Zadania do wykładu prof. Wojciech Gajda
Algebra 1
Zima 2021

Zadanie 1. Znaleźć rzędy wszystkich elementów w grupie G jeżeli:
(a) G=$\mathbf{Z}/16$ (b) G=$(\mathbf{Z}/36)^{\times}$ (c) G=Q_8 (d) G=D_5 (e) G=$\mathbf{Z}/2 \times \mathbf{Z}/8$
(f) G=S_4.

Zadanie 2. Obliczyć rząd elementu g w grupie G jeżeli:

(a) g=$\mathcal{O}_{270^o}$, G=D_4

(b) g=i, G=Q_8

(c) $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, G=$GL_2(\mathbf{F}_3)$

(d) g=$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 5 & 6 & 4 & 8 & 7 \end{pmatrix}$, G=S_8.

Zadanie 3. Ile elementów rzędu n posiada grupa G jeżeli:

(a) n=4, G=A_5

(b) n=6, G=$\mathbf{Z}/16$

(c) n=6, G=S_4

(d) n=6, G=S_6

(e) n=12, G=S_8

(f) n=10, G=$\mathbf{Z}/200$

(g) n=4, G=$\mathbf{Z}/24$?

Zadanie 4. Znaleźć wszystkie elementy rzędu 12 w grupie $\mathbf{Z}/360$.

Zadanie 5. Wyznaczyć wszystkie podgrupy w grupach: $\mathbf{Z}/6$, D_4, Q_8, S_3, $\mathbf{Z}/36$, $(\mathbf{Z}/18)^{\times}$, $\mathbf{Z}/3 \times \mathbf{Z}/3$, $S_3 \times \mathbf{Z}/2$, $GL_2(\mathbf{F}_2)$.

Zadanie 6. Wyznaczyć najmniejszy generator w grupach: $(\mathbf{Z}/22)^{\times}$, $(\mathbf{Z}/27)^{\times}$, $(\mathbf{Z}/59)^{\times}$.

Zadanie 7*. Niech G będzie podgrupą w $GL_2(\mathbf{Z})$ generowaną przez macierze: $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Pokazać, że G składa się z ośmiu elementów oraz, że G jest izomorficzna z D_4.

Zadanie 8. Niech będą dane elementy a, b i c grupy G. Dowieść, że:

(a) $\operatorname{rz} a = \operatorname{rz}(a^{-1})$

(b) $\operatorname{rz} a = \operatorname{rz}(bab^{-1})$

(c) $\operatorname{rz}(ab) = \operatorname{rz}(ba)$

(d) $\operatorname{rz}(abc) = \operatorname{rz}(bca)$.

Zadanie 9. Niech G będzie grupą cykliczną rzędu n, której generatorem jest $g \in G$. Dowieść, że dla każdego $k \in \mathbf{Z}$ mamy: $\operatorname{rz}(g^k) = \frac{n}{(n,k)}$, gdzie (a, b) oznacza największy wspólny dzielnik liczb całkowitych a i b.

Zadanie 10. Niech G będzie grupą cykliczną. Dowieść, że:

(a) Jeśli G jest grupą nieskończoną, to $G \simeq \mathbf{Z}$.

(b) Jeśli G jest grupą n-elementową, to $G \simeq \mathbf{Z}/n$.

(b) Jeśli G jest grupą n-elementową, to dla każdego $d|n$ istnieje dokładnie jedna podgrupa w G złożona z d elementów.

Zadanie 11*. Jeżeli G jest taką grupą, że $g^2 = 1$ dla każdego $g \in G$, to G jest grupą abelową.

Zadanie 12. Podaj przykłady, lub dowiedź, że nie ma:

(a) grupy nieskończonej w której istnieje właściwa podgupa skończona

(b) grupy skończonej rzędu > 3, która nie posiada podgrup właściwych

(c) grupy nieskończonej, która nie ma podgrup właściwych.

Zadanie 13. Niech H będzie podgrupą w grupie G oraz niech $a, b \in G$.

(a) Pokazać, że $Ha = Hb$ wtedy i tylko wtedy, gdy $ab^{-1} \in H$.

(b) Zdefiniujmy relację: $a\mathcal{R}b$ wtedy i tylko wtedy, gdy $ab^{-1} \in H$. Sprawdzić, że $\mathcal{R}$ jest relacją równoważności oraz, że Ha jest klasą abstrakcji a względem relacji $\mathcal{R}$.

(c) Sprawdzić, że opdowiedniość $aH \to Ha^{-1}$ określa bijekcję zbioru lewo- i prawostronnych warstw H w G.

Zadanie 14. Niech H będzie podgrupą w G indexu 2. Dowieść, że H jest dzielnikiem normalnym grupy G.

Zadanie 15. Niech H bedzie podgrupą w S_3 generowaną przez transpozycję $\tau = (1, 2)$. Wyznaczyć warstwy lewo- i prawostronne H w S_3 i sprawdzić czy H jest dzielnikiem normalnym.

Zadanie 16. Wyznaczyć wszystkie dzielniki normalne grup Q_8 i D_4 oraz obliczyć odpowiadające im grupy ilorazowe. Pokazać, że $SL_n(K)$ jest dzielnikiem normalnym w $GL_n(K)$. Obliczyć $GL_n(K)/SL_n(K)$.

Zadanie 17*. Niech $D_n =< r,\, s \quad | \quad r^n = s^2 = 1,\, rs = sr^{-1} >$ będzie grupą izometrii $n-$kąta foremnego. Sprawdzić, że D_n składa się z $2n$ elementów. Niech k będzie liczbą naturalną, która dzieli n. Pokazać, że $H =< r^k >$ jest dzielnikiem normalnym w D_n oraz, że $D_n/H \cong D_k$. Grupę D_n nazywamy $n-$tą **grupą dihedralną**.

Zadanie 18. Dla grupy G definiujemy **centrum**:

$$Z(G) \quad = \quad \{h \in G: \quad gh = hg \quad \text{dla wszystkich } g \in G\}.$$

(a) Obliczyć $Z(S_3)$, $Z(Q_8)$ i $Z(D_4)$.

(b) Dowieść, że $Z(G)$ jest dzielnikiem normalnym G.

Zadanie 19. Dowieść, że każdy element grupy ilorazowej $\mathbf{Q}/\mathbf{Z}$ ma skończony rząd.

Zadanie 20*. Sprawdzić, że A_4 nie posiada podgrupy rzędu 6, a w S_4 nie ma dzielników normalnych rzędów 3 i 8.

Zadanie 21. Sprawdzić czy podzbiór H grupy G jest podgrupą normalną, jeśli:

(a) $H{=}\{\mathcal{O}_{0^o}, symetria\}, \quad G{=}D_4$

(b) H jest podgrupą grupy abelowej G

(c) $H = \{A \in GL_3(\mathbf{F}_3): \quad A{=}\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\}, \qquad G{=}GL_3(\mathbf{F}_3).$

Zadanie 22. Znaleźć conajmniej jeden, nietrywialny homomorfizm:

(a) ϕ: $\mathbf{Z}/3 \longrightarrow \mathbf{Z}/9$

(b) ϕ: $\mathbf{Z}/15 \longrightarrow \mathbf{Z}/9$

(c) ϕ: $\mathbf{Z}/20 \longrightarrow \mathbf{Z}/12$

(d) ϕ: $D_4 \longrightarrow Q_8$

(e) ϕ: $S_4 \longrightarrow S_3$

(f) ϕ: $S_3 \longrightarrow D_4$.

Zadanie 23. Wyznaczyć wszystkie homomorfizmy grup:

(a) ϕ: $\mathbf{Z}/3 \longrightarrow \mathbf{Z}$

(b) ϕ: $S_3 \longrightarrow \mathbf{Z}/11$

(c) ϕ: $\mathbf{Z}/6 \longrightarrow \mathbf{Z}/6$

(d) ϕ: $\mathbf{Z}/12 \longrightarrow \mathbf{Z}/18$

(e)* ϕ: $D_4 \longrightarrow Q_8$.

Zadanie 24. Uzasadnić dlaczego grupy G_1 i G_2 nie są izomorficzne:

(a) $G_1{=}\mathbf{R}^\times, \quad G_2{=}\mathbf{C}^\times$

(b) $G_1{=}(\mathbf{R},+), \quad G_2{=}(\mathbf{Q},+)$

(c) $G_1{=}Q_8, \quad G_2{=}D_4$

(d) $G_1{=}D_{12}, \quad G_2{=}S_4$

(e) $G_1{=}S_n, \quad G_2{=}S_m$, gdzie $n \neq m$

(f) $G_1{=}Q_8, \quad G_2{=}\mathbf{Z}/8$.

Zadanie 25. Korzystając z pierwszego twierdzenia o izomorfiźmie dowieść, że: $\quad \mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/n, \quad D_4/\{obroty\} \simeq \mathbf{Z}/2, \quad GL_n(K)/SL_n(K) \simeq K^\times$.

Zadanie 26*. Niech G będzie grupą. Przyjmujemy oznaczenia:

$$Aut\,(G) = (\{\sigma : G \longrightarrow G, \sigma \text{ jest automorfizmem}\}, \quad \circ)$$

$$Int\,(G) = (\{\sigma_a : G \longrightarrow G\colon \sigma_a(g){=}aga^{-1}\}, \quad \circ)$$

gdzie $\circ$ oznacza operację składania funkcji. Dowieść, że $Int\,(G)$ jest podgrupą w $Aut\,(G)$ oraz, że $Int\,(G) \simeq G/Z(G)$, gdzie $Z(G)$ oznacza centrum grupy G, które zostało zdefiniowane w Zadaniu 18. $Int\,(G)$ nosi nazwę **grupy automorfizmów wewnętrznych** grupy G. Skonstruować izomorfizm grup: $Aut\,(\mathbf{Z}/n) \simeq (\mathbf{Z}/n)^\times$, obliczyć $Int\,(\mathbf{Z}/n)$.

Zadanie 27*. Niech G będzie grupą, a H jej podgupą. Dowieść, że H jest podgrupą normalną, jeżeli:

(a) $|G| = 33, \quad |H| = 11$

(b) $|G| = 15, \quad |H| = 5$

(c) $|G| = 35, \quad |H| = 7$

(d) $|G| = pn, \quad |H| = p$, gdzie $p > n$ jest liczbą pierwszą.

Zadanie 28. Niech G będzie grupą. Dowieść, że następujące warunki są równoważne:

(a) G jest grupą abelową

(b) funkcja ϕ: $G \longrightarrow G$ dana wzorem $\phi(g)=g^{-1}$ jest homomorfizmem grup

(c) funkcja ψ: $G \longrightarrow G$ dana wzorem $\psi(g)=g^2$ jest homomorfizmem grup.

Zadanie 29*. Niech G będzie grupą dla której $G/Z(G)$ jest grupą cykliczną. Dowieść, że wtedy G jest abelowa.

Zadanie 30. W grupie G określamy relację w następujący sposób: $a \sim b$, wtedy i tylko wtedy, gdy $a = gbg^{-1}$ dla pewnego $g \in G$.

(a) Sprawdzić, że $\sim$ jest relacją równoważności.

(b) Klasa abstrakcji elementu a względem relacji $\sim$ jest równa klasie sprzężoności C_a.

(c) Zawsze zachodzi: $a \in C_a$. Ponadto $C_a = \{a\}$ wtedy i tylko wtedy, gdy $a \in Z(G)$.

(d) $|C_a| = [G : C(a)]$, gdzie $C(a) = \{g \in G: \quad gag^{-1} = a\}$ jest centralizatorem elementu a w grupie G.

Zadanie 31*. Korzystając z opisu klas sprzężoności w grupie S_5 pokazać, że grupa A_5 nie posiada właściwych dzielników normalnych.
Uwaga: Grupę, która nie ma właściwych dzielników normalnych nazywamy **grupą prostą**. Przykładami grup prostych, poza A_5, są grupy cykliczne $\mathbf{Z}/p$ rzędu liczba pierwsza. Podczas wykładu z algebry ALG 312, dowiedziemy, że dla każdego $n>4$, grupa alternująca A_n jest prosta.

Zadanie 32. Jeżeli X jest zbiorem, to symbolem $Sym(X)$ oznaczamy zbiór wszystkich bijekcji $\sigma\colon X \to X$. Sprawdzić, że z działaniem składania funkcji $Sym(X)$ stanowi grupę. Oczywiście, $S_n = Sym(X)$, gdzie $X = \{1, 2, \dots, n\}$.

Zadanie 33. Niech $f\colon G \times X \to X$ będzie działaniem grupy G na zbiorze X. Pokazać, że f indukuje homomorfizm grup $\phi\colon G \to Sym(X)$ określony za pomocą wzoru: $\phi(g)(x)=f(g,x)$ dla $g \in G$ i $x \in X$. Obliczyć $ker\, \phi$.

Zadanie 34. Niech $f\colon G \times X \to X$ będzie działaniem grupy G na zbiorze X. Określamy relację $\sim$ na zbiorze X : $x{\sim}y$ wtedy i tylko wtedy, gdy $x=f(g,y)$ dla pewnego $g \in G$.

(a) Sprawdzić, że $\sim$ jest relacją równoważności.

(b) Klasa abstrakcji elementu x względem relacji $\sim$ jest równa orbicie Gx.

(c) Wywnioskować z (b), że zbiór X jest sumą rozłącznych orbit w działaniu G na X.

Zadanie 35*. Niech $S^1 = \{e^{2\pi it} = \cos(2\pi t) + i\sin(2\pi t): \quad t \in [0,1)\}$ oznacza okrąg jednostkowy na płaszczyźnie zespolonej. Niech

$$S^2 = \{x = (x_1, x_2, x_3) \in \mathbf{R}^3 : \ x_1^2 + x_2^2 + x_3^2 = 1\}$$

będzie brzegiem kuli jednostkowej w przestrzeni euklidesowej $\mathbf{R}^3$.

(a) S^1 z działaniem mnożenia liczb zespolonych jest grupą przemienną, która jest izomorficzna z grupą ilorazową $\mathbf{R}/\mathbf{Z}$.

(b) Określamy działanie $f: S^1 \times S^2 \to S^2$ za pomocą wzoru:

$$f(e^{2\pi it}, x) = (x_1\cos(2\pi t) - x_2\sin(2\pi t),\ x_1\sin(2\pi t) + x_2\cos(2\pi t),\ x_3).$$

Obliczyć orbity i stabilizatory punktów z S^2 przy tym działaniu.

Zadanie 36. Wyznaczyć klasę sprzężoności elementu g w grupie G.

(a) $g = (1\,2), \qquad G = S_3$

(b) $g = symetria, \qquad G = D_4$

(c) $g = (1\,2)(3\,4), \qquad G = S_5$

(d) $g = i, \qquad G = Q_8$.

Zadanie 37*. Dowieść, że $Z(S_n)$ jest grupą trywialną dla każdego $n > 2$.

Zadanie 38. Niech p będzie liczbą pierwszą. Niech G będzie grupą skończoną taką, że liczba p dzieli $|G|$.

(a) Zdefiniujmy zbiór $X = \{(g_1, g_2, \dots g_p) \in G^p : \quad g_1 g_2 \dots g_p = 1\}$. Niech $f: \mathbf{Z}/p \times X \to X$ będzie funkcją określoną wzorem:

$$f(\bar{1},\ (g_1, g_2, \dots g_p)) = (g_2, g_3, \dots g_p, g_1),$$

gdzie $\bar{1}$ jest generatorem grupy $\mathbf{Z}/p$ oraz $(g_1, g_2, \dots g_p) \in X$. Sprawdzić, że f definiuje działanie grupy $\mathbf{Z}/p$ na zbiorze X.

(b) Ile elementów liczy zbiór X ?

(c) Niech $X_0 = \{g \in G: \quad g^p = 1\}$. Korzystając z rozkładu zbioru X na rozłączne orbity działania z (a) (patrz Zadanie 34 (c)), dowieść, że $|X_0| > 1$.

(d) Wywnioskować z (c) twierdzenie Cauchy'ego: *W grupie skończonej, której rząd dzieli się przez liczbę pierwszą p, istnieje element rzędu p.*

Zadanie 39*. Niech p będzie liczbą pierwszą. Mówimy, że grupa G jest **p−grupą**, jesli każdy element z G, różny od 1 ma rząd, który jest potęgą liczby p. Na przykład, Q_8 i D_4 są 2−grupami, a $\mathbf{Z}/125$ jest 5−grupą.

(a) Dowieść, że skończona grupa G jest $p-$grupą wtedy i tylko wtedy, gdy rząd $|G|$ jest potęgą liczby p.

(b) Korzystając z równania klas z wykładu, dowieść, że centrum skończonej $p-$grupy jest nietrywialną grupą.

Zadanie 40. Niech p będzie liczbą pierwszą. Pokazać, że każda grupa rzędu p^2 jest abelowa.

Zadanie 41. W grupie G dane są dzielnik normalny N oraz podgrupa H. Dowieść, że HN jest podrupą w G.

Zadanie 42. Dowieść, że iloczyn grup $G\times H$ jest grupą cykliczną, jeśli $|G|=p$ oraz $|H|=q$, gdzie p i q są różnymi liczbami pierwszymi.

Zadanie 43. Sprawdzić, że $G\times H \simeq H\times G$ oraz $G\times(H\times K) \simeq (G\times H)\times K$, dla dowolnych grup G, H i K.

Zadanie 44. Skonstruować siedem nieizomorficznych grup abelowych rzędu 360. Przykładami takich grup są: $\mathbf{Z}/360$, $\mathbf{Z}/180\times\mathbf{Z}/2$ i $\mathbf{Z}/90\times\mathbf{Z}/4$.

Zadanie 45. Dowieść, ze grupa, któa ma tylko skończoną liczbę podgrup jest skończona.

Zadanie 46. Niech G będzie dowolną grupą. Oznaczmy przez G' podgrupę w G generowaną przez elementy postaci $[a,b]{:=}aba^{-1}b^{-1}$, dla $a,b \in G$. Pokazać, że:

(a) G' jest dzielnikiem normalnym w G

(b) G/G' jest grupą abelową

(c) jeśli H jest dzielnikiem normalnym w G takim, że G/H jest grupą abelową, to $G' \subset H$.

Zadanie 47. Czy grupa może być sumą mnogościową dwóch swoich właściwych podgrup ?

Zadanie 48*. Pokazać, że grupy rzędu: 33, 35 i 259 są grupami abelowymi.

Zadanie 49. (**Iloczyn i suma prosta dowolnej rodziny grup**)
Niech $\{G_i\}_{i\in I}$ będzie rodziną grup. Na iloczynie kartezjańskim

$$\prod_{i\in I} G_i = \{(x_i){:}\quad x_i \in G_i \quad \text{dla } i \in I\}$$

określamy mnożenie $(x_i)(y_i) = (x_i y_i)$. Sprawdzić, że z tak określonym mnożeniem zbiór $\prod_{i\in I} G_i$ stanowi grupę, która gdy $I=\{1,\, 2,\, \ldots, n\}$ równa jest $G_1\times G_2\times \ldots \times G_n$. Niech

$$\bigoplus_{i\in I} G_i \quad = \quad \{(x_i) \in \prod_{i\in I} G_i\colon \quad x_i{=}1_{G_i}\text{dla prawie wszystkich } i \in I\}.$$

Dowieść, że $\bigoplus_{i\in I} G_i$ jest podgrupą w $\prod_{i\in I} G_i$, która jest pdogrupą właściwą wtedy i tylko wtedy, gdy zbiór indeksów I jest nieskończony. Grupa $\prod_{i\in I} G_i$ nosi nazwę **iloczynu zewnętrznego** rodziny $\{G_i\}_{i\in I}$. Grupę $\bigoplus_{i\in I} G_i$ nazywamy **sumą prostą zewnętrzną** tej rodziny.

Zadanie 50*. (**Iloczyn półprosty grup**)
Niech bedą dane dwie grupy H i N oraz homomorfizm grup $\phi\colon H \longrightarrow Aut\,(N)$, który odpowiada działaniu grupy H na grupie N. Na zbiorze $H{\times}N$ określamy mnożenie:

$$(h_1, n_1)(h_2, n_2) = (h_1 h_2, \phi(h_2)(n_1)n_2)$$

gdzie $h_1, h_2 \in H$, $n_1, n_2 \in N$ oraz $\phi(h_2) : N \longrightarrow N$.

(a) Sprawdzić, że z tak oreślonym mnożeniem zbiór $H{\times}N$ jest grupą. Tą grupę nazywamy **iloczynem półprostym** grup H i N ze względu na homomorfizm ϕ.

(b) Jeśli $\phi(h){=}Id_N$ dla każdego $h \in H$, to iloczyn półprosty jest iloczynem prostym $H{\oplus}N$.

(c) Nieh H będzie podgrupą, a N dzielnikiem normalnym gupy G takimi, że $H{\cap}N{=}\{1\}$ oraz niech $\phi(h)(n){=}h^{-1}nh$ dla $h \in H$ i $n \in N$. Dowieść, że $H{\times_\phi}N \simeq HN$.

(d) Dowieść, że: $S_3 \simeq \mathbf{Z}/2{\times_\phi}\mathbf{Z}/3$, $D_4 \simeq \mathbf{Z}/2{\times_{\phi_1}}\mathbf{Z}/4$, $Q_8 \simeq \mathbf{Z}/2{\times_{\phi_2}}\mathbf{Z}/4$ oraz $A_4 \simeq \mathbf{Z}/3{\times_\phi}(\mathbf{Z}/2{\oplus}\mathbf{Z}/2)$.

Zadanie 51. Które z następujących pierścieni: $\mathbf{Z}/18$, $\mathbf{F}_2[x]/(x^2{+}1)$, $\mathbf{Q}(\sqrt{7}){=}\{a{+}b\sqrt{7}\colon a, b \in \mathbf{Q}\}$, $\mathbf{Z}{\oplus}\mathbf{Z}$, $\mathbf{R}[x]/(x^2{+}1)$, $\mathbf{R}[x]/(x^2{-}5x{+}6)$, $\mathbf{Q}[x]/(x^2{-}5)$ są ciałami ?

Zadanie 52. Które z następujących pierścieni: $\mathbf{Z}/19$, $\mathbf{Q}[x]/(x^2)$, $\mathbf{C}[x]/(x^2{+}1)$, $\mathbf{F}_5[x]/(x^3{+}x{+}1)$, $\mathbf{F}_5[x]/(x^3{+}4x{+}4)$, $\mathbf{R}[x]/(x^2{-}5x{+}6)$, $K[x, y]/(xy{-}1)$, gdzie K jest dowolnym całem, są dziedzinami całkowitości ?

Zadanie 53. Znaleźć wszystkie dzielniki zera, elementy nilpotentne i elementy odwracalne pierścienia: $\mathbf{Z}/20$, $\mathbf{Q}{\oplus}\mathbf{Z}$, $\mathbf{R}[x]/(x^2{-}1)$, $\mathbf{Z}/28$, $M_{2,2}(\mathbf{F}_2)$.

Zadanie 54. Dowieść, że w każdym skończonym pierścieniu przemiennym z jedynką element, który nie jest dzielnikiem zera jest elementem odwracalnym. Obliczyć 2^{-1} w pierścieniu $\mathbf{Z}/n$ jeśli $n{>}\ 2$ jest liczbą nieparzystą.

Zadanie 55.

(a) Dowieść, że pierścień ilorazowy $\mathbf{F}_2[x]/(x^2+x+1)$ jest ciałem 4−elementowym.

(b) Dowieść, że pierścień ilorazowy $\mathbf{F}_2[x]/(x^2)$ nie jest dziedziną całkowitości.

(c) Wyznaczyć wszystkie z dokładnością do izomorfimu pierścienie przemienne z jedynką, które składają się z czterech elementów.

Zadanie 56. Z ilu elementów składa się pierścień A/I jeśli:

(a) $A=\mathbf{F}_3[x], \quad I=(x^2)$

(b) $A=\mathbf{Z}/m[x], \quad I=(x^k)$

(c) $A=\mathbf{F}_7[x], \quad I=(x^5)$

(d) $A=\mathbf{Z}/6[x,y], \quad I=(x^5)+(y^8) \quad ?$

Zadanie 57. Niech X będzie zbiorem. Oznaczmy przez R zbiór wszystkich podzbiorów zbioru X. W R określamy działania:

$$A + B := (A - B) \cup (B - A)$$

$$AB := A \cap B.$$

Sprawdzić, że $(R, +, \cdot, \emptyset, X)$ jest pierścieniem przemiennym z jedynką.

Zadanie 58. Mówimy, że pierścień R jest **pierścineiem Boole'a** jeśli $a^2 = a$ dla każdego $a \in R$. Dowieść, że pierścień Boole'a jest pierścieniem przemiennym oraz, że $a+a=0$ dla każdego elementu a w pierścieniu Boole'a.

Zadanie 59. Nieh A będzie pierścieniem przemiennym z jedynką oraz załóżmy, że istnieje liczba pierwsza p taka, że w A mamy $p1 = 1+1+\ldots+1 = 0$. Dowieść, że:

(a) $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$ dla każdego $a, b \in A$ i liczby naturalenj n

(b) funkcja $\phi : A \longrightarrow A$ zadana wzorem $\phi(a) = a^p$ jest homomorfimem pierścieni z jedynką.

Zadanie 60. Niech A będzie pierścieniem przemiennym z jedynką. Czy grupa addytywna pierścienia $(A, +, 0)$ może być izomorficzna z grupą $\mathbf{Q}/\mathbf{Z}$?

Zadanie 61. Niech A będzie pierścieniem przemiennym z jedynką, a K ciałem. Korzystając z pierwszego twierdzenia o izomorfiźmie dowieść, że:

(a) $A[x]/I \simeq A$, gdzie $I{=}\{f \in A[x] : f(a){=}0\}$ dla ustalonego $a \in A$,

(b) $\mathbf{Q}[x]/(x^2{-}1) \simeq \mathbf{Q}{\oplus}\mathbf{Q}$,

(c) $\mathbf{F}_7[x]/(x^2{+}5) \simeq \mathbf{F}_7{\oplus}\mathbf{F}_7$,

(d) $\mathbf{F}_5[x]/(x^2{+}1) \simeq \mathbf{F}_5{\oplus}\mathbf{F}_5$,

(e) $K[x,y]/(x) \simeq K[y]$,

(f) $K[x,y]/(x^2{-}y) \simeq K[x]$.

Zadanie 62. Dowieść, że $I{=}(2,x){=}2\mathbf{Z}[x]{+}x\mathbf{Z}[x]$ nie jest ideałem głównym pierścienia $\mathbf{Z}[x]$.

Zadanie 63. Podać przykład podpierścienia, który nie jest ideałem.

Zadanie 64.

(1) Czy $K[x]$ jest ciałem, jeśli K jest ciałem ?

(2) Dowieść, że $A[x]$ jest dziedziną całkowitości, jeżeli A jest dziedziną całkowitości.

(3) Obliczyć grupę jedności pierścienia wielomianów $A[x]$, gdy A jest dziedziną całkowitości.

Zadanie 65. Niech $\mathbf{Z}[i] = \{a{+}b\,i\colon \quad a,b \in \mathbf{Z}\} \subset \mathbf{C}$ oznacza pierścień liczb całkowitych Gaussa.

(1) Dowieść, że $\mathbf{Z}[i]$ jest dziedziną całkowitości, ale nie jest ciałem.

(2) Obliczyć grupę jedności $\mathbf{Z}[i]^\times$.

Zadanie 66. Niech A będzie pierścieniem przemiennym z jedynką, który nie posiada ideałówwłaściwych. Dowieść, że A jest ciałem.

Zadanie 67*. Niech A będzie pierścieniem przemiennym z jedynką i niech $R = M_{n,n}(A)$ będzie pierścieniem macierzy $n{\times}n$ o współczynnikach z A.

(1) Załóżmy, że $\mathcal{I}$ jest ideałem obustronnym pierścienia R. Pokazać, że w A istnieje ideał I taki, że $\mathcal{I} = M_{n,n}(I)$. W szczególności, jeżeli A jest ciałem, to w R nie ma obustronnych ideałów właściwych.

Wskazówka. Jeśli $B{=}[b_{ij}]{\in}M_{n,n}(A)$, to $E_{p,r}BE_{s,q}$ jest macierzą, która na przecięciu p-tego wiersza i q-tej kolumny ma b_{rs}, a w pozostałych miejscach ma zera. $E_{i,j}$ oznacza tutaj macierz, która na przecięciu i-tego wiersza i j-tej kolumny ma 1, a w pozostałych miejscach zera. Dla ideału $\mathcal{I}$ z Zadania, rozważyć zbiór I złożony z takich $a \in A$, że $a = b_{11}$ dla pewnego $B{=}[b_{ij}]{\in}\mathcal{I}$.

(2) **Definicja. Centrum pierścienia** R nazywamy zbiór $Z(R)$ złożony z $a \in R$ takich, że dla każdego $b \in R$ jest $ab = ba$. Sprawdzić czy centrum pierścienia jet ideałem.

(3) Pokazać, że centrum pierścienia macierzy $R = M_{n,n}(K)$ o współczynnikach z ciała K składa się z macierzy diagonalnych $\alpha\, I_n$, gdzie $\alpha \in K$.

Zadanie 68. Niech I_1 oraz I_2 będą ideałami pierścienia przemiennego z jedynką A. Niech $\wp$ będzie ideałem pierwszym w A takim, że $I_1 \cap I_2 \subset \wp$. Pokazać, że wtedy $I_1 \subset \wp$ lub $I_2 \subset \wp$.

Zadanie 69. Niech m będzie ideałem pierścienia przemiennego z jedynką A. Dowieść, że m jest ideałem maksymalnym w A, wtedy i tylko wtedy, gdy dla każdego $a \notin m$ istnieje $b \in A$ taki, że $1 - ab \in m$.

Zadanie 70. Następujące trzy warunki są równoważne dla ideału $I \subset \mathbf{Z}$: I jest pierwszy, I jest maksymalny, $I = (p)$ dla liczby pierwszej p. Opisać ideały pierwsze i maksymalne pierścienia reszt $\mathbf{Z}/n$, gdzie $n > 1$.

Zadanie 71*. Mówimy, że pierścień przemienny z jedynką A jest *pierścieniem lokalnym* jeśli w A istnieje dokładnie jeden ideał maksymalny.

(1) Dowieść, że A jest lokalny wtedy i tylko wtedy, gdy dla każdego $a, b \in A$ z tego, że $a{+}b{=}1$ wynika, że $a \in A^\times$ lub $b \in A^\times$.

(2) Jeśli A jest pierścieniem przemiennym z jedynką, m jest ideałem maksymalnym z A, to A/m^n jest pierścieniem lokalnym dla każdego $n > 0$.

Zadanie 72.

(1) Niech $A = \mathbf{Z}/n$ oraz niech $S = \{a \in A: \quad a \neq 0\}$. Obliczyć pierścień ułamków $S^{-1}A$.

(2) Niech $A = \mathbf{Z}/6$ i $S = \{2, 4\}$. Dowieść, że $S^{-1}A$ jest ciałem trzyelementowym.

Zadanie 73*. Niech A będzie dziedziną całkowitości. Dowieść, że w ciele ułamków dziedziny A zachodzi równość

$$A = \bigcap A_m,$$

gdzie przekrój jest wzięty po wszystkich ideałach maksymalnych z A, a A_m oznacza lokalizację A na ideale m.

Zadanie 74. Rozwiązać układy kongruencji:

(1) w $K[x]$:

$$f(x) = 1 \mod (x-1)$$
$$f(x) = x \mod (x^2+1)$$
$$f(x) = x^3 \mod (x+1),$$

gdzie K jest ciałem charakterystyki różnej od 2

(2) w $\mathbf{Z}[i]$:

$$x = i \mod (i+1)$$
$$x = 1 \mod (2-i)$$
$$x = (1+i) \mod (3+4i).$$

Zadanie 75*. Niech p będzie liczbą pierwszą, $f(x) \in \mathbf{F}_p[x]$ unormowanym wielomianem nierozkładalnym stopnia n.

(1) Dowieść, że ideał główny $I = (f(x))$ jest maksymalny oraz, że pierścień ilorazowy $\mathbf{F}_p[x]/I$ jest ciałem, które składa się z p^n elementów.

(2) Niech $A = \mathbf{F}_p[x]/I^m$ dla pewnego $m \in \mathbf{N}$. Wyznaczyć elementy nilpotentne pierścienia A oraz liczbę elementów odwracalnych w A.

(3) Z ilu elementów składa się grupa jedności pierścieni ilorazowych: $\mathbf{F}_2[x]/(x^6-1)$ i $\mathbf{F}_3[x]/(x^6-1)$?

Zadanie 76. (Twierdzenie chińskie o resztach w $\mathbf{Z}$)
Niech $m_1, m_2, \ldots, m_n$ będą liczbami naturalnymi, które są parami względnie pierwsze. Niech będą dane liczby całkowite: $a_1, a_2, \ldots, a_n$.

(a) Dowieść, że istnieje liczba $x \in \mathbf{Z}$ taka, że spełniony jest układ kongruencji $x \equiv a_i \mod m_i$ dla $1 \leqslant i \leqslant n$ oraz, że x jest określona jednoznacznie modulo $m = m_1 m_2 \ldots m_n$.

(b) Przyjmijmy oznaczenie $m_i' = \frac{m}{m_i}$, gdzie $1 \leqslant i \leqslant n$. Zauważmy, że $(m_i, m_i') = 1$. Niech $t_i \in (\mathbf{Z}/m_i)^\times$ będzie takie, że $m_i' t_i \equiv 1 \mod m_i$, gdzie $1 \leqslant i \leqslant n$. Klasę reszt t_i łatwo możemy znaleźć za pomocą algorytmu Euklidesa. Pokazać, że $x = a_1 m_1' t_1 + a_2 m_2' t_2 + \ldots + a_n m_n' t_n$ jest rozwiązaniem układu kongruencji z (a).

(c) Korzystając z (b) rozwiązać dwa układy kongruencji:

$$(1) \qquad x \equiv 1 \bmod 8 \qquad x \equiv 2 \bmod 25 \qquad x \equiv 3 \bmod 81$$

$$(2) \qquad x \equiv 5 \bmod 8 \qquad x \equiv 12 \bmod 25 \qquad x \equiv 43 \bmod 81$$

Zadanie 77. Niech p będzie liczbą pierwszą, $d \in \mathbf{Z}$ liczbą, która nie jest kwadratem liczby całkowitej. W pierścieniu $\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d}\colon \quad a, b \in \mathbf{Z}\}$ rozważmy ideał główny $I = (p) = p\mathbf{Z}[\sqrt{d}]$. Dowieść, że I jest ideałem pierwszym wtedy i tylko wtedy, gdy klasa d reszt modulo p nie jest kwadratem w ciele $\mathbf{F}_p$.

Zadanie 78. Niech p będzie liczbą pierwsą i niech $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbf{Z}[x]$ będzie wielomianem o współczynnikach całkowitych. Oznaczmy przez $\bar{f}(x) = \bar{a}_n x^n + \ldots + \bar{a}_1 x + \bar{a}_0 \in \mathbf{F}_p[x]$ wielomian otrzymany z $f(x)$ za pomocą redukcji współczynników modulo p.

(a) Dowieść, że jeśli $a_n = 1$ oraz $\bar{f}(x)$ jest nierozkładalny w $\mathbf{F}_p[x]$, to $f(x)$ jest nierozkładalny w $\mathbf{Z}[x]$. Czy (a) pozostaje prawdziwe, jeśli $a_n \neq 1$?

(b) Korzystając z (a) (i z lematu Gaussa), sprawdzić, że wielomiany: $f_1(x) = x^4 - 10x^2 + 1$, $f_2(x) = x^3 + 6x^2 + 5x + 25$, $f_3(x) = x^3 + x + 1$ są nierozkładalne w $\mathbf{Q}[x]$.

Zadanie 79.

(a) Wyznaczyć wszystkie pierwiastki wymierne wielomianów: $x^3 - 6x^2 + 15x - 14$, $x^4 - 2x^3 - 8x^2 + 13x - 24$, $6x^4 + 19x^3 - 7x^2 - 26x + 12$.

(b) Wykazać, że wielomiany: $x^3 - 5$, $x^4 + 2$, $x^4 - x^2 + 2$ są nierozkładalne w $\mathbf{Q}[x]$.

(c) Wyznaczyć wszystkie nierozkładalne wielomiany stopnia 2 z $\mathbf{F}_2[x]$.

(d) Ile jest nierozkładalnych wielomianów stopnia 5 w pierścieniu $\mathbf{F}_2[x]$?

Zadanie 80. Które z podanych poniżej ciał są izomorficzne, które są równe parami, a które stanowią pary (podciało, ciało) ?

(a) $\mathbf{Q}$, $\mathbf{Q}(\pi)$, $\mathbf{Q}(i)$, $\mathbf{Q}(i\sqrt{2})$ $\mathbf{Q}(i+\sqrt{2})$, $\mathbf{Q}(i-\sqrt{2})$, $\mathbf{Q}(\sqrt{2}+\sqrt{3})$, $\mathbf{Q}(i, \sqrt{2})$, $\mathbf{Q}(\sqrt{2}-\sqrt{3})$, $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, $\mathbf{Q}(\sqrt{2}, -\sqrt{3})$, $\mathbf{Q}(\sqrt{2}, \sqrt{-3})$, $\mathbf{Z}[x]/(2, x)$, $\mathbf{Q}(\sqrt[4]{-4})$,

(b) $\mathbf{Q}$, $\mathbf{Q}(i)$, $\mathbf{Q}[x]/(x^3+2)$, $\mathbf{Q}[x]/(x^3-2)$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}[x]/(x^2+1)$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(\sqrt[3]{-2})$, $\mathbf{Q}(\sqrt[3]{2}\omega)$, $\mathbf{Q}(\sqrt[3]{2}\omega^2)$, $\mathbf{Q}(\omega)$, $\mathbf{Q}(\sqrt[3]{2}+\omega)$, $\mathbf{Q}[x]/(x^2-2)$, $\mathbf{Q}[x]/(x^2+2)$, $\mathbf{Q}[x]/(x-2)$, $\mathbf{Q}[x]/(x+2)$, $\mathbf{Q}(\sqrt{\omega})$, $\mathbf{Q}[z]/(z^2+z+1)$, gdzie $\omega^3 = 1$ oraz $\omega \neq 1$, $\mathbf{Q}(\omega^2)$, $\mathbf{Q}(x)$.

Zadanie 81*. Niech L/K będzie roszerzeniem algebraicznym ciał oraz niech A będzie dziedziną całkowitości taką, że $K \subset A \subset L$. Dowieść, że A jest ciałem.

Zadanie 82. Obliczyć stopień rozszerzenia $[K : \mathbf{Q}]$, gdy: $K = \mathbf{Q}(\sqrt{10})$, $\mathbf{Q}(\sqrt{2+\sqrt{2}})$, $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, $\mathbf{Q}(\pi)$, $\mathbf{Q}(\omega, \sqrt[3]{3})$, gdzie $\omega^3 = 1$ oraz $\omega \neq 1$.

Zadanie 83. Znaleźć wielomiany minimalne następujących liczb algebraicznych (tzn. elementów algebraicznych nad $\mathbf{Q}$): $\sqrt{3}$, $\sqrt[3]{3}$, $2+\sqrt{2}$, $\sqrt{2+\sqrt{2}}$.

Zadanie 84. Niech $f(x) = x^3-6x^2+8x+3$ oraz $\alpha \in \mathbf{C}$ będzie pierwiastkiem wielomianu $f(x)$. Wyrazić każdy z elementów α^4, α^5, $3\alpha^5-\alpha^4+2$, $(\alpha^2-6\alpha+8)^{-1}$ w bazie $\{1, \alpha, \alpha^2\}$ $\mathbf{Q}-$przestrzeni $K=\mathbf{Q}(\alpha)$.

Zadanie 85.

(a) Niech $I=(2, x^2+x+1)$ będzie ideałem w pierścieniu $\mathbf{Z}[x]$. Dowieść, że $\mathbf{Z}[x]/I$ jest ciałem czteroelementowym.

(b) Niech $I=(5, x^2+x+3)$ będzie ideałem w pierścieniu $\mathbf{Z}[x]$. Dowieść, że $\mathbf{Z}[x]/I \cong \mathbf{F}_5 \times \mathbf{F}_5$ oraz, że w $\mathbf{Z}[x]$ są dokładnie dwa ideały maksymalne: mianowicie $m_1 = (5, x-1)$ oraz $m_2=(5, x-3)$, które zawierają I.

(c) Niech p będzie liczbą pierwszą i niech $g(x) \in \mathbf{Z}[x]$ będzie wielomianem z 1 przy najwyższej potędze i takim, że $\bar{g}(x) \in \mathbf{F}_p[x]$ jest nierozkładalny. Dowieść, że $m=(p, g(x))$ jest ideałem maksymalnym w $\mathbf{Z}[x]$.

(d)* Pokazać, że każdy ideał maksymalny w $\mathbf{Z}[z]$ jest ideałem $(p, g(x))$ dla p i $g(x)$ jak w (c).

Uzupełnienia: II i III twierdzenie o izomorfiźmie*

Zadanie A. Niech H, K będą podgrupami grupy G. Definiujemy zbiór

$$HK = \{hk : \quad h \in H,\, k \in K\}.$$

Pokazać, że HK jest podgrupą w G wtedy i tylko wtedy, gdy $HK=KH$.

Zadanie B. Niech H, N będą podgrupami grupy G przy tym N jest dzielnikiem normalnym. Pokazać, że:

(a) $HN = NH$, czyli na mocy Zadania A, HN jest podgrupą w G.

(b) N jest dzielnikiem normalnym w HN

(c) $H \cap N$ jest dzielnikiem normalnym w H

Zadanie C. (Drugie twierdzenie o izomorfiźmie dla grup)
Niech grupy G, H i N będą takie jak w Zadaniu B. Dowieść, że wtedy:

$$HN/N \simeq H/H \cap N.$$

Zadanie D. (Trzecie twierdzenie o izomorfiźmie dla grup)
Załóżmy, zę H i N są dzielnikami normalnymi grupy G oraz, że $N \subset H$. Pokazać, ze H/N jest dzielnikiem normalnym w grupie ilorazowej G/N oraz, że:

$$G/H \simeq \frac{G/N}{H/N}.$$

Zadanie E. Niech ϕ: $G_1 \longrightarrow G_2$ będzie epimorfimem grup i niech N=$ker\ \phi$. Przyjmujemy oznaczenia:

$$X \quad = \quad \{H \text{ jest podgrupą w } G_1\text{:} \quad N \subset H\}$$

$$Y \quad = \quad \{\bar{H} \text{ jest podgrupą w } G_2\}$$

oraz Φ: $X \longrightarrow Y$ będzie funkcją określoną wzorem $\Phi(H)$=$\phi(H)$.

(a) Dowieść, że Φ jest bijekcją zbiorów.

(b) Niech $H \in X$ oraz $\bar{H}$=$\phi(H)$. Pokazać, że H jest dzielnikiem normalnym w G_1 wtedy i tylko wtedy, gdy $\bar{H}$ jest dzielnikiem normalnym w G_2 oraz, że wtedy
$$G_1/H \simeq G_2/\bar{H}.$$

(c) (Twierdzenie o odpowiedniości podgrup) Zastosować powyżej uzyskane własności (1) i (2) do epimorfizmu kanonicznego π_N: $G \longrightarrow G/N$, gdzie N jest dzielnikiem normalnym grupy G.

Zadanie F. (Drugie twierdzenie o izomorfiźmie dla pierścieni)
Nieh R będzie pierścieniem przemiennym, S jego podpierścieniem oraz, że I jest ideałem w R. Definiujemy zbiór:

$$S + I \quad = \quad \{x{+}y\text{:} \quad x \in S,\ y \in I\}.$$

(a) Dowieść, ze S+I jest podpierścieniem w R.

(b) Pokazać, że I jest ideałem w pierścieni S+I oraz, że $S \cap I$ jest ideałem w S.

(c) Dowieść, że
$$(S{+}I)/I \simeq S/S \cap I.$$

Zadanie G. (Trzecie twierdzenie o izomorfiźmie dla pierścieni)
Niech I i J będą ideałami pierścienia przemiennego R oraz niech $I \subset J$. okazać, że J/I jest ideałem w pierścieniu ilorazowym R/I oraz, że:

$$R/J \simeq \frac{R/I}{J/I}.$$

Zadanie H. Niech I będzie ideałem w pierścieniu przemiennym R i niech $\pi_I \colon R \longrightarrow R/I$ będzie epimorfizmem kanonicznyem $\pi_I(a)=a+I$. Definujemy zbiory:

$$X = \{S \text{ jest podpierścieniem w } R\colon \quad I \subset S\}$$
$$Y = \{T \text{ jest podpierścieniem w } R/I\}$$

oraz $\Phi\colon X \longrightarrow Y$ będzie funkcją $\Phi(S)=S/I$. Ponadto niech $\Psi\colon Y \longrightarrow X$ będzie funkcją daną wzorem $\Psi(T)=\pi_I^{-1}(T)$.

(a) Dowieść, że $\Psi \circ \Phi = Id_X$ oraz $\Phi \circ \Psi = Id_Y$ czyli Φ i Ψ określają bijekcję zbiorów X i Y.

(b) (Twierdzenie o odpowiedniości ideałów) Niech X_{id} (odpowiednio Y_{id}) będzie podzbiorem w X (odpowiednio, w Y) złożonym z ideałów pierścienia R (odpowiednio, pierścienia R/I). Dowieść, że funkcje Φ i Ψ określają bijekcję zbiorów X_{id} i Y_{id}.