Opracowanie zagadnień na egzamin teoretyczny z Algebry

Autorzy
Michał Posiadała
Mikołaj Mijakowski

1. Niech H będzie podgrupą, a G grupą.

   (a) Sformułuj twierdzenie Lagrange'a.

   TW. LAGRANGE'A

   $$\left.\begin{array}{r} G - \text{grupa} \\ H - \text{podgrupa} \\ [G:H] - \text{indeks grupy H w grupie G} \\ \text{(liczba warstw lewostronnych = liczba warstw prawostronnych)} \end{array}\right\} \implies |G| = |H| \cdot [G:H]$$

   (b) Wykaż, że jeśli $aH \cap bH \neq \emptyset$, to $aH = bH$, dla $a, b \in G$.

   Skoro $aH \cap bH \neq \emptyset$ to istnieją takie h, $g \in H$, że $ah = bg$ (element z przecięcia warstw).

   $$ah = bg$$

   $$a = bgh^{-1}$$

   $$a^{-1}b = hg^{-1} \in H$$

   $$a^{-1}b \in H$$

   Warstwy aH i bH są równe.

   Alternatywny dowód: Załóżmy że $z \in aH \cap bH$. Wtedy $z \in aH$, czyli $z = ax$ dla odpowiedniego $x \in H$, więc

   $$zH = axH = \{(xa)h \mid h \in H\} = \{x(ah) \mid h \in H\} = a(xH) = aH$$

   Tak samo dowodzimy, że $zH = bH$, czyli $aH = bH$.

   (c) Wykaż, że liczba warstw lewostronnych grupy G względem podgrupy H jest równa liczbie warstw prawostronnych (bez założenia o skończoności grupy G).

   $$aH = bH$$
   $$\Leftrightarrow$$
   $$b^{-1}a \in \text{H}$$
   $$\Leftrightarrow$$
   $$Ha^{-1} = Hb^{-1}$$

   więc $aH \mapsto Ha^{-1}$ jest różnowartościową funkcją. Jest też surjekcją, więc jest bijekcją między danymi zbiorami warstw, a więc są one równoliczne

2. (a) Podaj dwie różne (oczywiście równoważne) definicje rzędu ($o(a)$) elementu a grupy G.

   RZĄD ELEMENTU

   1. Najmniejsza liczba naturalna n, taka że $a^n = e$ lub ∞ jeśli takie n nie istnieje
   2. Rząd podgrupy (liczba elementów) generowanej przez element a

   (b) Udowodnij, że jeśli $a \in G$ ma rząd skończony oraz $\varphi : G \to H$ jest homomorfizmem grup, to $o(\varphi(a))$ dzieli $o(a)$.

   Niech $o(a) = n$. Wtedy:

   $$a^n = e$$

   $$\varphi(a^n) = \varphi(e) = e$$

   $$\varphi(a) \cdot \varphi(a) \cdot ... \cdot \varphi(a) = e$$

   $$\varphi(a)^n = e$$

   Tak więc rząd $\varphi(a)$ jest dzielnikiem rzędu a, udowodniliśmy więc tezę.

(c) Udowodnij, że jeśli $o(a) = n < \infty$, to $o(a^k) = \frac{n}{NWD(n,k)}$.

Niech $d = NWD(n, k)$, $\quad n = dr$, $\quad k = dm$ i $NWD(r, m) = 1$.

$$(a^k)^r = (a^{dm})^r = (a^{dr})^m = (a^n)^m = e$$

Wobec tego $o(a^k)|r$.
W drugą stronę przez $(a^k)^{o(a^k)} = (a^{o(a^k)})^{dm} = e$
Z tego wynika, że $n|ko(a^k)$, ale $dr|dmo(a^k)$, czyli $r|mo(a^k)$ i skoro r i m względnie pierwsze, to $r|o(a^k)$
Skoro mamy dwie podzielności $r|o(a^k)$ i $o(a^k)|r$, to w $\mathbb{Z}$ mamy $r = o(a^k)$,

3. (a) Podaj definicję permutacji parzystej. Wyjaśnij, dlaczego ta definicja jest poprawna.

Permutacja Parzysta
Permutację σ nazywamy parzystą jeśli można ją przedstawić jako złożenie parzystej liczby transpozycji. Definicja ta jest poprawna, ponieważ dowolne dwa różne przedstawienia σ jako złożenie pewnych transpozycji mają taką samą parzystość liczby elementów.
Ta definicja jest prawidłowa, ponieważ liczba elementów w każdych dwóch różnych złożeniach pewnych transpozycji ma tę samą parzystość (równość modulo 2).

Alternatywna definicja:
Permutację σ nazywamy parzystą jeśli wyznacznik macierzy permutacji jest równy 1 (odpowiednio -1 jeśli jest ona nieparzysta).
Ta definicja jest prawidłowa, ponieważ wiemy, że dla danej permutacji wyznacznik macierzy jest wyznaczony jednoznacznie, więc ma ona tą samą parzystość.

(b) Przedstaw permutację $\sigma = (23145)(678) \in S_{10}$ jako iloczyn pewnej liczby transpozycji.

Mamy:
$$(23145)(678) = (25)(24)(21)(23)(68)(67)$$

(c) Udowodnij, że zbiór A_n permutacji parzystych zbioru $\{1, ..., n\}$ jest podgrupą normalną indeksu 2 w S_n

Rozważmy funkcję
$$\phi : S_n \to \mathbb{Z}_2$$
przypisująca permutacji jej parzystość jest homomorfizmem (bo znak złożenia permutacji jest sumą znaków modulo 2, znak permutacji odwrotnej jest taki sam, a identyczność jest parzysta). Jądro tego homomorfizmu, czyli A_n, jest podgrupą normalną, a z twierdzenia o izomorfizmie grupa ilorazowa jest izomorficzna z $\mathbb{Z}_2$, więc ma dwa elementy, czyli indeks A_n to 2.

4. (a) Podaj definicję podgrupy w grupie G generowanej przez podzbiór $A \subseteq G$.

podgrupy G generowanym przez A
Jeśli $\langle A \rangle$ jest podgrupą G generowaną przez A, to $\langle A \rangle$ jest przecięciem wszystkich podgrup zawierających A.

(b) Załóżmy, że G jest grupą abelową i $a, b \in G$. Opisz wszystkie elementy podgrupy $\langle (a, b) \rangle$ generowanej przez zbiór $\{a, b\}$. Uzasadnij!

Zachodzi $< a, b >= \{a^i b^j \mid i, j \in \mathbb{Z}\}$.
Uzasadnienie
1) Zbiór $\{a^i b^j \mid i, j \in \mathbb{Z}\}$ jest podgrupą
Weźmy $x, y \in \{a^i b^j \mid i, j \in \mathbb{Z}\}$, więc $x = a^k b^l$ oraz $y = a^r b^s$ dla pewnych $k, l, r, s \in \mathbb{Z}$. Wówczas $xy^{-1} = a^k b^l b^{-s} a^{-r} = a^{k-s} b^{l-s} \in \{a^i b^j \mid i, j \in \mathbb{Z}\}$
2) $\langle a, b \rangle \subseteq \{a^i b^j \mid i, j \in \mathbb{Z}\}$
Zauważmy, że $a^1 b^0 = a \in \{a^i b^j \mid i, j \in \mathbb{Z}\}$ oraz $a^0 b^1 = b \in \{a^i b^j \mid i, j \in \mathbb{Z}\}$. Czyli zbiór $\{a^i b^j \mid i, j \in \mathbb{Z}\}$ jest pewną podgrupą zawierającą elementy a oraz b. Z definicji podgrupy generowanej przez zbiór wiemy, że $\langle a, b \rangle$ jest podgrupą będącą przecięciem wszystkich podgrup zawierających a oraz b. Z definicji przecięcia mamy, że podgrupa generowana przez a, b jest podzbiorem każdej podgrupy zawierającej te elementy, więc zachodzi zawieranie.
3) $\{a^i b^j \mid i, j \in \mathbb{Z}\} \subseteq \langle a, b \rangle$
Weźmy dowolny $x \in \{a^i b^j \mid i, j \in \mathbb{Z}\}$. Z definicji $x = a^g b^h$ dla pewnych $g, h \in \mathbb{Z}$. Załóżmy, że $g, h \geqslant 0$. Pokażmy, że $x \in \langle a, b \rangle$. Zauważmy, że skoro $< a, b >$ jest podgrupą i $a \in \langle a, b \rangle$, to $a \cdot \cdots \cdot a \in \langle a, b \rangle$ (przemnożone g razy) dla dowolnej naturalnej liczby g. Wobec tego $a^g \in < a, b >$. Tak samo z b mamy $b^h \in \langle a, b \rangle$. Skoro $a^g \in < a, b >$ oraz $b^h \in < a, b >$, to $a^g b^h = x \in < a, b >$, co było do wykazania.
Przypadki, gdy g, h są ujemne, są analogiczne, tylko wówczas należy rozpatrywać iloczyny odwrotności (które oczywiście należą do $< a, b >$, ponieważ jest to podgrupa).

(c) Uzasadnij, że jeśli G jest grupą cykliczną, to każda podgrupa i każdy obraz homomorficzny G jest grupą cykliczną.

Niech $G = \langle g \rangle$ oraz niech $H \leqslant G$.

Każdy element G (więc też i H) jest postaci g^n. Jeśli H - trywialna, teza oczywiście zachodzi.

Załóżmy że H - nietrywialna. Niech n będzie najmniejszą taką liczbą że $g^n \in H$ i pokażemy że $\langle g^n \rangle = H$.

Niech $e \neq h \in H$. wówczas $h = g^m$ dla pewnego m. Niech $k, r \in \mathbb{N}$, $\quad m = kn + r$ i $r < n$ (po prostu dzielenie z resztą). Wtedy:

$$h = g^m = g^{kn+r} = (g^n)^k g^r \implies g^r = (g^n)^{-k} h$$

A ponieważ $g^n, h \in H \implies g^r \in H$.
Zatem na mocy doboru n oraz nierówności $0 \leqslant r < n$ mamy $r = 0$. Zatem $m = kn$ i wobec tego $h = g^m = g^{nk} = (g^n)^k$

Niech $\varphi : G \to K$ będzie homomorfizmem grup. Ponieważ G jest cykliczna to $G = \langle g \rangle$ i $G = \{g^n : n \in \mathbb{Z}\}$. Wówczas $\varphi(G) = \{\varphi(h) : h \in G\} = \{\varphi(g^n) : n \in \mathbb{Z}\}$ czyli z własności homomorfizmu $\varphi(G) = \{\varphi(g)^n : n \in \mathbb{Z}\} = \langle \varphi(g) \rangle$.

5. (a) Wyjaśnij co to znaczy, że grupa G działa na zbiorze X.

Grupa G działa na zbiorze $X \neq \varnothing$, gdy dla dowolnego $g \in G$ dana jest funkcja $\varphi_g : X \to X$ i zachodzi
$\varphi_h(\varphi_g(x)) = \varphi_{hg}(x)$
$\varphi_e(x) = x$

(b) Udowodnij, że moc orbity $Orb(x)$ elementu $x \in X$ jest równa $[G : G_x]$, gdzie G_x oznacza stabilizator elementu x.

Zauważmy, że $gG_x = hG_x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow \varphi_{g^{-1}h}(x) = x \Leftrightarrow \varphi_h(x) = \varphi_g(x)$. Oznacza to, że przyporządkowanie $gG_x \mapsto \varphi_g(x)$ jest bijekcją pomiędzy $Orb(x)$, a zbiorem warstw.

6. Sformułuj twierdzenie Cauchy'ego.

Niech G będzie skończoną grupą i niech p będzie liczbą pierwszą dzielącą rząd G. Wtedy istnieje taki $x \in G$, że $o(x) = p$.

7. (a) Napisz, co oznacza, że podgrupa H grupy G jest podgrupą normalną. Podaj definicję grupy ilorazowej G/H.

<u>Podgrupa Normalna</u>
H jest podgrupą normalną grupy G, gdy dla dowolnego $a \in G$ mamy $aH = Ha$.
<u>Grupa Ilorazowa</u>
Grupa ilorazowa G/H to $\{aH : a \in G\}$ (tj. zbiór warstw lewostronnych H) z działaniem $aH \cdot bH = abH$.

(b) Wyjaśnij, jak w tej definicji korzysta się z założenia, że H jest podgrupą normalną.

Ponieważ wtedy działanie $aH \cdot bH = abH$ jest dobrze zdefiniowane:
Niech $aH = a'H$ i $bH = b'H$, wtedy $aH \cdot bH = abH$ i $a'H \cdot b'H = a'b'H$. Musimy pokazać, że $abH = a'b'H$. Wiemy, że $a^{-1}a' \in H$ i $b^{-1}b' \in H$ więc $(ab)^{-1}a'b' = b^{-1}a^{-1}a'b'$ istnieje takie $h \in H$ że $b'h = a^{-1}a'b'$ ($b'H = Hb'$ - tu jest wykorzystana normalność), czyli $b^{-1}a^{-1}a'b' = b^{-1}b'h \in H$ (ponieważ H jest zamknięta na mnożenie). Zatem $abH = a'b'H$.

8. (a) Podaj warunki konieczne i dostateczne na to aby grupa G była iloczynem prostym (wewnętrznym) swoich podgrup G_1 i G_2.

Grupa G jest iloczynem prostym wewnętrznym swoich podgrup G_1, G_2 jeśli:
- G_1, G_2 są podgrupami normalnymi grupy G
- $G_1 \cap G_2 = \{e\}$
- $G = G_1 \cdot G_2$

(b) Czy któraś z grup $\mathbb{Z}_{10}$, S_3 jest iloczynem prostym swoich dwóch podgrup właściwych? Każdą z odpowiedzi uzasadnij.

Weźmy dwie podgrupy grupy $\mathbb{Z}_{10}$: $A_1 = \{0,2,4,6,8\} = \langle 2 \rangle$ oraz $A_2 = \{0,5\} = \langle 5 \rangle$. Korzystamy ze stwierdzenia dla grup skończonych: A_1 i A_2 są normalne w $\mathbb{Z}_{10}$ (każda podgrupa grupy abelowej jest normalna), $|A_1| \cdot |A_2| = |\mathbb{Z}_{10}|$ oraz $A_1 \cap A_2 = \{0\}$. Zatem $\mathbb{Z}_{10}$ jest iloczynem prostym swoich podgrup właściwych.

S_3 nie jest takim iloczynem. Rząd S_3 to 6, więc jeśli chcemy rozpisać S_3 jako iloczyn prosty jej podgrup **właściwych**, to żadna z nich nie może mieć rzędu 1. Jedna z tych podgrup musi mieć rząd 2, a druga - 3. Obie są abelowe (i cykliczne). Ale iloczyn dwóch grup abelowych musi być abelowy, a S_3 nie jest abelowe.

9. Sformułuj twierdzenie o izomorfizmie dla grup.

<u>Tw. o Izomorfizmie Grup</u>
Niech $f : G \longrightarrow H$ - epimorfizm grup, a $h : G \longrightarrow G/\ker f$ - homomorfizm naturalny.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "h"'] & H \\ G/\ker f \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

Wtedy $\tilde{f}$ jest jednoznacznie wyznaczonym izomorfizmem grup.

10. (a) Podaj definicję p-podgrupy Sylowa skończonej grupy G.

<u>p - grupa</u>
Grupa której rząd jest równy p^n, dla p-liczby pierwszej i n naturalnej.

<u>p - podgrupa Sylowa</u>
Podgrupę nazywa się p-podgrupą Sylowa, jeśli jest p-grupą i jest największego możliwego rzędu, tzn., jeśli rząd grupy jest równy $p^n r$, gdzie $p \nmid r$ i $n \geqslant 1$, to rząd p-podgrupy Sylowa jest równy p^n.

(b) Sformułuj twierdzenie Sylowa.

<u>Tw. Sylowa</u>
Niech G - skończona grupa, $|G| = p^n m$, $p \nmid m$, $n \geqslant 1$. Oznaczmy s_p jako liczbę p-podgrup Sylowa w G. Wtedy:

1. Istnieje co najmniej jedna p-podgrupa Sylowa w G
2. $s_p \mid |G|$
3. $s_p \equiv 1 \mod p$
4. Każde dwie p-podgrupy Sylowa są sprzężone
5. Każda p-podgrupa w G jest zawarta w pewnej p-podgrupie Sylowa w G

(c) Wyjaśnij, dlaczego jeśli dla liczby pierwszej p dzielącej $|G|$ w grupie G jest tylko jedna p-podgrupa Sylowa, to jest ona podgrupą normalną.

Załóżmy że $H \leqslant G$ jest jedyną p-podgrupą Sylowa. Wiemy że każde sprzężenie podgrupy jest podgrupą, więc
$$gHg^{-1} \leqslant G$$
Wiemy że w grupie skończonej grupa i grupa do niej sprzężona mają ten sam rząd, więc
$$|gHg^{-1}| = |H|$$
ale H jest jedyną podgrupą rzędu H, więc każda grupa gHg^{-1} jest w istocie grupą H. Tak więc H jest sprzężona tylko z sobą samą, jest więc podgrupą normalną.

11. Podaj definicję komutantu $[G,G]$ grupy G. Wyznacz $[S_3,S_3]$ (uzasadnij!)

Komutant jest najmniejszą podgrupą normalną, której grupa ilorazowa jest abelowa, $[G,G] = \langle \{aba^{-1}b^{-1} | a,b \in G\} \rangle$.

$S_3 = \langle a, s : s^2 = a^3 =, sas = a^2 \rangle$. Wystarczy sprawdzić wszystkie możliwe komutatory. Dla $i,j \in \{0,1,2\}$: $a^i a^j a^{-i} a^{-j} = a^{i+j-i-j} = e$, $sss^{-1}s^{-1} = e$, $a^i s a^{-i} s^{-1} = a^{2i}$. Są to wszystkie możliwe kombinacje a,s (oczywiście $as = sa^2$), więc komutant jest złożony ze wszystkich otrzymanych wyników, czyli jest to $\{e, a, a^2\}$.

12. (a) Sformułuj twierdzenie Bezout o pierwiastkach wielomianu $f \in R[x]$ o współczynnikach z pierścienia R.

Tw. Bezout o pierwiastkach wielomianu
Niech $0 \neq f \in R[x]$

$$f(a) = 0 \iff \underset{g \in R[x]}{\exists} g(x) \cdot (x-a) = f(x)$$

Dodatkowo, $\deg g(x) = \deg f(x) - 1$

(b) Udowodnij to twierdzenie.

$\Longleftarrow$
Niech $f(x) = (x-a)g(x)$ dla pewnego $g \in R[x]$, wówczas $f(a) = (a-a)g(a) = 0 \cdot g(a) = 0$.

$\Longrightarrow$
Niech $f(a) = 0$. Dzielimy wielomian f z resztą przez $(x-a)$: $f(x) = (x-a)g(x) + r(x)$ dla pewnych $g,\ r \in R[x]$, ponadto $\deg r < \deg(x-a) = 1$. Mamy $f(a) = 0$, zatem $(a-a)g(a) + r(a) = 0$, więc $0 = 0 + r(a)$ czyli $r(a) = 0$ i jego stopień jest mniejszy niż 1 zatem $r = 0$.

Alternatywny dowód:
Niech $f(x) = a_n x^n + ... + a_0 \in R[x]$.
Korzystając ze wzoru $x^n - y^n = (x-y)(x^{k-1} + x^{k-2}y + ... + y^{k-1})$, zapisujemy:

$$f(x) - f(y) = (x-y)F(x,y), \qquad F(x,y) = \sum_{i,j \leqslant 0} a_{i+j+1} x^i y^i$$

gdzie $a_k = 0$ dla $k > \deg f(x)$
Widać, że $F(x,y)$ jest wielomianem stopnia $n-1$
Zakładając kolejno:

- $f(y) = 0 \implies f(x) = (x-y)F(x,y)$
- $f(x) = (x-y)F(x,y) \implies f(y) = 0$

otrzymujemy tezę

13. Sformułuj twierdzenie o izomorfizmie dla pierścieni.

Tw. O Izomorfizmie Pierścieni
Niech f będzie epimorfizmem pierścieni, a h będzie homomorfizmem naturalnym. Wtedy $\tilde{f}$ jest jednoznacznie wyznaczonym izomorfizmem.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "h"'] & S \\ R/\ker f \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

(Dodatkowo, istnieje wzajemnie jednoznaczna odpowiedniość między ideałami pierścienia $\varphi(R)$ a ideałami R zawierającymi $\ker \varphi$.)

14. (a) Podaj definicję ideału pierścienia R. Podaj definicję ideału pierwszego.

Ideał
Niepusty zbiór $I \subseteq R$ jest ideałem R, jeśli:

- $(I,+)$ jest podgrupą w $(R,+)$, czyli jest spełniony warunek $\underset{a,b \in I}{\forall} a - b \in I$
- Dla każdego $a \in I, \quad r \in R$ mamy $ar \in I$.

Ideał Pierwszy
Mówimy, że ideał $P \subseteq R$ jest pierwszy, gdy $\underset{a,b \in R}{\forall} ab \in P \implies a \in P \vee b \in P$.

(b) Udowodnij, że ideał P pierścienia R jest pierwszy wtedy i tylko wtedy gdy R/P jest dziedziną.

Przypomnijmy definicję ideału pierwszego:

$$ab \in P \implies a \in P \vee b \in P$$

$$\iff$$

$$ab + P = P \implies a + P = P \vee b + P = P$$

$$\iff$$

$$(a+P)(b+P) = P \implies a + P = P \vee b + P = P$$

Czyli w pierścieniu ilorazowym R/P dla $a,\ b \in R/P$ zachodzi:

$$ab = 0 \implies a = 0 \vee b = 0$$

Widzimy więc, że R/P nie ma żadnych dzielników zera (poza zerem), co jest równoważne definicji dziedziny (całkowitości).

(c) Udowodnij, że ideał M pierścienia R jest maksymalny wtedy i tylko wtedy, gdy pierścień R/M jest ciałem.

$\implies$

Niech M będzie ideałem maksymalnym w R oraz $R \ni a \notin M$. Rozważmy ideał w R/M generowany przez $a + M$. Jego przeciwobraz względem homomorfizmu naturalnego jest ideałem w R i jest ostro większy od M (ponieważ $a \notin M$), czyli jest całym pierścieniem (M jest maksymalny). Zatem $1 \in \varphi^{-1}((a+M))$, z czego wynika że $1 + M \in (a+M)R/M$ co zachodzi jedynie jeśli istnieje $b + M \in R/M$ takie, że $(a+M)(b+M) = 1 + M$. Więc $a + M$ jest odwracalny, z dowolności a wiemy, że R/M jest ciałem.

$\impliedby$

Niech M będzie ideałem w R i niech pierścień ilorazowy R/M będzie ciałem. Załóżmy, że $M \subset J \subseteq R$ jest ideałem. Rozważmy zbiór $\varphi(J) = \{j + M : j \in J\}$, gdzie φ jest homomorfizmem naturalnym, ponieważ φ jest epimorfizmem to zbiór ten tworzy ideał w R/M. Jednak R/M jest ciałem, zatem jedyne dwa ideały, jakie w nim występują, to ideał zerowy oraz cały pierścień. Jeśli $\varphi(J) = \{0 + M\}$ to $J \subseteq M$ a więc $M = J$, jeśli $\varphi(J) = R/M$ to $1 + M \in \varphi(J)$ wtedy i tylko wtedy, gdy istnieje $j \in J$ takie, że $j - 1 \in M$. Wówczas $j \in J$, $j - 1 \in J$ czyli $1 = j - (j-1) \in J$ skoro więc $1 \in J$ to $J = R$.

15. (a) Podaj definicję elementu pierwszego dziedziny R. Udowodnij, że element pierwszy jest nierozkładalny.

<u>Element Pierwszy</u> Niech $0 \neq p \in R, p \notin U(R)$.
p jest elementem pierwszym jeśli:

$$\underset{a,b \in R}{\forall} p \mid ab \implies p \mid a \vee p \mid b$$

Załóżmy że p - pierwszy oraz $p = ab$. Z definicji mamy $p \mid a$ lub $p \mid b$. Załóżmy (bez straty ogólności) że $p \mid a$ oraz oczywiście $a \mid p$, więc $a \sim p$, tak więc b musi być odwracalne.

(b) Załóżmy, że R jest dziedziną z jednoznacznością rozkładu. Udowodnij, że każdy element nierozkładalny jest pierwszy.

Załóżmy że $p \in R$ jest elementem nierozkładalnym, gdzie R jest DJR. Niech p dzieli ab, czyli $dp = ab$, $d \in R$.

Musimy pokazać że $p \mid a$ lub $p \mid b$. Jeśli a odwracalne to $pda^{-1} = b$ ($pdb^{-1} = a$), więc $p \mid b$ ($p \mid a$). Jeśli a, b są nieodwracalne, to jako że jesteśmy w DJR, możemy przedstawić je jako iloczyn elementów nierozkładalnych:

$$a = a_1 \cdot a_2 \cdot \ldots \cdot a_n \qquad b = b_1 \cdot b_2 \cdot \ldots \cdot b_m$$

Ale wtedy d jest nieodwracalny, inaczej $p \sim pd \implies pd$ jest nierozkładalny $\implies p = abd^{-1}$ co jest sprzeczne z nierozkładalnością p.

Dlatego d można przedstawią jako iloczyn elementów nierozkładalnych $d = d_1 \cdot d_2 \cdot \ldots \cdot d_k$

$$p \cdot d_1 \cdot d_2 \cdot \ldots \cdot d_k = a_1 \cdot a_2 \cdot \ldots \cdot a_n \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_m$$

Wszystkie czynniki są nierozkładalne zatem $k + 1 = n + m$ i p jest stowarzyszone z którymś pośród a_i lub b_j. Bez straty ogólności $p \sim a_i$, ale $p \sim a_i \mid a$, więc $p \mid a$.

(c) Udowodnij, że jeśli R jest dziedziną idełów głównych i $a \in R$ jest elementem nierozkładalny, to aR jest ideałem maksymalnym w R.

Gdyby dla pewnego $b \in R$ było $aR \subseteq bR$, to musiałoby być $a = bt$ dla pewnego $t \in R$. Jednakże a jest nierozkładalny, więc albo t jest odwracalny i $a \sim b$, czyli $aR = bR$, albo b jest odwracalny, czyli $bR = R$. W takim razie $aR \subsetneq bR$ zachodzi tylko dla $bR = R$.

16. (a) Podaj definicję dziedziny z jednoznacznością rozkładu.

<u>Dziedzina z Jednoznacznością Rozkładu</u>

Niech R będzie dziedziną całkowitości. Jest on dziedziną z jednoznacznością rozkładu wtedy i tylko wtedy gdy:

- dla dowolnego **niezerowego** elementu **nieodwracalnego** $a \in R$ istnieją elementy **nierozkaładalne** $a_1, a_2, ..., a_n \in R$ takie że $a = a_1 \cdot a_2 \cdot ... \cdot a_n$
- Jeśli $a = b$ przyjmując rozkład $a_1 \cdot a_2 \cdot ... \cdot a_n = b_1 \cdot b_2 \cdot ... \cdot b_n$ to oba rozkłady mają tę samą liczbę elementów, a $a_i \sim b_i$ po odpowiednim przenumerowaniu.

(b) Podaj przykład dziedziny, która nie ma tej własności. Wyjaśnij.

$\mathbb{Z}[\sqrt{5}]$. Mamy $(\sqrt{5}-1)(\sqrt{5}+1) = 2 \cdot 2$. Wszystkie te elementy są nierozkładalne, bo możemy wprowadzić funkcję potencjału $\varphi(a+b\sqrt{5}) = |a^2 - 5b^2|$ i zauważyć, że jej wartość dla elementów rozkładu na czynniki pierwsze jest mniejsza niż jej wartość dla elementu rozkładanego, a nie istnieją elementy nieodwracalne o mniejszym φ niż $\varphi(2) = \varphi(\sqrt{5}-1) = \varphi(\sqrt{5}+1) = 4$. Te elementy nie są stowarzyszone, bo w $\mathbb{Z}[\sqrt{5}]$ elementy odwracalne to ± 1 i $\pm 2 \pm \sqrt{5}$, więc $1 + \sqrt{5} \notin [2]_\sim$.

17. (a) Podaj definicję dziedziny euklidesowej R.

<u>Dziedzina Euklidesowa</u>

Taka dziedzina całkowitości, że istnieje funkcja $N : R \longrightarrow \mathbb{N}_{\geqslant 0}$ że:

- $N(a) = 0 \iff a = 0$
- $N(ab) = N(a)N(b)$
- dla dowolnych $a, b \in R$, gdzie $b \neq 0$, istnieją takie $q, r \in R$, że

$$a = bq + r$$

oraz $N(r) < N(b)$

(b) Udowodnij, że taka dziedzina jest dziedziną ideałów głównych.

Należy pokazać że każdy ideał w DE jest główny, czyli

$$I - \text{ideał} \implies \text{istnieje takie } b \text{ że } I = bR$$

Jeżeli $I = \{0\}$ to $I = 0 \cdot R$. Skorzystajmy z normy i wybierzmy niezerowy element $b \in I$ o najmniejszej normie (0 już rozważyliśmy).
Zauważmy, że $b \in I$, więc inkluzja w tą stronę jest oczywista, $bR \subseteq I$.

Niech $a \in I$, z założenia wiemy więc, że istnieją takie $q, r \in R$, że $a = bq + r$ i $N(r) < N(b)$. Ale r $= a - bq \in I$, a $N(b)$ jest minimalna w I, więc

$$r = 0 \implies a = bq \implies a \in bR \implies I \subseteq bR$$

Mamy więc inkluzję w dwie strony, udowodniliśmy więc tezę.

(c) Wyjaśnij dlaczego $U(R) = \{a \in R : N(a) = 1\}$.

Mamy $1 = 1 \cdot 1$, zatem $N(1) = N(1) \cdot N(1)$, w liczbach naturalnych oznacza to, że $N(1) = 1$. Niech $a \in U(R)$, wtedy istnieje $b \in R$ takie, że $ab = 1$. Z multiplikatywności normy $N(ab) = N(1) = 1 = N(a) \cdot N(b)$, jesteśmy w zbiorze liczb naturalnych, zatem $N(a) = N(b) = 1$

Niech teraz $N(a) = 1$. Podzielmy z resztą 1 przez a: $1 = aq + r$ gdzie $N(r) < N(a) = 1$ więc $N(r) = 0 \iff r = 0$. Czyli $1 = aq$ co oznacza, że $a \in U(R)$.

(d) Podaj opis elementów nierozkładalnych w pierścieniu $\mathbb{Z}[i]$.

<u>Elementy nierozkładalne w $\mathbb{Z}[i]$</u>

Są to:

- liczby pierwsze niebędące sumą kwadratów dwóch liczb całkowitych, oraz stowarzyszone do nich elementy $\mathbb{Z}[i]$
- liczby postaci $a + bi$, gdzie $a^2 + b^2$ jest liczby pierwszą

18. (a) Podaj definicję największego wspólnego dzielnika elementów a, b dziedziny R.

NAJWIĘKSZY WSPÓLNY DZIELNIK
Ogólnie: Element d jest $NWD(a_1, ..., a_n)$ jeśli:
- $d \mid a_i$
- jeśli $c \mid a_i$ to $c \mid d$

(b) Wykaż, że jeśli $NWD(a, b)$ istnieje, to jest jednoznaczny z dokładnością do stowarzyszenia.

Niech d_1 oraz d_2 spełniają warunki z definicji NWD. Wtedy, ponieważ d_1 spełnia dla samego siebie warunek 1) to z warunku 2) dla d_2 wiemy, że $d_1 \mid d_2$. Analogicznie pokazujemy, że $d_2 \mid d_1$, czyli $d_1 \sim d_2$.

Oczywiście, jeśli d jest $NWD(a_1, ..., a_n)$ i fd ($d = fu$ dla pewnego $u \in U(R)$) to $d \mid a_i \implies f \mid a_i$ ($a_i = dr = fur$) oraz $c \mid d \implies c \mid f$ ($d = cp \iff fu = cp \iff f = cpu^{-1}$).

(c) Niech R będzie dziedziną ideałów głównych. Udowodnij, że $aR + bR = dR$, gdzie d jest NWD elementów a, b.

Oczywiście $aR + bR \subseteq dR$, bo $ar_1 + br_2 = d(\frac{a}{d}r_1 + \frac{b}{d}r_2)$. Wiemy jednak, że $aR + bR$ jest ideałem głównym, oznaczmy go jako kR. Mamy $aR, bR \subseteq kR$, czyli $k \mid a$ oraz $k \mid b$ więc z definicji NWD $k \mid d$. Ale to oznacza, że

$$dR \subseteq kR = aR + bR$$

Mamy zawieranie w dwie strony, mamy więc równość, udowodniliśmy więc tezę.

19. (a) Podaj definicję wielomianu pierwotnego w pierścieniu $R[x]$, gdzie R jest dziedziną z jednoznacznością rozkładu.

Niech $f = \sum_{k=0}^{n} a_k x^k \in R[x]$. Wtedy:

$$f \text{ jest pierwotny} \iff NWD(a_0, ..., a_n) = 1$$

Przykłady:
- $3 - 5x^2$ jest pierwotny nad $\mathbb{Z}[x]$
- $3 - 9x^2$ nie jest pierwotny nad $\mathbb{Z}[x]$

(b) Sformułuj lemat Gaussa o wielomianach pierwotnych.

LEMAT GAUSSA O WIELOMIANACH PIERWOTNYCH
Iloczyn dwóch wielomianów pierwotnych jest wielomianem pierwotnym.

20. (a) Sformułuj kryterium Eisensteina.

Niech R będzie dziedziną, a $f = a_0 + a_1x + ... + a_nx^n \in R[x], \quad a_n \neq 0, n \geqslant 1$

$$\left.\begin{aligned} p \in R, \text{nierozkładalny} \\ p \nmid a_n \\ p^2 \nmid a_0 \\ p \mid a_i, i = 0, 1, ..., n-1 \end{aligned}\right\} \implies f \text{ jest nierozkładalny w Q(R)[x] (ciało ułamków)}$$

(b) Niech $f = 2x^{32} + 12x^{23} + 18x^9 + 6 \in \mathbb{Z}[x]$. Czy f jest nierozkładalny w $\mathbb{Q}[x]$? Czy f jest nierozkładalny w $\mathbb{Z}[x]$?

Skorzystamy z kryterium Eisensteina. Weźmy $p = 3$. Mamy

$$3 \nmid 2, \quad 3^2 \nmid 6, \quad 3 \mid 18, 12$$

Spełnione są więc założenia kryterium Eisensteina, wielomian jest więc nierozkładalny w $\mathbb{Q}[x]$
Ale jest rozkładalny w $\mathbb{Z}[x]$, bo $f = 2x^{32} + 12x^{23} + 18x^9 + 6 = 2(x^{32} + 6x^{23} + 9x^9 + 3)$ i 2 jest nieodwracalny w $\mathbb{Z}[x]$ tak samo jak ten wielomian. (fakt $U(\mathbb{Z}[x]) = U(\mathbb{Z})$)

21. Niech $K \subset L$ będzie rozszerzeniem ciała oraz niech $a \in L$.

(a) Wyjaśnij co oznacza, że a jest elementem algebraicznym nad K. Podaj definicję wielomianu minimalnego elementu a nad ciałem K.

Element Algebraiczny nad K
a jest elementem algebraicznym nad ciałem K jeśli

$$\underset{0 \neq f \in K[x]}{\exists} f(a) = 0$$

Wielomian minimalny elementu a nad K
Wielomian unormowany $0 \neq f \in K[x]$ taki, że $f(a) = 0$ minimalnego stopnia nazywamy wielomianem minimalnym elementu algebraicznego a.

Równoważnie: unormowany wielomian nierozkładalny $f \in K[x]$ taki, że $f(a) = 0$.

(b) Wyjaśnij, dlaczego $K[a] = K(a)$, jeśli a jest elementem algebraicznym nad K.

Rozważmy homomorfizm $\varphi : K[x] \longrightarrow L$

$$\varphi(w) = w(a) \in L$$

Mamy więc że

$$\varphi(K[x]) = K[a] = \{w(a) : w \in K[x]\}$$

Mamy więc dwa przypadki:
i. $\ker \varphi = 0$. Wtedy widać że $K[a] \cong K[x]$
ii. $\ker \varphi \neq 0$. Wtedy:

$$K[x]/\ker \varphi \cong \varphi(K[x])$$

22. (a) Podaj definicję podciała prostego w ciele K.

Podciało Proste
Część wspólna wszystkich podciał ciała K. Inaczej: podciało generowane przez $\{1\}$.

(b) Uzasadnij, że każde ciało zawiera podciało izomorficzne z $\mathbb{Q}$ lub z $\mathbb{Z}_p$, dla pewnej liczby pierwszej p.

Niech L - ciało. Rozważmy podciało K ciała L generowane przez zbiór $\{1\}$. Podciało jest podgrupą, zatem zawiera element będący sumą n jedynek lub minus jedynek (dla wygody oznaczmy je $s(n)$ oraz $s(-n)$). Mamy dwie możliwości:

i. $s(n) \neq 0$ dla dowolnego $n \in \mathbb{Z}$, możemy więc włożyć pierścień $\mathbb{Z}$ w ciało K, ponieważ K zawiera również wszystkie elementy przeciwne i odwrotne to $\mathbb{Q}$ wkłada się w ciało K - zatem K zawiera podciało izomorficzne z $\mathbb{Q}$.

ii. istnieje n takie, że $s(n) = 0$ i niech będzie ono najmniejsze. Jest to liczba pierwsza: załóżmy przeciwnie $n = kl$ i $k, l \neq 1$, wówczas $0 = s(n) = s(k) \cdot s(l)$ co jest sprzeczne z założeniem, że K jest dziedziną. Skoro więc n jest liczbą pierwszą to w ciało K możemy włożyć ciało $\mathbb{Z}_n$ - zatem posiada podciało izomorficzne z $\mathbb{Z}_n$.

(c) Podaj definicję charakterystyki $char(K)$ ciała K.

Najmniejsza liczba naturalna n taka, że suma n jedynek z danego ciała równa się zeru, a jeżeli takiej liczby nie ma, to jest ona z definicji równa 0. Charakterystyka ciała jest albo równa 0 albo jest liczbą pierwszą.

(d) Udowodnij, że jeśli F jest ciałem skończonym, to istnieją liczba pierwsza p i $n \in N$ takie, że $|F| = p^n$.

Niech F - ciało skończone oraz K - jego podciało izomorficzne z $\mathbb{Z}_{char(F)}$. Wtedy $|K| = p = char(F)$. Oczywiście $[F : K] < \infty$. Niech $[F : K] = n$, a $a_1, ..., a_n$ będzie bazą F nad K Wtedy każdy element $a \in F$ można jednoznacznie przedstawić w postaci pewnej kombinacji linowej z tej bazy.

Z tej jednoznaczności wynika że liczba elementów ciała F jest równa liczbie ciągów o wyrazach $a_1, ..., a_n$, czyli p^n

23. (a) Podaj definicję ciała algebraicznie domkniętego.

Ciało Algebraicznie Domknięte
Ciało, w którym każdy wielomian dodatniego stopnia ma w tym ciele pierwiastek.

(b) Podaj definicję algebraicznego domknięcia ciała K.

Algebraicznie Domknięcie Ciała
Algebraicznym domknięciem ciała nazywamy rozszerzenie $K \subseteq L$ takie że:
- L jest algebraiczne domknięte
- $K \subseteq L$ jest rozszerzeniem algebraicznym, czyli każde $a \in L$ jest algebraiczne nad K

(c) Czy istnieje ciało skończone, które jest algebraicznie domknięte? Uzasadnij.

Niech K będzie skończonym ciałem o elementach $a_1, ..., a_n$. Wówczas wielomian $f = (x - a_1) \cdot ... \cdot (x - a_n) + 1$ nie ma miejsc zerowych w K, bo $1 \neq 0$ w dowolnym ciele.

24. Wyjaśnij, jak się konstruuje ciało ułamków dziedziny R.

Wprowadzamy relację $\sim$ na zbiorze $R \times (R \setminus \{0\})$ określoną jako $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ (jest to relacja równoważności). Przez $\frac{a}{b}$ oznaczamy klasę abstrakcji pary (a, b), a przez $Q(R)$ zbiór wszystkich klas abstrakcji (zbiór ilorazowy). Definiując dodawanie jako

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

oraz mnożenie jako

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

dostajemy ciało ułamków dziedziny R.