(tylko) Konspekt wykładu Algebra I* 2019

http://duch.mimuw.edu.pl/%7Eaweber

v.13.11.2019

Notatki zawierają odsyłacze do podręczników

[BB] A. Białynicki-Birula, Zarys algebry, Bibl.Mat. 63, PWN, Warszawa 1987

[BT] A. Bojanowska, P. Traczyk, Algebra I (skrypt)
http://www.mimuw.edu.pl/%7Eaboj/algebra/algfinv1.pdf, http://dydmat.mimuw.edu.pl/algebra-i

[Br] J. Browkin, Teoria ciał, Bibl.Mat.49, PWN, Warszawa 1977

[KM] M. Kargapolov, J. Merzljakov, Podstawy teorii grup, PWN, Warszawa 1976.

1 Grupy

[Br], [BT], [KM]

1.1 Aksjomaty grupy $(G, \cdot, e)$:

- (łączność) $\forall a, b, c \in G \;\; (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- (własność elementu neutralnego) $\forall a \in G \;\; (a \cdot e) = e \cdot a = a$,
- (istnienie elementu odwrotnego) $\forall a \in G \; \exists a' \in G \;\; a \cdot a' = a' \cdot a = e$

Dowodzimy jednoznaczność jedynki, jednoznaczność elementu odwrotnego. Element odwrotny jest oznaczany przez a^{-1}. Element neutralny często oznaczany jest przez 1.

1.2 Ćwiczenie: jesli w grupie $ab = 1$ to $ba = 1$.

1.3 Zbiór $H \subset G$ jest pod grupą gdy:

- $H \neq \emptyset$,
- $a, b \in H \;\Rightarrow\; ab \in H$
- $a \in H \;\Rightarrow\; a^{-1} \in H$

1.4 Przykłady:

- Liczb całkowite $\mathbb{Z}$,
- Grupa addytywna ciała $(\mathbb{K}, +, 0)$.
- Grupa multiplikatywna $\mathbb{K}^* = (\mathbb{K} \setminus \{0\}, \cdot, 1)$, gdzie $\mathbb{K}$ jest ciałem.
- Grupa cykliczna $\mathbb{Z}_n = (\{0, 1, 2, \ldots, n-1\}, +_{\text{mod } n}, 0)$ jest izomorficzna z grupą pierwiastków z jedynki stopnia n

$$\mathbb{Z}_n \simeq \{z \in \mathbb{C} \mid z^n = 1\}$$

z działaniem mnożenia.

- grupy permutacji $S_n = \Sigma_n$, grupa permutacji parzystych A_n
- grupy liniowe $GL_n(\mathbb{K})$, $SL_n(\mathbb{K})$, macierze odwracalne górnotrójkątne, macierze odwracalne górnotrójkątne z jedynkami na przekątnej
- Grupa $SL_n(\mathbb{Z}) \subset SL_n(\mathbb{R})$ składająca się z macierzy o calkowitoliczbowych wyrazach.
- Grupa wolna $F(A)$, gdzie A jest dowolnym zbiorem, np $F(\{a, b\})$ grupa wolna o dwóch generatorach.

1.5 Grupy przekształceń: automorfizmy zbioru zachowujące jakąś strukturę np. izometrie $\mathbb{R}^n$, izometrie $\mathbb{R}^2$ zachowujące dany n-kąt formeny (grupy dihedralne D_{2n}), izometrie $\mathbb{R}^3$ zachowujące daną bryłę platońską.

1.6 Grupy dihedralne izometrii n-kąta formenego D_{2n}. Jest generowana przez deie symetrie s_1, s_2 względem osi przecinającymi się pod kątem π/n. Złożenie $R = s_2 s_1$ jest obrotem o kąt $2\pi/n$, zatem $R^n = (s_2 s_1)^n = id$. Grupę dihedralną można przedstawić za pomocą generatorów i relacji definiujących

$$D_{2n} = \langle s, R \mid s^2 = 1,\ sRs = R^{-1} \rangle .$$

1.7 Grupa izometrii ośmiościanu/sześcianu zachowujących orientację ma 24 elementy i jest izomorficzna z grupą Σ_4. (Izometrie permutują przekątne.)

1.8 Zadanie: Grupa izometrii 20-ścianu/12-ścianu zachowujących orientację ma 60 elementów i jest izomorficzna z grupą A_5.

1.9 Grupa warkoczy, relacja warkoczowa $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$.

2 Warstwy, Twierdzenie Lagrange'a, homomorfizmy, grupa ilorazowa

Patrz [Browkin roz.1 §1.1-1.5]

2.1 Grupa cykliczna, rząd elementu, rząd grupy.

2.2 Przecięcie podgrup jest podgrupą

2.3 Podgrupa generowana przez zbiór A to najmniejsza grupa zawierająca A

2.4 Warstwy grupy względem podgrupy H: lewostronne G/H, i prawostronne $H\backslash G$

2.5 Indeks podgrupy, tw Lagrangea $|G| = (G : H) \cdot |H|$

2.6 Tw Lagrangea: rząd elementu dzieli rząd grupy

2.7 Twierdzenie Lagrange'a i zastosowania: każda grupa rzędu pierwszego jest cykliczna,

2.8 Homomorfizm grup, obraz, jądro homomorfizmu

2.9 Podgrupa normalna, równość warstw prawostronnych i lewostronnych

2.10 Automorfizm wewnętrzny: $\phi_g : G \to G$, $\phi_g(h) = ghg^{-1}$.

2.11 Podgrupa $N < G$ jest normalna gdy dla każdego $g \in G$ mamy $gNg^{-1} = N$.

2.12 Jądro jest podgrupą normalną

2.13 Twierdzenie o izomorfizmie: $G/ker(f) \simeq im(f)$.

2.14 Przykłady ilorazów:
$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$
$\Sigma_n/A_n \simeq \mathbb{Z}_2$
$A_4/K \simeq \mathbb{Z}_3$
Gdy $n = 2m$ to $\{id, -id\} < D_{2n}$. Opisać $D_{2n}/\{id, -id\}$.

3 Działania

3.1 Homomorfizm $\phi : G \to H$ jest monomorfizmem wtedy i tylko wtedy, gdy $ker(\phi) = 0$.

3.2 Własność uniwersalna ilorazu: dla każdego homomorfizmu $\phi : G \to H$ takiego, że $N \subset ker(\phi)$ istnieje dokładnie jeden homomorfizm $\bar{\phi} : G/N \to H$ taki, że $\phi = \bar{\phi} \circ \pi$.

3.3 Działanie z lewej strony grupy G na zbiorze A, to homomorfizm $G \to Aut(A)$.

3.4 Działanie z prawej strony: $(g, x) \mapsto g(x)$, $g(h(x)) = (hg)(x)$, piszemy $g(x) = xg$, wtedy $(xh)g) = x(hg)$.

3.5 Działanie grupy na sobie przez przesunięcia:
– $h \mapsto gh$ (z lewej strony)
– $h \mapsto hg$ (z prawej strony)

3.6 Cayleya: każda podgrupa jest izomorficzna z pewną grupą przekształceń. Jeśli $|G| = n$, to $G \hookrightarrow \Sigma_n$.

3.7 Niech $H < G$. Rozwarzamy działanie (z prawej strony) H na G przez przesunięcia. Zbiór warstw G/H jest ilorazem zbioru G przez to działanie.

3.8 Działanie grupy na sobie przez sprzęganie. Automorfizmy wewnętrzne.

3.9 Orbity $G \cdot a$, stabilizatory G_a, zbiór punktów stałych A^G.

3.10 Dla $a \in A$ odwzorowania $G/G_a \to G \cdot a$, $gG_a \mapsto ga$ jest dobrze okrełone i jest bijekcją. Wniosek, jeśli $|G| < \infty$ to $|G \cdot a| = (G : G_a)$.

3.11 Definicja: Niech p będzie liczbą pierwszą. Mówimy, że G jest p-grupą, gdy $|G| = p^k$ dla pewnego $k \in \mathbb{N}$.

3.12 Twierdzenie: Jeśli G jest p-grupą, $|A| < \infty$, to $|A^G| \equiv |A| \mod p$.

3.13 Tw Cauchy'ego: Jeśli p dzieli rząd grupy, to istnieje element rzędu p.
Dowód: na zbiorze $A = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \ldots g_p = e\} \simeq G^{p-1}$ działa grupa $\mathbb{Z}_p$ przez cykliczną permutację ciągów, $A^{\mathbb{Z}_p}$ to ciągi stałe $(g, g, \ldots, g)$, $g^p = e$. Z poprzedniego twierdzenia p dzieli $|A^{\mathbb{Z}_p}|$, przy czym $A^{\mathbb{Z}_p} \neq \emptyset$.

3.14 Centrum p-grupy jest nietrywialne.
Dow. G działa na sobie przez sprzężenia, $G^G = Z(G)$. Skoro $e \in Z(G) \neq \emptyset$, to p dzieli $|Z(G)|$.

3.15 Wniosek. Jeśli $|G| = p^2$, to G jest abelowa.

4 Produkty, twierdzenia Sylowa

4.1 Wewnętrzna charakteryzacja produktu

4.2 Przykąd: $\mathbb{Z}_{12} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$ jako produkt podgrup

4.3 Produkt pólprosty $N \rtimes H$ w sytuacji gdy dana grupa N oraz homomorfizm $\phi : H \to Aut(N)$. Definiujemy działanie $(a, g)(b, h) = (ag(b), gh)$ spełnia aksjomaty grupy. (Ćwiczenie).

4.4 Przykład $D_{2n} \simeq \mathbb{Z}_n \rtimes \mathbb{Z}_2$. Produkt warkoczowy $G^n \rtimes \Sigma_n$.

4.5 Definicja: G jest grupą prostą gdy nie ma właściwej nietrywialnej podgrupy normalnej.

4.6 Przykłady grup prostych
– $\mathbb{Z}_p$,
– $A_n = \ker(sgn : \Sigma_n \to \mathbb{Z}_2)$ dla $n \geq 5$,
– $PSL_n(\mathbb{F}_q) = SL_n(\mathbb{F}_q)/Z(SL_n(\mathbb{F}_q))$ (poza $n = 2$ $q = 2$ lub 3),
– grupa monster $|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}$

4.7 Grupy Sylowa, twierdzenia Sylowa [BT]. Niech p będzie liczbą pierwszą, $p^n m = |G|$, przy czym n jest maksymalne. Wtedy
– istnieje podgrupa $S < G$ rzędu p^n (podgrupa Sylowa),
– wszystkie podgrupy o tym rzędzie są sprzężone,
– niech n_p oznacza ilość podgrup o rzędzie p^n (podgrup Sylowa). Wtedy

- $n_p | m$ (dokładniej $n_p = (G : N(S))$, gdzie $N(S)$ jest normalizatorem P w G,
- $n_p = 1 \mod p$.

4.8 Wniosek: jeśli $|G| = pq$ (p, q pierwsze), to G nie jest prosta.
Dow. załóżmy, że $p > q = m$. Wtedy n_p może przyjmować wartości $1, 1 + p, 1 + 2p, \ldots$. Z drugiej strony $n_p | q$ oraz $q < 1 + p$. Zatem $n_p = 1$, czyli p-grupa Sylowa jest normalna.

5 Twierdzenia Sylowa, abelianizacja, rozwiązalność

5.1 Lemat 1: jeśli p jest liczbą pierwszą, $p \not| m$, to współczynnik Newtona $\binom{mp^n}{p^n} \equiv m \mod p$.

5.2 Lemat 2: Niech grupa G działa na zbiorze A, $|G| = mp^n$. Niech $B = \{x \in A : p \not| |Gx|\}$. Wtedy $|A| \equiv |B| \mod p$.

Dowód tw Sylowa — patz [Browkin, Teoria Ciał]. Kroki dowodu:

5.3 W dowodzie twierdzenia Sylowa niech A będzie zbiorem podzbiorów p^n-elementowych w G. Grupa G działa na sobie poprzez przesunięcia. Stąd G działa na zbiorze wszystkich podzbiorów G, zachowuje liczebność zbiorów, więc działa na A. Skoro $|A| = \binom{mp^n}{p^n}$, z lematów $B \neq \emptyset$. Dowodzimy, że stabilizator S zbioru $X \in B$ ma p^n elementów oraz X jest postaci Sx. (Musi być $|S| = p^n r$, $r | m$. Z drugiej strony S działa na zbiorze X. To działanie jest wolne, więc $|S| \leq |X| = p^n$.)

5.4 Mamy bijekcję pomiędzy orbitami w B oraz podgrupami Sylowa. Każda orbita w B ma m elementów. Stąd $n_p m \equiv \binom{mp^n}{p^n} \equiv m \mod p$, więc $n_p \equiv 1 \mod p$.

5.5 Aby dowieść, że podgrupy Sylowa są sprzężone dowodzimy czegoś ogólniejszego: Niech $P < G$, $|P| = p^k$, wtedy istnieje $g \in G$ takie, że $P \subset gSg^{-1}$. Dowód: P działa na warstwach G/S. Skoro $|G/S| = m$, to istnieje punkt stały: $PgS = gS$. Zatem $\forall h \in P$ mamy $hg \in gS$. Stąd $h \in gSg^{-1}$, czyli $P \subset gSg^{-1}$.

5.6 Aby dowieść, że $n_p|m$ rozważamy inne działanie: G działa przechodnio (tzn jest jedna orbita) na grupach Sylowa przez sprzężenie oraz stabilizator S zawiera S.

⋆⋆⋆⋆⋆

5.7 Przykład: jeśli $|G| = 196$ to G nie jest prosta. Dowód: sprawdzamy, że $n_7 = 1$, zatem 7-podgrupa Sylowa jest normalna.

5.8 Grupa rzędu 255 jest cykliczna. (Bo 17-podgrupa Sylowa jest normalna oraz nie ma nietrywialnych działań $\mathbb{Z}_{15}$ na $\mathbb{Z}_{17}$.)

5.9 Komutant $[G, G]$ to podgrupa generowana przez komutatory $[a, b] := aba^{-1}b^{-1}$. Inne oznaczenie G'. Abelianizacja $Ab(G) = G/[G, G]$.

5.10 Dla grupy abelowej A mamy $\mathrm{Hom}(G, A) = \mathrm{Hom}(Ab(G), A)$.

5.11 Ćwiczenie: $Ab(GL_n(\mathbb{K})) =?$

5.12 Rozważamy ciągi podgrup $G = G_0 > G_1 > \cdots > G_n = \{1\}$ taki, że $G_i \rhd G_{i+1}$. (Nie koniecznie $G_i \rhd G$.)

5.13 Mówimy, że grupa jest rozwiązalna gdy istnieje ciąg taki, że G_i/G_{i-1} jest grupą abelową.

5.14 Gdy G_i/G_{i+1} jest abelowa, to $[G_i, G_i] < G_{i+1}$. Definiujemy ciąg minimalnej długości: $G_1 := [G, G] = G'$,..., $G^{(i+1)} := [G^{(i)}, G^{(i)}]$.

5.15 Stwierdzenie (oczywiste): Grupa jest rozwiązalna wtedy i tylko wtedy, gdy dla $i > i_0$ dla pewnego i_0 mamy $G^{(i)} = \{1\}$.

6 P-grupy, klasyfikacja grup abelowych, skończenie generowanych

6.1 p-grupy są rozwiązalne

6.2 Niech $p \neq 2$. Udowodnimy, że Grupa nieabelowa rzędu p^3 jest produktem półprostym $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$ lub $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p$ skoro $Z(G) \neq G$ i $G/Z(G)$ nie jest grupą cykliczną, to $Z(G) \simeq \mathbb{Z}_p$ i $G/Z(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Niech $a, b \in G$ będą takie, że $\pi(a)$ i $\pi(b)$ generują $G/Z(G)$.
– Mamy $[G, G] \subset Z(G)$.
– Grupa $H = \langle a, Z(G)\rangle$ ma p^2 elementów, jest abelowa i normalna ($bab^{-1} = [b, a]a \in H$). Jeśli $b^p = 1$, to $G = H \rtimes \langle b\rangle$. Przypuśćmy przeciwnie, $o(b) = p^2$ i także $o(a) = p^2$, a^p jest generatorem $Z(G)$. Wtedy

$b^p = a^{pk}$ dla pewnego k. Pokażemy, że $b' = a^{-k}b$ jest rzędu p. Zamieniając b na b' otrzymujemy produkt półprosty.
[– Lemat: jeśli $[d,b] \in Z(G)$ to $(db)^p = [d,b]^{\frac{p(p-1)}{2}} d^p b^p$
Dow: mamy $bd = bdb^{-1}d^{-1}db = [b,d]db = db[b,d]$. Uporządkowanie wyrażenia $(db)^k$ wymaga $\frac{p(p-1)}{2}$ przestawień.]
– Z lematu dla $d = a^{-k}$ mamy $(b')^p = b^p a^{-kp}[a^{-k}, b]^{\frac{p(p-1)}{2}} = b^p a^{-kp} = 1$, bo $[a^{-k}, b]^p = 1$.

6.3 Twiedzenie Jordan-Hölder: Niech $G = G_0 > G_1 > \cdots > G_n = \{1\}$ taki, że $G_i \rhd G_{i+1}$ oraz G_i/G_{i+1} jest grupą prostą (tzn ciągu nie można rozdrobnić). Wtedy, zbiór ilorazów wraz z krotnościami nie zależy od ciągu G_i. (bez dowodu)
Przykład: $D_{12} > \mathbb{Z}_6 > \mathbb{Z}_3$ i $D_{12} > D_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 > \mathbb{Z}_2$.

Twierdzenie strukturalne dla skończenie generowanych grup abelowych — Klasyfikacja

6.4 Każda grupa abelowa skończenie generowana jest izomorficzna z ilorazem $\mathbb{Z}^n/\Lambda$, gdzie Λ jest podgrupą w $\mathbb{Z}^n$.

6.5 Niech Λ będzie podgrupą w $\mathbb{Z}^n$. Istnieje baza $\mathbb{Z}^n$: $v_1, v_2, \ldots v_n \in \mathbb{Z}^n$, $s \leq n$ oraz liczby $n_1, n_2, \ldots n_s \in \mathbb{N}$, takie, że $n_1v_1, n_2v_2, \ldots, n_sv_s$ jest bazą Λ.
Dow: Powyższe stwierdzenie jest równoważne temu, że macierz całkowitoliczbową można sprowadzić do postaci $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$, gdzie D jest kwadratową macierzą diagonalna, a 0 oznacza prostokątny blok zerowy. Operacje dozwolone: przestawianie wierszy lub kolumny, transformacje $w_i' = w_i + aw_j$, $k_i' = k_i + ak_j$ dla $i \neq j$.

6.6 Wniosek: Podgrupy w $\mathbb{Z}^n$ są izomorficzne z $\mathbb{Z}^s$, $s \leq n$.

6.7 Wniosek: A skończenie generowana, to $A \simeq \prod_{i=1}^s \mathbb{Z}_{n_i} \times \mathbb{Z}^r$.

6.8 Rozkład skończonej grupy cyklicznej na produkt grup cyklicznych o rzędach względnie pierwszych.

6.9 Jednoznaczność przedstawienia skończenie generowanej grupy abelowej: Jeśli $A = \prod_{i=1}^s \mathbb{Z}_{p^{n_i}}$

$$|\{a \in A \ : \ a^{p^k} = 1\}| = \prod_{i=1}^{s} p^{min(n_i,k)}\,.$$

Z tego wzoru można wyznaczyć n_i.

7 Koniec grup

Grupy abelowe c.d., nilpotentne, wzrost grupy

7.1 Podpodgrupa elementów torsyjnych grupy abelowej

$$T(A) = \{a \in A \mid \exists n > 0 \ a^n = 1\},$$

p-torsja

$$T_p(A) = \{a \in A \mid \exists k > 0 \ a^{p^k} = 1\}.$$

7.2 $A/T(A)$ jest beztorsyjna czyli $T(A/T(A)) = 0$
Dw: $[a]^n = 1$ to $a^n \in T(A)$, więc $(a^n)^m = 1$.

7.3 Jeśli grupa jest skończenie generowana, to $A/T(A) \simeq \mathbb{Z}^r$. Liczba r jest nazywana rangą grupy $r = rk(A)$. (Ćw: $\mathbb{Z}^m \simeq \mathbb{Z}^n \Rightarrow m = n$.)

7.4 Jeśli A torsyjna (czyli $A = T(A)$), to $A = \bigoplus_{p \text{ pierwsza}} T_p(A)$
(to jest wewnętrzna suma prosta: tzn (i) $T_p(A)$ generują A, (ii) $\forall_p\ T_p(A) \cap \left(\bigoplus_{q<p} T_q(A)\right) = 0$.)
Dw: $a^m = 1$, $m = \prod_{i=1}^s p_i^{k_i}$, $m_j := \prod_{i \neq j} p_i^{k_i}$, $a_j := a^{m_j} \in T_{p_j}(A)$. Wspólny dzielnik $(m_1, \ldots, m_s) = 1$, więc $1 = \sum c_j m_j$ dla pewnych $c_j \in \mathbb{Z}$. Zatem $a = \prod a_j^{c_j}$.

7.5 Beztorsyjne grupy abelowe skończenie generowane są izomorficzne z $\mathbb{Z}^n$, czyli mają bazę.

7.6 Niech $n \in \mathbb{N}$. Wolna grupa abelowa $F_n^{ab} = \mathbb{Z}^n$ ma własność: dla grupy abelowej A mamy $Hom(\mathbb{Z}^n, A) = Funkcje([n], Zbiór\ A)$. Można też rozważać wolne grupy o generatorach w dowolnym zbiorze X. Taka grupa wolna FA_X jest zdefiniowana przez własność $Hom(F_X^{ab}, A) = Funkcje(X, Zbiór\ A)$. Grupa F_X^{ab} jest izomorficzna z $\bigoplus_{x \in X} \mathbb{Z}$ i jest właściwą podgrupą w $\prod_{x \in X} \mathbb{Z} = \mathbb{Z}^X$.

7.7 Jeśli F wolna abelowa i $A \to B$ epi wtedy $Hom(F, A) \to Hom(F, B)$ epi.

7.8 Ćwiczenie: Grupa beztorsyjna może nie mieć powyższej własności

7.9 Definicja. Grupa jest nilpotentna, jeśli istnieje ciąg podgrup $G = G_0 > G_1 > \cdots > G_s = 1$ taki, że $[G, G_i] < G_{i+1}$. Wtedy mamy $G_i \lhd G$, bo $gg_ig^{-1} \in [G, G_i]G_i \subset G_{i+1}G_i$. Ponadto $[G_i, G_i] < G_{i+1}$, stąd iloraz G_i/G_{i+1} jest abelowy.

7.10 Równoważnie: $Z(G/G_{i+1}) < G_i/G_{i+1}$.

7.11 Przykład: macierze górnotrójkątne z 1 na przekątnej.

7.12 Dla grupy nilpotentnej są dwa wyróżnione ciągi: pierwszy, zdefiniowany indukcyjnie $\Gamma_0 = G$, $\Gamma_{i+1} := [G, \Gamma_i]$ mamy $\Gamma_i = 1$ dla $i >> 0$. To jest ,,dolny ciąg centralny".

7.13 ,,Górny ciąg centralny", hipercentra: $Z_1 = Z(G)$, $Z_{i+1} = \pi_i^{-1}(Z(G/Z_i))$, gdzie $\pi_i : G \to G/Z_i$. Mamy

$$Z_{i+1} = \{g \in G \,|\, \forall h \in G\ [g, h] \in Z_i\}$$

7.14 Grupa jest nilpotentna wtedy i tylko wtedy gdy $Z_i = G$ dla $i >> 0$.

$$\begin{array}{ccccccccccccc}
1 & < & Z_1 & < & Z_2 & < \ldots \leq & Z_{s-1} & \leq & Z_s & \leq & Z_{s+1} \\
\| & & \vee & & \vee & & \vee & & \vee & & \vee \\
1 = G_{s+1} & < & G_s & < & G_{s-1} & < \ldots < & G_2 & < & G_1 & < & G_0 = G \\
\vee & & \vee & & \vee & & \vee & & \vee & & \| \\
\Gamma_{s+1} & \leq & \Gamma_s & \leq & \Gamma_{s-1} & \leq \ldots < & \Gamma_2 & < & \Gamma_1 & < & \Gamma_0
\end{array}$$

7.15 Stopień nilpotentności u. Dla dowolnych elementów $g_1, \ldots, g_{u+1}$ jest spełniona formuła:

$$[g_1[g_2[\ldots[g_u, g_{u+1}]\ldots] = 1\,.$$

7.16 Grupy nieskończone, ale skończenie generowane:
- norma $|g|$ = długość najkrótszego słowa reprezentującego g
- metryka słów $d(g,h) = |gh^{-1}|$,
- przestrzenie metryczne G z metryką słów,
- wzrost grupy: $f(n) = |Kula(1,n)|$. Różne wybory generatorów prowadzą do równoważnych funkcji wzrostu. Funkcje wzrostu porównywane są tak: $f \prec g$ jesłi istnieją stałe takie, że $f(n) < C\,g(dn)$ dla wszystkich n.

7.17 Grupy abelowe $\mathbb{Z}^r \times torsja$ mają wzrost wielomianowy n^r.

7.18 Grupa wolna o r generatorach ma wzrost wykładniczy $(2r-1)^n$.

7.19 Grupy nilpotentne maja wzrost wielomianowy (Tw Bassa) n^r, gdzie $r = \sum_{k\geq 0}(k+1)rk(\Gamma_k/\Gamma_{k+1})$. Np grupa Heisenberga $\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \subset GL_3(\mathbb{Z})$ ma wzrost $\sim r^4$.

7.20 Twierdzenie Gromowa: jeśli grupa ma wzrost wielomianowy to zawiera podgrupę nilpotentną skończonego indeksu.

7.21 Ćwiczenie: $SL_2(\mathbb{Z})$ ma wzrost wielomianowy.

Zadania o grupach 2019

4.12.2019

Zadania zawierają odsyłacze do podręczników

[BT] A. Bojanowska, P. Traczyk, Algebra I (skrypt) http://www.mimuw.edu.pl/%7Eaboj/algebra/algfinv1.pdf

[Br] J. Browkin, Teoria ciał, Bibl.Mat.49, PWN, Warszawa 1977

[KM] M. Kargapolov, J. Merzljakov, Podstawy teorii grup, PWN, Warszawa 1976.

[BJ] M. Bryński, J. Jurkiewicz, Zbiór zadań z algebry, PWN, Warszawa

Zadania zrobione oznaczone są przez ♠.

1 Przykłady

1.1 Uzasadnić, że grupa permutacji parzystych A_5 jest izomorficzna z grupą izometrii zachowujących orientację dwudziestościanu foremnego I_{60}.

1.2 ♠ Czy istnieje skończony układ generatorów grupy addytywnej ciała liczb wymiernych

$$\mathbb{Q}_+ := (\mathbb{Q}, +, 0) \ ?$$

1.3 ♠ Wykazać, że grupa wolna o 2 generatorach $F(\{a, b\})$ zawiera pod grupę, która nie jest generowana przez żaden skończony zbiór elementów.

1.4 ♠ Sprawdzić, że $SL_2(\mathbb{Z})$ jest generowana przez macierze $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

1.5 ♠ Znaleźć $|GL_n(\mathbb{F}_q)|$, $|SL_n(\mathbb{F}_q)|$, gdzie $\mathbb{F}_q$ jest ciałem q-elementowym.

1.6 ♠ Centrum grupy definiujemy jako $Z(G) = \{g \in G \ : \ \forall h \in G \ gh = hg\}$. Znaleźć $Z(GL_n(\mathbb{F}))$ i $Z(SL_n(\mathbb{F}))$, gdzie $\mathbb{F}$ jest ciałem.

1.7 Wskazać rozkład grupy izometrii kwadratu D_8 na sumę teoriomnogościową swoich trzech podgrup właściwych. Uzasadnić, że żadna grupa nie jest sumą dwóch swoich podgrup właściwych.

1.8 Niech G_1 i G_2 będą podgrupami pewnej ustalonej grupy. Udowodnić $|G_1 \cdot G_2| \cdot |G_1 \cap G_2| = |G_1| \cdot |G_2|$. Uwaga: zbiór $G_1 \cdot G_2 = \{g_1 g_2 \ : \ g_1 \in G_1, \ g_2 \in G_2\}$ nie musi być grupą.

1.9 ♠ Opisać znane grupy rzędu 8.

Następne dwa zadania to przykłady grup Coxetera, będziemy je robić w drugiej kolejności

1.10 Niech $G \subset GL_n(\mathbb{Z}[t, t^{-1}])$ będzie podgrupą generowaną przez permutacje współrzędnych i macierze diagonalne $Diag(t^{a_1}, t^{a_2}, \ldots, t^{a_n})$, $\sum_{i=1}^{n} a_i = 0$. Wykazać, że istnieje układ generatorów $s_0, s_1, \ldots s_{n-1}$, spełniający

$s_i^2 = 1$,

$s_i s_j = s_j s_i$ dla $i - j \not\equiv \pm 1 \ mod \ n$,

$(s_i s_{i+1})^3 = 1$ ($i + 1$ rozumiane modulo n).

1.11 Niech $G \subset GL_n(\mathbb{Z})$, $n \geq 4$ będzie podgrupą generowaną przez permutacje współrzędnych i macierze diagonalne $D = Diag(\pm 1, \pm 1, \ldots, \pm 1)$, $det(D) = 1$. Wykazać, że istnieje układ generatorów $s_1, s_2, \ldots s_{n-1}, s'_{n-1}$, spełniający
$s_i^2 = 1$, ${s'}_{n-1}^2 = 1$
$s_i s_j = s_j s_i$ dla $|i - j| \neq 1$,
$s_i s'_{n-1} = s'_{n-1} s_i$ dla $i \neq n - 2$,
$(s_i s_{i+1})^3 = 1$, $(s_{n-2} s'_{n-1})^3 = 1$

1.12 ♠ Wykazać, że 3-cykle generują grupę permutacji parzystych A_n.

1.13 ♠ Opisać kategoryjny produkt i sumę prostą w kategorii grup. Koproduktem (kategoryjną sumą prostą) grup G_1 i G_2 jest grupa G wraz z homomorfizmami $i_1 : G_1 \to G$, $i_2 : G_2 \to G$

$$\begin{tikzcd}
 & S \arrow[dd, dotted, "\exists!\,\phi"] & \\
G_1 \arrow[ur, "i_1"] \arrow[dr, "\forall f_1"'] & & G_2 \arrow[ul, "i_2"'] \arrow[dl, "\forall f_2"] \\
 & H &
\end{tikzcd}$$

spełniająca własność: dla każdej pary homomorfizmów $f_1 : G_1 \to H$, $f_2 : G_2 \to H$ istnieje dokładnie jeden homomorfizm $\phi : G \to H$ taki, że $\phi \circ i_k = f_k$ dla $k = 1, 2$. Czy w poprzednich zadaniach już pojawił się już koprodukt grup dla $G_1 = G_2 = \mathbb{Z}$?

2 Homomorfizmy, warstwy, ilorazy

2.1 ♠ Niech $|G| < \infty$. Wykazać, że ilość elementów rzędu pierwszego p jest podzielna przez $p - 1$.

2.2 Niech $(G, +, 0)$ będzie grupą przemienną. Mówimy, że G jest podzielna, jeśli

$$\forall g \in G\ \forall n \in \mathbb{N} \setminus \{0\}\ \exists h \in G\ nh = g.$$

(Przykład: $G = (\mathbb{Q}, +, 0)$.) Wykazać, że grupa podzienlna nie ma właściwych podgrup skończonego indeksu.

2.3 a) Niech $G \subset \mathbb{Q}$ będzie zbiorem ułamków, które w postaci nieskracalnej mają mianowniki będące potęgą liczby p. (Oznaczenie $\mathbb{Z}[1/p]$.) Czy $\mathbb{Z}[1/p]$ ma podgrupę skończonego indeksu?
b) Niech $G \subset \mathbb{Q}$ będzie zbiorem ułamków, które w postaci nieskracalnej mają mianowniki względnie pierwsze z liczbą p. (Oznaczenie $\mathbb{Z}_{(p)}$.) Czy $\mathbb{Z}_{(p)}$ ma podgrupę skończonego indeksu?

2.4 ♠ Wykazać, że istnieje epimorfizm $GL_2(\mathbb{Z}_3) \to \Sigma_4$ z jądrem $\{I, -I\}$.

2.5 ♠ Znaleźć epimorfizm $\Sigma_4 \to \Sigma_3$.

2.6 Opisać grupy $Aut(\mathbb{Z}_n)$ dla $n = 13,\ 15,\ 16,\ 20,\ 21,\ 24,\ 26,\ 28,\ 30$. Przedstawić je jako produkty grup cyklicznych. (Wskazówka: jeśli $(m, n) = 1$ to $Aut(\mathbb{Z}_{mn}) \simeq Aut(\mathbb{Z}_m \times \mathbb{Z}_n) \simeq Aut(\mathbb{Z}_m) \times Aut(\mathbb{Z}_n)$.)

2.7 ♠ Czy istnieje grupa cykliczna G taka, że $Aut(G) \simeq \mathbb{Z}_8$?

2.8 ♠ Udowodnić, że jeśli p jest liczbą pierwszą, to $Aut(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$.

2.9 Każda podgrupa indeksu 2 jest podgrupą normalną.

2.10 ♠ Udowodnić, że centrum $Z(G)$ jest podgrupą normalną w G. Wykazać, że jeśli G nieprzemienna, to $G/Z(G)$ nie jest grupą cykliczną.

3 Grupy permutacji itp

3.1 ♠ Grupa automorfizmów grupy nieprzemiennej nie jest cykliczna. (Wsk: z poprzedniego zadania.)

3.2 ♠ Niech p będzie liczbą pierwszą. $|G| = p^k$, $\{1\} \neq N \lhd G$ to $N \cap Z(G) \neq \{1\}$

3.3 ♠ Niech $Inn(G) < Aut(G)$ oznacza grupę automorfizmów wewnętrznych grupy G (tzn postaci $h \mapsto ghg^{-1}$). Wykazać, że $Inn(G)$ jest podgrupą normalną. Niech $Out(G) = Aut(G)/Inn(G)$. Znaleźć $Out(D_{2n})$.

3.4 ♠ Udowodnić wzór Burnsida

$$|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^{\langle g \rangle}|.$$

3.5 ♠ Niech p liczba pierwsza. Pokazać, że Σ_p jest generowana przez dowolny cykl długości p i dowolną transpozycję.

3.6 ♠ Opisać klasy sprzężoności elementów w Σ_5 i w A_5.

3.7 ♠ a) Wskazać podgrupę rzędu 5^6 w Σ_{25}. b) Niech p będzie liczbą pierwszą, $n \in \mathbb{N}$. Wskazać p-podgrupę Sylowa w Σ_n.

3.8 ♠ Czy $Inn(\Sigma_n) = Aut(\Sigma_n)$ dla $n = 2, 3, 4, 5$? Uwaga: wyjątkowo $Inn(\Sigma_6) \neq Aut(\Sigma_6)$.

Patrz np Wiki: Automorphisms of the symmetric and alternating groups.

3.9 ♠ a) Wskazać dwie nieizomorficzne nieprzemienne grupy rzędu 125. b) Czy istnieje jeszcze trzecia grupa nieprzemienna, która jest nieizomorficzna ze wskazanymi w punkcie a)?

3.10 ♠ Niech G będzie skończoną grupą abelową, która nie jest cykliczna. Wykazać, że istnieje $d < |G|$ takie, że dla każdego $g \in G$ mamy $g^d = 1$.

4 Grupy Sylowa

4.1 ♠ Niech H będzie grupą prostą (tzn H nie zawiera właściwej nietrywialnej podgrupy normalnej). $H \lhd G$, $|H|^2$ nie dzieli $|G|$. Udowodnić, że H jest jedyną izomorficzną z H podgrupą G.

4.2 ♠ Niech $n = 2^k m$, $2 \not| m$. Ile jest podgrup rzędu 2^{k+1} w D_{2n}?

4.3 ♠ Czy istnieje grupa zawierająca dokładnie 12 elementów rzędu 5.

4.4 ♠ Czy każda grupa rzędu 595 jest cykliczna?

4.5 ♠ Dla jakiego n istnieje grupa prosta rzędu $3^n \cdot 7$?

4.6 ♠ Jeśli $|G| = pqr$ (p, q i r liczby pierwsze), pokazać, że G zawiera nietrywialną podgrupę normalną.

4.7 ♠ Wykazać, że A_n jest prosta dla $n > 4$.

5

5.1 ♠ Niech G będzie grupą, zaś p będzie najmniejszym dzielnikiem pierwszym $|G|$. Podgrupa H jest taka, że $|G|/|H| = p$. Pokaż, że H jest normalna.

5.2 ♠ Niech K będzie podgrupą normalną grupy G i $|G/K| = n < \infty$. Pokazać, że
(a) dla każdego $g \in G$ mamy $g^n \in K$,
(b) jeśli $g \in G$, $g^m \in K$ oraz $(m, n) = 1$, to $g \in K$.

5.3 ♠ Niech G będzie grupą skończoną. Udowodnić, że jeżeli G jest grupą nieabelową, to $Aut(G)$ nie jest grupą cykliczną. Udowodnić, że nie istnieje grupa G taka, że grupa $Aut(G)$ jest cykliczna rzędu nieparzystego różnego od 1.

5.4 ♠ Niech A, B, C będą grupami abelowymi oraz $\phi : B \to C$ epimorfizmem. Składanie z ϕ indukuje przekształcenie $\phi_* : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$. Udowodnić, że jeśli A jest skończenie generowana i beztorsyjna, to ϕ_* jest epimorfizmem. Podać przykład grupy abelowej beztorsyjnej A takiej, że ϕ_* nie jest epimorfizmem.

5.5 ♠ Wskazać grupę G wraz z podgypą normalną H taką, że nie istnieje podgrupa normalna K o własności:
1) $K \simeq G/H$,
2) $G/K \simeq H$.
Podać taki przykład, by H i G/H były proste.

5.6 ♠ Niech $\Lambda = \langle (4, 4, 8), (2, 4, 5), (4, 6, 9) \rangle \subset \mathbb{Z}^3$. Przedstawić grupę $\mathbb{Z}^3/\Lambda$ jako produk grup cyklicznych.

5.7 ♠ Dana grupa abelowa $A = \mathbb{Z}^n/im(\phi)$, gdzie $\phi : \mathbb{Z}^m \to \mathbb{Z}^n$ jest zadane wzorem

$$\phi(a_1, a_2, \ldots, a_m) = \left(\sum_{i=1}^{m} a_i, \sum_{i=1}^{m} i\, a_i, \sum_{i=1}^{m} i^2 a_i, \ldots \sum_{i=1}^{m} i^{n-1} a_i \right).$$

Przedstawić A w postaci produktu grup cyklicznych.

6

6.1 ♠ Znaleźć wzrost grupy Heisenberga (tzn grupy macierzy górnotrójkątnych 3×3 z całkowitoliczbowych z jedynkami na przekątnej).

6.2 ♠ Niech $\iota : GrAb \to Gr$ będzie zanurzeniem kategorii grup abelowych do kategorii wszystkich grup. Znaleźć przekształcenie (funktor) $\phi : Gr \to GrAb$ i naturalną bijekcję $\mathrm{Hom}_{Gr}(G, \iota A) \simeq \mathrm{Hom}(\phi(G), A)$.

6.3 Czy $\mathbb{Q} \simeq \mathbb{Z}[1/p]$? Czy $\mathbb{Z}[1/q] \simeq \mathbb{Z}[1/p]$ ($p \neq q$ liczby pierwsze)? Czy $\mathbb{Q} \times \mathbb{Q} \simeq \mathbb{Q}$? Czy $\mathbb{Z}[1/p] \times \mathbb{Z}[1/p] \simeq \mathbb{Z}[1/p]$? (Chodzi o izomorfizmy grup abelowych.)

6.4 Wykazać, że podgrupa i iloraz grupy nilpotentnej jest grupą nilpotentną.

6.5 Udowodnić, że grupa nilpotentna ma wzrost wielomianowy. (Wsk. Znając wzrost $[G, G]$ oszacować wzrost G.)

6.6 Wykazać, że każda grupa skończenie generowana ma wzrost conajwyżej wykładniczy.

6.7 $SL_2(\mathbb{Z})$ ma wzrost wykładniczy.

6.8 Czy istnieje nietrywialna grupa G generowana przez elementy a, b, c, które spełniają relacje

$$[a, b] = b, \qquad [b, c] = c, \qquad [c, a] = a\,?$$

6.9 Udowodnić, że grupa permutacji Σ_n ma następujące przedstawienie
generatory: transpozycje $s_i = (i, i+1)$ dla $i = 1, s, \ldots, n-1$
relacje:
$s_i^2 = 1$,
$s_i s_j = s_j s_i$ dla $|i - j| \neq 1$,
$(s_i s_{i+1})^3 = 1$

6.10 Niech $G \subset GL_n(\mathbb{Z})$, $n \geq 4$ będzie podgrupą generowaną przez permutacje współrzędnych i macierze diagonalne $D = Diag(\pm1, \pm1, \ldots, \pm1)$, $det(D) = 1$. Wykazać, że istnieje układ generatorów $s_1, s_2, \ldots s_{n-1}, s'_{n-1}$, spełniający
$s_i^2 = 1$, ${s'}_{n-1}^2 = 1$
$s_i s_j = s_j s_i$ dla $|i - j| \neq 1$,
$s_i s'_{n-1} = s'_{n-1} s_i$ dla $i \neq n-2$,
$(s_i s_{i+1})^3 = 1$, $(s_{n-2} s'_{n-1})^3 = 1$

7 Zadania o pierścieniach

https://www.mimuw.edu.pl/%7Eaweber/zadania/algebra2019/pierscienie2019zad.pdf

ALGEBRA 1 18.01.2019

Dokładnie uzasadnij wszystkie odpowiedzi.

1. W pierścieniu $\mathbb{Q}$ opisz najmniejszą (najmniejszy)
   a) podgrupę multyplikatywną zawierająca $\frac{1}{4}$,
   b) podpierścień zawierający $\frac{1}{4}$,
   c) ideał zawierający $\frac{1}{4}$.
2. a) Wyznacz element pierścienia $\mathbb{Z}[i]$, który jest generatorem ideału $I = (3 + 9i, 6 + 6i)$.
   b) Ile jest ideałów maksymalnych pierścienia $\mathbb{Z}[i]$ zawierających I? Wskaż te ideały.
3. Niech $f = x^3 - x^2 + 2x - 2 \in \mathbb{R}[x]$ oraz niech $R = \mathbb{R}[x]/(f)$.
   a) Wskaż niezerowe dzielniki zera w pierścieniu R.
   b) Czy R jest iloczynem prostym ciał?
4. a) Znajdź wszystkie wielomiany nierozkładalne stopnia dwa w $\mathbb{Z}_2[x]$.
   b) Sprawdź, czy wielomian $x^4 + x + 1$ jest nierozkładalny w $\mathbb{Z}_2[x]$.
5. Niech $R = \{a/b \in \mathbb{Q} : a, b \in \mathbb{Z},\ \mathrm{NWD}(b, 15) = 1\}$.
   a) Wykaż, że R jest podpierścieniem w $\mathbb{Q}$.
   b) Wskaż wszystkie elementy nierozkładalne w R.
   c) Czy R jest dziedziną z jednoznacznością rozkładu?

(tylko) Konspekt wykładu Algebra I*: Pierścienie 2019

http://www.mimuw.edu.pl/%7Eaweber

v.26.1.2020

Notatki zawierają odsyłacze do podręczników

[AMcD] M. F. Atiyah, I. G. MacDonald, Introduction To Commutative Algebra (wiele wydań)

[BB] A. Białynicki-Birula, Zarys algebry, Bibl.Mat. 63, PWN, Warszawa 1987

[BT] A. Bojanowska, P. Traczyk, Algebra I (skrypt)
http://www.mimuw.edu.pl/%7Eaboj/algebra/algnowa13.pdf

[Br] J. Browkin, Teoria ciał, Bibl.Mat.49, PWN, Warszawa 1977

[Is] I. M. Isaacs, Algebra: A Graduate Course

1 Pierścienie

1.1 Definicja pierścienia przemiennego z 1: $(R, +, \cdot, 0, 1)$

1.2 Jedyność jedynki, $a \cdot 0 = 0$

1.3 *Niektóre elementy definicji pierścienia bywają opuszczane (przemienność, jedynka, a nawet czasami łączność mnożenia).*

1.4 *Macierze kwadratowe nad ustalonym ciałem (pierścień nieprzemienny z 1)*

1.5 *Pierścień grupowy (dla grupy skończonej)*

$$\mathbb{Z}(G) = Funkcje(G, \mathbb{Z}) \ni \sum_{g \in G} a_g e^g \,.$$

$$e^g \cdot e^h := e^{gh} \,.$$

Mnożenie w pierścieniu grupowym można zapisać jako splot funkcji na grupie

$$f_1 * f_2(g) = \sum_{h \in G} f_1(h) f_2(h^{-1} g) \,.$$

Mnożenie jest nieprzemienne jeśli grupa jest nieprzemienna.

1.6 *Funkcje na przestrzeni topologicznej o nośniku zwartym $C_0(X; \mathbb{R})$ (nie ma 1 jeśli X nie jest zwarta)*

1.7 Przykłady pierścieni (od tej pory będą tylko pierścienie przemienne z 1):

$\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}_n$, ciała.

1.8 Podpierścień. Podpierścienie $\mathbb{Q}$:
- $\mathbb{Z}[1/p]$,
- $\mathbb{Z}_{(p)}$

1.9 Pierścień wielomianów $\mathbb{Z}[x]$, $\mathbb{K}[x]$, pierścień szeregów formalnych $\mathbb{Z}[[x]]$, $\mathbb{K}[[x]]$, pierścień szeregów Laurenta $\mathbb{K}((x))$, $\mathbb{K}[\epsilon]$, $\epsilon^2 = 0$

1.10 Pierścień funkcji wielomianowych na $\mathbb{K}^n$

1.11 Pierścień liczb p-adycznych $\mathbb{Z}_p^\wedge$

$$\mathbb{Z}_p^\wedge \twoheadrightarrow \ldots \twoheadrightarrow \mathbb{Z}_{p^{n+1}} \twoheadrightarrow \mathbb{Z}_{p^n} \twoheadrightarrow \ldots \twoheadrightarrow \mathbb{Z}_{p^2} \twoheadrightarrow \mathbb{Z}_p \twoheadrightarrow 0$$

1.12 Pierścienie funkcji rzeczywistych (ciągłych, gładkich, ograniczonych) na $U \subset \mathbb{R}^n$.

1.13 Elementy specjalnego typu
– elementy odwracalne, grupa elementów odwracalnych $U(R)$,
– dzielniki zera,
– elementy nilpotentne,
– elementy nierozkładalne,

1.14 Elementy zdefiniowanych wcześniej typów w $\mathbb{Z}$, $\mathbb{K}[x]$, $\mathbb{K}[\epsilon]$
– dzielniki zera w $\mathbb{Z}_n$
– elementy odwracalne w $\mathbb{K}[x]$, $\mathbb{K}[[x]]$
– $U(\mathbb{Z}[i])$

1.15 Dzielniki zera, dziedzina = dziedzina całkowitości = pierścień bez dzielników zera.

1.16 Skończona dziedzina jest ciałem.

Homomorfizmy pierścieni

1.17 Homomorfizm pierścieni (zakładamy, że $1 \mapsto 1$), istnieje tylko jeden homomorfizm z $\mathbb{Z}$ do dowolnego pierścienia.

1.18 Homomorfizmy pierscieni z 1, izomorfizm, homomorfizm $\mathbb{Z}$ w $\mathbb{Z}_m$ oraz ewaluacja wielomianów: $R[x] \to R$, $f \mapsto f(a)$.

1.19 Różnica między $R[x]$ a funkcjami wielomianowymi $R \to R$

1.20 Jądro homomorfizmu: jeśli $a \in \ker(\phi)$ to $ab \in \ker(\phi)$.

1.21 definicja ideału, ideały generowane przez podzbiór, ideały w $\mathbb{Z}$, $\mathbb{Z}_n$ i w $\mathbb{K}[x]$

1.22 Iloraz przez ideał R/I

2 Ideały

2.1 Uniwersalna własność ilorazu. Twierdzenie o izomorfizmie $im(f) = R/kef(f)$.

2.2 A podpierścień R, I ideał w R (piszemy $I \lhd R$), wtedy $I \cap A \lhd A$, $A + I$ podierścień R, oraz $A/(I \cap A) \simeq (A + I)/I$

2.3 Uniwersalna własność pierścienia wielomianów: każdy homomorfizm pierścieni $R \to S$ można jednoznaciacznie przedłużyć do homomorfizmu $R[x_1, x_2, \ldots, x_n] \to S$ przy zadanych wartościach na x_i.

2.4 Ideały pierwsze, ideały maksymalne, ideały główne

2.5 Twierdzenie: ideałI jest maksymalny $\iff$ R/I jest ciałem.
($[a] \in R/I$ nie jest odwracalny to $(I, a) = I + Ra$ jest właściwym ideałem)

2.6 Twierdzenie: ideał I w R jest pierwszy $\iff$ R/I jest dziedziną.

2.7 Ideał główny $(n) \subset \mathbb{Z}$ dla $n \in \mathbb{N}$, $n > 1$ jest pierwszy wtedy i tylko wtedy gdy n jest liczbą pierwszą.

2.8 W $\mathbb{Z}$, $\mathbb{K}[x]$ każdy ideał jest główny. W tych pierścieniach działa algorytm euklidesa i Każdy element można rozłożyć na elementy nierozkładalne. Rozkład jest jednoznaczny z dokładnością do mnożenia przez elementy odwrotne i przestawianie czynników.

2.9 Plan na przyszłość. Będziemy rozważali trzy klasy pierścieni:
– DJR (ang UFD): pierścienie z jednoznacznoącią rozkładu.
– DIG (ang PID): każdy ideał jest generowany przez jeden element
– Euklidesowe: działa algorytm Euklidesa dla pewnej normy.

$$\text{Eukl.} \quad \subset \quad \text{DIG} \quad \subset \quad \text{DJR}$$

2.10 $\mathbb{Z}[x]$, $\mathbb{K}[x, y]$ DJR, ale nie DIG

2.11 $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ DIG, nie Euklidesowy

2.12 Operacje na ideałach: przecięcie, suma wstępująca, $(I \cup J) = I + J$,

2.13 **Ćwiczenie:** przeciwobraz, obraz ideału?

2.14 Ideał jest niewłaściwy ($I = R$) wtedy i tylko wtedy gdy $1 \in I$.

2.15 Każdy ideał maksymalny jest pierwszy bo ciało jest bez dzielników zera.

2.16 Ciała mają tylko trywialne ideały $\{0\}$, $\mathbb{K}$. Jeśli R zawiera tylko jeden ideał właściwy, to R jest ciałem.

2.17 R jest ciałem wtedy i tylko wtedy gdy 0 jest ideałem maksymalnym.

2.18 Każdy homomorfizm ciał do niezererowego pierścienia jest włożeniem.

2.19 Twierdzenie: każdy ideał właściwy jest zawarty w pewnym ideale maksymalnym.
Z lematu Kuratowskiego-Zorna: każdy wstępujący ciąg ideałów ma ograniczenie górne (jest nim suma ideałów), zatem istnieje element maksymalny.

2.20 Dla każdego pierścienia R i elementu nieodwracalnego $a \in R$ istnieje epimorfizm do ciała $\pi : R \to \mathbb{K}$ taki, że $\pi(a) = 0$.

2.21 R jest bez dzielników zera wtedy i tylko wtedy gdy 0 jest ideałem pierwszym.

2.22 Dopuszczamy (niechętnie) pierścień zerowy, w którym $0 = 1$. Jeśli w R mamy $0 = 1$ to $R = \{0\}$.

Jeszcze trochę przykładów

2.23 Podpierścienie generowane przez podzbiór np $k[x^2, y^2]$

2.24 Niech $S_{\mathbb{R}} \subset \mathbb{R}^n$ będzie stożkiem wypukłym. Pierścień półgrupowy $k[S]$, dla $S = S_{\mathbb{R}} \cap \mathbb{Z}^n$.

2.25 Przykład: $S_{\mathbb{R}} = \{a(1,1) + b(-1,1) \in \mathbb{R}^2 \ : \ a, b \geq 0\}$.
$k[S] \simeq k[u, v, w]/(uv - w^2)$

3 Teoria podzielności

3.1 Niech R pierścień bez dzielników zera. Podzielność to relacja porządku na $R/\sim$, gdzie $\sim$ to relacja stowarzyszenia:

$$a \sim b \iff a = ub \qquad \text{gdzie } u \text{ jest elementem odwracalnym.}$$

3.2 NWD nie zawsze musi istnieć $NWD(a, b) = c$ w jezyku relacji porządku oznacza $([d] \leq [a] \wedge [d] \leq [b]) \Rightarrow [d] \leq [c]$. Przykład bez NWD: $R = \mathbb{Z}[\sqrt{-3}]$, $a = 4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$, $b = 2 \cdot (1+\sqrt{-3})$

3.3 Element $p \in R$ jest pierwszy gdy ideał (p) jest pierwszy tzn $p|ab \implies p|a \ \vee \ p|b$.

3.4 W pierścieniu bez dzielników zera jeśli p jest pierwszy i $a|p$ to albo $a \sim p$, albo a jest odwracalny. Dw: $p = ab$ to $p|a$ lub $p|b$. W pierwszym przypadku $pc = a$, więc $p = pcb$, stąd $1 = bc$, czyli b odwracalny.

3.5 W $\mathbb{Z}[\sqrt{-3}]$ liczba 2 jest nierozkładalna, ale nie jest pierwsza: $2|4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ i nie dzieli czynników.

3.6 Element nierozkładalny a spełnia $a = bc$ to b lub c jest odwracalny. Tzn

$$a = bc \iff (a \sim c \ \vee \ a \sim b)\,.$$

3.7 Pierścienie bez dzielników zera i z jednoznacznością rozkładu, w skrócie DJR, ang UFD. Np $\mathbb{Z}$, $k[x_1, x_2, \ldots x_n]$. Konrtprzykład $k[x^2, x^3] = k[s, t]/(s^3 - t^2)$, $\mathbb{Z}[\sqrt{-3}]$.

3.8 $\mathbb{Z}$ i $k[x]$ są DJR. (Będzie tw Gaussa: R DJR to $R[x]$ DJR.)

3.9 R jest DJR $\Rightarrow$ $(\star)$ każdy ciąg ideałów głównych $(a_1) \subset (a_2) \subset (a_3) \subset (a_4) \subset \ldots$ stabilizuje się.
$(\star)$=ACC=ascending chain condition

3.10 $(\star) \Rightarrow$ każdy element rozkłada się na nierozkładalne. (Jednak rozkład nie musi być jednoznaczny.)

3.11 W DJR spełniony jest warunek
$(\star\star)$ każdy nierozkładalny element jest pierwszy ($a|bc$ to a występuje w rozkładzie bc, więc $a|b$ lub $a|c$).

3.12 $(\star)$ i $(\star\star) \iff R$ jest DJR.
Bo z $(\star)$ rozkład istnieje. Czynniki są pierwsze. Gdy $x_1x_2\dots x_n = y_1y_2\dots y_m$ to x_1 musi dzielić któryś y_k, więc być z nim stowarzyszony. Dalej indukcja ze względu na długość.

3.13 DIG = Dziedzina ideałów głównych. Przykład $\mathbb{Z}$, $k[x]$. Kontrprzykład: $(x, y) \subset k[x, y]$ nie jest główny.

3.14 DIGi są DJRami:
$(\star)$ jest spełnione, bo $\bigcup(a_i) = (b) \Rightarrow \exists i\ b \in (a_{i_0})$, on dzieli wszystkie a_i.
$(\star\star)$ (a) jest zawarty w pewnym ideale maksymalnym $\mathfrak{m} = (b)$, tzn $a = bc$. Gdy a nierozkładalny, b nieodwracalny, więc $a \sim b$ z (3.4).

3.15 Dodatkowo dostaliśmy: w DIG ideał generowany przez element nierozkładalny jest maksymalny.

3.16 Największy wspólny dzielnik podzbioru $A \subset R$ w DIGu to taki element b, że $(A) = (b)$.

3.17 Pierścienie Euklidesowe: to pierścienie z dzieleniem z resztą. Dana norma (waluacja) $v : R \setminus \{0\} \to \mathbb{N}$, taka, że dla każdego $a, b \in R$ albo $b|a$ albo istnieją $c, r \in R$ takie, że $a = bc + r$ i $v(r) < v(b)$.

3.18 Przykłady $\mathbb{Z}$, $\mathbb{Z}[i]$, $k[x]$
– $\mathbb{Z}[\sqrt{-2}]$, $v(a + b\sqrt{-2}) := a^2 + 2b^2$, ogólniej $\mathbb{Z}[\sqrt{d}]$, $v(a + \sqrt{d}b) = |a^2 - db^2|$ dla $d = -2, -1, 2, 3$ (w tym napisie $|x|$ oznacza zwykłą wartość bezwzględną w $\mathbb{Z}$).
– $\mathbb{Z}[\xi]$ gdzie ξ pierwiastek prymitywny z 1 stopnia 3, $v(a + b\xi) := a^2 - ab + b^2$

3.19 Algorytm Euklidesa tak jak w $\mathbb{Z}$. Największy wspólny dzielnik, jako wynik algorytmu.

3.20 Wykorzystanie algorytmu Euklidesa do przedstawienia $NWD(a, b)$ jako $ca + bd$. Zastosowanie: liczenie odwrotności w $R/(a)$.
(17,7)=(7,3)=(3,1)=(1)
17=2*7+3 więc 3=17-2*7
7=2*3+1 więc 1=7-2*3=7-2*(17-2*7)=5*7-2*17
stąd $7^{-1} = 5$ w $\mathbb{Z}_{17}$

3.21 Liczby Gaussa $\mathbb{Z}[i]$ (było na ćwiczeniach)
– Elementy pierwsze w $\mathbb{Z}[i]$ to dzielniki liczby pierwszej $p \in \mathbb{Z}$.
– Ponadto p jest rozkładalna w $\mathbb{Z}[i]$ wtedy i tylko wtedy gdy $p = a^2 + b^2$.
– Jeśli $p = 4k + 1$ to p rozkładalna (dow. $(p - 1)! \equiv_p -1$, $p|((2k)!)^2 + 1 = ((2k)! + i)((2k)! - i)$, ale $p \not| (2k)! + i$ więc p nie jest elementem pierwszym.)

3.22 Jeśli $f \in k[x]$ nierozkładalny, to $k[x]/(f)$ jest ciałem. (Bo $k[x]$ jest DIGiem, więc element nierozkładalny generuje ideał maksymalny.)

3.23 Twierdzenie: f w $k[x]$ jest nierozkładalny $\Rightarrow k[x]/(f)$ jest ciałem.

3.24 Wniosek: pierścień ilorazowy $k[x]/(f)$ jest nadciałem k, w którym f ma pierwiastek.

3.25 Przykłady: $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$, $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$, $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$, $\mathbb{F}_{27} = \mathbb{Z}_3[x]/(x^3 - x+1)$.

3.26 Jeśli $f \in k[x]$ jest nierozkładalny stopnia n, to ciało $k[x]/(f)$ jako przestrzeń liniowa nad k ma wymiar n.

3.27 W ciele p^n-elementowym każdy element $\neq 0$ spełnia tożsamość $x^{p^n-1} = 1$ (bo grupa multiplikatywna jest rzędu $p^n - 1$), zatem wielomian $x^{p^n} - x$ rozkłada się na p^n **różnych** czynników liniowych (z tw Bezout).

3.28 Przykład $p = 3$, $n = 2$: $f = x^9 - x = (x^3 - x)(1 + x^2 + x^4 + x^6)$. Pierwszy czynnik ma pierwiastki w $\mathbb{F}_3$

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

drugi czynnik ma pierwiastki w $\mathbb{F}_9 \setminus \mathbb{F}_3$. Rozkładamy dalej

$$(1 + x^2 + x^4 + x^6) = (x^2+1)(x^4+1) \equiv_3 \underbrace{(x^2+1)}_{f_1}\underbrace{(x^2+x-1)}_{f_2}\underbrace{(x^2-x-1)}_{f_3}\,.$$

Ciało $\mathbb{F}_3[x]/(f_k)$ ma 9 elementów (dla $k = 1, 2, 3$) i w nim wielomian f rozkłada się na czynniki liniowe.

Ćwiczenie: rozłożyć wielomian $x^2 + x - 1$ na czynniki liniowe w $\mathbb{F}_3[y]/(y^2+1)$.
(Dla uproszczenia nazwijmy obraz y w $\mathbb{F}_3[y]/(y^2+1)$ przez „i".)

4

Lokalizacja

4.1 $S \subset R$ system multiplikatywny $a, b \in S \Rightarrow ab \in S$. Gdyby $0 \in S$, to dalsza konstrukcja byłaby poprawna ale trywialna. Więc zakładamy, że $0 \notin S$. Np:
– $S = R \setminus I$, gdzie I jest ideałem pierwszym
– w szczegolności $S = R - 0$ gdy R jest bez dzielników zera
– $S = \{a^n \mid n \in \mathbb{N}\}$, gdzie a nie jest nilpotentny.

4.2 Pierścień $R_S = S^{-1}R$ to zbór ilorazowy $R \times S/\sim$, $(a, s) \sim (b, t)$, gdy istnieje $u \in S$ taki, że $uat = ubs$. Klasa $[(a, s)]$ oznaczana przez $\frac{a}{s}$

4.3 Jesli R bez dzielników zera, to mozna: $(a, s) \sim (b, t)$ gdy $at = bs$.

4.4 Dla R bez dzielników zera $S = R - 0$ ciało R_S oznaczane jest przez (R).

4.5 $k(x) := (k[x])$ ciało funkcji wymiernych o współczynnikach w k.

4.6 Przykłady lokalizacji $\mathbb{Z}$: $\mathbb{Z}_{(p)}$, $\mathbb{Q}$, $\mathbb{Z}[1/p]$.

4.7 Przekształcenie $\iota : R \to R_S$ ma jądro $Ann(S) = \{a \mid \exists s \in S\ sa = 0\}$. (Lokalizację można zrobić w dwóch krokach: najpierw podzielić przez $Ann(S)$, a potem użyć prostszej relacjii 4.3.

4.8 Uniwersalna własność: dane przekształcenie $f : R \to R'$, takie że $f(s)$ jest odwracalne. Wtedy istnieje dokładnie jedno $\bar{f} : R_S \to R'$ takie, że $f = \bar{f}\iota$.

4.9 Pierścienie lokalne i lokalizacja w ideale maksymalnym: $S = R \setminus \mathfrak{m}$.

4.10 Motywacja nazwy ,,pierścień lokalny,,: Niech X przestrzeń topologiczna $T_{3\frac{1}{2}}$ (tzn przestrzeń Tichonowa, tzn dla dowolnego zbioru domknietego i punktu poza nim istnieje funkcja zerująca się na tym zbiorze i nie zerująca się w danym punkcie), pierścień kiełków w x jest izomorficzny z $= C(X, \mathbb{R})/\mathfrak{m}_x$.

4.11 Dla $X = \mathbb{C}^n$ lub $\mathbb{R}^n$ zamiast funkcji ciągłych można brać funkcje C^∞, analityczne (tzn rozwijalne w szereg), algebraiczne (zadane wielomianem) itp.

Wielomiany o współczynnikach w pierścieniu DJR, podzielność

4.12 Każdy wielomian dzieli się z resztą przez $(x - a)$.

4.13 Ogólniej, jeśli wielomain g ma odwracalny wiodący współczynnik, to można dzielić z resztą przez g.

4.14 Tw Bezout $f(a) = 0$ to f dzieli się przez $x - a$ w $R[x]$. (Reszta z dzielenia f przez $x - a$ jest równa $f(a)$.)

4.15 Wniosek: Jeśli R jest nieskończonym pierścieniem bez dzielników zera, to przekształcenie $R[x] \to R^R$ (wielomian $f \mapsto$ funkcja wielomianowa $\bar{f}$) jest różnowartościowe.

Założenie: od tej pory do kryterium Eisensteina R DJR

4.16 Mówimy, że $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ jest prymitywny, jeśli a_i nie mają wspólnych czynników, tzn $NWD(a_0, a_1, \ldots, a_n) = 1$. Każdy wielomian można przedstawić jako $f = a \cdot prymitywny$.

4.17 Element $a = cont(f) = NWD(\text{wspólczynniki})$ z powyższego rozkładu nazywane jest zawartością wielomianu f.

4.18 Lemat: $cont(fg) = cont(f)cont(g)$.
Dowód: zakładamy, że f, g prymitywne. Niech $p|cont(fg)$. Redukujemy iloczyn fg modulo p. $\lightning$

4.19 Każdy wielomian można przedstawić jako produkt nierozkładalnych: elementów pierwszych z R i nierozkładalnych wielomianów prymitywnych. Pokażemy, że to rozkład na elementy pierwsze w $R[x]$.

4.20 Jeśli $p \in R$ jest pierwszy w R, to jest pierwszy w $R[x]$ (redukujemy $R[x]/(p) = (R/(p))[x]$ nie ma dzielników zera).

4.21 Jeśli $f, g \in R[x]$, f prymitywny. Niech $F = (R)$, $f|g$ w $F[x]$. Wtedy $f|g$ w $R[x]$
Dow: $cg = fh$ dla $c \in R$, $h \in R[x]$ i załóżmy, że c ma minimalną ilość czynników pierwszych. Przypuśćmy, że $p|c$, wtedy $p|h$ (bo $p \not| f$). $\lightning$

4.22 Lemat Gaussa: $0 \neq f \in R[x]$ i $f = gh$ w $F[x]$, to $f = g_0 h_0$ w $R[x]$, oraz $ag = g_0$, $bh = h_0$. (Wystarczy dla $g = g_0$ prymitywnego; z poprzedniego punktu.)

4.23 Jeśli $f \in R[x]$ prymitywny i nierozkładalny w $R[x]$, to pierwszy.
– f nierozkładalny w $F[x]$ (z Gaussa)
– $F[x]$ jest DIG, więc tam f jest pierwszy: $f|gh \Rightarrow f|g$ lub $f|h$. Podzielnośś w $F[x]$ implikuje podzielność w $R[x]$.

4.24 Wniosek: $f = x^n + \cdots + a_0$ ma pierwiastek w $F[x]$, to ma pierwiastek w $R[x]$.
Dw. Przypuśćmy, że $a \in F$ jest pierwiastkiem f, tzn $f = (x-a)g$ dla $g \in F[x]$. Piszemy $a = \frac{b}{c}$ dla $b, c \in R$, $(b, c) = 1$. Wtedy $(bx - c)|f$, $bx - c \in R[x]$. Zatem $f = (bx - c)h$ dla pewnego $h \in R[x]$, $h = dx^{n-1} + \ldots$. Współczynnik przy x^n w $(bx - c)h$ jest równy $bd = 1$. Zatem b jest odwracalny.

4.25 Wniosek: $R[x]$ jest DJR ($\star$ ACC i $\star\star$ nierozkładalne są pierwsze)

4.26 Wniosek: $R[x_1, x_2, \ldots, x_n]$ jest DJR.

5

5.1 Kryterium Eisensteina: założenia $f \in R[x]$, $p \not| a_n$, p dzieli pozostałe współczynniki wielomianu, ale $p^2 \not| a_0$. Wtedy f nierozkładalny w $F[x]$.
– po redukcji mod (p) $\bar{f} = \bar{a}_n x^n \neq 0$ w $R/(p)[x]$. Czynniki $\bar{f} = \bar{g}\bar{h}$, mają zerowe wyrazy wolne. Stąd wyraz wolny f podzielny przez p^2.

Ciała

5.2 Dla pary ciał $K \subset L$ definiujemy stopień rozszczerzenia $(L : K) = \dim_K L$.

5.3 Gdy $K \subset M \subset L$ to $(L : K) = (L : M)(M : K)$.

5.4 Niech $K \subset L$. Element $a \in L$ jest algebraiczny nad K gdy istnieje $f \in K[x]$ t.ż. $f(a) = 0$.

5.5 Załóżmy, że a jest algebraiczny nad K. Ideał $\{g \in K[x] \mid g(a) = 0\} = \ker(ev_a : K[x] \to L)$ jest główny, generowany przez pewien f o minimalnym stopniu. Ten wieleomian nazywa się wielomianem minimalnym, $K[x]/(f)$ jest ciałem. Obraz $K[x]$ w L jest podciałem, oznaczanym przez $K(a)$.

5.6 Element $a \in L$ jest algebraiczny nad K wtedy i tylko wtedy, gdy $(K(a) : K) < \infty$. Ponadto $(K(a) : K) = deg(f)$ jeśli f jest wielomioanem minimalnym.

5.7 Jeśl $a_1, a_2, \ldots, a_n \in L$ są algebraiczne nad K, to podpierścień

$$M = im(K[x_1, x_2, \ldots, x_n] \xrightarrow{ev_{a_\bullet}} L$$

jest podciałem i $(M : K) < \infty$.
Wniosek: jeśli a i b algebraiczne, to $a + b$ i ab są algebraiczne.

5.8 Różne typy rozszerzeń:
– rozszerzenia pojedyńcze $K(a)$ (każde rozszerzenie skończone nad ciałem charakterystyki 0 jest pojedyńcze – patrz [Browkin str 84, Tw. 22], np $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, ogólnie trzeba bracć $K(a, b) = K(a + tb)$ dla pewnego $t \in K$.)

– rozdzielcze: każdy $a \in L$ jest jednokrotnym pierwiastkem swojego wielomianu minimalnego. Tak jest zawsze dla ciał charakterystyki 0 i dla ciał skończonych. Kontrprzykładem jest $\mathbb{F}_p(x^p) \subset \mathbb{F}_p(x)$ (ciało funkcji wymiernych).
– rozszerzenie normalne: jeśli wielomian nierozkładalny $f \in K[x]$ ma pierwiastek w L, to rozkłada się na czynniki liniowe. Kontrprzykład $\mathbb{Q}(\sqrt[4]{2})$.

5.9 Ciało K jest algebraicznie domknięte, gdy każdy wielomioan ma pierwiastek. Równoważnie, każdy wielomian rozkłada się na czynniki liniowe.

5.10 Jeśli $K \subset L$ jest algebraicznym rozszerzeniem oraz każdy $f \in K[x]$ rozkłada się na czynniki liniowe w L, to L jest algebraicznie domknięte.
Dowód, przypuśćmy, że nierozkładalny $f \in L[x]$ nie ma pierwiastka. Niech L_0 będzie ciałem generowanym przez współczynniki f. Niech $M = L_0[x]/(f)$, $a := x \mod (f)$. Ciało M jest skończonym rozszerzeniem ciała K. Zatem a jest algebraiczny nad K i ma swój wielomian minimalny g. Z założenia g rozkłada się na czynniki liniowe w L, zatem $a \in L$. $\lightning$

5.11 Dla każdego wielomianu $f \in K[x]$ istnieje rozszerzenie algebraiczne L takie, że L rozkłada się na czynniki linowe w $L[x]$.

5.12 Konstrukcja algebraicznego domknięcia. Konstruujemy ciało L takie, że każdy $f \in K[x]$ rozkłada się na czynniki linowe w $L[x]$.

5.13 Przykład rozszerzeń niealgebraicznych: $\mathbb{Q}(\pi) \subset \mathbb{R}$, $\mathbb{Q}(\pi) \simeq \mathbb{Q}(x)$.

5.14 Każde dwa ciała charakterystyki 0, które s'a algebraicznie domknięte i mocy continnuum są izomorficzne:

$$\mathbb{Q}_p^\wedge\,, \qquad \mathbb{Q}(\{x_i\}_{i\in I})\,,$$

gdzie $\mathbb{Q}_p^\wedge$ jest ciałem ułamków $\mathbb{Z}_p^\wedge$ oraz $|I| = \mathfrak{c}$ mają algebraiczne domknięcia izomorficzne z $\mathbb{C}$.

5.15 Jeśli rozszerzenie L jest rozdzielcze i normalne bada się automorfizmy L, które są stałe na K. Jest to tzw grupa Galois $Aut_K(L) = G(L/K)$. Grupa Galois permutuje pierwiatki każdego nierozkładalnego wielomianu.

5.16 Przykład $G(\mathbb{Q}(\xi_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$, gdzie ξ_n jest pierwiastkiem pierwotnym z 1 stopnia n.

5.17 Dla $L = \mathbb{Q}(\sqrt[4]{2}, i)$ mamy $G(L/K) = D_8$.

5.18 Niech $\sigma_i(x_1, \ldots, x_n)$ będzie elementarną funkcją symetryczną. Niech $K = \mathbb{Q}(\sigma_1, \ldots, \sigma_m) \subset \mathbb{Q}(x_1, \ldots, x_m)$. Wtedy $GL/K) = \Sigma_n$.

5.19 $G(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \mathbb{Z}^\wedge$

5.20 $K \subset M \subset L$. Dla podgrupy $H < Gal(L, K)$ zbiór punktów stałych L^H jest ciałem. Dla podciała $M \subset L$ zbiór elementów grupy $G(L/K)$ stałych na L jest podgrupą.

5.21 Jeśli $K \subset L$ jest rozdzielcze i normalne to wyżej opisana odpowiedniość jest bijekcją pomiędzy podgrupami $G(L/K)$ a podciałami M zawierającymi K. W tej odpowiedniości podgrupy normalne odpowiadają rozszerzeniom normalnym.
Patrz teoria Galois.

6 Pierścienie Noetherowskie: odsyłacz [Eisenbud: Commutative Algebra with a View Toward Algebraic Geometry]

6.1 Pierścienie noetherowskie (definicja): każdy rosnący ciąg ideałów stabilizuje się. (Tzn. ACC, nie tylko dla ideałów głównych.)

6.2 Równoważny warunek: każdy ideał jest skończenie generowany.

6.3 W pierścieniu noetherowskim każdy element można przedstawić jako iloczyn elemntów nierozkładalnych (niekoniecznie pierwzych, np $k[x^2, x^3]$

6.4 Twierdzenie Hilberta o bazie: R noetherowski, to $R[x]$ noetherowski.
Dow. Skonstruujemy zbiór elementów f_m oraz ideał $I_m = (f_1, f_2, \dots, f_m) \subset I$. Pokarzemy, że dla pewnego n mamy $I_n = I$. Wielomian f_m dobieramy tak: to wielomian o najmniejszym stopniu należący do $I \setminus I_{m-1}$ jeśli $I_m \subsetneq I$. (W przeciwnym przypadku kończymy konstrukcję $\ddot{\smile}$.) Zauważmy $\deg f_\ell \geq \deg f_k$ dla $\ell > k$. Niech J będzie ideałem wiodących współczynników $J = (a_1, a_2, \dots)$ wielomianów f_m. Skoro R jest noetherowski, to $J = (a_1, a_2, \dots, a_n)$: wielomian $f_{n+1} \in I \setminus I_n$ ma wiodący współczynnik $a_{n+1} = \sum_{k \leq n} b_k a_k$. Biorąc kombinację wielomianów $\sum_{k \leq n} b_k f_k x^{\deg f_{n+1} - \deg f_k}$ dostajemy wielomian g z wiodącym współczynnikiem a_{n+1} i o tym samym stopniu, co f_{n+1}. Wielomian $f_{n+1} - g$ ma niższy stopień niż f_{n+1} co przeczy wyborowi f_{n+1}.

6.5 Wniosek $k[x_1, x_2, \dots, x_n]$ jest noetherowski.

6.6 Pierścień ilorazowy noetherowskiego są noetheowskie.

6.7 Pierścienie skończenie generowane nad noetherowskim są noetherowskie.

Związki z geometrią

6.8 Topologia Zariskiego w k^n: zbiory domknięte, to zbiory algebraiczne (tzn opisane skończonymi układami równań wielomianowych).
– jeśli $F_1, F_2 \in \mathfrak{F}$, to $F_1 \cup F_2 \in \mathfrak{F}$
– jeśli $A \subset \mathfrak{F}$, to $\bigcap_{F \in A} F \in \mathfrak{F}$
– $\emptyset, k^n \in \mathfrak{F}$

6.9 Indukowana topologia w podzbiorach algebraicznych.

6.10 Twierdzenie Hilberta o zerach *Nullstellensatz* (cz I). Gdy $k = \overline{k}$ to ideały maksymalne w $A = k[x_1, x_2, \dots x_n]$ są postaci $(x_n - a_n, x_1 - a_n, \dots, x_n - a_n)$ dla $(a_1, a_2, \dots, a_n) \in k^n$

$$\{\text{Ideały maksymalne w } A\} \;=\; k^n$$

(Równoważnie: każdy właściwy ideał ma wspólne zero.)
Oznaczenie: zbiór idałów maksymalnych $SpecMax\, A$.

6.11 Dowód wynika z tw Zariskiego: Jeśli $K \subset L$ jest rozszerzeniem ciał oraz L jest skończenie generowane jako pierścień nad K, to L jest roszerzeniem algebraicznym.
(złożenie $\phi : k \hookrightarrow k[x_1, x_2, \dots, x_n] \twoheadrightarrow k[x_1, x_2, \dots, x_n]/\mathfrak{m}$ jest izomorfizmem, $a_i := \phi^{-1}(x_1 + \mathfrak{m})$)

6.12 Jeśli $A = k[x_1, x_2, \dots x_n]/I$, $I = (f_1, f_2, \dots, f_m)$, to

$$\{\text{Ideały maksymalne w } A\} \;=\; X,$$

gdzie

$$X = \{(a_1, a_2, \dots, a_n) \in k^n \mid \forall j = 1, 2, \dots, m \quad f_j(a_1, a_2, \dots, a_n) = 0\}.$$

6.13 Dla $X \subset k^n$ niech

$$\mathfrak{I}(X) = \{f \in k[x_1, x_2, \dots, x_n] \,:\, \forall a \in X \;\; f(a) = 0\}.$$

To jest ideał.

6.14 Dla $E \subset k[x_1, x_2, \dots, x_n]$ niech $V(E)$ zbiór zer:

$$V(E) = \{(a_1, a_2, \dots, a_n) \in k^n \mid \forall f \in E \; f(a_1, a_2, \dots, a_n) = 0\}.$$

Jeśli I jest ideałem generowanym przez E, to $V(E) = V(I)$.

6.15 Z THoZ(cz I): jeśli $k = \bar{k}$ i $V(I) = \emptyset$ to $1 \in I$.

6.16 Twierdzenie Hilberta o zerach *Nullstellensatz* (cz II): Niech $I \subset k[x_1, x_2, \dots, x_n]$ będzie ideałem. Mamy

$$\mathfrak{I}(V(I)) = \sqrt{(I)}.$$

(Dow: Dla $f \in \mathfrak{I}(V(I)) = (f_1, f_2, \dots, f_k)$ niech $J = (I, 1 - fy) \subset k[x_1, x_2, \dots, x_n, y]$. Mamy

$$V(J) = (V(I) \times k) \cap V(1 - fy) \subset (V(f) \times k) \cap V(1 - fy) = \emptyset \subset k^{n+1}\,,$$

więc $1 \in J$

$$1 = \sum g_i f_i + h(1 - fy).$$

Bierzemy obraz w

$$k[x_1, x_2, \dots, x_n, 1/f] = k[x_1, x_2, \dots, x_n, y]/(1 - fy)\,.$$

mamy tożsamość $1 = \sum g_i f_i$, gdzie g_i zależą od $1/f$. Mnożąc przez f^N dostajemy tezę.)

6.17 Wniosek: Jeśli $X = V(I)$ jest zbiorem algebraicznym, to $V(\mathfrak{I}(X)) = X$. Ogólnie $V(\mathfrak{I}(X)) = \overline{X}$ jest domknięciem w topologi Zariskiego.

6.18 Abstrakcyjna definicja topologii Zariskiego w $SpecMax(A)$ nie odwołująca się do przedstawienia $A = k[x_1, x_x, \dots, x_n]/(f_1, f_2, \dots, f_k)$. Każdy ideał $I \subset A$ definiuje zbiór domknięty w $SpecMax(A) = \{$zbiór ideałów maksymalnych $\}$. Zbiory otwarte w języku ideałów

$$V(I) = \{\mathfrak{m} \in SpecMax(A) \,|\, I \subset \mathfrak{m}\}.$$

6.19 Zbiory otwarte w języku ideałów

$$U(I) = \{\mathfrak{m} \in SpecMax(A) \,|\, I \not\subset \mathfrak{m}\}.$$

Baza topologii

$$U(f) = \{\mathfrak{m} \in SpecMax(A) \,|\, f \notin \mathfrak{m}\},$$

gdzie $f \in A$.

6.20 Zbiory algebraiczne można rozkładać na składowe:
– $V(xy) = V(x) \cup V(y)$ suma osi, bo $(xy) = (x) \cap (y)$
– $V(x^2y, x^2z) = V(x^2) \cup V(y, z)$ suma prostej $y = z = 0$ i podwójnej płaszczyzny, bo $(x^2y, x^2z) = (x^2) \cap (y, z)$
– $V(xy, x^2) = V(x)$ ale $(xy, x^2) = (x) \cap (x^2, xy, y^2)$

6.21 Ideał prymarny: $ab \in I$, $b \notin I$ to $a^n \in I$ dla penego n (jedyne dzielniki zera w R/I to nilpotenty).

Rozkład ideału w pierścieniach noetherowskich - Rozkład prymarny [np R. Sharp: Steps in Commutative Algebra, roz. 4, Atiyah-MacDonald, roz 4]

6.22 R noetherowski, to każdy ideał dopuszcza przedstawienie $I = \bigcap Q_i$, gdzie Q_i nierozkładalny (Q_i nie da się przedstawić jako przecięcie większych ideałów).

6.23 Twierdzenie: R noetherowski, każdy Q nierozkładalny ideał jest prymarny.

7 Rozkład prymarny

7.1 Ex1 $R = K[x, y, z]/(xz - y^2)$, $P = (x, y)$ prymarny (a nawet pierwszy), ale P^2 nie.

7.2 Ex2 $R = K[x, y, z]$, $I = (x^2z^2, x(x + y^2), z(z - y^2))$.
Np w programie sage (`http://sage2.mimuw.edu.pl/`) trzeba napisać:

```
R.<x,y,z> = PolynomialRing(QQ)
I=(x^2*z^2,x*(x+y^2),z*(z-y^2))*R;
I.primary_decomposition()
```

A potem:

```
I.associated_primes()
```

7.3 Jeśli R jest noetherowski, to każdy ideał dopuszcza przedstawienie jako przecięcie ideałów nierozkładalnych. [Dowód taki jak: (ACC) $\Rightarrow$ każdy element jest iloczynem elementów nierozkładalnych.]

7.4 $V(I) \cup V(J) = V(I \cdot J) = V(I \cap J)$, zatem mając przedstawienie ideału

$$I = \bigcap Q_i$$

otrzymujemy rozkład

$$V(I) = \bigcup V(Q_i).$$

Jeśli ideały Q_i są nierozkładalne, to $V(Q_i)$ są zbiorami nierozkładalnymi. Udowodnimy, że ideały Q_i są prymarne, zatem $P_i = \sqrt{Q_i}$ są ideałami pierwszymi. Te ideały są nazywane stowarzyszonymi ideałami pierwszymi (pokażemy, że dla nieskracalnych rozkładów $ass(I)$ nie zależy od rozkładu). Mamy

$$V(I) = \bigcup_{P \in ass(I)} V(P).$$

W tym rozkładzie mogą się pojawić $P \subset P'$ (tzn $V(P) \supset V(P')$) więc wystarczy brać w rozkładzie $V(I)$ tylko minimalne ideały stowarzyszone.

7.5 Zbiór $(I : b) = \{x \in R \mid bx \in I\}$ jest idałem. Dla I prymarnego
– $\sqrt{(I : b)} = \sqrt{I}$ gdy $b \notin I$
– $(I : b) = R$ gdy $b \in I$

7.6 Twierdzenie: R noetherowski, każdy nierozkładalny ideał Q jest prymarny.
Dow: Niech $ab \in Q$, $b \notin Q$. Ciąg $\cdots \subset (Q : a^n) \subset (Q : a^{n+1}) \subset \ldots$ stabilizuje się. Załóżmy, że $(Q : a^n) = (Q : a^{n+1})$. Dowodzimy (*) $Q = (Q + (a^n)) \cap (Q + (b))$. Wtedy skoro $b \notin Q$, to $Q + (b) \neq Q$, więc $Q = Q + (a^n)$, czyli $a^n \in Q$.
(*) $r = g + ca^n = h + db \Rightarrow ca^{n+1} = ha + dab - ga \in Q \Rightarrow c \in (I : a^{n+1}) = (I : a^n) \Rightarrow r \in Q$.

7.7 Niech P będzie ideałem pierwszym. Mówimy, że Q jest ideałem P-prymarnym, jeśli $\sqrt{P} = Q$.
Lemat: Przecięcie ideałów P-prymarnych jest ideałem P-prymarnym.
Dowód: $ab \in Q_1 \cap Q_2$, $b \notin Q_1 \Rightarrow a^n \in Q_1 \Rightarrow a \in P = \sqrt{Q_1} = \sqrt{Q_1 \cap Q_2} = \sqrt{Q_2}$.

7.8 Mówimy, że rozkład $I = \bigcap Q_i$ jest minimalny, jeśli
1) wszystkie $P_i = \sqrt{Q_i}$ są różne,
2) dla każdego i mamy $\bigcap_{j \neq i} Q_j \not\subset Q_i$ (rozkład nieskracalny)
Każdy rozkład I na ideały prymarne można przerobić na rozkład minimalny.

7.9 Twierdzenie (bez dowodu): jeśli $I = \bigcap Q_i$ będzie nieskracalnym rozkładem na ideały prymarne, to zbiór ideałów pierwszych $\sqrt{Q_i}$ jest jednoznacznie wyznaczony.

8 Różne

8.1 Lemat: Jeśli $\sqrt{I} + \sqrt{J} = (1)$ to $I + J = 1$.
Dw: $a + b = 1$, $a^n \in I$, $b^m \in J$ to $1 = (a + b)^{m+n} \in I + J$.

8.2 Jeśli $\sqrt{I} = \mathfrak{m}$ jest ideałem maksymalnym, to I jest prymarny.
Dw: Niech $ab \in I$, $a \notin \sqrt{I}$, wtedy $(a) + \sqrt{I} = (1)$. Z lematu $(a) + I = (1)$, czyli $1 = ax + y$, $y \in I$. Stąd $b = abx + by \in I$.

Rozszerzenia przestępne ciał

8.3 Ciało funkcji wymiernych $k(x)$. Jeśli $\alpha \in k(x) \setminus k$, to rozszerzenie $k(\alpha) \subset k(x)$ jest algebraiczne.
Dow. $\alpha = f(x)/g(x)$, więc x spełnia równanie wielomianowe

$$\alpha g(x) = f(x)\,.$$

8.4 Twierdzenie Lürotha: Każde podciało $k \subsetneq L \subset k(x)$ jest izomrficzne z cia'lem funkcji wymiernych jednej zmiennej.
Dowód [Van der Waerden: Modern Algebra, Vol I (1949), §63 str. 198] korzysta z lematu Gaussa 4.21 oraz z następującego faktu:

8.5 Jeśli $g, h \in k[x]$ są względnie pierwsze to jeśli $f[z]$ dzieli $g[x]h[z] - h[x]g[z] \in k[x, z]$ to f jest stałą.
Dow: założyć, że k jest algebraicznie domknięte.

8.6 Niech L będzie skończenie generowanym rozszerzeniem ciała k. Mówimy, że układ elementów $a_1, a_2, \ldots, a_n$ jest algebraicznie zależny (nad k), jeśli istnieje nietrywialny wielomian $f(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$, taki, że $f(a_1, a_2, \ldots, a_n) = 0$.
Uwaga: Możemy też rpzważać układy nieskończone.

8.7 Jeśli układ elementów $a_1, a_2, \ldots, a_n$ jest algebraicznie zależny, to $k(a_1, a_2, \ldots, a_n)$ jest izomorficzny z ciałem ułamków pierścienia wielomianów $k[x_1, x_2, \ldots, x_n]$.

8.8 Załóżmy, że $\{a_1, a_2, \ldots, a_n\} \subset L$ jest układem algebraicznie niezależnym. Element $b \in L$ jest algebraicznie zależny, jeśli istnieje nietrywialny wielomian o współczynnikach w $k(a_1, a_2, \ldots, a_n)$, którego pierwiastkiem jest b.

8.9 Fundamentalny lemat (analog lematu o wymianie z algebry liniowej):
1) Załóżmy, że $\{a_1, a_2, \ldots, a_n\} \subset L$ jest układem algebraicznie niezależnym.
2) Załóżmy, że $\{a_1, a_2, \ldots, a_{n-1}, b\} \subset L$ jest układem algebraicznie nie zależnym.
3) Załóżmy, że $\{a_1, a_2, \ldots, a_n, b\} \subset L$ jest układem algebraicznie zależnym.
Wtedy a_n jest algebraiczne nad $k(a_1, a_2, \ldots, a_{n-1}, b)$.
Dw: Przyjmijmy $K = k(a_1, a_2, \ldots, a_{n-1})$. Z 3) istnieje wielomian $f[x, y] \in K[x, y]$, taki, że $f(a_n, b) = 0$. Wielomian musi zawieać zarówno x jak i y, bo inaczej 1) i 2) nie byłyby spełnione.

8.10 Dla każdego rozszerzenia $k \subset L$ istnieje maksymalny układ elementów algebraicznie niezależnych. Takie układy nazywają się bazami przestępnymi. Bazy przestępne są równoliczne. Liczebnośc bazy przest:epnej nazywa się stopniem przestępnym $degtr_k(L)$.

8.11 Każde rozszerzenie ciąła k można przedstawić jako złożenie

$$k \subset M = k(a_1, a_2, \ldots, a_n) \subset L = M/(f_1, f_2, \ldots f_r),$$

gdzie L jest rozszerzeniem algebraicznym, $f_i \in M[y_1, y_2, \ldots, y_m]$. Jeśli $char(k) = 0$, to można przyjąć, że rozszerzenie $M \subset L$ jest pojedyńcze i wtedy $m = 1$.

8.12 Geometryczna interpretacja M można traktować jako funkcje wymiernie na k^n, a L jako funkcje wymierne na podzbiorze $X \subset k^{n+m}$ opisanym przez funkcje wymierne f_i (zależące wielomianowo od y_j).

8.13 Ciała stopnia przestępnego 1 są izomorficzne z ciałami funkcji wymiernych na krzywych algebraicznych zdefiniowanych nad k.

8.14 Gdy $k = \mathbb{C}$ krzywe algebraiczne są powierzchniami Riemanna. Np krzywe eliptyczne opisane równaniem stopnia 3 w $\mathbb{C}^2$, można przyjąć, że równanie jest w postaci Weierstrassa $y^2 = x^3 + px + q$. Wtedy $L = \mathbb{C}(x)[y]/(y^2 - (x^3 + px + q))$.

Moduły

8.15 Moduły nad pierścieniem: przykłady
– wolny R^n

– ideał (to są dokładnie podmoduły R^1)
– R/I
– dla $R = k$: przestrzeń liniowa nad k
– dla $R = \mathbb{Z}$-moduł to grupa abelowa
– dla $R = k$, $k[x]$-moduł to przestrzeń liniowa nad k wraz z endomorfizmem.

8.16 Operacje na modułach
– suma prosta skończona = produkt skończony
– suma prosta nieskończona $\neq$ produkt nieskończony
– moduł ilorazowy
– jądro, kojądro
– iloczyn tensorowy
– operacje zmiany pierścienia bazowego

8.17 Klasyfikacja skończenie generowanych modułów nad pierścieniem DIG

$$M \simeq R^r \oplus \bigoplus_{i=1}^{N} R/(p_i^{k_i})$$

gdzie $p_i \in R$ element pierwszy, $k_i \in \mathbb{N}$.
(W przypadku gdy $M = R/I$, $I = \bigcap(a)$, $\prod p_i^{k_i}$ z tw chińskiego o resztach mamy tezę.)

8.18 Wnioski:
– Tw Jordana (dla $R = k[x]$), bo $p_i = (x - a_i)$, składnik wolny odpada, bo zakładamy $\dim M < \infty$
– Tw o klasyfikacji skończenie generowanych grup abelowych (dla $R = \mathbb{Z}$), bo p_i to liczby pierwsze.

8.19 Dla pierścieni noetherowskich mamy rozkład prymarny podmodułu w module skończenie generowanym. Jest to uogólnienie przypadku $I \subset M = R$.

Zadania o pierścieniach

24.1.2020

0.1 ♠ Udowodnić, że jeśli element u jest odwracalny, a n nilpotentny, to $u+n$ jest odwracalny.

0.2 ♠ Udowodnić, że zbiór elementów nilpotentnych jest ideałem.

0.3 ♠ Znaleźć elementy odwracalne w $\mathbb{Z}_4[X]$.

0.4 ♠ Pokazać, że jeżeli $a \in \mathbb{Z}_p^\wedge$ nie należy do ideału generowanego przez p, to a jest elementem odwracalnym.

0.5 ♠ Wykazać, że jeżeli R jest dziedziną całkowitości to $R[X]$ także jest dziedziną calkowitości. (Udowodnić także, że pierścień szeregów formalnych $R[[X]]$ jest dziedziną całkowitości.)

0.6 Niech $R = \mathbb{Z}[x]/(x^p - 1)$, gdzie p jest liczbą pierwszą.
a)♠ Czy R ma dzielniki zera?
b)♠ Czy R ma elementy nilpotentne?
c) Jakie elementy są odwracalne w $\mathbb{Q}[x]/(x^p - 1)$?

Uwaga: W $\mathbb{Z}[x]/(x^n - 1)$ jedynie dla $n = 1, 2, 3, 4, 6$ elementy odwracalne są postaci $\pm x^k$. W pozostałych przypadkach jest ich dużo więcej, np dla $n = 5$

$$(1 - x + x^2)(x + x^2 - x^4) = x + x^5 - x^6 \equiv 1\,.$$

patrz C. Polcino Milies, S.K. Sehgal - An Introduction to Group Rings-Springer (2002) §8, prop. 8.1.11-12, ex. 8.1.13.

0.7 Pomiędzy którymi pierścieniami istnieją odwzorowania: $\mathbb{Z}$, $\mathbb{Z}_{(p)}$, $\mathbb{Z}_{(q)}$, $\mathbb{Z}[1/p]$, $\mathbb{Z}_[1/q]$, $\mathbb{Z}_p^\wedge$, $\mathbb{Z}_q^\wedge$, $\mathbb{Z}_{p^n}$, $\mathbb{Z}_{q^m}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$?

0.8 ♠ Czy ideał $(7 + \sqrt{5})$ jest maksymalnym właściwym ideałem w $\mathbb{Z}[\sqrt{5}]$? A ideał $(4 + \sqrt{5})$?

0.9 ♠ Wykazać, że $R[x]$ jest DIG wtedy i tylko wtedy gdy R jest ciałem.

0.10 ♠ Wykazać, że następujące ideały są maksymalne:
a) $(2 + i) \lhd \mathbb{Z}[i]$
b) $(3 + \sqrt{2}) \lhd \mathbb{Z}[\sqrt{2}]$

0.11 ♠ Dla jakich liczb pierwszych ideał $(p) \lhd \mathbb{Z}[i]$ jest pierwszy?

0.12 ♠ Czy ideał $(x^2 + y^2 - 1, (x + y)^2 - 1)$ jest pierwszy w $\mathbb{R}[x, y]$?

0.13 Czy ideał $(x^2 + y^2 + 10y, x^2 - y) \lhd \mathbb{Q}[x, y]$ można przedstawić jako część wspólną ideałów maksymalnych?

0.14 Oznaczmy przez $\xi \in \mathbb{C}$ pierwiastek pierwotny z 1 stopnia n. Niech generator grupy $\mathbb{Z}_n$ działa na $\mathbb{C}[x, y]$ poprzez działanie na zmiennych $x \mapsto \xi x$, $y \mapsto \xi^{-1} y$. Udowodnić, że zbiór punktów stałych działania $\mathbb{Z}_n$ jest podpierścieniem w $\mathbb{C}[x, y]$. Przedstawić ten pierścien jako iloraz pierścienia wielomianów od 3 zmiennych.

0.15 ♠ Niech $I, J \lhd R$ będą ideałami, oraz $I + J = R$.
a) Niech IJ oznacza podgrupę R rozpiętą przez iloczyny ab, gdzie $a \in I,\ b \in J$. Udowodnić, że zbiór (ideał) IJ jest równy $I \cap J$.
b) Udowodnić, że dla każdej pary $a, b \in R$ istnieje element $x \in R$ taki, że

$$x = a \mod I \qquad \text{oraz} \qquad x = b \mod J\,.$$

Ponadto x jest wyznaczony jednoznacznie mod IJ.
Czy to ma coś wspólnego z tw Chińskim o resztach? Sformułować to twierdzenie w języku ideałów.

1 Euklid, DIG, DJR

1.1 ♠ Dla wybranego $d \in \{-2, 2, 3\}$ udowodnić, że $\mathbb{Z}[\sqrt{d}]$, $v(a + \sqrt{d}b) = |a^2 - db^2|$ jest pierścieniem euklidesowym (w tym napisie $|x|$ oznacza zwyłą wartość bezwzględną w $\mathbb{Z}$).

1.2 ♠ Udowodnić, że $\mathbb{Z}[\xi]$, gdzie ξ jest pierwiastkiem prymitywnym z 1 stopnia 3, wraz z normą $v(a + b\xi) := a^2 - ab + b^2$ jest pierścieniem euklidesowym.

1.3 ♠ Udowodnić, że $(x^2 - 2) \lhd \mathbb{Q}[x]$ jest ideałem maksymalnym.

1.4 ♠ Niech $R = \mathbb{Z}[\sqrt{-3}]/(p)$, gdzie p jest liczbą pierwszą. Udowodnić, że R jest izomorficzny z $\mathbb{F}_p \times \mathbb{F}_p$ (produkt pierścieni) jeśli $p \equiv 1 \mod 6$ lub $\mathbb{F}_{p^2}$ (ciało o p^2 elementach) gdy $p \equiv 5 \mod 6$.

1.5 ♠ Sprawdzić, że pierścień $\mathbb{Z}_7[X]/(X^3+2)$ jest ciałem. Znaleźć liczbe jego elementów. Korzystajac z algorytmu Euklidesa znaleźć w nim odwrotność elementu wyznaczonego przez wielomian $X + 1$.

1.6 ♠ W pierścieniu $\mathbb{Z}[i]$ znaleźć $NWD(2 + 11i, 1 + 3i)$. Znaleźć rozkład liczby 15 na czynniki nierozkładalne.

1.7 ♠ a) 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.
b) Pokazać, że istnieje nieskończenie wiele liczb pierwszych postaci $4k + 1$ oraz postaci $4k + 3$.

1.8 ♠ Pokazać, że w pierścieniu $\mathbb{Z}[\sqrt{5}]$ nie istnieje $NWD(4, 2 + 2\sqrt{5})$. Podać przykład elementu nierozkładalnego w $\mathbb{Z}[\sqrt{5}]$, który nie jest pierwszy. Podać przykład ideału w $\mathbb{Z}[\sqrt{5}]$, który nie jest główny.

1.9 ♠ Udowodnić, że z dokładnością do stowarzyszenia elementami pierwszymi w $\mathbb{Z}[\sqrt{2}]$ są:

(a) $\sqrt{2}$

(b) liczby pierwsze całkowite postaci $8n \pm 3$

(c) dzielniki $a + b\sqrt{2}$, $b \neq 0$ liczb pierwszych całkowitych postaci $8n \pm 1$.

1.10 ♠ W pierścieniu $\mathbb{Z}[\sqrt{-2}]$ znaleźć:

(a) $NWD(a + b\sqrt{-2}, a - b\sqrt{-2})$

(b) $NWD(6 + 4\sqrt{-2}, 8 - 2\sqrt{-2})$.

1.11 ♠ Znaleźć generator idału $I < \mathbb{Z}[\sqrt{2}]$
a) $I = (17, 6 + \sqrt[2]{\ })$
b) $I = (31, 8 + \sqrt[2]{\ })$

2 Zadania o ciałach skończonych

2.1 ♠ Rozłożyć wielomian $x^{16} - x \in \mathbb{F}_2[x]$ na wielomiany nierozkładalne.

2.2 ♠ Jeśli $K_1 \subset K_2$, to $|K_2| = |K_1|^d$.

2.3 ♠ Jeśli K jest ciałem, to $|K| = p^n$ dla pewnej liczby pierwszej.

2.4 ♠ W ciele q-elementowym wielomian $x^q - x$ rozkłada się na różne czynniki liniowe.

2.5 ♠ Grupa multiplikatywna ciała skończonego jest cykliczna.

2.6 ♠ Jeśli $K \supsetneq \mathbb{F}_p$ jest skończonym ciałem, to istnieje element ciała a nie należący do właściwego podciała, tzn $K = \mathbb{F}_p(a)$. (Za a można wziąć generator grupy cyklicznej.)

2.7 ♠ Jeśli $|K_1| = p^m$, $|K_2| = p^n$, $K_1 \subset K_2$, to $m|n$.

2.8 ♠ Jeśli $|K_1| = p^m$, $|K_2| = p^n$ i $m|n$ to isnieje włożenie $K_1 \to K_2$. Jeśli $|K_1| = |K_2| = p^n$ to $K_1 \simeq K_2$.

2.9 ♠ Jeśli K_1 i K_2 są podciałami ciała L i $|K_2| = |K_1|^d$, to $K_1 \subset K_2$. Jeśli K_1 i K_2 są równolicznymi podciałami ciała L to $K_1 = K_2$.

O automorfizmach ciał skończonych

2.10 ♠ Niech K ma p^n elementów. Przekształcenie $a \mapsto a^p$ jest homomorfizmem $K \to K$ (oznaczane ϕ od Frobeniusa).

2.11 ♠ Niech K ma p^n elementów. Zbiór rozwiązań równania $x^{p^k} - x$ jest podciałem K. Jeśli wielomian $x^{p^k} - x$ rozkłada się na czynniki liniowe w K, to k dzieli n. Wywnioskować, że dla każdego k istnieje ciało o p^k elementach.

2.12 ♠ Wszystkie podciała w K są postaci $K^{\phi^k} = \{a \in K \mid \phi^k(a) = a\}$. Niech $|\mathbb{F}_p(a)| = p^n$. Wykazać

$$\phi^k(a) = a \iff n|k.$$

2.13 Niech K ma p^n elementów i $n = st$, gdzie s i t są względnie pierwsze. Dane elementy $a, b \in K$ takie, że $|\mathbb{F}_p(a)| = p^s$ i $|\mathbb{F}_p(b)| = p^t$. Wtedy $\mathbb{F}_p(a + b) = K$. (Zbadać własności wielomianu $f_k(x) = \phi^k(x) - x$.)
Wskazówka: obliczyć wymiary $dim_{\mathbb{F}_p}(K)$, gdzie $K \in \{\mathbb{F}_p, \mathbb{F}_p(a), \mathbb{F}_p(b), \mathbb{F}_p(a, b)\}$ i udowodnić, że $\mathbb{F}_p(a) \subset \mathbb{F}_p(a + b)$.

2.14 ♠ Niech K ma p^n elementów. Rozłóżmy wielomian $x^{p^n} - x$ na nierozkładalne czynniki w $\mathbb{F}_p[x]$. Każdy element K jest pierwiastkiem dokładnie jednego czynnika. Jeśli $\mathbb{F}_p(a) = K$, to czynnik, którego a jest pierwiastkiem ma stopień n.

2.15 ♠ Niech K ma p^n elementów. Rozłóżmy wielomian $x^{p^n} - x$ na nierozkładalne czynniki w $\mathbb{F}_p[x]$. Jeden z czynników jest stopnia n i nie ma czynników wyższego stopnia.

2.16 ♠ Niech n_i będzie ciągiem liczb naturalnych takich, że $n_i|n_{i+1}$ oraz $\forall n \in \mathbb{N}\ \exists i \in \mathbb{N}\, n|n_i$. Niech K_i będzie ciałem o p^{n_i} elementach. Ustalmy włożenia $K_i \hookrightarrow K_{i+1}$. Niech $K = \bigcup K_i$. Udowodnić, że K jest algebraicznie domknięte.

2.17 Opisać grupę automorfizmów domknięcia algebraicznego $\mathbb{F}_p$.
Wskazówka: Wykazać, że każdy automorfizm ciała skończonego jest potęgą automorfizmu Frobeniusa $x \mapsto x^p$.

3 Inne

3.1 ♠ Czy $\mathbb{Z}_5[X]/(X^2+2)$ jest ciałem ? Znaleźć ideały maksymalne pierścienia $\mathbb{Z}_5[X]/(X^3+3X^2+2X+1)$.

3.2 ♠ Niech $K = (\mathbb{F}_p[x^p]) \subset L = (\mathbb{F}_p[x])$ będą ciałami funkcji wymiernych. Czy istnieje wielomian $f \in K[y]$, którego pierwiastkiem jednokrotnym w L jest x?

3.3 Czy ideał $(x^2+y^2+z^2-1, 4x^2+9y^2-1)$ jest pierwszy w $\mathbb{R}[x,y,z]$?

3.4 Czy jest prawdą, że: Pierścień R zawiera dokładnie jeden ideał pierwszy wtedy i tylko wtedy, gdy każdy jego element nieodwracalny jest nilpotentny.

3.5 Czy jest prawdą, że: każdy element pierścienia jest odwracalny lub nilpotentny lub podzielny przez element pierwszy.

3.6 Ideał Jacobsona definiujemy jako

$$J = \bigcap_{\substack{I < R \\ \text{maksymalny}}} I\,.$$

Wykazać, że $x \in J \Leftrightarrow \forall y \in R \;\; (1-xy)$ jest odwracalny.

3.7 ♠ Wykazać, że $\sqrt{I} = \{a \in R \mid \exists n \in \mathbb{N}\; a^n \in I\}$ jest ideałem.

3.8 ♠ Opisać grupę automorfizmów ciała $\mathbb{Q}(\sqrt[4]{2}, i)$, tzn grupę Galois $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$.

4 Zadania na po–świętach

4.1 ♠ Opisać grupę automorfizmów ciała $\mathbb{F}_{p^n}$

4.2 ♠ Niech p będzie liczbą pierwszą.
a) Udowodnić, że $\mathbb{Z}_p^\wedge[x]/(px-1)$ jest ciałem.
b) Czy wielomian $x^{p-1}-1$ rozkłada się na czynniki liniowe w $\mathbb{Z}_p^\wedge$?
c) Czy w $\mathbb{Z}_p^\wedge$ są pierwiastki z 1 stopnia p?

4.3 ♠ Korzystając z kryterium Eisensteina udowodnić, że

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

jest nierozkładalny w pierścieniu $\mathbb{Z}[X,Y]$.

4.4 ♠ Sprawdzić nierozkładalność wielomianów w $\mathbb{Z}[x]$ i $\mathbb{Q}[x]$:
a) $x^4+x^3+x^2+x+1$
b) x^3-7x^2+3x+3
c) $63x^3+21x^2+84$
d) $90x^3+135x+315$

4.5 ♠ Niech $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Znaleźć wielomian minimalny $\sqrt{2} + \sqrt{3} \in \mathbb{K}$ na $\mathbb{Q}$. Zbadać grupę automorfizmów $G(\mathbb{K}/\mathbb{Q}) = Aut(\mathbb{K})$.

4.6 ♠ Opisać grupę automorfizmów ciała $L = \mathbb{Q}(\sqrt[3]{2}, \xi)$, gdzie ξ jest pierwiastkiem wielomianu $x^2 + x + 1$. Opisać podciała $K \subset L$ i odpowiadające im podgrupy $G(L/K) \subset G(L/\mathbb{Q})$.

4.7 ♠ Pokazać, że dla pierścienia R następujące warunki są równoważne:
a) suma elementów nieodwracalnych jest elementem nieodwracalnym,
b) zbiór elementów nieodwracalnych jest ideałem,
c) w R istnieje dokladnie jeden ideał maksymalny.
Pierścien, jak wyżej nazywa sie lokalnym.

4.8 ♠ Udowodnić, że jeżeli $I \subset R$ jest ideałem pierwszym, zaś $S = R - I$ to pierścien $S^{-1}R$ jest lokalny.

4.9 ♠ Udowodnić, że $K[[X]]$ jest pierścieniem lokalnym, gdzie K jest ciałem.

Zadania „łatwe" o pierściemniach są w pliku
`https://www.mimuw.edu.pl/%7Eaweber/zadania/algebra2019/algebra2019latwe.pdf`
Przykładowe kolokwium o pierścieniach:
`https://www.mimuw.edu.pl/%7Eweber/zadania/algebra2014/kolok2.pdf`

5

5.1 ♠ Załóżmy, że jeżeli R jest pierścieniem Noetherowskim. Czy pierścień szeregów formalnych $R[[X]]$ jest także noetherowski?

5.2 ♠ Udowodnić, że jeśli $I \subset R$ jest ideałem przymarnym, to radykał $\sqrt{I}$ jest pierwszy. Poadać przykład, że odwrotne wynikanie nie zachodzi.

5.3 ♠ Znaleźć rozkład prymarny ideału $\langle x^2 + y^2 - 2y, x^2 - y\rangle \subset k[x, y]$.

5.4 ♠ Znaleźć conajmniej dwa rozkłady prymarne idału $\langle x^2, xy, xz\rangle \subset k[x, y, z]$. Obliczyć radykały czynników.

5.5 ♠ **Spektrum pierścienia** Niech R będzie pierścieniem i niech $Spec\, R$ oznacza zbiór ideałów pierwszych R. Dla dowolnego podzbioru $E \subset R$ niech $V(E)$ oznacza zbiór ideałów pierwszych zawierających E. Dla $a \in R$ oznaczamy $V(a) = V(\{a\})$. Sprawdzić, że: rodzina $\{V(E)\}_{E\subset R}$ spełnia aksjomaty rodziny podzbiorów domkniętych dla pewnej topologii na $Spec\, R$. Topologię tę nazywamy topologią Zariskiego.
Uwaga: w tej topologii punkty nie muszą by domknięte.

5.6 ♠ Udowodnić, że domknięcie dowolnego punktu $P \in Spec\, R$ w topologii Zariskiego to zbiór ideałów zawierających P. Ideały maksymalne są domkniętymi punktami.

5.7 ♠ Dany homomorfizm pierścieni $f : R \longrightarrow R'$. Wykazać, że branie przeciwobrazu ideału definiuje odwzorowanie ciągłe $f^* : Spec\, R' \longrightarrow Spec\, R$. Opisać odwzorowanie ciągłe $Spec\, \mathbb{C}[x] \to Spec\, \mathbb{R}[x]$ indukowane przez $\mathbb{R} \to \mathbb{C}$.

5.8 ♠ Przypuśćmy, że R zawiera dokładnie jeden ideał maksymalny $\mathfrak{m}$ oraz $\bigcap_{k=1}^{\infty} \mathfrak{m}^k = 0$.
– Mówimy, że ciąg elementów pierścienia spełnia warunek Cauchy'ego jeśli

$$\forall r \in \mathbb{N}\ \exists n_0 \in \mathbb{N}\ \forall m, n > n_0\ a_n - a_m \in \mathfrak{m}^r$$

– Mówimy, że ciąg elementów pierścienia jest zbieżny, jeśli istnieje $b \in R$ takie, że

$$\forall r \in \mathbb{N}\ \exists n_0 \in \mathbb{N}\ \forall n > n_0\ a_n - b \in \mathfrak{m}^r$$

Załóżmy że w R jest spełnione: *każdy ciąg Cauchy'ego jest zbieżny.*
Udowodnić Lemat Hensela: Niech $f = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in R[x]$. Przypuśćmy, że $f_0 = f \mod \mathfrak{m} \in R/\mathfrak{m}[x]$ rozkłada się na wielomiany $f_0 = (x - \bar{a})\bar{g}$ takie, że $\bar{g}(\bar{a}) \neq 0$. Wtedy istnieją wielomian $g \in R[x]$ i $a \in R$, takie, że $f = (x - a)g$ oraz $\bar{a} = a \mod \mathfrak{m}$ i $\bar{g} = g \mod \mathfrak{m}$.

(Mocniejsza wersja: patrz Eisenbud Th. 7.18.)

5.9 Niech X będzie przestrzenią topologiczną zwartą Hausdorffa i niech $C(X)$ będzie pierścieniem rzeczywistych funkcji ciągłych na X.

a) pokazać, że dla każdego punktu $x \in X$ ideał $I_x = \{f \in C(X) : f(x) = 0\}$ jest maksymalny.

b) (Gelfand) Udowodnić, że przekształcenie $\Phi : X \longrightarrow SpecMax\,(C(X))$, gdzie $\Phi(x) = I_x$ jest homeomorfizmem.

5.10 Niech X będzie przestrzenią topologiczną $x \in X$. Niech R będzie pierścieniem kiełków rzeczywistych funkcji ciągłych w x (elementy tego pierścienia są reprezentowane przez pary (U, f) gdzie U jest otoczeniem x, $f : U \to \mathbb{R}$)). Przy jakich załżeniach o X pierścień R jest lokalny?

5.11 Niech R będzie pierścieniem. Następujące warunki są równoważne:

a) $Spec\,R$ jest niespójne

b) $R \cong R_1 \times R_2$, gdzie R_1 i R_2 są pierścieniami niezerowymi.

c) R zawiera element $r \in R$, taki że $r^2 = r$, $r \neq 0$ i $r \neq 1$.

5.12 Niech $S \subset R$ będzie systemem multyplikatywnym w R, zaś $\iota : R \longrightarrow S^{-1}R$ homomorfizmem lokalizacji.

a) $\iota^* : Spec\,S^{-1}R \longrightarrow Spec\,R$ jest zanurzeniem homeomorficznym

b) jeżeli $S = \{1, a, a^2, ..\}$ to $\iota^*(Spec\,R_S) = U_a$

c) jeżeli $S = R \setminus I$, gdzie I jest ideałem pierwszym, to $\iota^*(Spec\,R_S) = \bigcap_{I \in U} U$, gdzie U jest otwartym otoczeniem I w $Spec\,R$.

5.13 Dana rodzina zbiorów $E_i \subset R$, $i \in I$. Załóżmy, że $\bigcup_{i \in I} U_i = SpecR$, gdzie $U_i = \{\mathfrak{p} \mid E_i \not\subset \mathfrak{p}\}$. Niech S_i będzie systemem multiplikatywnym generowanym przez S_i. Wykazać, że (omawiany na ćwiczeniach) ciąg

$$0 \to R \xrightarrow{\phi} \prod_{i \in I} S_i^{-1}R \xrightarrow{\psi} \prod_{i<j} S_i^{-1}S_j^{-1}R$$

jest dokładny, tzn ϕ jest mono, $im(\phi) = ker(\psi)$.

5.14 Gdyby powyższe zadanie sprawiało trudności, proszę założyć, że $R = \mathbb{C}[x_1, x_2, \ldots, x_n]$, zbiory E_i to układy równań wielomianowych, U_i to dopełnienie zbioru opisanego przez wielomiany ze zbioru E_i. Można założyć, że $|I| = 2$.
Zadanie sprowadza się do następującego stwierdzenia: Załóżmy, że $(f_1, f_2, \ldots, f_k, g_1, g_2, \ldots, g_\ell) = (1)$. Niech

$$F \in R[f_1^{-1}, f_2^{-1}, \ldots, f_k^{-1}], \qquad G \in R[g_1^{-1}, g_2^{-1}, \ldots, g_\ell^{-1}]$$

oraz $F = G$ w pierścieniu $R[f_1^{-1}, f_2^{-1}, \ldots, f_k^{-1}, g_1^{-1}, g_2^{-1}, \ldots, g_\ell^{-1}]$, wtedy F oraz G są obrazami pewnego elementu z R:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R & \xrightarrow{\Delta} & R[f_1^{-1}, \ldots, f_k^{-1}] \oplus R[g_1^{-1}, \ldots, g_\ell^{-1}] & \longrightarrow & R[f_1^{-1}, \ldots, f_k^{-1}, g_1^{-1}, \ldots, g_\ell^{-1}] \\ & & ? & \mapsto & (F, G) & \mapsto & F - G = 0 \end{array}$$

5.15 Niech k będzie ciałem, $L = k(a, b)$, Wykazać, że elementy a^3, b^3 i $a^2 + b^2 - 1$ są algebraicznie zależne.

5.16 Udowodnić twierdzenie Lürotha: Niech $L = k(x)$ oraz $M \subset L$ jest podciałem. Wykazać, że w M istnieje element y, taki, że $M = k(y)$.

Algebra I - Łatwe zadania do samodzielnego rozwiązania

1 Grupy

1 Sporządzić tabelkę działań dla grupy D_{2n}.

2 Sprawdzić, że w grupie D_{2n}, dla $n > 2$ istnieje tylko jedna podgrupa cykliczna rzędu n.

3 W grupie Σ_6 policzyć złożenie $(123)(546)(231)(46)$ przedstawiając je w postaci iloczynu cykli rozłacznych.

4 Cykl (453687) przedstawić w postaci transpozycji.

5 Permutację zbioru siedmioelementowego $f(1) = 4,\ f(2) = 2,\ f(3) = 6,\ f(4) = 3,\ f(5) = 1,\ f(6) = 7,\ f(7) = 5$ rozłożyć na cykle rozłączne.

6 Podać przykład podgrupy $H \subset D_6$ i elementu x takiego, że $xH \neq Hx$.

7 W grupie macierzy górnotrójkątnych o współczynnikach w $\mathbb{Z}$ rozmiaru 2×2 wskazać dwa elementy rzędu 2, których iloczyn ma rząd nieskończony.

8 Jakie są największe rzędy elementów w grupach permutacji Σ_9 i Σ_{15}.

9 Czy w Σ_{10} istnieją dwa elementy rzędu n, które mają różne rozkłady na cykle rozłączne? a) $n = 12$, b) $n = 9$.

10 Wypisać rzędy elementów w grupie cyklicznej $\mathbb{Z}_{12}$ i w D_{24}. Podać ile jest elementów danego rzędu.

11 a) Niech $Q_8 = \langle a, b\rangle \subset GL_2(\mathbb{C})$, $a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Ile elementów ma ta grupa? Opisać wszystkie podgrupy i znaleźć rzędy elementów.
b) Ile elementów ma grupa $\langle c, b\rangle \subset GL_2(\mathbb{C})$, $c = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$? Czy zawiera grupę Q_8?

12 Rozważmy grupy $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $\mathbb{Z}_{p^\infty} = \bigcup_{n\in\mathbb{N}} \mathbb{Z}_{p^n} \subset \mathbb{C}^*$, gdzie p jest ustaloną liczbą pierwszą. Udowodnić, że wśród tych grup żadne dwie nie są izomorficzne.

13 Niech $f : G \to H$ będzie homomorfizmem grup. $a \in G$. Wykazać, że $o(f(a))$ dzieli $o(a)$ o ile ten drugi jst skończony

14 Grupa $GL_n(\mathbb{C})$, tzn. macierzy odwracalnych $n \times n$ o współczynnikach w $\mathbb{C}$ działa na zbiorze wszystkich macierzy $n \times n$ poprzez sprzęganie:

$$C \cdot A := CAC^{-1}\,.$$

Opisać orbity działania.

15 Grupa macierzy odwracalnych $n \times n$ o współczynnikach w $\mathbb{R}$ działa na zbiorze symetrycznych macierzy w następujący sposób:

$$C \cdot A := CAC^{T}\,.$$

Opisać orbity działania.

16 Grupa macierzy izometrii $O(n)$ działa na zbiorze symetrycznych macierzy w następujący sposób:

$$C \cdot A := CAC^{T}\,.$$

Opisać orbity i stabilizatory punktów.

17 Niech $G < \Sigma_4$. Rozpatrzmy naturalne działanie G na zbiorze $\{1, 2, 3, 4\}$. Znaleźć orbity tego działania i grupy izotropii każdego punktu gdy $G = \langle(123)\rangle$ i $G = A_4$ (grupa parzystych permutacji).

18 Czy grupa rzędu 27 może działać na zbiorze 35 elementowym bez punktow stałych?

19 Przypuśćmy, że grupa G działa na zbiorze X oraz x i y leżą w jednej orbicie. Wykazać, że grupy izotropii G_x i G_y dla $x, y \in G$ są sprzężone (tzn $\exists g \in G\ gG_xg^{-1} = G_y$).

20 Niech $H < G$ i niech $\rho^H : G \to \Sigma_{|G/H|}$ będzie homomorfizmem odpowiadającym działaniu G na zbiorze warstw G/H danym wzorem: $g(g'H) = gg'H$. Znalezc $ker(\rho^H)$.

21 Ile jest homomorfizmów z Z_{24} do D_{24}?

22 Przypuśćmy, że grupa G ma pq elementów, gdzie p i q są liczbami pierwszymi, p nie dzieli $q - 1$. Udowodnić, że jeśli w G jest tylko jedna podgrupa rządu q, to G jest cykliczna.

23 Czy $D_4 = Q_8$? Opisać wszystkie homomorfizmy $D_4 \to Q_8$.

24 Znaleźć centralizator $g \in \Sigma_6$ gdy
– $g = (123)(45) \in \Sigma_6$,
– $g = (123)(456) \in \Sigma_6$,
– $g = (12)(34)(56) \in \Sigma_6$.
(Definicja: Centralizator elementu $C_G(g) = \{h \in G \mid \forall h \in G\ gh = hg\}$.)

25 Udowodnić, że dla $n > 2$, $Z(\Sigma_n) = 1$.

26 (a) Znaleźć $Z(A_4)$.
b) Wykazac, że w A_4 istnieje tylko jedna podgrupa rzędu 4, więc jest ona normalna.
c) Udowodnić, że w A_4 nie istnieje podgrupa rzędu 6.

27 Niech $H \triangleleft G$. Udowodnić, że dla dowolnych $x, y \in G$ jeżeli $xy \in H$ to $yx \in H$. Podać przykład, że jeżeli tylko $H < G$ to wynikanie nie ma miejsca.

28 Pokazać, że każda podgrupa w Q_8 jest normalna, choć Q_8 nie jest abelowa.

29 Udowodnić, że jeżeli $K \triangleleft G$ to $Z(K) \triangleleft G$. Podać przykład, w którym $Z(K) \neq K \cap Z(G)$.

30 Udowodnić, ze jeżeli $[G, G] \leq H$, to podgrupa H jest normalna w G.

31 Wykazać, że jeśli $|G| = p^2$, gdzie p jest liczbą pierwszą, to G jest abelowa.

32 Udowodnić, że $Q_8/\{1, -1\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

33 Załóżmy, że H_i jest podgrupą normalną w G_i dla $i = 1, 2$. Udowodnić, że $H_1 \times H_2$ jest normalna w $G_1 \times G_2$ i $(G_1 \times G_2)/(H_1 \times H_2) \simeq G_1/H_1 \times G_2/H_2$.

34 Niech $K < H < G$ oraz niech K i H będą podgrupami normalnymi. Wtedy $G/H \simeq (G/K)/(H/K)$.

35 Podać przykład grupy G i jej podgrup $K \triangleleft G$, $H \triangleleft G$ takich, że $K \simeq H$ ale $G/K \not\simeq G/H$.

36 Podac przyklad grupy G i jej podgrup $K \triangleleft G$, $H \triangleleft G$ takich, że $G/K \simeq G/H$ ale $K \not\simeq H$.

37 Niech $n > 2$. Udowodnić, że jeżeli n jest nieparzyste, to $Z(D_{2n}) = 1$, zaś jeżeli n jest parzyste to $|Z(D_{2n})| = 2$. Udowodnić, że w tym ostatnim przypadku $D_{2n}/Z(D_{2n}) \simeq D_n$ dla $n \geq 4$.
(Dla $n = 4$ mamy $D_8/Z(D_8) \simeq D_4 = \langle S, R \mid S^2 = 1,\ R^2 = 1,\ SRS = R\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.)

38 Niech $n > 2$. Opisać $D_{2n}/[D_{2n}, D_{2n}]$ w zależności od parzystości n.

2 Pierścienie

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

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

41 Znaleźć podpierścienie pierścienia $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

42 Udowodnić, że jeśeli R jest nieskonczoną, dziedziną calkowitości, to homomorfizm $\Phi : R[X] \to R^R$ dany wzorem $\Phi(f)(a) = f(a)$ jest monomorfizmem.

43 Udowodnić, że jeśeli x jest elementem nilpotentnym w pierścieniu R to $1 - x$ jest elementem odwracalnym. Wywnioskować, że suma elementu nilpotentnego i odwracalnego jest elementem odwracalnym.

44 Znaleźć elementy odwracalne w $\mathbb{Z}_4[X]$.

45 Udowodnić, że niezerowy pierścien skończony jest ciałem wtedy i tylko wtedy, gdy nie zawiera właściwych dzielnikow zera.

46 Wykazać, że jeżeli R jest dziedziną całkowitości to $R[X]$ także jest dziedziną calkowitości. (Udowodnić także, że pierścień szeregów formalnych $R[[X]]$ jest dziedziną całkowitości.)

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

48 Czy pierścień $\mathbb{Z}_8$ jest obrazem homomorficznym pierścienia Z_{24}?

49 Pokazać, że ideał pierścienia skończonego jest pierwszy wtedy i tylko wtedy gdy jest maksymalny.

50 Pokazać, że jeżeli $p|n$ to nie istnieje homomorfizm pierścieni $\mathbb{Z}[\frac{1}{n}] \to \mathbb{Z}_p$, gdzie $\mathbb{Z}[\frac{1}{n}]$ jest podpierścieniem $\mathbb{Q}$ generowanym przez $\frac{1}{n}$.

51 Udowodnić, że w $\mathbb{Z}[\sqrt{2}]$ każdy ideał jest główny.

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

53 Niech I_1 oraz I_2 będą ideałami pierścienia R. Wykazać, że zbiór $\{x_1 + x_2 \mid x_1 \in I_1,\ x_2 \in I_2\}$ jest ideałem generowanym przez $I_1 \cup I_2$.

54 Znaleźć wszystkie homomorfizmy pierścieni:
a) $\mathbb{Z}[X]/(X^2) \to Z_{24}$
b) $\mathbb{Z}[X, Y]/(X^2 - Y^3) \to \mathbb{Z}$
c) $\mathbb{Z}[X]/(X^n - 1) \to \mathbb{Q}$
d) $\mathbb{Z}[X]/(X^n - 1) \to \mathbb{C}$

55 Wykazać, że $\delta(a + b\sqrt{5}) = |a^2 - 5b^2|$ nie jest normą euklidesową, w pierścieniu $\mathbb{Z}[\sqrt{5}]$.

56 Znaleźć ciało ułamkow pierścienia $\mathbb{Z}[\sqrt{2}]$.

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

58 Udowodnić, że pierścień $\mathbb{Z}[\sqrt{2}]$ jest dziedziną z jednoznacznoscią rozkładu, a $\mathbb{Z}[\sqrt{5}]$ nią nie jest.

59 Udowodnić, że jeżeli K jest ciałem, to $K[X, Y]$ jest dziedziną z jednoznacznoscią rozkładu, ale $K[X, Y]/(X^2 - Y^2)$ nią nie jest, (jednoznaczność rozkladu nie dziedziczy się na pierścienie ilorazowe).

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

61 Znaleźć stosując algorytm Euklidesa $NWD(3456, 18564)$. Zapisać NWD jako kombinację liczb 3456 i 18564.

62 Wiedząc, że $\mathbb{Z}[\sqrt{-2}]$ jest pierścieniem euklidesowym znaleźć przy pomocy algorytmu Euklidesa $NWD(6 + 4\sqrt{-2}, 8 - 2\sqrt{-2})$.

63 W pierścieniu $\mathbb{Z}_5[X]$ znaleźć generator ideału $(x^3 - x^2 + 2x + 3, x^4 + 4x^3 + 3x^2 - 2x + 2)$.

64 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) $70x^4 + 315x^3 + 105$
d) $54x^4 - 108x^3 + 27$

65 Zbadać czy rozkładalne są wielomiany:
a) $x^4 + 15x^3 + 7$ w $\mathbb{Z}_5[x]$
b) $x^4 + 7$ w $\mathbb{Z}_{17}[x]$
c) $x^3 - 5$ w $\mathbb{Z}_{11}[x]$

66 Zbadać rozkladalność nad $\mathbb{Z}$ i $\mathbb{Q}$ wielomianu $x^4 + 15x^3 + 7$. (Wskazówka: zredukować modulo 5.)

67 Znaleźć kryterium nierozkladalności wielomianów stopnia 2 nad ciałem charakterystyki różnej od 2.

68 Wypisać nierozkładalne wielomiany stopnia 2 nad ciaiem $\mathbb{Z}_5$.

69 Udowodnić, że $\mathbb{C}[x, y]/(x^2 - y^3) \simeq \mathbb{C}[t^2, t^3]$.

70 Niech p będzie liczbą pierwszą. Udowodnić, że wielomian $x^{p-1} + ... + x + 1$ jest nierozkładalny w $\mathbb{Q}[x]$.

II Kolokwium z Algebry, 17 I 2020

Punktacja: zadania I–II po 10pt, zadanie III za 12pt, każdy podpunkt z części drugiej po 4pt. Rozwiązania zadań I–III proszę oddawać na oddzielnych kartkach.

Zadanie I.

Niech K będzie ciałem skonczonym, a $f \in K[X]$ wielomianem o niezerowym wyrazie wolnym. Wykazać, że f dzieli $X^n - 1$ dla pewnego n.

Zadanie II.

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.

Zadanie III.

Niech $\mathbb{K} \supset \mathbb{Q}$ będzie ciałem. Mówimy, że $a \in \mathbb{K}$ jest całkowity, gdy jest pierwiastkiem wielomianu postaci $a_o + a_1X + ... + a_{n-1}X^{n-1} + X^n$, $a_i \in \mathbb{Z}$. Pokazać, że jeżeli $d \in \mathbb{Z}$, $d \neq 0, 1$ i d bezkwadratowa, to zbiór elementów całkowitych ciała $\mathbb{Q}[\sqrt{d}]$ jest równy:

$$\mathbb{Z}[\sqrt{d}] \quad \text{dla} \quad d \equiv 2, 3\,(mod\ 4), \qquad\qquad \mathbb{Z}[\tfrac{-1+\sqrt{d}}{2}] \quad \text{dla} \quad d \equiv 1\,(mod 4).$$

Część Druga

Proszę podać krótkie uzasadnienie.

1 Zbadać, czy poniższy pierścień ilorazowy jest ciałem

$$\mathbb{Z}_3[X]/(x^3 + x^2 + x + 1, x^4 - x^2 + 1)\,.$$

2 Ile elementów ma pierścień $\mathbb{Z}[i]/(4+3i)$? Czy ma dzielniki zera?

3 Uzasadnić, że poniższy układ kongruencji ma rozwiązanie w pierścieniu $\mathbb{Z}[i]$:

$$a \equiv i \mod 1+2i\,, \quad a \equiv 1 \mod 7\,, \quad a \equiv 1+2i \mod 3.$$

4 Obliczyć $NWD(6+4\sqrt{-2}, 8-2\sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}]$.

5 Zbadać, czy wielomian $2X^8 + 22X^3 - 66X + 44$ jest nierozkładalny w pierścieniu $\mathbb{Z}[X]$ i w $\mathbb{Q}[X]$:

6 Czy $2 \in \mathbb{Z}[\sqrt{-3}]$ jest elementem nierozkładalnym, czy jest elementem pierwszym?

7 Znaleźć ideały maksymalne pierścienia $\mathbb{Z}_5[X]/(X^3 + 3X^2 + 2X + 1)$.

8 Znaleźć wszystkie homomorfizmy pierścienia $\mathbb{Z}[\sqrt{-5}][X]/(X^2+4)$ w pierścień $\mathbb{Z}_{10}$.

9 Niech $R = \mathbb{Z}_3[x]/(x^3+x^2+x+1)$. Opisać grupę automorfizmów R.

10 Niech $I = (x^7y^3, x^2 - zy^2) \subset \mathbb{C}[x,y,z]$. Przedstawić $\sqrt{I}$ jako część wspólną skończonej liczby idałów pierwszych.

Zadania

1. Niech B będzie podgrupą grupy G i niech A będzie podgrupą normalną grypy G.

a) Wykazać, że zbiór $A \cdot B = \{ab \mid a \in A,\ b \in B\}$ jest podgrupą grupy G. Czy $A \cdot B$ musi być podgrupą normalną grupy G? (uzasadnić lub podać kontrprzykład).

b) Niech $h : B \to (A \cdot B)/A$ będzie złożeniem $h = g \circ f$ homomorfizmu $f : B \to A \cdot B,\ f(b) = e \cdot b = b \quad \forall b \in B$ i homomorfizmu ilorazowego $g : A \cdot B \to (A \cdot B)/A$. Znaleźć $ker(h)$ i $im(h)$. Czy grupy $(A \cdot B)/A$ oraz $B/A \cap B$ są izomorficzne? (uzasadnić lub podać kontrprzykład).

2. Rozpatrzmy pierścień $R = Z_{18}[x]$.

a) Ile jest w pierścieniu R elementów nilpotentych postaci $ax^{10} + bx^2 + c$, gdzie $a, b, c \in Z_{18}$?

b) Ile jest w pierścieniu R elementów odwracalnych postaci $sx^7 + u$, gdzie $s, u \in Z_{18}$? Podać przykład takich $s, u \in Z_{18}, s \neq 0$, że element $sx^7 + u$ w R jest odwracalny oraz podać element do niego odwrotny.

3. Niech $R = Z[\sqrt{5}]$ i niech $S = Z_{11}$. Opisać wszystkie homomorfizmy pierścieni

a) $S \to R$,

b) $R \to S$.

4. W pierścieniu $R = Z[x, y]$ rozpatrzmy ideał $I = (2x, x + 3y)$. Czy ideał ten jest

a) główny?

b) pierwszy?

c) maksymalny?

5. Niech $R = Z[\sqrt{-7}]$.

a) Czy w pierścieniu R istnieje nierozkładalny element $a + b\sqrt{-7}$ taki, że $a^2 + 7b^2$ jest liczbą rozkładalną w Z?

b) Czy R jest dziedziną z jednoznacznością rozkładu?

PYTANIA NA EGZAMIN USTNY

♣ **2** Przykłady grup: cykliczne, wolne, liniowe, dihedralne, izometrii brył i inne

♣ **3** Warstwy G/H, indeks podgrupy

♣ **4** Twierdzenie Lagrange'a

♣ **5** Podgrupa normalna i grupa ilorazowa

♣ **6** Homomorfizmy, jądro, obraz

♣ **7** Twierdzenie o izomorfizmie

♣ **8** Produkt grup: prosty (kartezjański) i półprosty

♣ **9** Twierdzenie Cauchy'ego (o istnieniu elementu o pierwszym rzędzie)

♣ **W** Abelianizacja grupy, własność uniwersalna, przykłady

♣ **D** Działanie grup na zbiorze, orbity, stabilizatory, działanie na warstwach

♢ **2** Grupy permutacji, rozkład na cykle, własności grupy Σ_n

♢ **3** Przykłady grup prostych, prostota grupy A_n

♢ **4** p-grupy: moc zbioru punktów stałych działania, centrum, rozwiązalność

♢ **5** Twierdzenia Sylowa (dowód)

♢ **6** Twierdzenia Sylowa (zastosowania)

♢ **7** Grupy wolne

♢ **8** Grupy abelowe skończenie generowane, klasyfikacja

♢ **9** Grupy rozwiązalne, grupy nilpotentne

♢ **W** Wzrost grup skończenie generowanych

♢ **D** Pierścienie, ich homomorfizmy

♠ **2** Ideały (maksymalne, pierwsze, główne), iloraz przez ideał,

♠ **3** Pierścień wielomianów, jego i własności

♠ **4** Typy elementów (dzielniki zera, nilpotenty, idempotenty, elementy odwracalne, elementy nierozkładalne, elementy pierwsze)

♠ **5** Podzielność elementów, NWD (przykłady, że nie zawsze istnieje)

♠ **6** Nilradykał, radykał ideału

♠ **7** Pierscienie DJR. Warunek ACC

♠ **8** DIG $\Longrightarrow$ DJR

♠ **9** Pierścienie euklidesowe

♠ **W** Pierścień w $\mathbb{Z}[i]$ (liczby Gaussa), elementy pierwsze

♠ **D** Lokalizacja pierścienia w systemie multiplikatywnym

♡ **2** R jest DJR $\Longrightarrow$ $R[x]$ jest DJR

♡ **3** Kryterium Eisensteina

♡ **4** Rozszerzenia ciał (algebraiczność, stopień rozszerzenia). Ilorazy pierścienia $k[x]$.

♡ **5** Ciała skończone

♡ **6** Dowód istnienia algebraicznego domknięcia ciała

♡ **7** Pierścienie Noetherowskie. Twierdzenie Hilberta o bazie

♡ **8** Topologia Zariskiego w k^n (lub w $SpecMax(R)$)

♡ **9** Zbiory algebraiczne w k^n a ideały w $k[x_1, x_2, \ldots x_n]$, Twierdzenie Hilberta o zerach

♡ **W** Rozkład prymarny ideału pierścienia noetherowskiego

♡ **D** Rozszerzenia przestępne.