Spis treści

Rozdział 1

Grupy proste

1.1 Prostota grup A_n.

Udowodnimy twierdzenie:

Twierdzenie 1. *Grupa alternująca A_n jest prosta dla każdego $n \geq 5$.*

Dowód. Twierdzenie dowodzimy przez indukcję. Grupa A_5 jest prosta (skrypt). Załóżmy prawdziwość tezy dla $k < n$ i rozważmy naturalne działanie grupy A_n na zbiorze $\{1, 2, \ldots, n\}$. Zauważmy, że:

- działanie to jest tranzytywne, gdyż dla każdego $i \in \{2, 3, \ldots, n\}$ cykl $(1, i, j) \in A_n$;
- jeżeli $H_i \leqslant A_n$ jest grupą izotropii punktu i, to z tranzytywności wynika, że wszystkie te podgrupy są sprzężone i izomorficzne z $H_n = A_{n-1}$, a więc proste.

Niech $K \triangleleft A_n$. Wynika z tego, że $H_i \cap K \triangleleft H_i$, a zatem $H_i \cap K = H_i$ lub $H_i \cap K = \{1\}$. Mogą zajść dwa przypadki:

1) Istnieje i dla którego $H_i \cap K = H_i$;

2) dla każdego $1 \leq i \leq n$ $H_i \cap K = \{1\}$.

Pokażemy, że w pierwszym przypadku $K = A_n$ a w drugim, że $K = 1$.

Ad 1): Dla dowolnego j, istnieje $\sigma \in A_n$, $H_j = \sigma H_i \sigma^{-1} \leqslant \sigma K \sigma^{-1} = K$, a zatem $\langle H_1 \cup \cdots \cup H_n \rangle \leqslant K$. Niech $\tau \in A_n$. Jeżeli $\tau(1) = 1$, to $\tau \in H_1 \leqslant K$. Jeżeli $\tau(1) = j \neq 1$, to niech $k \neq j$ i $k \neq 1$. Ponieważ $n > 4$, to cykl $(j, 1, k) \in H_l$ dla pewnego l. Mamy $\tau = (k, 1, j)(j, 1, k)\tau$ oraz $(k, 1, j) \in H_l$ i $(j, 1, k)\tau \in H_1$, a więc $\tau \in K$.

Ad 2): Przypuśćmy, że istnieje $1 \neq \sigma \in K$. Z warunku 2) wynika, że dla każdego s, $\sigma(s) \neq s$. Niech $\sigma(1) = i \neq 1$. Niech j będzie takie, że $\sigma(j) \neq 1$, $j \neq i$. Niech $\sigma(j) = k$. Oczywiście $k \neq 1$, $k \neq i$, $k \neq j$. Ponieważ $n > 6$,

to istnieją jeszcze dwa elementy a, b różne od poprzednich. Rozpatrzmy permutację $\tau = (1i)(jkab)$ i sprzężenie $\tau\sigma\tau^{-1}$. Mamy $\tau\sigma\tau^{-1}(i) = 1$, więc $\tau\sigma\tau^{-1}\sigma(1) = 1$ i $\tau\sigma\tau^{-1}\sigma \in K \cap H_1$. Jednak $\tau\sigma\tau^{-1}\sigma \neq 1$, gdyż $\tau\sigma\tau^{-1}\sigma(j) = a$ i otrzymujemy sprzeczność. $\square$

Rozdział 2

Twierdzenie Sylowa - wnioski

2.1 Lemat Frattini

Zaczynamy od lematu, który pokazuje, że dla dowolnej skończonej podgrupy normalnej $N \trianglelefteq G$ można wskazać taką podgrupę, która wraz z N generuje G.

Lemat 1. (Frattini) *Niech G będzie dowolną grupą (niekoniecznie skończoną), $N \trianglelefteq G$ jej skończona podgrupą normalną, zaś $P \leqslant N$ pewną p – podgrupą Sylowa grupy N. Wówczas $G = N_G(P) \cdot N$.*

Dowód. Dla dowolnego elementu $g \in G$ podgrupa $gPg^{-1} \leqslant gNg^{-1} = N$ jest p – podgrupą Sylowa grupy N, a zatem istnieje $x \in N$, dla którego $xgPg^{-1}x^{-1} = P$. Oznacza to, że $xg \in N_G(P)$, czyli $g \in N_G(P) \cdot N$. □

Z powyższego lematu wynika użyteczny wniosek:

Wniosek 1. *Jeżeli $P \leqslant G$ jest podgrupą Sylowa i $N_G(P) \leqslant H$, to $H = N_G(H)$.*

Dowód. Zastosujmy lemat Frattini do $P \leqslant H \trianglelefteq N_G(H)$. Wynika z niego, że $N_G(H) = HN_G(P)$. Ale $HN_G(P) = H$ z założenia. □

2.2 Produkty półproste - istnienie przekroju

Wykorzystamy twierdzenie Sylowa do zbadania, kiedy normalna podgrupa $H \trianglelefteq G$ posiada dopełnienie, czyli kiedy grupa G jest produktem półprostym wewnętrznym.

2.3 Twierdzenie Schura – Zassenhausa

W tym rozdziale zajmiemy się bardzo użytecznym twierdzeniem, które podaje warunek dostateczny na to, by rozszerzenie

$$N \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } H$$

było produktem półprostym, co jak wiemy pozwala wiele powiedzieć o strukturze grupy G, jeśli znamy grupy H i N.

Twierdzenie 2. Schura – Zassenhausa *Jeżeli G jest grupa skończoną, $N \trianglelefteq G$ jej podgrupą normalną i $(|N|, [G\colon N]) = 1$, to podgrupa N ma dopełnienie w G.*

Dowód twierdzenia podamy za Rose [R] i poprzedzimy lematem, który jest szczególnym przypadkiem twierdzenia Schura – Zassenhausa.

Lemat 2. *Jeżeli G jest grupa skończoną, $A \trianglelefteq G$ jej przemienną podgrupą normalną i $(|A|, [G\colon A]) = 1$, to podgrupa A ma dopełnienie w G.*

Zaczniemy od udowodnienia twierdzenia Schura – Zassenhausa, przy założeniu prawdziwości lematu.

Dowód. Zauważmy, że wystarczy wskazać podgrupę rzędu $[G\colon N]$.

Zastosujemy indukcję ze względu na $|N| = m$. Jeżeli $m = 1$, to teza jest oczywista. Niech $P \leqslant N$ będzie pewną p – podgrupą Sylowa grupy N. Z lematu Frattini wynika, że

$$G = N_G(P) \cdot N,$$

a zatem

$$G/N \ = \ (N_G(P) \cdot N)/N \ \cong \ N_G(P)/(N \cap N_G(P)).$$

Mamy dwie możliwości: a) $N \cap N_G(P) \lneqq N$ i b) $N \cap N_G(P) = N$

a) $N \cap N_G(P) \lneqq N$:
Oczywiście $N \cap N_G(P) \trianglelefteq N_G(P)$ i $(|N \cap N_G(P)|, [N_G(P)\colon (N \cap N_G(P))]) = 1$. Z założenia indukcyjnego istnieje podgrupa $K \leqslant N_G(P)$, która jest dopełnieniem do $N \cap N_G(P)$ w $N_G(P)$. Wynika z tego, że $|K| = [N_G(P)\colon (N \cap N_G(P))] = [G\colon N]$, a zatem K jest także dopełnieniem do N w G.

b) $N \cap N_G(P) = N$:
Z równości $G = N_G(P) \cdot N$ wynika więc, że $G = N_G(P)$ i $P \trianglelefteq G$. Centrum $Z(P) \blacktriangleleft P$ jest podgrupą charakterystyczną, więc $Z(P) \trianglelefteq G$ i możemy rozpatrzeć $N/Z(P) \trianglelefteq G/Z(P)$. Zauważmy, że $N/Z(P) \trianglelefteq G/Z(P)$ spełnia założenia twierdzenia Schura – Zassenhausa i $|N/Z(P)| < |N|$, więc z założenia indukcyjnego istnieje $H \leqslant G/Z(P)$, które jest dopełnieniem podgrupy $N/Z(P)$ w $G/Z(P)$. Niech $H' = \pi^{-1}(H) \leqslant G$, gdzie

$\pi : G \to G/Z(P)$ jest rzutowaniem na grupę ilorazową. Mamy $Z(P) \trianglelefteq H'$ jest podgrupą przemienną i $[H' \colon Z(P)] = |H|$ jest względnie pierwszy z p, a więc i z $|Z(P)|$. Z lematu wynika więc, że istnieje podgrupa $K \leqslant H'$, która jest dopełnieniem $Z(P)$ w H'. Nietrudno sprawdzić,że K jest szukanym dopełnieniem N w G. □

Pozostaje nam udowodnić lemat.

Dowód. Oznaczmy przez n rząd grupy ilorazowej G/A. Rozpatrzmy rodzinę $\mathcal{T}$ wszystkich podzbiorów $X = \{x_1, \ldots, x_n\} \subset G$, dla których $x_1A, \ldots, x_nA$ są wszystkimi elementami grupy ilorazowej G/A. Na rodzinie $\mathcal{T}$ określamy działanie grupy G przez domnażanie z lewej strony, to znaczy $g(\{x_1, \ldots, x_n\}) = \{gx_1, \ldots, gx_n\}$ (jest oczywiste, że $g(X) \in \mathcal{T}$).

Dla zbiorów $X, Y \in \mathcal{T}$ definiujemy element grupy A będący ich "ilorazem" $X/Y = \prod_{i=1}^{n} x_i y_i^{-1}$, gdzie $x_iA = y_iA$. Zauważmy, że z przemienności grupy A wynika, że X/Y jest dobrze określone i nie zależy od kolejności mnożenia.

W rodzinie $\mathcal{T}$ wprowadzamy relację równoważności: $X \sim Y$ wtedy i tylko wtedy, gdy $X/Y = 1$. Łatwy rachunek przekonuje nas, że dla dowolnego elementu $g \in G$ jeżeli $X \sim Y$, to $gX \sim gY$. Wynika z tego, że grupa G działa na zbiorze klas abstrakcji $\mathcal{T}/\sim$. Pokażemy, że grupa izotropii dowolnego $[X] \in \mathcal{T}/\sim$ dla tego działania jest dopełnieniem podgrupy A w G.

W tym celu pokażemy, że działanie A na $\mathcal{T}/\sim$ będące ograniczeniem działania G ma:

✓ trywialne grupy izotropii,

✓ ✓ jedną orbitę.

Z tego, że A jest podgrupą normalną wynika, że dla każdego $a \in A$, $ax_iA = x_iA$ a zatem $a(X)/X = a^n$. Jeżeli $a([X]) = [X]$, to $a^n = 1$, co wobec $(|A|, n) = 1$ oznacza, że $a = 1$ i pierwsza własność jest udowodniona. Niech $[X], [Y] \in \mathcal{T}/\sim$ będą różnymi elementami i niech $X/Y = a$. Ponieważ $(|A|, n) = 1$, to istnieje element $b \in A$, taki że $b^n = a^{-1}$ ($a^{-1} = a^{k|A|+ln} = a^{ln}$ dla pewnych liczb całkowitych k, l). Zatem $b(X)/Y = b(X)/X \cdot X/Y = 1$ i $b([X]) = [Y]$.

Niech teraz $K \leqslant G$ będzie podgrupą izotropii elementu $[X] \in \mathcal{T}/\sim$. Z własności ✓ wynika, że $A \cap K = \{1\}$. Dla dowolnego $g \in G$, z własności ✓ ✓ wnioskujemy, że istnieje $a \in A$, dla którego $g([X]) = a([X])$, a zatem $a^{-1}g \in K$ i $g \in A \cdot K$. Zatem K jest dopełnieniem A w G. □

Rozważania przeprowadzone powyżej pozwalają udowodnić nie tylko istnienie dopełnienia, ale i jego jednoznaczność, z dokładnością do sprzężenia.

Stwierdzenie 1. *Jeżeli G jest grupą skończoną, $A \trianglelefteq G$ jej przemienną podgrupą normalną i $(|A|, [G\colon A]) = 1$, to każde dwa dopełnienia A w G są sprzężone.*

Dowód. Pozostajemy przy oznaczeniach z dowodu lematu. Jeżeli $L \leqslant G$ jest dopełnieniem A w G, to zbiór elementów L należy do $\mathcal{T}$ – jego obraz w $\mathcal{T}/\!\sim$ oznaczamy symbolem $[L]$. Grupa L jest oczywiście zawarta w grupie izotropii $[L]$ i z własności ✓ ✓ wnosimy, że istnieje element $x \in A$, taki że $xLx^{-1} \leqslant K$. Ponieważ $|L| = |K| = n$, to $xLx^{-1} = K$. □

Powstaje naturalne pytanie, czy w sytuacji ogólniejszej (bez założenia przemienności), ale przy założeniach twierdzenia Schura – Zassenhausa każde dwa dopełnienia do N w G są sprzężone. Okazuje się, że jest tak w istocie, ale dowód wymaga skorzystania ze wzmiankowanego już w rozdziale 5 bardzo trudnego twierdzenia Feita – Thompsona.

Rozdział 3

Grupy nilpotentne

Bardzo dobre własności p–grup skłaniają do wyodrębnienia klasy grup o podobnych własnościach. Odnotujmy jeszcze jedną własność p–grup.

Twierdzenie 3. *Jeżeli G jest p–grupą, to każda maksymalna podgrupa właściwa jest normalna i jest indeksu p.*

Dowód. Dowodzimy przez indukcję ze względu na rząd $|G|$. Niech $K \leqslant G$ będzie podgrupa maksymalną. Rozważmy $K \leqslant KZ(G) \leqslant G$. Z maksymalności K mamy $K = KZ(G)$ lub $KZ(G) = G$.

Jeżeli $K = KZ(G)$, to $Z(G) \leqslant K$ i $K/Z(G) \leqslant G/Z(G)$. Z nietrywialności centrum i założenia indukcyjnego mamy: $K/Z(G) \triangleleft G/Z(G)$ i $|G/Z(G) : K/Z(G)|$. Przechodząc do przeciwobrazu dostajemy tezę.

Jeżeli $KZ(G) = G$, to wobec $KZ(G) = N_G(K)$ wnioskujemy, że $K \triangleleft G$. Z maksymalności K, G/K nie może mieć nietrywialnych podgrup właściwych, więc $|G/K|$=p. □

Zauważmy, że zachodzi twierdzenie:

Twierdzenie 4. *Jeżeli każda maksymalna podgrupa grupy skończonej jest normalna, to każda podgrupa Sylowa jest normalna.*

Dowód. Niech $P \leqslant G$ będzie podgrupą Sylowa i rozważmy $P \leqslant N_G(P)$. Przypuśćmy, że $N_G(P)$ jest podgrupą właściwą. Niech $N_G(P) \leqslant K$, gdzie K jest podgrupą maksymalną. Z założenia $K \triangleleft G$, ale z wniosku z lematu Frattini wiemy, że $N_G(K) = K$, czyli $K = G$, co przeczy założeniu, że $N_G(P)$ jest podgrupą właściwą i $P \triangleleft G$. □

Skoro maksymalne podgrupy są istotne, to niech $\Phi(G)$ oznacza część wspólną wszystkich maksymalnych podgrup nietrywialnej grupy G. Jeżeli $G = \{1\}$, to przyjmujemy $\Phi(G) = \{1\}$. Grupa $\Phi(G)$ nazywa się podgrupą Frattini.

Zauważmy, że warunek iż każda maksymalna podgrupa jest normalna można wyrazić w terminach podgrupy Frattini.

Stwierdzenie 2. *Każda maksymalna podgrupa jest normalna wtedy i tylko wtedy, gdy* $[G,G] \leqslant \Phi(G)$.

Dowód. Jeżeli $K \triangleleft G$ jest maksymalna, to grupa ilorazowa nie ma właściwych podgrup, a więc jest izomorficzna z $\mathbb{Z}_p$. Wynika z tego, że $[G,G] \leqslant K$, a wobec dowolności K, $[G,G] \leqslant \Phi(G)$. Jeżeli zaś $[G,G] \leqslant \Phi(G)$ to dla maksymalnej podgrupy K, $[G,G] \leqslant K$ i $K/[G,G] \leqslant G/[G,G]$, więc $K/[G,G] \triangleleft G/[G,G]$ i $K \triangleleft G$. □

Przypomnijmy też istotne twierdzenie o istnieniu dla p–grup ciągu podgrup normalnych :

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

$$\{1\} = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_{m-1} \leqslant G_m = G,$$

taki że $G_i \triangleleft G$ i $|G_i| = p^i$.

Zauważmy, że w tym ciągu $G_{i+1}/G_i \leqslant Z(G/G_i)$ (homomorfizm $Z(G/G_i) \to Aut(G_{i+1}/G_i) \cong \mathbb{Z}_{p-1}$ jest trywialny). Cią podgrup z twierdzenia pozwala przedstawić grupę G jako kolejne rozszerzenia grupy cyklicznej $\mathbb{Z}_p$.

3.1 Ciągi. Twierdzenie Jordana Höldera.

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, $H_i \triangleleft H_{i+1}$.*

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

c) Ciąg nazywa się **właściwy** *jeżeli dla każdego i, $H_i \neq H_{i+1}$.*

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

e) Ciąg

$$J = K_0 \leqslant K_1 \leqslant \cdots \leqslant K_{n-1} \leqslant K_n = G$$

jest **zagęszczeniem** *ciągu*

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

jeżeli dla każdego i istnieje j, takie że $H_i = K_j$. Zagęszczenie jest właściwe, jeżeli istnieje j, takie że $K_j \neq H_i$ dla każdego i.

f) Właściwy ciąg subnormalny

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

nazywa się **ciągiem kompozycyjnym** *grupy G jeżeli nie zawiera właściwych zagęszczeń.*

Mamy oczywiste

Stwierdzenie 3. *Ciąg $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$ jest ciągiem kompozycyjnym wtedy i tylko wtedy, gdy jego ilorazy są grupami prostymi.*

Twierdzenie 5. *Każda grupa skończona ma ciąg kompozycyjny.*

Dowód. Przez indukcje ze względu na rząd. Dla grupy trywialnej teza jest oczywista. Jeżeli G jest grupą prostą, to $\{1\} \triangleleft G$ jest ciągiem kompozycyjnym. W przeciwnym przypadku istnieje właściwa nietrywialna podgrupa normalna $H \triangleleft G$ - możemy założyć, że H jest maksymalną normalną podgrupą i G/H jest grupą prostą. Z założenia indukcyjnego istnieje ciąg kompozycyjny dla H: $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = H$. Wówczas $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = H \leqslant H_{n+1} = G$ jest ciągiem kompozycyjnym dla grupy G. □

Twierdzenie nie jest prawdziwe dla grup nieskończonych, jak pokazuje przykład grupy $\mathbb{Z}$.

Przykład 1. *Ciąg kompozycyjny grupy nie jest wyznaczony jednoznacznie:*

a) Jeżeli $D_{12} = \langle \rho, \epsilon \rangle$ to ciągi

$$\{1\} \leqslant \langle \rho^2 \rangle \leqslant \langle \rho^2, \epsilon \rangle \leqslant D_{12},$$

$$\{1\} \leqslant \langle \rho^2 \rangle \leqslant \langle \rho \rangle \leqslant D_{12}$$

są różnymi ciągami kompozycyjnymi.

b) Dla grupy cyklicznej $\mathbb{Z}_{70}$ oba ciągi

$$\{1\} \leqslant \mathbb{Z}_2 \leqslant \mathbb{Z}_{10} \leqslant \mathbb{Z}_{70},$$

$$\{1\} \leqslant \mathbb{Z}_5 \leqslant \mathbb{Z}_{35} \leqslant \mathbb{Z}_{70}$$

są ciągami kompozycyjnymi.

W obu przykładach powyżej ciągi kompozycyjne, choć różne, są tej samej długości i mają te same ilorazy. Tak jest zawsze i mówi o tym twierdzenie Jordana Höldera. Sformułowanie poprzedzimy wygodną definicją.

Definicja 2. *Dwa ciągi subnormalne* $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$ *i* $\{1\} = K_0 \leqslant K_1 \leqslant \cdots \leqslant K_{m-1} \leqslant K_m = G$ *nazywamy równoważnymi jeżeli* $n = m$ *i ciągi ilorazów* $H_1, H_2/H_1, dots, G/H_{n-1}$ *i* $K_1, K_2/K_1, dots, G/K_{m-1}$ *różnią się tylko permutacją.*

Twierdzenie 6. Jordana-Höldera *Każde dwa właściwe ciągi kompozycyjne grupy są równoważne.*

Twierdzenie jest prawdziwe dla dowolnych grup i dowód można znaleźć w każdym podręczniku algebry. My podamy jego dowód dla grup skończonych, gdyż jest prostszy.

Dowód. Użyjemy indukcji ze względu na rząd grupy, Twierdzenie jest oczywiście prawdziwe dla grupy trywialnej.

Niech $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$ i $\{1\} = K_0 \leqslant K_1 \leqslant \cdots \leqslant K_{m-1} \leqslant K_m = G$ będą właściwymi ciągami kompozycyjnymi.
Jeżeli $H_{n-1} \cong K_{m-1}$, to teza wynika z założenia indukcyjnego.
Rozpatrzmy przypadek $H_{n-1} \neq K_{m-1}$. Zauważmy, że z założenia,że ciągi są kompozycyjne wynika, że $H_{n-1}K_{m-1} = G$. Rozważmy $H_{n-1} \cap K_{m-1}$ i zauważmy, że $H_{n-1}/H_{n-1} \cap K_{m-1} \cong G/K_{m-1}$ i $K_{m-1}/H_{n-1} \cap K_{m-1} \cong G/H_{n-1}$ są grupami prostymi. Niech $\{1\} = J_0 \leqslant J_1 \leqslant \cdots \leqslant J_k = H_{n-1} \cap K_{m-1}$ będzie ciągiem kompozycyjnym dla $H_{n-1} \cap K_{m-1}$. Mamy wówczas następujące ciągi kompozycyjne:

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

2) $\{1\} = J_0 \leqslant J_1 \leqslant \cdots \leqslant J_k = H_{n-1} \cap K_{m-1} \leqslant H_{n-1} \leqslant H_n = G$

3) $\{1\} = J_0 \leqslant J_1 \leqslant \cdots \leqslant J_k = H_{n-1} \cap K_{m-1} \leqslant K_{m-1} \leqslant K_m = G$

4) $\{1\} = K_0 \leqslant K_1 \leqslant \cdots \leqslant K_{m-1} \leqslant K_m = G$

Korzystając z założenia indukcyjnego i porównując ciągi 1) i 2) jako kompozycyjne dla H_{n-1} dostajemy $n-2 = k$ i ciągi ilorazów $H_1, H_2/H_1, \ldots, H_{n-1}/H_{n-2}$ oraz $J_1, J_2/J_1, \ldots, H_{n-1} \cap K_{m-1}/J_{n-3}, H_{n-1}/H_{n-1} \cap K_{m-1} \cong G/K_{m-1}$ różnią się permutacją.

Analogicznie porównując ciągi 3) i 4) jako kompozycyjne dla K_{m-1} dostajemy $m - 2 = k$ i ciągi ilorazów $K_1, K_2/K_1, \ldots, K_{m-1}/K_{m-2}$ oraz $J_1, J_2/J_1, \ldots, H_{n-1} \cap K_{m-1}/J_{n-3}, K_{m-1}/H_{n-1} \cap K_{m-1} \cong G/H_{n-1}$ różnią się permutacją.

Wynika już z tego, że ciągi kompozycyjne $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$ i $\{1\} = K_0 \leqslant K_1 \leqslant \cdots \leqslant K_{m-1} \leqslant K_m = G$ są równoważne.

□

3.2 Grupy nilpotentne.

Uogólnimy teraz własność ciągu kompozycyjnego dla p–grup.

Definicja 3. *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, $H_{i+1}/H_i \leqslant Z(G/H_i)$.

Lemat 3. *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 $0 \geq i \leq n-1$

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

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 grupy G.

Definicja 4. *Niech* G *będzie grupą,*

- *Niech* $\Gamma_1(G) = G$ *i niech* $\Gamma_n(G) = [G, \Gamma_{n-1}(G)]$ *dla każdego* $n > 1$. *Otrzymujemy* ***dolny ciąg centralny:***

$$G = \Gamma_1(G) \geqslant \Gamma_2(G) \geqslant \Gamma_3(G) \geqslant \ldots$$

- *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 4. *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 $i \geq 0$

$$\Gamma_{n-i+1}(G) \leqslant H_i \leqslant Z_i(G).$$

Jego dowód poprzedzimy lematem.

Lemat 4. *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 $L \triangleleft G$. Zatem $gklg^{-1} \in HL$, co dowodzi tezy. □

Dowód. stwierdzenia Stwierdzenie $H_i \leqslant Z_i(G)$ dowodzimy przez indukcję ze względu na i. Dla $i = 0$ jest ona oczywista. 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

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

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 $\Gamma_{j+1}(G) \leqslant H_{n-j}$. Jest to oczywiste dla $j = 0$ i załóżmy, że $\Gamma_j(G) \leqslant H_{n-j+1}$. Ciąg jest centralny więc z Lematu 3,

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

a więc

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

□

Wniosek 2. *Dla grupy G, n jest najmniejszą liczbą dla której $Z_n(G) = G$ wtedy i tylko wtedy, gdy n jest najmniejszą liczba dla której $\Gamma_{n+1}(G) = \{1\}$.*

Definicja 5. *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 7. *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 tego, że ciąg kompozycyjny dla skończonej p grupy jest centralny i z Stwierdzenia 4.

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

Ad c) Niech $H \triangleleft G$ 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 $\Gamma_i(G \times H) = \Gamma_i(G) \times \Gamma_i(H)$. $\square$

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, które nie są* 2 *grupami.*

3.3 Skończone grupy nilpotentne

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

Definicja 6. *Podgrupa $H \leqslant G$ nazywa się subnormalna w G, jeżeli istnieje ciąg subnormalny $H = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$*

Następne twierdzenie podaje warunki równoważne na to, by skończona grupa była nilpotentna.

Twierdzenie 8. *Dla skończonej grupy G następujące warunki są równoważne:*

1) G jest grupą nilpotentną;

2) Każda podgrupa grupy G jest subnormalna w G;

3) Jeżeli $H \leqslant G$ jest podgrupą właściwą, to $H \leqslant N_G(H)$ jest także podgrupą właściwą;

4) Każda podgrupa maksymalna jest normalna;

5) $[G.G] \leqslant \Phi(G)$, gdzie $\Phi(G)$ jest podgrupą Frattini;

6) Każda podgrupa Sylowa jest normalna w G;

7) G jest produktem grup, których rzędy są potęgami pewnych liczb pierwszych

Dowód. Równoważność warunków 4) i 5) została wykazana.
1) $\Rightarrow$ 2) Niech $H \leqslant G$. Niech $\{1\} = Z_0(G) \leqslant Z_1(G) \leqslant \cdots \leqslant Z_n(G) = G$, będzie górnym ciągiem centralnym. Wówczas mamy ciąg podgrup

$$H = Z_0(G) \leqslant HZ_1(G) \leqslant \cdots \leqslant HZ_n(G) = H.$$

Wystarczy pokazać, że $HZ_{i-1}(G) \triangleleft HZ_i(G)$. Centrum grupy jest zawarte w normalizatorze dowolnej podgrupy, więc

$$Z(G/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G) \leqslant N_{G/Z_{i-1}(G)}(HZ_{i-1}(G)/Z_{i-1}(G))$$

i

$$HZ_{i-1}(G)/Z_{i-1}(G) \triangleleft (HZ_{i-1}(G)/Z_{i-1}(G))(Z_i(G)/Z_{i-1}(G)) = HZ_i(G)/Z_{i-1}(G).$$

Przechodząc do przeciwobrazu homomorfizmu ilorazowego $HZ_{i-1}(G) \triangleleft HZ_i(G)$.

2) $\Rightarrow$ 3) Jeżeli $H \leqslant G$ jest podgrupą właściwą i $H = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$, to $n > 0$ i wówczas H jest właściwą podgrupą H_1. Ale $H \triangleleft H_1$, więc $H_1 \leqslant N_G(H)$.

3) $\Rightarrow$ 4) Niech H będzie podgrupą maksymalną. Z maksymalności $H = N_G(H)$ lub $N_G(H) = G$. Ten pierwszy przypadek wyklucza warunek 3), a więc $H \triangleleft G$

4) $\Rightarrow$ 6) Ta implikacja jest treścią Twierdzenia 5.

6) $\Rightarrow$ 7) Jeżeli każda podgrupa Sylowa jest normalna i wemy, ze dowolne dwie przecinają się wzdłuz podgrupy trywialnej i (np. ze względu na rzędy) generują całą grupę, to G jest produktem swoich podgrup Sylowa.

7) $\Rightarrow$ 1) Wynika z tego, że każda p grupa jest nilpotentna i tego, że produkt grup nilpotentnych jest nilpotentny. $\square$

Rozdział 4

Grupy nieskończone

Metody badania grup nieskończonych są odmienne od tych, które służą badaniu grup skończonych. Grupy nieskończone można podzielić na dwie klasy: "beznadziejnie nieskończone" i "residualnie skończone".

Definicja 7. *Grupa G nazywa się residualnie skończona wtedy i tylko wtedy, gdy istnieje rodzina $\{G_i\}_{i\in I}$ grup skończonych oraz epimomorfizmów $\varphi_i : G \to G_i$ dla której $\bigcap_{i\in I} \ker \varphi_i = \{1\}$.*

Równoważnie grupa G jest residualnie skończona wtedy i tylko wtedy, gdy część wspólna wszystkich podgrup normalnych skończonego indeksu (równoważnie wszystkich podgrup skończonego indeksu) jest trywialna. Takie grupy są podgrupami produktu grup skończonych.

Przykłady: Grupy skończone, grupy wolne, skończenie generowane grupy nilpotentne.

Obie klasy maja zupełnie inne właściwości. **Hipoteza Burnside'a** Niech G będzie skończenie generowaną grupą. Przypuśćmy, że istnieje $n \in \mathbb{N}$ takie, że dla każdego $g \in G$ $g^n = 1$. Czy wynika z tego, że $|G| < \infty$? Odpowiedź jest tak, dla $n = 2, 3, 4, 6$. Nie wiadomo dla $n = 5$. Ogólnie wiadomo, że nie (Novikov - przykład na 300 stron). Odpowiedź jest tak, dla grup residualnie skończonych. (Zelmanov - medal Fieldsa)

Rozdział 5

Teoria pierścieni

5.1 Pierścienie ułamków i lokalizacja

Definicja 8. *Pierścień R nazywamy lokalnym wtedy i tylko wtedy, gdy ma dokładnie jeden ideał maksymalny.*

Stwierdzenie 5. *Pierścień R jest lokalny wtedy i tylko wtedy, gdy zbiór elementów nieodwracalnych jest ideałem czyli wtedy i tylko wtedy, gdy suma dwóch elementów nieodwracalnych jest elementem nieodwracalnym.*

Przykład 2. Pierścień $k[[X]]$ szeregów formalnych nad ciałem k jest lokalny, a jego ideałem maksymalnym jest zbiór tych $\sum_{i=0}^{\infty} a_i X^i$, dla których $a_0 = 0$.

Przykład 3. Niech p będzie liczbą pierwszą. Niech $\mathbb{Z}_{(p)} =: \{\frac{a}{b}, p \nmid b\} \leqslant \mathbb{Q}$. Ideałem maksymalnym są te $\frac{a}{b}$, że $p \mid a$.

Przykład 4. Niech X będzie przestrzenią topologiczną, a $x_0 \in X$ punktem. Niech (V, f) oznacza parę - otwarte otoczenie V punktu x_0 i funkcje ciagłą $f : V \to \mathbb{R}$. W zbiorze par wprowadzamy relację:

$$(V, f) \sim (U, g) \iff f_{|U \cap V} = g_{|U \cap V}$$

- jej klasy abstrakcji nazywamy kiełkami w punkcie x_0. Pierścień kiełków (z oczywistymi działaniami) jest lokalny - ideałem maksymalnym są kiełki $[(V, f)]$ dla których $f(x_0) = 0$.

W przypadku pierścienia $\mathbb{Z}_{(p)}$ widać, że o tym, że jest on podpierścieniem $\mathbb{Q}$ decyduje fakt, że iloczyn dwóch liczb niepodzielnych przez p jest niepodzielny przez p. Można powiedzieć, że pierścień $\mathbb{Z}_{(p)}$ powstaje z pierścienia $\mathbb{Z}$ przez odwrócenie liczb niepodzielnych przez liczbę pierwszą p.

Definicja 9. *Niech R będzie pierścieniem. Podzbiór $S \subset R$ nazywamy systemem multyplikatywnym jeżeli $1 \in S$ oraz dla każdych dwóch elementów $x \in S$, $y \in S$ ich iloczyn $xy \in S$.*

Przykład 5. Niech $s \in R$, niech $S = \{1, s, s^2, \dots\}$ jest systemem multypliktywnym.

Przykład 6. Niech $I \triangleleft R$ będzie ideałem pierwszym. Wówczas $S = R \setminus I$ jest systemem multyplikatywnym.

Przykład 7. Niech $J \triangleleft R$ będzie dowolnym ideałem. Wówczas $S = \{1 + x \colon x \in J\}$ jest systemem multyplikatywnym.

Niech $S \subset R$ będzie systemem multyplikatywnym. W zbiorze $R \times S$ rozważmy relację:

$$(x, s) \sim (y, t) \iff \exists_{r \in S} \ r(xt - ys) = 0.$$

Relacja powyższa jest relacją równoważności, co jest to łatwym sprawdzeniem. Zauważmy przy tym, że jeżeli R posiada dzielniki zera, to relacja $(x, s) \sim (y, t) \iff (xt - ys) = 0$ relacją równoważności nie jest. Klasę abstrakcji elementu (x, t) oznaczamy symbolem $\frac{x}{t}$ a zbiór klas abstrakcji symbolem $S^{-1}R$. W zbiorze $S^{-1}R$ wprowadzamy działania:

$$\frac{x}{t} + \frac{y}{s} = \frac{xs + yt}{ts} \qquad \frac{x}{t}\frac{y}{s} = \frac{xy}{ts}.$$

Zauważmy, że działania te są dobrze zdefiniowane i wraz z elementem zerowym $\frac{0}{1}$ oraz jedynką $\frac{1}{1}$ spełniają aksjomaty pierścienia z 1.

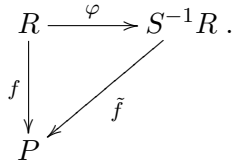
Definicja 10. *Pierścieniem ułamków pierścienia R względem systemu multyplikatywnego $S \subset R$ nazywamy zbiór $S^{-1}R$ z działaniami jak powyżej.*

Definicja 11. *Jeżeli R jest dziedziną całkowitości, to $S = R \setminus \{0\}$ jest systemem multyplikatywnym, Wówczas $S^{-1}R$ oznaczamy symbolem $Q(R)$ i nazywamy ciałem ułamków dziedziny R.*

Przykład 8. Niech k będzie ciałem. Ciało ułamków pierścienia wielomianów $k[X]$ nazywamy ciałem funkcji wymiernych i oznaczamy symbolem $k(X)$.

Zauważmy, że mamy naturalny homomorfizm $\varphi : R \to S^{-1}R$ zadany wzorem $\varphi(x) = \frac{x}{1}$. Homomorfizm ten i pierścień ułamków charakteryzuje następująca własność uniwersalna.

Twierdzenie 9. *Niech $f : R \to P$ będzie homomorfizmem pierścieni takim, że dla każdego $s \in S$ element $f(s) \in P$ jest odwracalny. Wówczas istnieje dokładnie jeden homomorfizm $\tilde{f} : S^{-1}R \to P$ dla którego przemienny jest diagram:*



Dowód. Jednoznaczność: Jeżeli diagram ma być przemienny, to $\tilde{f}(\frac{x}{1}) = f(x)$. Dla $s \in S$, $1 = \tilde{f}(1) = \tilde{f}(\frac{s}{1}\frac{1}{s}) = \tilde{f}(\frac{s}{1})\tilde{f}(\frac{1}{s}) = f(s)\tilde{f}(\frac{1}{s})$. Zatem $\tilde{f}(\frac{1}{s}) = f(s)^{-1}$ i wynika z tego, że $\tilde{f}(\frac{x}{s}) = \tilde{f}(\frac{1}{s})\tilde{f}(\frac{x}{1}) = f(x)f(s)^{-1}$.

Istnienie: Wystarczy sprawdzić, że wzór $\tilde{f}(\frac{x}{s}) = f(x)f(s)^{-1}$ jest dobrze zdefiniowany i jest szukanym homomorfizmem. □

Twierdzenie 10. *Niech $S \subset R$ będzie systemem multyplikatywnym, a $\varphi : R \to S^{-1}R$ kanonicznym homomorfizmem. Wówczas:*

a) dla każdego $s \in S$, $\varphi(s)$ jest elementem odwracalnym;

b) jeżeli $\varphi(x) = 0$ to istnieje $s \in S$ dla którego $xs = 0$;

c) każdy element pierścienia $S^{-1}R$ można zapisać w postaci $\varphi(x)\varphi^{-1}(s)$ dla pewnych $x \in R$ i $s \in S$.

Co więcej, jeżeli homomorfizm $f : R \to B$ spełnia warunki a), b), c), to istnieje izomorfizm $\tilde{f} : S^{-1}R \to B$, $\tilde{f} \circ \varphi = f$.

Dowód. a) $\varphi(s)^{-1} = \frac{1}{s}$

b) $\varphi(x) = 0$ oznacza, że $\frac{x}{1} = \frac{0}{1}$, czyli istnieje $s \in S$ dla którego $s(x1 - 01) = sx = 0$.

c) $\frac{x}{s} = \frac{x}{1}\frac{1}{s} = \varphi(x)\varphi(s)^{-1}$.

Jeżeli homomofizm $f : R \to B$ spełnia warunek a), to istnieje $\tilde{f} : S^{-1}R \to B$, $\tilde{f} \circ \varphi = f$. Warunek c) gwarantuje, że jest to epimorfizm, zaś warunek b), że monomorfizm. Jeżeli bowiem $\tilde{f}(\frac{x}{t}) = f(x)f(t)^{-1} = 0$, to $\tilde{f}(\frac{x}{t})f(t) = f(x) = 0$ czyli $sx = 0$ dla pewnego $s \in S$. Ale oznacza to, że $s(x1 - t0) = 0$, czyli $\frac{x}{t} = 0$ w $S^{-1}R$. □

Stwierdzenie 6. Niech $I \triangleleft R$ ideał pierwszy i niech $S = R \setminus I$. Wówczas pierścień ułamków $S^{-1}R$ jest pierścieniem lokalnym i nazywamy go lokalizacją pierścienia R w ideale pierwszym I.

Dowód. Zbiór $\{\frac{x}{s} : x \in I\}$ jest ideałem. Jest to jedyny ideał maksymalny, gdyż każdy element, który do niego nie należy jest odwracalny. □

Ideały w pierścieniach ułamków

Rozpatrzmy homomorfizm $\varphi : R \to S^{-1}R$.

Stwierdzenie 7. *Niech $J \triangleleft S^{-1}R$ będzie ideałem. Wówczas istnieje ideał $I \triangleleft R$, taki że $(\varphi(I)) = J$.*

Dowód. Niech $I = \varphi^{-1}(J)$. Jest jasne, że $(\varphi(I)) \subseteq J$. Niech $\frac{x}{s} \in J$. Wówczas $\frac{x}{s} = \frac{x}{1}\frac{1}{s} = \varphi(x)\frac{1}{s}$. Zatem $\frac{x}{s} \in (\varphi(I))$. □

Ideał $(\varphi(I)) \triangleleft S^{-1}R$ oznaczać będziemy symbolem $S^{-1}I$.

Zauważmy także, że ma miejsce następujący fakt.

Stwierdzenie 8. *Dla ideałów $I \triangleleft R$, $J \triangleleft R$*

$$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J.$$

Dowód. Zawieranie $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$ jest oczywiste. Niech $\frac{x}{s} = \frac{y}{t} \in S^{-1}I \cap S^{-1}J$, gdzie $x \in I$, $y \in J$, $s, t \in S$. Oznacza to, że dla pewnego $u \in S$, $utx = usy = z \in I \cap J$. Ale $\frac{x}{s} = \frac{z}{uts} \in S^{-1}(I \cap J)$. □

5.2 Pierścienie noetherowskie

Zauważmy, że ma miejsce następujący fakt z teorii mnogości.

Definicja 12. *Niech X będzie zbiorem częściowo uporządkowanym. Powiemy, że X ma własność ACC (ascending chain condition, czyli warunek wstępującego łańcucha) jeżeli dla każdego łańcucha*

$$a_1 \leqslant a_2 \leqslant \dots a_k \leqslant \dots$$

istnieje n, takie że $a_n = a_{n+1} = a_{n+2} = \dots$.

Warunek ten jest równoważny następującemu:

W każdym niepustym podzbiorze $\emptyset \neq A \subseteq X$ istnieje element maksymalny.

Wyróżnimy teraz klasę pierścieni, która spełnia ważny i wygodny dla dowodzenia twierdzeń warunek skończoności.

Stwierdzenie 9. *Niech R będzie pierścieniem. Następujące warunki są równoważne:*

a) zbiór ideałów pierścienia R uporządkowany przez inkluzje spełnia ACC, to znaczy dla każdego ciągu ideałów

$$I_1 \subseteq I_2 \subseteq \dots I_k \subseteq \dots$$

istnieje n, takie że $I_n = I_{n+1} = I_{n+2} = \dots$;

b) każdy niepusty zbiór ideałów ma element maksymalny;

c) każdy ideał jest skończenie generowany.

Jeżeli pierścień R spełnia wymienione wyżej warunki, to nazywamy go ***pierścieniem noetherowskim****.*

Dowód. Wiemy, że $a) \Leftrightarrow b)$.

$c) \Rightarrow a)$ Niech $I_1 \subseteq I_2 \subseteq \dots I_k \subseteq \dots$ będzie wstępującym ciągiem ideałów. Niech $I = \bigcup I_k \triangleleft R$. Ideał ten jest skończenie generowany $I = (x_1, \dots, x_k)$. Istnieje $n \in \mathbb{N}$, dla którego $\{x_1, \dots, x_k\} \subset I_n$. Oczywiście poczawszy od tego n łańcuch się stabilizuje.

$b) \Rightarrow c)$ Niech $I \lhd R$. Niech A będzie zbiorem skończenie generowanych ideałów R zawartych w I. Jest on niepusty, bo zawiera ideał zerowy, zatem zawiera element maksymalny J. Jeżeli $J \neq I$, to istnieje $x \in I \setminus J$. Wówczas $J \nsubseteq (J, x) \subseteq I$, co przeczy maksymalności J. Zatem $J = I$ i I jest skończenie generwany. □

Stwierdzenie 10. *Jeżeli R jest pierścieniem noetherowskim, a $I \lhd R$ ideałem, to pierścień ilorazowy R/I jest także pierścieniem noetherowskim.*

Dowód jest oczywisty (warunek ACC dla R/I jest spełniony).

Stwierdzenie 11. *Jeżeli R jest dziedziną noetherowską w której każdy element nierozkładalny jest pierwszy, to R jest dziedziną z jednoznacznością rozkładu.*

Dowód. Z twierdzenia w skrypcie wynika, że dziedzina w której elementy nierozkładalne są pierwsze i dla której spełniony jest warunek ACC dla ideałów głównych jest DJR. W dziedzinie noetherowskiej ten warunek oczywiście jest spełniony. □

Wiele jest przykładów pierścieni noetherowskich. Ich klasę powiększa twierdzenie Hilberta o bazie.

Twierdzenie 11. Hilberta o bazie *Jeżeli R jest pierścieniem noetherowskim, to pierścień wielomianów $R[X]$ jest także pierścieniem noetherowskim.*

Dowód. Pokażemy, że każdy ideał $I \lhd R[X]$ jest skończenie generowany. Niech

$$J_n = \{a \in R : \exists_{f \in I}\ f = a_0 + a_1 X + \cdots + aX^n\}.$$

Ponieważ $I \lhd R[X]$, to $J_n \lhd R$ oraz mamy wstępujacy ciąg ideałów:

$$J_0 \subseteq J_1 \subseteq \ldots J_k \subseteq \ldots.$$

Ciąg ten z założenia stabilizuje się i niech $J_n = J_{n+1} = \ldots$. Ideały są skończenie generowane, $J_k = (\{a_1^k, \ldots a_{i_k}^k\})$, $k \leq n$ i niech $\{f_1^k, \ldots f_{i_k}^k\}$ będą wielomianami z ideału I stopnia k o współczynnikach wiodących $a_1^k, \ldots a_{i_k}^k$ odpowiednio.

Niech $K \lhd R$, będzie ideałem generowanym przez zbiór wielomianów $\{f_i^k\}_{0 \leq k \leq n, 1 \leq i \leq i_k}$. Pokażemy, że $K = I$.
W tym celu wystarczy dla dowolnego wielomianu $f \in I$ wskazać wielomian $g \in K$ dla którego $deg(f - g) < degf$, bo dzięki indukcji dowodzi to tezy.
Niech $f = a_0 + \ldots a_s X^s$. Wówczas $a_s \in J_s$ i mamy dwa przypadki: $1) s \leq n$ i $2)$ $s > n$. W tym pierwszym przypadku $a_s = \sum_{i=1}^{i_s} x_i a_i^s$ dla pewnych $x_i \in R$. Wówczas dla $g = \sum_{i=1}^{i_s} x_i f_i^s$, $\deg(f - g) < s$. W drugim przypadku korzystamy z faktu, że $I_s = I_n$ i mamy $a_s = \sum_{i=1}^{i_n} x_i a_i^n$ oraz dla $g = \sum_{i=1}^{i_n} x_i f_i^n X^{s-n}$ mamy $\deg(f - g) < s$. □

Wniosek 3. *Jeżeli R jest pierścieniem noetherowskim, to pierścień wielomianów $R[X_1, X_2, \ldots, X_n]$ jest także pierścieniem noetherowskim.*