1 Grupy - wiadomości wstępne

1.1. Udowodnić, że w dowolnej grupie G, dla dowolnych dw"och element"ow x, $y \in G$, $o(xy) = o(yx)$.

1.2. Sprawdzić, że macierze postaci

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \qquad a, b, c \in \mathbb{R}, ac \neq 0$$

, tworzą podgrupę w $GL(2, \mathbb{R})$ i znaleźć w niej elementy rzędu 2. Wskazać dwa elementy rzędu dwa, których iloczyn ma rząd nieskończony.

1.3. Pokazać, że podgrupa dowolnej grupy skończonej generowana przez dwa nieprzemienne elementy rzędu dwa jest izomorficzna z grupą dihedralną.

1.4. Niech x, $y \in G$, przy czym $\langle x \rangle \cap \langle y \rangle = \mathbf{1}$. Pokazać, że jeżeli x i y są przemienne, to $\langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle$.

1.5. Niech x, $y \in G$, przy czym $o(x) = n < \infty$, a $o(y) = m < \infty$. Pokazać, że jeżeli $(n, m) = 1$ oraz x i y są przemienne, to $o(xy) = mn$.

1.6. Niech $x \in G$ i $o(x) = n$. Pokazać, że dla każdej liczby naturalnej $k \in \mathbb{N}$, $(k, n) = 1$ istnieje $y \in G$, dla którego $y^k = x$.

1.7. Jeżeli $\varphi : G \to H$ jest epimorfizmem, a $K \leqslant H$ dowolną podgrupą, to $[G : \varphi^{-1}(K)] = [H : K]$.

1.8. Niech $|G| = n$. Niech $\varphi : G \to \Sigma_n$ będzie homomorfizmem Cayleya. Rozłożyć na cykle rozłączne elementy obrazu $\varphi(G)$.

1.9. Udowodnić, że w skończonej grupie abelowej iloczyn wszystkich elementów jest równy iloczynowi elementów rzędu 2. Zastosować to stwierdzenie do grupy $\mathbb{Z}_p^*$ i wykazać Tw. Wilsona: $(p-1)! \equiv -1 \pmod{p}$.

1.10. Niech G będzie taką grupą, że część wspólna wszystkich podgrup nietrywialnych jest podgrupą nietrywialną. Pokazać, że każdy element G jest skończonego rzędu.

1.11. *Definicja: Podgrupę właściwą H grupy G nazywamy maksymalną, jeżeli nie istnieje właściwa podgrupa $K \leq G$, $K \neq H$ taka, że $H \leq K \leq G$.*

Pokazać, że jeżeli grupa skończona G ma dokładnie jedną podgrupę maksymalną, to G jest grupą cykliczną i $|G| = p^m$, gdzie p jest liczbą pierwszą i $m > 0$.

2 Grupy - działania

2.1. Pokazać, że jeżeli $H \leqslant G$ jest właściwą podgrupą skończonego indeksu, to zbiór $\bigcup_{g\in G} gHg^{-1}$ jest właściwym podzbiorem zbioru elementów grupy G. Pokazać rozpatrując podgrupę $S^1 \leqslant SO(3)$, że założenie skończoności indeksu jest istotne.

2.2. Znaleźć klasy sprzężoności elementów grupy D_{2n}.

2.3. Czy istnieje grupa, która ma dokladnie 36 elementów rzędu 7?

2.4. Znaleźć działania grupy D_{12} na zbiorze siedmioelementowym o dokładnie trzech orbitach.

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

2.6. Udowodnić, że dla każdej liczby $k \in \mathbb{N}$ istnieje liczba M_k, taka że jeżeli dla skończonej grupy G, $k(G) = k$, to $|G| \leq M_k$. Wykazać, że istnieje skończona liczba grup skończonych o zadanej liczbie klas sprzężoności.

2.7. Niech grupa skończona G działa na skończonym zbiorze X. Udowodnić wzór Burnside'a:

$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |X^g|$$

gdzie $|X/G|$ oznacza liczbę orbit działania G na X, a $|X^g|$ liczbę punktów stałych przekształcenia wyznaczonego przez $g \in G$.

3 Skończone podgrupy grupy $SO(3)$

Niech $G \leqslant SO(3)$ będzie skończoną podgrupą grupy $SO(3)$ ortogonalnych przekształceń przestrzeni euklidesowej trójwymiarowej. Rozważamy działanie G na dwuwymiarowej sferze $S^2 \subset \mathbb{R}^3$ podzbiór

$$B = \{x \in S^2 \colon G_x \neq \{1\}\}.$$

Zbiór B jest skończony i G - niezmienniczy oraz ma parzystą liczbę elementów. Każde ortogonalne przekształcenie $\mathbb{R}^3$ jest bowiem obrotem wokół pewnej osi, która przebija sferę S^2 w dwóch punktach, nazwijmy je biegunami. Zbiór B jest sumą biegunów elementów należących do G.

Załóżmy, że działanie G na zbiorze B ma n orbit $O_1, \ldots, O_n$ o rzędach grup izotropii $a_1, \ldots, a_n$, $a_i > 1$ dla $i = 1, \ldots, n$. Ze wzoru Burnside'a otrzymujemy:

$$n = \frac{1}{|G|}(2(|G| - 1) + |B|),$$

gdzie $|B|$ oznacza moc zbioru B. Przekształcamy ten wzór i dostajemy

$$n = \frac{1}{|G|}(2(|G| - 1) + \Sigma_{i=1}^{n} \frac{|G|}{a_i})$$

$$n = (2(1 - \frac{1}{|G|}) + \Sigma_{i=1}^{n} \frac{1}{a_i})$$

$$\Sigma_{i=1}^{n}(1 - \frac{1}{a_i}) = 2(1 - \frac{1}{|G|})$$

Liczba po prawej stronie równania należy do odcinka $[1, 2)$ a zatem $2 \leq n \leq 3$.

3.1. Pokazać, że jeżeli $n = 2$, to G jest grupą cykliczną obrotów wokół tej samej osi.

3.2. Pokazać, że jeżeli $n = 3$, to zakładając, że $2 \leq a_1 \leq a_2 \leq a_3$ jedyne możliwości opisuje poniższa tabela

a_1	a_2	a_3	$\|G\|$	$\|O_1\|$	$\|O_2\|$	$\|O_3\|$
2	2	$k(k \geq 2)$	$2k$	k	k	2
2	3	3	12	6	4	4
2	3	4	24	12	8	6
2	3	5	60	30	20	12

3.3. Pokazać, że w przypadku $(2, 2, k)$ mamy grupę symetrii podwójnego stożka nad k – kątem foremnym, czyli D_{2k}.

3.4. Pokazać, że w przypadku $(2, 3, 3)$ mamy grupę symetrii czworościanu, która jest izomorficzna z grupą A_4.

3.5. Pokazać, że w przypadku $(2, 3, 4)$ mamy grupę symetrii ośmiościanu (lub rownoważnie sześcianu), która jest izomorficzna z grupą Σ_4.

3.6. Pokazać, że w przypadku $(2, 3, 5)$ mamy grupę symetrii dwunastościanu (lub rownoważnie dwudziestościanu), która jest izomorficzna z grupą A_5.

4 Podgrupy normalne. Abelianizacja

4.1. Pokazać, że jeżeli $H \trianglelefteq G$, to każda podgrupa grupy G/H jest postaci K/H, gdzie $K \leqslant G$ jest podgrupą zawierającą H. Ponadto udowodnić, że $K/H \trianglelefteq G/H$ wtedy i tylko wtedy, gdy $K \trianglelefteq G$, i że wówczas

$$G/H \Big/ K/H \cong G/K.$$

4.2. Niech $H \trianglelefteq G$. Niech $\pi : G \longrightarrow G/H$ będzie rzutowaniem, a $K \leqslant G$ podgrupą. Udowodnić, że

a) $\pi^{-1}(\pi(K)) = K \cdot H = \{k \cdot h\colon\ k \in K, h \in H\} \leqslant G$. Ponadto $K \cdot H = H \cdot K = \langle\, K \cup H \,\rangle$

b) $K/(K \cap H) \cong (K \cdot H)/H$.

c) podać przykłady podgrup $H \leqslant G$ i $K \leqslant G$, takich że $K \cdot H$ nie jest podgrupą grupy G.

4.3. Rozpatrzmy grupę dihedralną D_{2n}.

a) Znaleźć abelianizację grupy D_{2n}.

b) Niech $n \geq 3$. Udowodnić, że jeżeli n jest nieparzyste, to $Z(D_{2n}) = 1$, a jeżeli n jest parzyste to $D_{2n}/Z(D_{2n}) \cong D_n$.

c) Pokazać, że podgrupa grupy obrotów grupy dihedralnej jest normalna. Pokazać, że jeżeli $k \cdot l = n$, to $D_{2n}/\langle\, \rho^k \,\rangle \cong D_{2k}$.

4.4. Wykazać, że jeżeli w grupie G istnieje podgrupa skończonego indeksu, to istnieje zawarta w niej podgrupa normalna skończonego indeksu.

4.5. Niech $N \trianglelefteq G$ i $|N| < \infty$. Niech $H \leqslant G$, $|G : H| < \infty$ i $(|G : H|, |N|) = 1$. Pokazać, że $N \leqslant H$.

Dowód. Niech $K = NH$. Oczywiście nadal $(|K : H|, |N|) = 1$. Rozpatrzmy przekształcenie zbiorów skończonych $f : N \to K/H$, $f(x) = xH$. Przekształcenie to jest "na" i zauważmy, że $f(x) = f(y)$ wtedy i tylko wtedy, gdy $y^{-1}x \in N \cap H$. Mamy więc bijekcję zbiorów warstw $N/N \cap H$ i K/H. Moce tych zbiorów dzielą $|N|$ i $|K : H|$, które są względnie pierwsze. Zatem $|N/N \cap H| = 1$, co kończy dowód. □

4.6. Pokazać, że jeżeli G jest grupą skończenie generowaną, a $m \in \mathbb{N}$ liczbą naturalną, to w G istnieje co najwyżej skończona liczba podgrup indeksu m.

Dowód. Każda podgrupa H indeksu m wyznacza homomorfizm $G \to \Sigma_m$ - jak G jest skończenie generowana to takich homomorfizmów jest skończenie wiele. Podgrupa H występuje jako grupa izotropii pewnego punktu - inne grupy izotropii są z nią sprzężone. Podgrup sprzężonych z H jest $|G : N_G(H)| < \infty$, bo H jest skończonego indeksu. □

4.7. Pokazać, że jeżeli p jest najmniejszą liczbą pierwszą dzielącą $|G|$ i $H \leqslant G$, $|G : H| = p$, to $H \trianglelefteq G$.

4.8. Udowodnić, że jeżeli $[G, G] \leqslant H \leqslant G$, to $H \trianglelefteq G$.

4.9. Jeżeli G jest skończoną grupą przemienną i $n \mid |G|$, to w grupie G istnieje podgrupa rzędu n i podgrupa indeksu n.

Dowód. Wystarczy pokazać jedno ze stwierdzeń. Pokażemy indeks. Dowód przez indukcję ze względu na rząd. Dla grup rzędu pierwszego teza jest jasna. Niech p będzie liczbą pierwszą dzielącą $\frac{|G|}{n}$. Z tw. Cauchy'ego istnieje $x \in G$, $o(x) = p$. Z zał indukcyjnego w $G/ < p >$ istnieje podgrupa indeksu n, bo $n \mid |G/ < p > |$.Jej przeciwobraz przy $\pi : G \to G/ < p >$ jest szukaną podgrupą. □

4.10. Niech G będzie grupą skończoną. Pokazać, że G zawiera podgrupę normalną indeksu p, gdzie p jest liczbą pierwszą, wtedy i tylko wtedy, gdy $p \mid |G/[G,G]|$.

4.11. Udowodnić, że jeżeli $|G| = 2r$, $r > 1$ i r jest liczbą nieparzystą, to G nie jest grupą prostą. (Wskazówka: rozpatrzeć rozkład na cykle rozłączne obrazów elementów grupy G przy homomorfizmie z tw. Caleya)

4.12. Niech $H \leqslant G$. Rozpatrzmy działanie G na zbiorze warstw G/H przez mnożenie z lewej strony i ograniczmy je do podgrupy $K \leqslant G$. Pokazać, że warstwa gH jest punktem stałym działania grupy K wtedy i tylko wtedy, gdy $K \leqslant gHg^{-1}$. W szczególności, jeżeli $K = H$, to $(G/H)^H = N_G(H)/H$

4.13. (Hölder) Niech $H \trianglelefteq G$, gdzie G jest grupą skończoną a H grupa prostą. Pokazać, że jeżeli $|H|^2$ nie dzieli $|G|$, to H jest jedyną podgrupą G izomorficzną z H.

Dowód. Przypuśćmy, że H' izo z H i różne od H. Z prostoty H' mamy $H \cap H' = \{1\}$ lub $H \cap H' = H'$. Ten drugi przypadek oznacza, że $H = H'$. W pierwszym przypadku $\pi_H : G \to G/H$ ograniczone do H" jest monomorfizmem, ale to oznacza, że $|H'| \mid |G/H|$ czyli $|H|^2 \mid |G|$. □

Definicja. *Grupę G nazywamy* ***doskonałą*** *jeżeli* $[G,G] = G$.

4.14. Niech G będzie grupą doskonałą, a $K \trianglelefteq G$ podgrupą cykliczną normalną. Pokazać, że $K \leqslant Z(G)$.

4.15. Pokazać, że grupa $SL(2, \mathbb{Z}_p)$, $p > 3$ jest doskonała. Znaleźć jej centrum.

4.16. Udowodnić, że jeżeli G jest grupą doskonałą, to centrum grupy ilorazowej $G/Z(G)$ jest trywialne. (lemat Grüna)

Dowód. Niech $\pi : G \to G/Z(G)$ i niech $Z' = \pi^{-1}(Z(G/Z(G))$. Zauważmy, że dla $z \in Z'$, $\pi([g,z]) = 0$, czyli $[g,z], [z,g] \in Z(G)$ dla każdego $g \in G$. Dla $z \in Z'$ definiujemy $\varphi_z : G \to G$, $\varphi_z(g) = [g,z]$. To jest homomorfizm, bo $\varphi_z(gg') = gzg^{-1}z^{-1}g'zg'^{-1}z^{-1} = gzg^{-1}[z^{-1},g']z^{-1} = gz[z^{-1},g']g^{-1}z^{-1} = \varphi_z(g)\varphi_z(g')$. Rozpatrzmy $\pi\varphi_z : G \to G/Z(G)$ - jest to homomorfizm zerowy, a więc $\mathrm{im}(\varphi_z) \subseteq Z(G)$ a więc $[G,G] \leqslant \ker(\varphi_z)$. Z doskonałości φ_z jest homomorfizmem zerowym, czyli $z \in Z(G)$. □

5 Grupy permutacji

5.1. W A_n, $n \geq 3$ znaleźć podgrupę generowaną przez 3-cykle.

5.2. Udowodnić, że dla $n \geq 3$, $Z(\Sigma_n) = 1$.

5.3. Niech $\sigma \in A_n$. Pokazać, że klasa sprzężoności w Σ_n elementu σ jest równa jego klasie sprzężoności w A_n jeżeli $C_{\Sigma_n}(\sigma) \not\subseteq A_n$ lub jest sumą dwóch różnych równolicznych klas sprzężoności w A_n jeżeli $C_{\Sigma_n}(\sigma) \subseteq A_n$.

5.4. Rozpatrzmy grupy Σ_4 oraz A_4.

a)Wyznaczyć klasy sprzężoności elementów Σ_4 oraz A_4 .

b)Wskazać dwa elementy A_4, które są sprzężone w Σ_4, a nie są sprzężone w A_4.

c) Znaleźć $Z(A_4)$.

d) Wykazać, że w A_4 istnieje tylko jedna podgrupa rzędu 4, więc jest ona charakterystyczna.

e) Udowodnić, że w A_4 nie istnieje podgrupa rzędu 6.

f) Znaleźć $[A_4, A_4]$.

6 Rozszerzenia. Produkty i produkty półproste

6.1. Niech $G \cong H \times K$. Załóżmy, że H nie jest izomorficzna z żadną podgrupą K. Czy $H \times \{1\}$ jest jedyną podgrupą G izomorficzną z H?

Udowodnimy następujące twierdzenie:

Twierdzenie 1. *Niech H, K będą grupami, a $\theta_i \colon K \to Aut(H)$ $(i = 1, 2)$ homomorfizmami. Niech $G_i = H \rtimes_{\theta_i} K$ będą odpowiadającymi produktami półprostymi. Niech H_i, K_i będą kanonicznymi obrazami H oraz K w G_i.*

$(\star)$ *Jeżeli istnieją izomorfizmy $\alpha : H \to H$ i $\beta : K \to K$ dla których przemienny jest diagram*

$$\begin{array}{ccc} K & \xrightarrow{\theta_1} & Aut(H) \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\varphi_\alpha} \\ K & \xrightarrow{\theta_2} & Aut(H), \end{array}$$

gdzie φ_α jest automorfizmem wewnętrznym grupy $Aut(H)$ wyznaczonym przez α, to istnieje izomorfizm $\Phi : G_1 \to G_2$, taki że $\Phi(H_1) = H_2$.

Jeżeli H jest grupą przemienną i izomorfizm Φ jak wyżej istnieje, to warunek $(\star)$ jest spełniony.

Dowód. Jeżeli $(\star)$ zachodzi, to definiujemy $\Phi : G_1 \to G_2$ wzorem

$$\Phi(h,k) = (\alpha(h), \beta(k)).$$

Jeżeli Φ istnieje, to niech $\tilde{\Phi} : G_1/H_1 \to G_2/H_2$ będzie izomorfizmem indukowanym. Niech $\alpha : H \to H$ i $\beta : K \to K$ będą złożeniami naturalnych izomorfizmów:

$$\alpha\colon H \xrightarrow{\sim} H_1 \xrightarrow{\Phi} H_2 \xrightarrow{\sim} H$$

$$\beta\colon K \xrightarrow{\sim} K_1 \xrightarrow{\sim} G/H_1 \xrightarrow{\tilde{\Phi}} G/H_2 \xrightarrow{\sim} K_2 \xrightarrow{\sim} K$$

Wystarczy sprawdzić, że przy tych definicjach i przemienności grupy H odpowiedni diagram jest przemienny. □

Jeżeli H nie jest grupą przemienną, to sytuacja jest bardziej skomplikowana i nie będziemy jej roztrząsać .

Definicja. *Niech G będzie grupą. Przekrojem grupy G nazywamy parę podgrup $K \leqslant L \leqslant G$ taką, że $K \trianglelefteq L$.*

6.2. Niech $K \leqslant G \times H$. Niech $G_1 = \{x \in G\colon \exists_{y \in H}(x,y) \in K\}$ zaś $G_2 = \{x \in G\colon (x,1) \in K\}$. Pokazać, że

a) $G_2 \leqslant G_1 \leqslant G$ jest przekrojem G.

b) Udowodnić, że $\phi : G_1/G_2 \to H_1/H_2$ dane wzorem $\phi(xG_2) = yH_2$, gdzie y jest dowolnym elementem dla którego $(x,y) \in K$, jest izomorfizmem.

c) Pokazać, że jeżeli $G_2 \leqslant G_1 \leqslant G$ oraz $H_2 \leqslant H_1 \leqslant H$ są przekrojami zaś $\phi : G_1/G_2 \to H_1/H_2$ izomorfizmem, to wyznacza to podgrupęproduktu $G \times H$.

6.3. Udowodnić następujące stwierdzenia:

a) Jeżeli $K \trianglelefteq G$ i $L \trianglelefteq G$ oraz $K \cap L = \{1\}$. Jeżeli KL/L ma dopełnienie w G/L, to K ma dopełnienie w G.

b) Niech K będzie taką grupą, że $Z(K) = 1$. Wówczas dla każdej grupy G, takiej że $K \trianglelefteq G$, K ma dopełnienie wtedy i tylko wtedy, gdy $Inn(K)$ ma dopełnienie w $Aut(K)$.

Dowód. Ponieważ $Z(K) = 1$, to $InnK \cong K$ i $K \trianglelefteq Aut(K)$. Zatem dowodu wymaga tylko implikacja "⇐".

Rozważmy homomorfizm $\varphi : G \to Aut(K)$ i jego obraz. Mamy $\varphi(K) = Inn(K) \leqslant \varphi(G) \leqslant Aut(K)$. Niech $H \leqslant Aut(K)$ będzie dopełnieniem K w $AutK$. Wówczas $H \cap \varphi(G)$ jest dopełnieniem $Inn(K)$ w $\varphi(G)$. Ponieważ $\ker(\varphi) = C_G(K)$ oraz $K \cap C_G(K) = Z(K) = \{1\}$, to $Inn(K) \cong K \cong K/K \cap C_G(K) \cong KC_G(K)/C_G(K)$ oraz $\varphi(G) \cong G/C_G(K)$. Zatem $KC_G(K)/C_G(K)$ ma dopełnienie w $G/C_G(K)$ i teza wynika z punktu a). □

6.4. Niech $K \trianglelefteq G$, G skończona. Załóżmy, że $InnK$ ma dopełnienie w $Aut(K)$. Pokazać, że jeżeli $(|G/K|, |Z(K)|) = 1$, to K ma dopełnienie w G.

7 p-Grupy

7.1. Pokazać, że dla p– grupy G, jeżeli r_s jest liczbą podgrup rzędu $p^s \leq |G|$, to $p^s \equiv 1(modp)$.

7.2. Pokazać, że dla p– grupy G, jeżeli n_s jest liczbą podgrup normalnych rzędu $p^s \leq |G|$, to $p^s \equiv 1(modp)$

7.3. Niech G będzie p–grupą. Pokazać, że dowolna właściwa podgrupa $H \leqslant G$ jest właściwą podgrupą swojego normalizatora $N_G(H)$.

7.4. Pokazać, że każda maksymalna podgrupa p- grupy jest normalna i ma indeks p.

7.5. Pokazać, że jeżeli G jest nieabelową grupą rzędu p^3 to $k(G) = p^2 + p - 1$, gdzie $k(G)$ oznacza liczbę klas sprzężoności elementów grupy G.

7.6. Pokazać, że jeżeli G jest p-grupą skończoną a $H \trianglelefteq G$ nietrywialną podgrupą normalną, to $H \cap Z(G) \neq \mathbf{1}$.

8 Wokół twierdzenia Sylowa

8.1. Niech G będzie grupą skończoną , a $H \leqslant G$ jej p–podgrupą Sylowa. Niech $K \trianglelefteq G$ będzie podgrupą normalną i niech $\pi : G \to G/K$ będzie epimorfizmem na grupę ilorazową . Udowodnić, że

a) $H \cap K$ jest p–podgrupą Sylowa grupy K i każda p–podgrupa Sylowa grupy K jest postaci $H' \cap K$, gdzie H' jest pewną p–podgrupą Sylowa grupy G.

b) grupa $\pi(H)$ jest p–podgrupą Sylowa grupy ilorazowej G/K i każda p–podgrupa Sylowa grupy G/K jest postaci $\pi(H')$ gdzie H' jest p–podgrupą Sylowa grupy G.

8.2. Pokazać, że dla liczby pierwszej p istnieje największa p–podgrupa normalna w G i dla grup skończonych jest ona częścią wspólną wszystkich p podgrup Sylowa. Oznaczamy ją $O_p(G)$. Pokazać, że istnieje najmniejsza podgrupa normalna, dla której grupa ilorazowa jest p–grupą.

8.3. Znaleźć podgrupy Sylowa w D_{2n}. Wyznaczyć ich liczbę.

8.4. Znaleźć 2-podgrupę Sylowa w Σ_4. Udowodnić, że jest ona izomorficzna z D_8. Ile różnych 2-podgrup Sylowa zawiera Σ_4?

8.5. Udowodnić, że każda grupa rzędu 85 jest cykliczna.

8.6. Udowodnić, że grupa prosta rzędu 60 jest izomorficzna z A_5.

8.7. Niech $n = p^m r$, gdzie m i r są liczbami naturalnymi, p jest liczbą pierwszą , $r > 1$, $\neg(p \mid r)$. Pokazać, że jeżeli istnieje grupa prosta rzędu $n = p^m r$, to $p^m \mid (r-1)!$. Wywnioskować, że dla $m \geq 4$ nie istnieje grupa prosta rzędu $2^m 5$.

8.8. Udowodnić, że nie ma grupy prostej rzędu 80.

8.9. Udowodnić, że nie ma grupy prostej rzędu 132.

8.10. Udowodnić, że nie ma grupy prostej rzędu 300.

8.11. Udowodnić, że nie istnieje grupa prosta rzędu $351 = 27 \cdot 13$.

8.12. Udowodnić, że nie istnieje grupa prosta rzędu $992 = 32 \cdot 31$.

8.13. Zbadać, czy każda grupa rzędu $17 \cdot 5 \cdot 7$ jest cykliczna.

8.14. Pokazać, że grupa rzędu 255 jest cykliczna.

8.15. Pokazać, że nie ma prostej grupy rzędu $180 = 2^2 3^2 5$.
Wskazówki: Przypuśćmy, że G jest grupą prostą rzędu 180

1) Pokazać, że $n_5 = 36$.
2) Niech H_1, H_2 dwie rożne 3– podgrupy Sylowa. Przypuść my, że $H_1 \cap H_2 \neq \{1\}$, Pokazać, że wówczas $|G : C_G(H_1 \cap H_2)| = 10$. Zauważyć, że to prowadzi do sprzeczności. Zatem $H_1 \cap H_2 = \{1\}$
3) Policzyć liczbę elementów w 3 i 5 podgrupach Sylowa, doprowadzając do sprzeczności.

8.1 Przykład - grupy rzędu 12

Zauważmy, że 2– podgrupa Sylowa jest izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2$ lub z $\mathbb{Z}_4$, zaś 3 – podgrupa Sylowa jest izomorficzna z $\mathbb{Z}_3$.

8.16. Jeżeli G jest grupą przemienną to $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ lub $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.
Oznaczmy 3 – podgrupę Sylowa przez K. Jest ona indeksu 4, więc mamy homomorfizm $\varphi : G \to \Sigma_4$. Jądro tego homomorfizmu, zawarte w K jest równe K lub jest trywialne.

8.17. Pokazać, że jeżeli $\ker\varphi = \{1\}$, to $G \cong A_4$.

Jeżeli $\ker\varphi = K$, to 3 – podgrupa Sylowa jest normalna, 2 – podgrupa jest jej dopełnieniem, zatem G jest produktem półprostym.

8.18. Jeżeli 2 – podgrupa Sylowa jest izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2$, to G jest izomorficzna z D_{12}.

8.19. Jeżeli 2 – podgrupa Sylowa jest izomorficzna z $\mathbb{Z}_4$, to G jest izomorficzna z $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ i jest tylko jeden taki produkt półprosty. Grupa ta jest generowana przez elementy a, b i relacje $a^6 = 1$, $b^2 = a^3 = (ab)^2$.

9 Pierścienie - wiadomości wstępne. Własności elementów pierścienia.

9.1. Udowodnić, że w pierścieniu nieskończonym nie ma elementów niezerowych i nieodwracalnych lub jest ich nieskończenie wiele.

9.2. Niech $f = a_0 + a_1x + ... + a_nx^n \in R[X]$ będzie wielomianem. Pokazać, że:

a) f jest elementem odwracalnym $\iff$ a_0 jest elementem odwracalnym zaś $a_1, ..., a_n$ są elementami nilpotentymi.

b) f jest nilpotentny $\iff$ $a_0, a_1, ..., a_n$ są nilpotentne.

c) f jest dzielnikiem zera $\iff$ istnieje $a \in R$, taki, że $af = 0$.

9.3. Znaleźć elementy odwracalne w pierścieniu szeregów formalnych $R[[X]]$.

9.4. Udowodnić, że jeżeli R jest nieskończoną dziedziną całkowitości, to homomorfizm $\Phi : R[X] \longrightarrow R^R$ dany wzorem $\Phi(f)(a) = f(a)$ jest monomorfizmem.

9.5. Pokazać, że jeżeli x jest elementem nilpotentnym, to $1+x$ jest elementem odwracalnym. Wywnioskować, że suma elementu nilpotentnego i odwracalnego jest elementem odwracalnym.

Definicja. *Element $x \in R$ nazywa się idempotentny, jeżeli $x^2 = x$.*

9.6. Pokazać, że jeżeli $x \in R$ jest elementem idempotentnym, to $x' = 1-x$ jest także elementem idempotentnym. Pokazać, że $xx' = 0$. Pokazać, że podzbiór $P_x = \{rx\colon r \in R\} \subset R$ jest pierścieniem z x jako jedynką, dodawaniem i mnożeniem jak w R (ale nie podpierścieniem R !). Pokazać, że $f : R \to P_x \times P_{x'}$ zadane wzorem $f(r) = (rx, rx')$ jest izomorfizmem. Pokazać, że każy izomorfizm pierścienia R z produktem jest zdefiniowany przez pewien element idempotentny i jego przeciwny.

9.1 Ideały pierścienia

9.7. Pokazać, że jeżeli $S \subset R$ jest systemem multyplikatywnym ($1 \in S$, $x, y \in S \implies xy \in S$), $I \trianglelefteq R$ ideałem, takim że $I \cap S = \emptyset$. Pokazać, że istnieje ideał pierwszy J, $I \subset J$, $J \cap S = \emptyset$.

9.8. Wywnioskowac z poprzedniego zadania, że nilradykał jest częścią wspólną ideałów pierwszych.

Definicja. *Pierścień nazywa się zredukowany wtedy i tylko wtedy, gdy nie zawiera niezerowych elementów nilpotentnych.*

9.9. Niech R będzie pierścieniem, a N jego nilradykałem. Pokazać,że pierścień R/N jest zredukowany.

9.10. Udowodnić, że pierścień $R[X]$ jest dziedziną ideałów głównych wtedy i tylko wtedy gdy R jest ciałem. Podać przykład ideału w $\mathbb{Z}[X]$, który nie jest główny.

Definicja. *Pierścień R nazywamy lokalnym jeżeli zawiera dokładnie jeden ideał maksymalny.*

9.11. Pokazać, że dla pierścienia R następujące warunki są równoważne:

a) suma elementów nieodwracalnych jest elementem nieodwracalnym

b) zbiór elementów nieodwracalnych jest ideałem

c) R jest pierścieniem lokalnym.

9.12. Niech R będzie pierścieniem lokalnym. Udowodnić, że jeżeli $x \in R$ oraz $x^2 = x$ to $x = 0$ lub $x = 1$.

9.13. Udowodnić, że jeżeli $I \subseteq R$ jest ideałem pierwszym, zaś $S = R - I$, to pierścień $S^{-1}R$ jest lokalny.

9.14. Udowodnić, że $k[[X]]$ jest pierścieniem lokalnym, gdzie k jest ciałem.

9.15. Niech $I_1, I_2, ..., I_n$ będą ideałami pierwszymi pierścienia R i niech J będzie ideałem takim, że $J \subseteq \bigcup_{i=1}^{n} I_i$. Udowodnić, że $J \subseteq I_i$ dla pewnego i.

9.16. Niech $J_1, J_2, ..., J_n$ będą ideałami pierścienia R i niech I będzie ideałem pierwszym takim, że $\bigcap_{i=1}^{n} J_i \subseteq I$. Udowodnić, że $J_i \subseteq I$ dla pewnego i. Pokazać, że jeżeli $\bigcap_{i=1}^{n} J_i = I$, to $I = J_i$ dla pewnego i.

9.17. Udowodnić, że jeżeli w pierścieniu R dla każdego elementu x istnieje $n \in N$ (zależne od x), $n > 1$ takie, że $x^n = x$, to każdy ideał pierwszy w R jest maksymalny.

9.18. Niech $I \trianglelefteq R$ będzie ideałem pierwszym. Jeżeli I nie zawiera dzielników zera różnych od zera, to R jest dziedziną całkowitości.

9.19. Niech $\varphi : R \to S$ będzie homomorfizmem pierścieni. Podać przykład ideału maksymalnego $I \trianglelefteq S$ dla którego $\varphi^{-1}(I)$ nie jest ideałem maksymalnym.

9.20. Niech X będzie przestrzenią zwartą a $C(X)$ pierścieniem funkcji ciągłych o wartościach rzeczywistych. Niech $x_0 \in X$. Wówczas:

a) Zbiór $I_{x_0} = \{f \in C(X) \colon f(x_0) = 0\}$ jest ideałem maksymalnym.

b) Pokazać, że jeżeli zbiór funkcji $f_1, \ldots, f_n$ nie ma wspólnych miejsc zerowych, to $(f_1, \ldots, f_n) = R$.

c) Pokazać, że każdy ideał maksymalny $C(X)$ jest postaci I_{x_0}, dla pewnego $x_0 \in X$.

9.21. Pokazać, że jeżeli $(x^2 + 1) \trianglelefteq \mathbb{R}[X]$ jest maksymalny. Jaki jest pierścień ilorazowy?

10 Dziedziny z jednoznacznością rozkładu

10.1. Niech R będzie dziedziną ideałów głównych, a $Q(R)$ jej ciałem ułamków. Niech $S \leqslant Q(R)$ będzie podpierścieniem zawierającym R. Pokazać, że

1. każdy element pierścienia S jest postaci $\frac{a}{b}$, gdzie $a \in R$ i $\frac{1}{b} \in S$
2. S jest dziedziną ideałów głównych.

10.2. Udowodnić, że jeżeli K jest ciałem, to podpierścień $K[X^2, X^5]$ pierścienia $K[X]$ nie jest dziedziną z jednoznacznością rozkładu. (jednoznaczność rozkładu nie dziedziczy się na podpierścienie).

10.3. Niech R będzie dziedziną noetherowską i załóżmy, że dla dowolnych $a, b \in R \setminus \{0\}$, istnieje $NWD(a, b)$ i jest on postaci $ka + lb$. Pokazać, że R jest DIG.

10.1 Dziedziny Euklidesowe

10.4. Niech $K[[X]]$ oznacza pierścień szeregów formalnych nad ciałem K. Niech dla $f \neq 0$,

$$o(f) = min\{n\colon a_n \neq 0\}.$$

Udowodnić, że:

a) $o(fg) = o(f) + o(g)$

b) $f \mid g$ wtedy i tylko wtedy gdy $o(f) \leq o(g)$

c) f jest odwracalny wtedy i tylko wtedy gdy $o(f) = 0$

d) jeżeli $f \neq 0$, to f jest stowarzyszony z $X^{o(f)}$.

e) jedynym elementem nierozkładalnym jest X

f) $K[[X]]$ jest dziedziną ideałów głównych i każdy ideał jest generowany przez X^k dla pewnego k.

g) Czy $K[[X]]$ jest dziedziną Euklidesową?

10.5. W dziedzinie Euklidesowej znaleźć algorytm rozwiązywania układu kongruencji.

10.6. Niech p będzie liczbą pierwszą i zdefiniujmy

$$\mathbb{Z}_p^{\wedge} = \{(a_1, a_2, ...) : a_k \in (\mathbb{Z}/p^k\mathbb{Z}),\, a_{k+1} \equiv a_k \,(mod\, p^k), \quad k \geq 1\}$$

a) Pokazać, że $\mathbb{Z}_p^{\wedge}$ z operacjami dodawania i mnożenia po współrzędnych jest pierścieniem z 1, zawierającym $\mathbb{Z}$ jako podpierścień. (jest to uzupełnienie $\mathbb{Z}$ w metryce p-adycznej).

b) Pokazać, że $\mathbb{Z}_p^{\wedge}$ jest pierścieniem lokalnym i Euklidesowym.

10.2 Pierścień liczb Gaussa $\mathbb{Z}[i]$

10.7. Pokazać, że w rozkładzie na czynniki pierwsze w $\mathbb{Z}$ liczby naturalnej będącej sumą kwadratów $l = m^2 + n^2$ każdy czynnik postaci 4k-1 występuje w potędze parzystej. Znaleźć wszystkie liczby całkowite, które można przedstawić w postaci sumy kwadratów dwóch liczb całkowitych.

10.8. Pokazać, że istnieje nieskończenie wiele liczb pierwszych postaci $4k + 1$ oraz postaci $4k + 3$.

10.9. Uzasadnić, że poniższy układ kongruencji ma rozwiązanie w pierścieniu $\mathbb{Z}[i]$ i znaleźć to rozwiązanie.

$$\begin{array}{lll} a \equiv & i & (mod\, 1+2i) \\ a \equiv & 1 & (mod\, 7) \\ a \equiv & 1+2i & (mod\, 3) \end{array} .$$

Zadania trudniejsze "na ochotnika" do zreferowania na zajęciach. Można rozwiązywać zespołowo.

10.10. Niech R będzie dziedziną euklidesową, która nie jest ciałem. Pokazać, ze istnieje niezerowy nieodwracalny element $c \in R$, takie że dla każdego $a \in R$ istnieją $q, r \in R$ dla których $a = qc + r$, przy czym $r = 0$ lub r odwracalny.

10.11. Rozpatrzmy $\mathbb{Q}[\sqrt{-19}]$ z waluacją $v(a + b\sqrt{-19}) = a^2 + b^2 19$. Niech

$$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}] = \{a + b\frac{1+\sqrt{-19}}{2} : \ a, b \in \mathbb{Z}\} \leqslant \mathbb{Q}[\sqrt{-19}]$$

a) Pokazać, że waluacja przyjmuje wartości $0, 1, 4, 5$ oraz, że $v(a+b\frac{1+\sqrt{-19}}{2}) \geq 5$ jeżeli $b \neq 0$.

b) Pokazać, że elementami odwracalnymi są ± 1.

c) Pokazać, że jeżeli $c \in \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ miałoby spełniać warunek z poprzedniego zadania, to c musiałoby być dzielnikiem 2 lub 3 w $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ i być równe ± 2 lub ± 3.

d) Pokazać, że nie istnieją $q, r \in \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ dla których $\frac{1+\sqrt{-19}}{2} = qc + r$ dla $c = \pm 2$ lub $c = \pm 3$ i $r = 0$ lub $r = \pm 1$.

e) Wywnioskować, że $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ nie jest dziedziną euklidesową.

10.12. Udowodnimy, że dziedzina $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ z poprzedniego zadania jest dziedziną ideałów głównych.

Definicja. *Niech R będzie dziedziną całkowitości. Funkcję $v : R\setminus\{0\} \to \mathbb{N}\cup\{0\}$ nazywamy waluacją Dedekinda -Hasse, jeżeli dla dowolnych $a, b \in R\setminus\{0\}$ mamy $(a, b) = (b)$ lub istnieje $r \in (a, b)$ takie, że $v(r) < v(b)$.*

Pokazać, że:

a) waluacja Euklidesowa jest waluacja Dedekinda- Hasse;

b) dziedzina R jest DIG wedy i tylko wtedy, gdy można na nim zdefiniować waluację Dedekinda- Hasse.

c) pokazać, że zdefiniowana w przykładzie powyżej waluacja na pierścieniu $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ jest waluację Dedekinda- Hasse.

Twierdzenie 2. Fermata dla pierścienia $\mathbb{C}[\mathbf{X}]$. *W pierścieniu $\mathbb{C}[X]$ równanie*

$$f^n + g^n = h^n$$

nie ma rozwiązań dla $n > 2$ i f, g, h nie będących wszystkie wielomianami stałymi.

10.13. Udowonić twierdzenie Fermata dla pierścienia $\mathbb{C}[X]$. Wskazówki: Dowodzić nie wprost.

1. zauważyć, że można założyć, że $NWD(f, g, h) = 1$
2. w $\mathbb{C}[X]$ wielomian $1 - X^n = \prod_{i=1}^{n}(1 - \zeta^i X)$, gdzie ζ jest n – tym pierwotnym pierwiastkiem z 1. Wywnioskować, że $f^n = \prod_{i=1}^{n}(h - \zeta^i g)$;
3. pokazać, że każdy czynnik $(h - \zeta^i g)$ jest n–tą potęgą.
4. niech $h - g = a^n$, $h - \zeta g = b^n$, $h - \zeta^2 g = c^n$ (bo n>2). Pokazać, że istnieją $\alpha, \beta, \gamma \in \mathbb{C}$, dla których $(\alpha a)^n + (\beta b)^n = (\gamma c)^n$. Pokazać,że prowadzi to do sprzeczności.

10.14. Stosując analogiczne rozumowanie udowodnić twierdzenie Fermata dla $\mathbb{Z}$ i $n = 3, 4$.

10.15. Jeżeli R jest dziedziną całkowitości, w której każdy ideał pierwszy jest główny, to R jest DIG.

10.16. Jeżeli pierścień R jest dziedziną z jednoznacznością rozkładu, w której każdy ideał pierwszy jest maksymalny, to R jest dziedziną ideałów głównych.

10.3 Jednoznaczność rozkładu w pierścieniach wielomianów.

10.17. Niech R będzie dziedziną z jednoznacznością rozkładu, zaś K jej ciałem ułamków. Udowodnić, że jeżeli dla $d \in R$ równanie $a^2 = d$ ma rozwiązanie w K, to ma rozwiązanie w R. Znaleźć kontrprzykład jeżeli R nie jest dziedziną z jednoznacznością rozkładu.

10.18. Niech R będzie dziedziną z jednoznacznością rozkładu. Udowodnić, że

$$f(X, Y) = X^4 + 2Y^2X^3 + 3Y^3X^2 + 4YX + 5Y + 6Y^2$$

jest nierozkładalny w $R[X, Y]$.

10.19. Zbadać, które z niżej podanych wielomianów są nierozkładalne w pierścieniu $\mathbb{Z}[X]$ i $\mathbb{Q}[X]$:

a) $2X^8 + 22X^3 - 66X + 44$

b) $X^4 - 21$

c) $X^3 - 7X^2 + 3X + 3$

d) $X^{p-1} + X^{p-2} + ... + X + 1$, gdzie p jest liczbą pierwszą.

e) $(X - a_1)(X - a_2)...(X - a_n) - 1$, gdzie $a_1, a_2, ..a_n$ są różnymi liczbami całkowitymi.

f) $X^4 + 15X^3 + 7$. (Wskazówka: Zredukować modulo 5.)

g) $X^n - p$, gdzie p jest liczbą pierwszą.

10.20. Niech R będzie dziedziną z jednoznacznością rozkładu i niech $f = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$. Pokazać, że jeżeli f ma pierwiastek w ciele ułamków R, to pierwiastek ten leży w R.

10.21. Znaleźć ciało ułamków pierścienia $\mathbb{Z}[X, Y]/(X^2 + Y^2)$

11 Rozszerzenia ciał

11.1. Pokazać,że $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

11.2. Niech $K \subset K(a)$ i niech a będzie elementem przestępnym nad K. Niech $K \subset L \subset K(a)$. Pokazać, że $L \subset K(a)$ jest rozszerzeniem algebraicznym.