwiastek tego wielomianu - każdy inny jest postaci $u\epsilon^i$, gdzie ϵ jest pierwiastkiem pierwotnym stopnia n z 1. Zatem $L = K(u)$ i dowolny automorfizm jest postaci $u \to u\epsilon^i$. Przekształcenie $Gal(L.K) \to \mathbb{Z}_n$, które automorfizmowi $u \to u\epsilon^i$ przyporządkowuje i jest monomorfizmem w grupę cykliczną $\mathbb{Z}_n$. □

Powyższe lematy są prawdziwe dla ciał dowolnej charakterystyki. Główne twierdzenie udowodnimy na początek dla ciał charakterystyki 0.

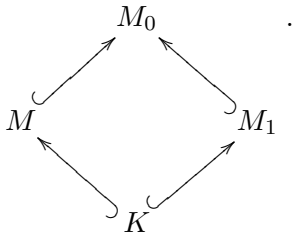
Twierdzenie 27. *Niech $\chi(K) = 0$. Niech $K \subset L \subset M$ i niech M będzie rozszerzeniem pierwiastnikowym. Wówczas $Gal(L, K)$ jest grupą rozwiązalną.*

Dowód. Zauważmy, że możemy poczynić pewne założenia, które pozwolą nam na posłużenie się twierdzeniem Galois.

- możemy założyć, że $K \subset L$ jest Galois, biorąc domknięcie K, czyli $L^{Gal(L,K)}$ - grupa Galois nie ulega zmianie.
- możemy założyć, że $K \subset M$ jest Galois, biorąc rozkładowe domknięcie M, z lematu wiemy, że jest pierwiastnikowe.
- wobec założenia $\chi(K) = 0$ wymóg rozdzielczości jest spełniony i twierdzenie Galois jest prawdziwe.

Przy powyższych założeniach $Gal(L, K)$ jest grupą ilorazową $Gal(M, K)$, więc wystarczy pokazać, że $Gal(M, K)$ jest rozwiązalna. Załóżmy, że $M = K(u_1, \ldots, u_n)$ i u_i są generatorami spełniającymi definicję rozszerzenia pierwiastnikowego. Dowód przez indukcję ze względu na n. Jeżeli $n = 0$ tzn $K = M$, to teza jest jasna.
Niech p będzie liczbą pierwszą dla której $u_1^p \in K$. Niech M_0, $K \subset M \subset M_0$ będzie ciałem rozkładu $X^p - 1$ nad M. Niech M_1, $K \subset M_1$ będzie ciałem rozkładu wielomianu $X^p - 1$ nad K.

Mamy następujący diagram rozszerzeń i wszystkie one są skończone, normalne i rozdzielcze, bo $\chi(K) = 0$.



Wystarczy pokazać, że grupa $Gal(M_0, K)$ jest rozwiązalna, bo $Gal(M, K)$ jest jej grupą ilorazową. W tym celu rozważamy rozszerzenia $K \subset M_1 \subset M_0$. Grupa $Gal(M_0, K)$ jest rozszerzeniem grupy $Gal(M_1, K)$ przez grupę $Gal(M_0, M_1)$. Grupa $Gal(M_1, K)$ jest przemienna, a więc rozwiązalna.
Wykażemy, że $Gal(M_0, M_1)$ jest rozwiązalna. Mamy $M_0 = M_1(u_1, \ldots, u_n)$ i ciąg rozszerzeń $M_1 \subset M_1(u_1) \subset \cdots \subset M_1(u_1, \ldots, u_n)$. Rozszerzenie $M_1 \subset M_1(u_1)$ jest ciałem rozkładu wielomianu $X^p - u_1^p$, gdyż M_1 zawiera wszystkie pierwiastki stopnia p z 1. Ponieważ rozszerzenie grupy rozwiązalnej przez rozwiązalną jest grupą rozwiązalną, to wystarczy wykazać rozwiązalność grupy $Gal(M_0, M(u_1))$, ale ona wynika z założenia indukcyjnego, bo jest to pierwiastnikowe rozszerzenie o $n - 1$ generatorach. □

Naturalnym pytaniem jest odwrotne. Czy jeśli grupa Galois wielomianu jest rozwiązalna, to takie wzory istnieją? Okazuje się, że tak, ale dowód tego faktu poprzedzamy przykładami.

2.3.1 Grupa Galois wielomianu

Definicja 22. *Niech $f \in K[X]$. Grupą Galois $Gal(f)$ wielomianu f nazywamy grupę Galois ciała rozkładu f nad K.*

Zauważmy, że jeżeli $\deg(f) = n$, to $Gal(f) \leqslant \Sigma_n$.

Twierdzenie 28. *Niech $\chi(K) = 0$ i niech $f \in K[X]$ będzie wielomianem nierozkładalnym. Niech $K \subset L$ będzie rozszerzeniem pierwiastnikowym zawierającym pewien pierwiastek wielomianu f. Wówczas $Gal(f)$ jest rozwiązalna.*

Dowód. Niech $K \subset L \subset N$, gdzie N rozkładowe domknięcie L. Wówczas $K \subset N$ jest pierwiastnikowe. Jeżeli M jest ciałem rozkładu f, to z nierozkładalności F i tego że N jest ciałem rozkładu wynika, ze wszystkie pierwiastki f leżą w ciele N i $K \subset M \subset N$. Zatem z poprzedniego twierdzenia wynika, że $Gal(M, K) = Gal(f)$ jest grupą rozwiązalną. □

Jeżeli chcemy wskazać wielomian, którego pierwiastki nie dadzą się wyrazić przez operacje arytmetyczne i pierwiastkowanie, to wystarczy znaleźć taki, którego grupą Galois jest Σ_n, $n > 4$. Skorzystamy z tego, że dla liczby pierwszej p, grupa Σ_p jest generowana przez dowolną transpozycję i dowolny cykl długości p.

Stwierdzenie 12. *Niech $f \in \mathbb{Q}[X]$ będzie nierozkładalnym wielomianem stopnia p, który ma dokładnie dwa pierwiastki nierzeczywiste. Wówczas $Gal(f) = \Sigma_p$.*

Dowód. Wiemy, że $Gal(f) \leqslant \Sigma_p$. Wystarczy pokazać, że transpozycja i cykl długości p należą do $Gal(f)$. Sprzężenie w $\mathbb{C}$ transponuje jedyne dwa pierwiastki nierzeczywiste wielomianu f. Na pewno $p \mid |Gal(f)|$, bo $\deg(f) = p$, więc $Gal(f)$ zawiera element rzędu p. Jedynym elementem rzędu p w Σ_p jest cykl długości p. □

Przykład 2. *Wielomian $X^5 - 6X + 3$ spełnia założenia poprzedniego stwierdzenia - jego grupa Galois jest równa Σ_5 i nie ma wzorów na pierwiastki tego wielomianu używających działań arytmetycznych i pierwiastkowania.*

Grupa Galois wielomianu stopnia 4.

Niech $f = X^4 + bX^3 + cX^2 + dX + e \in K[X]$ będzie wielomianem stopnia 4 o parami różnych pierwiastkach a_1, a_2, a_3, a_4 w ciele rozkładu M

wielomianu f. Niech

$$\begin{aligned}\alpha &= a_1a_2 + a_3a_4\\ \beta &= a_1a_3 + a_2a_4.\\ \gamma &= a_1a_4 + a_2a_3\end{aligned}$$

Łatwo sprawdzić, że elementy α, β, γ są parami różne, zbiór $\{\alpha, \beta, \gamma\}$ jest Σ_4 niezmienniczy i jest jedną orbitą. Wynika z tego, że grupa izotropii każdego z elementów jest 2 – podgrupą Sylowa i każda z nich zawiera podgrupę czwórkową Kleina V i co więcej V jest podgrupą Σ_4, która działa trywialnie. Zatem

$$M^{Gal(f)\cap V} = K(\alpha, \beta, \gamma)$$

a ponieważ $Gal(f) \cap V \trianglelefteq Gal(f)$, to rozszerzenie $K \subset K(\alpha, \beta, \gamma)$ jest Galois o grupie Galois $Gal(f)/Gal(f) \cap V/$ Oznaczmy przez $L -: K(\alpha, \beta, \gamma)$. Wielomian

$$g = (X - \alpha)(X - \beta)(X - \gamma)$$

jest $Gal(f)$ niezmienniczy, więc $g \in K[X]$ i widać, że L jest jego ciałem rozkładu. Wielomian g nazywa się rozwiązującym wielomianem stopnia 3 (ang: resolvent cubic) i można policzyć, że jeżeli $f = X^4+bX^3+cX^2+dX+e$, to

$$g = X^3 - cX^2 + (bd - 4e)X - b^2e + 4ce - d^2.$$

Niech teraz f będzie nierozkładalnym wielomianem rozdzielczym. Wówczas $Gal(f)$ działa tranzytywnie na zbiorze pierwiastków f więc $4 \mid |Gal(f)|$. Możliwe są następujące podgrupy:

$Gal(f)$	$\lvert Gal(f) \cap V\rvert$	$\lvert Gal(f)/Gal(f) \cap V\rvert$
Σ_4	4	6
A_4	4	3
V	4	1
D_8	4	2
$\mathbb{Z}_4$	2	2

Ostatnia kolumna, to grupa Galois rozszerzenia $K \subset L$, czyli ciała rozkładu wielomianu g. Widać, że wyznacza ona jednoznacznie grupę $Gal(f)$ z wyjątkiem przypadku, gdy $|L : K| = 2$. Wówczas $Gal(f) \cap V = Gal(M, L)$ jest równe: 4 gdy f jest nierozkładalny w $L[X]$ lub 2 gdy jest rozkładalny.

2.3.2 Twierdzenie Galois

Dowód twierdzenia odwrotnego do 27 zaczynamy od twierdzenia o niezależności automorfizmów, które jest ciekawe same w sobie.

Twierdzenie 29. (Dedekinda) *Każdy zbiór parami różnych automorfizmów ciała K jest liniowo niezależny (w przestrzeni liniowej wszystkich przekształceń $K \to K$).*

Dowód. Przypuśćmy przeciwnie i załóżmy, że $a_1\sigma_1 + a_2\sigma_2 + \cdots + a_n\sigma_n = 0$. $a_i \neq 0$ jest najkrótszą kombinacją liniową równą 0. Ponieważ $\sigma_1 \neq \sigma_2$, to dla pewnego $x \in K$, $\sigma_1(x) \neq \sigma_2(x)$. Mamy

$$\forall y \in K : a_1\sigma_1(y) + a_2\sigma_2(y) + \cdots + a_n\sigma_n(y) = 0$$

zatem

$$\forall_{y\in K} : a_1\sigma_1(x)\sigma_1(y) + a_2\sigma_1(x)\sigma_2(y) + \cdots + a_n\sigma_1(x)\sigma_n(y) = 0$$

oraz

$$\forall_{y\in K} : a_1\sigma_1(xy) + a_2\sigma_2(xy) + \cdots + a_n\sigma_n(xy) =$$
$$= a_1\sigma_1(x)\sigma_1(y) + a_2\sigma_2(x)\sigma_2(y) + \cdots + a_n\sigma_n(x)\sigma_n(y) = 0.$$

Po odjęciu stronami otrzymujemy krótszą nietrywialną kombinację liniową równą 0:

$$\forall_{y\in K} : a_2(\sigma_1(x) - \sigma_2(x)\sigma_2(y) + \cdots + a_n(\sigma_1(x) - \sigma_n(x))\sigma_n(y) = 0,$$

co prowadzi do sprzeczności. □

Twierdzenie 30. *Niech $K \subset K(a_1, a_2, \ldots, a_n)$ będzie skończonym rozszerzeniem $a_2, \ldots a_n$ rozdzielcze. Wtedy $K(a_1, a_2, \ldots, a_n) = K(d)$ dla pewnego d.*

Dowód. Dla ciala nieskończonego: Wystarczy dla $K \subset K(a, b)$, b rozdzielczy. Niech f min dla a, g min dla b. M ciało rozkładu $fg.a_1, ..a_s$ pierwiastki f, $b_1 = b, ..b_t$ pierw g. Z rozdzielczości: $\frac{a_i - a}{b - b_j} \in K$ $j \neq 1$. Niech c różne od nich. Niech $d = a + cb$. Rozważmy g i $f(d - cX)$. $g, f \in K(d)[X]$ i b jest ich jedynym wspólnym pierwiastkiem. Zatem $NWD(g, f(d - cX)) = X - b$. Zatem $b \in K(d)$ i $a \in K(d)$. □

Definicja 23. *Niech $K \subset L$ będzie skończonym rozszerzeniem Galois i niech $Gal(L, K) = \{\sigma_0 = id, \sigma_1, \ldots, \sigma_{n-1}\}$. Wówczas dla elementu $a \in L$ jego normą nazywamy iloczyn*

$$N(a) = \sigma_0(a)\sigma_1(a) \ldots \sigma_n(a).$$

Zauważmy, że dla każdego $a \in L$, $N(a) \in K$, $N(ab) = N(a)N(b)$ oraz dla $a \in K$, $N(a) = a^n$.

Twierdzenie Hilberta charakteryzuje elementy o normie 1.

Twierdzenie 31. (90 Hilberta) *Niech $K \subset L$ będzie rozszerzeniem normalnym stopnia n o cyklicznej grupie Galois $Gal(L, K) = \langle \sigma \rangle$. Wówczas dla $a \in L$, $N(a) = 1$ wtedy i tylko wtedy, gdy istnieje element $b \in L$, dla którego $a = \frac{b}{\sigma(b)}$.*

Dowód. Jeżeli $a = \frac{b}{\sigma(b)}$, to

$$N(a) = a\sigma(a)\sigma^2(a)\dots\sigma^{n-1}(a) = \frac{b}{\sigma(b)}\frac{\sigma(b)}{\sigma^2(b)}\dots\frac{\sigma^{n-1}(b)}{b} = 1.$$

Przypuśćmy, że $N(a) = 1$ i rozpatrzmy ciąg elementów:

$$\begin{aligned} c_0 &= a \\ c_1 &= a\sigma(a) \\ c_2 &= a\sigma(a)\sigma^2(a) \\ &\dots\dots \\ c_{n-1} &= a\sigma(a)\sigma^2(a)\dots\sigma^{n-1}(a) = 1. \end{aligned}$$

Zauważmy, że $c_{i+1} = a\sigma(c_i)$. Automorfizmy $id, \sigma, \dots, \sigma^{n-1}$ są liniowo niezależne, więc

$$c_0 id + c_1\sigma + \dots + n - 2\sigma^{n-2} + \sigma^{n-1} \neq 0.$$

Istnieje więc $d \in L$ dla którego

$$c_0 d + c_1\sigma(d) + \dots + n - 2\sigma^{n-2}(d) + \sigma^{n-1}(d) = b \neq 0.$$

Mamy

$$c_0\sigma(d) + \dots + n - 2\sigma^{n-1}(d) + d = \sigma(b).$$

Mnożac tę równość przez a i korzystając z tożsamości $c_{i+1} = a\sigma(c_i)$ i odejmując równosci stronami otrzymujemy tezę. □

Następujące twierdzenie charakteryzuje rozszerzenia o cyklicznej grupie Galois.

Twierdzenie 32. *Niech $K \subset L$ będzie rozszerzeniem normalnym stopnia n. Załóżmy, że $(\chi(K), n) = 1$ i niech K zawiera wszystkie pierwiastki stopnia n z 1. Jeżeli grupa Galois $Gal(L, K)$ jest cykliczna, to L jest ciałem rozkładu wielomianu $X^n - a$ dla pewnego $a \in K$*

Dowód. Jeżeli $(\chi(K), n) = 1$, to $(X^n - 1)' \neq 0$ i wielomian $X^n - 1$ ma w K n pierwiastków różnych, które tworzą multyplikatywną grupę cykliczną. Niech ϵ będzie pierwiastkiem pierwotnym stopnia n. $N(\epsilon) = \epsilon^n = 1$ więc z twierdzenia Hilberta istnieje $b \in L$, takie że $\epsilon = \frac{\sigma(b)}{b}$, gdzie $Gal(L, K) = \langle\, \sigma \,\rangle$. Zatem $\sigma(b) = b\epsilon$ i $\sigma(b^n) = \sigma(b)^n = b^n$ z czego wynika, ż $a = b^n \in K$. Rozpatrzmy wielomian $X^n - a \in K[X]$. Ponieważ, K zawiera wszystkie pierwiastki stopnia n z 1, to $K \subset K(b)$ jest ciałem rozkładu $X^n - a$, rozszerzenie $K \subset K(b)$ jest normalne, stąd automorfizmy $1, \sigma, \dots, \sigma^{n-1}$ zachowują $K(b)$. Zatem $|K(b) : K| \geq n$. Ale $K \subset K(b) \subset L$, $L : K| = n$, stąd $K(b) = L$. □

Możemy teraz przystąpić do dowodu twierdzenia:

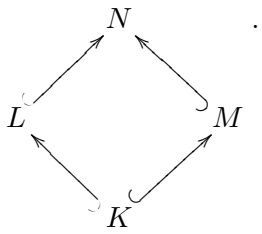
Twierdzenie 33. *Niech $\chi(K) = 0$. Niech $K \subset L$ będzie skończonym rozszerzeniem normalnym o rozwiązalnej gruppie Galois. Wówczas istnieje rozszerzenie pierwiastnikowe $K \subset N$, dla którego $K \subset L \subset N$.*

Dowód. Dowod przez indukcję ze względu na stopień n rozszerzenia. Oczywiście dla $n = 1$ teza jest prawdziwa.

Niech $n > 1$ i niech $p \mid n$ będzie taką liczbą pierwszą, dla której istnieje podgrupa $H \trianglelefteq Gal(L, K)$ indeksu p. Niech $f \in K[X]$ będzie takim wielomianem, że L jest jego ciałem rozkładu. Rozważmy następujące rozszerzenia:

- $L \subset N$, gdzie N ciało rozkładu $X^p - 1$ nad L;
- $K \subset M$, gdzie M ciało rozkładu $X^p - 1$ nad K

Ponieważ $\chi(K) = 0$, to rozszerzenia są rozdzielcze i ciała rozkładu są rozszerzeniami normalnymi. Mamy diagram zawierań:



Wiemy, że

- grupa $Gal(N, L)$ jest przemienna;
- rozszerzenie $K \subset N$ jest normalne, bo jest ciałem rozkładu wielomianu $f(X^p - 1)$
- grupa $Gal(N, K)$ jako rozszerzenie rozwiązalnej $Gal(L, K)$ przez przemienną $Gal(N, L)$.
- rozszerzenie $M \subset N$ jest normalne;
- rozszerzenie $K \subset M$ jest pierwiastnikowe, bo $M = K(\epsilon)$, ϵ pierwotny stopnia p..

Pokażemy, że istnieje rozszerzenie pierwiastnikowe $M \subset N'$, takie że $M \subset N \subset N'$. To wystarczy, bo wówczas $K \subset N'$ pierwiastnikowe i wobec $L \subset N$, mamy $K \subset L \subset N'$. Ponieważ $K \subset L$ jest normalne, to L jest niezmienniczym ciałem pośrednim i mamy dobrze zdefiniowany homomorfizm $\Gamma : Gal(N, M) \to Gal(L, K)$, który automorfizmowi σ przyporządkowuje $\sigma_{|_L}$. Homomorfizm ten jest monomorfizmem, bo jeżeli $\sigma_{|_L} = id$, to oznacza to, że σ jest identycznością na wszystkich pierwiastkach f, ale one są generatorami N nad M. Zatem $\sigma = id$. Rozpatrujemy dwa przypadki:

- $\Gamma(Gal(N,M)) \leqslant Gal(L,K)$ jest podgrupą właściwą.

  Wówczas z założenia indukcyjnego istnieje rozszerzenie pierwiastnikowe $M \subset N'$, takie że $M \subset N \subset N'$

- $\Gamma(Gal(N,M)) = Gal(L,K)$. Utożsamiając te grupy, niech $H \trianglelefteq Gal(N,M)$ będzie wybraną podgrupa indeksu p i niech P, $M \subset P \subset N$ będzie odpowiadającym H ciałem pośrednim. Grupa $Gal(P,M) = Gal(N.M)/H$ jest rzędu P więc jest cykliczna i z poprzedniego twierdzenia wiemy, że $M \subset P$ jest rozszerzeniem pierwiastnikowym. Grupa $Gal(N,P) = H$ ma rząd mniejszy od n i jest rozwiązalna, więc z założenia indukcyjnego istnieje rozszerzenie pierwiastnikowe $P \subset N'$, takie że $P \subset N \subset N'$. Zatem rozszerzenie $M \subset N'$ jest pierwiastnikowe.

□

Stwierdzenie 13. *Niech $K \subset L$ będzie skończonym rozszerzeniem Galois stopnia n. Niech $Gal(L,K) = \{1 = \sigma_1, \sigma_2, \ldots, \sigma_n\}$. Wówczas istnieje element $a \in L$ dla którego $a, \sigma_2(a), \ldots, \sigma_n(a)$ jest bazą przestrzeni liniowej L nad K.*

Dowód. Przypadek, gdy ciało K jest nieskończone.

Krok 1: Niech $F \in K[X_1, \ldots, X_n]$ będzie takim wielomianem, że dla każdego $a \in L$ $F(a, \sigma_2(a), \ldots, \sigma_n(a)) = 0$, to F jest tożsamościowo równe 0.

Przez odwracalną (twierdzenie Dedekinda) zmianę zmiennych

$$X_i = \sum_{j=1}^{n} Y_j \sigma_i(a_j)$$

otrzymujemy wielomian, który wyznacza zerową funkcję wielomianową. Dla nieskończonego ciała K oznacza to, że wielomian g jest tożsamościowo równy 0.

Krok 2: Definiujemy macierz A, w której na miejscu (i,j) stoi złożenie $\sigma_i\sigma_j$. Teraz w miejsce (i,j) wstawiamy zmienną X_k jeżeli $\sigma_i\sigma_j = \sigma_k$ i rozpatrujemy wielomian n – zmiennych $F(X_1, \ldots, X_n) = \det A$. Wielomian ten nie jest zerowy, więc istnieje $a \in L$, że $F(a, \sigma_2(a), \ldots, \sigma_n(a)) = \det(\sigma_i\sigma_j(a)) \neq 0$. Pokażemy, że elementy $a, \sigma_2(a), \ldots, \sigma_n(a)$ są liniowo niezależne nad K. Przypuśćmy przeciwnie:

$$\sum_{i=1}^{n} x_i \sigma_i(a) = 0 \text{ dla pewnych } x_i \in K..$$

Rozpatrzmy obraz tej kombinacji liniowej przy wszystkich automorfizmach grupy Galois. Dostajemy jednorodny układ równań o współczynnikach w L. Macierz tego układu, to $\sigma_i\sigma_j(a)$ – z konstrukcji jest ona nieosobliwa, więc jedynym rozwiązaniem jest zerowe.

Przypadek, gdy ciało K jest skończone.

Wówczas grupa Galois jest cykliczna i niech automorfizm σ rzędu n będzie jej generatorem. Rozpatrujemy σ jako automorfizm przestrzeni liniowej i niech $F[X]$ będzie jego wielomianem minimalnym. $F(\sigma) = 0$. Ponieważ $\sigma^n = id$, to $F \mid X^n - 1$. Z twierdzenia Dedekinda wynika, że automorfizmy $id, \sigma, \ldots, \sigma^{n-1}$ są liniowo niezależne, więc $F = X^n - 1$. Teraz mamy do czynienia z zadaniem z GAL i musimy pokazać, że przestrzeń liniowa L nad K jest cykliczna względem operatora σ. Pozostawiam to zadanie z GAL czytelnikom. Wrócimy do niego później w innym kontekście.

□

2.4 Zadania

2.4.1. Znaleźć $Gal(f)$, jeżeli $f = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$ (resolvent cubic:$(X - 4)(X^2 - 8)$)

2.4.2. Znaleźć $Gal(f)$, jeżeli $f = X^4 - 10X^2 + 4 \in \mathbb{Q}[X]$ (resolvent cubic:$(X + 10)(X^2 - 16)$)

2.4.3. Znaleźć $Gal(f)$, jeżeli $f = X^4 - 2 \in \mathbb{Q}[X]$ (resolvent cubic:$(X^3 + 8X)$)

2.4.4. Znaleźć $Gal(f)$, jeżeli $f = X^4 - 4X + 2 \in \mathbb{Q}[X]$

2.4.5. Czy wielomian $X^6 - 2X^3 - 2$ jest rozwiązywalny przez pierwiastniki?

2.4.6. Niech $f \in \mathbb{Q}[X]$ będzie rozkładalnym wielomianem stopnia 3. Pokazać, że jego ciałem rozkładu jest $\mathbb{Q}(\Delta(f))$, gdzie $\Delta(f) = \prod_{1 \leq i < j \leq 3}(a_i - a_j)$, gdzie a_1, a_2, a_3 sa pierwiastkami f w jego ciele rozkładu.

2.5 Test

2.5.1. Czy grupa Galois ciała rozkładu $X^3 - 7$ jest izomorficzna z Σ_3?

2.5.2. Czy ciała rozkładu wielomianów $X^2 - 7 \in \mathbb{Q}[X]$ i $X^2 - 11 \in \mathbb{Q}[X]$ są izomorficzne?

2.5.3. Czy grupa Galois wielomianu $X^5 - 2 \in \mathbb{Q}[X]$ jest przemienna?

2.5.4. Czy grupa Galois wielomianu $X^5 - 2 \in \mathbb{Q}[X]$ jest rozwiązalna?

2.5.5. Czy grupa Galois wielomianu $X^5 - 2 \in \mathbb{Q}(\zeta)[X]$, gdzie ζ jest pierwiastkiem stopnia 5, jest przemienna?

2.5.6. Czy ciało rozkładu wielomianu $X^3 - 5$ nad $\mathbb{Q}(\sqrt{7})$ zawiera podciało L, takie że $\mathbb{Q}(\sqrt{7}) \subset L$ jest Galois o cyklicznej grupie Galois rzędu 3?

2.5.7. Czy ciało rozkładu wielomianu $X^3 - 5$ nad $\mathbb{Q}(\sqrt{7})$ zawiera podciało L, takie że $\mathbb{Q}(\sqrt{7}) \subset L$ jest Galois o grupie Galois rzędu 2?

2.5.8. Czy istnieje rozszerzenie Galois $K \subset M$ stopnia n i $d|n$, dla którego nie istnieje ciało pośrednie $K \subset L \subset M$, $|L : K| = d$?

2.5.9. Niech $K \subset L$ będzie rozszerzeniem Galois, niech $K \subset M$ będzie rozszerzeniem rozdzielczym i niech $L \cap M = K$. Niech $\tilde{M}$ będzie domknięciem Galois rozszerzenia $K \subset M$. Czy wynika z tego, że $\tilde{M} \cap L = K$?

2.5.10. Niech $K \subset M$ będzie rozszerzeniem rozdzielczym i niech stopień wielomianu minimalnego dowolnego elementu jest $\leq n$. Czy wynika z tego, że $|M : K| \leq n$?

2.5.11. Niech $K \subset M$ będzie rozszerzeniem algebraicznym i niech stopień wielomianu minimalnego dowolnego elementu jest $\leq n$. Czy wynika z tego, że $|M : K| \leq n$?

Rozdział 3

Elementy teorii kategorii

3.1 Kategorie, funktory, transformacje naturalne

Teorię kategorii zapoczątkował artykuł: Samuel Eilenberg, Saunders Mac Lane *General Theory of Mathematical Equivalences*, Trans. of Mathematics 1945

Definicja 24. *Kategoria $\mathcal{C}$ to:*

- *klasa obiektów* $\mathrm{ob}\,\mathcal{C}$
- *dla każdych dwóch obiektów $X, Y \in \mathrm{ob}\,\mathcal{C}$ dany jest* **zbiór** *morfizmów* $\mathrm{Mor}_{\mathcal{C}}(X, Y)$
- *dla każdego obiektu $X \in \mathrm{ob}\,\mathcal{C}$ wyróżniony jest morfizm $id_X \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$*
- *dla każdych trzech obiektów $X, Y, Z \in \mathrm{ob}\,\mathcal{C}$ dana jest funkcja (składanie morfizmów)*

$$\begin{array}{rccc} \circ\colon & \mathrm{Mor}_{\mathcal{C}}(Y,Z) \times \mathrm{Mor}_{\mathcal{C}}(X,Y) & \longrightarrow & \mathrm{Mor}_{\mathcal{C}}(X,Z) \\ & (g, f) & \longrightarrow & g \circ f \end{array}$$

taka, że

$$(h \circ g) \circ f = h \circ (g \circ f)$$

$$id_Y \circ f = f \circ id_X = f$$

Kategorie oznaczamy na ogół literami $\mathcal{A}, \mathcal{B}, \mathcal{C}$ a zbiory morfizmów między obiektami $X, Y \in \mathrm{ob}\,(\mathcal{C})$ oznaczamy $\mathcal{C}(X, Y)$ lub $\mathrm{Mor}_{\mathcal{C}}(X, Y)$.

Dla każdej kategorii $\mathcal{C}$ możemy skonstruować kategorię przeciwną "odwracając" strzałki.

Definicja 25. *Dla kategorii $\mathcal{C}$ przez $\mathcal{C}^{op}$ oznaczamy kategorię przeciwną do kategorii $\mathcal{C}$, czyli taką, że $\mathrm{ob}\,\mathcal{C}^{op} = \mathrm{ob}\,(\mathcal{C})$ a dla dowolnych $A, B \in \mathrm{ob}\,\mathcal{C}^{op}$ definiujemy $\mathcal{C}^{op}(A, B) := \mathcal{C}(B, A)$ z oczywistą operacją składania.*

Definicja 26. *Morfizm* $f \in \mathrm{Mor}_{\mathcal{C}}(X,Y)$ *nazywamy izomorfizmem jeżeli istnieje morfizm* $g \in \mathrm{Mor}_{\mathcal{C}}(Y,X)$*, dla którego* $g \circ f = id_X$ *i* $f \circ g = id_Y$*.*

Definicja 27. *Kategoria* $\mathcal{C}'$ *jest podkategorią kategorii* $\mathcal{C}$*, jeżeli* $\mathrm{ob}\,\mathcal{C}' \subset \mathrm{ob}\,\mathcal{C}$ *oraz* $\mathrm{Mor}_{\mathcal{C}'}(X,Y) \subset \mathrm{Mor}_{\mathcal{C}}(X,Y)$ *z tą samą co w* $\mathcal{C}$ *operacją składania i tymi samymi wyróżninymi morfizmami identycznociowymi. Podkategoria* $\mathcal{C}' \subset \mathcal{C}$ *nazywa się pełna, jeżeli dla każdych* $X, Y \in \mathcal{C}'$*,* $\mathrm{Mor}_{\mathcal{C}'}(X,Y) = \mathrm{Mor}_{\mathcal{C}}(X,Y)$.

Definicja 28. *Kategorię* $\mathcal{C}$ *nazywamy* małą *jeśli klasa obiektów* $\mathrm{ob}\,(\mathcal{C})$ *jest zbiorem.*

Przykłady:

$\mathcal{S}et$ – kategoria zbiorów i ich dowolnych przekształceń,

$\mathcal{S}et_*$ – kategoria zbiorów z wyróżnionym punktem i przekształceń zachowujących te punkty,

$\mathcal{G}r$ – kategoria grup i homomorfizmów; $\mathcal{A}b \subset \mathcal{G}r$ pełna podkategoria grup abelowych,

$\mathcal{R}_1$ – kategoria pierścieni przemiennych z 1 i homomorfizmów,

$\mathcal{T}$ – kategoria przestrzeni topologicznych i przekształceń ciągłych,

$\mathcal{B}G$ – jeżeli G jest grupą, to przez $\mathcal{B}G$ oznaczać będziemy kategorię o jednym obiekcie, w której morfizmy odpowiadają elementom grupy a ich składanie jest wyznaczone przez działanie grupowe.

$\mathcal{E}G$ – jeżeli G jest grupą, to przez $\mathcal{E}G$ oznaczać będziemy kategorię, w której obiekty odpowiadają elementom grupy G, i w której jest dokładnie jeden $g_1 \to g_2$ wyznaczny przez element $g_2 g_1^{-1}$. Mamy oczywisty funktor $\mathcal{E}G \to \mathcal{B}G$.

$\mathcal{C}(X)$ – Jeżeli X jest zbiorem częściowo uporządkowanym, to możemy traktować go jako kategorię, której obiektami są elementy tego zbioru, zaś między obiektami x i y istnieje morfizm $x \to y$ jeżeli $x \leq y$. Funktory między takimi kategoriami, to funkcje zachowujące porządek. Kategorią taką oznaczamy symbolem $\mathcal{C}(X)$.

Definicja 29. *Funktor (kowariantny)* $F\colon \mathcal{C} \to \mathcal{D}$ *między kategoriami* $\mathcal{C}$ *i* $\mathcal{D}$ *jest zadany przez przyporządkowanie obiektom kategorii* $\mathcal{C}$ *obiektów kategorii* $\mathcal{D}$*:*

$$F\colon \mathrm{ob}\,(\mathcal{C}) \to \mathrm{ob}\,(\mathcal{D})$$

oraz odwzorowania

$$F_{X,Y}\colon \mathrm{Mor}_{\mathcal{C}}(X,Y) \to \mathrm{Mor}_{\mathcal{D}}(F(X),F(Y)),$$

określone dla dowolnych obiektów $X, Y \in \mathrm{ob}\,(\mathcal{C})$ *i takie, że*

$$F_{X,X}(\iota_X) = \iota_{F(X)} \qquad F_{X,Z}(gh) = F_{Y,Z}(g)F_{X,Y}(h).$$

Funktor kowariantny $F\colon \mathcal{C}^{op} \to \mathcal{D}$ nazywa się funktorem kontrawariantnym na $\mathcal{C}$.

Definicja 30. *Jeśli dane są dwa funktory $F_i\colon \mathcal{C} \to \mathcal{D}, i = 1,2$ to ich* transformacją naturalną *nazywamy przyporządkowanie każdemu obiektowi $X \in \mathrm{ob}(\mathcal{C})$ morfizmu (w $\mathcal{D}$) $\Phi_X\colon F_1(X) \to F_2(X)$ tak, że dla dowolnego morfizmu $f\colon X \to Y$ w $\mathcal{C}$ następujący diagram w kategorii $\mathcal{D}$ jest przemienny:*

$$\begin{array}{ccc} F_1(X) & \xrightarrow{\Phi_X} & F_2(X) \\ {\scriptstyle F_1(f)}\downarrow & & \downarrow{\scriptstyle F_2(f)} \\ F_1(Y) & \xrightarrow{\Phi_Y} & F_2(Y) \end{array}$$

Transformacja naturalna Φ nazywa się naturalną równoważnością funktorów *jeśli dla każdego obiektu $X \in \mathrm{ob}(\mathcal{C})$, morfizm Φ_X jest izomorfizmem.*

Definicja 31. *Funktor $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ jest równoważnością kategorii wtedy i tylko wtedy, gdy istnieje funktor $G : \mathcal{D} \longrightarrow \mathcal{C}$ oraz naturalne równoważności funktorów $F \circ G \simeq id_{\mathcal{D}}$ i $G \circ F \simeq id_{\mathcal{C}}$.*

Podamy znacznie wygodniejszy warunek na to, by funktor był równoważnościa kategorii - nie wymagający konstruowania funktora odwrotnego.

Twierdzenie 34. *Funktor $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ jest równoważnością kategorii wtedy i tylko wtedy, gdy*

1. *$F\colon \mathrm{Mor}_{\mathcal{C}}(A,B) \longrightarrow \mathrm{Mor}_{\mathcal{D}}(F(A),F(B))$ jest bijekcją dla dowolnych $A, B \in \mathrm{ob}(\mathcal{C})$;*
2. *każdy obiekt $Y \in \mathrm{ob}(\mathcal{D})$ jest izomorficzny z obiektem $F(A)$ dla pewnego $A \in \mathrm{ob}(\mathcal{C})$.*

Doskonałe wyjaśnienie motywacji tych definicji, a w szczególności transformacji naturalnej znajduje się we wstępie do oryginalnego artykułu Eilenberga-MacLane'a, w którym zostały wprowadzone do matematyki pojęcia teorii kategorii. Przytoczymy omawiany tam przykład:

Przykład 3. Zdefiniujemy kategorię skończenie wymiarowych, rzeczywistych przestrzeni wektorowych $\mathcal{V}ect_{\mathbb{R}}^{fin}$. Jej obiektami są skończenie wymiarowe rzeczywiste przestrzenie wektorowe. Dla dowolnych dwóch przestrzeni $V, W \in \mathrm{ob}(\mathcal{V}ect_{\mathbb{R}}^{fin})$, morfizmy to odwzorowania liniowe, czyli $\mathrm{Mor}(V,W) := \mathrm{Hom}_{\mathbb{R}}(V,W)$. Złożenie morfizmów to złożenie przekształceń liniowych a element neutralny to przekształcenie identycznościowe. Tak zdefiniowana $\mathcal{V}ect_{\mathbb{R}}^{fin}$ spełnia oczywiście aksjomaty kategorii Def. 24. Zauważmy przy okazji, że

kategoria $\mathcal{V}ect_{\mathbb{R}}^{fin}$ jest równoważna swojej podkategorii, której obiektami są przestrzenie wektorowe $\mathcal{N} := \{\mathbb{R}^n \,|\, n = 0, 1, 2, \dots\}$ a morfizmami wszystkie odworowania liniowe. Istotnie, włożenie $\mathcal{N} \to \mathcal{C}$ jest równoważnością kategorii, bo każda przestrzeń skończenie wymiarowa jest izomorficzna z pewną przestrzenią $\mathbb{R}^n$.

Na kategorii $\mathcal{V}ect_{\mathbb{R}}^{fin}$ rozpatrzymy dwa funktory, znane dobrze z Algebry Liniowej:

- Funktor kontrawariantny przestrzeni sprzężonej $^*\colon (\mathcal{V}ect_{\mathbb{R}}^{fin})^{op} \to \mathcal{V}ect_{\mathbb{R}}^{fin}$ przypisujący przestrzeni V przestrzeń sprzężoną V^* oraz odwzorowaniu liniowemu $f\colon V \to W$ przekształcenie liniowe $f^*\colon W^* \to V^*$.
- Funktor drugiej przestrzeni sprzężonej, czyli złożenie funktora * ze sobą. Jest to funktor kowariantny $^{**}\colon \mathcal{V}ect_{\mathbb{R}}^{fin} \to \mathcal{V}ect_{\mathbb{R}}^{fin}$, który przypisuje przestrzeni wektorowej V przestrzeń $V^{**} := (V^*)^*$ a homorfizmowi $f\colon V \to W$ przekształcenie liniowe $f^{**}\colon V^{**} \to W^{**}$.

Dla każdej przestrzeni liniowej V istnieje izomorfizm $V \simeq V^*$, ale do zdefiniowania go konieczny jest pewien wybór np. bazy w V lub iloczynu skalarnego w V.

Izomorfizm $V \simeq V^{**}$, może być zdefiniowany kanonicznie tzn. wyłącznie w terminach przestrzeni V, bez odwoływania się do dodatkowych struktur, jak w poprzednim przypadku. Dla dowolnej przestrzeni V zdefiniujmy przekształcenie liniowe $\Phi_V\colon V \to V^{**}$ wzorem $\Phi_V(v)(\varphi) := \varphi(v)$. przekształcenie Φ_V jest różnowartościowe, a więc dla skończenie wymiarowych przestrzeni wektorowych jest izomorfizmem, bowiem $\dim(V) = \dim(V^{**})$. Znane z Algebry Liniowej określenie Φ_V jako *kanonicznego izomorfizmu* znajduje ścisłe sformułowanie w postaci stwierdzenia, że Φ_V jest transformacją naturalną (równoważnością) funktora identycznościowego do funktora drugiej przestrzeni sprzężonej. Istotnie, dla dowolnego odwzorowania liniowego $f\colon V \to W$ diagram przekształceń liniowych:

$$\begin{array}{ccc} V & \xrightarrow{\Phi_V} & V^{**} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f^{**}} \\ W & \xrightarrow[\Phi_W]{} & W^{**} \end{array}$$

jest przemienny.

Zauważmy, że dla każdej z kategorii 1.–9. istnieje *funktor zapominania* $F\colon \mathcal{C} \to \mathcal{S}et$ prowadzący do kategorii zbiorów, polegający na przyporządkowaniu zbiorowi ze strukturą samego zbioru, a morfizmom odpowiednich przekształceń zbiorów. Funktor zapominania jest oczywiście różnowartościowy na zbiorach morfizmów, ale na ogół skleja klasy izomorfizmu obiektów

np. $F\colon \mathcal{G}r \to \mathcal{S}et$ przeprowadza nieizomorficzne grupy $\mathbb{Z}_4$ i $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ na izomorficzne zbiory czteroelementowe. Kategorie wyposażone w funktor zapominania do kategorii zbiorów (który można opisać aksjomatycznie) nazywają się *kategoriami konkretnymi.* Mówiąc nieformalnie, są to kategorie których obiektami są zbiory z wyróżnioną strukturą (np. porządkiem, działaniem lub topologią) a morfizmami przekształcenia zbiorów zachowujące tę strukturę.

Definicja 32. *Kategorię $\mathcal{C}$ nazywamy* małą *jeśli klasa obiektów* $\mathrm{ob}\,(\mathcal{C})$ *jest zbiorem.*

Obiekty w małych kategoriach często oznaczamy małymi literami, a więc $c \in \mathrm{ob}\,(\mathcal{C})$. Kategorie BG i EG są przykładami małych kategorii, kategoria

Przykład 4. Niech $(S, \leq)$ będzie zbiorem częściowo uporządkowanym (*poset*). Zdefiniujemy kategorię $\mathcal{C}_S$, w której $\mathrm{ob}\,(\mathcal{C}_S) := S$ oraz

$$\mathrm{Mor}(s_1, s_2) = \begin{cases} (s_2, s_1) & \text{jeśli} \quad s_1 \leq s_2 \\ \emptyset & \text{w przeciwnym przypadku.} \end{cases} .$$

Złożenie zdefiniowane jest w oczywisty sposób: $(s_3, s_2)(s_2, s_1) := (s_3, s_1)$.

Małe kategorie i funktory między nimi tworzą kategorię (bo funktory między małymi kategoriami tworzą zbiór!) oznaczaną $\mathcal{C}at$. Ostatnie przykłady oznaczają, że kategoria grup i kategoria zbiorów częściowo uporządkowanych są równoważne pewnym podkategoriom w $\mathcal{C}at$. Jedynym wspólnym obiektem obu odpowiednich podkategorii jest zbiór jednopunktowy.

3.2 Funktory reprezentowalne

Dowolny obiekt kategorii $\mathcal{C}$ wyznacza funktor kowariantny i funktor kontrawariantny do kategorii zbiorów.

Definicja 33. *Dla $X \in \mathrm{ob}\,\mathcal{C}$ definiujemy funktory:*

- *Funktor kowariantny $R_X\colon \mathcal{C} \to \mathcal{S}et$ reprezentowany przez obiekt X:*
  - $R_X(U) := \mathrm{Mor}_{\mathcal{C}}(X, U)$ *dla* $U \in \mathrm{ob}\,(\mathcal{C})$
  - $R_X(f)(g) := f \circ g$ *dla* $f : U \to V$ *i* $g : X \to U$
- *Funktor kontrawariantny $R^X\colon \mathcal{C} \to \mathcal{S}et$ reprezentowany przez obiekt X.*
  - $R^X(U) := \mathrm{Mor}_{\mathcal{C}}(U, X)$ *dla* $U \in \mathrm{ob}\,(\mathcal{C})$
  - $R^X(f)(g) := g \circ f$ *dla* $f : U \to V$ *i* $g : V \to X$

Definicja 34. *Funktor kontrawariantny $F : \mathcal{C} \to \mathcal{S}et$ nazywamy reprezentowalnym wtedy i tylko wtedy, gdy istnieje obiekt $X \in \mathcal{C}$ oraz naturalna równoważność funktorów $R^X \to F$. Analogicznie dla funktora kowariantnego.*

3.3 Funktory sprzężone

Adjoint functors arise everywhere.

Saunders Mac Lane

Pojęcie funktorów sprzężonych (dołączonych - *adjoint functors*) nawiązuje do pojęcia przekształcenia sprzężonego, znanego z algebry liniowej. Jeśli $(V, \langle -, - \rangle_V)$ oraz $(W, \langle -, - \rangle_W)$ są skończenie wymiarowymi rzeczywistymi przestrzeniami liniowymi wyposażonymi w iloczyn skalarny, to dowolnemu przekształceniu liniowemu $f\colon V \to W$ można przypisać przekształcenie sprzężone (lub dołączone) $f^!\colon W \to V$ takie, że dla dowolnych elementów $v \in V, w \in W$ zachodzi równość: $\langle v, f^!(w) \rangle_V = \langle f(v), w \rangle_W$. Puszczając nieco wodze matematycznej fantazji można myśleć o przyporządkowaniu parze obiektów kategorii zbioru morfizmów jako rodzaju "formy dwuliniowej", której wartościami są zbiory. Ten punkt widzenia prowadzi naturalnie do definicji funktorów sprzężonych dołączonych.

Definicja 35. *Funktory $F : \mathcal{C} \to \mathcal{D}$ i $G : \mathcal{D} \to \mathcal{C}$ nazywamy sprzężonymi (dołączonymi), gdy istnieje naturalna równoważność funktorów na kategorii $\mathcal{C}^{op} \times \mathcal{D}$ o wartościach w $\mathcal{S}et$*

$$\Phi\colon \operatorname{Mor}_{\mathcal{C}}(\cdot\,, G(\cdot)) \xrightarrow{\simeq} \operatorname{Mor}_{\mathcal{D}}(F(\cdot), \cdot\,)$$

tzn. dla dowolnej pary morfizmów $C_2 \xrightarrow{f} C_1$ w $\mathcal{C}$ oraz $D_1 \xrightarrow{h} D_2$ w $\mathcal{D}$ diagram:

$$\begin{array}{ccc} \operatorname{Mor}_{\mathcal{C}}(C_1, G(D_1)) & \xrightarrow[\simeq]{\Phi_{C_1,D_1}} & \operatorname{Mor}_{\mathcal{D}}(F(C_1), D_1) \\ \Big\downarrow{\scriptstyle G(h)_! f^!} & & \Big\downarrow{\scriptstyle h_! F(f)^!} \\ \operatorname{Mor}_{\mathcal{C}}(C_2, G(D_2)) & \xrightarrow[\simeq]{\Phi_{C_2,D_2}} & \operatorname{Mor}_{\mathcal{D}}(F(C_2), D_2) \end{array} \tag{3.1}$$

jest przemienny. Mówimy, że funktor F jest lewo-sprzężony *do funktora G, a G jest* prawo-sprzężony *do funktora F.*

Przykład 5. Zbiór morfizmów w kategorii zbiorów oznaczamy $\operatorname{Map}(-,-)$. Dla trzech zbiorów $X, Y, Z \in \operatorname{ob}(\mathcal{S}et)$ istnieje naturalna równoważność funktorów

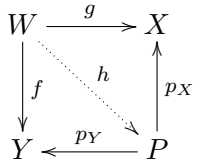
$$\Phi_{(X,Y,Z)}\colon \operatorname{Map}(X \times Y, Z) \simeq \operatorname{Map}(X, \operatorname{Map}(Y, Z))$$

dana wzorem $\Phi_{(X,Y,Z)}(f)(x)(y) := f(x, y)$. Ustalając zbiór Y otrzymujemy, że funktor $R_Y(Z) = \operatorname{Map}(Y, Z)$ posiada funktor lewo-dołączony $F(X) := X \times Y$.

Bardzo ważnymi przykładami funktorów dołączonych są funktory dołączone do funktorów zapominania.

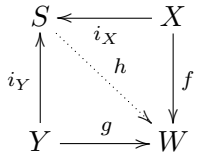
3.4 Produkty i koprodukty, granice i kogranice

Definicja 36. *Produktem (kartezjańskim) obiektów X i Y w kategorii $\mathcal{C}$ nazywamy obiekt P wraz z morfizmami $P \longrightarrow p_X X$ i $P \longrightarrow p_Y Y$, który ma następującą własność uniwersalności: dla dowolnych morfizmów $W \longrightarrow fX$ i $W \longrightarrow gY$ istnieje dokładnie jeden morfizm $W \longrightarrow hP$, dla którego $p_X \circ h = f$ i $p_Y \circ h = g$.*



(3.2)

Definicja 37. *Koproduktem obiektów X i Y w kategorii $\mathcal{C}$ nazywamy obiekt S wraz z morfizmami $X \longrightarrow i_X S$ i $Y \longrightarrow i_Y S$, który ma następująca własność uniwersalności: dla dowolnych morfizmów $X \longrightarrow fW$ i $Y \longrightarrow gW$ istnieje dokładnie jeden morfizm $S \longrightarrow hW$, dla którego $h \circ i_X = f$ i $h \circ i_Y = g$.*



(3.3)

Uwaga. Koprodukt obiektów X i Y w kategorii $\mathcal{C}$ jest produktem w kategorii $\mathcal{C}^{op}$.

3.4.1. *Podać definicję produktu i koproduktu dowolnej rodziny obiektów $\{X_j\}_{j \in J}$.*

Produkt (odpowiednio koprodukt) rodziny obiektów $\{X_j\}_{j \in J}$ oznaczamy:

$$\text{Produkt: } \prod_{j \in J} X_j \qquad \text{Koprodukt : } \coprod_{j \in J} X_j$$

Produkt rodziny obiektów nazywamy czasem *produktem kartezjańskim* a koprodukt *sumą prostą*.

Zdefiniujemy teraz ogólniejszą konstrukcję granicy (zwanej też granicą odwrotną) i kogranicy (zwanej też granicą prostą) diagramu modelowanego na małej kategorii.

Definicja 38. *Niech $\mathcal{I}$ będzie małą kategorią. Diagramem w kategorii $\mathcal{C}$ modelowanym na $\mathcal{I}$ nazywamy dowolny funktor $F : \mathcal{I} \to \mathcal{C}$. Powiemy, że rodzina morfizmów $\{f_j : W \to F(j)\}_{j \in \mathcal{I}}$ jest* zgodna *jeżeli dla każdego $\alpha_{ij} : i \to j$ morfizmu w $\mathcal{I}$, $F(\alpha_{ij}) \circ f_i = f_j$.*

Definicja 39. Granicą *(lub granicą odwrotną) diagramu* $F : \mathcal{I} \to \mathcal{C}$ *nazywamy obiekt* L *w kategorii* $\mathcal{C}$ *(oznaczamy go* $\lim_{\mathcal{I}} F$*) wraz ze zgodną rodziną morfizmów* $\{p_j : L \to F(j)\}_{j \in \mathrm{ob}\,\mathcal{I}}$*, który posiada następującą własność uniwersalności: dla każdego obiektu* W *i zgodnej rodziny* $\{f_j : W \to F(j)\}_{j \in \mathrm{ob}\,\mathcal{I}}$ *istnieje* **dokładnie jeden** *morfizm* $g : W \to L$*, dla którego* $p_j \circ g = f_j$ *dla każdego* $j \in \mathrm{ob}\,\mathcal{I}$*.*

Jeżeli odwrócimy strzałki dostaniemy dualne pojęcie granicy prostej (zwanej też kogranicą) diagramu.

Definicja 40. Kogranicą *(lub granicą prostą) diagramu* $F : \mathcal{I} \to \mathcal{C}$ *nazywamy obiekt* C *w kategorii* $\mathcal{C}$ *(oznaczamy go* $\mathrm{colim}_{\mathcal{I}} F$*) wraz ze zgodną rodziną morfizmów* $\{s_j : F(j) \to C\}_{j \in \mathrm{ob}\,\mathcal{I}}$*, który posiada następującą własność uniwersalności: dla każdego obiektu* W *i zgodnej rodziny* $\{f_j : F(j) \to W\}_{j \in \mathrm{ob}\,\mathcal{I}}$ *istnieje* **dokładnie jeden** *morfizm* $g : C \to W$*, dla którego* $g \circ s_j = f_j$ *dla każdego* $j \in \mathrm{ob}\,\mathcal{I}$*.*

Stwierdzenie 14. *Granica i kogranica diagramu, o ile istnieje, to tylko jedna z dokładnością do izomorfizmu.*

Przykład 6. Granica (odp. kogranica) diagramu modelowanego na kategorii dyskretnej (tzn. w której istnieją tylko morfizmy identycznościowe) jest izomorficzna z produktem (odp. koproduktem) rodziny obiektów.

Definicja 41. *Obiekt* $i_0 \in \mathrm{ob}\,\mathcal{C}$ *nazywa się początkowy, jeżeli dla każdego obiektu* $c \in \mathrm{ob}\,\mathcal{C}$ *istnieje dokładnie jeden morfizm* $i_0 \to c$*. Obiekt* $i_\infty \in \mathrm{ob}\,\mathcal{C}$ *nazywa się końcowy jeżeli jest obiektem początkowym w* $\mathcal{C}^{op}$*.*

Przykład 7. *Opiszemy bardzo ważne konstrukcje granicy i kogranicy diagramu zbiorów. Niech* $F\colon \mathcal{I} \to \mathcal{S}et$ *będzie diagramem w kategorii zbiorów.*

Granica diagramu F *jest podzbiorem zdefiniowanym następująco:*

$$\lim_{\mathcal{I}} F := \{\{x_i\} \in \prod_{i \in \mathrm{ob}\,\mathcal{I}} F(i) \quad | \quad \forall_{\alpha\colon i \to j}\ F(\alpha)(x_i) = x_j\}$$

Morfizmy $p_i\colon \lim_{\mathcal{I}} F \to F(i)$ *to obcięcia rzutowań z iloczynu kartezjańskiego na czynniki.*

Kogranicę diagramu definiujemy dualnie, jako zbiór ilorazowy sumy rozłącznej.

$$\mathrm{colim}_{\mathcal{I}} F := (\coprod_{i \in \mathrm{ob}\,\mathcal{I}} F(i))/\sim$$

gdzie $\sim$ *jest najmniejszą relacją zawierającą utożsamienia* $(x', i) \sim (x'', j)$ *jeśli istnieją morfizmy* $\alpha_i\colon i \to k$ *oraz* $\alpha_j\colon j \to k$ *takie, że* $F(\alpha_i)(x') = F(\alpha_j)(x'')$*. Morfizmy* $s_i\colon F(i) \to \mathrm{colim}_{\mathcal{I}} F$ *są zdefiniowane przez włożenia w koprodukt.*

Stwierdzenie 15. *Niech $F\colon \mathcal{I} \to \mathcal{C}$ będzie dowolnym diagramem. Obiekt $C \in \mathrm{ob}\,(\mathcal{C})$ z morfizmami strukturalnymi $\{C \to F(i)\}_{i\in \mathrm{ob}\,(\mathcal{I})}$ jest granicą odwrotną diagramu F wtedy i tylko wtedy, gdy reprezentuje funktor $G_F\colon \mathcal{C} \to \mathcal{S}et$ dany wzorem $G_F(X) = \lim_{\mathcal{I}} \mathrm{Mor}_{\mathcal{C}}(X, F(-))$ (gdzie* lim *jest obiektem w kategorii $\mathcal{S}et$) a morfizmy strukturalne odpowiadają elementowi $id \in G_F(C)$.*

Definicja 42. *Granicę diagramu modelowanego na kategorii $0 \rightrightarrows 1$ (czyli dwóch morfizmów między tymi samymi obiektami) nazywamy ekwalizatorem tych morfizmów (także jądrem różnicowym) i oznaczamy* Eq , *a kogranicę ich koekwalizatorem (także kojąderem różnicowym) i oznaczamy* Coeq.

Przykład 8. *Niech $f, g\colon V \rightrightarrows W$ będą dwoma odwzorowaniami liniowymi. Wtedy $\mathrm{Eq}(f,g) = \ker(f-g)$ a $\mathrm{Coeq}(f,g) = \mathrm{coker}(f-g)$. W szczególności jeśli $g = 0$, to jądro różnicowe jest po prostu jądrem przekształcenia f, a kojądro róznicowe, jego kojądrem.*

Stwierdzenie 16. *Jeśli w kategorii $\mathcal{C}$ istnieją ekwalizatory dla dowolnej pary morfizmów (odp. koekwalizatory) oraz produkty (odp. koprodukty) dowolnej (skończonej) rodziny obiektów , to istnieją w niej granice (odp. kogranice) dowolnych (skończonych) diagramów.*

Stwierdzenie 17. *Niech $F : \mathcal{I} \to \mathcal{C}$ będzie dowolnym diagramem. Niech $G : \mathcal{C} \to \mathcal{C}'$ będzie funktorem.*

a) Jeżeli w kategoriach $\mathcal{C}$ i $\mathcal{C}'$ istnieją granice i funktor G posiada funktor lewo-dołączony $H : \mathcal{C}' \to \mathcal{C}$, to istnieje naturalny izomorfizm

$$\lim_{\mathcal{I}}(G \circ F) \cong G \circ \lim_{\mathcal{I}} F$$

b) Jeżeli w kategoriach $\mathcal{C}$ i $\mathcal{C}'$ istnieją kogranice i funktor G posiada funktor prawo-dołączony $H : \mathcal{C}' \to \mathcal{C}$, to istnieje naturalny izomorfizm

$$\mathrm{colim}_{\mathcal{I}}(G \circ F) \cong G \circ \mathrm{colim}_{\mathcal{I}} F$$

Dowód. Udowodnimy punkt a), dowód b) jest analogiczny.

Istnieje naturalny morfizm w kategorii $\mathcal{C}'$, $G \circ \lim_{\mathcal{I}} F \to \lim_{\mathcal{I}}(G \circ F)$. Pokażemy, że jest on izomorfizmem. Dla dowolnego obiektu $Y \in \mathcal{C}'$ mamy ciąg izomorfizmów:

$$\begin{aligned} Mor_{\mathcal{C}'}(Y, G \circ \lim_{\mathcal{I}} F) &\cong Mor_{\mathcal{C}}(H(Y), \lim_{\mathcal{I}} F) \\ &\cong \lim_{\mathcal{I}} Mor_{\mathcal{C}}(H(Y), F) \\ &\cong \lim_{\mathcal{I}} Mor_{\mathcal{C}'}(Y, G \circ F) \\ &\cong Mor_{\mathcal{C}'}(Y, \lim_{\mathcal{I}}(G \circ F) \end{aligned}$$

Z tego wynika już teza wobec natępującego lematu. □

Lemat 8. *Jeżeli w kategorii $\mathcal{C}$ morfizm $f : X \to Y$ indukuje izomorfizm funktorów $\mathrm{Mor}_{\mathcal{C}}(\cdot, X) \to \mathrm{Mor}_{\mathcal{C}}(\cdot, Y)$ (lub $\mathrm{Mor}_{\mathcal{C}}(Y, \cdot) \to \mathrm{Mor}_{\mathcal{C}}(X, \cdot)$), to f jest izomorfizmem.*

Dowód. Dowód pozostawiamy czytelnikowi. □

3.5 Kategorie addytywne

Zauważmy, że w kategorii np. grup abelowych, przestrzeni liniowych skończony produkt i skończona suma to jest to samo. W tych kategoriach możemy też mówić o morfizmach zerowych. Wspólnym językiem dla tych pojęć jest kategoria addytywna.

Definicja 43. *Obiektem zerowym kategorii $\mathcal{C}$ nazywamy obiekt, który jest jednocześnie początkowy i końcowy.*

Definicja 44. *Kategorię $\mathcal{C}$ nazywamy addytywną, jeżeli :*

a) dla dowolnych obiektów $X, Y \in ob\mathcal{C}$, $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ jest grupą przemienną;

b) składanie morfizmów jest dwuliniowe;

c) w kategorii $\mathcal{C}$ istnieje obiekt zerowy;

d) w kategorii $\mathcal{C}$ istnieją skończone produkty;

e) w kategorii $\mathcal{C}$ istnieją skończone koprodukty

Pokażemy, ze dwa ostatnie warunki (przy spełnieniu pierwszych trzech) są równoważne i są równoważne następującemu:

Stwierdzenie 18. *Niech $\mathcal{C}$ będzie kategorią spełniającą warunki a), b), c). Rozważmy następujący warunek:*
f): Dla dowolnych dwóch obiektów $X, Y \in ob\mathcal{C}$ istnieje obiekt $Z \in ob\mathcal{C}$ oraz morfizmy $i_X : X \to Z$, $p_X : Z \to X$, $i_Y : Y \to Z$, $p_Y : Z \to Y$, które spełniaja następujace warunki:

$$\begin{array}{ll} p_X i_X = id_X & p_X i_Y = 0 \\ p_Y i_Y = id_Y & p_Y i_X = 0 \end{array}$$

$$i_X p_X + i_Y p_Y = id_Z$$

Wówczas warunki d),e),f) są równoważne oraz suma i produkt obiektów X,Y jest izomorficzna obiektowi Z. Obiekt ten będziemy oznaczać symbolem $X \oplus Y$ i nazywać sumą prostą.

Dowód. Pokażemy, że warunki d) i f) są równoważne. Niech $X \times Y$ będzie produktem. Pokażemy, że spełnia on warunek f), tak więc obiekt o pożądanych własnościach istnieje. Morfizmy $p_X = \pi_X$ i $p_Y = \pi_Y$ niech będą rzutowaniami. Niech i_X będzie zdefiniowany przez warunki $p_X i_X = id_X$ oraz $p_Y i_X = 0$, analogicznie dla i_Y. Wystarczy sprawdzić, że

$$i_X p_X + i_Y p_Y = id_{X \times Y}.$$

W tym celu liczymy złożenia:

$$p_X \circ (i_X p_X + i_Y p_Y) = p_X i_X p_X + p_X i_Y p_Y = id_X p_X + 0 p_Y = p_X$$

i analogicznie

$$p_Y(i_X p_X + i_Y p_Y) = p_Y.$$

Zatem z definicji produktu wnosimy, że

$$i_X p_X + i_Y p_Y = id_{X \times Y}.$$

Niech Z spełnia warunek f). Pokażemy, że (Z, p_X, p_Y) spełnia warunek uniwersalny definiujący produkt. Niech $g : W \to X$ i $h : W \to Y$ będą dowolnymi morfizmami. Definiujemy morfizm $i_X g + i_Y h : W \to Z$. Spełnia on $p_X(i_X g + i_Y h) = g$ oraz $p_Y(i_X g + i_Y h) = h$. Ponadto, jeżeli $k : W \to Z$ spełnia $p_X k = g$ i $p_Y k = h$, to $k = (i_X p_X + i_Y p_Y)k = i_X p_X k + i_Y p_Y k = i_X g + i_Y h$, co kończy dowód. Równoważność warunków e) i f) dowodzi się analogicznie, trzeba tylko odwrócić strzałki. □

Definicja 45. *Niech $\mathcal{C}$ i $\mathcal{D}$ będą kategoriami addytywnymi. Powiemy, że funktor $F : \mathcal{C} \to \mathcal{D}$ jest addytywny, jeżeli*

$$F : \mathrm{Mor}_{\mathcal{C}}(X, Y) \to \mathrm{Mor}_{\mathcal{D}}(F(X), F(Y))$$

jest homomorfizmem grup.

Stwierdzenie 19. *Niech $\mathcal{C}$ i $\mathcal{D}$ będą kategoriami addytywnymi. Funktor $F : \mathcal{C} \to \mathcal{D}$ jest addytywny wtedy i tylko wtedy, gdy*

$$F(0) = 0$$

i dla dowolnych obiektów $a, b \in ob\mathcal{C}$,

$$F(a \oplus b) = F(a) \oplus F(b).$$

W definicji kategorii addytywnej nie zakładamy istnienia granic i kogranic. Natomiast jeśli istnieje granica (ekwalizator) diagramu $x \underset{0}{\overset{f}{\rightrightarrows}} y$, to nazywamy ją jądrem morfizmu f i mamy

$$\ker f \xrightarrow{\ i\ } x \underset{0}{\overset{f}{\rightrightarrows}} y\ .$$

Analogicznie kogranica (koekwalizator), o ile istnieje, nazywa sie kojądrem morfizmu, jest oznaczana symbolem coker i mamy

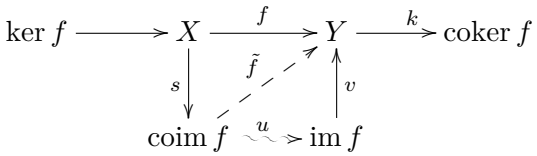
$$x \underset{0}{\overset{f}{\rightrightarrows}} y \xrightarrow{j} \operatorname{coker} f \ .$$

Zakładając istnienie odpowiednich jąder i kojąder mamy dalej: Koobrazem, oznaczanym symbolem coim, morfizmu $f : x \to y$ nazywamy kojądro $\ker f \to x$, czyli mamy $x \to \operatorname{coim} f$. Definiujemy także $\operatorname{im} f$ jako jądro $y \to \operatorname{coker} f$, czyli dostajemy morfizm $\operatorname{im} f \to y$.

Lemat 9. *Niech $f : x \to y$ będzie morfizmem w addytywnej kategorii $\mathcal{C}$, dla którego istnieją* $\ker f$, $\operatorname{coker} f$, $\operatorname{coim} f$ *oraz* $\operatorname{im} f$. *Wówczas morfizm f może być jednoznacznie przedstawiony jako złożenie:*

$$x \xrightarrow{s} \operatorname{coim} f \xrightarrow{u} \operatorname{im} f \xrightarrow{v} y \ .$$

Dowód. Rozważmy diagram:



Istnieje dokładnie jeden morfizm $\tilde{f} : \operatorname{coim} f \to y$, bo $\ker f \to x \to y$ jest morfizmem zerowym, a $\operatorname{coim} f$ koekwalizatorem. Rozważmy teraz homomorfizm $kf : X \to \operatorname{coker} f$. Istnieje z definicji koekwalizatora homomorfizm $\operatorname{coim} f \to \operatorname{coker} f$ i jest nim $k\tilde{f}$. Ale homomorfizm zerowy także czyni odpowiedni diagram przemiennym, więc $k\tilde{f}$ jest zerowy z jednoznaczności. Zatem z definicji jądra u istnieje. Wszystkie konstruowane morfizmy były jedyne, a zatem ich złożenie jest równe f. □

3.6 Kategorie abelowe

Definicja 46. *Kategoria addytywna $\mathcal{C}$ nazywa się abelowa, jeżeli*

a) każdy morfizm w $\mathcal{C}$ ma jądro i kojądro;

b) dla morfizmu $f : x \to y$ naturalny morfizm $u : \operatorname{coim} f \to \operatorname{im} f$ jest izomorfizmem.

3.7 Zadania

Transformacje naturalne, równoważność kategorii.

3.7.1. Udowodnić twierdzenie 34

3.7.2. Niech $f_0, f_1 \colon G \to H$ będą dwoma homomorfizmami grup. Udowodnić, że istnieje bijekcja zbioru transformacji naturalnych między wyznaczonymi przez nie funktorami $F_0, F_1 \colon \mathcal{B}G \to \mathcal{B}H$ a elementami $h \in H$ takimi, że dla każdego $g \in G$, $f_1(g) = hf_0(g)h^{-1}$, czyli $f_1 = c_h f_0$ gdzie $c_h \colon H \to H$ jest automorfizmem wewnętrznym wyznaczonym przez element $h \in H$.

3.7.3. Niech $f_0, f_1 \colon S \to T$ będą dwoma morfizmami posetów (odwzorowaniami zachowującymi porządek). Udowodnić, że istnieje transformacja naturalna (dokładnie jedna) między definiowanymi przez nie funktorami $F_0, F_1 \colon \mathcal{C}_S \to \mathcal{C}_T$ wtedy i tylko wtedy gdy $f_0(s) \leq f_1(s)$ dla każdego $s \in S$.

3.7.4. Mała kategoria $\mathcal{C}$ w której dla dowolnych dwóch obiektów $c, c' \in \mathrm{ob}\,(\mathcal{C})$ istnieje co najwyżej jeden morfizm $c \to c'$ jest równoważna (ale nie identyczna!) z kategorią definiowaną przez poset (zbiór częściowo uporządkowany).

3.7.5. Jeśli w małej kategorii każdy morfizm jest izomorfizmem oraz między każdymi dwoma obiektami istnieje morfizm, to ta kategoria jest równoważna kategorii $\mathcal{B}G$ definiowanej przez pewną grupę G. Podaj (nietrywialne) przykłady takich kategorii. Wyznacz grupę G taką,że $\mathcal{E}H \cong \mathcal{B}G$, dla dowolnej grupy H.

3.7.6. Pokazać,że jeżeli grupy G i H są izomorficzne, to kategorie $\mathcal{B}G$ i $\mathcal{B}H$ są równoważne. Czy prawdziwe jest twierdzenie odwrotne?

3.7.1 Funktory sprzężone

3.7.7. Pokazać, że funktor sprzężony do danego funktora, o ile istnieje, to jest wyznaczony jednoznacznie z dokładnością do naturalnej równoważności funktorów.

3.7.8. Pokazać, że jeżeli funktor $F : \mathcal{C} \to \mathcal{D}$ jest równoważnością kategorii, to istnieje funktor $G : \mathcal{D} \to \mathcal{C}$ sprzężony do F zarówno z prawej jak i lewej strony.

3.7.9. Pokazać, że istnieje funktor prawo sprzężony do funktora $F : \mathcal{C} \to \mathcal{D}$, wtedy i tylko wtedy gdy dla każdego obiektu $Y \in \mathcal{D}$ funktor $Mor_{\mathcal{D}}(F(\cdot), Y) : \mathcal{C} \to \mathcal{S}et$ jest reprezentowalny.

3.7.10. Niech $\mathcal{S}et_*$ będzie kategorią zbiorów z wyróżnionym punktem. Skonstruować funktor lewo-dołączony do funktora $R^*_X \colon \mathcal{S}et_* \to \mathcal{S}et_*$, gdzie punktem wyróżnionym w $R^*_X(Z) := \mathrm{Map}_*(X, Z)$ jest przekształcenie stałe w punkt wyróżniony w Z.

3.7.11. Wykazać, że funktory $F : \mathcal{C} \to \mathcal{D}$ i $G : \mathcal{D} \to \mathcal{C}$ są sprzężone wtedy i tylko wtedy gdy istnieją transformacje naturalne $\eta \colon id_{\mathcal{C}} \to FG$ oraz $\epsilon \colon GF \to id_{\mathcal{D}}$ takie, że złożenia

$$F \longrightarrow L\eta FGF \longrightarrow \epsilon GF \quad \text{oraz} \quad G \longrightarrow \eta RGFG \longrightarrow G\epsilon G$$

są identycznościami.

3.7.12. Skonstruuj funktory lewo-dołączone do funktorów zapominania:

a) $\mathcal{S}et_* \to \mathcal{S}et$;

b) $\mathcal{G}r \to \mathcal{S}et$ oraz $\mathcal{G}r \to \mathcal{S}et_*$ (punkt wyróżniony w zbiorze na którym określona jest struktura grupowa to element neutralny);

c) $\mathcal{A}b \subset \mathcal{G}r$, gdzie $\mathcal{A}b$ podkategoria grup abelowych;

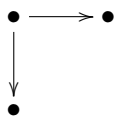
d) $\mathcal{A}b \to \mathcal{S}et$;

e) $\mathcal{S}et_G \to \mathcal{S}et_H$ – gdzie G jest grupą, a $\mathcal{S}et_G$ oznacza kategorię, której obiektami są G–zbiory a morfizmami G-przekształcenia, zaś dla podgrupy $H \subset G$ funktor $\mathcal{S}et_G \to \mathcal{S}et_H$ jest funktorem zapominania (obcięcia działania) do podgrupy H.

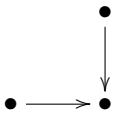
3.7.13. Czy jeśli dla funktora $F : \mathcal{C} \to \mathcal{D}$ istnieje funktor $G : \mathcal{D} \to \mathcal{C}$ sprzężony do F zarówno z prawej jak i lewej strony, to F jest równoważnością kategorii?

Granice i kogranice

3.7.14. Zbadać istnienie colim (nazywa się go push- outem) diagramu



oraz lim (nazywa się go pull - backiem) diagramu



w kategoriach $\mathcal{S}et$, $\mathcal{G}r$ i $\mathcal{A}b$

3.7.15. ♣ Udowodnić stwierdzenie 16.

Dowód. Niech C będzie granicą diagramu

$$C \longrightarrow \prod_{i \in ob\mathcal{C}} F(i) \underset{T}{\overset{S}{\rightrightarrows}} \prod_{i \to j \in Mor\mathcal{C}} F(j) \ ,$$

w którym S jest zdefiniowane przez warunek $p_{i\to j}S = F(i \to j)p_i$ zaś T przez warunek $p_{i\to j}T = p_j$. Łatwo sprawdzić, że $C = \lim_{\mathcal{I}} F$.

□

3.7.16. ♣ Jeśli kategoria $\mathcal{I}$ ma obiekt początkowy $i_0 \in \text{ob } \mathcal{I}$ (odpowiednio końcowy $i_\infty \in \text{ob } \mathcal{I}$), to dla dowolnego diagramu $F : \mathcal{I} \to \mathcal{C}$ istnieje jego granica i jest ona równa $\lim_{\mathcal{I}} F = F(i_0)$ (odpowiednio istnieje kogranica i jest ona równa $\text{colim}_{\mathcal{I}} F = F(i_\infty)$).

Dowód. Ponieważ istnieje dokładnie jeden morfizm $i_j : i_0 \to j$ dla dowolnego obiektu $j \in ob\mathcal{I}$, to $F(i_j) : F(i_0) \to F(j)$ jest odwzorowaniem w diagram. Pokażemy, że to jest granica. Dla obiektu W i zgodnej rodziny $\{f_j : W \to F(j)\}_{j\in \text{ob } \mathcal{I}}$ morfizm $f_{i_0} : W \to F(i_0)$ spełnia $f_{i_0}F(i_j) = f_j$, ze zgodności rodziny $\{f_j\}$. Ponadto, jeżeli $g : W \to F(i_0)$ jest innym morfizmem, to $gF(i_j) = f_j$ więc w szczególności dla $j = i_0$, $gF(i_{i_0}) = f_{i_0}$, Ale $F(i_{i_0}) = id$, stąd teza. Dla kogranic dowód jest bliźniaczy. □

3.7.17. ♣ Niech $\mathcal{C}(\mathbb{N})$ będzie małą kategorią wyznaczoną przez porządek w zbiorze liczb naturalnych, tzn. $n \to m \iff n \leq m$.

a) Niech $F : \mathcal{C}(\mathbb{N}) \to \mathcal{A}b$, $F(n) = \mathbb{Z}/p^n\mathbb{Z}$, $F(n \to m) : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, $F(n \to m)(x) = p^{m-n}x$. Pokazać, że $\text{colim } F \cong \{\frac{a}{p^n} \in \mathbb{Q},\ n \in \mathbb{N}\}/\mathbb{Z}$.

b) Niech $F : \mathcal{C}(\mathbb{N})^{op} \to \mathcal{A}b$, $F(n) = \mathbb{Z}/p^n\mathbb{Z}$, $F(m \to n) : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, jest naturalnym epimorfizmem . $\lim F := \mathbb{Z}_p$ nazywa się pierścieniem liczb całkowitych $p - adycznych$.(referacik)

3.7.18. ♣ Niech I będzie zbiorem liczb naturalnych uporządkowanych przez podzielność $n \leq m \iff n \mid m$. Niech $\mathcal{C}(I)$ będzie wyznaczoną przez ten porządek kategorią.

a) Niech $F : \mathcal{C}(I) \to \mathcal{A}b$, $F(n) = \mathbb{Z}/n\mathbb{Z}$, $F(n \to m)(x) = \frac{m}{n}x$. Pokazać, że colim $F \cong \mathbb{Q}/\mathbb{Z}$.

b) Niech $F : \mathcal{C}(I)^{op} \to \mathcal{A}b$, $F(n) = \mathbb{Z}/n\mathbb{Z}$, $F(m \to n) : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, jest naturalnym epimorfizmem. Pokazać, że $\lim F \cong \prod_p \mathbb{Z}_p$, gdzie produkt jest wzięty po zbiorze wszystkich liczb pierwszych.

3.7.19. Opisz ekwalizator i koekwalizator dowolnej pary morfizmów w kategorii $\mathcal{S}et$, $\mathcal{S}et*$, $\mathcal{G}r$, $\mathcal{A}b$ (zbadaj istnienie).

Kategorie addytywne

3.7.20. ♣ Niech $\mathcal{C}$ i $\mathcal{D}$ będą kategoriami addytywnymi, $F : \mathcal{C} \to \mathcal{D}$ funktorem, dla którego $F(a \oplus b) = F(a) \oplus F(b)$ dla dowolnych obiektów $a, b \in ob\mathcal{C}$ i $F(0) = 0$. Pokazać, że F jest funktorem addytywnym.

3.7.21.

Definicja 47. *Niech V będzie przestrzenią wektorową nad ciałem k. Jej filtracją (malejącą) nazywamy ciąg podprzestrzeni $\{F^n(V)\}_{n\in\mathbb{Z}}$, taki że*

$$V \supset \cdots \supset F^n(V) \supset F^{n+1}(V) \supset \ldots 0.$$

Rozważmy kategorię $\mathcal{V}ect_k^F$ w której obiektami są przestrzenie liniowe nad k z filtracją, a morfizmami przekształcenia liniowe zachowujące filtrację. Pokazać, że jest to kategoria addytywna. Czy spełnione są założenia lematu ? Rozważmy dwie filtracje przestrzeni liniowej V:

$$F^i(V) = \begin{cases} V \text{ jeżeli } i < 0 \\ 0 \text{ jeżeli } i \geq 0 \end{cases} \qquad \tilde{F}^i(V) = \begin{cases} V \text{ jeżeli } i \leq 0 \\ 0 \text{ jeżeli } i > 0 \end{cases} .$$

Pokazać, że $id_V : (V, F) \to (V, \tilde{F})$ jest morfizmem i sprawdzić, czy jest izomorfizmem w kategorii $\mathcal{V}ect_k^F$ (a tego wymagałoby stwierdzenie,że u jest izomorfizmem).

Rozdział 4

Teoria modułów

4.1 Definicja i podstawowe własności

Niech R będzie pierścieniem z 1, niekoniecznie przemiennym.
Definicja lewego (prawego) modułu. Przykłady (pierścień grupowy). Kategoria modułów nad ustalonym pierścieniem jest abelowa. Moduły wolne, moduły skończenie generowane, moduły noetherowskie.

Stwierdzenie 20. *Jeżeli R jest pierścieniem przemiennym, to dowolne dwie bazy modułu wolnego są równoliczne.*

4.2 Funktor $Hom(\cdot,\cdot)$. Moduły projektywne i injektywne.

Twierdzenie 35. *Następujące warunki sa równoważne:*

1. *moduł P jest projektywny;*
2. *każdy ciąg dokładny $0 \to N \to M \to P \to 0$ rozszczepia się;*
3. *P jest składnikiem prostym modułu wolnego.*

Twierdzenie 36. *Jeżeli R jest DIG, to moduł projektywny jest wolny.*

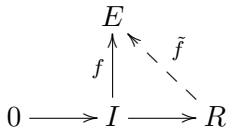
Twierdzenie 37. *Dla każdego modułu M istnieje jego rezolwenta projektywna, tzn ciąg dokładny $\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$, gdzie P_i są projektywne.*

Stwierdzenie 21. *Dowolna suma modułów projektywnych jest modułem projektywnym. Skończony produkt modułów projektywnych jest modułem projektywnym.*

Twierdzenie 38. *Moduł E jest injektywny wtedy i tylko wtedy, gdy ciąg dokładny $0 \to E \to M \to N \to 0$ rozszczepia się.*

Stwierdzenie 22. *Produkt dowolnej rodziny modułów injektywnych jest modułem injektywnym. Skończona suma modułów injektywnych jest modulem injektywnym.*

Twierdzenie 39. (Kryterium Baera) *R moduł E jest injektywny jeżeli dla dowolnego ideału $I \lhd R$ i dowolny homomorfizm modułów $f : I \to E$ rozszerza się do $\tilde{f} : R \to E$:*



Stwierdzenie 23. *Pierścień ułamków dziedziny całkowitości jest modułem injektywnym.*

Stwierdzenie 24. *Jeżeli R jest dziedziną całkowitości, to moduł injektywny jest podzielny.*

Twierdzenie 40. *Jeżeli R jest DIG, to moduł jest injektywny wtedy i tylko wtedy, gdy jest podzielny.*

Stwierdzenie 25. *Każda grupa przemienna jest podgrupą grupy podzielnej.*

Powyższe stwierdzenie jest prawdziwe dla modułów nad dowolnym pierścieniem i jego dowód w ogólnym przypadku korzystał z dołączenia iloczynu tensorowego i faktu, że dla dowolnego pierścienia R i podzielnej grupy przemiennej D, $Hom_{\mathbb{Z}}(R, D)$ jest injektywnym R modułem.

Twierdzenie 41. *Każdy moduł M jest podmodułem modułu injektywnego. Zatem dla każdego modułu istnieje jego rezolwenta injektywna:*

$$0 \to M \to E_0 \to E_1 \to E_2 \to \dots,$$

gdzie E_i są injektywne.

4.3 Iloczyn tensorowy modułów

Kategorię prawych R modułów oznaczamy przez $\mathcal{M}od_R$ a lewych przez ${}_R\mathcal{M}od$.

Definicja 48. *Jeżeli M jest prawym R modułem, a N lewym R modułem zaś G grupą abelową, to funkcję $f : M \times N \to G$ nazywamy biaddytywną, jeżeli*

$$\begin{aligned} f(m + m', n) &= f(m, n) + f(m', n) \\ f(m, n + n') &= f(m, n) + f(m, n') \\ f(mr, n) &= f(m, rn) \end{aligned}$$

dla dowolnych $m \in M$, $n \in N$, $r \in R$.

Jeżeli R jest pierścieniem przemiennym, a K R-modułem, to funkcję biaddytywną $f : M \times N \to K$ nazywamy dwuliniową, jeżeli ponadto

$$f(mr, n) = f(m, rn) = rf(m, n)$$

dla dowolnych $m \in M$, $n \in N$, $r \in R$.

Przykłady: M, N prawe R – moduły, to $Hom_R(M, N)$ jest lewym R modułem i ewaluacja $e : M \times Hom_R(M, N) \to N$ jest biaddytywna.

Definicja 49. *Iloczynem tensorowym $N \in Mod_R$ i $M \in_R \mathcal{M}od$ nazywamy grupę abelową $M \otimes N$ wraz z biaddytywną funkcją $M \times N \to M \otimes N$. taką, że dla dowolnej biaddytywnej funkcji $f : M \times N \to G$ istnieje dokładnie jeden homomorfizm $\tilde{f} : M \otimes N \to G$, dla którego diagram*

$$\begin{array}{ccc} M \times N & \longrightarrow & M \otimes N \\ \downarrow{\scriptstyle f} & \swarrow_{\tilde{f}} & \\ G & & \end{array}$$

jest przemienny.

Twierdzenie 42. *Istnieje funktor $\otimes : \mathcal{M}od_R \times_R \mathcal{M}od \to \mathcal{A}b$, który jest iloczynem tensorowym. Ponadto jeżeli pierścień jest przemienny, to funktor ten przyjmuje wartości w kategorii R modułów.*

Stwierdzenie 26. *Przy ustaleniu jednej ze współrzędnych funktor iloczynu tensorowego jest addytywny.*

Definicja 50. *Grupę przemienną M nazywamy (R, S) bimodułem, jeżeli M jest lewym R modułem i prawym S modułem przy czym $(rm)s = r(ms)$ dla dowolnych m, r, s.*

Kategorię bimodułów oznaczamy ${}_R\mathcal{M}od_S$.

Lemat 10. *Jeżeli $N \in_S \mathcal{M}od_R$ i $M \in_R \mathcal{M}od$ to $N \otimes M$ jest lewym S modułem: $s(n \otimes m) = sn \otimes m$. Analogicznie dla $N \in \mathcal{M}od_R$ i $M \in_R \mathcal{M}od_S$ to $N \otimes M$ jest prawym S modułem*

Stwierdzenie 27. *Jeżeli R jest pierścieniem przemiennym, to*

$$M \otimes N \cong N \otimes M.$$

Przykład: Rozszerzanie skalarów. Jeżeli $S \leqslant R$ jest podpierścieniem, $M \in_S \mathcal{M}od$, to $R \otimes_S M \in_R \mathcal{M}od$.

Bardzo ważne twierdzenie o tym, że iloczyn tensorowy jest funktorem dołączonym do Hom.

Twierdzenie 43. *Dla $M \in \mathcal{M}od_R$, $N \in_R \mathcal{M}od_S$, $K \in \mathcal{M}od_S$ homomorfizm*

$$\tau_{M,N,K} : Hom_S(M \otimes N, K) \to Hom_R(M, Hom_S(N, K))$$

zadany wzorem

$$\tau_{M,N,K}(f) = f^*, f^*(m)(n) = f(m \otimes n)$$

definiuje naturalny izomorfizm funktorów.

Mówimy, że funktor iloczynu tensorowego jest lewo – dołączony do funktora Hom.

Twierdzenie 44. *Funktor mnożenia tensorowego przez ustalony moduł jest prawodokładny, tzn. dla modułu $M \in \mathcal{M}od_R$ dokładnego ciągu lewych R modułów*

$$N' \to N \to N'' \to 0$$

dokładny jest ciąg grup abelowych

$$M \oplus N' \to M \oplus N \to M \oplus N'' \to 0.$$

Analogiczne twierdzenie jest prawdziwe dla mnożenia przez lewy R moduł.

Dowód twierdzenia korzysta z lewodokładności funktora Hom i dołączenia, a także lematu:

Lemat 11. *Niech R będzie pierścieniem przemiennym, zaś $N' \to N \to N''$ ciągiem R modułów, takim że dla dowolnego R modułu M dokładny jest ciąg*

$$0 \to Hom(N'', M) \to Hom(N, M) \to Hom(N', M).$$

Wówczas ciąg

$$N' \to N \to N'' \to 0$$

jest dokładny.

Definicja 51. *Jeżeli funktor mnożenia tensorowego przez R moduł M jest dokładny, to mówimy, ze moduł M jest płaski.*

Stwierdzenie 28. *Każdy moduł projektywny jest płaski.*

4.4 Klasyfikacja skończenia generowanych modułów nad dziedzinami ideałów głównych

Niech R będzie pierścieniem przemiennym.

Definicja 52. *Niech M będzie R modułem i niech $x \in M$.*

$$ann(x) = \{r \in R \colon rx = 0\} \lhd R$$

Definicja 53. *Dla R modułu M niech*

$$tM = \{x \in M \colon ann(x) \neq 0\}.$$

Jeżeli R jest dziedzina całkowitości, to $tM \leqslant M$ jest podmodułem i nazywamy go ***podmodułem torsyjnym*** *modułu M.*

Stwierdzenie 29. *Jeżeli R jest dziedziną całkowitości, to przyporządkowanie $M \rightsquigarrow tM$ jest funktorem.*

Wynika z tego w szczególności, że jeżeli $M \cong M'$, to $tM \cong tM'$ i $M/tM \cong M/tM'$. **Od tej pory zakładamy, że M jest dziedziną całkowitości.**

Definicja 54. *Moduł nazywa torsyjny jeżeli $tM = M$ a beztorsyjny jeżeli $tM = 0$.*

Stwierdzenie 30. *Moduł M/tM jest beztorsyjny.*

Twierdzenie 45. *Jeżeli R jest DIG, a M jest skończenie generowanym R modułem to :*

a) jeżeli M jest beztorsyjny, to M jest wolny;

b) jeżeli M jest wolny i $N \leqslant M$ jest podmodułem, to N jest wolny i $\operatorname{rank} N \leq \operatorname{rank} M$*;*

c) jeżeli M jest projektywny, to M jest wolny;

d) $M = tM \oplus F$, gdzie F jest skończenie generowanym modułem wolnym;

e) jeżeli M' jest skończenie generowany, to $M \cong M'$ wtedy i tylko wtedy gdy $tM \cong tM'$ i $\operatorname{rank} M/tM \cong \operatorname{rank} M'/tM'$

Uwaga:stwierdzenia a), b), c) są prawdziwe także dla modułów niekoniecznie skończenie generowanych.(to nieobowiazkowe)

Wniosek 4. *Jeżeli R jest DIG, to M jest skończenie generowany R moduł jest płaski wtedy i tylko wtedy, gdy jest beztorsyjny.*

Uwaga: Tutaj także założenie skończonej generowalności można pominąć (to nieobowiazkowe)

Zajmiemy się klasyfikacją modułów torsyjnych. **Odtąd, do końca paragrafu zakładamy, że R jest DIG.**

Definicja 55. *Niech $I = (p) \triangleleft R$ będzie ideałem pierwszym. Jeżeli M jest R modułem, to podmoduł*

$$M_{(}p) = \{x \in M \colon \exists_{n \in \mathbb{N}}\, p^n x = 0\}$$

nazywa się (p) prymarnym składnikiem modułu M.

Twierdzenie 46. *Każdy moduł torsyjny jest sumą prostą modułów prymarnych.*

Dowód. Przedstawić generator d anihilatora dowolnego elementu $x \in M$ jako iloczyn potęg elementów pierwszych $d = p_1^{n_1} \dots p_k^{n_k}$. Zauważmy, że $r_i x \in M_{(p_i)}$, gdzie $r_i p_i^{n_i} = d$ oraz istnieją $s_i \in R$, takie że $\sum s_i r_i = 1$. Zatem $x = \sum s_i(r_i x) \in < \bigcup M_{(p)} >$. Wystarczy sprawdzić, że to jest suma prosta. □

Stwierdzenie 31. *Dla ideału pierwszego (p) przyporządkowanie $M \rightsquigarrow tM_{(p)}$ jest funktorem. Dwa moduły torsyjne M i M' są izomorficzne wtedy i tylko wtedy, gdy dla każdego ideału pierwszego (p), $M_{(p)} \cong M'_{(p)}$.*

W dalszym kroku moduł prymarny przedstawiamy jako sumę prostą modułów cyklicznych (tzn generowanych przez jeden element), po to by otrzymać:

Twierdzenie 47. *Jeżeli M jest skończenie generowanym modułem nad R DIG, to M jest sumą prostą modułów cyklicznych, przy czym każdy składnik cykliczny jest bądź izomorficzny z R, bądź jest prymarny.*

Dowód. Wystarczy rozłożyć na cykliczne moduł prymarny. Dowód przez indukcję ze względu na liczbę generatorów. Niech M, (p) prymarny, $M =< x_1, \dots, x_n >$, $p^{e_i} x_i = 0$. Załóżmy, że dla każdego i, $e_n \geq e_i$ i rozpatrzmy moduł cykliczny $< x_n >$. Mamy ciąg dokładny:

$$0 \to < x_n > \to M \to M/ < x_n > \to 0$$

i wystarczy pokazać, że jest rozszczepialny. W tym celu pokażemy, że $< x_n >$ jest R modułem injektywnym. Zauważmy, że cały ciąg możemy traktować jako ciąg $R/(p^{e_n})$ modułów. Wówczas z kryterium Baera $< x_n >$ jest $R/(p^{e_n})$ modułem injektywnym i ciąg rozszczepia się jako ciąg $R/(p^{e_n})$ modułów. Ale to rozszczepienie jest także rozszczepieniem R modułów. □

Cykliczne składniki modułu prymarnego nie są wyznaczone jednoznacznie, ale jednoznaczne są anihilatory tych składników. Jeżeli $(p) \triangleleft R$ jest ideałem pierwszym to dla dowolnego modułu M, moduł ilorazowy M/pM jest przestrzenią liniową nad ciałem $R/(p)$. Definiujemy:

$$d(M) = \dim(M/pM).$$

Definicja 56. *Dla modułu (p) prymarnego M niech*

$$U_{(p)}(n, M) = d(p^n M) - d(p^{n+1} M).$$

Twierdzenie 48. *Jeżeli $(p) \triangleleft R$ jest ideałem pierwszym, a M modułem (p) prymarnym, to każdy rozkład modułu M na sumę prostą modułów cyklicznych ma $U_{(p)}(n, M)$ składników o anihilatorze (p^{n+1}).*

Wniosek 5. *Jeżeli M i M' są (p) prymarnymi modułami, to są one izomrficzne wtedy i tylko wtedy gdy dl każdego $n \in \mathbb{N} \cup \{0\}$, $U_{(p)}(n, M) = U_{(p)}(n, M')$*

Definicja 57. *Jeżeli $(p) \lhd R$ jest ideałem pierwszym, a M modułem (p) prymarnym, to ideały (p^{n+1}) każdy liczony $U_{(p)}(n, M)$ razy nazywają się dzielnikami elementarnymi modułu M.*

Reasumując mamy twierdzenie klasyfikacyjne

Twierdzenie 49. *Jeżeli M, M' są skończenie generowanymi modułami nad DIG, to M i M' są izomorficzne wtedy i tylko wtedy gdy ich części wolne są tej samej rangi, zaś części torsyjne mają ten sam zestaw dzielników elementarnych.*

Można składniki proste pogrupować inaczej:

Twierdzenie 50. *Każdy skończenie generowany moduł M nad DIG można przedstawić w postaci sumy prostej*

$$M = R/(x_1) \oplus R/(x_2) \oplus \cdots \oplus R/(x_k)$$

gdzie

$$x_1|x_2|\ldots x_{k-1}|x_k.$$

Uwaga: W oznaczeniach z powyższego twierdzenia, $annM = (x_k)$.

Definicja 58. *Ideały $(x_1)\ldots(x_k)$ nazywają się niezmienniczymi dzielnikami modułu M.*

4.4.1 Zastosowanie do algebry liniowej

Jeżeli V jest skończenie wymiarową przestrzenią liniową nad ciałem k i dany jest endomorfizm $f : V \to V$, to V ma strukturę skończenie generowanego modułu nad pierścieniem wielomianów $k[X]$.

Rozkład V na sumę prostą $k[X]$ modułów cyklicznych wyznaczonych przez dzielniki niezmiennicze odpowiada przedstawieni V jako sumy prostej niezmienniczych podprzestrzeni cyklicznych. Rozkład na moduły cykliczne odpowiadające dzielnikom elementarnym (o ile wielomian charakterystyczny rozkłada się w ciele k na czynniki liniowe) odpowiada rozkładowi na klatki Jordana.

Ostatni dział poświęcony modułom nad pierścieniami nieprzemiennymi, ze szczególnym uwzględnieniem modułów nad pierścieniem grupowym $k[G]$, był już "rzutem na taśmę" i egzamin nie będzie go obejmował.