(tylko) Konspekt wykładu Algebra I*

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

v.16.11.2014

Notatki zawierają odsyłacze do podręczników

[BB] A. Biaynicki-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

[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 Przykłady: grupy permutacji, $\mathbb{K}_+$, $\mathbb{K}^*$, $\mathbb{Z}_n$, grupy liniowe $GL_n(\mathbb{K})$.

1.2 Grupy przekształceń: automorfizmy zbioru zachowujące jakąś strukturę np. dyfromorfizmy $\mathbb{R}$, 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.

1.3 Aksjomaty grupy. Jednoznaczność jedynki, jednoznaczność elementu odwrotnego.

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

1.5 Grupy wolne, grupy warkoczy

1.6 Grupa cykliczna, rząd elementu, rząd grupy.

1.7 Przedstwienie grupy (przyklad dla D_{2n}, Σ_n)

1.8 **Ćwiczenie:** sprawdzić, że wszystkie relacje w grupie dihedralnej wynikają z $S^2 = 1$, $R^n = 1$ i $SRS = R^{-1}$.

1.9 Podgrupy: wystarczy sprawdzić warunek $a, b \in H \;\Rightarrow\; ab^{-1} \in H$

1.10 Grupy macierzowe. Zanurzenie $\mathbb{Z} \hookrightarrow GL_2(\mathbb{R})$.

1.11 $SL_2(\mathbb{Z})$ generowana przez $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Relacje $A^4 = I$, $B^6 = I$, $A^2 = B^3$. (dość trudne do wykazania, ale że A i B generują można zrobić elementarnie.)

1.12 Przecięcie podgrup jest podgrupą

1.13 Podgrupa generowana przez zbiór A to najmniejsza grupa zawierająca A

1.14 Charakteryzacja wewnętrzna produktu.

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

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

1.17 Tw Lagrangea: rząd elementu dzieli rząd grupy

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

1.19 Małe tw Fermata $p|(a^p - a)$. Z tw Lagrange'a dla $G = \mathbb{Z}_p^*$ (p liczba pierwsza)

1.20 **Ćwiczenie:** Co dostajemy dla p nie będącej liczbą pierwszą? (tw Eulera)

2 Homomorfizmy

2.1 Homomorfizm grup, obraz, przeciwobraz podgrupy

2.2 Podgrupa normalna, równość warstw prawostronnych i lewostronnych

2.3 Jądro homomorfizmu, $f : G \to H$ jest monomorfizmem wtedy i tylko wtedy gdy $ker(f) = \{1_G\}$

2.4 Grupa ilorazowa, własność uniwersalna

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

2.6 Przykłady:
iloraz przestrzeni wektorowych,
$\mathbb{Z}_{mn}/\mathbb{Z}_m = \mathbb{Z}_n$ (Uwaga: jeśli $(m, n) \neq 1$, to $\mathbb{Z}_{mn} \not\simeq \mathbb{Z}_m \times Z_n$)
$\mathbb{Q}/\mathbb{Z}$=wszystkie pierwiastki z 1;
$Q_8/\{1, -1\} = \mathbb{Z}_2^2$ (ale $Q_8 \not\simeq Z_2^3$)

2.7 **Ćwiczenie:** $H/(N \cap H) \simeq (H \cdot N)/N$

2.8 **Ćwiczenie:** $N \subset H \subset G$, N normalna podgrupa, to $(G/N)/(H/N) \simeq G/H$

2.9 Produkt grup. Własność uniwersalna produktu.

3 Produkty, abelianizacja, działania

3.1 Wewnętrzna charakteryzacja produktu

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

3.3 Produkt pólprosty $A \rtimes H$ w sytuacji gdy dana grupa przemienna A oraz homomorfizm $\phi : H \to Aut(A)$. **Ćwiczenie:** Sprawdzić, że działanie $(a, g)(b, h) = (a + g(b), gh)$ spełnia aksjomaty grupy.

3.4 Komutant $[G, G]$ (generowany przez komutatory elementów $[a, b]$) i abelianizacja $Ab(G) = G/[G, G]$ (funktorialność).

3.5 Dla grupy abelowej A mamy $Hom(G, A) = Hom(Ab(G), A)$.

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

3.7 Grupy rozwiązalne $G_0 = G$, $G_{i+1} = [G_i, G_i]$ oraz dla pewnego i mamy $G_i = 1$.

3.8 G jest grupą prostą gdy nie ma właściwej nietrywialnej podgrupy normalnej.

3.9 Twiedzenie Jordan-Hölder (bez dowodu)

3.10 Przykłady grup prostych (dowody być może na ćwiczeniach)
– $\mathbb{Z}_p$,
– $A_n = \ker(sgn : \Sigma_n \to \mathbb{Z}_2)$ 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 $|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}$

3.11 Działanie (z lewej) grupy G na zbiorze X, to homomorfizm $G \to Aut(X)$.

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

3.13 Działanie grupy na sobie (z lewej i z prawej i przez z sprzęganie).

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

3.15 Automorfizmy wewnętrzne i zewnętrznie $Inn(G) := G/Z(G) \hookrightarrow Aut(G)$, $Out(G) := Aut(G)/Inn(G)$.
Ćwiczenie: $Inn(G) \lhd Aut(G)$

3.16 **Ćwiczenie:** Czy $Out(\Sigma_5) \neq 1$? Uwaga: $Out(\Sigma_6) \neq 1$.

4 Działania

4.1 **Ćwiczenie:** Rozkład permutacji z Σ_n na cykle rozłączne jako rozkład zbioru $\{1 \dots n\}$ na rozłaczne orbity działania podgrupy cyklicznej generowanej przez tę permutacje.

4.2 **Ćwiczenie:** Permutacje parzyste $A_n \subset \Sigma_n$. Twierdzenie: dla $n > 4$ grupa A_n jest prosta.

4.3 Jeśli G jest nieprzemienną grupą prostą, a $H < G$ podgrupą, to $(G : H) \geq 5$ i $|G|$ dzieli $(G : H)$

4.4 Przyklady: działanie grupy permutacji i grup liniowych, działanie grupy permutacji Σ_n przez zero-jedynkowe macierze z GL_n

4.5 Orbita działania Gx, stabilizator elementu (grupa izotropii) G_x, punkty stałe działania X^G. Iloraz X/G.

4.6 Działanie trywialne, działanie wolne, działanie efektywne, dzialanie przechodnie (tranzytywne)

4.7 Bijekcja $G/G_x \simeq Gx$ Moc orbity = indeks stabilizatora.

4.8 Przykład: dziłanie $G = \Sigma_5$ na $X = \{1, 2, 3, 4, 5\}$.
- To działanie jest nietrywialne, efektywne, przechodnie, ale nie jest wolne.
- G_5 = stabilizator elementu 5 jest izomorficzny z Σ_4, grupą permutacji zbioru $\{1, 2, 3, 4\} \subset X$. Utożsamaimy Σ_4 z $G_5 \subset \Sigma_5$.
- Orbita elementu 5 to $G \cdot 5 = X$ (bo działanie jest przechodnie)
- Mamy bijekcje $G/G_5 = \Sigma_5/\Sigma_4 \overset{\simeq}{\to} X$, $[\sigma] \mapsto \sigma(5)$.

4.9 Ćwiczenie: G działa na X. Jeśli $N \lhd G$, to jest dobrze określone diałanie G/N na X^N,

$$gN \cdot x := gx$$

4.10 Jeśli $|G| = p^k$, p liczba pierwsza, G działa na zbiorze X, to $|X| \equiv |X^G| \; mod \, p$

4.11 Działanie grupy na sobie przez automorfizmy wewnętrzne,
– orbity = klasy sprzężoności elementów,
– centrum grupy jako jądro odwzorowania $G \to Aut(G)$
– podgrupa normalna, jest podzbiorem zachowywanym przez sprzężenie
– centralizator podgrupy (lub zbioru) $C_G(H)$ 2 grupie G.
– normalizator podgrupy $N_G(H)$

4.12 Ćwiczenie: Centrum p-grupy jest nietrywiale.

4.13 Ćwiczenie: p-grupy są rozwiązalne.

4.14 Twierdzenia Sylowa (dokładnie wg [BT], str. 41-43)

5 Grupy abelowe, skończenie generowane

5.1 Przykład zastosowania twierdzenia Sylowa: Jeżeli p i q są różnymi liczbami pierwszymi i $|G| = pq$, $(p, q-1) = 1$, to $G \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_q$ jest cykliczna.

5.2 Jeżeli p i q są różnymi liczbami pierwszymi i $|G| = pq$, $(p-1, q) = (p, q-1) = 1$, to G jest cykliczna.

5.3 Istnieje dokładnie jedna (z dokładnością do izomorfizmu) grupa rzędu 255. (Bo 17-podgrupa Sylowa jest normalna oraz nie ma nietrywialnych działań $\mathbb{Z}_15$ na $\mathbb{Z}_17$.)

5.4 (do uzupełnienia) Jeśli $s_p = 1$ to p-grupa Sylowa jest *charakterystyczna*, czyli zachowywana przez każdy automorfizm. W szczególności jest normalna. Inne podgrupy charakterystyczne to np $[G, G]$, $Z(G)$.

Grupy abelowe=przemienne

5.5 Podpodgrupa elementów torsyjnych grupy abelowej $T(A)$, p-torsja $T_p(A)$

5.6 $A/T(A)$ jest beztorsyjna czyli $T(A/T(A)) = 0$

5.7 Produkty kartezjańskie i wolne w świecie grup (niekoniecznie przemiennych) oraz produkty kartezjańskie i sumy proste w świecie grup przemiennych. Porównanie własności uniwersalnych.

5.8 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) $\forall_p\ T_p(A) \cap \left(\bigoplus_{q<p} T_q(A)\right) = 0$.)

5.9 Ćwiczenie: Sprawdzić, że powyższa wewnętrzna suma prosta spełnia warunek: dla dowolnej rodziny homomorfizmów $f_p : T_p(A) \to B$ istnieje przekształcenie $f : A \to B$ takie, że $f_{|T_p(A)} = f_p$

5.10 Twierdzenie strukturalne dla skończenie generowanych grup abelowych

6 Klasyfikacja grup abelowych

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

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

6.3 Ćwiczenie: Grupa beztorsyjna może nie mieć powyższej własności

6.4 Jeśli $A < B$ i A/B wolna, wtedy $A \simeq B \times A/B$

6.5 $\mathbb{Z}^m \simeq \mathbb{Z}^n \Rightarrow m = n$

Grupy skończenie generowane

6.6 Jeśli $B \lhd A$, B generowane przez m generatorów, A/B generowane przez n generatorów, to A generowane przez $m + n$ generatorów (też jest prawda dla grup nieabelowych).

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

6.8 Podgrupy w $\mathbb{Z}^n$ są izomorficzne z $\mathbb{Z}^m$, $m \leq n$.

6.9 Doprowadzanie macierzy całkowitoliczbowej do postaci $(D, 0)$, gdzie G jest kwadratową macierzą diagonalna, a 0 oznacza blok zerowy

6.10 Niech Λ będzie podgrupą w $\mathbb{Z}^n$. Istnieje baza $\mathbb{Z}^n$: $v_1, v_2, \ldots v_n \in \mathbb{Z}^n$, oraz liczby $m \leq n$, $a_1, a_2, \ldots a_m \in \mathbb{N}$, takie,że $\mathbb{Z}^n$: $\lambda_1 v_1, \lambda_2 v_2, \ldots \lambda_m v_m$ jest bazą Λ.

6.11 Twierdzenie strukturalne dla skończenie generowanych grup abelowych

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

6.13 Jednoznaczność przedstawienia skończenie generowanej grupy abelowej.

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

6.15 Grupa abelowa skończenie generowana to $A \simeq A/T(A) \times T(A)$.

7 Koniec grup

7.1 Twierdzenia z algebry liniowej
a) twierdzenie Jordana – opis klas sprzężoności w $GL_n(\mathbb{C})$
b) diagonalizacja elementów grupy unitarnej $U(n)$ – sprzężenia torusa $(S^1)^n$ wypełniają $U(n)$ (analogicznie dla $SO(n)$)
c) rozkład KAN — grupa $GL_n(\mathbb{C})$ jest równa produktowi grup zwartej, abelowej i nilpotentnej (jako produkt zbiorów)

7.2 Było: Grupa jest rozwiązalna, jeśli istnieje ciąg podgrup $G = G_0 > G_1 > \cdots > G_s = 1$ taki, że $G_{i+1} > [G_i, G_i]$.

7.3 Równoważnie: w ciągu zdefiniowanym indukcyjnie $G_0 = G$, $G_{i+1} := [G_i, G_i]$ mamy $G_i = 1$ dla $i >> 0$.

7.4 Grupa jest nilpotentna, jeśli istnieje ciąg podgrup $G = G_0 > G_1 > \cdots > G_s = 1$ taki, że $G_{i+1} > [G, G_i]$. („Ciąg centralny")

7.5 Przykład: macierze górnotrójkątne z 1 na przekątnej.

7.6 Dla grupy nilpotentnej mamy $G_i \lhd G$, dla rozwiązalnej niekoniecznie.

7.7 Równoważnie: w ciągu zdefiniowanym indukcyjnie $\Gamma_0 = G$, $\Gamma_{i+1} := [G, \Gamma_i]$ mamy $\Gamma_i = 1$ dla $i >> 0$. To jest „dolny ciąg centralny".

7.8 „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

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

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

7.10

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

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

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

7.12 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 przy różnych wyborach generatorów są kwaziizometryczne: istnieje stała C, taka, że $\frac{1}{C} d_1(g, h) < d_2(g, h) < C\, d_1(g, h)$,
- wzrost grupy.

7.13 Grupy abelowe mają wzrost wielomianowy r^n, gdzie n to lilość generatorów.

7.14 Grupa wolna ma wzrost wykładniczy $(2n)^r$.

7.15 Ćwiczenie: Grupy nilpotentne maja wzrost wielomianowy: np grupa Heisenberga $\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$ ma wzrost $\sim r^4$.

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

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