1 Seria I do oddania 18 października

Imię i Nazwisko :

1.1. Pokazać, że w grupie skończonej liczba elementów rzędu dwa wynosi 0 lub jest liczbą nieparzystą.

Dowód. Rząd grupy jest liczbą parzystą, bo rząd elementu dzieli rząd grupy. Elementów nietrywialnych rzędu nieparzystego jest parzyście wiele, bo każdy występuje w parze ze swoją odwrotnością. Zatem razem z elementem trywialnym elementów rzędu różnego od dwóch jest nieparzysta liczba. □

1.2. Czy istnieje grupa, w której elementów rzędu 12 jest dokładnie 10?

Dowód. Nie, liczba elementów rzędu 12 jest wielokrotnością $\varphi(12) = 4$ □

1.3. Niech grupa G będzie generowana przez zbiór X. Niech $f, g : G \to H$ będą homomorfizmami takimi, że dla każdego $x \in X$, $f(x) = g(x)$. Pokazać, że $f = g$.

Dowód. Zbiór $A = \{y \in G\colon f(y) = g(y)\}$ jest podgrupą zawierającą zbiór X. Zatem $G = \langle X \rangle \leqslant A$. □

1.4. Czy istnieje monomorfizm $Q_8 \to \Sigma_4$?

Dowód. Nie. W obu grupach jest po sześć elementów rzędu cztery, a rząd elementu jest zachowywany przez monomorfizm. Ale w Q_8 kwadratem każdego elementu jest -1, a kwadraty elementów rzędu cztery w Σ_4 są różne. □

Inny elegantszy (moim zdaniem) argument podany przez pana Karola Janowicza:

Dowód. Istnienie monomorfizmu $\varphi : Q_8 \to \Sigma_4$ oznacza istnienie wiernego działania Q_8 na zbiorze czteroelementowym. Orbity są najwyżej czteroelementowe, więc grupa izotropii każdego punktu jest nietrywialna. Każda nietrywialna podgrupa Q_8 zawiera podgrupę $\{1, -1\}$, zatem część wspólna grup izotropii wszystkich punktów też zawiera podgrupę $\{1, -1\}$. Ale to jest $\ker \varphi$ - sprzeczność z założeniem wierności działania. □

1.5. W grupie permutacji Σ_4 niech $H = \langle\, (123)\, \rangle \leqslant \Sigma_4$. Wypisać wszystkie elementy warstwy $(34)H$.

Dowód. $(34)H = \{(34), (1243), (1432)\}$ □

1.6. Niech $SO(n) \leqslant O(n)$ będzie podgrupą. Jaka jest moc zbioru warstw lewostronnych podgrupy $SO(n)$ w grupie $O(n)$?

Dowód. Homomorfizm $det : O(n) \to \{1, -1\} \simeq \mathbb{Z}_2$ jest epimorfizmem o jądrze $SO(n)$. Zatem $|O(n) : SO(n)| = |\mathbb{Z}_2 : \{1\}| = 2$. Jedną warstwą jest $SO(n)$ a drugą $O(n) \setminus SO(n)$ składająca się z przekształceń ortogonalnych zmieniających orientację. □

1.7. Czy w grupie $O(3)$ można wskazać symetrię względem pewnej prostej i symetrię względem pewnej płaszczyzny, które należą do tej samej warstwy lewostronnej $O(3)$ względem podgrupy $SO(3)$?

Dowód. Nie. Każda symetria względem prostej należy do $SO(n)$, zaś ta względem dowolnej płaszczyzny do warstwy $O(n) \setminus SO(n)$. □

1.8. Niech H_1, H_2 będą podgrupami grupy $D_{16} = \{1, \rho, \rho^2 \dots \rho^7, \epsilon, \epsilon\rho, \dots, \epsilon\rho^7\}$ izometrii ośmiokąta foremnego. Niech $H_1 = \{1, \epsilon\rho\}$ zaś $H_2 = \{1, \epsilon\rho^2\}$. Rozpatrujemy działanie D_{16} na zbiorach warstw D_{16}/H_1 i D_{16}/H_2 przez mnożenie z lewej strony. Czy D_{16} zbiory D_{16}/H_1 i D_{16}/H_2 są ekwiwariantnie izomorficzne?

Dowód. Trzeba zbadać, czy podgrupy H_1 i H_2 są sprzężone w D_{16}. Nie są, bo elementy $\epsilon\rho$ i $\epsilon\rho^2$ nie są sprzężone. □

2 Seria II do oddania 25 października

Imię i Nazwisko :

2.1. Czy grupy $\mathbb{Z}_8 \times \mathbb{Z}_{25}$ i $\mathbb{Z}_{200}$ są izomorficzne?

Dowód. Tak, bo 8 i 25 są względnie pierwsze. □

2.2. Niech $H \leqslant G$ będzie podgrupą, zaś $x, y \in G$ takimi elementami, że $xH = Hy$. Czy wynika z tego, że $xH = Hx$?

Dowód. Tak. Z równości wynika, że $x \in Hy$ czyli $Hx = Hy = xH$. □

2.3. Czy istnieje działanie grupy rzędu 55 na zbiorze 27 elementowym z dokładnie trzema orbitami?

Dowód. Z tw. Cauchyego wynika, ze w grupie rzędu 55 istnieją podgrupy indeksu 5 (czyli rzędu 11) i indeksu 11 (czyli rzędu 5). $27 = 11 + 11 + 5$ więc istnieje działanie o dwóch orbitach 11 elementowych i jednej 5 elementowej. □

2.4. Czy grupa przemienna rzędu 231 jest cykliczna?

Dowód. $231 = 3 \cdot 7 \cdot 11$. Z twierdzenia Cauchyego istnieją elementy $x, y, z \in G$ o rzędach równych $3, 7, 11$ odpowiednio. Podgrupa generowana przez $< x, y > \cong \mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$. Niech $o(w) = 21$. Analogicznie podgrupa $< w, z > \cong \mathbb{Z}_{231} = G$. □

2.5. Niech H_1 i H_2 będą podgrupami rzędu 7 w grupie Σ_{11}. Czy Σ_{11} zbiory Σ_{11}/H_1 i Σ_{11}/H_2 są ekwiwariantnie izomorficzne?

Dowód. Tak, bo podgrupa rzędu 7 jest cykliczna, a jedyne elementy rzędu 7 w $\mathbb{Z}_{11}$ mają rozkład postaci (• • • • • • •) a więc dowolne dwie podgrupy rzędu 7 są sprzężone. □

2.6. Niech H_1 i H_2 będą podgrupami rzędu 7 w grupie Σ_{14}. Czy Σ_{14} zbiory Σ_{14}/H_1 i Σ_{14}/H_2 są ekwiwariantnie izomorficzne?

Dowód. Nie. Podgrupy cykliczne generowane przez elementy o rozkładzie (• • • • • • •) i (• • • • • • •)(• • • • • • •) nie są sprzężone. □

2.7. Niech G będzie grupą skończoną, która działa na zbiorze X. Załóżmy, że dla $x, y \in G$, zbiór $\{g \in G \colon g(x) = y\}$ jest niepusty. Pokazać, że jego moc jest dzielnikiem rzędu grupy G.

Dowód. Niech $g_0 \in \{g \in G \colon g(x) = y\}$. Wystarczy zauważyć, że $\{g \in G \colon g(x) = y\} = g_0 G_x$. □

2.8. (J.Okniński) Udowodnić, że jeżeli G jest grupą rzędu 10 i G ma dokładnie jeden element rzędu 2, to G jest grupą cykliczną.

Dowód. Niech $o(x) = 2$, zaś $o(y) = 5$. Mamy $o(yxy^{-1}) = 2$ a zatem $yxy^{-1} = y$. Z przemienności i faktu, że rzędy są względnie pierwsze wynika iż $< x, y > \cong \mathbb{Z}_{10}$. □

3 Seria III do oddania 31 października

3.1. Podać przykład takich podgrup $K \trianglelefteq H$ i $H \trianglelefteq G$, że $K \ntrianglelefteq G$.

Dowód. Niech $G = \Sigma_4$, $H = \{1, (14)(23), (12)(34), (13)(24)\} \trianglelefteq \Sigma_4$, $K = \{1, (12)(34)\} \trianglelefteq H$, bo K jest przemienna. Oczywiście $K \ntrianglelefteq G$, bo $(123)(12)(34)(321) = (14)(23)$.

Takich przykładów jest bardzo wiele. Tak wiele, że interesujące są warunki, w których implikacja ma miejsce. Jeden, to $K \blacktriangleleft H$, inny to na przykład $K \trianglelefteq Z(G)$. □

3.2. Udowodnić, że jeżeli $K \trianglelefteq G$ to $Z(K) \trianglelefteq G$.

Dowód. Wynika to z faktu, że $Z(K) \blacktriangleleft K$ i stwierdzenia z wykładu. □

3.3. Udowodnić, że grupa $GL(2, \mathbb{Z}_3)/Z(GL(2, \mathbb{Z}_3))$ jest izomorficzna z grupą Σ_4.

Dowód. W przestrzeni liniowej $\mathbb{Z}_3^2$ są cztery podprzestrzenie jednowymiarowe. Oczywiście grupa $GL(2, \mathbb{Z}_3)$ działa na zbiorze podprzestrzeni jednowymiarowych. Mamy więc homomorfizm $\varphi : GL(2, \mathbb{Z}_3) \to \Sigma_4$. Wystarczy pokazać, że jądrem tego homomorfizmu jest $Z(GL(2, \mathbb{Z}_3))$, czyli jednokładności. Niech α_1, α_2 będzie bazą $\mathbb{Z}_3^2$. Jeżeli przekształcenie liniowe zachowuje $\text{lin}\{\alpha_1\}$ i $\text{lin}\{\alpha_2\}$, to macierz tego przekształcenia w bazie $\text{lin}\{\alpha_1\}$ i $\text{lin}\{\alpha_2\}$ jest diagonalna o wyrazach a, b na przekątnej. Z tego, że zachowane jest $\text{lin}\{\alpha_1 + \alpha_2\}$ wynika, że $a = b$, czyli przekształcenie należy do $Z(GL(2, \mathbb{Z}_3))$. Zawieranie $Z(GL(2, \mathbb{Z}_3)) \leqslant \ker \varphi$ jest oczywiste. Teza wynika z twierdzenia o izomorfizmie. □

3.4. (J.Okniński) Wykazać, że grupa $\mathbb{Q}/\mathbb{Z}$ jest izomorficzna z grupą F wszystkich pierwiastków zespolonych z 1 (wszystkich możliwych stopni) względem działania mnożenia. Tutaj $\mathbb{Z}$ i $\mathbb{Q}$ są rozpatrywane jako grupy względem działania dodawania.

Dowód. Rozważmy homomorfizm $\exp_{|_{\mathbb{Q}}} : \mathbb{Q} \to S^1$, $\exp(q) = (\cos(2\pi q), \sin(2\pi q))$. Oczywiście $\ker \exp_{|_{\mathbb{Q}}} = \mathbb{Z}$. Liczba $(\cos(2\pi q), \sin(2\pi q))$ jest pierwiastkiem stopnia n z 1 jeśli $q = \frac{m}{n}$ i każdy pierwiastek stopnia n z 1 leży w obrazie $\text{im}(\exp_{|_{\mathbb{Q}}})$. Teza wynika z twierdzenia o izomorfizmie. □

3.5. (J.Okniński) Niech $|G| = 20$ oraz niech $H \trianglelefteq G$ będzie podgrupą normalną rzędu 4. Pokazać, że G jest grupą abelową.

Dowód. Niech $x \in G$ będzie elementem rzędu 5, którego istnienie jest zagwarantowane przez tw. Cauchy'ego. Podrupa H rzędu 4 jest izomorficzna z $\mathbb{Z}_4$ lub z $\mathbb{Z}_2 \times \mathbb{Z}_2$. W pierwszym przypadku $\text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, w drugim $|\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 6$. Ponieważ $H \trianglelefteq G$, to mamy działanie $< x >$ na H przez automorfizmy wewnętrzne, czyli homomorfizm $\mathbb{Z}_5 \cong < x > \to \text{Aut}(H)$. Ponieważ w obu przypadkach $(5, |\text{Aut}(H)|) = 1$, to homomorfizm ten jest trywialny. Oznacza to, że element x jest przemienny z elementami H. Oczywiście $< x \cup H >= G$, więc G jest przemienna. □

3.6. Niech $H \leqslant \Sigma_n$, $n > 1$. Udowodnić, że jeżeli H zawiera permutację nieparzystą, to H zawiera podgrupę indeksu 2.

Dowód. Niech $i : H \to \Sigma_n$ będzie włożeniem. Rozważmy homomorfizm będący złożeniem $H \to \Sigma_n \to \Sigma_n/A_n \cong \mathbb{Z}_2$. Homomorfizm ten jest epimorfizmem, gdyż H zawiera permutację nieparzystą. Jądro tego epimorfizmu jest szukaną podgrupą indeksu 2. □

3.7. Niech $H_1 \trianglelefteq G$ i $H_2 \trianglelefteq G$ będą podgrupami normalnymi takimi, że $H_1 \cap H_2 = \{1\}$ oraz grupy ilorazowe G/H_1 i G/H_2 są przemienne. Pokazać, że grupa G jest przemienna.

Dowód. Rozpatrzmy homomorfizm: $\pi_{H_1} \times \pi_{H_2} : G \to G/H_1 \times G/H_2$. Jądro $\ker(\pi_{H_1} \times \pi_{H_2}) = H_1 \cap H_2 = \{1\}$, więc G jest izomorficzne z podgrupą przemiennej grupy $G/H_1 \times G/H_2$, zatem jest przemienne. □

3.8. Pokazać, że jeżeli G jest grupą skończoną i $[G : [G, G]] = 10$ to istnieje podgrupa $K \leqslant G$ izomorficzna z $\mathbb{Z}_{10}$.

Dowód. Grupa przemienna rzędu 10 jest cykliczna. Istnieje element $x \in G$, taki że $o(\pi_{ab}(x)) = 10$, gdzie $\pi_{ab} : G \to G/[G, G]$ jest epimorfizmem abelianizacji. Zatem $10 \| o(x)$. W grupie cyklicznej $< x >$, której rząd jest podzielny przez 10 istnieje podgrupa rzędu 10, która jest cykliczna. Istnieje więc element rzędu 10. □

3.9. Niech $\Phi : G \to Aut(G)$ będzie działaniem przez automorfizmy wewnętrzne. Niech $\Re$ będzie zbiorem podgrup grupy G i rozpatrzmy na nim działanie grupy G wyznaczone przez Φ. Wówczas:

a) Podgrupa $H \in \Re$ jest punktem stałym rozpatrywanego działania wtedy i tylko wtedy, gdy $H \trianglelefteq G$.

Dowód. Wprost z definicji: $\forall_{g \in G} gHg^{-1} = H \iff H \trianglelefteq G$. □

b) Grupą izotropii podgrupy $H \in \Re$ jest jej normalizator

$$N_G(H) = \{g \in G \colon gHg^{-1} = H\} \leqslant G.$$

Dowód. Jak powyżej z definicji. □

c) Liczba podgrup G sprzężonych z H, czyli moc orbity H, jest równa indeksowi $[G : N_G(H)]$ i dzieli indeks $|G : H|$.

Dowód. Z twierdzenia Lagrange'a $|G| = [G : H]|H| = [G : N_G(H)]|N_G(H)| = [G : N_G(H)]|N_G(H) : H||H|$, zatem $[G : H] = [G : N_G(H)]|N_G(H) : H|$ □

d) (J.Okniński) Jeżeli $|G| = p^k$ (dla pewnej liczby pierwszej p), to liczba podgrup G, nie będących podgrupami normalnymi w G jest podzielna przez p.

Dowód. Jeśli podgrupa H nie jest normalna, to $N_G(H)$ jest właściwą podgrupą jej orbita ma $[G : N_G(H)]$ elementów, co jest liczbą podzielną przez p. Zbiór podgrup nie będących normalnymi jest sumą mnogościową niejednoelementowych orbit. □

4 Seria IV do oddania 8 listopada

Imię i Nazwisko :

4.1. (J.Okniński) Czy istnieje tranzytywne (tzn. posiadające jedną orbitę) działanie grupy $\Sigma_4 \times A_5$ na zbiorze 144 elementowym?

Dowód. Rząd $|\Sigma_4 \times A_5| = 24 \cdot 60 = 144 \cdot 10$. Wystarczy więc w $\Sigma_4 \times A_5$ wskazać podgrupę rzędu 10 i zbiór warstw względem niej z działaniem mnożenia z lewej strony jest szukanym $\Sigma_4 \times A_5$ zbiorem. Taką podgrupą jest $< \sigma > \times < \tau >$, gdzie $\sigma \in \Sigma_4$ jest dowolną permutacją rzędu 2 (są dwie klasy sprzężoności takich podgrup), zaś τ jest cyklem długości 5. □

4.2. (J.Okniński) Znaleźć grupę ilorazową $Q_8/\{1, -1\}$.

Dowód. $Q_8/\{1, -1\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, gdyż grupa ilorazowa jest rzędu 4, a każdy jej nietrywialny element jest rzędu 2. □

4.3. (J.Okniński) Czy każde dwa elementy grupy Σ_{12} rzędu 21 są sprzężone?

Dowód. Element rzędu 21 w rozkładzie na cykle rozłączne musi składać się z cykli długości 7 i cykli długości 3. Jedyna możliwość to jeden cykl długości 7 i jeden długości 3 - zatem wszystkie są sprzężone. □

4.4. (J.Okniński) Wskazać element maksymalnego rzędu w grupie Σ_6.

Dowód. Rozpatrując wszystkie możliwe rozkłady na cykle najwyższy rząd to 6 i jest to albo cykl długości 6 albo cykl o rozkladzie $2 + 3$. □

4.5. (J.Okniński) Znaleźć wszystkie homomorfizmy $\Sigma_3 \to \mathbb{Z}_2 \times \mathbb{Z}_6$.

Dowód. Przeciwdziedzina jest grupą abelową, więc każdy homomorfizm jest złożeniem $\Sigma_3 \to \Sigma_3/[\Sigma_3, \Sigma_3] \to \mathbb{Z}_2 \times \mathbb{Z}_6$. Mamy $[\Sigma_3, \Sigma_3] =< (1, 2, 3) >$ i $\Sigma_3/[\Sigma_3, \Sigma_3] \cong \mathbb{Z}_2$. Homomorfizmów $\mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_6$ są 4 – trywialne i trzy przeprowadzające generator $\mathbb{Z}_2$ na jeden z trzech elementów rzędu 2 w $\mathbb{Z}_2 \times \mathbb{Z}_6$. □

4.6. (J.Okniński) Wyznaczyć klasę sprzężoności w grupie Σ_n i w grupie A_n permutacji σ jeżeli $\sigma = (1, 2, 3, 4, 5) \in A_5$ oraz jeżeli $\sigma = (1, 2)(3, 4) \in A_4$.

Dowód. Klasa sprzężoności $\sigma = (1, 2, 3, 4, 5)$ w A_5 ma 12 elementów, zaś klasa sprzężoności $(1, 2)(3, 4)$ w A_4 ma tyle samo elementów co w Σ_4 czyli 3. □

4.7. Czy istnieje grupa G, w której elementów rzędu 7 jest dokładnie 30?

Dowód. Taka grupa nie istnieje. Miałaby ona dokładnie 5 podgrup rzędu 7 - K_1, K_2, K_3, K_4, K_5. Rozpatrując działanie jednej z nich, np. K_1 na zbiorze $\{K_1, K_2, K_3, K_4, K_5\}$ indukowane przez działanie przez automorfizmy wewnętrzne, widzimy, że jedyne możliwe to działanie trywialne, bo orbity mogą być 1 lub 7 elementowe . Mamy więc homomorfizm $K_1 \to \mathrm{Aut}(K_2) \cong \mathbb{Z}_6$. Ze względu na rzędy homomorfizm ten musi być trywialny, czyli $\langle K_1 \cup K_2 \rangle \cong \mathbb{Z}_7 \times \mathbb{Z}_7$, a ta podgrupa ma już 48 elementów rzędu 7. □

4.8. Niech $k(G)$ oznacza liczbę klas sprzężoności elementów grupy G. Udowodnić, że jeżeli G jest skończoną grupą nieprzemienną to $k(G) > |Z(G)| + 1$.

Dowód. Jeżeli $k(G) = |Z(G)| + 1$, to

$$|G : C_G(x)||C_G(x)| = |G| = |Z(G)| + |G : C_G(x)|$$

dla pewnego elementu $x \in G \setminus Z(G)$ (G nieprzemienna). Niech $k = |C_G(x)|$, $l = |G : C_G(x)|$. Zauważmy, że $l \geq 2$, i $k > |Z(G)| \geq 1$, bo $x \notin Z(G)$. Mamy więc $2(k-1) \leq l(k-1) = |Z(G)| < k$, a to oznacza, że $k < 1$. Sprzeczność. □

5 Seria V do oddania 16 listopada

Imię i Nazwisko :
Uwaga: kolokwium i egzamin trwały 2godz. i było 20 pytań. Zatem rozwiązanie elementarza powinno zająć ok. 50 - 60 minut.

5.1. (P.Traczyk - kolokwium) Czy w pewnej grupie G istnieją elementy g i h, które są przemienne i $o(g) = 9$, $o(h) = 9$, $o(gh) = 3$

Dowód. Tak, w $\mathbb{Z}_9$, $o(\rho^2) = o(\rho^4) = 9$, zaś $o(\rho^6) = 3$. □

5.2. (P.Traczyk - kolokwium) Czy istnieje epimorfizm grupy $\Sigma_3 \times \Sigma_3 \times \Sigma_3$ na grupę $\mathbb{Z}_8$?

Dowód. NIe, bo w $\Sigma_3 \times \Sigma_3 \times \Sigma_3$ są elementy rzędu $1, 2, 3, 6$ i nie ma elementu o rzędzie podzielnym przez 8. □

5.3. (P.Traczyk - kolokwium) Czy istnieje epimorfizm grupy izometrii własnych 105–kąta foremnego D_{210} na grupę izometrii własnych siedmiokąta foremnego D_{14}?

Dowód. Tak. $D_{210}/\langle \rho^7 \rangle \cong D_{14}$, co pokazywaliśmy na ćwiczeniach. □

5.4. (P.Traczyk - kolokwium) Czy w grupie Σ_{17} istnieją takie dwie permutacje α i β, obydwie rzędu 2, że ich złożenie $\alpha \circ \beta$ jest elementem rzędu 17?

Dowód. Tak. Mamy monomorfizm $D_{34} \to \Sigma_{17}$ obrazy dwóch symetrii np. ϵ i $\epsilon\rho$ są szukanymi permutacjami rzędu 2, których złożenie jest obrazem ρ czyli elementu rzędu 17. □

5.5. (P.Traczyk - kolokwium) Czy w grupie Σ_{117} istnieją takie dwie permutacje α i β, jedna o rozkładzie na cykle typu $5+3$, a druga o rozkładzie na cykle typu $3+3$, że ich złożenie $\alpha \circ \beta$ jest elementem rzędu $133 = 7 \cdot 19$?

Dowód. Nie, element rzędu $133 = 7 \cdot 19$ musi w rozkłdzie na cykle rozłączne mieć elementy rzędu 7 i rzędu 19, czyli co najmniej 26 różnych elementów. Tymczasem w permutacjach o rozkładzie na cykle typu $5 + 3$ i $3 + 3$ jest co najwyżej 14 różnych elementów. □

5.6. (P.Traczyk - kolokwium) Czy jedyną grupą skończoną, w której każde dwa elementy nietrywialne są sprzężone jest grupa $\mathbb{Z}_2$?

Dowód. Tak. Jeśli założenia są spełnione to

$$|G| = |G : C_G(x)||C_G(x)| = 1 + |G : C_G(x)|,$$

czyli $(|C_G(x)| - 1)|G : C_G(x)| = 1$, co oznacza $(|C_G(x)| - 1) = |G : C_G(x)| = 1$, czyli $|C_G(x)| = |G| = 2$. □

5.7. Czy istnieje grupa w której każde dwa elementy nietrywialne są sprzężone?

Dowód. Tak, jest to grupa $\mathbb{Z}_2$. □

5.8. (P.Traczyk - egzamin) Niech $\mathbb{R}$ będzie grupą liczb rzeczywistych z dodawaniem jako działaniem grupowym. Czy grupy $\mathbb{R}$ i $\mathbb{R} \times \mathbb{R}$ są izomorficzne?

Dowód. Tak. Obie grupy są grupami addytywnymi izomorficznych przestrzeni liniowych nad $\mathbb{Q}$. □

5.9. (P.Traczyk - egzamin) Niech G będzie grupą, $x, y \in G$, $x, y \neq 1$. Czy wynika z tego, że wówczas $x^{-2}y^3[G,G] = y^2x^{-1}y[G,G]$?

5.10. (P.Traczyk - egzamin) Niech G będzie grupą, $x, y \in G$, $x, y \neq 1$. Czy wynika z tego, że wówczas $x^{-2}y^3[G,G] \neq y^2x^{-1}y[G,G]$?

Dowód. (obu punktów 5.9 i 5.10) Grupa $G/[G,G]$ jest przemienna, więc $y^{-1}xy^{-2}x^{-2}y^3[G,G] = x^{-1}[G,G]$. Równość więc zachodzi, wtedy i tylko wtedy, gdy $x \in [G,G]$. □

6 Seria VI

6.1. W grupie permutacji Σ_8 komutant $[\Sigma_8, \Sigma_8]$ jest równy $\underline{A_8}$.

Dowód. $\{1\} \neq [\Sigma_8, \Sigma_8] \trianglelefteq \Sigma_8$ i $[\Sigma_8, \Sigma_8] \leqslant A_8$. Wobec prostoty grupy A_8 oznacza to, że $[\Sigma_8, \Sigma_8] = A_8$ □

6.2. W grupie permutacji Σ_4 komutant $[\Sigma_4, \Sigma_4]$ jest równy $\underline{A_4}$.

Dowód. $[\Sigma_4, \Sigma_4] \leqslant A_4$, a jedyna nietrywialna właściwa podgrupa A_4, to podgrupa Kleina K, ale A_4/K jest sześcioelementową grupą nieprzemienną, co latwo sprawdzić. Zatem teza. □

6.3. Czy istnieje epimorfizm (tzn. homomorfizm, który jest "na") $\Sigma_5 \to \mathbb{Z}_5$?.

Dowód. Nie istnieje. Grupa $\mathbb{Z}_5$ jest przemienna, więc homomorfizm taki musiałby faktoryzować się przez $(\Sigma_5)_{ab} = \mathbb{Z}_2$. □

6.4. Czy w grupie permutacji parzystych A_n, $n \geq 2$ element σ jest zawsze sprzężony z elementem σ^{-1}?

Dowód. Nie. Grupa $A_3 = \langle\, (1,2,3) \,\rangle$ jest abelowa, więc element $(1,2,3)$ nie jest sprzężony z $(1,2,3)^{-1} = (3,2,1)$. □

6.5. Czy grupa $GL(2, \mathbb{Z}_{11})$ zawiera normalną podgrupę indeksu 5?

Dowód. Tak. Rozważamy epimorfizm det : $GL(2, \mathbb{Z}_{11} \to \mathbb{Z}_{11}* \cong \mathbb{Z}_{10}$. W grupie $\mathbb{Z}_{10}$ istnieje podgrupa indeksu 5 i jej przeciwobraz jest szukaną podgrupą $GL(2, \mathbb{Z}_{11})$. □

6.6. Czy w grupie G rzędu $7 \cdot 11 \cdot 29$ normalna podgrupa rzędu 7 jest zawsze zawarta w centrum?

Dowód. Tak. Ponieważ podgrupa $K \cong \mathbb{Z}_7$ rzędu 7 jest normalna, to mamy homomorfizm $G \to Aut(K) \cong \mathbb{Z}_6$ zadany przez automorfizmy wewnętrzne. Rzędy są względnie pierwsze, więc homomorfizm jest trywialny, co oznacza $K \leqslant Z(G)$. □

6.7. Pokazać, że jeżeli P jest p – grupą nieprzemienną, to centrum $Z(P)$ nie posiada dopełnienia w P.

Dowód. Przypuśćmy, że K jest tym dopełnieniem. Wówczas $Z(K) \neq \{1\}$ i $P = Z(P) \cdot K$. Widać, że element postaci xy, $x \in Z(P)$, $1 \neq y \in Z(K)$ jest przemienny z dowolnym elementem ab, $a \in Z(P)$, $b \in K$, ale nie należy do centrum. Sprzeczność. □

6.8. Czy grupa rzędu $11 \cdot 15$ zawiera element rzędu 33?

Dowód. Tak. Liczba 11– podgrup Sylowa musi dzielić 15 i przystawać modulo 11 do 1, jest więc równa 1, co oznacza, że 11– podgrupa Sylowa K jest normalna. Z twierdzenia Cauchy'ego istnieje element rzędu 3, który generuje podgrupę H. Oczywiście $H \cap K = \{1\}$, więc podgrupa $K \cdot H$ ma 33 elementy.Ponieważ $11 \not\equiv 1(mod 3)$ i $3 \not\equiv 1(mod 11)$, to grupa rzędu 33 jest cykliczna. □

7 Seria VII

Ta seria, to takie próbne kolokwium. Kolokwium będzie składało się z dwóch części - pierwsza 45 min (13:45 - 14:30), to otwarte pytania, na które trzeba udzielić odpowiedzi i je uzasadnić. Pytań będzie 6. Druga część (15:00-16:00), to nieco trudniejsze od pytań zadania - tych będzie 3 lub 4.

Część I

7.1. Czy każda skończona grupa nieprzemienna G zawiera podgrupę przemienną H, taką że $Z(G)$ jest właściwą podgrupą H?

Dowód. Tak. Niech $x \notin Z(G)$ i niech $H = \langle Z(G), x \rangle$. H jest oczywiście przemienna i jest właściwa, bo G nieprzemienna. □

7.2. Niech $|G| = 25 \cdot 9 \cdot 7$ i niech P będzie 5-podgrupą Sylowa. Czy P jest właściwą podgrupą swojego normalizatora $N_G(P)$?

Dowód. Tak. 5 podgrup Sylowa jest 1 lub 21. W obu przypadkach ich indeks jest mniejszy od $9 \cdot 7$. □

Albo alternatywnie:

Dowód. Tak. $N_G(P) = P$ wtedy i tylko wtedy, gdy $|G : N_G(P)| = 9 \cdot 7$. Indeks $|G : N_G(P)|$ jest równy liczbie 5 podgrup Sylowa i z twierdzenia Sylowa przystaje do 1 mod 5. Ale $9 \cdot 7 \not\equiv 1 \bmod 5$ skąd teza. □

7.3. Niech $|G| = 63$. Czy G zawiera podgrupę rzędu 21?

Dowód. Z twierdzenia Sylowa wynika, że 7 podgrupa Sylowa S_7 jest normalna i izomorficzna z Z_7. Mamy więc homomorfizma $S_9 \to Aut\mathbb{Z}_7 \cong \mathbb{Z}_6$. Homomorfizm ten ma w jądrze element x rzędu 3. Zatem $\langle x, S_7\rangle \cong \mathbb{Z}_{21}$. □

W zadaniu pytanie jest tylko o podgrupę rzędu 21. Można więc prościej:

Dowód. Z twierdzenia Cauchyego wiemy, że grupa G zawiera podgrupę K rzędu 3. Z twierdzenie Sylowa wynika, że 7 podgrupa Sylowa S_7 jest normalna. Zatem dobrze jest zdefiniowana grupa $K \cdot S_7$ i ponieważ $K \cap S_7 = \{1\}$ to ma ona 21 elementów. □

7.4. Czy grupa $\mathbb{Q}$ liczb wymiernych z działaniem dodawania zawiera podgrupę skończonego indeksu?

Dowód. Nie. Przypuśćmy, że $H \leqslant \mathbb{Q}$ jest indeksu n. Wówczas dla każdego $x \in \mathbb{Q}$, $nx \in H$. Jednak dla dowolnego $x \in \mathbb{Q}$, $n\frac{x}{n} = x \in \mathbb{Q}$, czyli $H = \mathbb{Q}$. □

7.5. Jeżeli $A \trianglelefteq G$ jest abelową podgrupą normalną, to czy $Z(G) \leq A$?

Dowód. Nie. $J \times \{1\} \trianglelefteq D_{10} \times \mathbb{Z}_5$, $Z(D_{10} \times \mathbb{Z}_5) = \{1\} \times \mathbb{Z}_5$. □

7.6. Czy dla dowolnych elementów $x_1, \dots x_n$ grupy G ich "długi komutator" $x_1x_2 \dots x_nx_1^{-1}x_2^{-1} \dots x_n^{-1} \in [G, G]$?

Dowód. Tak, bo abelianizacja jest przemienna i mamy równość warstw $x_1x_2 \dots x_nx_1^{-1}x_2^{-1} \dots x_n^{-1}[G, G] = 1[G, G]$. □

Część II

7.7. Niech $P \leqslant G$ będzie p–podgrupą Sylowa i $P \leqslant Z(G)$. Pokazać, że zbiór $C = \{x \in G \colon p \nmid o(x)\}$ jest podgrupą i $PC = G$.

Dowód. $P \leqslant Z(G)$, to $P \trianglelefteq G$. Z Sch-Zass istnieje D dopełnienie. Jasne, że $D \subset C$. Dla $g \in C$ mamy $g = yx$, $y \in P$, $x \in D$. Niech $p^k = o(y)$. Ponieważ $P \leqslant Z(G)$, to $g^{p^k} = y^{p^k}x^{p^k} = x^{p^k} \in D$. Ale $o(g^{p^k}) = \frac{o(g)}{(o(g),p^k)} = o(g)$ więc g^{p^k} jest generatorem grupy cyklicznej $\langle\, g \,\rangle$ i $g \in D$. □

7.8.

Definicja. *Element $x \in G$ nazywa się antygeneratorem wtedy i tylko wtedy, gdy dla każdego podzbioru $X \subseteq G$ jeżeli $\langle X \cup \{x\} \rangle = G$, to $\langle X \rangle = G$.*
Pokazać, że dla grupy skończonej G, podgrupa $\Phi(G)$ jest zbiorem antygeneratorów.

Dowód. Niech $x \in \Phi(G)$. Niech $\langle X \cup \{x\} \rangle = G$ i przypuśćmy, że $\langle X \rangle \neq G$. Wówczas istnieje podgrupa maksymalna H, taka że $\langle X \rangle \leqslant H$. Ale jeżeli $x \in \Phi(G)$, to $x \in H$ i $\langle X \cup \{x\} \rangle \leqslant H$. Sprzeczność.

Niech x będzie antygeneratorem, zaś H maksymalną podgrupą. Jeżeli $x \notin H$, to z maksymalności $\langle H \cup \{x\} \rangle = G$ i oczywiście $\langle H \rangle = H$. Sprzeczność, czyli $x \in H$. □

7.9. Opisać wszystkie (z dokładnością do izomorfizmu) grupy rzędu 18.

Dowód. Z twierdzenia Sylowa wynika, że jest tylko jedna 3 – podgrupa Sylowa, gdyż $2 \not\equiv 1(mod 3)$. Oznacza to, że 3 – podgrupa Sylowa jest normalna, a 2 – podgrupa Sylowa jest izomorficzn z $\mathbb{Z}_2$ i jest jej dopełnieniem. 3 – podgrupa Sylowa P jest izomorficzna z $\mathbb{Z}_9$ lub z $\mathbb{Z}_3 \times \mathbb{Z}_3$.

$P = \mathbb{Z}_9$: $\mathrm{Aut}(P) \cong \mathbb{Z}_6$ i są dwa homomorfizmy $\mathbb{Z}_2 \to \mathrm{Aut}(P)$ - trywialny, i taki, że generator przechodzi na automorfizm $g \to g^{-1}$. W pierwszym przypadku otrzymujemy $\mathbb{Z}_9 \times \mathbb{Z}_2 \cong \mathbb{Z}_{18}$. W drugim przypadku $\mathbb{Z}_9 \rtimes \mathbb{Z}_2 \cong D_{18}$.

$P = \mathbb{Z}_3 \times \mathbb{Z}_3$: $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3) = GL(2, \mathbb{Z}_3)$ i ma rząd $8 \cdot 6 = 16 \cdot 3$. Rozpatrujemy homomorfizmy $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$. Jeżeli homomorfizm jest trywialny, to otrzymujemy $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2$. Homomorfizmy nietrywialne prowadzą do produktów półprostych, które nie są proste. Zgodnie z zadaniem 6.1 dwa homomorfizmy prowadzą do izomorficznych produktów półprostych wtedy i tylko wtedy, gdy różnią się one o automorfizm wewnętrzny $GL(2, \mathbb{Z}_3)$. Macierzy rzędu 2 jest 13, macierz $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ należy do centrum i to jedna klasa sprzężoności. Łatwo jest wypisać pozostałe 12 macierzy rzędu 2 - troche więcej pracy wymaga policzenie ich klas sprzężoności. *(Przyznaję, że troche przesadziłam z tym zadaniem - na kolokwium takich rachunków na pewno nie będzie)* □

8 Seria VIII - do oddania 13 grudnia 2018

8.1. Czy $\mathbb{Z}_{24}$ zawiera podpierścień izomorficzny z $\mathbb{Z}_8$?

Dowód. Nie. Podpierścień zawiera 1 i musi już być całym pierścieniem. □

8.2. Znaleźć dzielniki zera, elementy odwracalne i nilpotentne w $\mathbb{Z}_{24}$ i $\mathbb{Z}_{16}$.

Dowód. W pierścieniu $\mathbb{Z}_n$ liczba k jest elementem odwracalnym wtedy i tylko wtedy, gdy k jest względnie pierwsze z n, jest dzielnikiem zera wtedy i tylko wtedy, gdy nie jest odwracalna. Liczba k jest elementem nilpotentnym wtedy i tylko wtedy, gdy k jest podzielna przez każdą liczbę pierwszą, która dzieli n. W szczególności, jesli $n = p^s$, to każdy dzielnik zera jest elementem nilpotentnym.

$\mathbb{Z}_{24}$	–	dzielniki zera:	$0, 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22$
	–	elementy nilpotentne	$0, 6, 12, 18$
	–	elementy odwracalne	$1, 5, 7, 11, 13, 17, 23$
$\mathbb{Z}_{16}$	–	dzielniki zera:	$0, 2, 4, 6, 8, 10, 12, 14$
	–	elementy nilpotentne	$0, 2, 4, 6, 8, 10, 12, 14$
	–	elementy odwracalne	$1, 3, 5, 7, 9, 11, 13, 15$

□

8.3. W pierścieniu $\mathbb{Z}$ znaleźć część wspólną ideałów $(15) \cap (35)$.

Dowód. $k \in (15) \cap (35) \iff 15 \mid k \,\text{i}\, 35 \mid k \iff 105 \mid k$. Zatem $(15) \cap (35) = (105)$. □

8.4. Znaleźć wszystkie ideały pierścienia $\mathbb{Z}_{15}$ i $\mathbb{Z}_{16}$. Wskazać wśród nich pierwsze i maksymalne. Znaleźć pierścienie ilorazowe.

Dowód. Niech $\pi : R \twoheadrightarrow R/I$ będzie epimorfizmem na pierścień ilorazowy. Korzystamy z faktu, że istnieje wzajemnie jednoznaczna odpowiedniość między ideałami
$J \lhd R/I$ a ideałami R zawierającymi I dana przez $J \leftrightsquigarrow \pi^{-1}(J)$. Ponieważ $R/\pi^{-1}(J) \cong R/I\Big/J$ to przy tej odpowiedniości ideałom pierwszym odpowiadają pierwsze a maksymalnym maksymalne. Ponadto w pierścieniu R, $(x) \subseteq (y) \iff x = yz$ dla pewnego $z \in R$.

Ideały $\mathbb{Z}_{15}$ to obrazy ideałów $(15) \lhd \mathbb{Z}$, $(3) \lhd \mathbb{Z}$, $(5) \lhd \mathbb{Z}$, $(1) \lhd \mathbb{Z}$ i pierścieniami ilorazowymi są odpowiednio: $\mathbb{Z}_{15}$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, 0. Stąd ideały pierwsze i jednocześnie maksymalne w $\mathbb{Z}_{15}$ to $\pi((3)) = (3)$ i $\pi((5)) = (5)$.

Podobnie dla $\mathbb{Z}_{16}$ ideały to (0), (8), (4), (2), (1) a pierścienie ilorazowe to odpowiednio $\mathbb{Z}_{16}$, $\mathbb{Z}_8$, $\mathbb{Z}_4$, $\mathbb{Z}_2$, 0. Jedynym pierwszym, a jednocześnie maksymalnym jest ideał (2). □

8.5. Niech k będzie ciałem, niech $a \in k$. Niech $\Phi_a : k[X] \to k$ będzie homomorfizmem zadanym wzorem $\Phi_a(f) = f(a)$. Znaleźć $\ker \Phi_a$ i napisać izomorfizm wynikający z twierdzenia o izomorfizmie.

Dowód. $\ker \Phi_a = \{f : f(a) = 0\} = (X - a)$, gdyż dowolny wielomian f można podzielić z resztą przez wielomian $X-a$ i przedstawić w postaci $f = (X-a)g+b$, $b \in K$. Widać więc, że $\{f : f(a) = 0\} = \{f : f = (X-a)g; g \in k[X]\} = (X-a)$. Zatem:

$$k[X]/(X - a) \cong K.$$

□

8.6. Niech k będzie ciałem, niech $a_1, \ldots, a_n \in k$. Rozważmy homomorfizm

$$\Phi_{a_1,\ldots,a_n} : k[X] \to \underbrace{k \times \cdots \times k}_{n},\ \Phi_{(a_1,\ldots,a_n)}(f) = (f(a_1), \ldots, f(a_n)).$$

Znaleźć $\ker \Phi_{a_1,\ldots,a_n}$ i napisać izomorfizm wynikający z twierdzenia o izomorfizmie.

Dowód. Jak wyżej $\ker \Phi_{a_1,\ldots,a_n} = \ker \Phi_{a_1} \cap \cdots \cap \ker \Phi_{a_n} = ((X-a_1)\ldots(X-a_n))$ i

$$k[X]/((X - a_1)\ldots(X - a_n)) \cong \underbrace{k \times \cdots \times k}_{n}$$

. □

8.7. Czy pierścień $\mathbb{Z}[X]/(X^n - 1)$ jest dziedziną całkowitości?

Dowód. Nie, gdyż ideał $(X^n - 1) \lhd \mathbb{Z}[X]$ nie jest pierwszy, ponieważ $X - 1 \notin (X^n - 1)$ i $X^{n-1} + \cdots + X + 1 \notin (X^n - 1)$ a $(X - 1)(X^{n-1} + \cdots + X + 1) = X^n - 1 \in (X^n - 1)$. □

8.8. Udowodnić, że jeżeli w pierścieniu R dla każdego elementu $x \in R$ istnieje $n \in N$ (zależne od x), $n > 1$ takie, że $x^n = x$, to każdy ideał pierwszy w R jest maksymalny. (Wskazówka: rozpatrzyć tę równość w pierścieniu ilorazowym przez ideał pierwszy.)

Dowód. Niech $I \lhd R$ ideał pierwszy. Niech $x \notin I$. W R/I mamy $(x+I)^n = x+I$, zatem $(x + I)(x^{n-1} - 1 + I) = 0$. Ponieważ R/I jest dziedziną całkowitości i $x + I \neq 0$, to $(x + I)^{n-1} = x^{n-1} + I = 1 + I$ co dowodzi odwracalności $x + I$. Zatem R/I jest ciałem i I jest ideałem maksymalnym. □

6.12.2018

Kolokwium Algebra I* - Część I

1. *(3 pkt)* Niech G będzie grupą i niech $K \trianglelefteq G$ będzie skończoną podgrupą normalną. Załóżmy, że dla pewnej liczby pierwszej p, $p \mid |K|$, grupa K ma dokładnie jedną p – podgrupę Sylowa $P \leqslant K$. Czy wynika z tego, że $P \trianglelefteq G$?

   Dowód. Tak. Jeżli P jest jedyną p podgrupą Sylowa, to $P \blacktriangleleft K$. Teza wynika ze stwierdzenia: Jeśli $H \blacktriangleleft K$ i $K \trianglelefteq G$, to $H \trianglelefteq G$. □

2. *(3 pkt)* Niech G będzie skończoną grupą prostą i niech p będzie największą liczbą pierwszą dzielącą rząd G. Czy dla każdej właściwej podgrupy $H \leqslant G$, indeks $|G : H| \geq p$?

   Dowód. Tak. Rozpatrujemy nietrywialny homomorfizm $G \to \Sigma_{|G;H|}$ zdefiniowany przez działanie G na zbiorze warstw G/H prze mnożenie z lewej strony. Jeżeli G jest grupą prostą, to homomorfizm ten jest monomorfizmem i $|G| \mid |G : H|!$. W szczególności $p \mid |G : H|!$ więc $|G : H| \geq p$ □

3. *(4 pkt)* Niech grupa skończona G, $|G| > 2$, ma cykliczną 2 – podgrupę Sylowa. Czy G może być grupą prostą?

   Dowód. Nie. NIech $|G| = n$. Rozpatrzmy monomorfizm Cayley'a $\varphi\colon G \to \Sigma_n$. Obraz generatora 2 – podgrupy Sylowa jest iloczynem nieparzystej liczby cykli parzystej długości (równej rzędowi 2 – podgrupy Sylowa), jest więc permutacją nieparzystą. Zatem $\varphi^{-1}(A_n)$ jest właściwą normalną podgrupą. □

4. *(4 pkt)* Niech H będzie podgrupą w grupie skończonej G i niech H będzie p – grupą dla pewnej liczby pierwszej p. Załóżmy, że $p \mid |G : H|$. Czy wynika z tego, że $p \mid |N_G(H) : H|$?

   Dowód. Tak. Rozpatrzmy działanie H na zbiorze warstw G/H. Punkty stałe tego dzialania to $N_G(H)/H$. Mamy $|N_G(H)/H| \equiv |G/H|(modp)$. Ponieważ $|G : H| \equiv 0(modp)$, to $|N_G(H)/H| \equiv 0(modp)$ i mamy tezę, □

5. *(3 pkt)* Podać przykład produktu półprostego, w którym nie każde dwa dopełnienia są sprzężone.

   Dowód. D_{4k} jest produktem półprostym wewnętrznym $J \cdot \langle\, \epsilon\rho^k \,\rangle$, gdzie $J \trianglelefteq D_{4k}$ jest podgrupą obrotów, a $\epsilon\rho^k$ dowolną symetrią. Ale symetrie w grupie D_{4k} tworzą dwie klasy sprzężoności. □

6. *(3 pkt)* Czy grupa rzędu $25 \cdot 13$ jest przemienna?

Dowód. Tak. Z tw. Sylowa 13 podgrup Sylowa może być 1, 5, 25, ale tylko tylko 1 przystaje do $1(mod13)$, więc 13 podgrupa Sylowa, jest normalna. Ponieważ $13 \not\equiv 1(mod5)$, to 5 – podgrupa Sylowa też jest normalna. Tak więc grupa jest produktem swoich podgrup Sylowa. Obie podgrupy Sylowa są abelowe: 13– podgrupa Sylowa jest izomorficzna z $\mathbb{Z}_{13}$, zaś 5 – podgrupa Sylowa jest izomorficzna z $\mathbb{Z}_{25}$ lub z $\mathbb{Z}_5 \times \mathbb{Z}_5$. Zatem grupa rzędu$25 \cdot 13$, jako produkt dwóch grup przemiennych jest przemienna. □

6.12.2018

Kolokwium Algebra I* - Część II

1. Niech G będzie grupą, dla której grupa $\mathrm{Aut}(G)$ jest cykliczna.

   a) *(3 pkt)* Udowodnić, że wówczas G jest grupą abelową.

   Dowód. Mamy homomorfizm $\Phi : G \to \mathrm{Aut}(G)$, $\ker \Phi = Z(G)$, $\mathrm{im}\,\Phi = \mathrm{Inn}(G) \leqslant Aut(G)$. Podgrupa grupy cyklicznej, jest cykliczna, zatem $G/Z(G)$ jest cykliczna, a więc jest tryywialna i G jest abelowa. □

   b) *(5 pkt)* Czy prawdziwe jest zdanie, że jeżeli grupa $\mathrm{Aut}(G)$ jest cykliczna, to G jest grupą cykliczną?

   Dowód. Odpowiedź jest "tak" dla grup skończonych.Wiemy, że G jest abelowa - stosujemy zapis addytywny. Jeżeli G jest skończona i nie jest cykliczna, to w rozkładzie na produkt grup p– grup cyklicznych musi zawierać $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^l}$, $l \geq k$. Ponieważ $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^l}$ jest czynnikiem prostym, to $\mathrm{Aut}(\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^l}) \leqslant \mathrm{Aut}(G)$. Ale grupa $\mathrm{Aut}(\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^l})$ nie jest przemienna!
   Definiujemy automorfizmy ϕ i ψ zadając je na generatorach. Niech

   $$\begin{array}{ll} \phi((1,0)) = (1,0) & \psi((1,0)) = (1,p^{l-k}) \\ \phi((0,1)) = (1,1) & \psi((0,1)) = (0,1) \end{array}.$$

   Obie definicje są poprawne, bo $o(0,1) = o(1,1)$ i $o(1,0) = o(1,p^{l-k})$. Ponadto ϕ i ψ są automorfizmami, bo odwrotne są zadane przez

   $$\begin{array}{ll} \phi^{-1}(1,0) = (1,0) & \psi^{-1}((1,0)) = (1,-p^{l-k}) \\ \phi^{-1}(0,1) = (-1,1) & \psi^{-1}((0,1)) = (0,1) \end{array}.$$

   Homomorfizmy przemienne nie są:

   $$\begin{array}{ll} \phi\psi((1,0)) = (1+p^{l-k}, p^{l-k}) & \psi\phi((1,0)) = (1,p^{l-k}) \\ \phi\psi((0,1)) = (1,1) & \psi\phi((0,1)) = (1,1+p^{l-k}) \end{array}.$$

   Można podać przykład grupy nieskończonej abelowej, różnej od $\mathbb{Z}$, której grupa automorfizmów jest równa $\mathbb{Z}_2$. Rozważmy grupę addytywną ciała liczb wymiernych $\mathbb{Q}$. Automorfizmami jest mnożenie przez niezerową liczbę wymierną (tę na którą przechodzi 1). Szukamy takiej podgrupy, którą "ruszają z miejsca" te automorfizmy. Jest nią podgrupa $G = \{\frac{p}{q} \colon (p,q) = 1, k^2 \nmid q, k - \text{liczba pierwsza}\}$ złożona z tych liczb

wymiernych, że mianownik skróconego ułamka nie jest podzielny przez kwadrat liczby pierwszej. Jedynym nietrywialnym automorfizmem tej grupy jest mnożenie przez -1, więc $\mathrm{Aut}(G) \cong \mathbb{Z}_2$. □

2. Niech G będzie grupą. Podgrupą Frattini $\Phi(G)$ nazywamy część wspólną wszystkich maksymalnych podgrup grupy G.

   a) *(2 pkt)* Pokazać, że $\Phi(G) \blacktriangleleft G$ jest podgrupą charakterystyczną.

   Dowód. Wynika z tego, że obraz podgrupy maksymalnej przy automorfizmie jest podgrupą maksymalną. □

   b) *(7 pkt)* Niech P będzie p – grupą dla pewnej liczby pierwszej p. Udowodnić, że grupa ilorazowa $P/\Phi(P)$ jest izomorficzna z produktem $\underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \ldots \mathbb{Z}_p}_{k}$, dla pewnego $k \geq 1$.

   Dowód. Korzystamy z faktu, że maksymalna podgrupa p – grupy jest normalna i jest indeksu p. Niech $H_1, \ldots, H_l$ będzie listą maksymalnych podgrup w P. Niech $\pi_j : P \to P/H_j$ będzie epimomorfizmem na grupę ilorazową. Rozważmy homomorfizm

   $$\Phi : P \to P/H_1 \times P/H_2 \times, \ldots, \times P/H_l \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times, \ldots, \times \mathbb{Z}_p}_{l}.$$

   Jądrem tego homomorfizmu jest $\Phi(P)$, zaś obraz grupą przemienną skończoną, w której każdy nietrywialny element jest rzędu p. Taka grupa jest izomorficzna z $\underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \ldots \mathbb{Z}_p}_{k}$, dla pewnego $k \geq 1$. □

3. *(13 pkt)* Niech G będzie grupą rzędu $2^2 \cdot 3 \cdot 7 \cdot 13 \cdot 17$. Pokazać, że 17 – podgrupa Sylowa jest normalna.

   Wskazówka: Niech P będzie 13 *podgrupą Sylowa. Pokazać, że $N_G(P)$ zawiera pewną* 17 *podgrupę Sylowa Q. Zbadać $P \cdot Q$ i wyciągnąć wnioski dotyczące $|N_G(Q)|$.*

   Dowód. Skorzystamy ze wskazówki:

   - Liczba 13 podgrup Sylowa dzieli $2^2 \cdot 3 \cdot 7 \cdot 17$ i przystaje do $1 (mod 13)$ - możliwe są liczby 1 i 14. Liczba 13 – podgrup Sylowa jest indeksem normalizatora dowolnej z nich - zatem $|N_G(P)| = 2^2 \cdot 3 \cdot 7 \cdot 17$ lub $|N_G(P)| = 2 \cdot 3 \cdot 17$ i w każdym razie rząd $N_G(P)$ jest podzielny przez 17.
   - Niech Q będzie 17 podgrupą Sylowa zawartą w $N_G(P)$. Oczywiście $P \trianglelefteq N_G(P)$, więc zbiór $P \cdot Q$ jest podgrupą $N_G(P)$ rzędu $13 \cdot 17$. Ponieważ $13 \not\equiv 1 (mod 17)$ i $17 \not\equiv 1 (mod 13)$, to jest to grupa przemienna (izomorficzna z $\mathbb{Z}_{13 \cdot 17}$).
   - Z przemienności grupy $P \cdot Q$ wnioskujemy, że $P \leqslant N_G(Q)$, a więc $13 \nmid |G : N_G(Q)|$.

- Liczba 17 podgrup Sylowa dzieli $2^2 \cdot 3 \cdot 7 \cdot 13$ i przystaje do $1(mod 17)$ - możliwe są liczby 1, $4 \cdot 13$, $3 \cdot 7 \cdot 13$.
- Ponieważ $13 \nmid |G : N_G(Q)|$, to liczby $4 \cdot 13$, $3 \cdot 7 \cdot 13$ odpadają i w grupie G jest dokładnie jedna 17 podgrupa Sylowa, a zatem jest ona normalna.

□

9 Seria IX - świąteczno - noworoczna - do oddania 10 stycznia 2018

9.1. Czy każdy ideał pierścienia $P \times R$ jest postaci $I \times J$, gdzie I i J są ideałami pierścieni P i R odpowiednio?(to, że $I \times J$ jest ideałem uważamy za oczywiste)

Dowód. Tak. Niech $K \triangleleft P \times R$. Niech $I = \pi_P(K)$ i $J = \pi_R(K)$, gdzie π_P i π_R są rzutami. Są to ideały jako obrazy ideału K przy epimorfizmie. Jest jasne, że $K \subseteq I \times J$. Jeżeli $a \in I$ i $b \in J$, to istnieją $a', b' \in K$ dla których $(a, b'), (a', b) \in K$. Wówczas $(a, 0) = (a, b')(1, 0) \in K$ oraz $(0, b) = (a', b)(0, 1) \in K$. Zatem $(a, 0) + (0, b) = (a, b) \in K$, co dowodzi $I \times J \subseteq K$. □

9.2. Niech $I \triangleleft P$, $J \triangleleft R$ będą ideałami. Kiedy $I \times J$ jest ideałem pierwszym?

Dowód. Mamy $P \times R/I \times J \cong P/I \times R/J$, więc jeśli to ma być dziedzina całkowitości, to jeden z pierścieni ilorazowych musi być zerowy. Zatem ideały pierwsze są postaci $I \times R$ i $P \times J$, gdzie I i J są ideałami pierwszymi. □

9.3. Niech $I \triangleleft P$, $J \triangleleft R$ będą ideałami. Kiedy $I \times J$ jest ideałem maksymalnym?

Dowód. Jak wyżej $P \times R/I \times J \cong P/I \times R/J$ i ideały maksymalne są postaci $I \times R$ i $P \times J$, gdzie I i J są ideałami maksymalnymi. □

9.4. Niech R będzie dziedziną ideałów głównych, a $S \subseteq R$ systemem multyplikatywnym. Czy $S^{-1}R$ jest dziedziną ideałów głównych?

Dowód. Tak. Dowodziliśmy, że jeżeli $\varphi R \to S^{-1}R$ jest kanonicznym homomorfizmem, to każdy ideał jest generowany przez $\varphi(J)$ dla pewnego ideału $J \triangleleft R$. Zatem jeżeli każdy ideał pierścienia R jest główny, to każdy ideał pierścienia $S^{-1}R$ też jest główny. □

9.5. Niech R będzie dziedziną z jednoznacznością rozkładu, a $S \subseteq R \setminus \{0\}$ systemem multyplikatywnym.

a) Jakie są elementy nierozkładalne w $S^{-1}R$?

Dowód. $S^{-1}R$ jest dziedziną, np. dlatego że jest to podpierścień ciała ułamków. Każdy element jest stowarzyszony z elementem postaci $\frac{a}{1}$. Element $\frac{a}{1} = \frac{a_1}{1}\frac{a_2}{1}\ldots\frac{a_n}{1}$, gdzie a_i, $1 \leq i \leq n$ są elementami nierozkładalnymi w R.
Wystarczy więc zbadać kiedy dla nierozkładalnego $a \in R$ element $\frac{a}{1} \in S^{-1}R$ jest nierozkładalny:

(a) element $\frac{a}{1} \in S^{-1}R$ jest odwracalny wtedy i tylko wtedy, gdy a jest dzielnikiem pewnego elementu należącego do systemu S. Istotnie jeżeli $s = ar$, $s \in S$, to $\frac{a}{1}\frac{r}{s} = 1$. Odwrotnie - jeżeli $\frac{a}{1}$ odwracalny, to $\frac{a}{1}\frac{r}{s} = \frac{ar}{s} = 1$. Zatem dla pewnego $t \in S$, $t(ar - s) = 0$. Ponieważ $0 \notin S$, a R jest dziedziną, to $ar = s$.

(b) W przeciwnym przypadku $\frac{a}{1}$ jest elementem pierwszym a więc nierozkładalnym pierścienia $S^{-1}R$. Przypuśćmy bowiem, że $\frac{a}{1} \mid \frac{r_1}{s_1}\frac{r_2}{s_2}$, czyli $\frac{a}{1}\frac{r_3}{s_3} = \frac{r_1}{s_1}\frac{r_2}{s_2}$, czyli istnieje $t \in S$, że $t(ar_3s_1s_2 - s_3r_1r_2) = 0$. Tak jak poprzednio oznacza to, że $ar_3s_1s_2 = s_3r_1r_2$. Element a nierozkładalny w R jest pierwszy (R jest DJR) i a nie dzieli s_3, więc $a \mid r_1r_2$, co z kolei oznacza, że $a \mid r_1$ lub $a \mid r_2$. Zatem $\frac{a}{1} \mid \frac{r_1}{s_1}$ lub $\frac{a}{1} \mid \frac{r_2}{s_2}$.

□

b) Czy $S^{-1}R$ jest dziedziną z jednoznacznością rozkładu?

Dowód. Tak. Wystarczy pokazać, że każdy element jest iloczynem nierozkładalnych. Jednoznaczność wynika z poprzedniego punktu, gdyż pokazaliśmy, że nierozkładalne elementy są pierwsze. Niech $\frac{a}{s} \in S^{-1}R$. Ponieważ R jest DJR, to $\frac{a}{s} = \frac{1}{s}\frac{a_1}{1}\frac{a_2}{1}\ldots\frac{a_n}{1}$ i czynniki są bądź odwracalne, bądź nierozkładalne. □

9.6. Stosując metodę z "chińskiego twierdzenia o resztach" znaleźć liczbę całkowitą a, taką że $a \equiv 1 \pmod 3$, $a \equiv 2 \pmod{226}$, $a \equiv 5 \pmod 7$.

Dowód.

$$\begin{array}{ccccc} (-75)\cdot 3 & + & 1\cdot 226 & = & 1 \\ (-2)\cdot 3 & + & 1\cdot 7 & = & 1 \\ 97\cdot 7 & + & (-3)\cdot 226 & = & 1 \end{array}$$

Zatem liczba $97 \cdot 7 \cdot (-75) \cdot 3$ daje resztę 1 przy dzieleniu przez 226 oraz resztę 0 przy dzieleniu przez 3 i przez 7, zaś $2 \cdot 97 \cdot 7 \cdot (-75) \cdot 3$ daje resztę 2 przy dzieleniu przez 226 oraz resztę 0 przy dzieleniu przez 3 i przez 7. Liczba $226 \cdot 7$ daje resztę 1 przy dzieleniu przez 3 oraz resztę 0 przy dzieleniu przez 7 i przez 226. Liczba $5 \cdot (-2) \cdot 3 \cdot (-3) \cdot 226$ daje resztę 5 przy dzieleniu przez 7 oraz resztę 0 przy dzieleniu przez 3 i przez 226. Ostatecznie liczba

$$226 \cdot 7 + 2 \cdot 97 \cdot 7 \cdot (-75) \cdot 3 + 5 \cdot (-2) \cdot 3 \cdot (-3) \cdot 226 + k \cdot 3 \cdot 226 \cdot 7, \quad k \in \mathbb{Z}$$

jest ogólnym rozwiązaniem kongruencji.

□

9.7. (JO) Sprawdzić, czy element a jest nierozkładalny w pierścieniu $\mathbb{Z}[\sqrt{-5}]$.

a) $a = 2 + 3\sqrt{-5}$;

Dowód. Element ten jest nierozkładalny. Jego waluacja $v(2 + 3\sqrt{-5}) = 49$, więc jeśli byłby rozkładalny, to musiałby być iloczynem dwóch elementów o waluacji równej 7. Takich elementów jednak nie ma, bo nie istnieją liczby całkowite $m, n \in \mathbb{Z}$ dla których $m^2 + n^2 5 = 7$. □

b) $a = 7 + \sqrt{-5}$;

Dowód. Mamy $7 + \sqrt{-5} = (1 + \sqrt{-5})(2 - \sqrt{-5})$.Oba czynniki są nieodwracalne, gdyż ich waluacje (6 i 9 odpowiednio) są różne od 1. □

c) $a = 3$. Czy 3 jest elementem pierwszym w $\mathbb{Z}[\sqrt{-5}]$?

Dowód. Element jest nierozkładalny. Jego waluacja $v(3) = 9$, więc jeśli byłby rozkładalny, to musiałby być iloczynem dwóch elementów o waluacji równej 3. Takich elementów jednak nie ma, bo nie istnieją liczby całkowite $m, n \in \mathbb{Z}$ dla których $m^2 + n^2 5 = 3$. Element 3 nie jest pierwszy, gdyż $3 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, ale nie dzieli żadnego z czynników. □

9.8. (JO) Wyznacz rozkład elementu $a = 45{-}15i$ na iloczyn czynników nierozkładalnych w pierścieniu $\mathbb{Z}[i]$.

Dowód.

$$45{-}15i = 5 \cdot 3 \cdot (3 - i) = (2 + i) \cdot (2 - i) \cdot 3 \cdot (1 + i) \cdot (1 - 2i).$$

Czynniki tego rozkładu są elementami nierozkładalnymi, gdyż waluacje elementów $(2 + i)$, $(2 - i)$, $(1 + i)$, $(1 - 2i)$ są liczbami pierwszymi, zaś nie istnieją liczby całkowite $m, n \in \mathbb{Z}$ dla których $m^2 + n^2 = 3$ a to jest warunek konieczny i dostateczny na to, by 3 byla rozkładalna. □

9.9. (JO) Czy w pierścieniu $\mathbb{Z}[\sqrt{-3}]$ istnieje $\mathrm{NWD}(4, 2{-}2\sqrt{-3})$?

Dowód. Nie. Przypuśćmy, że NWD istnieje i jest równy $a + b\sqrt{-3}$. NWD musi być podzielny przez 2 oraz przez $1 - \sqrt{-3}$, bo $4 = (1 - \sqrt{-3})(1 + \sqrt{-3})$. Łatwy rachunek przekonuje. że musi być podzielny przez ilocznyn. Ale $2{-}2\sqrt{-3} \not| 4$. □

9.10. (JO) Czy ideał $(3{-}i, 8{-}i)$ jest ideałem maksymalnym w pierścieniu $\mathbb{Z}[i]$?

Dowód. Pierścień $\mathbb{Z}[i]$ jest DIG, więc $(3{-}i, 8{-}i) = (\mathrm{NWD}(3{-}i, 8{-}i))$. Ten największy wsólny dzielnik możemy policzyć korzystając z algorytmu Euklidesa, lub rozkładając oba elementy na czynniki nierozkładalne. Algorytm Euklidesa wygląda tak:

$$\begin{array}{rcl} 8 - i & = & (3 - i)2 \qquad + \quad (2 + i) \\ 3 - i & = & (2 + i)(1 - i) \end{array}.$$

Zatem $\mathrm{NWD}(3{-}i, 8{-}i)) = 2 + i$. Element $2 + i$ jest nierozkładalny, bo jego waluacja (=5) jest liczbą pierwszą. Pierścień $\mathbb{Z}[i]$ jest dziedziną z jednoznacznością rozkładu, więc element ten jest pierwszy i ideał przez niego generowany jest pierwszy. Pierścień $\mathbb{Z}[i]$ jako Euklidesowy jest DIG, a więc każdy ideał pierwszy jest maksymalny. □

9.11. Czy $I \triangleleft R$ jest ideałem pierwszym w R?

a) $I = (3i)$, $R = \mathbb{Z}[i]$

Dowód. Tak. $I = (3i) = (3)$, bo i jest elementem odwracalnym. 3 jest elementem nierozkładalnym jak każda liczba pierwsza, która przystaje do 3 mod 4 (patrz skrypt). Tu zresztą łatwo się przekonać, że 3 nie jest sumą kwadratów. Jako element nierozkładalny w DJR jest elementem pierwszym, a więc ideał gló ny przez niego generowany jest pierwszy. □

b) $I = (X^5-1)$, $R = \mathbb{Z}[X]$

Dowód. Nie, Element $X^5-1 = (X-1)(X^4+X^3+X^2+X+1)$ jest rozkładalny, bo żaden z czynników nie jest odwracalny. Jako element rozkładalny nie jest pierwszy, a więc ideał przez niego generowany też nie jest pierwszy. □

9.12. (JO) Czy ideał $(X, X^3-7) \lhd \mathbb{Z}[X]$ jest ideałem głównym? Czy jest ideałem maksymalnym?

Dowód. Zauważmy, że $(X, X^3-7) = (X, 7)$. Ideał ten jest maksymalny, bo $\mathbb{Z}[X]/(X, 7) = \mathbb{Z}_7$ i jest ciałem. Ideał nie jest główny, bo gdyby $(7, X) = (f)$ to $f \mid 7$ i $f \mid X$, co oznacza, że $f = 1$, ale to nie jest możliwe, bo ideał $(X, 7)$ jest właściwy. □

9.13. (JO) Czy pierścień $K[X]/(X^n)$ jest lokalny, gdzie K jest dowolnym ciałem?

Dowód. Tak. Ideały pierwsze pierścienia $K[X]/(X^n)$ są we wzajemnie jednoznacznej odpowiedniości z ideałami pierwszymi pierścienia $K[X]$ zawierającymi ideał (X^n). Ideały pierwsze $K[X]$, są postaci (f), gdzie f jest nierozkładalny. Zawieranie $(X^n) \subseteq (f)$ oznacza, że $f \mid X^n$ - jest tylko jeden wielomian nierozkładalny o tej własności i jest nim X. Zatem pierścień $K[X]/(X^n)$ ma tylko jeden ideał pierwszy, będący obrazem ideału (X) więc tylko jeden ideał maksymalny.

Inaczej - jest jasne, że pierścień ilorazowy pierścienia lokalnego jest pierścieniem lokalnym. Pierścień $K[[X]]$ jest lokalny (suma dwóch elementów nieodwracalnych, czyli postaci $a_1X + a_2X^2 + \dots$ jest elementem nieodwracalnym) i oczywiście $K[[X]]/(X^n) \cong K[X]/(X^n)$.

□

9.14. Czy pierścień $Z[i]/(3+i)$ jest ciałem lub iloczynem prostym ciał? Jeżeli tak, to jakie to ciało (lub iloczyn prosty jakich ciał)?

Dowód. Mamy $3 + i = (1 + i)(2 - i)$ jest rozkładem na czynniki nierozkładalne (waluacje czynników są liczbami pierwszymi) i niestowarzyszone. Z chińskiego twierdzenia o resztach mamy:

$$Z[i]/(3 + i) \cong Z[i]/(1 + i) \times Z[i]/(2 - i).$$

Pokażemy, że $Z[i]/(1 + i) \cong \mathbb{Z}_2$ zaś $Z[i]/(2 - i) \cong \mathbb{Z}_5$. Robiliśmy takie zadanie na ćwiczeniach, teraz trochę inny argument: $a+bi = a-b+b(1+i)$. Zauważmy, że $2 \in (1+i)$. Zdefiniujmy przekształcenie $\varphi : Z[i] \to \mathbb{Z}_2$, $\varphi(a+bi) = a-bmod2$. Należy sprawdzić, że jest to homomorfizm, co jest nietrudnym rachunkiem. Jego jądro to oczywiście $(1 + i)$. Drugi iloraz można policzyć podobnie.

□

10 Seria X

Ta seria, to też próbne kolokwium. Kolokwium będzie składało się z dwóch części - pierwsza 60 min (10:00 - 11:00), to otwarte pytania, na które trzeba udzielić odpowiedzi i je uzasadnić. Pytań będzie 6. Druga część (11:30-12:30?), to nieco trudniejsze od pytań zadania - tych będzie 3.

Część I

10.1. Czy jeżeli pierścień ilorazowy pierścienia $K[X]$, gdzie K jest ciałem, jest dziedziną całkowitości, to jest ciałem?

Dowód. Tak. $K[X]$ jest DIG, więc ideały pierwsze są maksymalne. □

10.2. Czy pierścienie $\mathbb{C}[X,Y]/(X^2-Y^2)$ i $\mathbb{C}[X,Y]/(XY)$ są izomorficzne?

Dowód. TAK. Homomorfizm $\mathbb{C}[X,Y]$, który jest identycznością na $\mathbb{C}$ oraz $X \to X-Y$ i $Y \to X+Y$ jest oczywiście automorfizmem przy którym $(XY) \to (X^2-Y^2)$, co kończy dowód. Można też z tewierdzenia chińskiego o resztach pokazać, że oba piercienie ilorazowe są izomorficzne z $\mathbb{C}[X] \times \mathbb{C}[X]$. □

10.3. Z jakim pierścieniem izomorficzny jest pierścień $\mathbb{Z}[i]/(5)$?

Dowód. $5 = (2+i)(2-i)$, oba czynniki są nierozkładalne (waluacja jest liczbą pierwsza 5) i niestowarzyszone. Pokazywaliśmy, że $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}_5$. Analogicznie $\mathbb{Z}[i]/(2-i) \cong \mathbb{Z}_5$. Zatem z chińskiego twierdzenia o resztach $\mathbb{Z}[i]/(5) \cong \mathbb{Z}_5 \times \mathbb{Z}_5$. □

10.4. Czy w pierścieniu $K[[X]]$ szeregów formalnych o współczynnikach w ciele K, każdy niezerowy ideał pierwszy jest maksymalny?

Dowód. Tak. Jest wiele argumentów - to pierścień euklidesowy, a więc DIG. Albo - jedyne ideały są postaci (X^n) więc jedyny pierwszy jest jedynym maksymalnym i jest to (X). □

10.5. Czy jeżeli I jest niezerowym ideałem w pierścieniu $\mathbb{Z}[\sqrt{d}]$ to $I \cap \mathbb{Z} \neq \{0\}$?

Dowód. Tak. $(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - b^2 d \in I \cap \mathbb{Z}$. □

10.6. Niech $K \subset L$ będą ciałami. Niech $f, g \in K[X]$. Czy największy wspólny dzielnik wielomianów f i g w pierścieniu $K[X]$ jest równy ich największemu wspólnemu dzielnikowi w pierścieniu $L[X]$?

Dowód. NWD wylicza się z algorytmu Euklidesa, który jest tożsamy dla obu ciał. □

Część II

10.7. Niech $I \triangleleft R$ i $J \triangleleft R$ będą ideałami. Niech

$$IJ = \{\sum_{i=1}^{n} a_i b_i \colon a_i \in I, b_i \in J, n \in \mathbb{N}\}.$$

Sprawdzić, że IJ jest ideałem. Pokazać, że jeżeli I i J są ideałami względnie pierwszymi, to $IJ = I \cap J$.

Dowód. Jest jasne, że $IJ \subseteq I \cap J$. Jeżeli I oraz J sa względnie pierwsze, to $I + J = R$, więc istnieją $a \in I$, $b \in J$, $a + b = 1$. Dla $c \in I \cap J$, $c = c(a + b) = ac + cb \in IJ$. □

10.8. Niech $D = \det \begin{bmatrix} x & y \\ z & w \end{bmatrix}$ będzie wielomianem $D \in \mathbb{Z}[x, y, z, w]$.

a) Pokazać, że $(D) \triangleleft \mathbb{Z}[x, y, z, w]$ jest ideałem pierwszym.

Dowód. Wielomian $xw - yz \in (K[y, z, w])[x]$ jest nierozkładalny, bo to niezerowy wielomian stopnia 1, więc ideał prze niego generowany jest pierwszy, bo z twierdzenia Gaussa $\mathbb{Z}[x, y, z, w]$ jest DJR a tam elementy nierozkładalne są pierwsze. □

b) Zbadać, czy pierścień ilorazowy $\mathbb{Z}[x, y, z, w]/(D)$ jest dziedziną z jednoznacznością rozkładu.

Dowód. Nie jest. $xw + (D) = yz + (D)$ są dwoma róznymi rozkładami. □

10.9. Niech R będzie dziedziną noetherowską, taką że dla dowolnych dwóch elementów $a, b \in R \setminus \{0\}$ istnieje ich wspólny dzielnik i jest on postaci $ar + bs$ dla pewnych $r, s \in R$. Pokazać, że R jest dziedziną ideałów głównych.

Dowód. Każdy ideał jest skończenie generowany. Pokazujemy, że ideał generowany przez n elementów, jest generowany przez $n - 1$ elementów. Niech $I = (a_1, \ldots, a_{n-1}, a_n)$. Niech $d = NWD(a_{n-1}, a_n)$. Oczywiście $a_n, a_{n-1} \in (a_1, \ldots, a_{n-2}, d)$ Więc $(a_1, \ldots, a_{n-1}, a_n) \subset (a_1, \ldots, a_{n-2}, d)$. Ponieważ$d = a_n r + a_{n-1} s$, to $d \in (a_1, \ldots, a_{n-1}, a_n)$ i mamy zawieranie przeciwne. □

19.1.2019

Kolokwium Algebra I* - Część I

Imię i Nazwisko:

1. *(3 pkt)* Wskazać ideały maksymalne pierścienia $\mathbb{R}[X]/(X^2-3X+2)$.

   Dowód. Ideały maksymalne $\mathbb{R}[X]/(X^2-3X+2)$ są obrazami przy przekształceniu ilorazowym ideałów maksymalnych pierścienia $\mathbb{R}[X]$ zawierających ideał (X^2-3X+2). Mamy $X^2-3X+2=(x-1)(x-2)$. Pierścień $\mathbb{R}[X]$ jest DIG i ideały maksymalne zawierające (X^2-3X+2) są generowane przez nierozkładalne czynniki X^2-3X+2, czyli są to ideały $(X-1)$ i $(X-2)$.

   Można też z tw. chińskiego o resztach:

   $\mathbb{R}[X]/(X^2-3X+2) \cong \mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X-2) \cong \mathbb{R}\times\mathbb{R}$, a w tym ostanim produkcie sa dwa ideały maksymalne $\mathbb{R}\times\{0\}$ i $\{0\}\times\mathbb{R}$. □

2. *(3 pkt)* Niech R będzie pierścieniem, niech $a \in R$. Czy w pierścieniu wielomianów $R[X]$ ideały $(f_1,\ldots,f_n,X-a)$ i $(f_1(a),\ldots,f_n(a),X-a)$ są równe?

   Dowód. Tak. Mamy $f_i=(X-a)g_i+f_i(a)$, gdyż wielomian f_i możemy podzielić z resztą przez unormowany wielomian $X-a$. Zatem $f_i(a)\in(f_1,\ldots,f_n,X-a)$. Równości $f_i=(X-a)g_i+f_i(a)$ oznaczają, że $f_i\in(f_1(a),\ldots,f_n(a),X-a)$. □

3. *(4 pkt)* Niech $I\triangleleft R$, $J\triangleleft R$ i $P\triangleleft R$ będą ideałami, przy czym P jest ideałem pierwszym. Czy $IJ\subset P$ wtedy i tylko wtedy gdy $I\cap J\subset P$?
   (Przypomnienie: $IJ=\{\sum_{i=1}^n a_ib_i\colon a_i\in I, b_i\in J, n\in\mathbb{N}\}$)

   Dowód. Tak. Ponieważ $IJ\subset I\cap J$, to należy pokazać, że jeśli $IJ\subset P$, to $I\cap J\subset P$. Jeżeli $a\in I\cap J$, to $a^2\in IJ$ i $a^2\in P$. Ponieważ P jest ideałem pierwszym, to $a\in P$. □

4. *(3 pkt)* Niech $I\triangleleft R$, $J\triangleleft R$ i $P\triangleleft R$ będą ideałami, przy czym P jest ideałem pierwszym. Czy z tego, że $I\cap J\subset P$ wynika, że $I\subset P$ lub $J\subset P$?

   Dowód. Tak. W przciwnym przypadku istnieją elementy $a\in I\setminus P$ oraz $b\in J\setminus P$. Element $ab\in I\cap J\subseteq P$, więc $a\in P$ lub $b\in P$, bo P jest pierwszy - sprzeczność. □

5. *(3 pkt)* Niech $a,b\in\mathbb{Z}$ będą liczbami całkowitymi. Czy ich największy wspólny dzielnik w pierścieniu liczb całkowitych $\mathbb{Z}$ jest równy ich największemu wspólnemu dzielnikowi w pierścieniu liczb Gaussa $\mathbb{Z}[i]$?

   Dowód. Tak. Niech d będzie największym wspólnym dzielnikiem a i b w pierścieniu liczb całkowitych. Oczywiście d dzieli też a i b w pierścieniu Gaussa $\mathbb{Z}[i]$. Niech $\alpha\in\mathbb{Z}[i]$ dzieli a i b w $\mathbb{Z}[i]$. Wiemy jednak, że $d=ak+bl$, więc $\alpha\mid d$ w pierścieniu $\mathbb{Z}[i]$. Czyli d jest największym wspólnym dzielnikiem elementów a i b w pierścieniu liczb $\mathbb{Z}[i]$. □

6. *(3 pkt)* Czy ideał $(7+\sqrt{5})$ jest maksymalny w pierścieniu $\mathbb{Z}[\sqrt{5}]$?

   Dowód. Nie. $7+\sqrt{5} = (3+\sqrt{5})(4-\sqrt{5})$, więc pierścień ilorazowy nie jest nawet dziedziną całkowitości. □

7. *(6 pkt)* W pierścieniu wielomianów $K[X]$ nad ciałem K, wielomian stopnia n, $f = a_0 + a_1X + \dots a_nX^n$, $a_0 \neq 0$ jest nierozkładalny. Czy wynika z tego że wielomian $a_n + a_{n-1}X + \cdots + a_0X^n$ jest nierozkładalny?

   Dowód. Tak. Można przekonać się bezpośrednim rachunkiem, że jeżeli $a_n+a_{n-1}X+\cdots+a_0X^n = (b_k+b_{k-1}X+\cdots+b_0X^k)(c_l+c_{l-1}X+\cdots+c_0X^l)$, $k,l \geq 1$ jest rozkładem, to $a_0+a_1X+\dots a_nX^n = (b_0+b_1X+\dots b_kX^k)(c_0+c_1X+\dots c_lX^l)$ też jest rozkładem. Można rachunków uniknąć rozpatrując równość $a_n + a_{n-1}X + \cdots + a_0X^n = (b_k + b_{k-1}X + \cdots + b_0X^k)(c_l + c_{l-1}X+\cdots+c_0X^l)$ w ciele funkcji wymiernych $K(X)$, mnożąc obie strony równości przez $\frac{1}{X^n}$ a potem podstawiając $\frac{1}{X} = Y$, Tak zrobiło kilka osób. (:. □

19.1.2019

Kolokwium Algebra I* - Część II

Zadanie 1 Niech $a, b \in \mathbb{Z}$, $a > 1$, $b \neq 0$. W pierścieniu ilorazowym $\mathbb{Z}/(a)$ rozpatrzmy system multyplikatywny $S = \{b^n + (a) \colon n \geq 0\}$, przy czym przyjmujemy, że $b^0 = 1$.

a) *(6 pkt)* Obliczyć $S^{-1}\mathbb{Z}/(a)$.

Dowód. Niech $a - p_1^{n_1} \dots p_k^{n_k}$ bedzie rozkładem a na iloczyn potęg parami różnych liczb pierwszych. Wówczas $\mathbb{Z}/(a) \cong \prod_{i=1}^{k} \mathbb{Z}/(p_i^{n_i})$. Pkażemy, że $S^{-1}\mathbb{Z}/(a) \cong \prod_{p_i \nmid b} \mathbb{Z}/(p_i^{n_i})$. Niech $\pi : \mathbb{Z}/(a) \to \prod_{p_i \nmid b} \mathbb{Z}/(p_i^{n_i})$ będzie naturalną projekcją. Zauważmy, że $\pi(b + (a))$ jest odwracalne w $\prod_{p_i \nmid b} \mathbb{Z}/(p_i^{n_i})$. Z uniwersalnej własności lokalizacji mamy przemienny diagram:

$$\begin{array}{ccc} \mathbb{Z}/(a) & \xrightarrow{S^{-1}} & S^{-1}\mathbb{Z}/(a)\ . \\ {\scriptstyle\pi}\big\downarrow & \swarrow_{\varphi} & \\ \prod_{p_i \nmid b} \mathbb{Z}/(p_i^{n_i}) & & \end{array}$$

Pokażemy, że φ jest izomorfizmem.

Z przemienności diagramu i faktu, że π jest epimorfizmem wiemy, że φ jest epimorfizmem.

Obraz $\varphi(\frac{x+(a)}{b^l+(a)}) = \pi(x + (a))\pi(b + (a))^{-l} = 0$ wtedy i tylko wtedy, gdy $0 = \pi(x + (a)) \in \prod_{p_i \nmid b} \mathbb{Z}/(p_i^{n_i})$, czyli dla $1 \leq i \leq k$ takich, że $p_i \nmid b$, $p_i^{n_i} \mid x$. Jeżeli m jaest liczbą naturalną większą bądź równą $max\{n_j\}$ dla tych j, że $p_j \mid b$. Wówczas $b^m(x + (a)) = 0$ w $\mathbb{Z}/(a)$, co oznacza, że $S^{-1}(x + (a)) = 0$ i $\frac{x+(a)}{b^l+(a)=0}$.

□

b) *(5 pkt)* Dla jakich a, b homomorfizm $\mathbb{Z}/(a) \to S^{-1}\mathbb{Z}/(a)$ jest monomorfizmem?

Dowód. Jądro $\ker S^{-1} = \{x + (a) \colon \exists_{m\in\mathbb{N}}\ b^m(x + (a)) = 0\}$, czyli istnieje $m \in \mathbb{N}$ takiże $a \mid b^m x$. Zatem lokalizacja jest monomorfizmem wtedy i tylko wtedy, gdy a i b są względnie pierwsze. □

Zadanie 2*(9 pkt)* Niech K będzie ciałem i niech $I \lhd K[X, Y]$ będzie ideałem, $I = (X - XY^2, Y^3)$. Niech $R = K[X, Y]/I$. Pokazać, że jedynym ideałem pierwszym pierścienia R jest ideał $J = (X + I, Y + I)$.

Dowód. Ideały pierwsze pierścienia R są obrazami przy przekształceniu ilorazowym ideałów pierwszych pierścienia $K[X, Y]$ zawierającymi ideał $(X - XY^2, Y^3)$. Jeżeli P jest takim ideałem, to $Y^3 \in P$, więc $Y \in P$. Skoro tak, to $(X, Y) \subset P$. Jednak $K[X, Y]/(X, Y) = K$, więc (X, Y) jest ideałem maksymalnym a zatem $(X, Y) = P$ i jego obraz jest jedynym ideałem pierwszym pierścienia R. □

Zadanie 3 Niech R będzie dziedziną z jednoznacznością rozkładu, w której każdy ideał pierwszy jest maksymalny.

a) *(7 pkt)* Pokazać, że każdy ideał pierwszy jest główny.

Dowód. Jeżeli $a \in I$ oraz I pierwszy, to musi istnieć nierozkładalny (a więc pierwszy) $c \mid a$, $c \in I$, bo R jest DJR i a jest iloczynem elementów nierozkładalnych. Ideał $(c) \subseteq I$ i (c) jest maksymalny z założenia. Zatem $(c) = I$. □

b) *(8 pkt)* Pokazać,że każdy ideał jest główny. Wskazówka: Założyć nie wprost, że zbiór ideałów, które nie są główne jest niepusty, skorzystać z lematu Zorna i punktu a) dochodząc do sprzeczności.

Dowód. Przypuśćmy, że zbiór X ideałów, które nie są główne jest niepusty. Każdy łańcuch posiada ograniczenie górne, bo suma ideałów, które nie są główne nie jest ideałem głównym. Niech I element maksymalny. On nie jest główny, więc nie jest pierwszy i istnieją a, b, $ab \in I$, $a \notin I$ oraz $b \notin I$. Zatem $(I \cup \{a\})$ oraz $(I \cup \{b\}$ są ideałami głównymi. W pierwszym odruchu bierzemy ideał główny $(I \cup \{a\})(I \cup \{b\})$, ale ten ideał nie jest równy I - może być jego właściwym podideałem - trzeba więc wziąć coś większego. Niech $(I \cup \{a\}) = (u)$. Niech $J = \{r \in R \colon ar \in I\}$. Oczywiście $b \in J$ i $I \subsetneq J$, więc z maksymalności I, $J = (v)$. Oczywiście $(I \cup \{a\})J = (uv)$. Pokażemy, że tym razem już $(I \cup \{a\})J = I$.

Mamy $u = i + ar$ dla pewnych $i \in I$ oraz $r \in R$. Zatem $uv = iv + avr$. Ponieważ $v \in J$, to $av \in I$, więc $uv \in I$, co dowodzi $(uv) \subseteq I$. Dla wykazania inkluzji przeciwnej niech $x \in I$ będzie dowolnym elementem ideału I. Ponieważ $I \subseteq (u)$, to $x = ur$ dla pewnego $r \in R$, ale także $a = ur'$ dla $r' \in R$. Zauważmy, że $ar = ur'r = xr' \in I$ więc $r \in J$ (tu jest różnica - r nie musi należeć do $(I \cup \{b\}$!) i $r = r"v$. Zatem $x = uvr"$, czyli $x \in I$ co dowodzi inkluzji $I \subseteq (uv)$.

Sprzeczność - zatem zbiór X jest pusty, czyli każdy ideał jest główny. □

11 Seria XI - Rozszerzenia ciał

11.1. Niech $f(X) = X^3 - X^2 + X + 2 \in \mathbb{Q}[X]$ będzie wielomianem nierozkładalnym. Niech $L = K[X]/(f)$. Oznaczmy przez $a \in L$ pierwiastek w L wielomianu f.

a) Przedstawić iloczyn $(a^2 + a + 1)(a^2 - a)$ jako kombinację liniową wektorów bazy $1, a, a^2$ przestrzeni L nad K.

Dowód. -4a-2 □

b) Przedstawić $(a - 1)^{-1}$ jako kombinację liniową wektorów bazy $1, a, a^2$ przestrzeni L nad K

Dowód. Mamy $1 = \frac{1}{3}(a^3 - a^2 + a + 2) - \frac{1}{3}(a - 1)(a^2 + 1)$ (ogólnie stosujemy algorytm Euklidesa). Zatem $(a - 1)^{-1} = -\frac{1}{3}(a^2 + 1)$. □

c) Znaleźć wielomian $g \in \mathbb{Q}[X]$ dla którego $g(a) = (a - 1)^{-1}$.

Dowód. Taki wielomian jest postaci $h(X)(X^3 - X^2 + X + 2) - \frac{1}{3}(a^2 + 1)$, gdzie h jest dowolnym wielomianem. □

11.2. Czy ciało $625 = 5^4$ elementowe zawiera podciało 125 elementowe?

Dowód. **NIE** – Ciało 5^4 elementowe jest rozszerzeniem stopnia 4 nad $\mathbb{Z}_5$ i stopień rozszerzenia dowolnego ciała pośredniego musiałby dzielić 4, a $3 \nmid 4$. □

11.3. Przedstawić $\sqrt{2}$ jako wielomian o współczynnikach wymiernych od $\sqrt{2} + \sqrt{3}$.

Dowód. Niech $a = \sqrt{2} + \sqrt{3}$. Wówczas $\sqrt{2} = \frac{1}{2}(a^2 - 5) - 2a$. □

11.4. Niech $K \subseteq L$ będzie rozszerzeniem algebraicznym. Niech R będzie pierścieniem, takim że $K \subseteq R \subseteq L$. Czy wynika z tego, że R jest ciałem?

Dowód. **TAK** – Możemy założyć, że $K \neq R$. Niech $a \in R \setminus K$. Ponieważ $K \subseteq L$ jest rozszerzeniem algebraicznym, to $[K(a) : K] < \infty$. Przekształcenie $\varphi : K(a) \to K(a)$ zadane wzorem $\varphi(x) = ax$ jest przekształceniem liniowym skończenie wymiarowej przestrzeni liniowej $K(a)$ nad K, które jest monomorfizmem. Jest więc ono izomorfizmem i istnieje $b \in K(a) \subseteq R$ dla którego $ab = 1$. □

11.5. Niech $K \subset L$ będzie rozszerzeniem skończonym. Niech dla $a \in L$, $\varphi_a \colon L \to L$ będzie zadane wzorem $\varphi_a(x) = ax$. Niech f_a będzie wielomianem charakterystycznym przekształcenia liniowego φ_a. Czy $f_a(a) = 0$?

Dowód. Z algebry liniowej wiemy, że $f_a(\varphi_a)$ jest przekształceniem zerowym. Łatwy rachunek pokazuje, że $f_a(\varphi_a)(x) = f_a(a)x$, a zatem $f_a(a) = 0$ □

11.6. Skonstruować ciało 7^3 elementowe.

Dowód. Wystarczy znaleźć nierozkładalny wielomian (f) stopnia 3 nad $\mathbb{Z}_7$ i wziąć $\mathbb{Z}_7[X]/(f)$. Takim wielomianem jest na przykład $X^3 + 2$. □

To była ostatnia seria - nie oddajemy jej. Dziękuję Wam za udział w zajęciach.