# Notatki z algebr z tożsamościami

**wykład: prof. Jan Krempa**

spisał i uzupełnił: Arkadiusz Męcel (2010 r.)

## 1 Elementy algebry uniwersalnej

**Definicja 1.1** *Niech $D$ będzie rodziną symboli, przy czym $D = \dot{\bigcup} D_i$ gdzie $D_i$ – symbole $i$-argumentowe.* ***Algebrą*** *ze zbiorem działań $D$ nazwiemy zbiór $X$ wraz z przyporządkowaniem każdemu symbolowi $\phi_i \in D_i$ działania $i$-argumentowego w $X$. Formalnie, parę $\mathcal{F} = (F, \mu)$, gdzie $F$-zbiór, zaś $\mu : F \to \mathbb{N}$ nazywamy* ***typem algebry****. Mówimy, że para $A = (\underline{A}, F_A)$ jest algebrą typu $\mathcal{F}$ jeśli zbiory $F_A$ i $F$ są równoliczne i dla każdego $f \in F$ istnieje $f_A \in F_A$, że $f_A : A^{\mu(f)} \to A$. Element $f$ nazywamy* ***operacją $\mu(f)$-argumentową****.*

Przykłady:

1. **Krata:**

   $D_0 = \varnothing, D_1 = \varnothing, D_2 = \{\vee, \wedge\}$. Spełnione są przy tym następujące warunki równościowe:

$$\begin{array}{ccccccc} x \vee x & = & x & \quad & x \wedge x & = & x \\ x \vee y & = & y \vee x & & x \wedge y & = & y \wedge x \\ (x \vee y) \vee z & = & x \vee (y \vee z) & & (x \wedge y) \wedge z & = & x \wedge (y \wedge z) \\ x \vee (x \wedge y) & = & x & & x \wedge (x \vee y) & = & x \end{array}$$

   Przykłady krat:

   - Jeśli $X$ jest zbiorem niepustym, wówczas zbiór $2^X$ jest kratą ze względu na sumę i przecięcie.
   - Jeśli $X$ jest zbiorem niepustym z częściowym porządkiem $\leq$, przy czym dla dowolnych $x, y \in X$ istnieje $\sup x, y$ oraz $\inf x, y$. Wówczas operacje $\sup, \inf$ można przyjąć za działania kratowe.
   - Rozważmy zbiór liczb naturalnych $\mathbb{N}$. Wówczas jest on kratą ze względu na operacje $NWW(a, b)$, $NWD(a, b)$.

2. **Półgrupa:**

   $D_0 = \varnothing, D_1 = \varnothing, D_2 = \{\circ\}$. Spełniony jest przy tym następujący warunek:

$$x \circ (y \circ z) = (x \circ y) \circ z.$$

   Element $1 \in X$ nazywamy **jedynką półgrupy** jeśli $1x = x1 = x$. Element $0 \in X$ nazywamy **zerem półgrupy** jeśli $0x = x0 = 0$. Półgrupy z jedynką nazywamy **monoidami**.

3. **Grupa:**

   $D_0 = \{e\}, D_1 = \{^{-1}\}, D_2 = \{\circ\}$. Jest to monoid, w którym spełniony jest warunek: dla każdego $a \in G$ istnieje $b \in G$, że $a^{-1} = b$ oraz $aa^{-1} = e$.

   **Twierdzenie 1.2** *Zbiór $X$ z działaniem $\circ$ jest grupą ze względu na $\circ$, pewne działanie 1-argumentowe i pewne działanie 0-argumentowe $e$ wtedy i tylko wtedy, gdy $\circ$ jest łączne oraz dla każdego $x \in X$ istnieją: dokładnie jeden $z \in X$, że $xz = y$ i istnieje dokładnie jeden taki $t \in X$, że $tx = y$ oraz $X$ jest monoidem.*

**Definicja 1.3** ***Podalgebrą*** *algebry $A$ z działaniami $F_A$ nazwiemy taki niepusty podzbiór $B \subseteq A$, że dla każdego $\phi \in F_A$ przekształcenie $\phi|_B$ jest działaniem w $B$.*

Iloczyn kartezjański algebr tego samego rodzaju można wyposażyć w strukturę algebry.

**Definicja 1.4 (Homomorfizm)** *Niech $X, Y$ będą algebrami ze zbiorem działań $D = D_0 \cup D_1 \cup D_2 \cup \ldots$ Przekształcenie $\phi : X \to Y$ nazwiemy* ***homomorfizmem algebr*** *jeżeli dla każdego $d_i \in D_i$ i dla każdych $x_1, x_2, \ldots, x_i \in X$ mamy:*

$$\phi(d_i(x_1, x_2, \ldots, x_i)) = d_i(\phi(x_1), \phi(x_2), \ldots, \phi(x_i)).$$

Jeśli $X \subseteq Y$ jest podalgebrą, wówczas naturalne zanurzenie $X \to Y$ jest homomorfizmem. Jeśli $X_s$, $s \in S$ jest rodziną algebr tego samego typu, to naturalne rzutowania z produktu na współrzędne są homomorfizmami algebr.

**Definicja 1.5 (Kongruencja)** *Niech $\equiv$ będzie relacją w algebrze $X$. Powiemy, że jest to* ***kongruencja*** *jeżeli jest to relacja równoważności przy czym dla każdego $d_i \in D_i$ i dowolnych elementów $x_1, x_2, \ldots, x_i, y_1, y_2, \ldots, y_i \in X$ zachodzi następująca implikacja:*

$$x_1 \equiv y_1, x_2 \equiv y_2, \ldots, x_i \equiv y_i \Rightarrow d_i(x_1, x_2, \ldots, x_i) \equiv d_i(y_1, y_2, \ldots, y_i).$$

Każdy homomorfizm $\phi : X \to Y$ określa pewną kongruencję $\equiv_\phi$ na $X$ zadaną warunkiem:

$$x \equiv_\phi y \Leftrightarrow \phi(x) = \phi(y).$$

Na zbiorze ilorazowym tej kongruencji określić można działanie indukowane z algebr. Istotnie, jeśli $A$ jest algebrą i $\equiv$ jest kongruencją na $A$, wówczas zbiór $A/_\equiv$ jest również algebrą tego samego typu, jeśli dla dowolnego $m \geq 0$ i działania $m$-argumentowego $\phi$ przyjmiemy:

$$\phi_\equiv([a_1], [a_2], \ldots, [a_m]) := [\phi(a_1, a_2, \ldots, a_m)].$$

Wystarczy tu sprawdzić, że działanie $m$-argumentowe $\phi_\equiv$ jest dobrze określone. Ale to jest dość proste.

Niech $\alpha : A \to A/_\equiv$ będzie określone wzorem $\alpha(a) = [a]$. Okazuje się, że jest to homomorfizm algebr.

**Twierdzenie 1.6** *Niech $A, B$ będą algebrami tego samego typu i niech $\phi : A \to B$ będzie homomorfizmem algebr. Niech $\equiv_\phi$ będzie kongruencją odpowiadającą temu przekształceniu. Wówczas istnieje dokładnie jeden homomorfizm $\beta : A/_\equiv \to B$ spełający warunek $\phi = \alpha\beta$.*

**Definicja 1.7 (Krata zupełna)** *Każdy podzbiór tej kraty ma kres górny i dolny.*

**Twierdzenie 1.8** *Jeśli $A$ jest algebrą, to zbiór kongruencji algebry $A$ jest kratą zupełną z 0 i 1.*

**Definicja 1.9** *Jeśli $L$ jest kratą i $x \leq y \in L$, to zbiór $\{z \in L, x \leq z \leq y\}$ nazywamy* ***przedziałem*** *o końcach $x, y$. Taki przedział jest zawsze kratą z zerem $x$ i jedynką $y$.*

**Twierdzenie 1.10** *Niech $A$ niech będzie algebrą i $\equiv \in Con(A)$. Wówczas krata $Con(A/_{\equiv})$ jest naturalnie izomorficzna z przedziałem $[\equiv, 1]$.*

Dowód. Niech $\rho$ będzie kongruencją w $A$ taką, że $\equiv \leq \rho$. Przyjmujemy, że $[a]_{\equiv}\rho'[a']_{\equiv}$ wtedy i tylko wtedy, gdy $a\rho b$. W takim razie $\rho \to \rho'$, ■

**Wniosek 1.11** *Niech $\equiv \in Con(A)$ i niech $\rho' \in Con(A/_{\equiv})$. Wówczas algebry $(A/_{\equiv})/\rho'$ i $A/\rho$ są izomorficzne, gdzie $\rho$ to podniesienie $\rho'$ do $A$.*

Z algebrą można też związać kratę podalgebr ale tu mogą być pewne problemy. Rozważmy półgrupę bicykiczną $S = \{x^i y^j \mid (i, j) > (0, 0)\}$. Mnożenie dane jest wzorem:

$$(x^i y^j)(x^k y^l) = x^{i+k} y^{j+l}.$$

Jest to półgrupa przemienna. Zbiór potęg $x$ i zbiór $y$ to też podpółgrupa, a ich część wspólna jest pusta. Ale możemy wyjątkowo dopuścić zbiór pusty jako podalgebrę. Nie ma takiego problemu jeśli w algebrze występują działania 0-argumentowe.

**Definicja 1.12 (Algebra wolna)** *Niech $X$ będzie dowolnym zbiorem i niech $\tau$ będzie typem algebr. Algebrę $F(X)$ nazwiemy* ***algebrą wolną*** *typu $\tau$ jeśli $F(X)$ jest typu $\tau$, $X \subseteq F(X)$ jako podzbiór. Co więcej, dla dowolnej algebry $B$ typu $\tau$ i odwzorowania $X \to B$ istnieje dokładnie jeden homomorfizm $\overline{\phi} : F(X) \to B$, że $\overline{\phi}|_X = \phi$.*

**Twierdzenie 1.13** *Dla dowolnego typu $\tau$ i dla dowolnego niepustego zbioru $X$ istnieje algebra wolna $F(X)$.*

**Definicja 1.14** *Niech $\tau$ – typ algebr. Klasa $K$ algebr typu $\tau$ jest* ***definiowalna równościowo*** *jeśli w algebrze absolutnie wolnej $F(X)$, gdzie $X$ jest zbiorem przeliczalnym, istnieje zbiór par elementów $\{(f_i, g_i)\}$, że dla każdej algebry $B$ z klasy $K$ i dla każdego homomorfizmu $\phi : F(X) \to B$ mamy $\phi(f_i) = \phi(g_i)$, dla każdego $i$. Jeżeli zaś $C$ jest typu $\tau$, ale nie należy do $K$, to istnieje para $(f_i, g_i)$ i homomorfizm $\overline{\phi} : F(X) \to C$, że $\overline{\phi}(f_i) \neq \overline{\phi}(g_i)$. Jeśli $f_i \neq g_i$ to mówimy, że „$f_i = g_i$" jest tożsamością w klasie $K$.*

**Lemat 1.15** *Niech $\tau$ – typ algebr i niech $K$ – klasa algebr definiowalnych równościowo typu $\tau$. Załóżmy, że klasa ta wyznaczona jest przez zbiór tożsamości $f_i = g_i$, gdzie $f_i, g_i \in F(X)$. Niech $\equiv$ będzie najmniejszą kongruencją w $F(X)$ zawierającą wszystkie pary $(f_i, g_i)$. Wówczas:*

- *algebra $F(X)/\equiv$ jest wolna w klasie $K$,*
- *kongruencja $\equiv$ ma tę własność, że dla dowolnego homomorfizmu $\phi : F(X) \to F(X)$ jeśli $a \equiv b$, to $\phi(a) \equiv \phi(b)$ (tzw. kongruencja całkowicie charakterystyczna).*

**Twierdzenie 1.16 (Birkhoff)** *Jeśli $\tau$ jest typem algebr, to klasa $K$ algebr typu $\tau$ jest definiowalna równościowo wtedy i tylko wtedy, gdy klasa $K$ jest zamknięta ze względu na branie podalgebr, obrazów homomorficznych i produktów kartezjańskich. Klasę taką nazywamy* ***rozmaitością****.*

Załóżmy, że $\tau$ jest typem algebr, $X$ – zbiorem przeliczalnym, zaś $F(X)$ – algebrą wolną typu $\tau$ o zbiorze generatorów $X$.

**Twierdzenie 1.17** *Istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy rozmaitościami algebr typu $\tau$ i całkowicie niezmienniczymi kongruencjami algebry $F(X)$.*

Dowód. Szkic. Jeżeli $\equiv \in Con(F)$ jest całkowicie niezmiennicza, to jej przyporządkowujemy rozmaitość $V_\equiv$ takich algebr $A$ typu $\tau$, że każda para równoważna w $F(X)$ ma ten sam obraz w $A$ przy dowolnym homomorfizmie. To jest rozmaitość (BYŁO). Klasa $V_\equiv$ jest niepusta, bo $F(X)/\equiv \in V_\equiv$. Istotnie, jeśli $\phi : F \to F$ i jeśli $f \equiv g$, to $[\phi(f)] = [\phi(g)]$, z założenia o $\equiv$. Algebra $F(X)/\equiv$ jest algebrą wolną w rozmaitości $V_\equiv$ o zbiorze generatorów $X/\equiv$.

W drugą stronę. Jeśli $V$ jest rozmaitością, to relację $\equiv$ definiujemy w następujący sposób: $(f,g) \in \equiv$ jeśli dla dowolnej algebry $A \in V$ i dowolnego homomorfizmu $\phi : F(X) \to A$ mamy $\phi(g) = \phi(f)$. Ten homomorfizm wyznacza pewną kongruencję $\phi_\equiv$. Mamy więc zbiór algebr $A_i$ i zbiór homomorfizmów $\phi_i : F(X) \to A_i$ takich, że $\equiv$ jest przecięciem wszystkich kongruencji wyznaczonych przez $\phi_i$. Możemy więc stwierdzić, ze $F(X)/\equiv$ zanurza się w produkt prosty $A_i$, a więc jest także elementem rozmaitości $V$. Niech $\psi : F(X) \to F(X)$ będzie dowolnym endomorfizmem. Niech $\lambda : F(X) \to F(X)/\equiv$ będzie homomorfizmem naturalnym. Wówczas złożenie $\lambda\psi$ to homomorfizm $F(X) \to F(X)/\equiv \in V$. Wobec tego te pary, które przechodzą na to samo, muszą siedzieć w kongruencji. Zatem $\psi(f) = \psi(g) \Rightarrow f \equiv g$.

Pozostaje dowód wzajemnej jednoznaczności tej odpowiedniości. Jeśli przyporządkuję relacji $\equiv$ rozmaitość $V_\equiv$, to wiem, że $F(X)/\equiv \in V_\equiv$. Co więcej, z istnienia przekształcenia naturalnego wynika, że wszystkie tożsamości z $V_\equiv$ to $\equiv$. Podobnie w drugą stronę. Jeśli $V$ to rozmaitość, a $\equiv$ to odpowiadająca jej kongruencja, wówczas wszystkie algebry spełniające $\equiv$ to $V$. Istotnie, $F(X)/\equiv \in V$. Każda przeliczalnie generowana algebra spełniająca $\equiv$ też leży w $V$. Jeśli $Y$ jest dowolnym zbiorem, a $F(Y)$ – wolna algeba o zbiorze wolnych generatorów $Y$, wówczas w $F(Y)$ określić można relację równoważności $\rho$ w taki sposób, że jeśli $Z \subseteq Y$ jest przeliczalnym podzbiorem, to $F(Z) \subseteq F(Y)$ i na $F(Z)$ zadaję $\rho$ z $F(X)$. Wtedy $F(Y)/\rho \in V$.
■

**Definicja 1.18** *Niech $K$ – klasa algebr typu $\tau$.* ***Produktem prostym*** *zbioru algebr $A_i$, $i \in I$, że $A_i \in K$ jest taka algebra $A \in K$ oraz rodzina homomorfizmów $\pi_i : A \to A_i$, że dla każdej algebry $B$ i homomorfizmu $\phi_i : B \to A_i$ istnieje dokładnie jeden homomorfizm $\phi : B \to A$, że $\phi_i = \pi_i \circ \phi$.*

**Definicja 1.19** *Niech $K$ – klasa algebr typu $\tau$.* ***Produktem wolnym*** *zbioru algebr $A_i$, $i \in I$, że $A_i \in K$ jest taka algebra $A \in K$ oraz rodzina homomorfizmów $\sigma_i : A_i \to A$, że dla każdej algebry $C$ i homomorfizmu $\phi_i : A_i \to C$ istnieje dokładnie jeden homomorfizm $\phi : A \to C$, że $\phi_i = \phi \circ \sigma_i$.*

**Twierdzenie 1.20** *W rozmaitościach istnieją produkty proste i produkty wolne.*

**Definicja 1.21** *Algebrę $A$ nazywamy* ***rezidualnie skończoną*** *jeżeli $A$ można zanurzyć homomorficznie w produkt prosty algebr skończonych.*

**Konstrukcja półgrupy wolnej.**

Niech $X$ – zbiór niepusty. Niech $S(X)$ – zbiór skończonych słów o alfabecie $X$. Jako działanie dwuargumentowe w $S(X)$ przyjmujemy konkatenację.

**Twierdzenie 1.22** *Zbiór $S(X)$ jest półgrupą wolną o zbiorze wolnych generatorów $X$. Jeśli dodamy słowo puste, to otrzymamy monoid wolny o zbiorze wolnych generatorów $X$.*

**Konstrukcja grupy wolnej.**

Niech $X$ – dowolny zbiór. Bierzemy zbiór $X'$ – równoliczny z $X$, że jeśli $x \in X$, to odpowiada mu $x' \in X'$. Niech $Y = X \cup X'$. Biorę $S(Y)$, a więc monoid wolny nad $Y$. Niech słowo puste będzie jedynką. Rozważmy kongruencję półgrupową na $Y$, która utożsamia pary $xx' \sim 1$ oraz $x'x \sim 1$, dla każdego $x \in X$. Niegh $G(X) = S(Y)/\sim$. Elementy $G(X)$ mają reprezentantów postaci $y_1 y_2 \dots y_n$, gdzie $y_i \in X$ lub $y_i \in X'$. Z tego napisu można wykreślić pary $y_i y_{i+1}$, że jeden z elementów to $x$, a drugi to $x'$, dla pewnego $x \in X$. W ten sposób można dojść do słowa, w którym pary definiujące kongruencję nie występują. Jeśli $w_1$, $w_2$ są nieskracalne, to $w_1 w_2$ powstaje przez dopisanie. Takie $w_1 w_2$ ma reprezentanta o postaci skróconej. Mnożenie w $G(X)$ jest łączne, bo $G(X)$ to obraz homomorficzny półgrupy. Jedynka jest elementem neutralnym mnożenia i każdy element z $G(X)$ jest odwracalny. Wiadomo też, że $X \subseteq G(X)$. Wykażemy, że $G(X)$ jest wolne. Niech $G$ – dowolna grupa i niech $\phi : X \to G$ będzie dowolnym przekształceniem. Teraz rozszerzam $\phi$ to $\phi_1 : Y \to G$, gdzie $\phi_1(x) = \phi(x)$, zaś $\phi_1(x') = (\phi(x))^{-1}$. Skoro $G$ to monoid, to istnieje dokładnie jeden homomorfizm $\phi_2 : S(Y) \to G$, że $\phi_2|_Y = \phi_1$. No i teza, bo dla $x \in X$ mamy $\phi_2(xx') = \phi(x)(\phi(x))^{-1} = 1 = \phi_2(1)$. Wobec tego skoro generatory są w $X$, to istnieje dokł. jeden $\overline{\phi} : G(X) \to G$.

Można wprost wkazać grupę, że jest jednoznaczność zapisu. Jest to grupa macierzy generowana przez macierze postaci:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Jest też pewna ciekawostka. Wiadomo, że jeśli zamiast 2 wstawimy dowolną liczbę zespoloną o module różnym od 2, to grupa zostaje wolna. Ale dla liczb o module 2 nie wiadomo kiedy tak jest.

# 2 C-algebry

**Definicja 2.1 (C-algebra)** *Niech $C$ będzie pierścieniem przemiennym i łącznym z 1. Zbiór $A$ nazywamy algebrą nad $C$, jeżeli $A$ jest $C$-modułem, a mnożenie w $A$ jest $C$-dwuliniowe.*

Każdy pierścień jest $\mathbb{Z}$–algebrą.

Niech $R$ będzie pierścieniem. Niech $M_i$ $(i \in I)$ będzie rodziną lewostronnych $R$-modułów. Wówczas $\prod_{i \in I} M_i$ wraz z naturalnymi rzutowaniami $\pi_i$ jest produktem.

**Twierdzenie 2.2** *Niech $M = \prod_{i \in I} M_i$ oraz $\sigma_i : M_i \to M$ będą zanurzeniami. Niech $\bigoplus_{i \in I} M_i$ będzie podmodułem w $\prod_{i \in I} M_i$ generowanym przez $\sigma_i(M_i)$, dla $i \in I$, tzn. $\bigoplus_{1 \in I} = \sum_{i \in I} \sigma_i(M_i)$. Wówczas moduł $\bigoplus_{i \in I} M_i$ wraz z zanurzeniami $\sigma_i$ jest sumą prostą (koproduktem) rodziny modułów $\{M_i, i \in I\}$.*

Dowód. Jeśli $\alpha_i : M_i \to N$, to definiujemy: $\alpha : \bigoplus_{i\in I} M_i \to N$ wzorem $\alpha(f) = \sum_{i\in I} \alpha_i(f_i)$. Zauważmy, że $f_i = f(i) \in M_i, f : I \to \sum_{i\in I} M_i$. ■

Niech $R_i = R$ (zakładamy, że $R$ jest pierścieniem z 1). Wtedy $\bigoplus_{i\in I} R_i$ jest $R$-modułem wolnym, ze zbiorem generatorów $\sigma_i(1)$. Oczywiście ${}_RR$ jest $R$-modułem wolnym i $1 \in_R R$ jest wolnym generatorem $R$-modułu $R$. Ponieważ jeśli ${}_RN$ jest $R$-modułem i $n \in N$ oraz $\phi(1) = n$ (dla $\phi \in Hom_R(R,N)$), to wtedy $\phi(r) = \phi(r\cdot 1) = r\phi(1) = n$. Stąd $Hom_R(R,N) \simeq N$.

**Lemat 2.3** *Niech $\{A_i\}_{i\in I}$ będzie rodziną algebr wolnych typu $\tau$ o rozłącznych zbiorach wolnych generatorów $\{X_i\}_{i\in I}$. Wówczas koprodukt algebr z tej rodziny jest algebrą wolną typu $\tau$ ze zbiorem wolnych generatorów $X = \bigcup_{i\in I} X_i$.*

Dowód. Niech $B$ będzie $\tau$-algebrą oraz $\alpha : \sum_i X_i \to B$. Wtedy $\alpha_i : X_i \to B$ rozszerza się jednoznacznie do homomorfizmu $\tau$-algebr $\overline{\alpha_i} : A_i \to B$. Ponadto z definicji koproduktu mamy jednoznaczne rozszerzenie: $\overline{\alpha} : \coprod_{i\in} A_i \to B$. ■

Korzystając z lematu wiemy, że $\bigoplus_{i\in I} R_i = R^{(I)}$ jest modułem wolnym nad $R$ z bazą $\sigma_i(1) : i \in I\}$ równoliczną z I. Uwaga: grupa addytywna $\mathbb{Z}$ jest wolna o jednym generatorze. Zatem $\coprod_{i\in I} \mathbb{Z}$ jest grupą wolną o zbiorze wolnych generatorów równolicznym z $I$.

**Przykład 2.4** *Niech $A$ będzie grupą abelową i niech $End_{\mathbb{Z}}(A)$ będzie zbiorem endomorfizmów grupy abelowej. Wówczas $E = End_{\mathbb{Z}}(A)$ jest pierścieniem.*

Przyjmujemy, że:

$$(\alpha+\beta)(x) := \alpha(x) + \beta(x)(\alpha\cdot\beta)(x) := (\alpha\circ\beta)(x) = \alpha(\beta(x)).$$

Przy tym $x \in A$ oraz $E$ jest pierścieniem łącznym z $1 = Id_A$. Teraz $A$ jest $E$-modułem lewostronnym jeśli przyjmiemy:

$$\alpha\cdot x := \alpha(x), \qquad \text{dla } \alpha \in E, x \in A.$$

$$\begin{aligned} End_E(A) &= \{\phi : A \to A \,|\, \phi \,\text{jest R-liniowe}\} = \\ &= \{\phi \in E \,|\, \phi\circ\psi = \psi\circ\phi \,\text{dla}\, \psi \in E\} = \\ &= Z(E) \subseteq E. \end{aligned}$$

Jeśli $R$ jest dowolnym pierścieniem, to $End_{\mathbb{Z}}(R)$ jest pierścieniem. Ponadto dla $r \in R$ mamy $\phi_r(x) = rx$ dla $x \in R$. Wówczas $\phi_r \in End_{\mathbb{Z}}(R)$. Mamy homomorfizm $R \xrightarrow{\phi} End_{\mathbb{Z}}(R)$. Jeśli $lann(R) = 0$, to $\phi$ jest homomorfizmem.

Niech $R$ będzie $C$-algebrą (gdzie $C$ jest pierścieniem łącznym i przemiennym z 1). Niech $R^1 = R\oplus C$, jako $C$-moduł. Wprowadzamy mnożenie:

$$(r_1,c_1)(r_2,c_2) = (r_1r_2 + c_1r_2 + c_2r_1, c_1c_2)$$

$$(r_1+c_1)(r_2+c_2) = (r_1r_1 + c_1r_2 + c_2r_1, c_1c_2)$$

Widzimy więc, że zapis $(r, c) = r + c$ jest jednoznaczny. Wtedy $R^1$ jest $C$-algebrą z jedynką $(0, 1)$. Dodajmy, że $R \triangleleft R^1$ oraz $C$ jest $C$-podalgebrą w $R^1$.

**Przykład.**
Niech $R$ będzie $C$-algebrą, $R^1$ zaś $C$-algebrą $R$ z dołączoną 2. Wówczas mamy: $R^1 \ni r \to \phi_r \in End_{\mathbb{Z}}(R^1)$ (zanurzenie) czyli:

$$R \to R^1 \in End_{\mathbb{Z}}(R^1).$$

Mamy dla $r, s \in R$:

$$(r \circ s)(x) = r(s(x)), \quad \text{zaś } (rs)(x) = (rs)(x).$$

Jeśli $R$ nie jest łączna, to nie musi być $(rs) = r(sx)$, to $R^1$ nie musi być łączna, ale obie zanurzają się w algebrze łącznej $End_C(R^1)$.

Niech algebra $B$ będzie wyposażona w jedno 2-argumentowe działanie $\star$. Niech $R$ będzie pierścieniem łącznym z 1. Rozpatrzmy $R$-moduł wolny $R[B]$ o zbiorze wolnych generatorów $B$. Ponadto wprowadźmy w $R[B]$ mnożenie (rozszerza się dwuliniowo):

$$(r_1 b_1)(r_2 b_2) = (r_1 r_2)(b_1 \star b_2)$$

Ponadto mamy $B \ni b \to 1 \cdot b \in R[B]$, $(B \subseteq R[B])$. Wiadomo, że $R[B]$ jest łączny wtedy i tylko wtedy, gdy $\star$ jest łączna w $B$.

**Definicja 2.5 (Kwazigrupa)** *Zbiór $Q$ z działaniem dwuargumentowym $\star : Q \times Q \to Q$ spełniającym następującą własność: dla każdych $a, b \in Q$ równania $a \star x = b, y \star a = b$ mają jednoznaczne rozwiązania. Kwazigrupa z elementem neutralnym nazywana jest* ***pętlą.***

**Twierdzenie 2.6** *Niech $C$ będzie algebrą przemienną z 1, zaś $S$ – półgrupą wolną w zbiorze wolnych generatorów $X$. Wówczas $C[S]$ jest $C$-algebrą wolną w klasie $C$-algebr łącznych ze zbiorem wolnych generatorów $X$. Piszemy: $C\langle X \rangle = C[S]$.*

Dowód. Niech $A$ będzie $C$-algebrą łączną i niech $\phi : X \to A$. Wobec tego $\phi$ rozszerza się jednoznacznie do homomorfizmu półgrup: $\phi_1 : S \to A$. Ponieważ $C\langle X \rangle = X[S]$ jest $C$-modułem wolnym o bazie $S$, to $\phi_1$ rozszerza się jednoznacznie do homomorfizmu $C$-modułów: $\psi : C[S] \to A$ spełniającego $\psi|_S = \phi_1$. Podnadto $\psi$ jest również homomorfizmem $C$-algebr (zachowuje mnożenie). ■

# 3 Tożsamości w grupach

**Definicja 3.1** *Niech $G$ będzie grupą. Jeśli $x, y \in G$ to* ***komutatorem*** *$[x, y]$ tych elementów nazywamy wyrażenie $x^{-1}y^{-1}xy$. Grupę $G' = \langle\, [x.y] \,|\, x, y \in G \,\rangle$ nazywamy* ***komutatntem*** *grupy $G$.* ***Ciągiem pochodnym*** *grupy $G$ nazywamy ciąg:*

$$G^{(0)} = G, \quad G^{(1)} = G', \quad \ldots, \quad G^{(n+1)} = (G^{(n)})'.$$

*Grupę $G$ nazywamy* ***rozwiązalną*** *klasy $n$ gdy $G^{(n)} = 1$ oraz $G^{(n-1)} \neq 1$.*

**Definicja 3.2** *Niech $G$ – grupa, zaś $H, K$ – jej podgrupy.* ***Wzajemnym komutantem*** *tych podgrup, ozn. $[H, K]$ nazywamy podgrupę $G$ generowaną przez wszystkie komutatory $[h, k]$, gdzie $h \in H, k \in K$.*

**Definicja 3.3** *Podgrupę $H$ grupy $G$ nazywamy* ***charakterystyczną****, jeżeli $\phi(H) = H$ dla dowolnego automorfizmu $\phi$ grupy $G$. $H$ jest* ***całkowicie charakterystyczna*** *jeśli jest charakterystyczna oraz dla $\phi$ będących endomorfizmami mamy $\phi(H) \subseteq H$.*

**Lemat 3.4** *Niech $H \leq G$ – podgrupa. Jeśli $H$ jest charakterystyczna, to jest normalna. Jeśli jest całkowicie charakterystyczna, to jest charakterystyczna. Jeśli $G \triangleleft N$ i $H$ jest charakterystyczna w $G$, to $H \triangleleft N$.*

**Lemat 3.5** *Niech $H, K$ – podgrupy.*

- *Jeżeli $H, K \triangleleft G$, to $[H, K] \triangleleft G$.*
- *Jeżeli $H, K$ są charakterystyczna w $G$, to $[H, K]$ jest charakterystyczna w $G$ (tak samo dla całk. charakt.)*

Obejrzymy teraz kilka przykładów.

- W grupie abelowej część torsyjna jest całkowicie charakterystyczna.
- Ciąg pochodny każdej grupy ma wyrazy charakterystyczne.
- Można wykonać następującą konstrukcję ciągów: górnego i dolnego centralnego.
  - Górny ciąg centralny $Z_n(G)$ grupy $G$. Jako $Z_0(G)$ kładziemy grupę trywialną. Dalej:
  $$Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G)).$$
  - Dolny ciąg centralny $\Lambda_1(G) = [G, G] = G'$. Dalej:
  $$\Lambda_n(G) = [\Lambda_{n-1}(G), G].$$

  **Definicja 3.6** *Grupę $G$ nazywamy* ***nilpotentną*** *jeśli jej dolny ciąg centralny jest skończony.*

  **Twierdzenie 3.7** *Niech $G$ będzie grupą. Następujące warunki są równoważne.*

  1. *$G$ jest nilpotentna,*
  2. *w $G$ jest spełniona tożsamość $[x_1, x_2, \ldots, x_n] = 0$, dla pewnego $n$,*

  **Twierdzenie 3.8 (Baer)** *Niech $G$ będzie grupą nilpotentną. Następujące warunki są równoważne.*

  - *$G$ jest skończenie generowana*
  - *$G/G'$ jest skończenie generowana*
  - *$G$ spełnia warunek maksymalności na podgrupy*
  - *jeśli $\gamma_1(G)$ jest beztorsyjna, to każdy czynnik górnego ciągu centralnego jest też beztorsyjny.*

**Definicja 3.9** *Grupę nazywamy* ***rozwiązalną****, gdy jej ciąg pochodny stabilizuje się.*

Warto zanotować następującą uwagę: klasa grup rozwiązalnych jest zamknięta na branie rozszerzeń. Ale klasa grup nilpotentnych juz nie. Nawet rozszerzenie abelowej grupy przez abelową nie musi być nilpotentne. Rozszerzenie grupy abelowej przez grupę abelową nazywamy grupą **metabelową**.

**Twierdzenie 3.10** *Niech $G$ będzie grupą. Następujące warunki są równoważne.*

- *$G$ jest metabelowa*
- *$G'$ jest abelowe*
- *$G$ spełnia tożsamość: $[[x_1, x_2], [x_3, x_4]]$.*

Możemy rozpatrywać tożsamości ogólniejsze niż ta występująca wyżej. Niech $F(X) = F$ będzie grupą wolną o nieskończonym zbiorze wolnych generatorów $X$. Kładziemy:

$$\omega_1 = [x_1, x_2], \quad \dots, \quad \omega_{n+1} = [\omega_n(x_1, \dots, x_{2^n}), \omega_n(x_{2^n+1}, \dots, x_{2^{n+1}})].$$

**Twierdzenie 3.11** *Dla grupy $G$ równoważne są warunki:*

1. *$n$-ty wyraz ciągu pochodnego równy jest 1, dla pewnego $n \geq 1$,*
2. *$\omega_n(x_1, x_2, \dots, x_{2^n})$ jest tożsamością w $G$ dla pewnego $n \geq 1$,*
3. *istnieje ciąg podnormalny $1 = H_0 \triangleleft H_1 \triangleleft H_2 \dots \triangleleft H_r = G$ o czynnikach abelowych, dla pewnego $r \geq 1$.*

Dowód. Zaczniemy od implikacji $1 \Rightarrow 2$. Jeżeli $g_1, \dots, g_{2^n} \in G$, to:

$$\omega_1([g_1, g_2]) \in G'$$
$$\omega_2([g_1, g_2], [g_3, g_4]) \in G''$$
$$\dots$$
$$\omega_n(g_1, g_2, \dots, g_{2^n}) = 1.$$

Ale nasz początkowy ciąg został wybrany dowolnie. Mamy więc 2).

Teraz implikacja 2) $\Rightarrow$ 1). Indukcja ze względu na $n$. Jeśli $n = 1$, to $G$ jest abelowa i $G' = 1$. Niech $\omega_{n-1}$ nie będzie tożsamością. Niech $A$ będzie zbiorem postaci $\{\omega_{n-1}(g_1, \dots, g_{2^{n-1}})\}$. Co wiemy o zbiorze $A$? Jest on zamknięty na sprzęganie w $G$. Co więcej, $[a, b] = 1$, dla dowolnych $a, b \in A$. Zatem podgrupa $\langle A\rangle$ jest abelowa i jest normalna w $G$. Ale w $G/\langle A\rangle$ spełniona jest tożsamość $\omega_{n-1}$. Z założenia indukcyjnego mamy zatem, że $i$−ty wyraz ciągu pochodnego jest zawarty w $\langle A\rangle$. Zatem $i+1$-wyraz jest jedynką, bo $\langle A\rangle$ − abelowe.

Implikacja 1) $\Rightarrow$ 3) jest oczywista, zaś 3) $\Rightarrow$ 1) dowodzi się podobnie jak $1 \Rightarrow 2$).

■

**Twierdzenie 3.12** *Niech $G$ będzie grupą skończoną. Następujące warunki są równoważne:*

- *wszystkie czynniki kompozycyjne $G$ są cykliczne i ich rzędy są liczbami pierwszymi*
- *$G$ ma ciąg podnormalny o czynnikach cyklicznych*
- *każdy nietrywialny obraz $G$ ma nietrywialny abelowy dzielnik normalny*
- *ciąg pochodny grupy $G$ stabilizuje się na 1.*

Warunki te są równoważne **rozwiązalności** grupy skończonej. Jeżeli opuścimy warunek skończoności i w (2) dopuścimy grupy cykliczne nieskończone, to dostajemy klasę grup **policyklicznych.** Związek między rozwiązalnością a policyklicznością wyraża następujące twierdzenie:

**Twierdzenie 3.13 (P. Hall)** *Grupa rozwiązalna $G$ jest policykliczna wtedy i tylko wtedy, gdy spełnia warunek maksymalności na podgrupy.*

**Definicja 3.14 (Podgrupa Frattiniego)** *Jest to część wspólna wszystkich maksymalnych podgrup grupy $G$. Oznaczamy ją przez $\Phi(G)$. Jeśli w $G$ nie ma podgrup maksymalnych przyjmujemy, że jest to całe $G$ (interpretacja modułowa – radykał Jacobsona).*

**Definicja 3.15** *Element $g \in G$ nazywamy* ***niegeneratorem*** *grupy $G$ jeśli $g$ może być usunięty ze zbioru generatorów grupy $A$, tzn. dla dowolnego zbioru $S \subseteq G \setminus \{g\}$ jeśli $\langle S \cup \{g\} \rangle = G$, to $\langle S \rangle = G$.*

**Twierdzenie 3.16** *Jeśli $\Phi(G)$ jest skończona, to $G$ jest nilpotentna.*

**Lemat 3.17** *Jeśli $G$ jest rozwiązalna, to $G' \subseteq \Phi(G)$.*

**Definicja 3.18** *Niech $H \subseteq G$ będzie podgrupą, wówczas* ***normalizatorem*** *podgrupy $H$ w $G$, ozn. $N_G(H)$ oznaczamy największą podgrupę $P \subseteq G$ taką, że $H \triangleleft P$. Innymi słowy:*

$$N_G(H) = \{g \in G \,|\, g^{-1}Hg = H\}.$$

**Twierdzenie 3.19** *W grupie nilpotentnej każda podgrupa właściwa jest od swego normalizatora.*

**Twierdzenie 3.20** *Niech $G$ – skończona. Następujące warunki są równoważne.*

- *$G$ jest nilpotentna*
- *$G$ jest iloczynem prostym swoich $p$-podgrup Sylowa*
- *każda właściwa podgrupa w $G$ jest różna od swego normalizatora.*

* * *

Opowiemy o dwóch problemach Burnside'a:

1. [**General Burnside Problem**] Czy każda skończenie generowana grupa torsyjna jest skończona?
2. [**Bounded Burnside Problem**] Czy każda skończenie generowana grupa o skończonym wykładniku jest skończona?

**Twierdzenie 3.21** *BBP ma pozytywne rozwiązanie dla grupy $G$ w każdym z następujących przypadków:*

- *$G$ jest grupą rozwiązalną (odpowiedź jest wówczas pozytywna także dla GBP)*
- *$Exp(G) = 2$ (jasne, musi być wtedy abelowa)*
- *$Exp(G) = 3$ (Burnside)*

**Definicja 3.22** *Niech $\mathbb{K}$ będzie ciałem. Pogrupę $G \subseteq Gl_n(\mathbb{K})$ nazywamy* ***nieprzywiedlną*** *jeśli jej elementy generują $M_n(\mathbb{K})$ jako przestrzeń liniową nad $\mathbb{K}$. Podgrupy $Gl_n(\mathbb{K})$ nazywają się* ***grupami liniowymi****.*

**Twierdzenie 3.23 (Burnside)** *Niech $\mathbb{K}$ będzie ciałem i niech $G \subseteq Gl_n(\mathbb{K})$ będzie grupą nieprzywiedlną. Jeśli $G$ jest ograniczonego wykładnika, to $G$ jest skończona.*

Dowód. Dla dowolnych $A, B \in M_n(\mathbb{K})$ ślad jest operatorem dwuliniowym i przemiennym, tzn. mowa tu o funkcji: $(A, B) \to tr(AB)$. Jest to dodatkowo forma niezdegenerowana, to jest jeśli $tr(AB) = 0$ dla każdego $B \in M_n(\mathbb{K})$, wówczas $A = 0$.

Niech $e = Exp(G)$. Możemy założyć, że $\mathbb{K} = \overline{\mathbb{K}}$. Wynika stąd, że macierze dadzą się sprowadzić do postaci Jordana. Ponadto dla $g \in G$ wartości własne są pierwiastkami stopnia e z jedynki, bo $g^e = 1$. Ślad jak wiadomo jest ich sumą, zatem $|\{tr(g) \,|\, g \in G\}| < \infty$. Niech zbiór ten składa sie z elementów $\{\alpha_1, \ldots, \alpha_t\}$. Ponieważ $G$ jest nieprzywiedlna, to istnieją $g_1, g_2, \ldots, g_{n^2} \in G$, które tworzą bazę $M_n(\mathbb{K})$ nad $\mathbb{K}$.

Jeśli $x = (x_{ij}) \in G$, to $xg_i \in G$, a stąd $tr(xg_i) = \alpha_m$, dla pewnego $m \in \{1, \ldots, t\}$. Czyli mamy układ liniowy na współczynniki $x_{ij}$. Skończona liczba $g_i$ oraz $\alpha_m$ (oraz nieprzywiedlność) daje skończenie wiele rozwiązań, zatem rząd grupy $G$ jest skończony. ∎

**Wniosek 3.24** *Niech $char\mathbb{K} = 0$. Jeśli $G \subseteq Gl_n(\mathbb{K})$ ma ograniczony wykładnik, to $G$ jest grupą skończoną.*

Dowód. Indukcja względem $n$. Jeśli $n = 1$, wówczas $G \subseteq K^*$. Jeśli e = Exp(G), to $|G| \leq e < \infty$. Niech teraz $n > 1$. Możemy założyć, że $\mathbb{K} = \overline{\mathbb{K}}$. Jeśli $G$ jest nieprzywiedlna, to $|G| < \infty$ na mocy twierdzenia Burnside'a. Jeśli $G$ jest przywiedlna, to w $\mathbb{K}^n$ istnieje podprzestrzeń $G$-niezmiennicza $0 \neq V \subsetneq \mathbb{K}^n$, tzn. $G$ jest zawarta w macierzach postaci:

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Przestrzeń ta ma wymiar $0 < d < n$. Niech $\phi : G \to G_1 \times G_2$ przypisuje macierzy $g = \left(\begin{smallmatrix} a & * \\ 0 & b \end{smallmatrix}\right)$ parę macierzy $(a, b)$, przy czym $a \in M_d(\mathbb{K}), b \in M_{n-d}(\mathbb{K})$. Z założenia indukcyjnego $G_1, G_2$ są skończone. Ponadto jądro $\phi$ jest zawarte w zbiorze macierzy postaci $\left(\begin{smallmatrix} 1 & * \\ 0 & d \end{smallmatrix}\right)$. Ponieważ $char\mathbb{K} = 0$, to jądro musi być trywialne, inaczej nie byłoby skończonego wykładnika. ∎

**Twierdzenie 3.25 (Burnside, Schur)** *Niech $\mathbb{K}$ będzie ciałem dowolnej charakterystyki. Wówczas jeśli $G$ jest liniowa, skończenie generowana i torsyna, wówczas jest skończona.*

W twierdzeniu Burnside'a-Schura skończona generowalność ma znaczenie. Niech $char\mathbb{K} = p > 0$. Niech $n > 1$. Niech $G = UT_n(\mathbb{K})$ będzie grupą macierzy unitrójkątnych rozmiaru $n$. Wówczas $G$ jest skończonego wykładnika i jest nieskończona, gdy $\mathbb{K}$ jest nieskończone.

**Twierdzenie 3.26 (Sanow)** *BBP ma pozytywne rozwiązanie dla wykładnika równego 4.*

**Twierdzenie 3.27 (Higman, Hall)** *BBP ma pozytywne rozwiązanie dla wykładnika równego 6.*

Warto odnotować następującą uwagę. Niech $Exp(G) = 6$. Niech $G$ będzie skończenie generowana. Niech $G_2$ będzie maksymalną 2-podgrupą w $G$, zaś $G_3$ będzie maksymalną 3-podgrupą w $G$. Istnieją one na mocy tw. Sylova. Wiadomo, że $Exp(G_2) = 2, Exp(G_3) = 3$. Nie wiadomo jednak, czy grupy te są skończenie generowane.

Z rozumowania Higmana-Halla wynikło ponadto to, że RBP wystarczy rozważać wykładniki pierwsze. W późniejszych latach Adjan udowodnił, że wśród grup generowanych przez $d \geq 3$ elementy o wykładnikach nieparzystych większych lub równych 665, istnieją grupy nieskończone.

Rozważa się jeszcze kolejne dwa problemy:

3) Czy każda torsyjna grupa skończenie aproksymowalna (zanurzalna w produkt grup skończonych – produkt podprosty) jest skończona?

4) Czy wśród skończonych grup wykładnika $n$ o $d$–argumentach istnieje zawsze podgrupa największego rzędu? (Restricted Burnside Problem)

**Twierdzenie 3.28 (Kostrikin)** *Problem 4 ma pozytywne rozwiązanie gdy $n$ jest liczbą pierwszą, zaś $d$ jest dowolne.*

**Twierdzenie 3.29 (Zelmanov)** *Problem 4 ma pozytywne rozwiązanie dla dowolnych $n$ i $d$.*

**Twierdzenie 3.30 (Golod)** *Dla dowolnej liczby pierwszej $p$ i dowolnego $d \geq 2$ istnieje nieskończona $p$-grupa o $d$-generatorach, która jest nieskończona, skończenie aproksymowalna i każda jej podgrupa o co najwyżej $d$-1 generatorach jest skończona.*

Wynik Gołoda dostarczył negatywnej odpowiedzi na GBP oraz (3). Adian, Łysianok i Olszański podali przykłady obalające BBP.

**Definicja 3.31** *Niech $n, d > 1$. **Grupą Burnside'a** wykładnika $n$ o $d$ generatorach nazywamy grupę $B(d,n)$, która jest wolną grupą o $d$ generatorach w rozmaitości grup danej przez tożsamość $x^n = 1$.*

Drugi problem Burnside'a można sformułować tak: czy dla danych $n, d$ grupa $B(d,n)$ jest skończona? Niech $\overline{B}(d,n)$ będzie największą grupą skończoną wykładnika $n$ o $d$ generatorach. Istnienie jest zapewnione przez wyniki Zelmanova. Jest to obraz homomorficzny grupy $B(d,n)$ i przy ustalonych generatorach niech $H(d,n)$ będzie jądrem naturalnego homomorfizmu $B(d,n) \to \overline{B}(d,n)$. Wtedy drugi problem Burnside'a pyta czy $H(d,n)$ jest trywialna, czy nie?

**Twierdzenie 3.32** *Przy przyjętych oznaczeniach mamy:*

1. *$\overline{B}(d,n)$ jest grupą wolną w klasie grup skończonych o wykładniku $n$ (nie jest to rozmaitość) i ma $d$ wolnych generatorów,*

2. *jeśli $H(d,n)$ jest nietrywialna to ma prosty obraz homomorficzny nieskończony, ale skończenie generowany.*

Dowód. Niech $x_1, \dots, x_d$ będą generatorami $B(d,n)$, zaś $y_1, \dots, y_d$ będą generatorami $\overline{B}(d,n)$. Ponieważ $\overline{B}(d,n)$ jest wykładnika $n$, to siedzi w rozmaitości wyzn. przez $B(d,n)$. Mamy więc naturalny homomorfizm $\phi : B(d,n) \to \overline{B}(d,n)$ zadany wzorem $\phi(x_i) = y_i$. Chcemy pokazać, że $\overline{B}(d,n)$ jest wolna. Niech $G$ – skończona grupa wykładnika $n$ i niech $g_1, \dots, g_d \in G$. Bierzemy funkcję $\alpha(y_i) = g_i$. Chcemy móc rozszerzyć $\alpha$ do homomorfizmu. Przyjjmiemy więc, że $\beta(x_i) = g_i$. Jeżeli tak, to $\beta$ mogę rozszerzyć, bo jesteśmy w rozmaitości. Istnieje więc $\overline{\beta} : B(d,n) \to G$, że $\overline{\beta}(x_i) = \beta(x_i)$. Jak wygląda jądro $\overline{\beta}$? O $\overline{B}(d,n)$ wiemy, że jest największa w danej klasie. Weźmy pomocniczy homomorfizm $\gamma : B(d,n) \to \overline{B}(d,n) \times \langle g_1, \dots, g_d \rangle$ dany wzorem $\gamma(x_i) = (y_i, \alpha(y_i))$. Przekształcamy grupę wolną, więc można zadań przekształcenie jak chcemy na generatorach i rozszerzyć. Obraz $\gamma$ jest skończony i można go zrzutować na pierwszą współrzędną, czyli na $\overline{B}(d,n)$. Stąd obraz ma rząd nie mniejszy niż rząd samej grupy $\overline{B}(d,n)$, która jest rzutem tegoż. Ale $\overline{B}(d,n)$ była największego rzędu o $d$ generatorach. Zatem rzut jest różnowartościowy, a stąd tak naprawdę wynika, że drugi rzut musi być homomorfizmem. Łatwo widzieć, że $\ker(\gamma) = H(d,n)$. W tej sytuacji możemy określić homomorfizm $\overline{\beta} : \overline{B}(d,n) \to G$ przez przyjęcie, że $\overline{\alpha}(y_i) = \overline{\beta}(x_i)$.

Druga część dowodu. Przypuśćmy, że $H(d,n) \neq 1$. Z tego wynika, że $H(d,n)$ jest nieskończona, bo $\overline{B}(d,n)$ było największym obrazem. Ponieważ $H(d,n)$ma skończony indeks, to jest skończenie generowana (bo sk. ind. w sk. gen. jest sk. gen.), a jeśli tak, to niech $M$ – maksymalna podgrupa w $H(d,n)$ (istnieje, bo $H(d,n)$ skończenie generowana). Gdyby $M$ była skończonego indeksu, to $M$ moglibyśmy zastąpić mniejszą podgrupą, najpierw normalna, a potem charakterystyczną skończonego indeksu, nazwijmy ją $N$ (mamy prawo, bo jesteśmy w grupie sk. generowanej). Zatem $N \triangleleft B(d,n)$. Mielibyśmy więc skończony obraz grupy Burnside'a, którego obraz jest większego rzędu, niż $\overline{B}(d,n)$. Zatem $M$ ma indeks nieskończony. Tym bardziej, jeśli przyjmiemy, że $K \leq H(d,n)$ będzie maksymalnym dzielnikiem normalnym $H(d,n)$. On też ma indeks nieskończony. Teraz wystarczy wziąć $H(d,n)/K$. Jest ona prosta, nieskończona i skończenie generowana i ma wykładnik $n$. Nie wiemy, swoją drogą, ile generatorów ma $H(d,n)$.
■

**Twierdzenie 3.33 (Olszański)** *Niech $P$ będzie dostatecznie dużą liczbą pierwszą. Wówczas istnieje nieskończona $P$-grupa, w której każda właściwa podgrupa ma rząd $p$. Nazywa się ją Monstrum Tarstkiego, albo Monstrum Tarskiego-Olszańskiego.*

Przenosimy się na chwilę do świata półgrup. Tu też są klasy rozmaitości półgrup zadawane przez jedną zmienną. Nazywa się je periodycznymi. Równości te mają często postać:

$$x^k = x^l, \quad k < l$$

lub w przypadku półgrup z zerem: $x^k = 0$. Jest jeszcze inna klasa półgrup, która różni się od półgrup zadanych przez tożsamości jednej zmiennej. Nie jest rozmaitością, ale ma grupy wolne i jest ważna.

**Definicja 3.34** *Półgrupę $S$ nazywamy* ***skracalną****, czyli jeśli dla dowolnych $a, b, c \in S$ mamy implikacje:*

$$ac = bc \Rightarrow a = b, \quad ca = cb \Rightarrow a = b.$$

Klasa ta zawiera wszystkie grupy, ale też półgrupę wolną nad dowolnym alfabetem. Czy każda półgrupa skracalna jest podpółgrupą w pewnej grupie? Takie było pytanie.

**Twierdzenie 3.35** *Jeśli $S$ jest półgrupą przemienną i skracalną, to $S$ jest zanurzalna w grupę. Jest to grupa ułamków.*

Ogólnie, takie zanurzenie da się zrobić w różnych klasach, ale nie zawsze. Jest jednak przykład (Malcev) skończenie generowanej grupy skracalnej, która nie daje się zanurzyć w grupę. Półgrupy skracalne to nie jest, przy okazji, rozmaitość, bo warunki nie są tożsamościami, ale implikacjami. Okazuje się, że nie ma elementarnego kryterium (równościowego) kiedy półgrupę skracalną da się zanurzyć w grupę.

# 4 Tożsamości w algebrach

**Definicja 4.1 (Centroid)** *Niech $R$ będzie pierścieniem (niekon. z 1, a raczej bez).* ***Centroidem*** *pierścienia $R$ nazywamy zbiór*

$$C(R) = \{\phi : R_+ \to R_+ \,|\, \phi(ab) = \phi(a)b = a\phi(b) \,|\, a, b \in R\}.$$

Zauważmy, że $C(R)$ jest pierścieniem łącznym z 1, ze względu na dodawanie przekształceń i składanie. Prawie zawsze $C(R)$ jest przemienny. Dlaczego prawie zawsze? Gdyby pierścień $R$ miał zerowe mnożenie, wtedy byłyby to po prostu endomorfizmy grupy abelowej. A znaleźć grupę abelową, której pierścień endomorfizmów jest nieprzemienny, to jest ok. Niech $\alpha, \beta \in C(R)$. Policzmy $(\alpha\beta - \beta\alpha)(ab)$. Z definicji jest to $\alpha\beta(ab) - \beta\alpha(ab)$. Mamy więc tak: $\alpha(a\beta(b)) - \beta(\alpha(a)b)$. A dalej: $\alpha(a)\beta(b) - \alpha(a)\beta(b) = 0$. Tak wiec komutator dwóch elementów z centroidu zeruje $R^2$.

**Definicja 4.2** *Niech $C$ będzie przemiennym pierścieniem z 1. Pierścień $R$ nazywamy $C$-algebrą jeśli zadany jest homomofizm: $\phi : C \to C(R)$ taki, że $\phi(1) = 1$.*

Jeśli $R$ jest pieścieniem z 1, wówczas możemy przyjąć, że $\alpha(f) := f(1)$, dla $f \in C(R)$. Wtedy okaże się, że $\alpha$ jest homomorfizmem $C(R)$ w $R$ i obraz będzie podpieścieniem w centrum $R$. Jeśli $C_1$ i $C_2$ są przemienne i $\alpha : C_1 \to C_2$, że $\alpha(1) = 1$, to każda $C_2$-algebra jest $C_1$ algebrą. Może się więc zdarzyć, że nasze współczynniki w algebrze są zbyt rozdmuchane. Np. niech $K$ będzie ciałem. Każda $K[t]$-algebra jest $K$-algebrą, bo $K \subset K[t]$. Ale jeśli $A$ jest $K[t]$-algebrą, to bierzemy $tK[t]$ oraz iloraz: $A/(tK[t]A)$. Widzimy, że dostajemy $K$-algebrę. Teraz $K \simeq K[t]/tK[t]$.

Niech $C$ będzie pierścieniem przemiennym z 1. Niech $C\{X\}$ będzie $C$-algebrą wolną o nieskończonej liczbie generatorów. Niech $I$ – ideał w $C$. Wówczas $C\{X\}/IC\{X\} \simeq C/I\{X\}$ jest algebrą wolną nad $C/I$. Wprowadzimy oznaczenie. Jeśli $f \in C\{X\}$, to niech $z(f)$ będzie ideałem w $C$ generowanym przez współczynniki wielomianu $f$ (jako elementy algebry wolnych). Nazwiemy to **zawartością** tego elementu. Jeśli $S \subseteq C\{X\}$ jest podzbiorem, to zawartością $S$ nazwiemy zbiór $z(S)$, czyli ideał generowany przez $z(f)$, po wszystkich $f \in S$.

**Definicja 4.3** *Niech $A$ będzie $C$-algebrą. Powiemy, że $A$ jest* ***PI-algebrą****, jeśli ideał w $C\{X\}$ złożony z tożsamości na $A$ ma zawartość równą $C$.*

**Definicja 4.4** *Niech $n \geq 2$. Następujący wielomian:*

$$p_n(x_1, \dots, x_n) = \sum_{\sigma \in S_n} (-1)^\sigma x_{\sigma(1)} \dots x_{\sigma(n)}$$

*nazywany jest* ***n-tym wielomianem standardowym****.*

Zauważmy, że jeśli $1 \in C$, wówczas istnieją $f_1, \dots, f_r \in C\langle X \rangle$ takie, że $Z(\{f_1, \dots, f_r\}) = C$. Niech $\deg(f_i)$ to stopień ze względu na wszystkie możliwe zmienne. Powiemy, że $A$ jest PI algebrą stopnia $\leq d$ jeśli istnieje tożsamość stopnia $d$, za pomocą której można wygenerować 1.

**Lemat 4.5** *Niech $A$ będzie PI algebrą stopnia $d$. Wówczas istnieje skończony zbiór $S$ tożsamości stopnia $\leq d$ takich, że w każdej tożsamości każda zmienna występuje w każdym jednomianie. Jeśli niezerowe współczynniki tożsamości z $S$ są regularne*[1] *w $A$, to rodzinę $S$ można zastąpić przez tożsamości wieloliniowe.*

Dowód. Załóżmy, że $A$ spełnia tożsamość $f = f(x_1, x_2, \dots, x_n)$ stopnia $d$. Niech $f = f_1(x_1, x_2, \dots, x_n) + f_2(x_2, x_3, \dots, x_n)$, przy czym każdy jednomian w $f_1$ zawiera zmienną $x_1$, a $f_2$ nie zawiera $x_1$ w żadnym jednomianie. Wówczas kładąc $x_1 = 0$ widzimy, że $f_2$ jest tożsamością w $A$, a więc także $f_1$ nią jest. Bierzemy więc $f_1$ i wyróżniamy w nim sumę wielomianów, z których pierwszy w każdym jednomianie zawiera $x_2$, a drugi nie zawiera $x_2$ w żadnym jednomianie... Postępując analogicznie zredukujemy naszą wyjściową tożsamość do takiej, gdzie każda zmienna występuje w każdym jednomianie.

Załóżmy teraz, że $A$ ma tożsamość $f$ o współczynnikach regularnych. Na mocy powyższej procedury możemy założyć, że $f$ zawiera w każdym wielomianie każdą zmienną. Załóżmy, że nie jest to wciaż tożsamość wieloliniowa. Załóżmy na przykład, że zmienna $x_1$ ma wyższy stopień niż 1 w jednym z jednomianów tożsamości $f$. Wówczas rozważamy wielomian:

$$g(x_1, \dots, x_n, x_{n+1}) = f(x_1 + x_{n+1}, x_2, \dots, x_n) - f(x_1, x_2 \dots, x_n) - f(x_{n+1}, x_2, \dots, x_n).$$

Zauważmy, że jest to tożsamość na $A$. Łatwo widzieć, że jej stopień się nie zmienia. Z regularności dostajemy, że maksymalny stopień $x_1$ jest w $g$ o 1 niższy niż był w $f$. W ten sposób powoli redukujemy sprawę do tożsamości wieloliniowej. ∎

**Wniosek 4.6** *Jeśli $C$ jest ciałem, to każda PI algebra stopnia $d$ nad $C$ spełnia tożsamość wieloliniową stopnia $d$.*

Odnotujmy, że zgodnie z twierdzeniem Birkhoffa każda podalgebra PI algebry jest PI. Podobnie z obrazami homomorficznymi i produktami. Jeśli $f_1, f_2, \dots, f_n$ są tożsamościami dla algebr $A_1, \dots, A_n$, to iloczyn tych tożsamości jest tożsamością dla produktu prostego tych algebr. Stąd na przykład każda skończenie wymiarowa algebra nad swoim centrum (które jest PI-podalgebrą) jest PI.

[1] Element $c \in C$ jest regularny w $A$ jeśli $ca = 0 \Rightarrow a = 0$ dla $a \in A$.

**Definicja 4.7** *Pierścień $R$ nazywamy pierwszym jeśli w $R$ iloczyn niezerowych ideałów jest zawsze niezerowy.*

Dlaczego nas interesują pierścienie pierwsze?

**Lemat 4.8** *Jeśli $R$ jest pierścieniem pierwszym, wówczas centroid $C(R)$ jest dziedziną przemienną i jego elementy niezerowe są regularne w $R$.*

Dowód. Zakładamy, że $R$ jest pierścieniem niezerowym. Niech $\alpha \in C(R)$. Wiadomo, że $\ker(\alpha)$ oraz $\alpha(R)$ są ideałami w $R$. Zauważmy, że dla każdego $r \in \ker(\alpha)$ oraz $t \in R$ mamy: $r\alpha(t) = \alpha(r)t = 0$. Stąd $\ker(\alpha) \cdot \alpha(R) = 0$. Z pierwszości $R$ wynika, że jeśli $\alpha$ było elementem niezerowym $C(R)$, to $\ker(\alpha) = 0$.

Dlaczego $C(R)$ jest dziedziną. Załóżmy, że $\alpha, \beta \in C(R)$ oraz $\alpha\beta = 0$. Wówczas dla każdego $r \in R$ mamy $\alpha(r)\beta(r) = 0$. Stąd:

$$r\alpha(\beta(r)) = \beta(\alpha(r))r = 0.$$

Jeśli tylko r był niezerowy, to mamy inkluzje:

$$\ker(\beta) \subset \alpha(R), \quad \ker(\alpha) \subset \beta(R).$$

Wobec rozumowania wyżej albo $\alpha$ jest niezerowe, albo $\ker(\alpha) = 0$, zatem albo $\alpha = 0$, albo $\beta = 0$.

Pozostała przemienność. Rozważmy przekształcenie $\alpha\beta - \beta\alpha$. Jeśli jest ono zerowe, to mamy tezę. Jeśli nie, to jądro $\alpha\beta - \beta\alpha$ jest zerowe. Ale wiadomo, że komutant dwóch elementów z $C(R)$ zeruje się na $R^2$. Zatem $R^2 = 0$. Ale z pierwszości $R$ wynika, że $R = 0$, a więc sprzeczność. ∎

**Twierdzenie 4.9** *Każdy pierścień pierwszy jest podpierścieniem algebry pierwszej nad ciałem zanurzonym przy pomocy centralnej lokalizacji.*

Dowód. Niech $R$ – pierścień, zaś $S \subseteq C(R)$ – multiplikatywnie zamknięty. Niech $C(R)$ przemienny (wystarczy $S \subset$ centrum R). Zauważmy, że $1 \in S$, $0 \notin S$ (regularność). Teraz definiujemy lokalizację $RS^{-1}$ względem $S$. Pamiętamy, że elementy $S$ są w centroidzie. W ten sposób otrzymamy algebrę nad pierścieniem $CS^{-1}$. Mamy oczywiście przekształcenie naturalne $\phi : R \to R_S$ takie, że $\phi(r) = r/1$. Elementy z $S$ są regularne, a więc $\phi$ jest zanurzeniem. Jeśli $R$ jest pierwszy i $S = C(R) \setminus \{0\}$, to $R_S$ jest szukanym pierścieniem, który jest algebrą nad ciałem $C(R)_S$. Pozostaje pokazać, że $R_S$ jest pierwsza. Jeśli $0 \neq I \triangleleft R_S$, to $I \cap \phi(R)$ jest też niezerowe i to już z pierwszości $R$ wystarcza. ∎

**Definicja 4.10** *$R$ jest pierścieniem. $R$ moduł $M$ nazywamy* ***nieprzywiedlnym*** *jeśli $M \neq 0$, nie ma właściwych podmodułów i $RM = M$. $R$-moduł $M$ nazywamy* ***wiernym*** *jeśli $\{r \in R : rM = 0\} = \{0\}$. Pierścień $R$ nazwiemy* ***lewostronnie prymitywnym*** *jeśli istnieje wierny i nieprzywiedlny $R$-moduł lewostronny.*

**Twierdzenie 4.11 (GM Bergman)** *Istnieją pierścienie lewostronnie prymitywne, które nie są lewostronnie prymitywne.*

**Definicja 4.12 (Radykał Jacobsona)** *Nazywamy tak cześć wspólną takich ideałów $I$ pierścienia $R$, że $R/I$ jest lewostronnie prymitywny. Oznaczamy go przez $J(R)$.*

Okazuje się, że radykał ten to także cześć wspólna prawostronnych ideałów prymitywnych pierścienia $R$.

**Twierdzenie 4.13 (Jacobson)** *$J(R)$ jest największym ideałem pierścienia $R$, który jest grupą ze względu na działanie $\circ$:*

$$x \circ y = x + y - xy.$$

Jeśli $1 \in R$, wówczas $1 - (x \circ y) = (1 - x)(1 - y)$

**Wniosek 4.14** *Jeśli $R$ jest nil-pierścieniem, to $J(R) = R$.*

**Twierdzenie 4.15 (Rowen)** *Niech $R$ będzie PI-pierścieniem pierwszym z centroidem $C$. Niech $S = C \setminus \{0\}$, zaś $R_S$ – centralna lokalizacja $R$. Wówczas $R \subset R_S$, poza tym $R_S$ jest algebrą pierwszą nad ciałem $C_S$. Każda (nietrywialna) tożsamość nad $C$ spełniona w $R$ jest spełniona w $R_S$, zatem $R_S$ jest PI-algebrą nad ciałem.*

Dowód. Część własności została omówiona na wykładzie 9. Zacznijmy od przypadku, gdy $C$ jest ciałem. Wtedy jednak $R_S = R$, zaś $C_R = C$. Więc teza jest jasna.

Załóżmy, że $C$ nie jest ciałem. Niech $c \in S$ będzie nieodwracalny. Elementy $c, c^2, c^3, \ldots$, są parami różne. Istotnie, jeśli $c^i = c^j$, gdzie $i > j$, to $c^i(1 - c^{j-i}) = 0$. Ale w pierścieniu pierwszym centroid jest dziedziną, zaś $c \neq 0$, więc skracając przez $c^i$ dostajemy, że $c^{j-i} = 1$, a więc $c$ jest odwracalne.

Niech $f = \sum_{i=1}^{d} f_i$ będzie tożsamością dla $R$ nad $C$ gdzie $f_i$ są wielomianami jednorodnymi stopnia $i$ (ze względu na wszystkie zmienne). Niech $a_1, a_2, \ldots, a_n \in R$. Mamy, że:

$$f(a_1, a_2, \ldots, a_n) = 0 = \sum_{i=1}^{d} f_i(a_1, \ldots, a_n).$$

Co więcej:

$$f(c^j a_1, \ldots, c^j a_n) = \sum_{i=1}^{d} f_i(c^j a_1, \ldots, c^j a_n) = \sum_{i=1}^{d} c^{ij} f_i(a_1, \ldots, a_n).$$

Jeżeli na tę równość popatrzymy w $R_S$ traktowanej jako przestrzeń liniową nad $C_S$ to mamy do czynienia z układem równań, którego macierzą jest macierz Vandermonde'a. Ponieważ wyznacznik ten jest w naszym przypadku postaci $\prod_{i<j} (c^j - c^i) \neq 0$, a stąd dla każdego $i$ mamy $f_i(a_1, \ldots, a_n) = 0$. Zatem $f_i$ są tożsamościami dla $R$.

Teraz jak weźmiemy $n$ elementów z naszej lokalizacji, wtedy możemy sprowadzić je do wspólnego mianownika. Dokładniej, jeśli $b_1, b_2, \ldots, b_n \in R_S$, to istnieje element $d \in S$, że $b_i = a_i/d$, dla pewnych $a_i \in R$. Zatem $f(b_1, \ldots, b_n) = d^{-i} f(a_1, \ldots, a_n) = 0$. Zatem $f$ jest tożsamością w $R_S$. Ale $f$ było wzięte jako dowolna tożsamość, co kończy dowód. ∎

**Lemat 4.16** *Niech $R$ - pierścień prymitywny z centroidem $C$ i modułem nieprzywiedlnym i wiernym $M$. Wówczas $R$ jest pierścieniem pierwszym, $M$ zaś jest w naturalny sposób $C$-modułem. Mnożenie z $R \times M \to M$ jest $C$-dwuliniowe. Jeżeli $S = C \setminus \{0\}$, to istnieje lokalizacja $M_S$ i $R_S$ jest prymitywny z modułem nieprzywiedlnym $M_S$.*

Dowód. Niech $I, J \lhd R$. Zauważmy, że $IJM = I(JM)$. Zauważmy, że $JM$ jest podmoułem w $M$. Ponieważ $J \neq 0$, więc ten podmoduł jest $\neq 0$, bo moduł jest wierny. Zatem $JM = M$. Zatem $IJM = IM = M \neq 0$. Stąd $IJ \neq 0$. Zatem mamy pierwszość $R$.

Niech $0 \neq m \in M$. Zatem $M = Rm$. Jeśli tak, to istnieje element $r \in R$, że $m = rm$. Zatem dla $c \in C$ przyjmujemy: $c \cdot m = crm$, a każdy inny element jest postaci $rm$. W naturalny sposób określamy $M_S$:

$$M_s = \{(x, c), x \in M, c \in C\}, \quad (x_1, c_1) = (x_2, c_2) \Leftrightarrow c_2 x_1 = c_1 x_2.$$

$M_S$ jest wiernym i nieprzywiedlnym $R_S$-modułem (sprawdza się bezpośrednio). Co więcej, $R_S$ jest algebrą nad ciałem $C_S$. ∎

**Twierdzenie 4.17 (O gęstości)** *Niech $R$ będzie prymitywny z wiernym nieprzywiedlnym modułem $M$. Niech $D = End_R(M)$. Wówczas:*

1. *$D$ jest pierścieniem z dzieleniem i $M$ jest $D$-modułem,*
2. *Jeżeli $M$ jest $n$ wymiarowym $D$-modułem, to $R \simeq M_n(D)$,*
3. *Jeżeli wymiar $M$ nad $D$ jest nieskończony, to dla każdego $n \geq 1$ istnieje podpierścień $R_n \subseteq R$ i jego homomorfizm na pierścień macierzy $M_n(D)$.*

W punkcie 2. jeśli $R$ było $C$-algebrą, to $R_n$ można uważać za $C$-podalgebry i homomorfizm na $M_n(D)$ jest $C$-homomorfizmem. $D$ jest też $C$-algebrą.

Naszym celem będzie dowód twierdzenia Kaplansky'ego klasyfikującego prymitywne PI-algebry nad ciałem. Potrzebujemy przypomnieć w tym celu następujące definicje i fakty.

**Definicja 4.18 (Centralne rozszerzenie)** *Niech $R \subseteq S$ będzie rozszerzeniem pierścieni. Powiemy, że jest to **rozszerzenie centralne** jeśli $S$ jest, jako pierścień, generowany przez elementy $R$ oraz elementy z centrum $S$.*

Zauważmy, że jeśli $R$ jest $PI$-algebrą nad ciałem, to jej centralne rozszerzenie jest również PI.

**Lemat 4.19** *Niech $R \simeq M_t(D)$, gdzie $D$ jest z dzieleniem. Niech $L$ będzie maksymalnym podciałem w $D$, zaś $K$ – centrum $D$. Niech $M$ będzie nieprzywiedlnym modułem takim, że $D \simeq End(M_R)$. Wówczas:*

- *$S = R \otimes_K L$ jest prosta, zaś $M$ jest prostym $S$-modułem, że $L \simeq End(M_S)$.*
- *Jeśli $M$ ma wymiar $m$ nad $L$, wtedy $S \simeq M_m(L)$ i $[R : K] = m^2$.*

**Definicja 4.20** *Niech $K$ będzie ciałem, zaś $R$ – prostą skończenie wymiarową $K$ algebrą z centrum równym $K$. Wówczas $R$ nazywamy* ***prostą algebrą centralną****. Zgodnie z twierdzeniem Artina-Wedderburna $R \simeq M_n(D)$, dla pewnego pierścienia z dzieleniem $D$.*

**Twierdzenie 4.21 (Amitsur-Levitzki)** *Niech $K$ będzie dziedziną przemienną. Jeśli $n \geq 2$, to $M_n(\mathbb{K})$ nie spełnia żadnej nietrywialnej tożsamości stopnia mniejszego niż 2n, ale $p_{2n}$.*

**Twierdzenie 4.22 (Kaplansky)** *Niech $R$ będzie prymitywną PI algebrą nad ciałem $K$ stopnia $d$ z modułem nieprzywiedlnym i wiernym $M$. Wówczas $R$ jest algebrą prostą z 1 i ma nad centrum wymiar nie większy niż $(d/2)^2$. Czyli $R \simeq M_n(D)$, gdzie $D$ jest skończenie wymiarową algebrą z dzieleniem nad swoim centrum.*

Dowód. Zgodnie z twierdzeniem o gęstości, albo $R \simeq M_n(D)$, dla pewnego pierścienia z dzieleniem $D$, albo dla każdego $n$ istnieje epimorfizm podpierścienia $R_n \subseteq R$ na macierze $M_n(D)$. Załóżmy, że $R \not\simeq M_n(D)$, dla pewnego $n$. Niech $L$ będzie maksymalnym podciałem w $D$. Wówczas $M_n(D)$ jest, zgodnie z twierdzeniem Amitsura-Levitzkiego, stopnia 2n, zatem stopień $M_n(D)$, a wraz z nim i $R_n$ wynosi co najmniej 2n. Zatem w $R$ istnieją PI-podpierścienie dowolnie wysokiego stopnia, co przeczy temu, że $R$ jest PI. Zatem $R \simeq M_n(D)$ i $R$ jest prosty.

Niech $H$ będzie centrum $D$, zaś $L$ – maksymalnym podciałem $D$. Wówczas $R \otimes_H L$ jest prymitywną $H$-algebrą nad ciałem i spełnia dokładnie te same tożsamości co $R$. Stąd jest ona PI. Zgodnie z rozumowaniem podanym wyżej jest ona izomorficzna z $M_t(L)$, gdzie $t$ jest pewną liczbą naturalną. Zgodnie z lematem widzimy, że $[R : H] = t^2$. Zatem $R$ jest prostą algebrą centralną. Zgodnie z twierdzeniem Amitsura-Levitzkiego $R$ spełnia ona $p_{2t}$, ale nie $p_{2t-1}$. Stąd $d = 2t$ i $[R : F] = \left(\frac{d}{2}\right)^2$.

■

**Wniosek 4.23** *Niech $d$ będzie liczbą parzystą. Każda prymitywna PI algebra stopnia $d$ nad ciałem $K$ spełnia tożsamość standardową stopnia $d$.*

Co w tym wniosku jest ważne? Okazuje się, że gdy w algebrze nad ciałem mamy tożsamość, to w sumie można się pozbyć współczynników, bo w tożsamości standarowej są 0 i 1.

**Wniosek 4.24** *Niech $R$ będzie prymitywnym pierścieniem spełniającym nietrywialną tożsamość stopnia $d$. Wówczas $R$ jest PI algebrą i spełnia tożsamość standardową stopnia parzystego $\leq d$.*

Istotnie, jeżeli jest spełniona nietrywialna tożsamość, to przenoszę się do prymitywnej algebry nad ciałem, tam stosuję wniosek pierwszy, a jej współczynniki siedzą w centrodzie, więc mogę wrócić z nią z powrotem.

**Lemat 4.25** *Załóżmy, że $R$ jest pierścieniem prymitywnym (lewostronnie) z 1. Wówczas $J(R) = 0$.*

Dowód. Oczywiście wiadomo to na podstawie faktu, że radykał jest przecięciem ideałów prymitywnych. Ale można to zrobic po prostu. Załóżmy, że $J$ jest niezerowy. Niech $M$ będzie nieprzywiedlnym $R$-modułem wiernym, zaś $0 \neq x \in M$. Wówczas $Rx = M$ oraz $JM = Jx$, ponieważ $M$ nie ma nietrywialnych podmodułów. Wiemy jednak, że $JM = M$ lub $JM = 0$. Drugi przpadek jest niemożliwy, ponieważ $M$

jest modułem wiernym, a więc $J(R) \subseteq ann_R(M) = (0)$, zatem $JM = Jx = M$. Stąd istnieje $a \in J(R)$, że $ax = x$. Ale wówczas $(1-a)x = 0$, a więc skoro 1-a jest odwracalny, stąd $x = 0$, sprzeczność. ■

**Wniosek 4.26** *Niech $R$ będzie $C$-algebrą i PI algebrą stopnia $d$. Jeśli $J(R) = 0$, to istnieje zanurzenie algebrowe $R$ w $M_n(F)$, gdzie $F$ jest przemienną $C$-algebrą bez elementów nilpotentnych i $n \leq (d/2)^2$. Stąd $R$ spełnia tożsamość standardową stopnia $2n$.*

Co to znaczy, że radykał Jacobsona jest zerowy? Oznacza to, że istnieje rodzina $I_t, t \in T$ ideałów w $R$, że $R/I_t$ jest prymitywną algebrą oraz $\bigcap_{t \in T} I_t = 0$. Zatem $R$ jest iloczynem podprostym. Widzimy więc, że każdy pierścień półprymitywny jest produktem półprostym pierścieni prymitywnych. Do każdego $R/I_t$ można stosować twierdzenie Kaplansky'ego i jego wnioski.

**Twierdzenie 4.27 (Amitsur)** *Załóżmy, że pierścień $R$ nie ma $\neq 0$ nil ideałów. Wóczas $J(R[t]) = 0$.*

Jeśli $R$ jest pierwszy i PI, to spełnia nietrywialną tożsamość nad centroidem. Zatem z twierdzenia Rowena można założyć, że centroid jest ciałem. Stąd $R$ spełnia nietrywialną tożsamość wieloliniową stopnia nie większego niż $d$, a skoro jest ona wieloliniowa, to spełnia ją też $R[t]$. Nie ma więc gwarancji, że przeniosę wszystkie tożsamości. Ale przeniosę jakąś nie powiększając stopnia. Skoro tak to z tw. Kaplansky'ego (a wł. jego skutek), a więc wielomiany zanurzyć w macierze $M_n(F)$ o współczynnikach przemiennych bez elementów nilpotentnych. Co więcej, $n \leq 2$

**Definicja 4.28** *Pierścień $R$ nazywa się* ***półpierwszy****, jeśli przecięcie wszystkich ideałów pierwszych w $R$ jest ideałem zerowym.*

**Wniosek 4.29** *Niech $R$ będzie półpierwszą PI algebrą stopnia $d$. Wówczas $R \subseteq M_n(F)$, gdzie $F$ przemienny bez elementów nilpotentnych. $R$ jest algebrą bez niezerowych nil ideałów.*

Dowód. Niech niezerowy element $r \in R$. W $RrR$ istnieje takie $a$, które nie jest nilpotentne. Niech $I_a$ będzie maksymalnym ideałem w $R$ wśród tych, że $a^n \notin I_a$ dla każdego $n$. Taki element istnieje z lematu Zorna. Zatem $R/I_a$ jest pierwszy i nie ma niezerowych nil-ideałów. Skoro $R$ jest PI stopnia $d$, to $R/I_a$ jest PI stopnia nie większego niż $d$. Także element $r \notin I_a$. Stąd wynika, że $\bigcap I_a = 0$. ■

Innymi słowy widzimy, że każda algebra PI algebra półpierwsza zanurza się w pierścień macierzy nad pierścieniem przemiennym, a więc spełnia pewną tożsamość standardową.

**Twierdzenie 4.30** *Niech $C$ będzie pierścieniem przemiennym z 1. Jeśli $R$ jest $C$-algebrą, to NSWR:*

1. *$R$ jest PI algebrą nad $C$ (stopnia d),*
2. *$R$ spełnia potęgę pewnej tożsamości standardowej,*
3. *$R$ spełnia tożsamość wieloliniową stopnia $m$ nad $\mathbb{Z}$ postaci:*

$$\sum_{\sigma \in S_m} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(m)}, \quad \alpha_\sigma \in \mathbb{Z}, \alpha_{id} = 1 \in \mathbb{Z}.$$

**Wniosek 4.31** *Niech $R$ będzie $C$-algebrą, niech $D$ będzie pierścieniem przemiennym takim, ze $D$ jest $C$-algebrą. Wtedy $D \otimes_C R$ jest $D$-algebrą, jest ona PI jeśli $R$ było PI.*

**Twierdzenie 4.32 (Rager)** *Jeśli $C$ jest ciałem oraz $R, S$ są PI algebrami nad $C$, to $R \otimes_C S$ jest PI.*

**Definicja 4.33** *Niech $C$ – ciało, zaś $A$ – $C$ algebra. Wówczas:*

- *$A$ jest **algebrą algebraiczną**, jeżeli dla każdego $a \in A$ istnieje $f_a \in C[t]$ taki, że $f_a(a) = 0$. W razie braku jedynki w $A$ zakładamy, że $f_a$ nie ma wyrazu wolnego.*
- *$A$ jest **lokalnie skończona** jeśli każda skończenie generowana $C$-podalgebra w $A$ jest skończenie wymiarowa.*
- *$A$ jest **algebraiczna** stopnia $\leq n$ gdy dla każdego $a \in A$ zakładamy, że $f_a$ nie ma wyrazu wolnego.*

**Twierdzenie 4.34** *Jeśli $A$ jest algebraiczna ograniczonego stopnia $n$, to $A$ jest PI.*

DOWÓD. Istnieje $n < \infty$, że dla $a \in A$ elementy $a, a^2, \ldots, a^n$ są liniowo zależne. Jeżeli $b \in A$, to elementy $[a,b], [a^2,b], \ldots, [a^n,b]$ są liniowo zależne. Niech:

$$f(x,y) = p_n([x,y],[x^2,y],\ldots,[x^n,y]) \in C\langle x,y\rangle$$

będzie tożsamością dla $A$. Istotnie, $f(x,y) \neq 0$, a liniowa zależność $[a,b],[a^2,b],\ldots,[a^n,b]$ zapewnia znikanie $p_n$ (tożsamości standardowej na tym układzie). ∎

**Problem Kurosha**. Czy każda algebra algebraiczna jest lokalnie skończona?
**Problem Levitzkiego**. Czy każda nilalgebra jest lokalnie nilpotentna?

Niech $C$ – ciało, $d \geq 2$oraz $T = C\langle x_1, \ldots, x_d\rangle$. Niech $I \subseteq T$ będzie ideałem generowanym przez elementy jednorodne stopnia $\geq 2$. Niech $r_j$ – ilość generatorów stopnia $j$ w $I$. Wówczas:

**Lemat 4.35 (Golod)** *Jeśli istnieje $\epsilon > 0$ takie, że $r_j < \epsilon^c(d - 2\epsilon)^{j-c}$ dla każdego $j \geq 2$, to algebra $C\langle x_1, \ldots, x_n\rangle / I$ jest nieskończenie wymiarowa.*

**Twierdzenie 4.36 (Golod)** *Niech $C$–ciało, $d \geq 2$. Wówczas istnieje algebra z 1 $A = C\langle a_1, a_2, \ldots, a_n\rangle = C\langle x_1, x_2, \ldots x_n\rangle / I$, taka że $dim_C(A) = \infty$, $A$ ma gradację w której $deg(a_i) = 1$. Ideał $J = (a_1, \ldots, a_n) \triangleleft A$ jest nil, zaś każda podalgebra generowana przez nie więcej niż d-1 elementów jest skończenie wymiarowa.*

Jak to się ma do problemu Burnside'a? Niech $R$ będzie dowolną $C$-algebrą i niech $V \subseteq R$ będzie podprzestrzenią wymiaru $n$. Wówczas podprzestrzeń generowana przez $v^r$, $v \in V$ ma wymiar, który jest wielomianową funkcją od $R$. Jeśli char C = p ¿ 0, to elementy $1 - a_i$ generują torsyjną p-grupę w elementach odwracalnych $A$ (ozn. G). Bierzemy $C[G]$, która jest podalgebrą w $A$ i mamy: $\alpha_i \in C[G]$, zatem $A = C[G]$ czyli $G$ jest nieskończona.

Jest też problem związany bezpośrednio z **problemem Kothe** (mówi ona, że w każdym pierścieniu suma dwóch nil ideałów lewostronnych jest nil). Niech $A$ będzie nil algebrą nad ciałem $C$. Pytanie czy algebra macierzy $M_2(A)$ jest nil? Wiadomo, że jest tak, gdy $C$ jest ciałem nieprzeliczalnym. Zobaczymy, że problem Kurosha ma pozytywne rozwiązanie dla PI algebr.

Przypomnijmy, że $\mathbb{K}$-algebra $A$ jest **lokalnie skończona** jeśli każda skończenie generowana podalgebra $A' \subseteq A$ jest skończenie wymiarowa nad $\mathbb{K}$. Przypomnijmy też, że algebra $A$ jest **algebraiczna** jeśli każdy jej element jest algebraiczny nad ciałem, tzn. dla każdego $a \in A$ rozszerzenie ciał $\mathbb{K} \subseteq \mathbb{K}(a)$ jest skończone. Jest oczywiste, że każda algebra lokalnie skończona jest algebraiczna. Odwrotnie – niekoniecznie. Przykład podał Gołod.

Łatwo widzieć, że radykał Jacobsona algebry algebraicznej musi być nil-ideałem. Prymitywna algebra algebraiczna jest izomorficzna z gęstym podzbiorem algebry endomorfizmów przestrzeni liniowej nad pierścieniem z dzieleniem. Naszym celem będzie pokazanie, że w przypadku PI-algebr algebra algebraiczna jest lokalnie skończona.

Jest to analogia do teorii grup gdzie wyróżniliśmy grupy lokalnie skończone i torsyjne. Wiadomo, że każda grupa lokalnie skończona jest torsyjna, ale odwrotnie niekoczniecznie – tego dotyczyły problemy Burnside'a. W każdej grupy istnieje największy dzielnik torsyjny i iloraz już nie ma dzielników torsyjnych. W przypadku lokalnie skończonych grup także: w każdej grupie jest największy dzielnik lokalnie skończony i jak przez niego podzielimy to nie ma dzielników lokalnie skończonych. W dowolnym pieścieniu mamy radykał Jacobsona i znowu: jest to największy iloraz o pewnej własności i iloraz już nie ma takich ideałów. Tak samo z górnym nil-radykałem, największy nil-ideał, że iloraz już nie ma nil. Tak samo dolny nil-radykał. W latach 50' pojawiła się teoria radykałów.

Ten największy ideał będziemy nazywali **radykałem**. Iloraz będziemy nazywali półprostym. Co więcej, jeśli mieliśmy jednostronny ideał zawarty w ideale równym swojemu radykałowi, to jest on zawarty w dwustronnym ideale równym swojemu radykałowi. Takie radykały nazywamy silnymi. Takie są: radykał Jacobsona, dolny nil-radykał. Radykał lokalnie nilpotentny, że każdy skończenie generowany podpieścień jest nilpotentny też jest silny. Jednostronne ideały lokalnie nilpotentne są zawarte w dwustronny.

**Lemat 4.37** *Niech $\mathbb{K}$ – ciało, zaś $A$ – skończenie generowana $\mathbb{K}$-algebra, zaś $I \subseteq A$ – ideał skończonego kowymiaru, czyli $A/I$ jest sk. wymiarowa. Wówczas $I$ jest algebrą skończenie generowaną.*

**Twierdzenie 4.38** *Lokalna skończoność jest radykałem silnym.*

Dowód. Niech $A$ będzie algebrą. Suma łańcucha ideałów lokalnie skończonych jest ideałem lokalnie skończonym. Z lematu Zorna wynika, że istnieje największy ideał lokalnie skończony (0 jest lokalnie skończony), oznaczmy go przez $LF(A)$. Teraz czemu w ilorazie nie ma ideałów lokalnie skończonych? Udowodnimy, że jeśli $J \supseteq LF(A)$ i $J/LF(A)$ jest lokalnie skończona, to $J = LF(A)$. Niech $B \subseteq J$ będzie podalgebrą skończenie generowaną. Wówczas $(B+LF(A))/LF(A) \simeq B/(B \cap LF(A))$. Iloraz ten jest skończenie wymiarowy, a zatem $B/(B \cap LF(A))$ jest sk. wymiarowy. Zatem z lematu wynika, że $B \cap LF(A)$ jest sk. generowane jako algebra. Ale to przecięcie siedzi w $LF(A)$, a więc ma skończony wymiar. Zatem także $B$ ma skończony wymiar. Ale $B$ było dowolną skończenie generowana podalgebrą w $J$. Zatem $J$ jest lokalnie skończony, a więc $J = LF(A)$.

A czemu radykał jest silny? Czemu jednostronne ideały lokalnie skończone są zawarte w dwustronnych? Niech $I \subseteq A$ będzie lewostronnym ideałem lokalnie skończonym. Niech $A^1$ będzie $A$ z 1 dołączoną przy pomocy ciała. Niech $J = IA^1 \subseteq A$, bo $A^1$ jako przestrzeń liniowa to $A \oplus \mathbb{K}$, a jedynki potrzebuję po to, by $I \subseteq J$. Teraz chcemy pokazać, że $J$ jest ideałem lokalnie skończonym. Niech $B \subseteq J$ będzie skończenie generowana. Mogę wziąć generatory $B = \langle x_1 a_1, \dots, x_n a_n \rangle$. Oczywiście $x_i \in I, a_i \in A^1$. Niech $V$ będzie podprzestrzenią w $A^1$ generowaną przez $a_1, \dots, a_n$. Niech $W$ będzie podgalgebra generowana przez $a_i x_j$, dla $1 \leq i, j \leq n$ (ideał jest jednostronny). Oczywiście $W \subseteq I$. Co więcej $I$ jest skończenie generowana, a więc $W$ jest skończenie wymiarowa. Zauważmy, że $B \subseteq W \cdot V$. Skoro $WV$ jest skończenie wymiarowa, to $B$ też skończenie wymiarowa. Z dowolności $B$ wynika, że $J$ jest ideałem lokalnie skończonym. ∎

**Wniosek 4.39** *Jeśli $A$ jest lokalnie skończona, to $M_n(A)$ jest też lokalnie skończona.*

**Definicja 4.40** *Pieścień $R$ nazywamy **zredukowanym** jeśli nie ma on niezerowych elementów nilpotentnych.*

W przypadku przemiennym zredukowany jest półpierwszy. Ale już macierze są proste, ale nie zredukowane. Jak to się ma do radykału? Można wskazać taki radykał, że klasa pierścieni zredukowanych to pierścienie półproste względem tego radykału.

**Lemat 4.41** *Niech $A$ będzie zredukowaną algebrą algebraiczną. Niech $B = \langle b_1, b_2, \dots, b_n \rangle$ będzie podgalgebrą. Wówczas istnieje idempotent $e \in B$, który jest jedynką w $B$.*

Dowód. Dowód to indukcja po n. Niech $B = \langle b_1 \rangle$, gdzie $b_i$ - algebraiczny. Mamy więc:

$$b_1^r = \alpha_1 b_1^{r+1} + \dots \alpha_s b_1^{r_s}$$

przy czym $b_1^{r+1} f(t)$, gdzie $f(t) \neq 0$. Mamy: $b_1^r(1 - b_1 f(b_1) = 0 \Rightarrow (b_1(1 - b_1 f(b_1)))^r$. Ale nie ma niezerowych elementów nilpotentnych, zatem $b_1(1 - b_1 f(b_1)) = 0$. Stąd $b_1 = b_1(b_1 f(b_1))$. Niech $e_1 = b_1 f(b_1)$. Wówczas $e_1^2 = b_1^2 (f(b_1))^2 = (b_1^2 f(b_1)) f(b_1) = b_1 f(b_1)$. Teraz korzystamy z rozkładu Pierce'a. Jeśli $e$ jes idempotentem, to $R = eRe + eR(1-e) + (1-e)Re + (1-e)R(1-e)$ i jest to suma prosta grup abelowych. Pojawia się tu jedynka w zapisie, ale to nie szkodzi. Ale gdy $R$ jest zredukowany, to rozkład ten jest krótszy, a więc $R = eRe + (1-e)R(1-e)$ i $e$ jest centralny. Zatem $e_1$ jest centralnym idempotentem i wiemy, że $b_1 = b_1 e_1$.

Ciąg dalszy indukcji. Załóżmy, że skonstruowaliśmy już idempotenta $e_M$, że $b_i e_M = b_i$, dla $i \leq m$. Jeżeli $m < n$, to to mamy, że $b_{m+1} = b_{m+1} e_M + b_{m+1}(1 - e_M)$. Dla elementu $b_{m+1}(1 - e_m)$ konstruujemy idempotenta $f$ takiego, że $b_{m+1}(1 - e_m) = b_{m+1}(1 - e_m) f$. Wtedy przyjmiemy $e_{m+1} = e_m + f$. Z konstrukcji wyminak ,że $e_m f = 0$, zatem $e_{m+1}$ jest szukanym idempotentem. ∎

**Wniosek 4.42** *Niech $A$ będzie sk. generowaną PI-algebrą algebraiczną i zredukowaną . Wowczas w $A$ istnieje niezerowy ideał lokalnie skończony.*

Dowód. Zauważmy, że skoro $A$ jest algebraiczna, to $J(A)$ jest nil-ideałem, a więc $J(A) = 0$ (bo $A$ jest zredukowany). Niech $P$ będzie prymitywnym ideałem w $A$. Na mocy tw. Kaplansky'ego wiemy, że $A/P$, jako prymitywna PI algebra, ma 1 i jest skończenie generowana nad swoim centrum. Jako obraz $A$ jest to jednocześnie algebra algebraiczna, a więc $A/P$ jest skończenie wymiarowa. Z lematu wynika zatem, że $P$ jest skończenie generowana. Z innego lematu wynika, że $P = eP$, a więc z rokładu Pierce'a mamy $A/P \simeq A(1-e)$ – ideał w $A$. Jest on skończenie wymiarowy. Oczywiście $P \neq A$, a wiec nasz ideał $A(1-e)$ jest niezerowy. ∎

**Twierdzenie 4.43** *Każda algebraiczna PI algebra jest lokalnie skończona.*

Dowód. Niech $A$ będzie taką algebrą. Niech $I$ – radykał lokalnie skończony $A$. Niech $B = A/I$. Trzeba pokazać, że $B = 0$. Załóżmy przeciwnie. Wiadomo (poprzedni wykład), że $B$ nie zawiera jednostronnych ideałów lokalnie skończonych. Będzie indukcja ze względu na stopień tożsamości wieloliniowej spełnianej przez $B$. Stopień 1 dla tożsamości wieloliniowej oznacza $x = 0$. Wtedy $B = 0$. Załóżmy więc, że stopień $B$ jest $\geq m$ i mniejszy być nie może. Mogą zajść dwa przypadki:

- Niech $0 \neq b \in B$, że $b^2 = 0$. Weźmy ideał prawostronny $bB^1$. To jest na pewno niezerowe. To także spełnia tożsamość wieloliniową stopnia $m$, to możemy napisać ją w postaci równości:

  $$f = f_1(x_1, x_2, \ldots, x_{n-1})x_n + f_2(x_1, x_2, \ldots, x_n),$$

  gdzie w jednomianach $f_2$ nie ma na końcach $x_n$. Mogę założyć, że identyczność ma niezerowy współczynnik, więc $f_1 \neq 0$. Niech $x_1 = br_1, x_2 = br_2, \ldots, x_{n-1} = br_{n-1}, x_m = b$, gdzie $r_i \in B^1$. Po podstawieniu dostajemy:

  $$0 = f_1(br_1, br_2, \ldots, br_{n-1}, b) + 0 \qquad \text{bo } b^2 = 0.$$

  Zatem $0 = f_1(br_1, \ldots, br_{n-1})bB^1 = 0$. Niech $J = \{t \in bB^1 \,|\, tbB^1 = 0\}$. Zatem $J^2 = 0$ oraz $f_1(br_1, br_2, \ldots, br_{n-1}) \in J$. Zatem $f_1$ jest tożsamością dla ilorazu $bB^1/J$. Z założenia indukcyjnego iloraz $bB^1/J$ jest lokalnie skończony. Co więcej $J^2 = 0$, więc $J$ też jest lokalnie skończony. Stąd także $bB^1$ jest lokalnie skończona, ale to przecież jednostronny ideał w $B$, zatem dostajemy sprzeczność, bo tam takich ideałów miało nie być.

- Załóżmy, że $B$ nie ma niezerowych elementów nilpotentnych. Pokażemy, że dowolna skończenie generowana podalgebra $R \subseteq B$ jest lokalnie skończona. Skorzystajmy z tego co było tydzień temu. $R$, jako algebra zredukowana zawiera niezerowy ideał lokalnie skończony. Jest on generowany przez idempotenta. Stąd $R$ jest lokalnie skończona. Ale $R$ to była dowolna skończenie generowana podalgebra w $B$. Zatem $B$ jest lokalnie skończona i znów sprzeczność.

∎

W analogiczny sposób dowodzi się rozstrzygnięcie problemu Levitzkiego dla PI pierścieni.

**Twierdzenie 4.44** *Jeżeli nil-algebra jest PI, to jest lokalnie nilpotentna.*

Korzysta się tu z faktu, że każda PI algebra spełnia potęgę tożsamości standardowej, a zatem istnieje tożsamość wieloliniowa, która ma przy identyczności współczynnik jeden.

Mówiliśmy, że radykał pierwszy to część wspólna wszystkich ideałów pierwszych (lub cały pierścień, gdy ich nie ma). A teraz inna definicja.

**Definicja 4.45** *Niech R – dowolny pierścień.* ***Radykałem Wedderburna*** *pierścienia R, ozn. W(R), nazywamy sumę wszystkich ideałów nilpotentnych pierścienia R.*

Przykład. Niech $C$ – pierścień przemienny z 1, przy czym nil-radykał $C$, który nie jest ideałem nilpotentnym. Niech $n > 1$. Weźmy w $M_n(C)$ podpierścień:

$$R = \begin{pmatrix} Nil(C) & C & C & \dots & C \\ Nil(C) & Nil(C) & C & \dots & C \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ Nil(C) & Nil(C) & Nil(C) & \dots & Nil(C) \end{pmatrix}$$

Łatwo pokazać, że $W(R) = M_n(Nil(C))$. Zatem $R/W(R)$ jest nilpotentny indeksu $n$. Widzimy więc, że radykał Wedderburna nie jest prawdziwym radykałem.

Niech $R$ – dowolny. Przyjmujemy, że $W_0(R) = 0, W_1(R) = W(R)$. Dalej jeśli $\alpha \in Lim$, to $W_\alpha(R) = \sum_{\beta<\alpha} W_\beta(R)$. Jeśli $\alpha = \beta + 1$, to $W_\alpha(R)$ jest przeciwobrazem w $R$ ideału $W(R/W_\beta(R))$.

**Twierdzenie 4.46** *Dla dowolnego pierscienia R ciąg $W_\alpha$ stabilizuje sie na radykale pierwszym R. Dla dowolnego $\alpha$ istnieje taki pierścień R, że $W_\beta(R) < W_\alpha(R) = W_{\alpha+1}(R)$.*

A jak jest algebra skończenie generowana? To coś pomaga? W przypadku skończonie wymiarowym, albo przemiennym nad ciałem, radykał jest nilpotentny. Z przykładu macierzowego wynika, że automatycznie nie przechodzi to na PI.

**Twierdzenie 4.47** *Jeśli R jest PI algebrą i spełnia tożsamość znormalizowaną (jedynka przy id) stopnia d, to $Nil(R)^{[d/2]} \subseteq W(R)$.*

Dowód. Niech $R$ - jw. Niech $B \subseteq R$ będzie nilpotentną podalgebrą. W pewnej potędze jest zerem. Jest $n$ będzie najmniejszą taką liczbą, że $R^1B^nR^1$ jest nilpotentny Pokażemy, że $n \leq [d/2]$. Przypuśćmy przeciwnie. Dla dowolnego $1 \leq i \leq n$ przyjmemy $U_{2i-1} = B^{n-1}R^1B^{i-1}$ oraz $U_{2i} = B^{n-1}R^1B^i$. Mamy:

$$U_1 = B^{n-1}R^1, \quad U_2 = B^{n-1}R^1B, \quad U_3 = B^{n-2}R^1B, \quad U_4 = B^{n-2}R^1B^2.$$

Jeżeli $i > j$, to $U_iU_j \subseteq R^1B^nR^1 \subseteq W(R)$. Dalej:

$$U_1 \dots U_j \subseteq (B^{n-1}R^1B)^d B^{[d/2]}.$$

Z istnienia tożsamości znormalizowanej mamy:

$$x_1x_2 \dots x_d = \sum_{\sigma \neq id} \alpha_\sigma x_{\sigma_1} \dots x_{\sigma(n)}.$$

Stąd $(B^{n-1}R^1)^{d+1} \subseteq R^1B^nR^1$. Teraz ideał generowany przez $B^{n-1}$, a więc $R^1B^{n-1}R^1$ jest ideałem nilpotentnym.

Niech $a_1, \dots, a_{[d/2]} \in Nil(R)$, $A = \langle a_1, \dots, a_{[d/2]} \rangle$ jest nilpotentna, $B^{[d/2]} \subseteq W(R)$, a więc $a_1, \dots, a_{[d/2]} \in W(R)$. ∎

**Wniosek 4.48** *Niech $R$ będzie półpierwszą $PI$-algebrą i spełnia tożsamość stopnia $d$. Wówczas $R$ nie ma niezerowych nil-ideałów jednostronnych. Każda nil-podalgebra w $R$ jest nilpotentna stopnia $\leq [d/2]$.*

**Twierdzenie 4.49** *Niech $R$ będzie skończenie generowaną PI algebrą nad ciałem. Wówczas $J(R)$ jest ideałem nilpotentnym.*

Dowód. Tu tylko szkic dowodu. Ogólnie to jest trudne. Niech $R$ będzie pierwsza i skończenie generowana. Istnieje skończenie generowana przemienna algebra $C$, oraz $n \geq 1$ takie, że $R \subseteq M_n(C)$ jako podalgebra. Niech $J$ będzie radykałem Jacobsona w $R$. Niech $I$ będzie ideałem maksymalnym w $C$. Wobec tego $M_n(I) \triangleleft M_n(C)$, a więc mamy homomorfizm $\phi_i : R \to M_n(C/I)$. Ale $C/I$ jest ciałem i skończonym rozszerzeniem. Zatem $\phi_i(J) \subseteq J(\phi_i(R))$, czyli $\phi_i(J)$ jest nilpotentny, a ze względów macierzowych $J^n \subseteq M_(I)$. Ale I było dowolne, a więc $J^n \subseteq M_n(J(I))$. A więc jeśli $R$ dowolny i $P$ – pierwszy, to $J^n \subseteq P$. Ale to $n$ zależało od stopnia tożsamości, a nie od ideału pierwszego. Stąd $J^n \subseteq Nil(R)$, a więc w $J \subseteq W_2(R)$. A dalej są schody... ■

Dla skończenie generowanych algebr też te indeksy przy radykale Wedderburna mogą być prawie dowolne.

**Twierdzenie 4.50 (Amitsur-Levitzki)** *Dla każdego ciała $\mathbb{K}$ algebra macierzy $M_n(\mathbb{K})$ spełnia tożsamość standardową $p_{2n}$ i nie spełnia żadnej tożsamości wielomianowej niższego stopnia. Z dokładnością do stałej multiplikatywnej spełnia tylko $p_{2n}$.*

**Lemat 4.51** *$M_n(\mathbb{K})$ nie spełnia tożsamości wielomianowej stopnia mniejszego niż 2n. Co więcej jeśli $P(x_1, x_2, \ldots, x_n)$ jest wieloliniową tożsamością wielomianową st. 2n, dla $x_i \in M_n(\mathbb{K})$, to*

$$f(x_1, \ldots, x_n) = \alpha S_{2n}(x_1, x_2, \ldots, x_{2n}), \alpha \in \mathbb{K}.$$

Dowód. Jeśli $M_n(\mathbb{K})$ spełnia tożsamość wielomianową stopnia $k < 2n$, to spełnia też tożsamość wieloliniową stopnia $k < 2n$. Spełnia teżsatem tożsamość wieloliniową stopnia k postaci:

$$f(x_1, \ldots, x_k) = \sum_{\sigma \in S_k} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} ldots x_{\sigma(k)}.$$

Niech $e_{ij}$ będą jedynkami macierzowami. Wtedy:

$$0 = f(e_{11}, e_{12}, \ldots, e_{pq}) = \alpha_{id} e_{1q} \Rightarrow \alpha_{id} = 0.$$

Podobnie pokazujemy, że pozostałe $\alpha$ są zerami, a więc nasza tożsamość jest trywialna, sprzeczność.

Teraz niech $f(x_1, x_2, \ldots, x_{2n}) = \sum_{\sigma \in S_{2n}} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(2n)}$. Mamy:

$$0 = f(e_{11}, e_{11}, e_{12}, \ldots, e_{nn}) = (\alpha_{id} + \alpha_{(12)}) e_{1n} - \alpha_{id} = \alpha_{12}.$$

Zatem każda tożsamość wieloliniowa jest pewną wielokrotnością tożsamości standardowej. ■

**Lemat 4.52** *Jeśli $M_n(\mathbb{Q})$ spełnia tożsamość standardową stopnia 2n, to algebra $M_n(\mathbb{K})$ też ją spełnia.*

Dowód. Mamy:

$$\tau_p = \sum_{i,j=1}^{n} a_{ij}^{(p)} e_{ij}, \quad p = 1, 2 \ldots, 2n, \quad a_{ij}^{(i)} \in \mathbb{K}.$$

Wiadomo, że $p_{2n}$ jest wielomianem antysymetrycznym, a więc $p_{2n}(\tau_1, \tau_2, \ldots, \tau_{2n})$ jest kombinacją liniową elementów postaci:

$$p_{2n}(e_{i_1 j_1}, \ldots, e_{i_{2n} j_{2n}}) = 0.$$

■

**Lemat 4.53** *Niech $\xi_1, \xi_2, \ldots, \xi_n$ – wartości własne $a \in M_n(\mathbb{K})$. Niech $e_q = e_q(\xi_1, \ldots, \xi_n)$, gdzie $e_q = \sum_{i_1 < i_2 \ldots i_q} x_{i_1} \ldots x_{x_{i_q}}$., wówczas: $a^n + \sum_{q=1}^{n} e_q a^{n-q} = 0$ i $tr(a^q) = \xi_1^q + \ldots + \xi_n^q$. Co więcej, jeśli charakterystyka ciała jest zerowa, to $e_q$ można wyrażać za pomocą współczynników śladu $tr(a^s)s$, gdzie $s = 1, \ldots, n$.*

Dowód.[Razmysłow] Dla uproszczenia rozważymy przypadek n=2. Pozostałe są jedynie trudniejsze obliczeniowo. Zauważmy, że właściwie trzeba pokazać tylko, że spełnia $p_4$. Z lematu 2 możemy przyjąć, że $\mathbb{K} = \mathbb{Q}$. Z lematu 3 wiemy, że $M_n(\mathbb{Q})$ spełnia tożsamość śladową. Trzeba ją linearyzować... ■

Tydzień temu było o tym, że nie każda PI algebra jest zanurzalna w macierze, ale znamy klasy, które się zanurzają w macierze, np. półpierwsze PI algebry. Zajmiemy się algebrą wolną dla algebry macierzy nad ciałem nieskończonym (ogólniej – dziedziną nieskończoną przemienną).

NIech $C$–dziedzina przemienna nieskończona. Niech $n > 1$ i $d \geq 1$. Możemy wziąć pierścień wielomianów od przemiennych zmiennych: $C[t_{i_j}^{(k)}]$, gdzie $1 \leq i, j \leq n, k \leq d$. Bierzemy te wielomiany bez wyrazu wolnego. Niech $Y^{(k)}$ będzie macierzą $n \times n$ o wyrazach $t_{ij}^{(k)}$. Weźmy algebrę $U(C, n, d) = C[Y^{(1)}, \ldots, Y^{(d)}] \subseteq M_n[C[t_{ij}^k]]$. Są macierze uniwersalne stopnia n o d generatorach.

**Twierdzenie 4.54** *$U(C, n, d)$ jest algebrą wolną w klasie wszystkich $C$-algebr spełniających wszystkie tożsamości algebry $M_n(C)$.*

Dowód. Zauważmy, że jeśli $f \in C\langle X \rangle$ jest tożsamością dla $M_n(C)$, to jest też tożsamością dla algebry $M_n(C[T])$, gdzie $T$ – przemienne zmienne. Wobec tego jest ona spełniona przez $M_n(A)$, gdzie $A$ jest dowolną $C$-algebrą przemienną.[2] Zatem algebra $U(C, n, d)$ spełnia wszystkie tożsamości macierzy $M_n(C)$.

Niech $A$ będzie dowolną $C$-algebrą spełniającą wszystkie tożsamości algebry $M_n(C)$. Niech $a_1, \ldots, a_d \in A$. Skoro $A$ jest w rozmaitości generowanej przez $C$ a więc obrazem podagebry $D \subseteq \prod_{i \in I} M_n(C) \simeq M_n\left(\prod_{i \in I} C\right)$. Niech $b_k$ będzie taka, że $a_k$ jest jej obrazem. Zatem $b_k = (\phi_{ij}^k)$, gdzie $1 \leq i, j \leq n$, zaś $\phi_{ij} \in \prod C$. Niech $\alpha(t_{ij}^k) = \phi_{ij}^k$. Zatem $\alpha(y^{(k)})$ jest macierzą o wyrazach $\phi_{ij}^k = b_k$. Zatem $M_n(\alpha)$ jest homomorfizmem macierzy $M_n(t_{ij}^k)$ w $M_n(\prod C)$. Jedyność tego homomorfizmu jest podobno prosta. ■

Ciekawe jest to, że nasza algebra wolna zanurza się w macierze nad pierścieniem przemiennym.

**Twierdzenie 4.55** *Niech $C$ będzie noetherowską dziedziną nieskończoną, zaś $A$ niech będzie $C$-algebrą skończenie generowaną przez elementy $a_1, \ldots, a_n$. Dla każdego $n \geq 1$ algebra $A$ spełnia warunek maksymalności na takie ideały $J$, że $A/J \subseteq M_n(D)$, gdzie $D$ jest $C$-algebrą przemienną.*

[2] Wynika stąd, że $U(C, n, d)$ jest wolna w klasie algebr spełniających wszystkie tożsamości spełniane w klasie $C$-algebr.

**Wniosek 4.56** *Niech $C$ będzie ciałem nieskończonym. Wówczas każda skończenie generowana PI algebra spełnia warunek maksymalności na ideały półpierwsze.*

Dowód. Niech $A$ spełnia tożsamość znormalizowaną stopnia $n$. Jeśli $I$ jest ideałem półpierwszym w $A$, to $A/I$ zanurza się w macierze stopnia r/2 o współczynnikach przemiennych. ∎

**Wniosek 4.57** *Niech $C$ będzie ciałem nieskończonym i $A$ – PI algebrą skończenie generowaną nad $C$. Wówczas każdy ideał półpierwszy jest przecięciem skończonej liczby ideałów pierwszych.*

Przypuśćmy, że $I \triangleleft A$ jest półpierwszy i nie jest częścią wspólną skończonej liczby ideałów pierwszych. Możemy założyć, że $I$ jest maksymalny o tej własności. Wiadomo, że $I$ nie jest w szczególności ideałem pierwszym. Istnieją więc ideały $J, K \triangleleft A$, że $I \subsetneq J, I \subsetneq K$, ale $JK \subseteq I$. Mamy $(J \cap K)^2 \subseteq JK \subseteq I$. Zatem z półpierwszości $J \cap K = I$. Mogę powiększyć ideały $J, K$ aby były półpierwsze. (Gdyby $L^2 \subseteq K$ oraz $K \subseteq L$, to $(JL)^2 \subseteq J \cap K = I$, z półpierwszości $I$, mamy $JL \subseteq I$. ) Z wyboru $I$ wynika, że $J, K$ są skończonymi przecięciami ideałów pierwszych, a wobec tego $I$ też jest.

**Twierdzenie 4.58** *Jeśli $K$ jest ciałem nieskończonym oraz $n, d \geq 1$, to algebra $U(K, n, d)$ jest dziedziną. Dziedzina ta ma algebrę centralnych ułamków, która jest algebrą z dzieleniem. Nazywamy ją* ***uniwersalną algebrą z dzieleniem*** *$U(D(K, n, d))$.*

**Twierdzenie 4.59 (1958)** *Niech $R$ będzie pierścieniem pierwszym. Wówczas $R$ ma klasyczny lewostronny pierścień ułamków (powstający przed odwracanie elementów regularnych) izomorficzny z $M_n(D)$, gdzie $D$ jest z dzieleniem wtedy i tylko wtedy, gdy spełnia lewostronne warunki Goldiego.*

**Twierdzenie 4.60 (Posner 1960)** *Niech $R$ będzie pierwszym PI-pierścieniem. Wówczas $R$ spełnia lewostronne i prawostronne warunki Goldiego i ma klasyczny pierścień ułamków, który też jest PI.*

**Definicja 4.61 (Ułamki Martindale'a)** *Niech:*

$$\mathcal{F} = \{(I, \alpha) \mid I \triangleleft R \text{ oraz } \alpha \in Hom_R(I_R, R_R)\}.$$

*Powiemy, że $(I, \alpha) \sim (J, \beta)$ gdy $\alpha = \beta$ na $0 \neq K \subseteq I \cap J$, $K \triangleleft R$. Dla $a \in R$, mamy elementy $(R, \alpha_a)$. Aby w $F/\sim$ nie zlepiały się $a, b \in R$, to dla dowolnego $0 \neq K \triangleleft R$ powinno być $lann(K) = 0$, bo $(R, \alpha_a) \sim (R, \alpha_b) \Leftrightarrow a - b \in lann(K)$, dla pewnego $0 \neq K \triangleleft R$.*

**Definicja 4.62** ***Lewostronnym (klasycznym) pierścieniem ułamków Ore'go*** *pierścienia $R$ nazywamy pierścień $Q(R)$ taki, że:*

1. *$R$ jest podpierścieniem $Q(R)$*

2. *każdy element regularny pierścienia $R$ jest odwracalny w $Q(R)$*

3. *każdy element $x \in Q(R)$ jest postaci $x = r^{-1}s$, gdzie $r, s \in R$ oraz $r$ jest regularny.*

**Definicja 4.63** *Pierścień $R$ spełnia* ***lewostronny warunek Ore'go*** *$\Leftrightarrow$ dla każdych $a, b \in R$ takich, że $b$ jest regularny istnieją takie $a_1, b_1 \in R$, gdzie $b_1$ jest regularny, t.że $b_1 a = a_1 b$.*

**Twierdzenie 4.64 (Ore)** *Pierścień $R$ posiada lewostronny klasyczny pierścień ułamków Ore'go wtedy i tylko wtedy, gdy $R$ spełnia lewostronny warunek Ore'go.*

Dowód. Załóżmy, że pierścień $R$ posiada klasyczny pieścień ułamków. Wówczas jeśli $a, b \in R$ przy czym $b$ – regularny, to $a, b \in Q(R)$, oraz $b^{-1} \in Q(R)$, a więc $ab^{-1} \in Q(R)$. Stąd istnieją takie $a_1, b_1$, przy czym $b_1$ jest regularny:

$$b_1^{-1} a_1 = ab^{-1} \Rightarrow a_1 b = b_1 a.$$

Załóżmy teraz, że spełniony jest lewostronny warunek Ore'go. Wykonujemy serię kroków.

- Zaczynamy od pewnych własności elementów regularnych w $R$. Nazywamy je $M$. Zauważmy, że jeśli $a, b$ są regularne, to ich iloczyn też.
- Relacja równoważności jest taka. niech $P = M \times R$. Wówczas mamy pary: $(a, b) \sim (c, d)$ wtedy i tylko wtedy, gdy istnieją takie $a_1, c_1 \in M$, ze $c_1 a = a_1 c$ i $c_1 b = a_1 d$. Dowodzimy dalej, że jest to relacja równoważności. Dalej natomiast określamy działania i wykonujemy serię koszmarnie interesujących sprawdzeń.

■

Na koniec powiemy kilka słów o lemacie Posnera. Najpierw kilka definicji:

**Definicja 4.65** *Powiemy, że $R$ spełnia* ***acc na lewostronne anihilatory****: każda niepusta rodzina anihilatorów lewostronnych ma element maksymalny.*

**Definicja 4.66** ***Lewostronnym pierścieniem Goldiego*** *nazywamy pierścień spełniający następujące warunki:*

- *$R$ spełnia acc na lewostronne anihilatory*
- *każda suma prosta niezerowych lewostronnych ideałów w $R$ jest skończona (alt. wymiar Goldiego jest skończony)*

**Twierdzenie 4.67 (Goldie)** *Niech $R$ będzie pierścieniem, $S$ – zbiór elementów regularnych w $R$. NSWR:*

- *$R$ ma prawostronny pierścień klasycznych ułamków Orego $R_S$ – (pół)prosty artinowski, a więc postaci $M_n(D)$ – z dzieleniem (suma...)*
- *$R$ jest prawostronnie Goldiego i (pół)pierwszy*

Informacja o tym, że pierwszy PI jest Goldiego byłaby więc nie do przecenienia...

**Twierdzenie 4.68 (Posner)** *Następujące warunki są równoważne:*

- *$R$ jest pierwszym PI pierścieniem*
- *$R$ ma dwustronny pierścień ułamków $M_n(D)$, $D$ – z dzieleniem*